AVAYA

Avaya Device Adapter Snap-in Reference

Contents

Contents

Contents

Comments on this document? infodev@avaya.com

Comments on this document? infodev@avaya.com

Comments on this document? infodev@avaya.com

Chapter 1: Introduction

Purpose

This document describes the characteristics and capabilities of Avaya Device Adapter Snap-in, including overview and feature descriptions, interoperability, and performance specifications. It also provides instructions on how to configure and troubleshoot Avaya Device Adapter Snap-in. People who need to install and configure this snap-in; for example, administrators will find this guide useful.

Change history

The following changes are made to this document since the last issue:

Issue	Date	Summary of changes
5	October 2020	For Release 8.1.3, added the following sections and topics: • Added the following topics under Virtual Office section in "Appendix H: Call processing features and services": • <u>VO DVLA Timer</u> on page 583 • <u>DVLA logout timer</u> on page 584 • <u>DVLA timer reset</u> on page 585 • <u>Difference between VOLO and DVLA phones</u> on page 585 • <u>Configuring SM for making emergency calls from a DVLA phone</u> on page 589 • Added the following new chapter: - Appendix I: Avaya SBCE configuration for Device Adapter • Added the following topics in "Appendix J: Legacy Avaya Aura® SIP endpoint feature and Communication Manager feature support": • <u>Limit Number of Concurrent Calls (LNCC)</u> on page 620 • <u>Configuring LNCC on CS1000</u> on page 620 • Added the following topic in "Appendix K: CS 1000 FFC and Communication Manager FAC mapping": • <u>CS2100</u> on page 638 For Release 8.1.3, updated the following topics: • Updated the following topic <u>Administering an analog station with the hotline target as a digit string</u> on page 471 in "Appendix H: Call processing features and services". • Updated the following topic <u>Service Attributes</u> on page 157 for additional fields in IP Security (IPSec), Daylight Saving Rules, Virtual Office/ Emergency Calls and Remote Cluster features • Updated the following topic <u>Configuring Virtual Office support for Device Adapter UNIStim endpoint</u> on page 585 for the VO DVLA Timer feature. • Updated the following topic <u>Configuring Session Manager to make emergency calls from a VO logged out phone</u> on page 588 for the VO DVLA feature.

Table continues…

Issue	Date	Summary of changes

4	March 2020	For Release 8.1.2, added the following chapters, sections, and topics:
		
		• Supported phone types in an Avaya Aura Call Center Elite environment on page 55
		
		• Cluster considerations for a call center environment on page 142
		
		• CS 1000 call center capabilities and features supported by Avaya Device Adapter Snap-in for Call Center Elite on page 51
		
		• Added the following new chapters and added topics under it:
		
		  - Chapter 8: Administration of call center feature buttons for Device Adapter phones
		
		  - Created Chapter 9: CTI controlled phones in call centers
		
		• Added the "User experience differences for call center features" section and added topics under it.
		
		• IPv6 support on page 69
		
		• Added the following sections and added topics under it in "Appendix H: Call processing features and services":
		
		  - Auto-Answer
		
		  - Private Line Service
		
		  - Group Paging
		
		  - Loudspeaker paging
		
		  - Sequential Registration and MDA in a Call Center Elite environment on page 539
		
		• Added the following topics under the "User experience differences for UC call processing features and services" section:
		
		  - Auto-Answer on page 668
		
		  - Private Line Service on page 705
		
		  - Group Paging on page 684
		
		  - Loudspeaker paging on page 689
		
		• Migrating the Personal Directory data from Device Adapter 8.1.1 and earlier to 8.1.2 on page 189
		
		• Added the following topics under the "NT1R20 Off-Premise Station Analog Line card" section:
		
		  - About NT1R20 Off-Premise Station Analog Line card on page 650
		
		  - Configuring NT1R20 OPS analog line card on page 650
		
		• Added the following topics for context-sensitive soft keys for voice mail:
		
		  - Context-sensitive soft keys for voice mail on Device Adapter endpoints on page 409

Table continues…

Issue	Date	Summary of changes
		- Configuring context-sensitive soft keys for voice mail on Device Adapter endpoints on page 411
		• Considerations before downgrading Device Adapter from Release 8.1.2 to Release 8.1.1 on page 190
		• Incorrect name and extension displayed on a CC phone after downgrading Device Adapter from Release 8.1.2 to Release 8.1.1 on page 297
		• Added the Planning for Avaya Breeze platform and Device Adapter upgrades on page 173 topic and added topics under it.
		For Release 8.1.2, updated the following topics:
		• Frequently asked questions on page 36
		• Updated the following topics for storing Personal Directory data in PPM:
		- Importing Personal Directory data for UNIStim endpoints from CS 1000 on page 123
		- Personal Directory issues on page 284
		• Service attributes on page 157
		• Updated the following topic for the `ada-report` command:
		- Collecting debug logs for Device Adapter and Avaya Breeze platform on page 280
		• Updated the following topic for the `tnInfo` command:
		- Maintenance commands on page 250
		• Cluster considerations for a Unified Communications environment on page 141
		• CS 1000 telephony features supported by Avaya Device Adapter Snap-in on page 48
		• Updated the High Availability and Geo-Redundancy on page 73 topic and topics under it.
		• Updated the CS 1000 endpoints migration using ProVision and Nortel Migration Tool on page 97 topic and topics under it.
		• Updated the topics under Multi-Device Access on page 493.
		• Updated the topics under Sequential Registration on page 529.
		• Updated the following topics for disabling IP security before upgrading the Avaya Device Adapter Snap-in:
		- Avaya Device Adapter Snap-in upgrade on page 184
		- Upgrading the Device Adapter Snap-in on page 185
		• Certificate handling on page 70

Table continues…

Issue	Date	Summary of changes

		• Updated the firmware version in Upgrading firmware and loadware on page 95.
		
		• Updated the following topics for the Ring Again feature limitation over the CO trunk:
		  - Ring Again on page 706
		  - Ring Again feature description on page 525
		Removed the following topic:
		• Functionality of Device Adapter sets as a CTI controlled AACC SIP endpoint

3	October 2019	For Release 8.1.1, added or updated the following topics for the respective features:
		
		• Call Forward All Calls on behalf of another user station feature:
		  - "Busy Indicator" section in "Appendix H: Call processing features and services"
		  - Busy Indicator on page 670
		• Virtual Office feature:
		  - "Virtual Office" section in "Appendix H: Call processing features and services"
		  - Virtual Office on page 718
		• Support for pcap commands:
		  - Troubleshooting commands on page 257
		• Device Adapter phones as CTI controlled phones in Avaya Aura® Contact Center:
		  - Functionality of Device Adapter sets as a CTI controlled AACC SIP endpoint
		• Support for `daHelp` command:
		  - Viewing the list of Device Adapter maintenance and troubleshooting commands on page 250
		• Filtering of dsa log components:
		  - Setting the filter for DSA log components on page 279
		• Updated the following topics for enhancement in the `mgcShow` command:
		  - Maintenance commands on page 250
		  - Troubleshooting MGC connection problems on page 304

Table continues…

Issue	Date	Summary of changes
2	July 2019	For Release 8.1 Issue 2, updated the following topics: • Moved the licensing information from the "What licensing is required for Device Adapter?" section to Licensing on page 82. • Updated the "Performance and capacity constraints and requirements" topic for information about the maximum number of Device Adapter endpoints in a cluster. • Updated Overview of Avaya Breeze platform and Avaya Device Adapter Snap-in upgrade on page 172. • Updated Checklist for upgrading the Avaya Breeze platform and Device Adapter snap-in in a geo-redundant model on page 187. • Updated Checklist for upgrading the Avaya Breeze platform for a Device Adapter snap-in on page 181.
1	June 2019	Release 8.1 document.

Prerequisites

Administrators who deploy and administer the Avaya Device Adapter Snap-in must have a working knowledge of Avaya Breeze® platform and Avaya Aura®.

Intended audience

This document is intended for people who need to install and configure Avaya Device Adapter Snap-in. This document contains specific information about this snap-in.

Chapter 2: Avaya Device Adapter Snap-in Overview

Avaya Device Adapter Snap-in Overview

Avaya Device Adapter Snap-in is a modular, reusable solution that enables Unified Networks IP Stimulus (UNIStim) IP, digital, and analog phones that are used as Unified Communications (UC) phones and that work with Avaya Communication Server 1000 (CS 1000) to migrate to Avaya Aura® without significant investment on the existing infrastructure. Device Adapter offers a feasible solution to CS 1000 customers to take advantage of Avaya Aura® features while minimizing expenses on the cables and hardware.

Device Adapter is deployed on the Avaya Breeze® platform. A Device Adapter node runs on an Avaya Breeze® platform cluster that can have one or more Avaya Breeze® platform servers. A standard deployment solution has one or more Avaya Breeze® platform clusters. Implementing Device Adapter does not introduce any new hardware. Device Adapter works as a part of the Avaya Breeze® platform solution.

In this deployment, phone sets are connected to Device Adapter by replacing CS 1000. For SIP signaling and terminal registration of phone sets, Device Adapter is connected to Avaya Aura® Session Manager. Session Manager communicates with Avaya Aura® Communication Manager to provide call-related services to the terminals. Device Adapter communicates with Avaya Aura® System Manager for management operations as available in a typical Avaya Aura® deployment.

To support analog and digital/TDM set migration, Media Gateway Controllers (MGC) or Media Gateway Extended Peripheral Equipment Controllers (MG-XPEC) must be in place to drive the Digital/Analog Line Cards. Only Intelligent Peripheral Equipment (IPE) Digital/Analog Line cards are supported.

Device Adapter support in an Avaya Aura® Call Center Elite environment

Device Adapter Release 8.1.2 supports migration of call center (CC) endpoints that are used in an Avaya Aura® Call Center Elite environment and that work with a CS 1000 environment to Avaya Aura®. Device Adapter retains the Call Center Elite functions on these endpoints and provides a near CS 1000 user experience to the call center agents and supervisors.

Device Adapter supports only 1140e (1140) IP phone and i2050 (2050) soft phone in a call center environment.
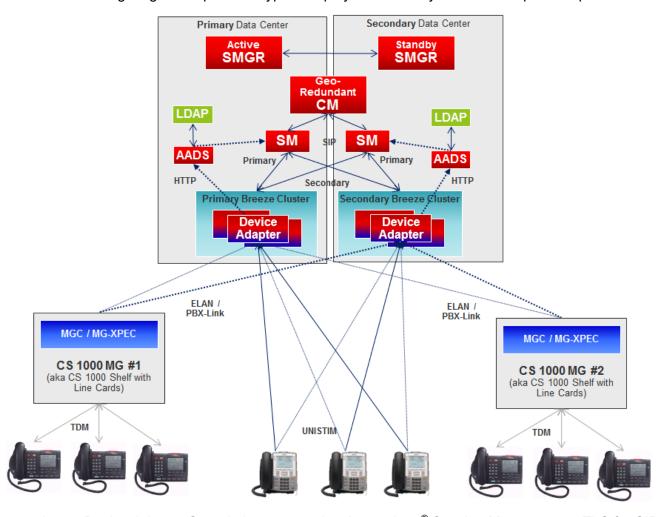
Customers can use these phones either as Unified Communications (UC) or Call Center (CC) phones in their call center environment. When a call center agent or supervisor logs in to the phone, the phone operates as a CC phone and provides the call center features. Otherwise, it

operates as a UC phone. Customers can also use these phones exclusively as UC phones in their call center environment.

Device Adapter for call center does not support any services that are not supported by a 96x1 SIPCC endpoint.

Architecture and topology

The following diagram depicts the typical deployment of Avaya Device Adapter Snap-in.

Avaya Device Adapter Snap-in is connected to Avaya Aura® Session Manager over TLS for SIP signaling. Session Manager works with Avaya Aura® Communication Manager for call services and Avaya Aura® System Manager for management traffic.

The CS 1000 UNIStim endpoints and Media Gateways connect to Avaya Device Adapter Snap-in over the IP network. The snap-in then presents these endpoints as Avaya SIP Telephony (AST) sets to Session Manager. The Personal Directory for UNIStim endpoints migrates to Avaya Device Adapter Snap-in. Corporate directory support for UNIStim and digital endpoints using Avaya Aura® Device Services (AADS) is optional.

New in this release

What's new in Avaya Device Adapter Release 8.1.3

Device Adapter Release 8.1.3 provides the following new capabilities:

- Supports additional Idle time interval range for DVLA phones before automatic virtual office logout functionality in the **Virtual Office/Emergency Calls** section.

- Supports Avaya SBCE setup with Device Adapter end users by implementing the **Remote Cluster** feature thereby overriding user defined Session Manager addresses for all Device Adapter endpoints.

- Supports activation and deactivation of the **LimitInCalls** feature key on the CS 1000 phones for the Limit Number of Concurrent Calls (LNCC) feature.

- With Release 8.1.3, you can use Device Adapter to manage phones migrated from the CS 2100 product.

What's new in Avaya Device Adapter Release 8.1.2

Device Adapter Release 8.1.2 provides the following new capabilities:

- Supports Call Center Elite features and capabilities on a limited subset of Device Adapter phones.

  Call Center Elite agents and supervisors can use these phones to perform both UC and call center-specific operations.

- Supports Avaya Workspaces CTI application with Call Center Elite.

- Supports Avaya Workspaces and Avaya Aura® Agent Desktop CTI applications with Avaya Aura® Contact Center.

- Allows phones to be CTI controlled in a call center environment.

- Supports IPv6 between Device Adapter and the Avaya Aura® components.

- Supports the Private Line Service (PVR/PVN) feature.

- Supports the `ada-report` command, which provides the Device Adapter and Avaya Breeze® platform logs in one .zip file.

- Supports the `tnInfo` command, which displays a list of TNs of the Device Adapter endpoints that are configured in System Manager.

- Supports multiple node IDs and System IDs on one Avaya Breeze® platform cluster during migration of endpoints from CS 1000 to Avaya Aura®.

- Stores Personal Directory data in the PPM instead of the Cluster database of Avaya Breeze® platform for Data Privacy.

- Avaya Breeze® platform restart is not required if you modify any of the Avaya Breeze® platform trusted certificates after Device Adapter is installed.

- Supports NT1R20 off-premise station analog line cards.

- Supports the Group Paging feature.

- Supports the Auto-Answer feature.

- Supports context-sensitive soft keys for voice mail on UNIStim IP desk phones and 3900 series digital desk phones.

What's new in Avaya Device Adapter Release 8.1.1

Device Adapter Release 8.1.1 provides the following new capabilities:

- Supports the Communication Manager operation of managing Call Forward All Calls (CFW) from a user extension on behalf of another user extension.

  A user can use the CFW feature along with the Busy Indicator feature to manage CFW on behalf of another user extension.

- Supports the Virtual Office (VO) feature that allows a user to log in at a guest station by using VO credentials.

- Allows a VO user to make an emergency call irrespective of whether the VO user is logged in or logged out of the phone.

- Supports the following CS 1000 pcap commands to monitor network packets that are sent and received by the network interfaces of the Avaya Breeze® platform: `pcapHelp`, `pcapStart`, `pcapStop`, `pcapStatus`, `pcapRestart`, `pcapConfigShow`, and `pcapConfig`.

- Allows all Device Adapter UNIStim, analog, and digital endpoints to be used as CTI controlled SIP endpoints for Avaya Aura® Contact Center.

- Supports the `daHelp` command that displays a list of Device Adapter-specific maintenance and troubleshooting commands at the Avaya Breeze® platform CLI interface.

- Supports filtering of the DSA log components.

- The `mgcShow` command now also shows the type of the registered controllers; for example, MGC or MG-XPEC, and the number of voice gateways; that is, DSP resources that can be allocated to the TDM stations.

What's new in Avaya Device Adapter

This chapter provides an overview of the new and enhanced features of Avaya Device Adapter Release 8.1.x.

For more information about these features and administration, see the *Avaya Device Adapter Snap-in Reference* guide.

Avaya Device Adapter feature matrix

The following table lists the feature matrix of Avaya Device Adapter.

⊛ **Note:**

The feature list is not a comprehensive feature list.

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3
Ad hoc conference	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Autodial	UNIStim	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital
Busy Indicator	Not supported	Not supported	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital
Call Forward All Calls (CFW) along with the Busy Indicator feature to manage CFW on behalf of another extension	Not supported	Not supported	Not supported	UNIStim[1], Digital[1] This feature is not supported on 2001 and 3901 endpoints.	UNIStim1, Digital1 This feature is not supported on 2001 and 3901 endpoints.	UNIStim1, Digital1 This feature is not supported on 2001 and 3901 endpoints.
Call Forward - all calls / busy / no answer	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Caller List / Redial List / Personal Directory	UNIStim	UNIStim, Digital[1]	UNIStim, Digital[1]	UNIStim, Digital[1]	UNIStim, Digital[1]	UNIStim, Digital[1]
Call Pickup (Directed / Group / Ringing Number)	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Call Park and Call Pickup	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Call Waiting	UNIStim	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital
Corporate Directory	Not supported	UNIStim[1], Digital[1]	UNIStim[1], Digital[1]	UNIStim[1], Digital[1]	UNIStim[1], Digital[1]	UNIStim[1], Digital[1]

Table continues…

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3
Context-sensitive key access - idle / offhook / dialed / ringing / active call state	UNIStim	UNIStim, Digital[1]	UNIStim, Digital[1]	UNIStim, Digital[1]	UNIStim, Digital[1]	UNIStim, Digital[1]
End-to-end signaling (DTMF)	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Fixed feature key access	UNIStim	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital
Hold / retrieve	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Hot Line - multiple types on CS 1000	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Last Number Redial	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Making, answering, and releasing a basic call	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Make Set Busy	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Malicious Call Trace	Not supported	Not supported	UNIStim, Digital	UNIStim, Digital	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Message Waiting Indication (including audio)	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Message Waiting Key and Lamp for voice mail	UNIStim	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]
Multiple Appearance Directory Numbers (MADN)	UNIStim	UNIStim, Digital, Analog[2]	UNIStim, Digital, Analog[2]	UNIStim, Digital, Analog[2]	UNIStim, Digital, Analog[2]	UNIStim, Digital, Analog[2]

Table continues…

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3
Multiple Device Access: Allows concurrent registrations of a minimum of 2 up to a maximum of 10 SIP devices with the same extension. However, Avaya recommends that out of the 10 devices, only 1 device should be a Device Adapter UNIStim endpoint.	Not supported	Not supported	UNIStim	UNIStim	UNIStim	UNIStim
Release key - disconnect a call	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Ring Again	UNIStim	UNIStim, Digital	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Set Display - calling / called / redirecting name and number.	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Set Display - time and date, call timer, and so on.	UNIStim	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]	UNIStim, Digital, Analog[1]
Speed Dial	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Sequential Registration: Allows registration of only one endpoint at one time.	UNIStim[3]	UNIStim[3], Digital[3], Analog[3]	UNIStim[4], Digital[3], Analog[3]	UNIStim[4], Digital[3], Analog[3]	UNIStim[4], Digital[3], Analog[3]	UNIStim[4], Digital[3], Analog[3]

Table continues…

Avaya Device Adapter Snap-in Reference

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3
Support for 50 Avaya Breeze® platform nodes and 2,00,000 endpoints.	Support for 35 Avaya Breeze® platform nodes.	50 Avaya Breeze® platform nodes retroactively supported.	Yes	Yes	Yes	Yes
SMGR IU for Device Adapter	No	Yes	Yes	Yes	Yes	Yes
SMGR IU for Media Gateway	No	Yes	Yes	Yes	Yes	Yes
Transfer - blind as well as consultative	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Privacy Release	UNIStim	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Presence Service Notification: Provides presence status indication to non-Device Adapter endpoints	Not supported	Not supported	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog	UNIStim, Digital, Analog
Virtual Office (VO)	Not supported	Not supported	Not supported	UNIStim with soft keys The endpoint must support Home and Virtual soft keys.	UNIStim with soft keys The endpoint must support Home and Virtual soft keys	UNIStim with soft keys The endpoint must support Home and Virtual soft keys
Virtual Office Emergency dialing	Not supported	Not supported	Not supported	UNIStim with soft keys The endpoint must support Emergency soft key.	UNIStim with soft keys The endpoint must support Emergency soft key	UNIStim with soft keys
Virtual Office DVLA Timer	Not supported	Not supported	Not supported	Not supported	Not supported	UNIStim with soft keys
Remote Cluster	Not supported	Not supported	Not supported	Not supported	Not supported	UNIStim
Limit Number of Concurrent Calls (LNCC)	Not supported	Not supported	Not supported	Not supported	Not supported	UNIStim

Table continues…

Features	Release 8.0	Release 8.0.1	Release 8.1	Release 8.1.1	Release 8.1.2	Release 8.1.3
CS2100	Not supported	Not supported	Not supported	Not supported	Not supported	UNIStim, Digital, Analog

[1] Applies to a subset of the set types. For example, Digital[1] may apply to the 39xx phones, that is, 3903, 3904, and so on.

[2] Analog stations may have a MADN assigned, but have only one available line appearance. Digital and UNIStim stations may have one or more line appearances for the directory number.

[3] Used for recovery in an event of a network failure.

[4] In addition to providing recovery in an event of a network failure, can also be used for switching between UNIStim endpoints.

Frequently asked questions

What is Device Adapter? What does it do?

Device Adapter is an Avaya Breeze® platform snap-in that acts as a protocol converter between UNIStim IP, digital, and analog devices and an Avaya Aura® solution. Devices are serviced by the Avaya Aura® solution by converting the proprietary signaling to Avaya SIP.

What is the main benefit of Device Adapter?

Device Adapter enables deployed UNIStim IP, digital, and analog devices to be reused in an Avaya Aura® solution.

What is the terminology used in this document to differentiate between the SIP endpoint families for programming?

- UNIStim desk phones can be either CS1K-IP SIP endpoints (UC endpoints) or CS1K-IPCC SIP endpoints (call center endpoints).
- Digital desk phones are subdivided into three families of SIP endpoints:
  - M3900 series digital desk phones are programmed as CS1K-39XX endpoints.
  - M2216 and M2616 digital desk phones are programmed as CS1K-2COL endpoints. Note that 2COL represents the two columns of 8 keys on these desk phones.
  - M2006 and M2008 digital desk phones are programmed as CS1K-1COL endpoints. Note that 1COL represents the single column of 6 or 8 keys on these desk phones.
  - European digital desk phones conform to this endpoint nomenclature as well, based on the number of key/lamp strips.
- Analog desk phones are CS1K-ANA SIP endpoints.

What is the terminology used in the document to differentiate between a physical desk phone and a SIP endpoint?

- UNIStim phones:

  - Desk phone nomenclature:

    - The terms "UNIStim desk phone" or "UNIStim phone" are used to refer to the UNIStim IP desk phone family.

    - The terms "UNIStim desk phone" or "UNIStim phone" are used along with the model number to refer to a specific UNIStim IP desk phone. For example, UNIStim 1140e desk phone or UNIStim 1140e phone.

  - SIP entity nomenclature:

    - The term "UNIStim endpoint" is used to refer to the family of UNIStim IP desk phones as SIP entities.

    - The term "UNIStim endpoint" is used along with the model number to refer to a specific UNIStim SIP entity variant. For example, UNIStim 1140e endpoint or UNIStim 1140 endpoint.

      Note that the "e" in 1140e refers to the desk phone being used with IP (the Ethernet). Similarly, the prefix "I", which stands for IP, is often not added to the i2000 series phones.

- M3900 series digital desk phones:

  - Desk phone nomenclature:

    - The terms M3900 series digital desk phone, M3900 series desk phone, M3900 phone, or M3900 are used to refer to the family of M3900 series digital desk phones.

    - The terms M3900 series digital desk phone, M3900 series desk phone, M3900 phone, or M3900 are used along with the model number to refer to the specific M3900 phone models. For example, M3904 phone or 3904 phone.

  - SIP entity nomenclature:

    - The terms 39XX endpoint, 39xx endpoint, or CS1K-39XX are used to refer to the family of M3900 series digital desk phones as SIP entities.

    - The terms 39XX endpoint, 39xx endpoint, or CS1K-39XX are used along with the model number to refer to a specific M3900 SIP entity variant. For example, M3904 endpoint or 3904 endpoint.

  - All other digital desk phones:

    - The 1COL and 2COL phones are not usually described as families. These phones were part of the Aries family in CS 1000.

    - The terms "2616 phones" or "2616 desk phones" are used to refer to desk phones.

    - The term "2616 endpoint" is used to refer to the SIP entity.

A multi-line digital or UNIStim phone on CS 1000 can be assigned multiple numbers (extensions). How do I configure the same functionality on Communication Manager? Are there licensing implications?

Each Device Adapter endpoint must be associated with a Communication Manager station. A Communication Manager station is administered with a single number/extension. If an additional

number/extension must be associated with a Communication Manager station, the station has to "bridge" the number of another Communication Manager station by means of the bridged appearance button. This means that another Communication Manager station must be administered with the desired number as the extension. So, for every distinct number/extension used on a multi-line phone, there must be a Communication Manager station administered that has the extension of that number. Note that several stations can bridge the same number. Also note that the bridging can be administered in a Single Call Arrangement (SCA) mode (using the "regular" Communication Manager bridged appearance button) or in a Multiple Call Arrangement (MCA) mode (using the "MCA" Communication Manager bridged appearance button). This may have licensing implications. If a set of numbers/extensions is larger than the set of physical phones sharing them, additional Suite Licenses are required to administer the so-called phantom or "X-Port" stations to "host" the extra numbers/extensions.

What are the options for deploying Device Adapter?

Device Adapter is deployed co-resident with Avaya Aura® on premise or in the Cloud with an option for remote site deployment for local survivability. For more information, see the following topics:

- Device Adapter and Avaya Aura On Premises on page 59
- Device Adapter and Avaya Aura in the Cloud on page 60
- Device Adapter On Premises and Avaya Aura in the Cloud on page 58
- Device Adapter deployment for Local Survivability on page 61
- Device Adapter support for Amazon Web Services on page 62

How is local survivability configured?

Local survivability requires the Device Adapter and Avaya Breeze® platform instances to be deployed co-resident with Branch Session Manager and the local gateway. Device Adapter registers to Branch Session Manager for continued service if connectivity to the primary and secondary Session Managers becomes unavailable. For more information, see Device Adapter deployment for Local Survivability on page 61.

Can Device Adapter be deployed on a General-Purpose Avaya Breeze® platform cluster with other snap-ins?

Device Adapter is a CPU-intensive, call processing application. Device Adapter must be deployed on a Core Platform cluster only. Only Device Adapter snap-in and selected Avaya-developed snap-ins such as CallEventController and EventingConnector can be installed. Device Adapter snap-in cannot be co-resident with any other snap-in on this cluster type.

How is data migrated from CS 1000 to an Avaya Aura® solution?

Avaya ProVision is used to migrate the CS 1000 endpoint information to the Avaya Aura® solution. Avaya ProVision can do the following:

- Create a data set corresponding to a CS 1000 instance by collecting data from the running instance.
- Create a data set corresponding to a Communication Manager instance by collecting data from the running instance.
- Migrate stations from a CS 1000 solution to an Avaya Aura® solution on a group-by-group basis.

> ✱ **Note:**
>
> All members of a groups should be migrated during the same step, and to the same Communication Manager instance, to preserve group features such as Multiple Appearance Directory Numbers (MADN).

> ✱ **Note:**
>
> - The class of service (CLS) of CS1K_IPCC stations is AGN or SPV.
>
> - The stations belonging to multiple CS 1000 instances can be migrated to the same Communication Manager instance if sufficient Communication Manager capacity exists. Avaya ProVision provides a directory number prefixing mechanism to resolve directory number conflicts, and TN replacement mechanism to avoid TN conflicts. However, you may still encounter TN conflicts.
>
>   Till Device Adapter Release 8.1.1, this TN conflict could be resolved by configuring the appropriate System ID and deploying multiple Device Adapter instances.
>
>   In Device Adapter Release 8.1.2, you can migrate endpoints from multiple CS 1000s to a single Avaya Breeze® platform cluster. This is because ProVision of the latest release, which is used with Device Adapter Release 8.1.2, allows you to modify the TNs during migration.

- ProVision creates System Manager Managed Elements for Media Gateway Controllers.

What licensing is required for Device Adapter?

For information about the licensing required for Avaya Device Adapter Snap-in, see

How is an endpoint associated with a Device Adapter cluster?

Device Adapter is deployed on a cluster of Avaya Breeze® platform servers referred to as the Device Adapter cluster.

A CS 1000 endpoint is associated with the whole Device Adapter cluster by associating the Cluster IP with the S1 (primary) and S2 (secondary) server values of the endpoint. This association between an endpoint and Device Adapter cluster is not administered in System Manager. The endpoint can then register with any Device Adapter cluster by changing the Cluster IP in the S1 Server or S2 Server settings.

> ✱ **Note:**
>
> The SecureLink IP is used instead of the Cluster IP in single server deployments.

> ❗ **Important:**
>
> A Device Adapter cluster is allocated to a specific CS 1000 system. All endpoints registered to the cluster must belong to the CS 1000 system allocated to the cluster.

Can an endpoint be associated with more than one Device Adapter cluster?

A CS 1000 endpoint can be associated with a maximum of two clusters, the primary and secondary Device Adapter cluster. This is achieved through the S1 (primary) and S2 (secondary) server settings. Each cluster consists of multiple Avaya Breeze® platform servers and nodes.

Registration with the primary cluster provides high availability failover from a single node failure. Registration with the secondary cluster provides geographic redundancy. Existing calls are preserved but cannot be modified after the originally registered node fails.

Are endpoints able to connect to different Device Adapters simultaneously?

An endpoint is registered to a single Device Adapter server in a Device Adapter cluster at any one time. The endpoint registers with another server in the cluster if the connected registered server or the link to the server fails. The endpoint registers with the secondary Device Adapter cluster if none of the servers in the primary cluster are available.

Does Device Adapter require user provisioning information from System Manager?

Yes. Device Adapter requires user provisioning information from System Manager.

How is Device Adapter administered?

System Manager provides a graphic interface to administer Device Adapter. The Avaya Breeze® platform section of System Manager is used to create the Avaya Breeze® platform cluster, install the snap-in, and administer all attributes. Media Gateways are administered as Managed Elements in System Manager.

Can multiple Device Adapter instances be deployed to accept overlapping TNs to support two CS 1000 systems consolidating to one Communication Manager?

There are two ways to perform a migration where several CS 1000 systems are migrated to the same Avaya Aura® solution.

1. The TN space of the migrated systems is manually merged in such way that any overlap of endpoint TNs is eliminated.

   • This may require a lot of manual administrative changes.

   • This assumes that the desired capacity can be achieved using a single TN space.

   • A single Device Adapter cluster can be used for all CS 1000 systems.

     * **Note:**

       A single Device Adapter cluster using multiple CS 1000 system leads to Terminal Number overlap.

   • This assumes that the desired capacity can be achieved using a single Device Adapter cluster.

2. The TN space on each CS 1000 system is left as is even though there might be overlaps in usage of endpoint TNs.

   • This avoids the need for the manual TN space merger.

   • This requires deployment of a dedicated Device Adapter cluster for each migrated CS 1000 system.

   • This migration solution has better scalability.

3. When collapsing multiple CS 1000 systems into a single Avaya Breeze® platform cluster, ProVision can be used to change TNs to avoid TN overlapping.

* **Note:**

The System ID, Loop, and Shelf value for each MGC in a solution should be unique.

How many endpoints are supported by a single Device Adapter node?

The capacity of a virtual machine running the snap-in depends on the resources reserved for the virtual machine and if any other snap-ins are deployed on the same Avaya Breeze® platform cluster.

In addition, the capacity of a virtual machine running the snap-in for a call center environment also depends on the capacities and capabilities of the call center. Because every call center environment is different, no fixed capacity rules can be defined. The figures provided in this section for a CC environment are guidelines for cluster considerations in a CC environment.

The capacity figures provided in this section apply when Device Adapter is the only snap-in installed on the cluster.

Cluster capacity for a UC environment:

- Up to 1000 endpoints per Device Adapter node running on an Avaya Breeze® platform Profile 2 virtual machine.
- Up to 5000 endpoints per Device Adapter node running on an Avaya Breeze® platform Profile 4 virtual machine.
- Up to 40 MGCs with digital or analog endpoints per Device Adapter node running on an Avaya Breeze® platform Profile 4 virtual machine.

  However, the number of endpoints, including the endpoints on the MGCs and the UNIStim endpoints, cannot exceed the maximum of 5000 on an Avaya Breeze® platform Profile 4 virtual machine.

Cluster capacity for a CC environment:

- Up to 1000 UC or 1000 CC endpoints, or a total of 1000 UC + CC endpoints per Device Adapter node running on an Avaya Breeze® platform Profile 2 virtual machine.
- Up to 5000 UC or 5000 CC endpoints, or a total of 5000 UC + CC endpoints per Device Adapter node running on an Avaya Breeze® platform Profile 4 virtual machine.

For more information, see

How many Device Adapter nodes are administered by a single System Manager pair?

In a solution managed by a single System Manager pair, the maximum number of Device Adapter nodes supported in an Avaya Breeze® platform cluster is 50.

This number is the same regardless of whether the Device Adapter nodes are on Avaya Breeze® platform profile 2 or 4. To the System Manager, it is the existence of the node and not its profile that has the impact.

How many Device Adapter clusters are administered by a single System Manager pair?

If each cluster has exactly one Device Adapter node, then there can be no more than 50 clusters because the maximum number of nodes supported is 50.

Cluster capacity is increased by adding Device Adapter nodes to the cluster. Adding nodes to a cluster also creates a high-availability environment where the failure of one node is compensated by the other cluster participants. The maximum number of nodes in a cluster is currently limited to 6 (5+1 for High Availability).

The total number of clusters administered by a single System Manager pair varies based on how many clusters are single node or High Availability (1+1, 2+1, 3+1, 4+1, or 5+1) clusters. These cluster sizes can be mixed, as long as the sum does not exceed a total of 50 virtual machine nodes.

Is an endpoint firmware upgrade required to use Device Adapter?

UNIStim and 39XX endpoints are upgraded to the latest supported firmware version the first time it connects to Device Adapter. Subsequent upgrades will also be handled by the snap-in.

Is a loadware upgrade required for Media Gateway Controllers to use Device Adapter?

Yes. There is a new Device Adapter-specific loadware that the MGC is upgraded to when the MGC connects to Device Adapter for the first time.

How does Device Adapter use the high availability features of Avaya Breeze® platform?

Device Adapter has two points of high availability support.

- High availability between endpoints and Device Adapter is part of Device Adapter:

  - For UNIStim endpoints, UNIStim endpoints handle the fail over.

  - For analog and digital endpoints, the MGC of the analog and digital endpoints handles the fail over.

- High availability between Device Adapter and the Avaya Aura® components, including Session Manager, is provided by Avaya Breeze® platform.

For more information, see

Device Adapter Release 8.1.1 and earlier used the Sequential Registration feature to provide fail-over support between Device Adapter and Avaya Aura® for endpoints. You can use the Multi-Device Access feature configuration fields, which is part of the Session Manager user profile configuration, to configure Sequential Registration.

To configure Sequential Registration, you must set the maximum number of simultaneously registered devices to 1, and allow new registrations. Sequential Registration allows only one device to be registered at one time.

In Sequential Registration, Session Manager terminates an existing registration when a new device registration request is received. Sequential Registration is crucial for providing endpoint fail-over support and other useful operations.

Sequential Registration provides the following fail over and operational support:

- An endpoint can re-register without waiting for the original SIP registration to fail. This fail-over mechanism minimizes the recovery time.

- Sequential Registration for UNIStim endpoint registration is supported since Device Adapter Release 8.0.

- Since Device Adapter Release 8.0.1, Sequential Registration also provides fail-over support for analog and digital endpoints that are on an MGC in an event of a network failure. However, the Sequential Registration feature itself is not supported for analog and digital endpoints.

For more information, see

Device Adapter 8.1.2 allows an improved recovery. Session Manager uses the device ID to identity an endpoint. In Release 8.1.2, irrespective of which Device Adapter node handles the endpoint, Device Adapter sends the same device ID to Session Manager during endpoint registration. In an event of the network failure when the endpoint fails over and tries to re-register, Session Manager processes the endpoint registration request as re-registration request through a different path because the device ID is the same. Session Manager does not wait for the original registration to fail to allow the re-registration. Hence, you can configure Sequential Registration to allow new registrations, although you may use the Sequential Registration configuration to block new registrations.

Regardless of the release, Device Adapter takes full advantage of the Avaya Breeze® platform clustering mechanism.

High Availability between Device Adapter and Avaya Aura®

The Avaya Breeze® platform clustering mechanism monitors the connection between Avaya Breeze® platform server and Session Manager. When an outage is detected, Avaya Breeze® platform server tries to fail over to another instance of the primary Session Manager. If the fail-over attempt at the primary Session Manager is not successful, Avaya Breeze® platform server tries to fail over to the alternate Session Manager. After the connection is established, Device Adapter initiates the re-registration request.

High Availability between Device Adapter and the endpoint by using the Avaya Breeze® platform load balancer and TPS capabilities

Installing Device Adapter on a cluster creates a Device Adapter cluster. The Device Adapter cluster is similar in function to a CS 1000 TPS Node. The Avaya Breeze® platform load balancing node is similar in function to the CS 1000 TPS Node Leader server and distributes the endpoint registrations over the nodes in the Device Adapter cluster. The Avaya Breeze® platform load balancing node binds to the Cluster IP. The Avaya Breeze® platform Cluster IP is analogous to the TPS Node IP.

If one of the Avaya Breeze® platform nodes fails or a network outage separates the endpoints from their current node, the endpoints that were registered on the failing node or on the failing LAN segment re-register through the load balancing node. The load balancing node distributes the endpoint registrations over the remaining nodes in the Device Adapter cluster. If there is an insufficient capacity – for example, the cluster was not set up as N+1 – the endpoints that are attempting to register fail to register. However, this behavior is also seen in CS 1000 when a number of TPS nodes fail and no alternate load balancing server was defined, resulting in the number of devices that require registration exceed the available capacity.

SIP registration by Device Adapter requires registering the endpoint to Session Manager. Normally, Session Manager allows one endpoint to register as a user identity.

When a network failure occurs, then:

- Till Device Adapter Release 8.1.1, the original endpoint registration through Device Adapter to Session Manager may not have failed yet; therefore, a new registration request fails. Sequential Registration resolved this registration delay by allowing Session Manager to force the original registration to end and register the new device before the failure is detected by the keep-alive signaling.

- In Device Adapter Release 8.1.2, the TPS registration uses the hardware identity (device ID) of the device to register. This device ID does not change if the device changes the TPS nodes in a cluster or TPS (Avaya Breeze® platform cluster) load balancers. Hence, the re-registration is allowed even if the prior registration has not ended. The re-registration request

is processed as a request to extend the current registration. Hence, Sequential Registration becomes optional.

If the Avaya Breeze® platform load balancing node fails, another node takes over the load balancing duties. However, there might be some registrations in progress when the load balancer node failed. Sequential Registration processes these incomplete registrations. Sequential Registration works in parallel with the load balancer fail-over. Any incomplete registrations that were in progress when the load balancing node failed successfully reattempt the registration for the endpoint by using Sequential Registration.

However, the following are the limitations:

- In an Avaya Breeze® platform cluster, only the dedicated active and standby servers can take over the Cluster IP, even if the cluster consists of more than two servers. This is different from CS 1000 where any TPS on a server in CS 1000 can act as the primary TPS and take over the Node IP.

    If both the Avaya Breeze® platform active and standby servers are down, no phones or media gateways can register.

- If Device Adapter stops, is uninstalled, or fails on the currently active server, no phones or media gateways can register, even if Avaya Breeze® platform is running properly.

How is general troubleshooting and traffic monitoring handled?

The monitoring and troubleshooting tools available for SIP endpoints in Session Manager and Communication Manager are also available for Device Adapter endpoints. Device Adapter also provides troubleshooting tools equivalent to those provided by the CS 1000 TPS.

Does Device Adapter support handing off a call from the desk phone to the Avaya Workplace Client on a mobile device?

The desk phone itself does not have the features to perform such a hand off. This type of hand off is performed by Avaya Workplace Client.

When is user data first imported into the PPM?

User data is first imported into the PPM when one of the following events occurs:

- When the Personal Directory data is imported from CS 1000 to Device Adapter.
- When the user registers their phone for the first time.
- When the administrator adds the user manually using the Personal Directory command line interface.

How is Corporate Directory support implemented?

LDAP Corporate Directory support is implemented using Avaya Aura® Device Services.

What IPE cards are supported after migration from CS 1000?

Refer to the section Supported TDM hardware on page 55 for information on supported IPE cards.

Are faxes and modems supported?

No. You must use faxes and modems connected to Communication Manager.

Are attendant consoles supported?

No. Attendant consoles are not supported in this release.

How are Device Adapter endpoints associated with Communication Manager stations?

Device Adapter endpoints are associated with Communication Manager stations in the following ways:

- A Communication Manager station representing a Device Adapter endpoint associates the station with a unique System ID and TN combination.

  A Communication Manager station administered with the Station Type of `CS1k-xxxx` has System ID and TN attributes. These two attributes form a unique combination at the solution level for every station representing a Device Adapter endpoint.

- A Device Adapter cluster is administered with a System ID.

  When a Device Adapter endpoint registers with a Device Adapter it submits a TN attribute value. Device Adapter locates the Communication Manager station that contains the same unique combination of the cluster System ID and the TN value submitted by the endpoint.

⊛ **Note:**

Migrating multiple CS 1000 systems into a single Avaya Breeze® platform cluster may cause TN conflicts. Hence, System ID is used to facilitate the migration and reduce TN conflicts. Till Device Adapter 8.1.1, using the System ID lessened the probability of TN conflicts, but required you to deploy a separate Device Adapter cluster for each migrated CS 1000 system. Provision of the latest release, which is used with Device Adapter 8.1.2, allows you to modify TNs and resolve TN conflicts during the migration. Therefore, you can migrate endpoints from multiple CS 1000 systems into a single Avaya Breeze® platform cluster.

How are Device Adapter endpoints associated with Session Managers?

Device Adapter endpoints are associated with Primary, Secondary, and Branch Session Managers in the following way:

- A user's Communication Profile, administered in System Manager User Management, associates a Communication Manager station with a Primary, Secondary, and Branch Session Manager.

- A Communication Manager station is associated with a unique System ID and TN combination.

- A Device Adapter cluster is administered with a System ID.

  When a Device Adapter endpoint registers with a Device Adapter it submits a TN attribute value. Device Adapter locates the Communication Manager station that contains the same unique combination of the cluster System ID and the TN value submitted by the endpoint. Device Adapter then uses the Session Manager information to determine the Primary, Secondary, and Branch Session Manager for the endpoint.

  ⊛ **Note:**

  Device Adapter does not support different Primary, Secondary, and Branch Session Manager for different endpoints in the same Device Adapter cluster.

How are Device Adapter endpoints associated with a Node?

The Avaya Device Adapter Snap-in has a configuration attribute called Node ID. The Node ID is an integer between 0 and 9999. One Device Adapter cluster is configured with a single Node ID.

This is functionally similar to the Node ID used in CS 1000 TPS clusters; one Node ID was assigned to each TPS cluster.

A UNIStim endpoint submits a Node ID and TN when it registers with a Device Adapter cluster. The registration is rejected if the Node ID submitted by the endpoint does not match the Node ID of the cluster.

✳ **Note:**

The two least significant digits of the Node ID are ignored during the matching operation. For example, Node ID 300 and 310 are considered a match.

Consider the following if a CS 1000 system with multiple TPS clusters that have different Node IDs is being migrated using a single Device Adapter cluster:

- The Device Adapter cluster must have sufficient capacity to accept all endpoints from the multiple TPS clusters.

- All endpoints must be configured to use the Node ID of the Device Adapter cluster. This may mean changing the configuration of some endpoints while leaving others unchanged after the migration. This can be done using the same configuration file the endpoints will use to get the new S1 and S2 values.

How does ProVision/NMT interact with the CS 1000 and Avaya Aura® systems?

ProVision/NMT can only retrieve information from the CS 1000 solution. It can retrieve and send information to Avaya Aura® applications such as System Manager and Communication Manager.

Device Adapter features

The following is a list of the key features of the Avaya Device Adapter Snap-in solution:

- Existing CS 1000 server components such as Terminal Proxy Server (TPS) and Personal Directory are migrated to Avaya Device Adapter Snap-in as an integral part of Avaya Device Adapter Snap-in.

- Existing CS 1000 endpoints interact directly with the snap-in.

- Terminal adaptation from CS 1000 Stimulus to Avaya SIP Telephony (AST) is implemented on Avaya Device Adapter Snap-in.

- Provisioning of the Avaya Device Adapter Snap-in configuration is done through Avaya Breeze® platform Service Attributes.

- All CS 1000 endpoints are administered by Avaya Aura® System Manager.

- CS 1000 style Park and Page functionality is available when Avaya Device Adapter Snap-in is paired with Avaya Call Park and Page Snap-in.

  ✳ **Note:**

  Avaya Call Park and Page Snap-in must be deployed in a dedicated Avaya Breeze® platform cluster to enable this functionality.

- Avaya Device Adapter Snap-in uses the ProVision/NMT utility to migrate most CS 1000 endpoint data to Communication Manager stations.

- Communication Manager supports administering the CS 1000 endpoints as Avaya SIP Telephony (AST) endpoints connected to Session Manager.

- The Avaya Device Adapter Snap-in-based solution supports High Availability and Geo-redundant operation to preserve call connection and state of CS 1000 endpoints.

- Corporate directory support using Avaya Aura® Device Services.

- TDM endpoint and hardware support. See Supported phones on page 53 and Supported TDM hardware on page 55 for additional information.

Snap-in components

Every Avaya Device Adapter Snap-in server deployment consists of the following components:

Component	Description
Terminal Proxy Server (TPS)	Provides access to media engines and I/O operations.
Digital Set Adapter (DSA)	Provides communication with TPS and performs SIP endpoint emulation.
Personal Directory	Provides redial, callers, and Personal Directory functionality for UNIStim phones. Makes use of the Avaya Breeze® platform PPM.
Java Snap-in	Provides configuration for every endpoint through access to Avaya Aura® System Manager.

Infrastructure capabilities and telephony features

Avaya Device Adapter Snap-in infrastructure capabilities

Device Adapter provides the following infrastructure capabilities:

- Endpoint registration:

  - UNIStim endpoint registration mapped to SIP registration with Session Manager.

    Sequential Registration is required to support UNIStim endpoint fail-over.

  - Analog and digital endpoint registration between Media Gateway Controller and Device Adapter carrying out SIP registration with Session Manager on behalf of each device.

    Sequential Registration fail-over configuration is required to support MGC fail-over for analog and digital endpoints.

- Both UNIStim endpoints and MGC have primary and backup registration entities.

  Device Adapter does SIP registration on behalf of the UNIStim endpoints it is supporting. Device Adapter supports a S1 (primary Session Manager) and S2 (secondary Session Manager) to perform the endpoint registrations. Configuration of a secondary Session Manager ensures continued telephony service if an interruption occurs in the primary Session Manager.

  Similarly, MGC supports a primary Device Adapter and two alternate Device Adapters. The digital and analog endpoints are connected to the MGC. The MGC establishes a proprietary PBXLink connection to the Device Adapters. After the connection is established, Device Adapter registers the digital and analog endpoints to Session Manager.

  This provides the endpoints the capability of redundant Device Adapter access. Device Adapter allows a primary and backup link to Session Manager in one of the two data centers or in a branch.

  Fail-over may result in Device Adapter trying to SIP register an endpoint before the existing registration is unregistered. Sequential Registration allows the new registration to complete, without waiting for the prior registration to be declared failed.

- Feature key labels:

  - Provided by the firmware for labels without customization by System Manager.

  - Custom labels downloaded to the UNIStim stations as defined by the administrator on System Manager.

  - Tone and Cadence settings based on the country, as configured in the Device Adapter attributes.

  - Context-sensitive soft key support for station types with the capability to provide these keys.

  - Key Expansion Module support, varying by station type among stations supporting this capability. For example, analog endpoints do not support expansion modules.

  - Media Security options (None, Best Effort, Always).

  - Signaling Security options.

CS 1000 telephony features supported by Avaya Device Adapter Snap-in

Device Adapter supports the following CS 1000 telephony features:

- Auto-answer

- Autodial

- Busy Forward Status

The Busy Forward Status feature of CS 1000 is similar to the Busy Indicator feature of Device Adapter, but with some differences.

• Call forwarding of all calls, busy calls, or no answer calls.

• Call park and parked call pickup. Call park requires the Avaya Call Park and Page Snap-in.

• Call Pickup

  - Directed

  - Group

  - Ringing number

• Call waiting

• Caller lists, redial lists, and Personal Directory.

• Call Number Display Denied.

• Conference, by using the Communication Manager style ad hoc conferencing.

• Conference, by using the Communication Manager style no hold conferencing.

• Context-sensitive key access: Idle, Off hook, Dialed, Ringing, and Active call state.

• Display of calling or called numbers.

• End-to-end signaling (DTMF).

• Fixed feature key access (not FFC based).

  - Feature access by FFC / Feature Access Codes for endpoints without programmable keys.

• Hold and retrieve

• Hotline one-way

• Hotline two–way

• Hotline Intercom

• Last number redial

• Loudspeaker paging

• Make set busy

• Making, answering, and releasing a basic call.

  - Dialing a destination number.

  - Answering a call.

  - Releasing a call, including using the Release key.

• Malicious call trace (MCT).

• Message waiting using Avaya Aura® Messaging.

• Message waiting key and indicator for voice mail.

- Mobile Extensions (Mobile X)

  The Mobile Extensions (Mobile X) feature of CS 1000 is similar to the Extension to Cellular (EC500) feature of Avaya Aura®.

  Use the EC500 feature in Device Adapter to provide the Mobile X service to the users.

- Multiple Appearance Directory Numbers.

  - Privacy and Privacy Release for multiple appearance SCA numbers.

- Multi-device access (MDA)

  Since Device Adapter Release 8.1, Device Adapter allows a UNIStim endpoint to register concurrently with other Avaya Aura® SIP endpoints for MDA.

  The configuration parameters used for Multi-Device Access remain the same as the ones that were used for the endpoint registration and fail-over prior to Device Adapter Release 8.1.

  CS 1000 does not have a feature named MDA, although administrative options provided a close match. However, CS 1000 used similar sets with identical features and keys defined, and shared all line appearances between each other. This behaves like two Avaya SIP legacy endpoints, with only bridged appearance keys and with identical key layouts, sharing the extension of an X-Port. Neither of the CS 1000 endpoints owns the extension assigned to the keys. Each station has its own unique identity, which is the TN as opposed to the Avaya Aura® extension.

  In Device Adapter, an administrator can configure a maximum of 10 endpoints for a user with the same station feature and button layout. These endpoints can include UNIStim endpoints, such as 11xx, 12xx, or a 2050 soft client, and one or more Avaya Aura® SIP endpoints. However, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint. This is because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA.

  Because MDA allows the same user to use multiple phones, only one license is required to register the phones.

  In CS 1000, registering two devices requires two station definitions; and therefore, two licenses are required. However, although the sets are frequently a paired soft client and hard phone, the sets are not necessarily intended for the same user.

  As compared to CS 1000, which requires one license for each device, in Device Adapter, you can have one Avaya Aura® license for a Communication Manager extension. You can use the same license to configure multiple devices for MDA or Sequential Registration.

- Mute

- Presence notification

- Private Line Service

  You can make outgoing calls and receive incoming calls on the private trunks assigned to your endpoint using the Private Line Service feature.

- Release key to disconnect a call.

- Ring again

- Send all calls when DND is active

- Sequential Registration

  Sequential Registration allows registration of only one endpoint at one time.

  In addition to providing fail-over support for UNIStim endpoints, Sequential Registration also provides fail-over support for analog and digital endpoints.

  CS 1000 has several features that shared similarities with Sequential Registration, including the Virtual Office feature and the unnamed capability to define two stations with identical layout and behavior, which pairs two phones.

  For more information, see Sequential Registration on page 710.

- Speaker on/off

- Speed dial (Speed Call)

- Time and date, call timer, and other similar set display features.

- Transfer - Blind and consultative

- Virtual Office

  Device Adapter supports Virtual Office (VO) only for UNIStim endpoints.

  When a user does a Virtual Office login at a guest station, the endpoint takes over the identity of the home station, which means that the endpoint logs out from the home station. When the user log out from the guest station, then the endpoint reverts to its original identity. In MDA and Sequential Registration feature, if the user logs out from a registered SIP endpoint and tries to register again then the endpoint will not return to the original identity

  Emergency Dialing is also supported using Virtual Office feature.

For information about the Avaya Aura® feature support on Device Adapter, see Legacy Avaya Aura SIP endpoint feature support on Device Adapter on page 619.

CS 1000 call center capabilities and features supported by Avaya Device Adapter Snap-in for Call Center Elite

The following are the CS 1000 call center capabilities and features supported by Avaya Device Adapter Snap-in for Call Center Elite:

- Activate Send All Calls (SAC) when Do Not Disturb (DND) is active

  This is equivalent to Make Set Busy (MSB) when Do Not Disturb is active in CS 1000.

- Agent log in and log out

  The agent login and logout feature handling differ in Device Adapter and CS 1000.

  Device Adapter uses the same key as a toggle key for login and logout.

- Agent skill set management

  The function is similar to that of the Multiple Queue Assignment feature of CS 1000, but is controlled differently.

- Agent auto answer

  This is equivalent to the Call Forcing feature of CS 1000.

- Call observation and supervisor calling an agent
- Call work codes

  This is equivalent to the Activity Code feature of CS 1000.

- Call recording

  Device Adapter does not support on-demand call recording by an agent. However, you can use bulk call recording or other recording modes that are supported by the call center server.

- Forced logout of an agent and forced logout by time of day override

  Device Adapter supports only the "forced logout by time of day override" feature to override the forced logout. Device Adapter does not support any other method to override forced logout.

- Forced transition of an agent into an Unavailable state.

  This is equivalent to the Not Ready feature of CS 1000 when the agent does not accept a call.

- Malicious Call Trace (MCT) as Emergency
- Multiple call type handling by an agent:

  - Automatic Call Distribution (ACD) calls

    ACD call handling in Device Adapter is equivalent to handling a call from an ACD queue in CS 1000.

  - Direct Agent Calls (DAC)

    DAC calls are not used frequently in CS 1000. An exception is the call from a supervisor to the agent.

  - Station extension calls

    Station extension call handling in Device Adapter is equivalent to Individual Directory Number (IDN) call handling in CS 1000.

  - Bridged appearance calls including MADN

    This is the equivalent for handling calls to Directory Numbers that are shared by two or more users in CS 1000.

  - Call modification of all call types that are received or originated.

- Queue status display

  An agent can view the number of calls in the queue, oldest call in the queue, and lamp states when thresholds exceed.

- Supervisor assistance request by an agent

- VDN Return Destination

  Supports post-call activities such as processing the feedback received through a customer survey.

- Work modes in which an agent is available to receive incoming calls:

  - Auto In

    Auto In is equivalent to transition of an agent state to Available to receive incoming calls in CS 1000.

  - Manual In

    Manual In is an additional work mode equivalent to transition of an agent state to Available in CS 1000. In Device Adapter, after the agent ends a call, the agent's work mode automatically transitions to After Call Work (ACW). The agent must press the Manual In button to become available to receive call center calls.

- Work modes in which an agent is unavailable to receive incoming calls:

  - After Call Work mode

    This is equivalent to the Not Ready feature of CS 1000, where an agent performs call-related work after ending the call and is not available to receive incoming calls.

  - Auxiliary Work mode

    This is equivalent to the Not Ready feature of CS 1000, where an agent is not available to receive incoming calls for any other reasons.

Supported phones

Avaya Device Adapter Snap-in supports the following CS 1000 phones.

✱ **Note:**

For information on upgrading the phone firmware, see Upgrading firmware and loadware on page 95. Device Adapter requires a minimum of Release 7.6.x firmware.

- UNIStim (including UNIStim IP 200X phones)

  - 1110, 1120, 1140, 1150, 1165, 1210, 1220, 1230, i2050 soft phone

  - 2001 Phase 1 and 2

  - 2002 Phase 1 and 2

  - 2004 Phase 0, 1, and 2

  - 2007

- Digital (including both 39xx and digital 200X phones)
  - 2006, 2008
  - 2216, 2616
  - 3110, 3310, 3820
  - 3901, 3902, 3903, 3904, 3905
- Analog

  All third-party dial pulse, 12 button DTMF analog phones, and analog phones with display.

- Key Expansion Modules (KEM) and Graphic Expansion Modules (GEM)
  - UNIStim
    - 24–key KEM for IP 200x series. Up to two KEMs can be connected that allow a phone to use 48 additional buttons. The maximum of 48 keys can be also achieved with a single KEM using the Shift key.
    - 18–key KEM for i2050. Up to 3 KEMs can be connected that allow a phone to use 54 additional buttons.
    - 18–key GEM for 11xx series. Max 3 GEMs with 18 buttons providing 54 extra keys. Can have 1 GEM and use the Shift button to allow 36 keys.
    - 12–key GEM for 12xx series. Up to 4 GEMs allowed providing 48 extra keys. Can have 1 or 2 GEM and use the Shift button to achieve the maximum of 48 keys.
  - Digital
    - 22–key Add-on Module (AOM) for 2216 and 2616 phones. Maximum of two modules.
    - 22–key Key-Based Accessory (KBA) for 39xx series. Maximum of two modules. This is functionally the same as the AOM for the 2216 and 2616 stations.
    - 8–key Display-Based Accessory (DBA) for 39xx series. Maximum of one module. Up to 3 pages with 24 keys by using Shift key on DBA.
    - 22–key KEM for European 3820 phone. Functionally identical to AOM. The 3820 is a European equivalent of the 2616 station.

For more information about administrative screens, see Appendices. Although manual configuration is not required because the configuration is migrated by using ProVision.

> ❗ **Important:**
>
> - Fax and modems are not supported through Device Adapter. Customers should use fax and modems supported by Avaya Aura®.
> - Device Adapter only supports the digital phones listed above. Other digital phones are not supported at this time.
> - Attendant consoles are not supported through Device Adapter. Customers should use attendant consoles supported by Avaya Aura®.
> - The I2033 Conference phone is not supported.

Supported phone types in an Avaya Aura® Call Center Elite environment

Device Adapter supports the following UNIStim phones in an Avaya Aura® Call Center Elite environment:

- 1140
- 1150
- 1230
- 2004
- 2007
- i2050 soft phone

Call center agents and supervisors can use these phones to perform call center-specific operations. The call center-specific features and options that are available on these phones depend on what features and options are configured by a system administrator for the phones. The call center-specific features and options are available on these phones only when an agent or supervisor is logged in to the phone. Otherwise, the phone operates as a normal Unified Communications (UC) phone.

Supported TDM hardware

Several of the circuit packs required to migrate from CS 1000 or Meridian 1 to Device Adapter have two vintages: E5 and E6. These packs are identical, except that E5 uses a leaded solder, and E6 uses a lead-free solder. The lead-free version is still available, but the leaded version is no longer manufactured. Either E5 or E6 can be used.

For more information, see "Appendix L: Hardware requirements for migration."

The following CS 1000 TDM-to-IP hardware is required to support converting a Meridian 1 or CS 1000 to Device Adapter.

- For IPE shelves (Meridian 1 large system, CS 1000M large system):
  - MG-XPEC: NTDW20AAE6.
  - All Extended System Monitors (XSMs) that are connected directly to the MG-XPEC must be NT8D22AEE5 or NT8D22AEE6.

    For more information about settings for the switches on the XSM, see "Appendix L: Hardware requirements for migration."
  - Correct cabling and cable kits are required.

- For cabinets and chassis (Meridian 1 Option 11, CS 1000M Option 11, Meridian 1 Option 11C Mini, CS 1000E, and MG1010):

  - MGC: NTDW60BA, NTDW60BBE5, NTDW98AAE5, NTDW98AAE6, or NTDW98AAGS.
  - DSP daughterboards:

    - MGC DSP Daughterboard 128 ports (NTDW78AAE5, NTDW78AAE6, or NTDW78AAGS).
    - MGC DSP Daughterboard 96 ports (NTDW64AAE5 or NTDW64AAGS).
    - MGC DSP Daughterboard 32 ports (NTDW62AAE5 or NTDW62AAGS).

The following TDM hardware is supported:

- For large systems:

  - NT8D37 IPE shelves (any version).
  - In a partly or mostly TDM large system, an NT8D37 IPE shelf can be used for Fiber Remote or Carrier Remote, using a specific replacement for the XPEC to provide transport to the remote CS 1000.

    - If the NT8D37 IPE shelf is used for Carrier Remote, you must replace the T1 or E1 (Carrier Remote) with an IP network connection. The MG-XPEC does not connect to Device Adapter over T1 or E1.
    - If the NT8D37 IPE shelf is used for Fiber Remote, replace the fiber connection with an IP network connection. The infrastructure for the fiber remote may be capable of providing IP support, but IP connectivity must be established. If the fiber infrastructure allows IP over fiber, then the existing infrastructure can be used.
  - AC or DC country specific power supply for the shelf.
  - Ringing generators NT8D21 (any version; supplies AC power) or NT6D42 (any version; supplies DC power) if any analog phones are controlled by this IPE shelf:

    - Only one IPE shelf from the former CS 1000 needs to connect to the MG-XPEC.
    - All other XSMs can chain together to connect to the XSM.

      That is, XSM 1 can be part of a string of XSMs.

      - If XSM 1 connects to the MG-XPEC, then the XSM must be NT8D22AEE5 or NT8D22AEE6.
      - Otherwise, if the XSM is not connected to the MG-XPEC, it can be an older vintage.

- For small system cabinets and chassis:

  - Option 11 and derivative cabinets and chassis:

    - All cabinets or chassis include a slot for the MGC and additional slots for line cards.
    - NTAK11 (any version) – ten slots for line cards.

      - If this cabinet is used for carrier remote or fiber remote, it can be migrated to Device Adapter. This cabinet supports MGC.

- NTC310AAE6 – ten slots for line cards.
- NTDK91BB – four slots for line cards.
  - The NTDK16 card in slot 4 provides a card slot 5 and 6 equivalent.
  - NTDK92 Chassis Expander – adds 4 additional slots for line cards and requires NTDK91BB.
- NTDU14CA – four slots for line cards.
  - NTDU15CA Chassis Expander – adds 4 additional slots for line cards and requires NTDU14CA.
- The following cabinets are not supported for Device Adapter:
  - NTDK50 Main or expansion cabinet for Carrier Remote.

    This cabinet does not support MGC.
  - NTAK12 Expansion cabinet for Carrier Remote and Fiber Remote.

    This cabinet does not support MGC.
  - Users who use NTAK12 or NTDK50 and want to retain the CS 1000 stations must migrate to an NTAK11 cabinet. Alternatively, you can replace the endpoints on the NTAK12 or NTDK50 cabinets with Avaya J-series endpoints.
- For all systems:
  - AC or DC country specific power supply for the shelf, cabinet, or chassis.
  - Pedestals, mount kits, and other hardware.
  - Analog and digital line cards to provide signaling connections with the sets.

Device Adapter provides support for sending SNMP traps to System Manager for alarms on the MGC and MG-XPEC shelves. Specifically, Device Adapter sends XSM and PSTAT signals to System Manager. Therefore, if some event happens with PSTAT or XSM, the administrator should examine the alarm in System Manager in **Services** > **Events** > **Alarms**.

Related links

Interoperability

Avaya Device Adapter Snap-in Release 8.1.2 interoperates with the following applications:

- Avaya Aura® Session Manager 8.1.2
- Avaya Aura® Communication Manager 8.1.2
- Avaya Aura® System Manager 8.1.2

- Avaya Session Border Controller for Enterprise 8.1
- Avaya Aura® Media Server 8.0.2
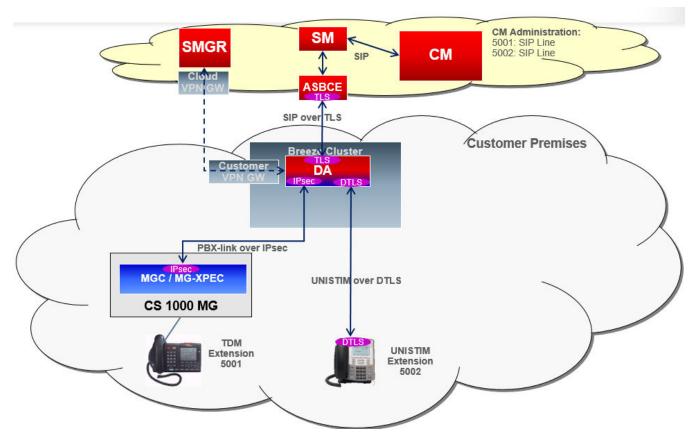
  😀 **Note:**

    - Avaya Device Adapter Snap-in requires Avaya Aura® Media Server to be installed for Avaya Aura® Communication Manager.

    - Avaya Device Adapter Snap-in does not require Avaya Aura® Media Server for Avaya Breeze® platform.

- Avaya Breeze® platform 3.7
- Avaya Aura® Device Services 8.0.1
- Avaya Oceana® 3.6
- Avaya Aura® Contact Center 8.1.2
- Avaya Aura® Call Center Elite 8.1.2

Deployment scenarios

Device Adapter On Premises and Avaya Aura® in the Cloud

The following diagram depicts a Device Adapter deployment where the snap-in is deployed On Premises and the Avaya Aura® solution is in the Cloud:
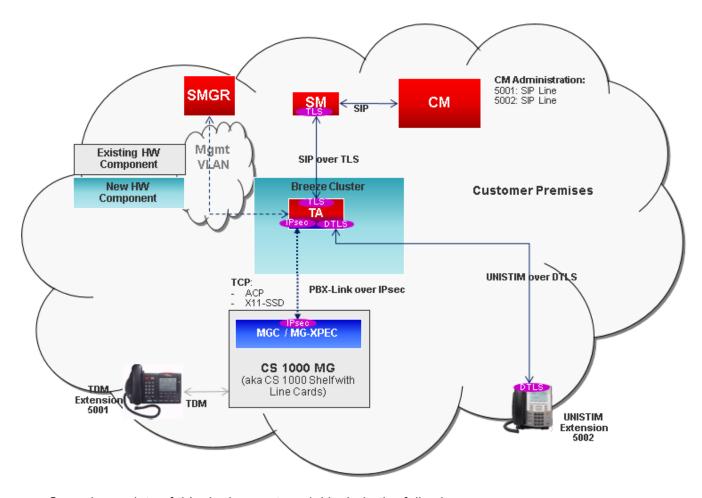
Some key points of this deployment model include the following:

- Avaya Aura® Cloud VPN solution is used for management operations.
- Device Adapter provides secure signaling in the following manner:
  - SIP signaling (towards Session Manager) is protected by TLS.
  - UNIStim signaling (towards UNIStim endpoints) is protected by DTLS.
  - TDM-set signaling (towards MGC) is protected by IPSec.
- Avaya Breeze® platform provides support for TLS.
- Device Adapter TPS component provides support for DTLS.
- Device Adapter provides support for IPSec.
- Typical Session Border Controller implementation is the Avaya Session Border Controller for Enterprise.

Device Adapter and Avaya Aura® On Premises

The following diagram depicts a Device Adapter deployment where both Device Adapter and the Avaya Aura® solution are deployed On Premises.
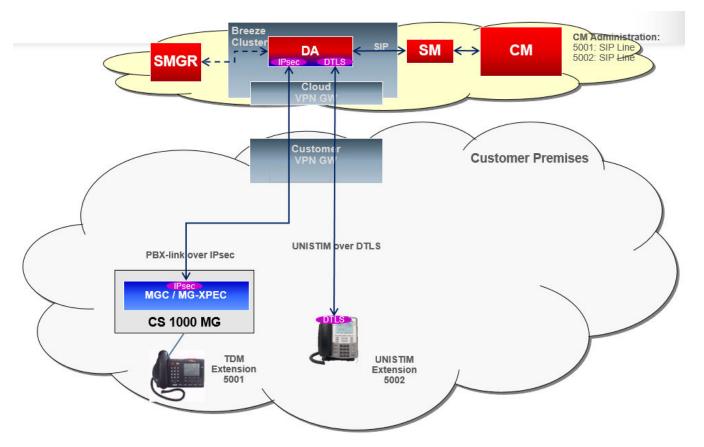
Some key points of this deployment model include the following:

- Device Adapter provides secure signaling in the following manner:
    - SIP signaling (towards Session Manager) is protected by TLS.
    - UNIStim signaling (towards UNIStim endpoints) is protected by DTLS.
    - TDM-set signaling (towards MGC) is protected by IPSec.
- Avaya Breeze® platform provides support for TLS.
- Device Adapter TPS component provides support for DTLS.
- Device Adapter provides support for IPSec.

Device Adapter and Avaya Aura® in the Cloud

The following diagram depicts a Device Adapter deployment where both Device Adapter and the Avaya Aura® solution are deployed in the Cloud.
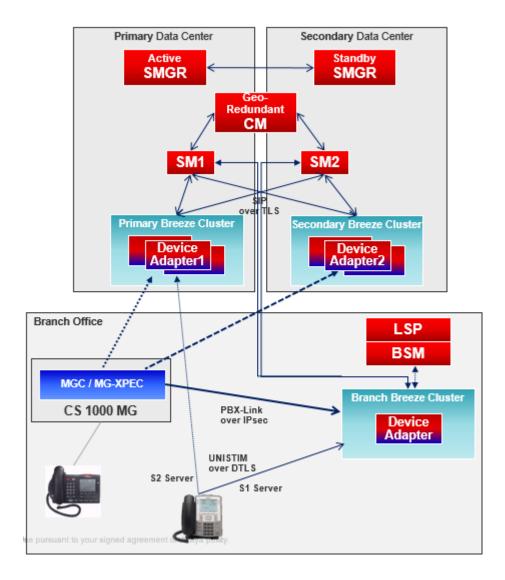
Some key points of this deployment model include the following:

- Avaya Aura®Cloud VPN solution is used for PBX-Link and UNIStim signaling.
- A VPN router is required on every subnet with UNIStim endpoints and Media Gateways.
- Device Adapter provides secure signaling in the following manner:
  - SIP signaling (towards Session Manager) is protected by TLS.
  - UNIStim signaling (towards UNIStim endpoints) is protected by DTLS.
  - TDM-set signaling (towards MGC) is protected by IPSec.
- Avaya Breeze® platform provides support for TLS.
- Device Adapter TPS component provides support for DTLS.
- Device Adapter provides support for IPSec.

Device Adapter deployment for Local Survivability

The following diagram depicts a Device Adapter deployment configured for Local Survivability.
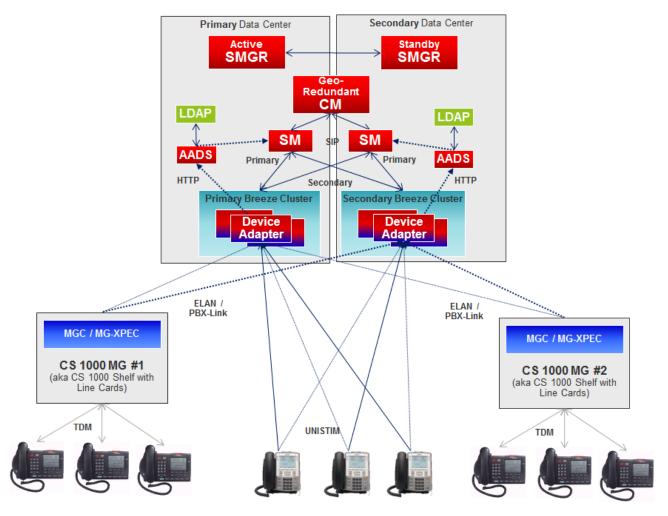
Device Adapter support for Amazon Web Services

Device Adapter supports deployment with Amazon Web Services using standard Avaya Aura® deployment practices. For more information and procedures about using Amazon Web Services, see the following documents:

- *Deploying Avaya Aura® applications on Amazon Web Services*
- *Deploying Avaya Aura® System Manager on Amazon Web Services for Avaya Aura®*
- *Deploying Avaya Breeze® platform on Amazon Web Services for Avaya Aura®*

Download these documents from https://support.avaya.com/.

Device Adapter On Premises connected to Media Gateway Controller

Some key points of this deployment model include the following:

- Media Gateways connect to Device Adapter over the IP network.
- No trunks are migrated.

Configurations related to Avaya Aura® Session Manager for Avaya Device Adapter Snap-in

Avaya Device Adapter Snap-in uses the following features of Avaya Aura® Session Manager to perform tasks:

- Avaya Device Adapter Snap-in performs challenge and authentication on behalf of an UNIStim or TDM station with Avaya Aura® Session Manager.

- Avaya Device Adapter Snap-in indicates the signaling location of a call by the IP address located in the via header of the INVITE request. Signaling locations must be administered using IP address patterns.

- Avaya Device Adapter Snap-in indicates the media location of a call by the IP address located in the SDP.

For every Avaya Breeze® platform server running Avaya Device Adapter Snap-in, an additional SIP Entity of the **Endpoint Concentrator** type must be defined. A number of Entity links between the SIP Entity and one or more Avaya Aura® Session Managers must also be defined. The Entity links must have a Connection Policy set to Endpoint Concentrator. An Avaya Aura® Session Manager Communication Profile must also be defined for every user or endpoint.

The location has an implication to the personnel who perform the migration and maintain the Device Adapter clusters.

This requires the following three levels in the hierarchy of configuration:

- Location: The location of the site must be defined in the locations data. This allows the calls to receive different routing based on the site in question.

- Network region: Each location has one or more network regions. For example, a university may have multiple campuses. Each campus may have multiple buildings, large buildings may have multiple floors, and each floor may be an individual region.

- Network address map: Each IP subnet (or possibly every IP address) maps to a suitable network region. Each entry may also include a number allowing calls back from the PSAP.

For more information, see "Appendix N: Location-based operations."

Configurations related to Avaya Aura® System Manager for Avaya Device Adapter Snap-in

You must configure the following for all the users with CS 1000 endpoints:

- Session Manager Communication Profile

> **Note:**
>
> The association of endpoints with Session Managers is done with the Session Manager Communication Profile. All users in a Branch must have the same associations with the Session Manager.

- Communication Manager Communication Profile

> **Note:**
>
> Some Device Adapter telephony features can be customized with the Avaya Breeze® platform Service Profile and is associated with a user through the Avaya Breeze® platform Communication Profile. Additional configuration using the Avaya Breeze® platform Communication Profile may be necessary.

Supported service ports for Avaya Device Adapter Snap-in

Avaya Device Adapter Snap-in uses the following ports:

> **Important:**
>
> The ports are declared as IP Service Ports in Avaya Device Adapter Snap-in. Changing any of these service ports is not supported and leads to malfunction of Device Adapter.

Port	Transport Protocol	Application Protocol	Traffic Purpose	Default Port State
4100, 4101	UDP	UNIStim	Connection service	Open
8300, 8301	UDP	UNIStim	TPS load balancing	Open
5100, 5101	UDP	UNIStim	VTM registration	Open
5105	UDP	UFTP	Firmware upgrade	Open
10000	UDP	TPS	NAT discovery	Open
16540, 16550	UDP	TPS	Mastership, set info	Open
1024 - 65535	TCP	SIP	SIP signaling	Open
443	TCP	PPM	PPM data	Open
15000	TCP	PBX Link	PBX Link	Open
15003	UDP	PBX Link	PBX Link	Open
21	TCP	FTP	Legacy MGC loadware upgrade	Closed
111	TCP	PORTMAP	Legacy MGC loadware upgrade	Closed
32788	TCP	RPC	Legacy MGC loadware upgrade	Closed

Table continues…

Port	Transport Protocol	Application Protocol	Traffic Purpose	Default Port State
32789	TCP	RPC	Legacy MGC loadware upgrade	Closed
22	TCP	SSH/SFTP	MGC administration, file sync	Open

For information about the ports for Avaya Breeze® platform solution, see *Administering Avaya Breeze® platform* at https://support.avaya.com/.

For information about the ports for Avaya Aura® solution, see the applicable product port matrix document listing at https://support.avaya.com/.

Phased migration

A phased migration from an existing CS 1000 solution to an Avaya Aura® solution involves dividing the existing endpoints into groups and migrating them in batches instead of all at once. Phased migration is the preferred migration strategy as it ensures:

- All endpoints in a solution are not affected by a migration activity.
- Less down time during a particular migration activity.
- Less likelihood of a catastrophic fault during the migration activity.

The following must be addressed if a phased migration is planned:

- Group features such as Multiple Appearance Directory Numbers (MADN) can be lost if all endpoints and participants in the feature group are not migrated in the same migration phase. If MADN members are spread across multiple Media Gateway Controllers, all MGCs must be migrated at the same time.
- PSTN access to migrated endpoints must be configured so that the migrated endpoints can initiate or receive PSTN calls. This configuration can be done by moving the migrated users to the centralized SIP trunks of the Avaya Aura® solution. You can also keep the existing CS 1000 TDM DID trunks and use them in combination with the Vacant number routing administered on the CS 1000 solution. Vacant number routing is administered to route calls to vacant numbers in the Avaya Aura® solution.
- Routing of internal calls to the migrated endpoints must be configured by using Vacant number routing to route calls from CS 1000 to the Avaya Aura® solution. You can also use specific digit manipulation tables on the CS 1000 solution to route calls to the migrated endpoints on the Avaya Aura® solution.
- You must route internal calls to the endpoints still in the CS 1000 solution from the migrated endpoints in the Avaya Aura® solution. On the Avaya Aura® solution, you must configure SIP routing into the CS 1000 solution for the range of extensions still deployed there. Alternately, if a SIP endpoint and a SIP route exists for a particular number, the Avaya Aura® solution will deliver the call to the SIP endpoint.

• The Avaya Aura® solution must be configured with the resources necessary to accommodate the increased number of endpoints. A CS 1000 endpoint requires the same resource allocation in an Avaya Aura® solution as any other Avaya Aura® SIP endpoint.

Phased migration by using ProVision

This topic provides a high-level overview about using ProVision and the associated Nortel Migration Tool (NMT) to migrate existing CS 1000 endpoints to an Avaya Aura® solution.

• For migrating digital and analog endpoints, consider the following:

- Migrate all endpoints that are connected to a given MGC during the same phase.

- Manually account for analog directory numbers (DNs) created on Phantom type superloops. DNs on Phantom loops are virtual and are not connected to physical endpoints.

• After you retrieve the CS 1000 data into ProVision, you can modify individual table records. Do not delete any table record. Removing records could negatively affect the built-in logic of the Nortel Migration Tool due to data interdependencies.

• The following are the two options for phased migration of endpoints by using ProVision and the associated NMT:

- Use NMT to map all extensions:

• You can run NMT once and map all sets. You can group the endpoints later by using ProVision.

• To support the procedure of grouping the endpoints, you must reference the source CS 1000 cs dnb and cs tnb tables along with the target Communication Manager station table in ProVision.

• After grouping the stations, create separate configuration folders, copies of the one populated by NMT run, for the target Communication Manager and System Manager.

• You can modify the tables in each configuration folder so that the tables contain only the stations that you want to migrate in the phase.

- Use NMT to map only selected extensions:

• Use ProVision to reference the source CS 1000 cs dnb and cs tnb tables to select and group the endpoints.

• You must run NMT every time for each planned migration phase. NMT maps only the endpoints that you select for a given migration phase during the process.

• Each time you run NMT, NMT uses the same settings that you have configured, especially the extension range that you provide in the **Additional Extension Pool** field of NMT.

For more information, see

You must create separate configuration folders for the target Communication Manager and System Manager for each migration phase.

For more information, see the ProVision and Nortel Migration Tool documentation.

- After you run the Send Stations transaction on ProVision to migrate the data to the target Communication Manager, examine the event log of ProVision. The event log contains problems that are reported by Communication Manager. Investigate and rectify any warnings or errors before you proceed with the migration process.

- Use the File Connection feature of ProVision to support retrieving and sending transactions between ProVision and System Manager. Do the following:

    - Export existing users from System Manager.

    - Use the XML file that you exported as the preferred connection of the target System Manager in ProVision.

    - After you add new users to the XML file by using the Send Transactions feature of ProVision, import the XML file into System Manager.

    For more information, see the *ProVision Job Aid*, *SMGR Connection Methods* on the Avaya ProVision website.

Caveats

- For CS 1000 analog stations, there is a cross-platform analog to SIP limitation for Communication Manager version that is supported with the respective Device Adapter version.

    The behavior for Multiple Appearance Directory Number on analog sets will always be Multiple Call Arrangement and is not set to Single Call Arrangement. That is, each endpoint may make an individual outgoing call and any idle endpoint can receive an incoming call. However, because these are MCA, none of the other users sharing the number can bridge into it.

    The analog stations are defined as SIP station and will have virtual buttons to handle the line appearances, including the appearance used to transfer a call or to create a conference. When these are shared, the appearances for the analog stations are defined as bridged appearances. Because no privacy release key is available, all analog station brdg-appr buttons are created as Bridged: all (B: a) buttons instead, concrete index "B: <number>" (Bridged: specific call appearance).

- ProVision and Nortel Migration Tool function need some Class-of-Service (COS) tables. This provides the default settings that can be used to set the following parameters for migrated stations:

    - Bridging Exclusion Override

    - Automatic Exclusion (privacy settings to enable privacy release)

    - Automatic Callback (ring again)

    The administrator must ensure that sufficient COSs are administered with the desired values. This can be done directly on Communication Manager or System Manager.

- ProVision and Nortel Migration Tool function need some Class-of-Restriction (COR) tables. This provides the default settings that can be used to set the following parameters for migrated stations:

    - Can Be Picked Up By Directed Call Pickup

- Can Use Directed Call Pickup
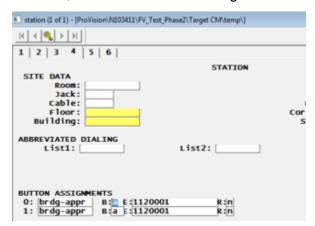
The administrator must ensure that sufficient CORs are administered with the desired values. This can be done directly on Communication Manager or System Manager.

• Call pickup groups can include only 100 users.

• Extended call pickup groups can include only 25 call pickup groups.

• CS 1000 based Call Park makes use of an independent Avaya Breeze® platform snap-in. This is not created by migrating data from CS 1000 by using ProVision tools. CS 1000 based Call Park is defined in Avaya Aura® as Call Park and Page.

The administrator must pre-install the Call Park and Page snap-in on an independent Avaya Breeze® platform server and cluster. Device Adapter cannot be co-located in the same Avaya Breeze® platform as the Call Park and Page snap-in.

• Migration of analog stations may leave a single bridged appearance button as Button 0 in the configuration tables. If this occurs, the analog station will fail to transfer or conference calls.

To resolve this problem, edit the station definition and copy the Button 0 configuration to Button 1, as shown in the following illustration. Ensure that this is Bridged all (B:a).

IPv6 support

Starting from Release 8.1.2, Avaya Device Adapter Snap-in supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) for signaling within the Avaya Aura® deployment.

The signaling between Device Adapter and the endpoints still uses only IPv4 connection because the endpoints support only the IPv4.

The signaling between Device Adapter and Avaya Aura® components can be IPv4 or IPv6.

Device Adapter uses the IP version that a server negotiates as the preferable version. The Device Adapter determines which IP version to use based on the data received from Avaya Aura® System Manager and Avaya Breeze® platform. When both sides of a connection, for example, Avaya Breeze® platform and Session Manager support both IPv4 and IPv6, Device Adapter makes the decision in accordance with the IP address family preference service attribute.

The following servers can use IPv6 with Device Adapter:

- Avaya Aura® System Manager (SMGR)
- Avaya Aura® Session Manager (SM)
- Personal Profile Manager (PPM)
- Avaya Aura® Device Services (AADS)
- Survivability server

Requirements to the network configuration for the IPv6 support

For implementing the IPv6 support on Device Adapter, the following components must support IPv6:

- Avaya Aura® components
- Avaya Breeze® platform

Certificate handling

TLS or DTLS protects the following types of connections between a Device Adapter node and other solution components:

- UNIStim signaling between an endpoint and the Device Adapter node.

  - The connection is initiated by the endpoint.

  - The Device Adapter node acts as the DTLS server and presents its certificate to the endpoint.

  - The endpoint acts as the DTLS client. The endpoint may be requested to authenticate and present its own certificate to the Device Adapter node.

- HTTPS signaling between a Device Adapter node and a PPM node.

  - The connection is initiated by the Device Adapter node.

  - The PPM node acts as the TLS server and presents its certificate to the Device Adapter node.

  - The Device Adapter node acts as the TLS client. The node may be requested to authenticate and present its own certificate to the PPM node.

- SIP signaling between a Device Adapter node and a Session Manager node.

  - The connection is initiated by the Device Adapter node.

  - The Session Manager node acts as the TLS server and must present its certificate to the Device Adapter node

  - The Device Adapter node acts as the TLS client. The node may be requested to authenticate and present its own certificate to the Session Manager node.

Identity and trust management are important for these connections to be successful. Device Adapter relies on the certificate management provided by the Avaya Breeze® platform. The following identity and trusted certificate pairs are relevant to the operation of Device Adapter:

- Security Module HTTPS identity and trusted certificates for UNIStim and HTTPS secure connections.

- Security Module SIP identity and trusted certificates for SIP secure connections.

These certificates are made available to Device Adapter for secure communications when Device Adapter is installed on an Avaya Breeze® platform server.

😊 **Note:**

If you modify any of the Avaya Breeze® platform identity certificates after Device Adapter is installed, you must restart Avaya Breeze® platform.

If you modify any of the Avaya Breeze® platform trusted certificates after Device Adapter is installed, you need not restart Avaya Breeze® platform.

Reinstallation of Device Adapter on the affected Avaya Breeze® platform cluster is not required. Device Adapter automatically applies the changes and restarts the dsa, tps, and csv services within 5 minutes after you modify the certificates. This procedure will not impact the cluster administration data.

This is service impacting. Avaya recommends that you modify the preceding identity or trusted certificates on Avaya Breeze® platform during the maintenance window to minimize the impact on endpoint registration and call handling.

FIPS compliance

Device Adapter complies with Federal Information Processing Standards Publication (FIPS) 140-2, Security Requirements for Cryptographic Modules, which specifies the security requirements to be met by the cryptographic modules.

Device Adapter version 8.1.3 or later is compliant to FIPS 140-2. Device Adapter uses Avaya Breeze® platform utilities and FIPS mode must be enabled on Avaya Breeze® platform to use the fully FIPS compliant Device Adapter.

Device Adapter uses the following crypto modules:

- TLS to connect to Avaya Aura® Session Manager. Breeze® (RedHat Enterprise Linux 7). FIPS 140-2 compliant provides the TLS module.

- DTLS to secure Unistim traffic between TPS and Unistim phones. The built-in Mocana NanoSec library drives the DTLS.

- IPSec to secure signaling traffic between the Device Adapter and the Media Gateways. Libreswan is FIPS compliant for RHEL 7 unless Breeze® operates in FIPS mode.

- SSH protocol to push or pull files from the Media Gateways.

> ✳ **Note:**
>
> Media Gateway connections, such as IPSec and SSH are FIPS 140-2 compliant. Media Gateway stays non-FIPS compliant since it is a legacy product.

Enabling FIPS mode on Breeze server

About this task

You can enable FIPS mode separately on each Breeze® server through `fips_mode.sh` CLI command. Currently, there are no SMGR UI means to enable FIPS mode for the entire system or group of Breeze® servers.

Procedure

Enter the following commands:

```
./fips_mode.sh // no parameter, check the fips status

./fips_mode.sh <mode> // mode is "enable" or "disable"
```

After entering the command, it will prompt you to confirm the status change.

Upgrading media gateway controller

About this task

MGC loadware that comes with Avaya Device Adapter Snap-in supports stronger cryptographic suites for IPSec and SSH connections. MGC old loadwares that come with Avaya Device Adapter Snap-in do not have stronger cryptographic support, and MGC fails to connect to Breeze® server operating in the FIPS mode.

Procedure

1. Do one of the following:

   - Disable the FIPS mode on Breeze® server.

     - Make sure the FIPS mode is disabled on Breeze server:

       ```
       [root@breeze5 ~]# fips_mode.sh

       /opt/Avaya/bin/fips_mode.sh: FIPS mode is disabled in the OS
       ```

     - Use the CLI command to disable the FIPS mode: `fips_mode.sh disable`

   - Disable the IPSec.

2. Install Avaya Device Adapter Snap-in 8.1.3.

3. Wait until all Media Gateways are upgraded.

> ⊛ **Note:**
>
>> You can verify the new MGC loadware version and upgrade status through `mgcShow` command.

Next steps

Do the following:

- If you disable the FIPS mode in Step 1, enable the FIPS mode.
- If you disable the IPSec in Step 1, enable the IPSec.

Related links

[Configuring IP security](#) on page 131

High Availability and Geo-Redundancy

An IP network exists between the following components:

- UNIStim endpoints or MGC of the TDM endpoints and the Device Adapter nodes (Avaya Breeze® platform nodes where the Device Adapter Snap-In is installed):

  - An IP network exists between the UNIStim endpoints and the Device Adapter nodes in the cluster.

    An IP connection failure may occur between a UNIStim endpoint and the Device Adapter node serving the endpoint.

  - An IP network exists between the MGC of the TDM endpoints (digital and analog endpoints) and the Device Adapter nodes in the cluster.

    An IP connection failure may occur between an MGC serving multiple TDM endpoints and the Device Adapter node serving the MGC.

- An IP network exists between the Avaya Breeze® platform cluster that has the Device Adapter nodes and the remainder of the Avaya Aura® components.

  An IP connection failure may occur between the Avaya Breeze® platform cluster and the Avaya Aura® components.

Device Adapter uses two high availability capabilities in conjunction to minimize or eliminate single points of failure, where an IP network or server failure causes an endpoint to lose communications capability:

- HA between a UNIStim endpoint or MGC and the Device Adapter nodes.

  HA in this scenario is handled by any one of the following two mechanisms. Both UNIStim phone and MGC rely on health check for their registrations. However:

  - Both UNIStim phone and MGC use a form of geo-redundancy. If the primary server is unreachable, the UNIStim phone or MGC tries an alternate data center.

- Both UNIStim phone and MGC may use an N+1 intra-cluster redundancy. This may be limited. In CS 1000, the MGC could have an active and backup call server core with which the MGC registers. However, in Device Adapter, TPS clusters scale in a manner effectively identical to the Device Adapter clusters. There could be multiple TPS node clusters with an extra "+1" node to handle large sized CS 1000 systems.

  For more information, see [HA between UNIStim endpoints or MGC of TDM endpoints and Device Adapter nodes: Intra-cluster redundancy (N+1 clusters)](#) on page 74.

- HA between the Avaya Breeze platform cluster that has the Device Adapter nodes and other Avaya Aura® components.

  High availability between the Avaya Breeze® platform cluster and Avaya Aura® components is handled by Avaya Breeze® platform. This may include both N+1 high availability within a Session Manager, and geo-redundancy involving two Session Managers.

  For more information, see the "HA and geo-redundancy between Avaya Breeze® platform clusters and Avaya Aura® components" topic.

You may choose the redundancy option that best suits your requirements. For example, for a smaller CS 1000 environment that is migrating to Device Adapter, it may be worth using the intra-cluster redundancy with an N+1 node environment. If you have a site with 800 devices, you may use a 1+1 environment without Geo-Redundancy, provided you are fine with outages caused because of a failure in the data center where the Device Adapters reside.

Avaya recommends the you carefully analyze the redundancy options before using them. For example, if you have two geographically separated data centers, and if the Device Adapters located at one location are out-of-contact because of a natural calamity, the Device Adapters located at other location can take over.

HA and geo-redundancy between UNIStim endpoints or MGCs and Device Adapter nodes

HA between UNIStim endpoints or MGC of TDM endpoints and Device Adapter nodes: Intra-cluster redundancy (N+1 clusters)

Avaya Breeze® platform supports the Device Adapter solution by using the Avaya Breeze® platform model for intra-cluster redundancy. In this model, endpoints registered with Device Adapter use the cluster IP address of the Avaya Breeze® platform cluster load balancer, instead of individual IP addresses of the Avaya Breeze® platform servers.

Intra-cluster redundancy supports a maximum N+1 configuration in the Avaya Breeze® platform cluster. The maximum number of supported servers in a cluster is 6. This means the maximum useful capacity of a cluster is 5 servers so that the cluster has an N+1 configuration. If a failure occurs with one server or a network fault isolates the server, the registered endpoints are redistributed to the other servers in the cluster. The cluster itself uses a leader/follower model for the load balancer and cluster IP. As a result, if the server that hosts the cluster IP address is unavailable, the cluster IP address will be taken over by one of the other servers.

The maximum number of Device Adapter nodes supported in a solution is 50. These nodes are grouped into clusters with no more than six nodes per cluster (High Availability supports up to a 5+1 footprint). Because there can be 1 to 6 nodes per cluster, the maximum number of clusters supported in a solution varies based on the total number of nodes per cluster. However, the maximum of 50 nodes still places a fixed limit on the number of nodes and users per System Manager. If all clusters are single node, there can be no more than 50 clusters defined.

An N+1 cluster configuration allows Device Adapter the capability to be fully functional even if any one cluster encounters outages or is taken down for maintenance. Call handling and endpoint registrations are performed normally. Because in an N+1 environment the load balancer ensures that all nodes have equivalent registration loading, different device IP ports can register the device to any of the other five available nodes. However, in an N+1 cluster configuration, redundancy is not supported if any one cluster is not functional.

Whereas, an "N+0" cluster configuration provides a smaller footprint for the number of users, but does not allow Device Adapter the capability to be fully functional if any one cluster encounters outages or is taken down for maintenance. For example, if a site has a 5+0 cluster configuration and the services on one node are stopped to perform node maintenance, all the user endpoints on that node are taken out of service and the endpoints are non-deterministic. Out of the 5 clusters, only 4 clusters are functional. Hence, 20% of the call handling and registration capability is lost until the node under maintenance starts running again.

Fail-over handling by MGC in an intra-cluster redundancy model (N+1 clusters)

MGC follows the following fail-over process an intra-cluster redundancy model:

1. During initial registration, the MGC uses the cluster IP address of the Avaya Breeze® platform cluster to register to the Device Adapter node. This cluster IP is configured on the MGC by the system administrator.

2. If the Device Adapter node does not have the required capacity, the Device Adapter cluster load balancer redirects the MGC to a Device Adapter node that has the required capacity within the cluster. MGC registers the endpoints with the node.

3. If a connection failure occurs at the node, MGC tries to fail over by using the same cluster IP address. The Device Adapter cluster load balancer provides the cluster IP of the cluster that has the required capacity.

4. MGC registers the endpoints to the new Device Adapter node within the cluster.

Geo-redundancy between UNIStim endpoints or MGC and Device Adapter nodes: Inter-cluster redundancy
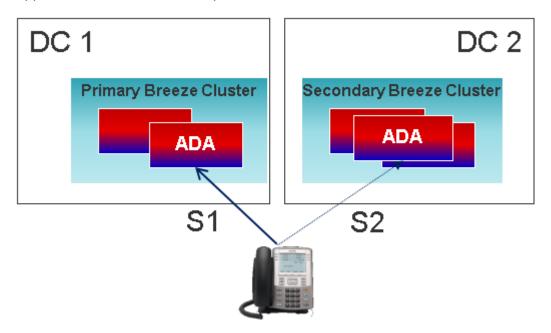
The geo-redundancy model is slightly different for UNIStim endpoints and the Device Adapter nodes, and for MGC of the TDM endpoints and the Device Adapter nodes.

Geo-redundancy between UNIStim endpoints and Device Adapter nodes

UNIStim endpoints have a two-server fail-over model for geo-redundancy, that is, primary server (S1) and secondary server (S2).

The term server refers to the active load balancer for the TPS cluster, including the TPS processing on the Avaya Breeze® platform clusters that have the Device Adapter nodes. The active load balancer resides on one of the nodes in the TPS or Avaya Breeze® platform cluster.

All elements of the Avaya Aura® product family support the Device Adapter solution that can create geographically redundant deployments. Configuration of geographically redundant clusters require administering phones with two Avaya Breeze® platform clusters, and their associated parts, that are not co-located. In this configuration, the first three digits of each cluster node ID must match. For example, if a phone is provisioned with ID 103, then node IDs 1035 and 1037 would match. You must configure this type of redundancy with enough capacity in each cluster to support the total number of endpoints that connect to the solution.
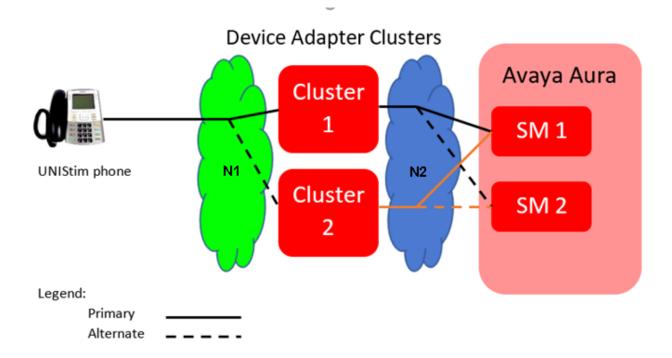
If a UNIStim endpoint loses connectivity, the endpoint tries to register to a node that has the required capacity within S1. Although, the load balancer of the cluster uses the IP address of S1, the final registration is with a single node in the cluster. The endpoint tries to fail over to S2 only when connection to all the TPS nodes on S1 is lost and the load balancer is offline as a result, or if the remaining nodes on S1 do not have the required capacity to support the fail over.

Loss of the primary server (S1) registration connection indicates the node where the phone registered is unavailable. If this happens, the phone tries to register to another node that has the required capacity within S1. If no capacity is available on any of the nodes in S1 or if S1 fails to respond, the endpoints try to fail over to S2.

Example

In the following figure, N1 represents the IP network between the UNIStim endpoint and Device Adapter node. N2 represents the IP network between the Device Adapter node and the Avaya Aura® components.

Device Adapter Clusters
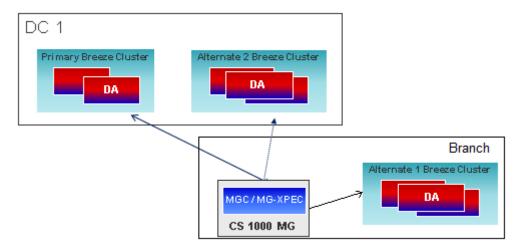
The UNIStim phone registers through the N1 IP network to the Device Adapter node. The solid line represents a registration to the primary cluster S1. The dashed line indicates a possible registration to the alternate cluster S2.

If there is a failure at cluster 1, then either the N1 network, the cluster 1, or the N2 network have experienced an outage, and the endpoint is isolated from the Session Manager and the Avaya Aura® infrastructure. The phone tries registering with cluster 2 by using the dashed line path.

If neither of the registration attempt succeeds, the outage was probably too close to the phone to be resolved by HA and redundancy. For example, the IP cable that connects the phone to the LAN segment may have failed. The phone tries to register periodically till a service personnel rectifies the cable or LAN device failure, and the endpoint registration succeeds.

Geo-redundancy between MGCs of TDM endpoints and Device Adapter nodes

Geographic redundancy for Media Gateway Controllers (MGC) is configured by using Primary, Alternate 1, and Alternate 2 Avaya Breeze® platform clusters.

CS 1000 supports a single core server model and a 1+1 server model for high availability. If both the primary server and, if configured, the secondary server fail to respond, the entire CS 1000 is unavailable. CS 1000 also supports a branch office model that provides fail over support if the CS 1000 is unavailable.

However, Device Adapter reuses the load balancer and multiple Device Adapter nodes to provide a broader coverage of fail-over registration. In a single-node cluster, the MGC tries to fail over to an alternate cluster if the load balancing server fails. In an N+1 node cluster, the MGC tries to fail over to an alternate cluster if the load balancing server and all the nodes in the cluster fail, or if the remaining functional nodes do not have the required capacity to support the fail over.

Device Adapter retains the existing CS 1000 logic for triple MGC registration fail over. During normal operating conditions all devices are registered to the Primary cluster. If the Primary cluster fails, the MGC tries to register the endpoints with the Alt 1 cluster.

An MGC can be programmed to register with one of up to three different clusters: Primary, Alternate 1, and Alternate 2 clusters.

- Registrations are given a predefined period of time to succeed. If the MGC is unable to succeed in that interval, the registration is declared failed.

- The MGC always tries to register with the Primary cluster first.

- If registration to the Primary cluster fails, MGC attempts to register with the Alternate 1 cluster.

- If registration to the Alternate 1 cluster also fails, the MGC attempts to register with the Alternate 2 cluster.

- If registration to the Alternate 2 cluster also fails, the MGC attempts to register with the Primary cluster.

All Avaya Breeze® platform clusters (all servers in a cluster), which are programmed as Primary, Alternate 1, or Alternate 2, receive the configuration of media gateways that are assigned to them. Therefore, the MGC can connect to any of the applicable server clusters and download the config files.

For example, assume that the following clusters are configured:

- Cluster A: Servers 1,2,3
- Cluster B: Servers 4,5,6
- Cluster C: Servers 7,8,9

Assume that a specific MGC is configured as:

- Primary: Cluster A
- Alternate 1: Cluster C
- Alternate 2: none

As a result, the configuration data for this MGC is present on servers 1, 2, and 3 (cluster A) and servers 7, 8, and 9 (cluster C). An administrator can enter the eth0 address for any of these servers to receive the proper config files.

😊 **Note:**

- MGCs can be configured with two features that may attempt to reconnect to the Primary cluster before connecting to Alternate 1.

  The Dual Homing feature defines an alternative connection route to the Primary cluster. If this feature is configured, the MGC will attempt to use this alternative connection route before connecting to Alternate 1.

  The short-term failure timer provides a mechanism for the Primary cluster to be unreachable for a time period before connecting to Alternate 1.
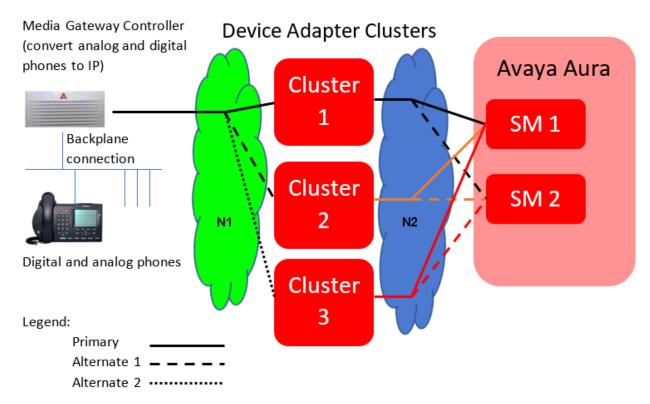
- All MGC resources are reset when the connection transitions to a different cluster. This clears all ongoing calls.

- After the Primary cluster (cluster 1) starts functioning, the MGC switches back to the Primary cluster.

  Alternatively, an administrator can manually configure the switch back option. In this case, the MGC remains registered with the Alternate cluster until the administrator manually runs a command to re-register with the Primary cluster.

  When the MGC fails over or switches back, all MGC resources are reset, which has an impact on endpoint registration and call handling. Hence, you can use the manual switch back option to switch back the MGC during a low traffic window to reduce the impact on endpoint registration and call handling.

Example

In the following figure, the MGC that serves the TDM endpoints registers the endpoints through the N1 IP network to Device Adapter. The solid line represents a registration to the Primary cluster. The dashed and dotted lines indicate a possible registration to the Alt 1 and Alt 2 cluster respectively.

If there is a failure at cluster 1 (Primary cluster), then either the N1 network, the cluster 1, or the N2 network has experienced an outage, and the phone is isolated from Session Manager and the Avaya Aura® infrastructure. The phone tries registering with cluster 2 (Alt 1 cluster) by using the dashed line path.

If the registration attempt at cluster 2 fails, then either the N1 network, the clusters 1 and 2, or the N2 network has experienced an outage, and the endpoint is isolated from Session Manager and the Avaya Aura® infrastructure. The phone tries registering with cluster 3 (Alt 2 cluster) by using the dotted line path.

If none of the registration attempts succeed, the outage was probably too close to the phone to be resolved by HA and redundancy. For example, the IP cable that connects the MGC to the LAN segment may have failed, the line card for the phone may have failed, or other hardware issues may have occurred. The MGC tries to register the endpoints periodically till a service personnel rectifies the cable or LAN device failure, and the MGC registers the endpoints.
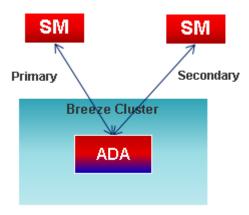
Note that the MGC to Device Adapter is the single point with the capability of defining three options for support within Device Adapter.

HA and geo-redundancy between Avaya Breeze platform clusters and Avaya Aura components

Redundancy by using a primary and secondary Session Manager
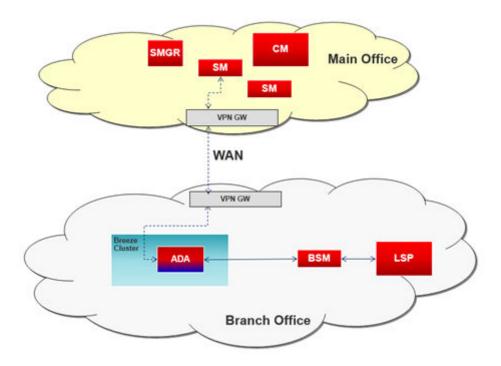
Device Adapter carries out SIP registration on behalf of the UNIStim and TDM endpoints it is supporting.

Configuration of a secondary Session Manager ensures continued telephony service if an interruption occurs on the primary Session Manager.

Redundancy by using branch Session Manager

Device Adapter can be provisioned to use a tertiary branch Session Manager that is not co-located with the primary and secondary Session Managers. When both the primary and secondary Session Managers are unavailable, Device Adapter can use the branch Session Manager to ensure continued telephony service.

Licensing

The following licensing is required to migrate to and use Device Adapter:

- Avaya Device Adapter Snap-in

  Each instance of the Avaya Device Adapter Snap-in requires a license. For more information about the material code for this license, see the Avaya Aura® Offer Definition.

- Avaya Breeze® platform

  The first instance of the Avaya Breeze® platform server is a Suite entitlement. Licenses must be purchased for all subsequent instances of the Avaya Breeze® platform server.

- ProVision / Nortel Migration Tool

  The ProVision application and the associated Nortel Migration Tool (NMT) are provided free of charge to the Device Adapter users for migration of Media Gateway Controllers (MGC) and CS 1000 UNIStim IP, digital, and analog phones.

- Avaya Aura®

  The migrated CS 1000 endpoints have an associated licensing cost in Avaya Aura®. Contact your Avaya sales associate for the cost of the endpoint licensing.

Chapter 3: Migration from CS 1000 to Device Adapter

Migration and deployment checklist

Use the following checklist to complete the migration of CS 1000 configuration to Device Adapter.

> ✱ **Note:**
>
> All documents referenced in this section are available on the Avaya Support Portal at https://support.avaya.com/.

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
1	CS 1000 discovery.	Determine existing deployment elements: • Get KRS records for CS 1000 and associated applications. • Run "orderpro" and generate the summary and detail report. • Determine licensing requirements from the summary report. • Determine gateway and cabinet layout from the detail report. • Determine trunking, RAN, Music, BRI, RLC, and other elements from the detail and summary reports. • Determine applications in use such as AACC, CallPilot, and others. • Create a summary of the system to be used in the migration discussion.	Both			
2	User migration discovery.	• Determine the strategy for migrating users to Avaya Aura®. • Use ProVision or another tool to retrieve the TNB information to determine user eligibility for the migration to Device Adapter.	Both			
3	Determine migration approach.	Users who cannot be migrated to Device Adapter must be moved to other gateways. This includes rewiring phone connections and necessary software configuration changes.	Both			

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
4	Determine migration dial plan.	Examine the existing dial plans to build the migration dial plan approach: • Determine conflicts between systems. • Determine vacant number routing. • Determine session management.	Both			
5	Design the Avaya Aura® solution to accommodate migration and finished states.	• Avaya Aura® core • Applications • Licensing requirements • Hardware and software • Trunking	Both			
6	Define the transition plan.	• Number of phases. • Phased approach or flash cut. • Parallel system connectivity. • CS 1000 software levels and features for integration during migration. • Message waiting lamp.	Both			
7	Deploy Avaya Aura® core and applications.	• Core deployment. • PSTN connectivity. • Connectivity to CS 1000 for migration strategy.	Both			

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
8	Ensure System Manager, Session Manager, and Communication Manager are deployed, active, and ready to accept the migrated CS 1000 configuration. Make test call with 2 Aura SIP sets (96xx).	See the following documents for information and procedures: • *Deploying Avaya Aura® System Manager* • *Deploying Avaya Aura® Session Manager* • *Deploying Avaya Aura® Communication Manager* ✱ **Note:** Information and procedures may be required from additional documents in the product suite depending on individual network and installation environments.	Both	Prerequisite	No	
9	Install and configure Avaya Aura® Device Services if Corporate Directory support is part of the solution.	See Configuring Corporate Directory support on page 201.	Both	Prerequisite	No	
10	Prepare a Personal Directory backup XML file.	See Exporting Personal Directory data on page 95. ✱ **Note:** Configure the Personal Directory backup rule to specify the external FTP server where the backup file should be placed.	UNIStim	30-60 minutes	No	
11	Prepare a CS 1000 Call Server database backup archive. This will be used later to migrate custom feature key labels.	See *Communication Server 1000E Maintenance* for information and procedures on creating this backup file.	UNIStim	15-30 minutes	No	

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
12	Record the CS 1000 properties used by the migration process.	Record the following properties. • Node IP and Node ID. • Codec list including payload size, jitter settings, and VAD. • DTLS policy and client authentication settings. • System-wide LD 15/21 custom timers for interdigit + dialtone (DIDT) and busy/overflow tone (BOTO). • LD 17/22: - PCML: companding law - MSEC: media system security policy, secured number of packets, session key validity time - IDLE_SET_DISPLAY: Idle set display string - DLAC: default "log all calls" option • LD 17/97 (Analog Set Timers): - Minimum Switchhook Flash - Maximum Switchhook Flash - Off Hook Validation - Dial Pulse - Interdigit - Dial Pulse On - Post Flash • LD 56: - Note if the tones and cadences are configured for specific country requirements. Avaya Device Adapter Snap-in provides an option to set a COUNTRY parameter that	UNIStim	60-90 minutes	No	

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
		applies country specific tones and cadences. It will not provide an ability to configure custom tones and cadences. • LD 117: - prt zdst: phone time & date parameters: GMT offset, dst parameters				

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
13	Plan and configure the primary and secondary Session Manager and Communication Manager assigned to each user; including dial plan implementation.	See *Avaya Aura®Solution Design Considerations and Guidelines* for information on this planning task. ⊛ **Note:** The following considerations should also be noted. • Signaling locations must be administered using IP address patterns. • Media locations must be administered using IP address patterns. • Select **Elements** > **Session Manager** > **Application Configuration** > **Applications** from the menu in System Manager and confirm an Application is created for each Communication Manager. • Log in to Communication Manager using SSH and verify that SIP-Signaling group, SIP-trunk group, AAR dial table, Extensions, Codec settings, CompandingLaw, and RoutePattern are configured. • Verify Communication Manager licensing has enough SIP stations, SIP Off-pbx stations, and SIP trunks to support your desired configuration.	Both	4-6 hrs	No	

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
		🛈 **Important:** The ProVision tool does not migrate TN media security policy CLS (MSNV, MSAW). The Administrator should record these for every phone and then implement them through a service profile Media security attribute.				
14	Migrate the CS 1000 endpoint-related data and Media Gateway configuration with the ProVision tool.	See [Migrating the endpoint and MGC-related data](#) on page 99. ✱ **Note:** Select **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** from the menu in System Manager to verify or edit imported endpoints.	Both	2-4 hrs	No	
15	Deploy and configure Avaya Breeze® platform.	See [Avaya Breeze platform deployment checklist](#) on page 138.	Both	60-90 minutes	No	
16	Deploy and configure Avaya Device Adapter.	See [Snap-in deployment checklist](#) on page 169.	Both	30-45 minutes	No	
17	Import the Personal Directory data for UNIStim endpoints.	See [Importing Personal Directory data for UNIStim endpoints from CS 1000](#) on page 123.	UNIStim	60-90 minutes	No	
18	Perform the necessary DHCP configuration to prepare for updating the S1 and S2 IP addresses of the UNIStim endpoints.			2-4 hrs	No	

Table continues…

Avaya Device Adapter Snap-in Reference

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
19	Import Media Gateway Controller configuration into System Manager.	See Importing Media Gateway Controller configuration on page 114.	TDM		No	
20	Switch the UNIStim endpoints from CS 1000 to Device Adapter. Endpoint firmware upgrades automatically.	• See Switching from CS 1000 to Avaya Device Adapter Snap-in on page 125. • See Upgrading firmware and loadware on page 95.	UNIStim	Endpoint switch to Device Adapter takes 15-30 minutes if using DHCP. Endpoint upgrade takes 5-10 minutes.	Yes	
21	Configure Media Gateway Controllers for Device Adapter environment.	Media Gateway Controllers migrated from CS 1000 using ProVision do not need to be added to the solution using System Manager. If you are adding a new Media Gateway Controller to the solution, see Configuring Media Gateway Controllers on page 126 for the configuration procedure. Before you install a new MGC that is shipped from a factory or upgrade an existing MGC, enable the **Enable legacy loadware upgrades** attribute on System Manager. After the MGC is installed or upgraded, disable the **Enable legacy loadware upgrades** attribute. For more information, see MGC installation, upgrade, and registration process on page 125.	TDM			

Table continues…

Step	Action	Description	UNIStim / TDM / Both	Approximate time required	Maintenance window required	✔
22	Register Media Gateway Controllers.	Perform the following tasks for Media Gateway Controllers migrated from CS 1000: 1. Use SSH or a serial connection to connect to the MGC. 2. Remove the MGC from the security domain. 🛈 **Important:** Removing the MGC from the security domain reverts it back to local authentication. Note the local password as this is the only way to access the MGC until it registers with Device Adapter. 3. Change the Call Server IP address to the Avaya Breeze® platform Cluster IP address. 4. Save the new configuration. 5. Reboot the MGC.	TDM		Yes	
23	Configure IP security for Media Gateway Controllers.	See Configuring IP security on page 131.	TDM	5 minutes	No	

Hardware migration

The information in this section describes how TDM hardware is migrated and reused in the Device Adapter environment.

Opt 81C / Opt 51C / Opt 61C / CS 1000M

- EPE modules are replaced by MGC-hosted cabinets.

- IPE modules are reused.

  - NT8D01 XPEC controller card is replaced by MG-XPEC NTDW20 card.

    - MG-XPEC converts the IPE module into two Media Gateway shelves.

    - The MG-XPEC card can be thought of as two separate MGCs bolted together with the left board (motherboard) controlling the left half of the of the IPE shelf and the right (daughterboard) controlling the right half of the IPE shelf.

- NT8D21 ring generator is reused.

- IPE Line ALC and DLC cards are reused.

- Non-IPE Line ALC and DLC cards are replaced by IPE ALC and DLC cards.

- Other IPE cards (such as TDS, DTR, and XUT) are not reused.

- MC32 and MC32s cards are not reused.

- CLASS Modem cards are not reused. Instead, the DSP that is assigned to the CLASS set for voice traffic handles the necessary function, such as, modulate the caller's name and number.

Opt 11

- NTAK11BD, NTDU14CA, and NTDU14CB cabinets are reused.

- The SSC is replaced with an MGC (NTDW60 and NTDW98) card with one or two DSP DB NTDW78.

  - The number of required DSP DBs depends on DSP capacity engineering rules.

- IPE Line ALC and DLC cards are reused.

- Other line cards are not reused.

- CLASS Modem cards are not reused. Instead, the DSP that is assigned to the CLASS set for voice traffic handles the necessary function, such as, modulate the caller's name and number.

CS 1000E

- All cabinets are reused.

- MGC controller (NTDW60 and NTDW98) is reused.

  - It might be required to replace old DSP daughterboards with DB128 to provide higher DSP capacity to serve more endpoints. Refer to the capacity calculation rules below.

- CPMG cards must be replaced by NTDW60 and NTDW98 MGC controllers.

- IPE Line ALC and DLC cards are reused.

- Other line cards are not reused.

- MC32 and MC32s cards are not reused.

- CLASS Modem cards are not reused. Instead, the DSP that is assigned to the CLASS set for voice traffic handles the necessary function, such as, modulate the caller's name and number.

Related links

TDM endpoint capacity rules

- Estimate the number of registered endpoints for every Media Gateway.
    - Estimate the number of connected digital sets
    - Estimate the number of analog line cards.

        ✱ **Note:**

        Analog line cards that are used by CS 1000 and Device Adapter cannot detect whether an analog endpoint is connected, until the endpoint is registered and used.

        If you install an analog line card, Device Adapter registers all 16 endpoints on the analog line card, even if these endpoints are not connected.

- A DSP is required for every endpoint. Support for 160 endpoints would require 160 DSPs provisioned as Voice Gateway (VGW) channels.
    - MGXPEC: Always carries DB96 + DB96.
    - MGC (NTDW60, NTDW98): Has two daughterboard slots for DB32, DB96, or DB128. The second slot (DB2) must be used for a DB with less or the same channel capacity as the first slot (DB1).
        - If the estimated endpoints are more than the number of channels provided, there are two options:
            - If one DB is present, then buy a DB128, insert it to DB1 and the existing one to DB2.
            - If both DB1, DB2 are present, replace one or both daughterboards with DB128.
- If the migration is done from Small System Controller (SSC) with Media Cards (ITG-P, MC32, MC32s):
    - Acquire an MGC (NTDW60, NTDW98) with one or two DB128 depending on estimated endpoint value.

Device Adapter cluster has the following capacity limitations:

- The maximum number of all endpoints registering to Avaya Aura®.
- The maximum number of TDM endpoints.

Device Adapter cluster must be sized to meet the number of endpoints supported.

However, in an MGC-only environment, the maximum number of MGCs supported per cluster is 128. Each MGC supports a maximum of 160 DSP channels. This means that no more than 20,480 TDM endpoints can be placed in a cluster.

In an MGXPEC-only environment, the maximum number of MGXPECs supported per cluster is 64. Each MGXPEC supports a maximum of 256 DSP channels. Hence, a maximum of 16,384 TDM endpoints are supported per cluster.

As the largest cluster is the Large 5+1 deployment with High Availability. Only the 5+1 cluster supports over 20,000 endpoints, supporting up to 25,000 endpoints. Therefore, capacity on Device Adapter cluster remains unused.

Because the cluster allows up to 25,000 endpoints, you can use the following remaining capacity for UNIStim endpoints:

- In an MGC-only environment, you can add up to 4,520 UNIStim endpoints if all MGCs and endpoints on the MGCs are defined.

- In an MGXPEC-only environment, you can add up to 8,616 UNIStim endpoints if all MGXPECs and endpoints on the MGXPECs are defined.

For more information about cluster sizing considerations, see Cluster considerations for a Unified Communications environment on page 141.

Related links

Hardware migration on page 92

Exporting Personal Directory data

Procedure

1. Log in to the CS 1000 Signaling Server by using SSH and the appropriate credentials.

2. Enter the command line interface by running the command: `vxShell`.

3. Create a backup file of the Personal Directory information by running the command: `pd pdExp`.

4. Download the backup file from `/var/opt/nortel/pd/pd.xml`.

5. Log out of the Signaling Server.

Upgrading firmware and loadware

Device Adapter supports the upgrade of UNIStim IP and digital phone firmware and Media Gateway Controller loadware. Phones that are not upgraded before migration are automatically upgraded the first time they register with Device Adapter. Device Adapter is configured with the most current version of firmware for each type of supported phone.

> **Important:**
>
> Please note the firmware file distributed with Device Adapter cannot be changed. Future firmware updates are distributed with a new Device Adapter release that incorporates the new firmware. This new version must be installed to upgrade the associated phones.

The following table lists the exact firmware version Device Adapter applies to each UNIStim phone model.

Model	Firmware version
IP Phone 2001 Phase 2	DCO
IP Phone 2002 Phase 1	B76
IP Phone 2002 Phase 2	DCO
IP Phone 2004 Phase 0/1	B76
IP Phone 2004 Phase 2	DCO
IP Phone 2007 Phase 2	C96
IP Phone 1110	C98
IP Phone 1120E	C98
IP Phone 1140E	C98
IP Phone 1150E	C98
IP Phone 1165E	C98
IP Phone 1210	C98
IP Phone 1220	C98
IP Phone 1230	C98

Upgrades are performed using the UFTP protocol. Device Adapter does not provide a built-in TFTP server.

❗ Important:

A two-step upgrade may be required for some 1120E and 1140E IP desk phones. 1120E and 1140E IP desk phones using firmware earlier than 0624C1B and 0625C1B must first be upgraded to this firmware version or newer using CS 1000 before they will accept upgraded firmware from Device Adapter. Avaya recommends upgrading to 0624C3G and 0625C3G firmware for this intermediary step.

✳ Note:

Device Adapter upgrades of UNIStim phone firmware can be disabled using CLI commands or through the Device Adapter management screens in System Manager.

✳ Note:

Avaya strongly recommends upgrading the firmware of 39XX phones to version 7.65 before migrating to Device Adapter. CS 1000 provides functionality for system-wide scheduled upgrades of digital phones. This speeds the migration and deployment of 39XX phones into the Device Adapter solution. After migrating to Device Adapter, 39XX phones can only be upgraded on an phone-by-phone basis.

39XX phones with firmware Release 25.40 or later can patch the present release and then download the 7.65 firmware. For more information, see "Dynamic PDSL installation" in the *Telephones and Consoles Fundamentals Avaya Communication Server 1000, Release 7.6 (NN43001-567)* guide on the Avaya Support portal.

CS 1000 endpoints migration using ProVision and Nortel Migration Tool

The ProVision application and the Nortel Migration Tool (NMT) are used to migrate CS 1000 endpoint and MGC-related data. These tools are provided free of charge to Avaya Device Adapter users, for migration of CS 1000 UNIStim IP, digital, and analog phones and Media Gateway Controllers (MGC). You must register at https://provision.avaya.com to receive your licensed copy of the software.

Visit the ProVision web portal to download ProVision software, retrieve a license key, and learn more about using ProVision. Existing users can login with their current credentials while new users should click the New User? Register now link to get started. Whether an existing or new user, contact the ProVision Help Desk to request the free Device Adapter subscription after portal registration is complete.

> ✱ **Note:**
>
> Existing users with a current (paid) subscription should visit the Licensing -> Subscription Administration page and retrieve a fresh license key as Device Adapter features are now included at no additional charge. This allows our users with paid subscriptions to maintain a fully featured ProVision while performing Device Adapter migrations.

This site also provides training in the set up and use of these tools. See the ProVision *Getting Started* guide available at https://provision.avaya.com/iProVision/secured/downloads/default.aspx?docID=645 for a list of recommended courses that includes:

- *What is ProVision*
- *Introduction to ProVision*
- *Connecting to a Switch Using ProVision*
- *Using Grids and Forms in ProVision*
- *Setting Up and Managing Projects in ProVision*
- *Using Models*

The *Getting Started* guide also provides information on how to obtain the templates necessary to complete this procedure.

Installation and initial configuration of ProVision is not covered by this procedure.

The following items are exported from the CS 1000 database and imported into the Avaya Aura® solution.

- LD 20 TNB (set, DN, and speed/hotline list data)
- LD 21 (redirect, attendant data)
- LD 22 (system data)
- Feature Key Labels
- PDT shell (MGC configuration data)

> **✴ Note:**
>
> This tool will connect to CS 1000, do an overlay printout, and convert the data into Avaya Aura® users and Communication Manager stations. The tool provides a choice of endpoints to migrate and modify the generated Communication Manager stations.

You must run ProVision on Microsoft Windows with Administrator privileges to function properly. For more information on configuring an application to run with Administrator privileges on Microsoft Windows, see the following procedure from Microsoft: https://technet.microsoft.com/en-us/library/ff431742.aspx.

ProVision considerations

The ProVision tool suite, including the Nortel Migration Tool, allows the administrator to migrate either a subset or all of the terminals from CS 1000 into the ProVision database, carry out manipulation of data as needed, and then load the data on the applicable Avaya Aura® servers. ProVision also allows the administrator to replace TNs when collapsing multiple CS 1000 systems into a single Avaya Breeze® platform cluster. After collapsing, the Nortel Migration Tool creates a `.csv` file for each collapsed CS 1000 which contains TN data.

However, the migration does not provide the complete infrastructure.

- Some elements, such as an Avaya Breeze® platform cluster to provide the Call Park and Page service, must be manually created before using the service on Device Adapter.

- Some elements, such as class-of-service data and class-of-restriction data, must be defined to assign them to Device Adapter endpoints.

- The other servers in the infrastructure do not fall under the migration and data setup of the stations migrated from CS 1000 to Device Adapter. It is possible that the tools may be used to program the servers after they are deployed, but that is out of scope for this document.

- For SCR/SCN and MCR/MCN:

  - You can map SCR and MCR with the appropriate button type and set the per button ring control to Ringing during migration.

  - You can map SCN and MCN with the appropriate button type and set the per button ring control to Non-ringing during migration.

  However, ProVision does not support setting the per button ring control to Delayed and Abbreviated for SCR and MCR. After the migration is completed, you can manually set the per button ring control to Delayed or Abbreviated for SCR and MCR by using System Manager or Communication Manager.

  For more information, see "Basic and Per Button Ring Control" in "Appendix H: Call processing features and services."

For more information about the migration procedure, see the ProVision Getting Started guide and tutorials that are available at: https://provision.avaya.com/iProVision/secured/downloads/default.aspx?docID=645

For more information about the feature operation of the migration tools, see the ProVision documentation.

Migrating the endpoint and MGC-related data

About this task

You can use the ProVision application and the associated Nortel Migration Tool to migrate the CS 1000 endpoint data.

Before you begin

Ensure you are using the latest version of ProVision.

If required, prepare Communication Manager for feature migration. For more information about this additional preparation work, see Preparing Communication Manager for feature migration on page 115.

Procedure
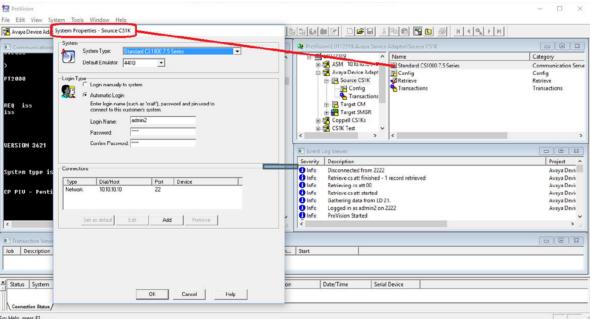
1. Retrieve data from CS 1000 on page 99

2. Start Nortel Migration Tool and assign a station type to the CS 1000 endpoints on page 103

3. Review the new stations on page 110

4. Review the MGC Import.xml file on page 111

5. Review the new SIP users on page 112

6. Send transactions to target Communication Manager and System Manager on page 113

Retrieving data from CS 1000
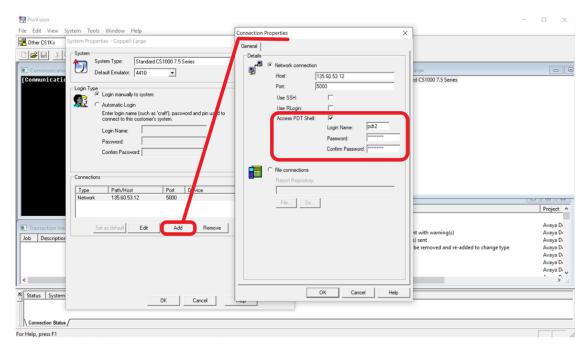
Procedure

1. Start ProVision.

2. Apply System properties for the source CS 1000.
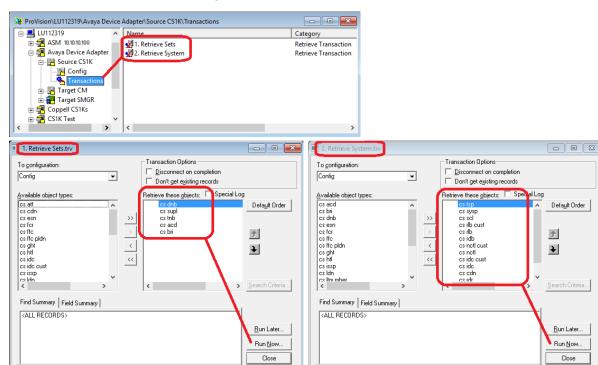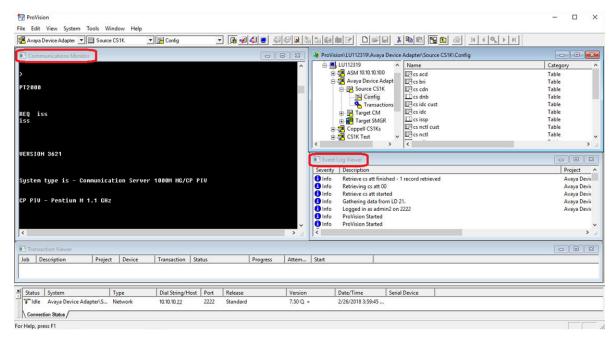
3. Do the following to retrieve Media Gateway Controller (MGC) information:

   a. Click **Add** on the **System Properties** window.

   b. Select **Access PDT Shell**.

   c. Enter the appropriate credentials in fields provided.

   d. Click **OK**.

Avaya Device Adapter Snap-in Reference

4. Retrieve the CS 1000 data using the transactions available in the **Source CS1K** folder.
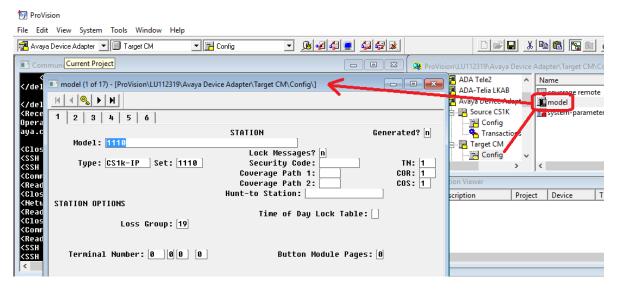
5. Process progress is displayed on the **Communications Monitor** and **Event Log Viewer**.

6. Review Communication Manager models.

The **Model** window is located in the `Config` folder of the Target Communication Manager in the migration project. Models are templates that define global attributes for groups of
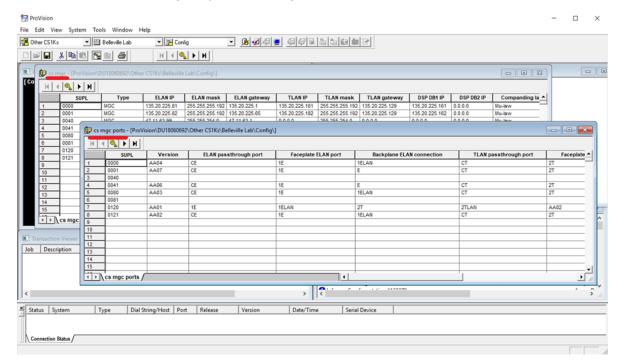
stations related to the target ProVision project. Models should be created before the Nortel Migration Tool is run.

7. Review the `cs mgc` and `cs mgc ports` tables, located in the `config` folder of the source CS1K project, to verify Media Gateway Controller data retrieved from the PDC shell.

✳ **Note:**

These tables are used by the Nortel Migration Tool to create an XML file that is imported into the target System Manager.

8. Make any necessary changes to the Media Gateway Controller data.

Related links
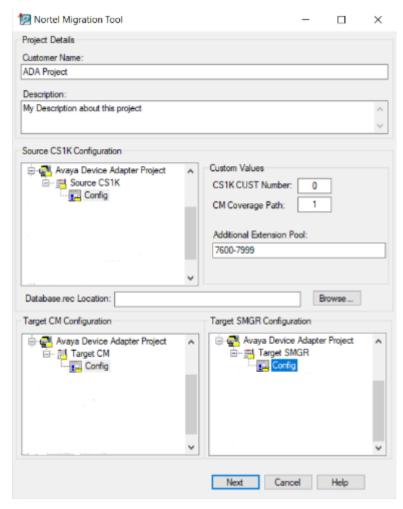
[Migrating the endpoint and MGC-related data](#) on page 99

Starting Nortel Migration Tool and assigning a station type to the CS 1000 endpoints

Procedure
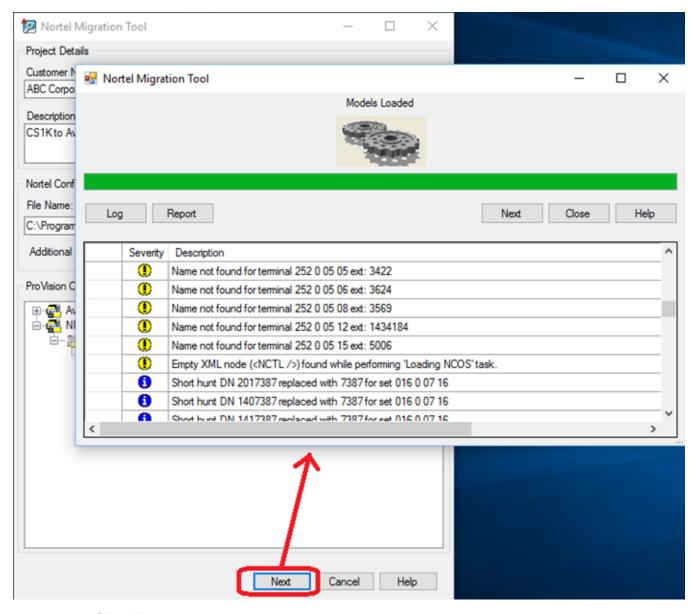
1. Start the Nortel Migration Tool (NMT) by selecting **Tools** > **Migration Tools** > **Nortel Migration Tool** from the menu.

2. Enter the following information to begin the migration.

   - Customer name.

   - Customer description.

   - Source CS 1000 CUST number.

   - Additional extension pool — a range of numbers used to create stations with a unique primary extension.

   - Source CS 1000 deployment.

   - Target System Manager and Communication Manager deployment.

   - Select **FKL Integration**.

   - Click **Browse**, locate, and select the `Database.rec` file.
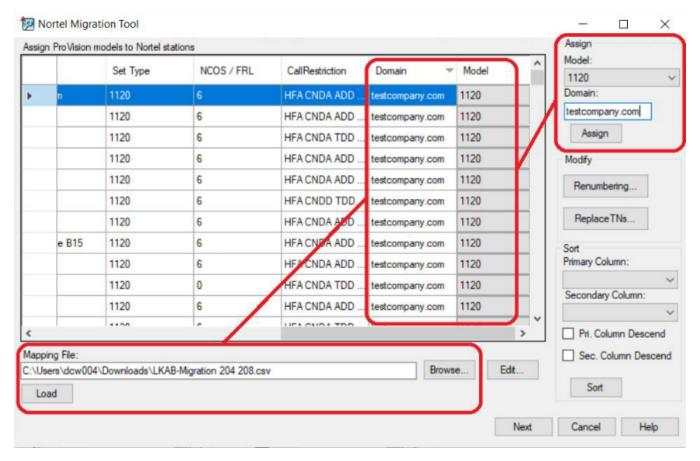
⊛ **Note:**

For more information, see Feature Key Label (FKL) migration for UNIStim endpoints on page 120.

3. Click **Next**.

4. A progress window is displayed. Note any errors or warnings displayed during the migration process.
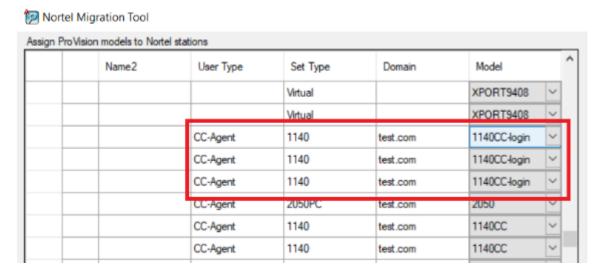
5. Click **Next**.

6. Assign each migrated CS 1000 set a Communication Manager station type and SIP domain.

   ⚹ **Note:**

   • Assign XPORT9408 to all virtual stations

   • Station types are populated from the target project Communication Manager **Model** window. The SIP domain is provided by the customer.
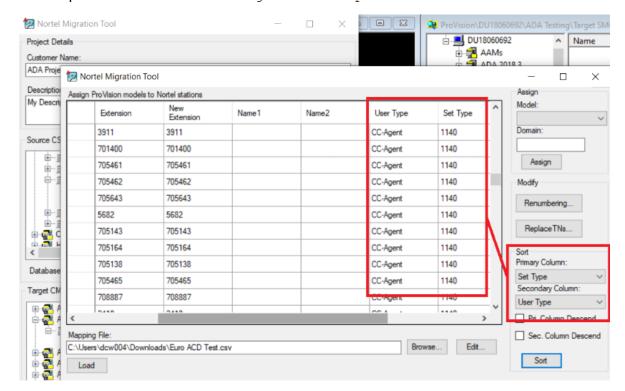
7. For each Call Center (CC) endpoint, apply the required model.

   *** Note:**

   You can apply the default CS1K-IPCC model or create custom models. The field values defined in custom models, for example, buttons, override the field values generated by NMT.

CC endpoints are identified as `CC-Agent` or `CC-Supervisor`.
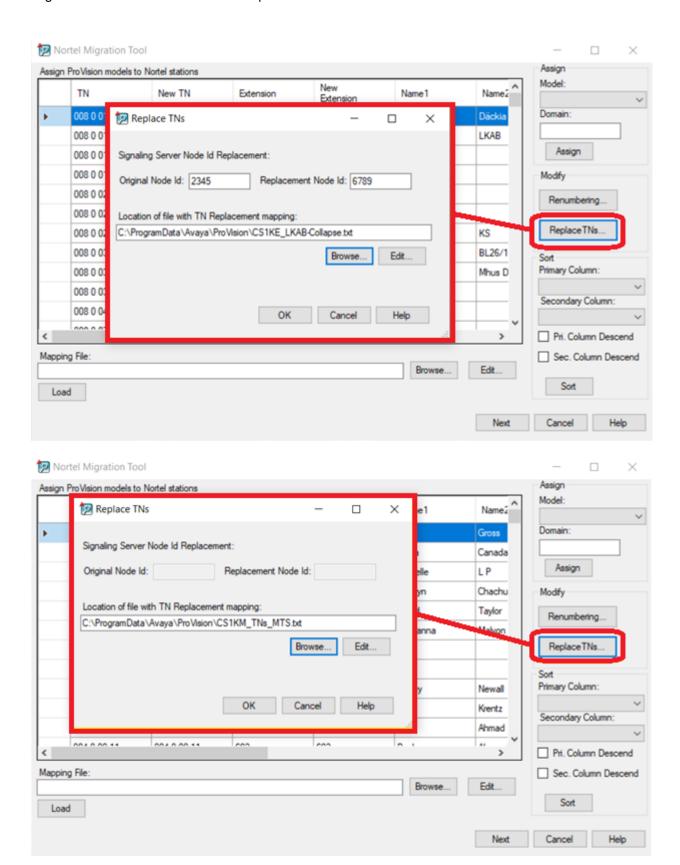
8. Create a TN mapping file.

   For more information about the TN mapping file, see on page 110.

9. Click **Replace TNs**.

10. In the Replace TNs dialog box, click **Browse**.

11. Select the TN mapping file.

12. **(Optional)** For CS 1000E, type the old and new node IDs in **Original Node Id** and **Replacement Node Id** fields.
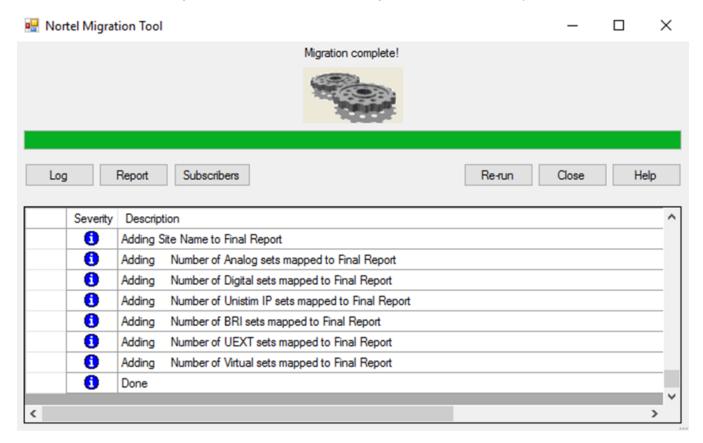
    You can use the original node ID as the replacement node ID if it is not already assigned on the Avaya Breeze® platform cluster.

    For CS 1000M, the **Original Node Id** and **Replacement Node Id** fields are disabled, as CS 1000M is a TDM system which is directly wired and does not have node IDs.

13. Click **OK**.

14. Click **Next**.

    When the migration is complete, a final progress window is displayed.

15. **(Optional)** To view logs, a final report, and all station-related data processed during migration, click the following :

    • **Log**
    • **Reports**
    • **Subscribers**

    NMT generates an `.xlsx` file that contains log entries, reports, or subscriber information.

    For CC endpoint migrations, log entries provide additional details for each CC station added.

16. Click **Close**.

Next steps

Re-configure the TN data on endpoints.

For more information, see Re-configuring TN data on endpoints

Related links

Migrating the endpoint and MGC-related data

TN mapping file requirements

When collapsing multiple CS 1000, use the Replace TNs feature to avoid terminal number (TN) conflicts. To use this feature, you must create a TN mapping file.

The TN mapping file must meet the following requirements:

- Have the `.csv` or `.txt` format.

- Contain original TN and replacement TN separated by a comma.
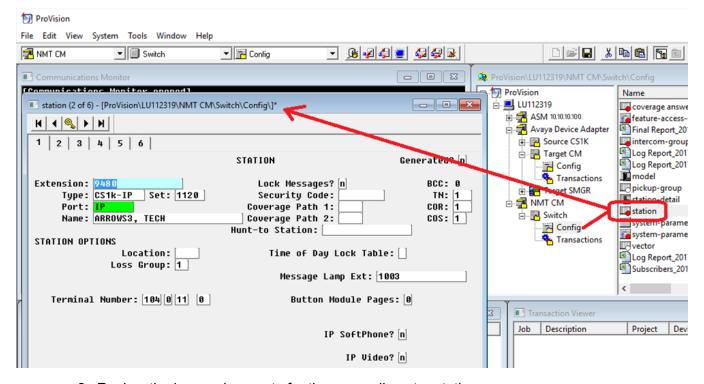
For a CS 1000E system, both original TN and replacement TN must include a loop and shelf. For example: `008 0, 028 0`

For a CS 1000M system, the original TN must include a loop and shelf, and the replacement TN must include only a loop. For example: `004 0, 008`
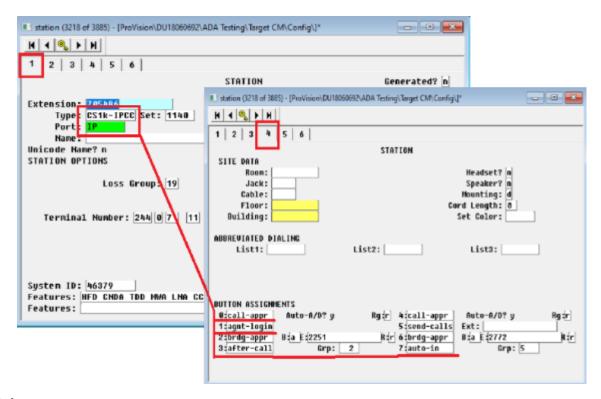
Reviewing the new stations

Procedure

1. Review the new stations in ProVision.

2. Review the key assignments for the new call center stations.

Related links
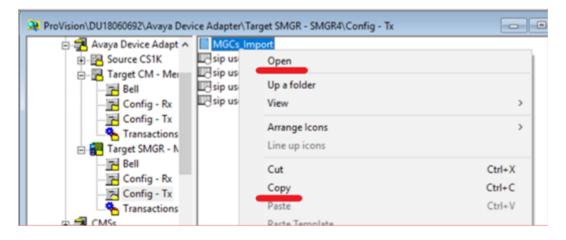
[Migrating the endpoint and MGC-related data](#) on page 99

Reviewing the MGC Import.xml file

Procedure
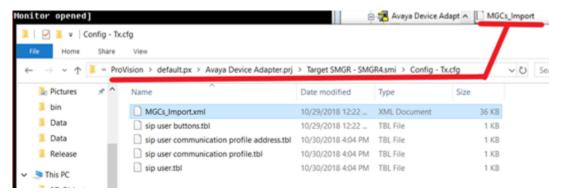
In Provision, review the MGC_Import.xml file in the target System Manager `Config` folder.

This file is imported into System Manager through the web UI separately. Open the file for review or to be saved to another location by doing one of the following:

• Right-click the file and click **Copy** or **Open**.

- Use Windows Explorer to navigate to the file location on the local system.

Related links
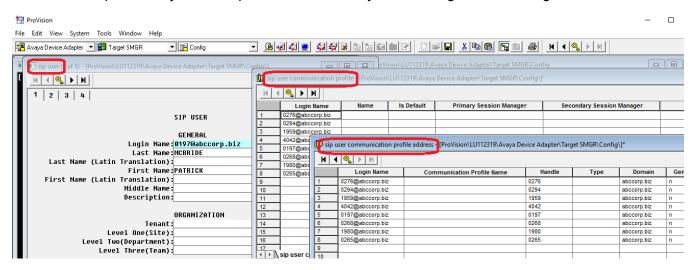
[Migrating the endpoint and MGC-related data](#) on page 99

Reviewing the new SIP users

Procedure

In ProVision, review the new SIP users.

Fill all required Avaya Aura® specific cells in the System Manager tables using the GRID form.

Related links
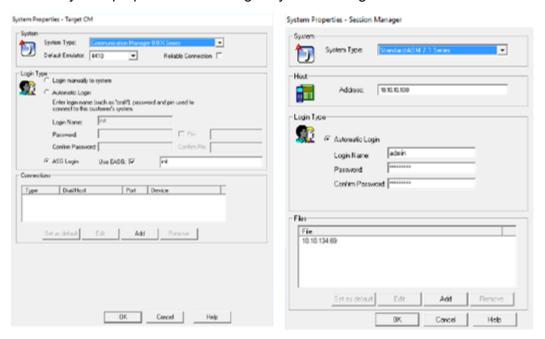
[Migrating the endpoint and MGC-related data](#) on page 99

Sending transactions to target Communication Manager and System Manager

Procedure
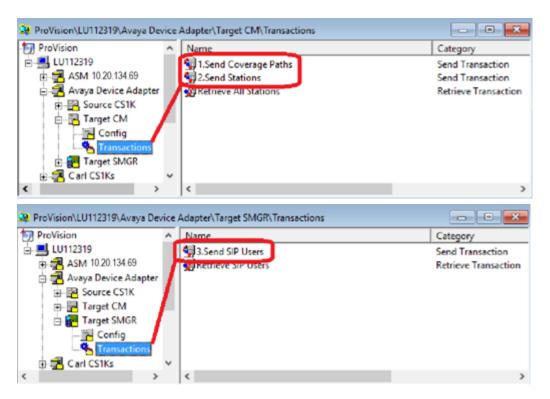
1. Set the system properties for the target System Manager and Communication Manager.

2. Send the migrated data to the target System Manager and Communication Manager using the available **Send** transactions.

   ❗ **Important:**

   Transactions must be run in the following order:

   a. Send Coverage Paths

   b. Send Stations

   c. Send SIP Users

Process progress is displayed on the **Communications Monitor** and **Event Log Viewer**.

The migration process is complete.

Related links

Importing Media Gateway Controller configuration

About this task
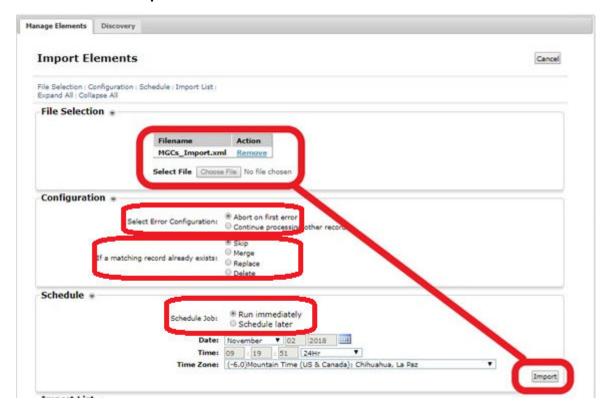
Use the following procedure to import the Media Gateway Controller configuration file created by ProVision.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Select **Services** > **Inventory** > **Manage Elements** from the menu.

3. Select **More Actions** > **Import**.

4. Click **Choose File**.

5. Select the `MGC_Import.xml` file created by ProVision.

6. Click **OK**.

7. Select **Abort on first error** in the **Select Error Configuration** field.

8. Select **Skip** in the **If a matching record already exists** field.

9. Select **Run immediately** in the **Schedule Job** field.

10. Click **Import**.

Preparing Communication Manager for feature migration

Note the following actions and information while preparing Communication Manager for feature migration:

- Station Migration

  - Ensure there are no conflicts between existing Communication Manager extensions and migrated extensions

  - Administrator should configure Dialplan and Routing so that it satisfies all migrated extensions.

  - Review CS 1000 NARS, BARS, and CDP migration into Communication Manager AAR and ARS.

  - In case the number of migrated sets is less than the number of DNs on these sets, administrators should define an extension pool to be used to assign extensions for sets that does not win any DN as an extension.

- Multiple Appearance DN

  - In the case that the number of DNs is greater than the number of sets, such a DN is translated as Virtual/XPORT Station type: 9408. See Configuring XPORT 9408 on page 201 for more information.

- Short Hunt

  - Short Hunting is generally translated as multiple call appearance buttons on the station.

  - When the short hunt is to a number that is not a call appearance (extension) of any station, the short hunt virtual station XPORT 9408 is created for the purposes of this feature.

  Example

  1. Assume that a user has Short Hunt on their endpoint.

     User 0 Extensions:

     - on key 0 is 5381234

     - on key 1 is 5385000

     - on key 2 is 5385001

     - on key 3 is 5385002

     If these extra 3 DNs do not exist anywhere else in the CS 1000, then this can be changed to:

     User 0 Extensions:

     - on button 1 is 5381234, appearance 0

     - on button 2 is 5381234, appearance 1

     - on button 3 is 5381234, appearance 2

     - on button 4 is 5381234, appearance 3

     No need for XPort.

  2. Assume that some other user has Short Hunt on their endpoint but hunts to a MADN appearance of 5381234.

     User 0 Extensions:

     - on key 0 is 5381234

     - on key 1 is 5385000

     - on key 2 is 5385001

     - on key 3 is 5385002

     User 1 Extensions:

     - on key 0 is 5384321

     - on key 1 is 5381234

     If these extra 3 DNs do not exist anywhere else in the CS 1000, then this can be changed to:

     User 0 Extensions:

     - on button 1 is 5381234, appearance 0

- on button 2 is 5381234, appearance 1

- on button 3 is 5381234, appearance 2

- on button 4 is 5381234, appearance 3

User 1 Extensions:

- on button 1 is 5384321, appearance 0

- on button 2 is 5381234:

    - bridged appearance to call appearance 0 would be normal

    - bridged appearance to any call appearance is also valid

No need for XPort. If the map was to a secondary DN, XPort is needed.

3. Assume that some other user has Short Hunt on their endpoint but hunts to a MADN appearance of 5385000 that has no endpoint where this can be the station extension.

User 0 Extensions:

- on key 0 is 5381234

- on key 1 is 5385000

- on key 2 is 5385001

- on key 3 is 5385002

User 1 Extensions:

- on key 0 is 5384321

- on key 1 is 5385000

If the short hunt DN is not a call appearance anywhere on the CS 1000, then this can be changed to:

User 0 Extensions:

- on button 1 is 5381234, appearance 0

- on button 2 is 5385000, any appearance

- on button 3 is 5385000, any appearance: it is possible that the button is not needed.

- on button 4 is 5385000, any appearance: it is possible that the button is not needed.

- (If the user is to put up to 3 calls on hold to answer a fourth, then all four buttons are needed.)

User 1 Extensions:

- on button 1 is 5384321, appearance 0

- on button 2 is 5385000, any appearance

XPORT Extensions:

- on button 1 is 5385000, appearance 0

- on button 2 is 5385000, appearance 1

- on button 3 is 5385000, appearance 2

- on button 4 is 5385000, appearance 3

XPort is needed.

- Call Waiting

  - The Call Waiting key is translated as a call appearance button on the station.

- Privacy Release

  - Administrators should configure Communication Manager / System / System Parameters – Features / AUTOMATIC EXCLUSION PARAMETERS: **Automatic Exclusion by COS? Y**

  - The ProVision/NMT tool sets COS #1 for all migrated stations.

  - Administrators should configure Communication Manager / System / Class Of Service: Number: 1 Automatic Callback: Y

- Autodial

  - CS 1000 ADL key destination number is not translated to an autodial button during migration. Phone users should configure it after migration. These autodial buttons have no administratively configured number.

- Call Forward Busy / No Answer / Make Set Busy

  - Call Forward Busy / No Answer/ MSB features are translated to the Coverage feature.

  - It is represented by coverage path and coverage remote tables.

  - Redirect numbers that do not represent Directory Numbers in migrated extensions are treated as Coverage Remote entries:

    - TNB:

      - FDN

      - HUNT

    - ATT_DATA:

      - ATDN (in case of Customer redirection(RDR_DATA: FNAL/D) configuration is ATT)

  - For Redirect numbers that represent Coverage Remote entries, dialplan / routing should be properly configured. Take into account uniform dialplan.

  - Administrator should configure System parameters call coverage / call forwarding Maintain SBA At Principal: N

  - Short Hunting feature also may use Coverage Path in some special cases.

- Call Pickup

  - Call Pickup is translated to pickup groups.

  - A pickup group only supports 100 extensions.

  - Administrator should allow Extended; Direct pickup in System Parameters Features.

  - ProVision / NMT tool sets COR #1/2/3/4 for all migrated stations.

  - Administrator should configure Communication Manager / System / Class Of Restriction With the exact correspondence of Numbers and parameters:

    COR Number: 1 Can Be Picked Up By Directed Call Pickup? N Can Use Directed Call Pickup? N

    COR Number: 2 Can Be Picked Up By Directed Call Pickup? Y Can Use Directed Call Pickup? N

    COR Number: 3 Can Be Picked Up By Directed Call Pickup? N Can Use Directed Call Pickup? Y

    COR Number: 4 Can Be Picked Up By Directed Call Pickup? Y Can Use Directed Call Pickup? Y

- Group Call Pickup

  - Group Call Pickup uses Extended Pickup groups.

  - User experience is changed for group call pickup.

  - To access another group, user should enter Pickup Number from the Extended Pickup Group associated with Pickup Group Number.

  - Pickup Group Index may not match with Pickup Group Number on CS 1000.

  - Extended pickup group supports only 25 groups within itself.

- Message Waiting Indicator; Message / Inbox Key; Call Park

  - VoiceMail and Call Park deployment should to be preconfigured and integrated with Aura.

  For more information about configuring the Park and Page service for the network, see the Avaya Aura® configuration documentation.

  For more information about deploying and configuring the voice mail system, see the documentation for deploying and configuring the voice mail system that is used with the Avaya Aura® cloud. The voice mail server that is used is dependent on interoperability with Communication Manager and not Device Adapter.

- Message / Inbox Key

  - Voice Main Number of User should be filled in ProVision.

  - Fill user communication profile ProVision table column: Endpoint Profile – Voice Mail Number by voicemail system number using GRID editor after the NMT tool conversion.

- Speed Dial, Hotline

  - Speed Dial and Hotline translate to abbreviated-dialing group lists.
  - Need to configure Abbreviated Dialing List1/2/3 Access Code.
  - Special hotline virtual station XPORT 9408 is created for purposes of this feature.

Feature Key Label (FKL) migration for UNIStim endpoints

> ✴ **Note:**
>
> FKL migration is only applicable to UNIStim endpoints. 39XX endpoints store Feature Key Labels locally and cannot be migrated.

The migration administrator or customer is responsible for providing the CS 1000 `database.rec` binary file used for FKL migration. The file is obtained by performing a backup of the CS 1000 data prior to migration activities. Performing Overlay 43 EDD will initiate the process and create the backup file when complete.

The file is saved to the directory location `/u/db/database.rec`. The file can be retrieved through an FTP connection or by using a removable media (flash drive) device.

The migration administrator is provided the `database.rec` file and places it on to the computer running ProVision and the Nortel Migration Tool (NMT). The recommended location is: `C:\ProgramData\Avaya\ProVision`. The migration administrator runs the remaining steps related to migration preparation, retrieving set and system data using ProVision, as described. During the migration process, the NMT tool converts CS 1000 data into Communication Manager and System Manager table data. Any associated FKL data is stored in the target System Manager `sip user buttons` table for each endpoint with what will now be button label data.

The following are the main NMT tool dialog fields related to FKL migration:

- **FKL migration checkbox** — Enables the text field and button used to provide path to the `database.rec` file. The default path is `C:\ProgramData\Avaya\ProVision`.
- **Browse... button** — Used to navigate to and select the path to `database.rec` file through a standard Windows dialog.

Re-configuring TN data on endpoints

About this task

During the migration from CS 1000 system to a Avaya Breeze® platform cluster, the nodes and terminal numbers can be changed. To configure multiple endpoints with new node and TN data, use the `adaSetReconfigure` command.

Use the remapping file which the ProVision tool creates during CS 1000 data migration.

Before you begin

Migrate CS 1000 system data to an Avaya Breeze® platform cluster with Nortel Migration Tool. For more information, see .

Procedure

1. Transfer the remapping file to the Avaya Device Adapter Snap-in master node using FTP.

   The target directory on the master node is `/home/cust directory`.

2. On the master node, run the following command to start re-configuring CS 1000 device TNs:

   `adaSetReconfigure enable /home/cust/<remapping file name>.txt`

3. **(Optional)** To view the status of re-configuration, run the following command:

   `adaSetReconfigure status`

   You can view the remapping file name and the re-configuration status. The status can be `ENABLED` or `DISABLED`.

4. To stop re-configuring, run the following command:

   `adaSetReconfigure disable`

Reverting endpoint reconfiguration

About this task

If any issue occurs during the reconfiguration process, use the revert method. To revert the endpoint data, use the same remapping file that was used for reconfiguration.

Before you begin

Run the **`adaSetReconfigure disable`** command to disable reconfiguration.

Ensure that the devices are registered with Device Adapter.

Procedure

1. To enable reverting, run the following command:

   `adaSetReconfigure enablerevert /home/cust/<remapping file name>.txt`

2. To start reverting, run the following command:

   `adaSetReconfigure revertall`

3. **(Optional)** To view the status of reverting, run the following command:

   `adaReconfigure revertstatus`

4. To disable reverting, run the following command:

   `adaSetReconfigure disablerevert`

Reverting reconfiguration on a single endpoint

About this task

The **`revertsingle`** command allows the administrator to revert a single endpoint data reconfiguration.

Before you begin

Run the `adaSetReconfigure disable` command to disable reconfiguration.

Ensure that the devices are registered with your server.

Procedure

1. To enable reverting, run the following command:

   `adaSetReconfigure enablerevert /home/cust/<remapping file name>.txt`

2. To revert data reconfiguration on a single endpoint, run the following command:

   `adaSetReconfigure revertsingle <loop> <shelf> <card> <unit>`

   For example: `adaSetReconfigure revertsingle 100 0 0 2`

3. To disable reverting, run the following command:

   `adaSetReconfigure revert`

Reverting example

The following is the process of configuring and reverting TNs on an 1140 endpoint when the ProVision configuration is completed and the data is migrating to the Avaya Aura® system.

1. The endpoint TN is 4 0 0 0. It is currently registered to node 2000 on an existing CS 1000 system.

2. The endpoint is transferred from CS 1000 to Device Adapter. Device Adapter uses node 3500, however there is another endpoint that is already configured on Device Adapter with TN 4 0 0 0.

3. ProVision maps this endpoint to TN 252 0 0 0.

4. The administrator uploads the remapping file generated by the ProVision tool to the Avaya Breeze® platform master node using FTP and runs the `adaSetReconfigure enable /home/cust/<provisionmapfile>.txt` command.

5. The DHCP server is reconfigured to have S1 as the Avaya Breeze® platform master node instead of the CS 1000 TPS.

6. The endpoint restarts.

7. The endpoint tries to register with the Avaya Breeze® platform node as node 2000 and TN 4 0 0 0, which it has in memory.

8. Device Adapter with the relocation feature enabled recognizes the endpoint in the map and sends it a message to change the node and TN, and then restarts the endpoint.

9. The endpoint registers to Device Adapter with node 3000 and TN 252 0 0 0. Registering is mandatory for the reverting functionality to work correctly.

10. The `adaSetReconfigure revert` command reads the map and detects that endpoint with TN 252 0 0 0 and node 3000 is registered. Then the endpoint receives a command to change the TN and node back to the original data: node 2000 and TN 4 0 0 0.

11. After the DCHP server is reverted and the S1 of this endpoint is changed back to CS 1000, the endpoint can register back to CS 1000.

Loading an additional remapping file

About this task

You can load an additional remapping file for endpoint data reconfiguration.

Before you begin

Generate a remapping file in ProVision.

Procedure

1. Transfer the remapping file to the Avaya Device Adapter Snap-in master node using FTP.

   The target directory on the master node is `/home/cust directory`.

2. On the master node, run the following command:

   `adaSetReconfigure loadfile /home/cust/<additional remapping file name>.txt`

Removing a remapping file

About this task

You can remove a remapping file from the TN conversion table or map.

Before you begin

Ensure you have multiple remapping files loaded to the TN conversion table or map.

Procedure

To remove a remapping file, run the following command:

`adaSetReconfigure removefile /home/cust/<additional remapping file name>.txt`

Importing Personal Directory data for UNIStim endpoints from CS 1000

About this task

Use this procedure to import Personal Directory data for UNIStim endpoints. Note that this procedure is intended only for new installations of Device Adapter and overwrites any data currently in the cluster database for Releases 8.1.1 and earlier and in PPM for Release 8.1.2.

> ⊛ **Note:**
>
> 39XX endpoints store Personal Directory data locally. It cannot be migrated.

Procedure

1. Locate the `pd.xml` file created in the 'Exporting Personal Directory data'.

2. Upload the `pd.xml` file to any directory in the active server in the Avaya Breeze® platform cluster.

3. Log in to the active server by using SSH and the appropriate credentials.

4. **(Optional)** Enter the command line interface by running the command: **`vxShell`**.

5. Run the **`pdImport`** command to import the Personal Directory contacts either from CS 1000 or Device Adapter snap-in. CS 1000 and Device Adapter snap-in Release 8.1.1 and earlier saves the imported contacts in the cluster database where as Device Adapter snap-in Release 8.1.2 saves the contacts in the PPM.

   ⊛ **Note:**

   - The `pd.xml` file in **`pdImport <full_path_to_pd.xml_file>`** command is obtained from a CS 1000 system.

   - You must run the **`pdImport`** command only if the endpoints are configured but not registered with System Manager.

   - The **`pdImport`** command works only if the `pd.xml` file is saved in either `/var/tmp` or `chmod 755 /home/cust` location on Avaya Breeze® platform server.

   To see usage help, enter **`pdImport`** with no arguments

   The command syntax when importing PD contacts from Device Adapter snap-in is **`pdImport <full_path_to_pd_xml_file>`**.

   The command syntax when importing PD contacts from CS 1000 are:

   - **`pdImport <full_path_to_pd_xml_file> <customer number> <domain>`**

   - **`pdImport <full_path_to_pd_xml_file> <customer number> <domain> <prefix>`**

   - **`pdImport <full_path_to_pd_xml_file> <customer number> <domain> <hloc> <prefix>`**

   For example, **`pdImport /var/tmp/pd.xml 9 ada.avaya.com 343 111`** command will import the PD contacts of users with customer number 9 and hloc value 343 from CS 1000.

   If a prefix is not required, provide customer number and domain name only.

   Validation: If the data was imported successfully for the specified customer number, the following log is printed:

```
pdImport /opt/Avaya/snap_in/da/pd/pd.xml 9.ada.avaya.com 343 111
=== PD ===
Parsing completed.
140 user(s) have been imported for customer 9.
```

Switching from CS 1000 to Avaya Device Adapter Snap-in

About this task

Use the following procedure to switch from CS 1000 to Avaya Device Adapter Snap-in.

Procedure

1. Put the Avaya Breeze® platform cluster into Accept Service mode.

2. Update the node IP address (S1) of UNIStim endpoints that you want to migrate either manually or by using DHCP.

   Update all endpoints if you want to move them simultaneously. If you want to perform a phased migration, update only those endpoints that you want to move in a phase.

3. Do the following:

   ❶ Important:

   This procedure requires a maintenance window of approximately one hour post completion.

   • Shut down the CS 1000 signaling servers that host only IP lines for UNIStim endpoints.

   • Remove the IP lines from the CS 1000 signaling server if the CS 1000 signaling server hosts IP lines along with other components such as H.323 and SIP trunks, gatekeeper, and proxy servers.

MGC installation, upgrade, and registration process

About this task

This topic provides an overview of an MGC installation, upgrade, and registration process.

Before you begin

Before you upgrade an existing MGC that is running the CS 1000 software, enable the **Enable legacy loadware upgrades** attribute on System Manager. The **Enable legacy loadware upgrades** attribute temporarily enables a program on the Avaya Breeze® platform node that accepts MGC registrations by using the sunPRC protocol. The sunPRC protocol is the old CS 1000 call server protocol used to register and upgrade an MGC.

If you want to replace an existing MGC or add an additional new MGC from the factory, enable the **Enable legacy loadware upgrades** attribute on System Manager. MGCs that are shipped from the factory are programmed by using the CS 1000 version of the MGC software. These MGCs require an upgrade to the Device Adapter software by using the **Enable legacy loadware upgrades** attribute.

Procedure

1. Log in to MGC by using SSH.

2. At the MGC CLI command prompt, run the following command to turn off central authentication on CS 1000 and leave the security domain:

   leaveSecDomain

3. After the security domain is removed, use the local authentication password until the MGC registers to Device Adapter.

4. Change the call server IP address to Avaya Breeze® platform cluster IP address.

5. MGC reboots and registers to Device Adapter by using sunRPC and upgrades the loadware.

6. MGC again reboots and re-registers to Device Adapter by using pbxLink.

7. If you encounter problems during the registration, do the following:

   a. Run the following command to revert to CS 1000 call server:

      ldb>swapActivePartition

      value = 0 = 0*0

   b. Use the following command to change the call server IP address to CS 1000 IP address:

      mgcsetup

Next steps

After the MGC registers to Device Adapter, disable the **Enable legacy loadware upgrades** attribute on System Manager.

Related links

[Media Gateway controller registration](#) on page 345

Configuring Media Gateway Controllers

About this task

In most cases, the Media Gateway Controller (MGC) migration is carried out by using the ProVision tools and no administrative operation is required.

For more information, see the ProVision documentation.

However, you can validate and change the configuration. You can do this by using System Manager.

Use the following procedure to add a new MGC to a Device Adapter solution. MGCs that are migrated by using ProVision from a CS 1000 solution do not require this configuration.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Navigate to **Services** > **Inventory**.

3. Click **Manage Elements**.

4. On the **Manage Elements** tab, click **New**.

5. On the New Elements page, on the **General** tab, in the **Type** field, click **Device Adapter Media Gateway**.

6. On the Add Device Adapter Media Gateway page, on the **General** tab, specify the configuration information for the MGC or MG-XPEC.

   In the **Loop/Shelf** field, specify the first two parts of the TN. For example, TN 20-1-3-14, refers to loop 20, shelf 1, card 3, and unit 14 on the card.

   In the **ELAN IP** field, specify the ELAN IP address that is used to communicate with Device Adapter.

   In the **DSP DB1 IP** and **DSP DB2 IP** fields, specify the DSP daughterboard IP addresses. One daughterboard cannot support an entire MGC if it is fully populated. An MGC with some cards unused can use a single daughterboard.

7. On the **Device Adapter** tab, specify the cluster information.

   You must specify the primary cluster. The other alternate clusters are used only for redundancy.

8. On the **VoIP** tab, specify the media stream information.

   This includes supported codecs, options in those codecs, and the codec preference (first, second, third).

9. On the **Analog Sets** tab, specify the information for analog endpoints.

   These settings typically do not change. But, you can edit the information such as DTMF parameters and CLASS endpoint settings.

10. On the **Miscellaneous** tab, specify the information such as labels in alarm reports.

11. Click **Commit**.

12. Open Avaya Breeze® platform.

13. Select **Configuration** > **Attributes** from the menu.

14. Select the **Service Clusters** tab.

15. Select the applicable cluster in the **Cluster** field.

16. Select **DeviceAdapter** in the **Service** field.

17. Navigate to the **IP Telephony Node** section.

18. Locate the **Node Id** attribute.

19. Select **Override Default**.

20. Enter the applicable Node ID in the **Effective Value** field.

21. Click **Commit**.

Considerations to connect MGC to a data network

Media Gateway Controller (MGC) has the following four network connectors on the faceplate:

- 1E, which is the ELAN port
- 2T, which is the TLAN port
- CE
- CT

Consider the following to connect MGC to a data network:

- Connect only the 1E and 2T connectors to a layer 2 switch to support the Device Adapter environment. Do not connect the CE and CT connectors.
- On System Manager, administer the following four IP addresses to configure the MGC managed element:

  - ELAN IP address

    This address is internally bound to the 1E (ELAN) port. The MGC loadware uses this address.

  - TLAN IP address

    This address is internally bound to the 2T (TLAN) port. The MGC loadware uses this address to communicate with the DSP daughterboards.

  - DSP DB1 IP address

    This address is internally bound to the 2T (TLAN) port. The DSP DB1 VoIP media streams use this address.

  - DSP DB2 IP address

    This address is internally bound to the 2T (TLAN) port. The DSP DB2 VoIP media streams use this address.

- The TLAN, DSP DB1, and DSP DB2 IP addresses must be on the same subnet, which is the TLAN subnet.
- The ELAN IP address is on an ELAN subnet.
- Connect the 1E (ELAN) port to a Layer 2 switch of the ELAN subnet.
- Connect the 2T (TLAN) port to a Layer 2 switch of the TLAN subnet.
- Unlike in the CS 1000 environment, in the Device Adapter environment, separation of the ELAN subnet from the TLAN subnet is not mandatory. The ELAN and TLAN subnets can be the same subnet and you can connect the 1E and 2T ports to the same layer 2 switch.
- For network implementation, ensure the following:

  - Connectivity between the MGC ELAN subnet and the Device Adapter Security Module subnet.

  - Connectivity between the MGC TLAN subnet and other media termination points, such as media sources and sinks, in the solution.

    The one-way network delay for both ELAN (signaling) connections and TLAN (media) connections should be below 50 milliseconds (100 milliseconds RTT).

- Administration of any additional IP routes on the MGC in the Device Adapter environment is not required.

- Redundant data connectivity, that is, redundant wiring and layer 2 switches for each ELAN and TLAN ports, is supported by using the E and T networking connectors on the MGC chassis. For more information, see the CS 1000 documentation.

Connecting a new or an existing MGC to a data network

About this task

The following procedure provides a high-level overview about connecting a new or an existing MGC to a data network.

Procedure

1. On System Manager, administer the following four IP addresses to configure the managed element that represents the Device Adapter media gateway:

   - ELAN IP address

   - TLAN IP address

   - DSP DB1 IP address

   - DSP DB2 IP address

   TLAN IP, DSP DB1 IP, and DSP DB2 IP addresses must be on the same TLAN subnet.

   ELAN IP address can be on a separate ELAN subnet.

2. For a new MGC deployment, do the following:

   a. Connect the MGC 1E faceplate port to the layer 2 switch of the ELAN subnet.

   b. Connect the MGC 2T faceplate port to the layer 2 switch of the TLAN subnet.

      Unlike in the CS 1000 environment, in the Device Adapter environment, separation of the ELAN subnet from the TLAN subnet is not mandatory. The ELAN and TLAN subnets can be the same subnet and you can connect the 1E and 2T ports to the same layer 2 switch.

   c. **(Optional)** Establish redundant data connectivity, such as, redundant wiring and layer 2 switches for each ELAN and TLAN ports, by using the E and T networking connectors on the MGC chassis.

      For more information, see the CS 1000 documentation.

3. For an existing MGC deployment, disconnect any cables connected to the CE and CT ports on the MGC faceplate.

4. Ensure the following:

   - Connectivity between the MGC ELAN subnet and the Device Adapter Security Module subnet.

- Connectivity between the MGC TLAN subnet and other media termination points, such as media source and sinks, in the solution.

The one-way network delay for both ELAN (signaling) and TLAN (media) connections should be below 50 milliseconds (100 milliseconds RTT).

If this connectivity does not exist, administer additional routing rules on the solution routers as required.

Secure connection between Device Adapter and MGC by using IPSec

IPSec is an IP-layer protocol intended to secure traffic between a pair of hosts, also known as targets. In the context of this topic, these targets are MGC and Device Adapter.

There are a number of related protocols and methods that provide host authentication, encryption, and operation modes. These protocols and methods involve a handshaking dialog between the two peer targets to negotiate cryptocontexts that are used to secure the traffic.

The handshaking dialog contains two phases:

- Phase 1

  Uses the ISAKMP protocol to authenticate the host by using the pre-shared key that you specify in the **Preshared key value for IPsec** attribute. For more information, see "Configuring IP security."

- Phase 2

  Uses the IKE protocol over an encrypted channel that is created during Phase 1 to negotiate the new cryptocontext of 1024 bits and more. This cryptocontext is used to secure traffic between the peer targets.

MGC runs on the VxWorks platform, and currently, low-level IPSec functionality is provided by using the Mocana NanoSec product. Avaya Breeze® platform uses the Linux IPSec module, which is based on the libreswan IPSec package.

The following are the differences when IPSec is used with CS 1000 and Device Adapter:

- In CS 1000, IPSec is highly configurable with different security levels such as OPTI and FULL.

- In Device Adapter, there is only one IP port between Device Adapter and MGC. All traffic goes through this port.

  Because there is only one protocol and one port, there are no configuration options. All communication between Device Adapter and MGC is secured by using Intra-System Signaling Security (ISSS).

IPSec feature is implemented to secure traffic between Avaya Breeze® platform and MGC servers. All tools and libraries that are required for IPSec are installed on Avaya Breeze® platform during

Device Adapter installation. Additional manual configuration on Avaya Breeze® platform is not required. If you uninstall the Device Adapter snap-in from Avaya Breeze® platform, these tools are also automatically removed.

In some scenarios, manual synchronization of IPSec configuration is required for media gateways. For more information, see

Related links

Configuring IP security

About this task

Use the following procedure to configure IP security for the Media Gateway Controllers in the solution.

The values that you specify in the **Enable IPsec for Media Gateways** and **Preshared key value for IPsec** fields are global. You cannot have different pre-shared keys (PSK) on different Avaya Breeze® platform and MGC servers.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Click **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. On the Attributes Configuration page, click the **Service Globals** tab.

5. In the **Service** field, click **DeviceAdapter**.

6. Navigate to the **IP Security (IPsec)** area.

7. In the **Enable IPsec for Media Gateways** field, in **Effective Value**, click **Yes**.

   The default value is **No**.

8. In the **Preshared key value for IPsec** field, in **Effective Value**, type the pre-shared key for data cyphering.

   ⊛ **Note:**

   Key must be 16 to 32 characters in length and can contain only numbers and letters.

   If you enable the FIPS mode on Avaya Breeze® platform server the pre-shared key must be 32 characters in length.

9. **(Optional)** To override the default values, select the **Override Default** check box.

Result

IPsec is automatically enabled on the Media Gateway Controller when this configuration is complete.

The following configuration files are created:

- For Avaya Breeze® platform server: The `swan.secrets` and `swan.conf` files are created in the `/etc/ipsec.d` folder. These files are used by the `libreswan` system IPSec library. These files contain the PSK and list of connections with MGCs assigned to the cluster. Avaya Breeze® platform server contains two connections per MGC, for UDP and TCP ports. If the cluster contains more than one Avaya Breeze® platform, additional connection is added with the cluster IP.

- For MGC server: The `ipsec.xml` and `activate.txt` files are created, in human-readable form, in the `/e/sdm` folder. The XML file contains settings for all MGC servers configured in System Manager. It is parsed by MGC loadware and data reliable to this MGC is stored in the `/e/db/isec/isss.dat` file, which is used to init IPSec during startup.

Related links

[Manually synchronizing IPSec configuration](#) on page 133

Media gateway configuration

No configuration is required when a media gateway is already registered and an administrator changes the IPSec state. In this case, the IPSec information, which is the PSK and the allowed targets, is uploaded to MGC automatically. The PSK is stored securely on the MGC compact flash.

Otherwise, manual synchronization of IPSec configuration is required. This requirement protects Device Adapter from unauthorized MGC registrations.

Manual synchronization is required in the following scenarios:

- A new media gateway is added while IPSec is turned on in Device Adapter.

- Media gateway boots from Gold image while IPSec is turned on in Device Adapter. This happens after MGC compact flash is erased or when MGC is delivered from factory.

- Media gateway is moved to another Avaya Aura® system where Device Adapter has the IPSec turned on.

- Media gateway that is previously registered with Avaya Aura® (1) with IPSec turned on, is moved to Avaya Aura® (2) where IPSec is turned off.

- There are MGC registration issues.

Caveats

- Change in parameters, such as On/Off status or PSK key, leads to connection breach for several seconds. After that MGC servers reconnect with the new settings.

- MGC restarts when primary or alternate cluster changes, irrespective of whether IPSec is enabled or disabled. After restarting, MGC connects to a new Avaya Breeze® platform cluster.

⊛ **Note:**

> When MGC with the old loadware tries to connect to Avaya Breeze® platform server with FIPS mode enabled and Avaya Device Adapter Snap-in installed, then you should upgrade the MGC loadware using steps mentioned in the MGC installation, upgrade, and registration process.

Related links

Manually synchronizing IPSec configuration on page 133

Manually synchronizing IPSec configuration

Procedure

1. Log in to media gateway over SSH or serial connection by using the admin2 account.

2. Type the `mgcsetup` command.

3. Do the following:

   a. Skip to the `Configure IPsec now?` prompt and type `y`.

   b. Type the management IP address (eth0) of any Avaya Breeze® platform server in a cluster where the MGC is assigned.

      The cluster can be Primary, Alternate 1, or Alternate 2 cluster.

   c. Type the Avaya Breeze® platform server management credentials that are used to get CLI access over SSH (cust or root, and appropriated password, both are acceptable).

   d. Upon successful synchronization, MGC shows the `Successfully retrieved ipsec.xml file` message.

   e. Restart MGC for the synchronization to take effect.

Related links

Media gateway configuration on page 132

Migration examples

Migration example: one Device Adapter cluster for CS 1000

The following description is an example of the migration of a three-site CS 1000 installation into a geographically redundant pair with branch survivability.

Existing CS 1000 installation

The existing CS 1000 installation consists of three sites: Main Site, M Site, and Q Site. The Main Site migrates from CS 1000.1. The M Site migrates from CS 1000.2. The Q Site migrates from CS 1000.3.

Post-migration topology

The Main Site and M Site are configured as a geographically redundant pair.

- A System Manager is configured on each site as a geographically redundant pair.
- A Duplex Communication Manager is configured.
- A pair of Session Managers is configured on each site.
- A high availability Device Adapter cluster is configured on each site.
- Two Profile 4 Virtual Machines provide highly available Device Adapter service for up to 5000 endpoints.
- Each additional Profile 4 Virtual Machine adds support for an additional 5000 endpoints.
- All resources on the Main Site and M Site are engineered to be able to handle all endpoints from the solution across all sites.
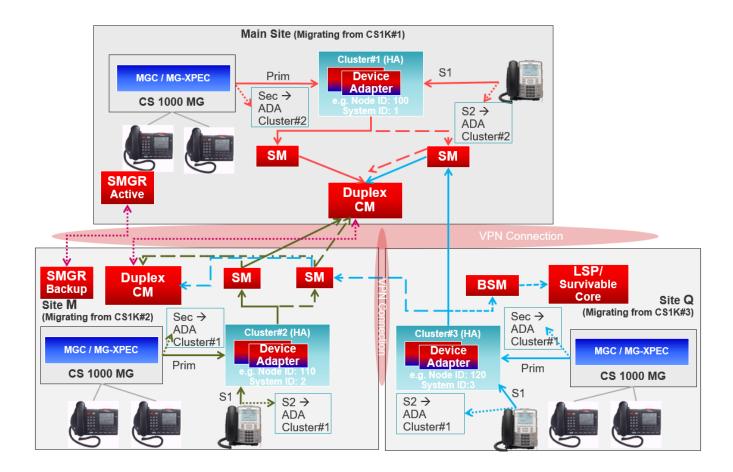
The Q Site is configured as a survivable branch.

- An LSP / Survivable Core is configured.
- A Branch Session Manager is configured.
- A high availability Device Adapter cluster is configured.
- Two Profile 4 Virtual Machines provide highly available Device Adapter service for up to 5000 endpoints.
- Each additional Profile 4 Virtual Machine adds support for an additional 5000 endpoints.
- All resources in the Q Site are engineered to be able to handle all endpoints on the Q Site only.

😊 **Note:**

This migration involves three CS 1000 systems. Using three separate Device Adapter clusters minimizes the administration involved in the migration.

The following diagram is the topology of the post-migration configuration.

Migration example: collapsing three CS 1000s into one cluster

The following description is an example of the migration of a three-site CS 1000 installation into a geographically redundant Device Adapter cluster with branch survivability.

Existing CS 1000 installation

The existing CS 1000 installation consists of three sites: Main Site, M Site, and Q Site.

- The Main Site migrates from CS 1000.1
- The M Site migrates from CS 1000.2
- The Q Site migrates from CS 1000.3

Migration

The three sites of the existing CS 1000 installation have duplicated TN ranges. However, not all sites have the same duplication.

The following TNs are used in this example:

- Main Site – uses 100 0 x x (including 100 1 x x), 108 0 x x, and 116 0 x x
- M Site – uses 104 0 x x and 124 0 x x
- Q Site – uses 100 0 x x, 104 0 x x, and 108 0 x x

This means Q Site has three duplicated TN ranges: 100 0 and 108 0 with the Main Site, and 104 0 with M Site. As Q Site has all the duplications, it is decided to change the TNs on Q Site only.

Mapping duplicate TN ranges to new ranges is implemented as follows:

TN range	Main Site	M Site	Q Site
100 0 x x	Left as 100 0 x x	Not used	Moved to 112 0 x x
104 0 x x	Not used	Left as 104 0 x x	Moved to 120 0 x x
108 0 x x	Left as 108 0 x x	Not used	Moved to 128 0 x x
112 0 x x – Not initially used	Not used	Not used	Used for Q Site
116 0 x x	Only used here. Left as 116 0 x x	Not used	Not used
120 0 x x – Not initially used	Not used	Not used	Used for Q Site
124 0 x x	Not used	Only used here. Left as 124 0 x x	Not used
128 0 x x – Not initially used	Not used	Not used	Used for Q Site

The numbers of the three sites analyzed do not have any duplications. Furthermore, the dial plan in all three sites provides direct dialing using the extensions of the site. That is, if 555xxxx is on the Main Site, 556xxxx on the M Site, and 557xxxx is on the Q Site, Main Site user 5551234 can dial 5561234 to reach the M Site user. Creating a dial plan is based on this model.

Post-migration topology

The sites are configured as a single cluster in geographically redundant data centers. The data centers have their own cluster, but also have a failover cluster for the other data center.

For example, data center 1 is the data center for the three sites that aligns for the Sunny Day scenario.
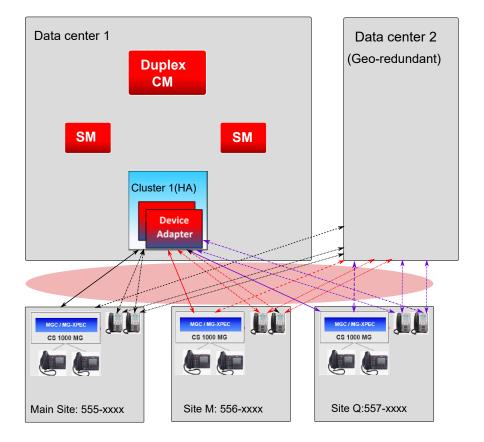
- All resources in data centers are engineered to be able to handle all endpoints from the solution across all sites.
- A System Manager is configured in each data center as a geographically redundant pair.
- A Duplex Communication Manager is configured per data center.
- A pair of Session Manager is configured in each data center.
- A high availability Device Adapter cluster is configured in each data center.
  - Two Profile 4 Virtual Machines provide highly available Device Adapter service for up to 5000 endpoints.

- Each additional Profile 4 Virtual Machine adds support for an additional 5000 endpoints.
- Additional resiliency can be configured for improved resiliency for MGCs:
    - An LSP / Survivable Core with a local (scaled down) Device Adapter is configured.
    - A Branch Session Manager is configured.
    - A high availability Device Adapter cluster is configured, with a suitable size.
    - All resources in the survivable site are engineered to be able to handle only MGCs that fail over to this data center.

⊛ **Note:**

This migration involves three CS 1000 systems. Using one Device Adapter cluster with geographical redundancy minimizes the migration administration.

The following diagram is the topology of the post-migration configuration.

Chapter 4: Avaya Breeze® platform deployment for Device Adapter

Avaya Breeze® platform deployment checklist

Use the following checklist for deployment planning.

No.	Task	Description	Notes	✔
1	Review performance and capacity information.	See Performance and capacity constraints and requirements for both UC and CC environment on page 139.		
2	Review Avaya Breeze® platform cluster considerations.	See Avaya Breeze platform cluster considerations on page 141.		
3	Review hardware requirements.	See Avaya Breeze platform hardware requirements on page 146.		
4	Review snap-in licensing requirements.	See Licensing on page 82.		
5	Download snap-in software from PLDS.	See Downloading software from PLDS on page 148.	Download the file `DeviceAdapter-8.x.x.x.x.`	
6	Deploy and configure Avaya Breeze® platform.	See Deploying and configuring Avaya Breeze platform on page 149.	Avaya Breeze® platform requires a VMware ESXi 6.0 or 6.5 instance with a minimum of a Standard license.	

Performance and capacity constraints and requirements for both UC and CC environment

The following table summarizes the capacity constraints of Device Adapter for both UC and CC environments:

Capacity	Maximum supported number	Notes
Maximum number of Avaya Breeze® platform nodes in an Avaya Aura® solution managed by a single System Manager.	50	Avaya recommends that all System Managers be implemented as a pair, with High Availability. This allows System Manager to handle network events more gracefully.
Maximum number of Avaya Breeze® platform nodes in a cluster.	6 (with 5+1)	Supported options include a single node per cluster or N+1 clusters, with N nodes for call handling and 1 for redundancy. N can be 1 to 5.
Maximum number of Device Adapter endpoints in an Avaya Aura® solution managed by a single System Manager.	200,000	Device Adapter endpoints can be any combination of UNIStim, digital, and analog endpoints.
Maximum number of Device Adapter endpoints in a single Avaya Breeze® platform Profile 2 node.	1000	
Maximum number of Device Adapter endpoints in a single Avaya Breeze® platform Profile 4 node.	5,000	
Maximum number of Device Adapter endpoints in a cluster.	• Avaya Breeze® platform Profile 2 node: 5,000 • Avaya Breeze® platform Profile 4 node: 25,000	
Maximum number of digital and analog endpoints per Media Gateway and MGC.	160	Maximum number of digital and analog endpoints per Media Gateway is based on a 10 card (NTAK11 or NTC310AAE6) chassis. Other models have a different capacity. For more information about different platforms, see Supported TDM hardware on page 55.
Maximum number of digital and analog endpoints per IPE shelf and MG-XPEC.	256 (2x128)	The IPE shelf is handled by the MG-XPEC as two separate 8–slot MGCs. However, the MG-XPEC itself is a single card.

Table continues…

Capacity	Maximum supported number	Notes
Maximum number of MGCs per Avaya Breeze® platform node profile 2.	6	This number is based on fully occupied 10–slot media gateway cabinets.
Maximum number of MGCs per Avaya Breeze® platform node profile 4.	31	
Maximum number of MG-XPECs and IPE shelves per Avaya Breeze® platform node profile 2.	3	If all IPE shelves are fully populated, then only 3 shelves (profile 2) or 19 shelves (profile 4) can be used. Any additional shelves that are fully populated exceed the maximum number of endpoints for the Device Adapter node.
Maximum number of MG-XPECs and IPE shelves per Avaya Breeze® platform node profile 4.	19	
Maximum number of DSPs per MG-XPEC card.	192	The maximum number of DSPs per MG-XPEC card is 256 (2*128).

The following constraints should also be considered:

- A single Device Adapter cluster can only manage the endpoints of one CS 1000 system.
- Multiple Device Adapter clusters can handle the endpoints of the same CS 1000 system.
- A standard Avaya Breeze® platform OVA is deployed with a CPU speed of 2.2 Ghz. This must be changed to 2.4Ghz after the OVA is deployed.

Additional performance and capacity constraints and requirements for a CC environment:

In addition to the preceding performance and capacity constraints, performance and Busy Hour Call Completion (BHCC) ratings in a call center also depends on the capacities and capabilities of the call center. For example, the number of announcements, Computer Telephony Integration (CTI) applications that are used, the type of announcement and conference server, and whether calls are recorded.

Furthermore, the time till which the call is in queue before it is routed to an agent affects the sustained rate.

Device Adapter capacity is utilized only during the time a user or an agent answers the call.

The following is a comparison of Device Adapter capacity utilization for a UC and a CC call:

- The total call processing time required for a UC call is any of the following:
  - The duration till which the phone rings plus the duration for which the user answers the call before hanging up.
  - The duration till which the phone rings before the call is transferred to a voice mail plus the duration till which the caller leaves a voice message before hanging up.
- The total call processing time required for a CC call is the following:
  - The duration till which the call is in the queue before it is transferred to the agent and the duration for which the agent answers the call before hanging up.

    In addition to the above, a call center might offer additional services before, during, and after the call. For example, allow the caller to leave a feedback after the call. These

services are handled by Call Center Elite. Hence, Device Adapter capacity remains unutilized during this period.

Until the queue in a call center reaches a steady state, the additional time required per call queue rate means that fewer CC calls are handled per hour as compared to UC calls. After the queue time reaches a steady state, either because of overflowing the calls to another queue or less time required for call servicing, the CC call handling rate is approximately the same as the UC call handling rate.

But if the CC calls overflow because they were in the queue for too long, the overall average CC call handling rate remains below the UC call handling rate.

If the calls do not overflow to another queue in the call center and the caller abandons the call, the calls are cleared without being answered and the Busy Hour Call Completion rate considers these as failed calls.

For more information about performance and capacity constraints and requirements in a call center environment, see the *Avaya Aura® Call Center Elite Overview and Specification* guide.

Avaya Breeze® platform cluster considerations

The capacity of a solution, administered by a single System Manager or a High Availability System Manager pair, is limited to the maximum number of Avaya Breeze® platform servers that can be deployed in a solution. A maximum of 50 Avaya Breeze® platform servers can be deployed in a solution that has the Avaya Device Adapter Snap-in loaded. If you want more Device Adapter nodes, an additional System Manager or High Availability pair of System Manager is needed to administer the nodes.

> ✳ **Note:**
>
> Avaya recommends that you use a High Availability System Manager pair in a call center environment.

For information about the Avaya Breeze® platform virtual machine profiles, see Avaya Breeze platform hardware requirements on page 146.

Cluster considerations for a Unified Communications environment

The following table contains information about the Avaya Device Adapter Snap-in cluster capacity for a UC environment:

Avaya Device Adapter Snap-in Configuration	Description	Number of Avaya Breeze® platform Nodes	Avaya Breeze® platform Profile	Capacity
1	Small one server deployment without High Availability.	1	2	Up to 1000 endpoints
2	Small 1+1 deployment with High Availability.	1+1 = 2		Up to 1000 endpoints
3	Small 2+1 deployment with High Availability.	2+1 = 3		Up to 2000 endpoints
4	Small 3+1 deployment with High Availability.	3+1 = 4		Up to 3000 endpoints
5	Small 4+1 deployment with High Availability.	4+1 = 5		Up to 4000 endpoints
6	Small 5+1 deployment with High Availability.	5+1 = 6		Up to 5000 endpoints
7	Large 1+1 deployment with High Availability.	1+1 = 2	4	Up to 5000 endpoints
8	Large 2+1 deployment with High Availability.	2+1 = 3		Up to 10000 endpoints
9	Large 3+1 deployment with High Availability.	3+1 = 4		Up to 15000 endpoints
10	Large 4+1 deployment with High Availability.	4+1 = 5		Up to 20000 endpoints
11	Large 5+1 deployment with High Availability.	5+1 = 6		Up to 25000 endpoints

Note:

The capacity listed in the preceding table is based on the assumption that the Avaya Device Adapter Snap-in is the only snap-in running on the Avaya Breeze® platform cluster.

Cluster considerations for a call center environment

Device Adapter Release 8.1.2 supports using 1140 and 2050 IP phones in a Call Center Elite environment. Customers can use these phones either as Unified Communications (UC) or Call Center (CC) phones in a call center. When a call center agent or supervisor logs in to the phone, the phone operates as a CC phone and provides the call center features. Otherwise, it operates as a UC phone. Customers can also use these phones exclusively as UC phones in their call center environment.

Determining the Device Adapter cluster capacity for a call center environment depends on the following factors:

- Capacities of other elements in the Avaya Aura® network. For example, a single Communication Manager supports a maximum of 10,000 simultaneously logged in call center agents.

- Call center considerations:

  - Call Center Elite supports a maximum of 10,000 simultaneously logged in SIP endpoints.

    For example, a call center has a total of 15,000 endpoints. Out of these 15,000 endpoints, call center agents have simultaneously logged in to 10,000 endpoints. The remaining 5,000 endpoints operate as UC endpoints. If another agent tries to log in, Call Center Elite rejects the log in attempt.

    A Device Adapter cluster that has more than 10,000 simultaneously logged in agents must have two or more Communication Managers and Call Center Elite servers.

  - If an endpoint is configured as a CC endpoint and when the endpoint registers with Avaya Aura®, Device Adapter considers it as a UC endpoint. Call center features are available on the endpoint only after the agent logs in to the endpoint. Because there is no mechanism to determine how many agents will log in at any given time, the capacity is determined by how many CC endpoints can register and log in simultaneously.

  - Call center message flows contain more messages, for both call control and notifications, than UC message flows. Therefore, there is more message traffic per user, per call in a call center environment.

  - Even though an Avaya Breeze® platform profile supports a given number of agents per node, the number of agents who actually log in is generally fewer. Hence, you can use the excess capacity that is available on the cluster for UC devices.

  - The requirements of different call centers differ. For example:

    - Some call centers record all calls, while others do not.

    - Some call centers have announcements every 30 seconds, while others may take several minutes.

    - The number of CC and UC users differ in different call centers.

You can use the following formula to determine the cluster capacity in a call center environment:

- For Avaya Breeze® platform Profile 2:

  UC endpoints + CC endpoints <= 1000xN

- For Avaya Breeze® platform Profile 4:

  UC endpoints + CC endpoints <= 5000xN

Where,

- N = The number of nodes in an N+1 cluster.

- UC endpoints = The number endpoints that will be used as UC endpoints.

- CC endpoints = The number of endpoints that will be used as CC endpoints. After a call center agent logs in to the endpoint, call center capability is available on the endpoint and the endpoint functions as a CC endpoint. Till then, the endpoint functions as a UC endpoint.

Because every call center environment is different, no fixed capacity rules can be defined. Instead, this topic provides general guidelines and target limits for cluster considerations for a call center environment.

The following table contains information about the Avaya Device Adapter Snap-in cluster capacity for a call center environment:

Avaya Device Adapter Snap-in cluster configuration	Description	Number of Avaya Breeze® platform Nodes	Avaya Breeze® platform Profile	Capacity
1	Small 1+1 with High Availability	1+1 = 2	2	Any one of the following: • Up to 1000 UC endpoints. • Up to 1000 CC endpoints. • Up to 1000 UC + CC endpoints.
2	Small 2+1 with High Availability	2+1 = 3		Any one of the following: • Up to 2000 UC endpoints. • Up to 2000 CC endpoints. • Up to 2000 UC + CC endpoints.
3	Small 3+1 with High Availability	3+1 = 4		Any one of the following: • Up to 3000 UC endpoints. • Up to 3000 CC endpoints. • Up to 3000 UC + CC endpoints.
4	Small 4+1 with High Availability	4+1 = 5		Any one of the following: • Up to 4000 UC endpoints. • Up to 4000 CC endpoints. • Up to 4000 UC + CC endpoints.
5	Small 5+1 with High Availability	5+1 = 6		Any one of the following: • Up to 5000 UC endpoints. • Up to 5000 CC endpoints. • Up to 5000 UC + CC endpoints.
6	Large 1+1 with High Availability	1+1 = 2	4	Any one of the following: • Up to 5000 UC endpoints. • Up to 5000 CC endpoints. • Up to 5000 UC + CC endpoints.

Table continues…

Avaya Device Adapter Snap-in cluster configuration	Description	Number of Avaya Breeze® platform Nodes	Avaya Breeze® platform Profile	Capacity
7	Large 2+1 with High Availability	2+1 = 3		Any one of the following: • Up to 10000 UC endpoints. • Up to 10000 CC endpoints. • Up to 10000 UC + CC endpoints.
8	Large 3+1 with High Availability	3+1 = 4		Any one of the following: • Up to 15000 UC endpoints. • Up to 15000 CC endpoints. • Up to 15000 UC + CC endpoints.
9	Large 4+1 with High Availability	4+1 = 5		Any one of the following: • Up to 20000 UC endpoints. • Up to 20000 CC endpoints. • Up to 20000 UC + CC endpoints.
10	Large 5+1 with High Availability	5+1=6		Any one of the following: • Up to 25000 UC endpoints. • Up to 25000 CC endpoints. • Up to 25000 UC + CC endpoints.

✱ **Note:**

- The capacity shown in the preceding table is based on the assumption that the Avaya Device Adapter Snap-in is the only snap-in running on the Avaya Breeze® platform cluster.

- Do not use Avaya Breeze® platform Profile 2 for a large call center environment. You can use Profile 2 for small call centers that can have a maximum of 400 simultaneously logged in agents at any point of time. Use Profile 4 for a call center that has more than 400 logged in agents.

- The services and options provided by a call center has an impact on the cluster capacity.

  Device Adapter VMs perform the call handling for user display and media termination, and agent key-press operations. Device Adapter does not handle tasks on other servers in a Call Center Elite environment. Hence, other activities performed in a call center, such as time allocated to an agent for Timed After Call Work, and the maximum performance capacity of the call center application have an impact on the number of Device Adapter VMs that are required.

Avaya Breeze® platform hardware requirements

Avaya Device Adapter Snap-in does not introduce any new hardware products.

The following table lists the Avaya Breeze® platform virtual machine profiles supported by Avaya Device Adapter Snap-in.

Avaya Breeze® platformProfile	Number of Cores	RAM (GB)	Disk Storage (GB)	Minimum CPU clock speed	CPU Reservation	Comments
2	4	8	100	2400 MHz (see note below)	9600 MHz	
4	8	16	100/ 150		19200 MHz	A minimum of 100 GB is recommended for disk storage and 150 GB for SDM deployments.

Note:

The Avaya Breeze® platform 3.7 OVA has a default setting of less than 2400 MHz minimum CPU clock speed. This must be changed to 2400 MHz after OVA deployment. See Configuring OVA CPU speed on page 146 for information and procedures on this process.

Avaya Solutions Platform

Device Adapter supports Avaya Solutions Platform 120 series servers configured with Profile 4 or 5. These server profiles provide support for up to 2.6 GHz per core. Lower server profiles cannot support 2.4 GHz per profile and are not supported.

Configuring OVA CPU speed

About this task

Use the following procedure to change the CPU speed of a deployed Avaya Breeze® platform virtual machine.

Before you begin

- Determine the maximum CPU clock speed available for each CPU.

Procedure

1. Log in to the host using VMware vSphere or vCenter with the appropriate administrative credentials.
2. Select the appropriate virtual machine.
3. Right-click the host.
4. Select **Edit Settings**.

5. Select the **Resources** tab.

6. Click **CPU**.

7. Enter `9600` in the **Reservation** field if using an Avaya Breeze® platform Profile 2 host or `19200` if using an Avaya Breeze® platform Profile 4 host.

8. Click **OK**.

Other deployments

Device Adapter can be deployed in all environments and hypervisors supported by the Avaya Breeze® platform. CPU resources and memory must meet or exceed the same levels as VMware deployment:

- Profile 2
  - CPU: 9600 Mhz or higher
  - RAM: 8GB
- Profile 4
  - CPU: 19200 Mhz or higher
  - RAM: 16GB

The equivalent AWS deployment would be the following:

- Profile 2
  - M4.xlarge, E5-2676 v3 or higher
  - CPU: 9600 Mhz or higher
  - RAM: 16GB
- Profile 4
  - M4.2xlarge, E5-2676 v3 or higher
  - CPU: 19200 Mhz or higher
  - RAM: 32GB

It is acceptable to exceed the minimum requirement. To get the CPU reservation, the AWS virtual machine has twice the RAM required. Being higher than necessary is acceptable; being low will result in slow registration on reboot.

The references used to retrieve the AWS values are shown below.

Figure 1: Profile 2 equivalent

Figure 2: Profile 4 equivalent

Select the desired profile when planning for AWS and use these when getting the AWS resources.

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.

2. On the PLDS website, enter your Login ID and password.

3. On the Home page, select **Assets**.

4. Select **View Downloads**.

5. Click the search icon ( ) for Company Name.

6. In the Search Companies dialog box, do the following:

    a. In the **%Name** field, type `Avaya` or the Partner company name.

    b. Click **Search Companies**.

    c. Locate the correct entry and click the **Select** link.

7. Search for the available downloads by using one of the following:

    • In **Download Pub ID**, type the download pub ID.

    • In the **Application** field, click the application name.

8. Click **Search Downloads**.

9. Scroll down to the entry for the download file, and click the **Download** link.

10. Select a location where you want to save the file, and click **Save**.

11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.

12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Deploying and configuring Avaya Breeze® platform

About this task

Use the following procedure to deploy and configure Avaya Breeze® platform.

 Note:

For every Avaya Breeze® platform server running Avaya Device Adapter Snap-in, an additional SIP Entity of the **Endpoint Concentrator** type must be defined. A number of Entity links between the SIP Entity and one or more Avaya Aura® Session Managers must also be defined. The Entity links must have a Connection Policy set to Endpoint Concentrator. An Avaya Aura® Session Manager Communication Profile must also be defined for every user or endpoint.

Procedure

1. Install and configure the required number of Avaya Breeze® platform servers.

    Note:

    See the *Deploying Avaya Breeze® platform* and *Administering Avaya Breeze® platform* guides for information and procedures related to this task.

2. Set the disk size of each server to 100GB or greater.

   ⊛ **Note:**

   See Avaya Breeze platform hardware requirements on page 146 for additional server information.

3. Configure SIP entities and Entity Links for all servers as per Avaya Breeze® platform deployment requirements.

   ⊛ **Note:**

   If you intend to deploy the Breeze server in a single node cluster, consider using the previous CS 1000 Node IP as the value of the **IP Address** field of the SIP Entity. This will enable performing a migration that will move all endpoints in one step. Do not do this if you are performing a phased migration or if you are deploying a multi-node cluster.

   ⊛ **Note:**

   See *Deploying Avaya Breeze® platform* for information and procedures related to this task.

4. Configure additional SIP entity and Entity Links for all servers as per Device Adapter deployment requirements.

   ⊛ **Note:**

   See Configuring additional SIP Entity and Entity Links for Avaya Breeze platform servers running Avaya Device Adapter Snap-in on page 151.

5. Select **Elements** > **Avaya Breeze** > **Server Administration** > **New** to configure the required number of Avaya Breeze® platform servers. Use the previously administered SIP entities.

6. Configure an Avaya Breeze® platform cluster.

   a. Use the procedure Configuring a single node Avaya Breeze platform cluster on page 153 to configure a single node cluster or Configuring a multiple node Avaya Breeze platform cluster on page 154 to configure a multiple node cluster.

   b. Ensure the cluster is in **Deny Service** mode.

7. Load and apply Avaya Device Adapter Snap-in using the information and procedures in the Snap-in deployment checklist on page 169.

8. Configure Avaya Device Adapter Snap-in service attributes with the information in Service attributes on page 157.

9. Configure PPM for Personal Directory data.

   ⊛ **Note:**

   See the *Maintaining and Troubleshooting Avaya Breeze® platform* guide for information and procedures related to this task.

Related links

Configuring additional SIP Entity and Entity Links for Avaya Breeze® platform servers running Avaya Device Adapter Snap-in

About this task

Use the following procedure to configure additional SIP Entity and Entity Links for every Avaya Breeze® platform servers running Avaya Device Adapter Snap-in.

The SIP Entity administered in a previous step will be referred to as the Breeze SIP Entity. The new entity created in this procedure will be referred to as the Device Adapter SIP Entity.

Procedure

1. Log on to System Manager by using the appropriate credentials.

2. Select **Elements** > **Routing** > **SIP Entities** from the menu.

3. Verify that the corresponding Breeze SIP Entity is configured with TLS enabled. Note the port values used for the "SIP Entity 1" (presumably SM) and the "SIP Entity 2" (presumably the Breeze SIP Entity) in the associated Entity Links.

4. Click **New**.

5. Enter the name of the new entity.

6. Enter the servers Security Module IP address in the **FQDN or IP Address** field.

   🛈 **Important:**

   This is the same IP address used to configure the corresponding Breeze SIP Entity.

7. Select Endpoint Concentrator in the **Type** field.

8. Create an Entity Link for every relevant Session Manager.

   a. Select the Session Manager in the **SIP Entity 1** field.

   b. Select **TLS Protocol**.

   c. Enter the Session Manager Port (SIP Entity 1 Port)

   🛈 **Important:**

   The Session Manager Port used in Entity Links of the Device Adapter SIP Entity must be different than the Session Manager Port used in corresponding Entity Links of the corresponding Breeze SIP Entity.

   d. Select the Device Adapter SIP Entity being administered in the **SIP Entity 2** field.

   e. Enter the Device Adapter SIP Entity Port (SIP Entity 2 Port).

> ❗ **Important:**
>
> The SIP Entity 2 Port used in Entity Links of the Device Adapter SIP Entity must be the same as the SIP Entity 2 Port used in corresponding Entity Links of the corresponding Breeze SIP Entity.

      f. Select endpt conc in the **Connection Policy** field.

9. Click **Commit**.

Configuring the Session Manager SIP entity to create SIP entity links between Session Manager and Communication Manager

About this task

You must configure the following:

- Session Manager SIP entity to create SIP entity links between Session Manager and Communication Manager.
- At least one listening port for endpoints in a domain. Session Manager listens for endpoint connections on these ports.

If you do not perform the preceding configurations, endpoint registration fails and the endpoints display a blank screen.

If you do not configure a listening port, the PPM data request to Session Manager generates errors.

Procedure

1. Log on to System Manager by using the appropriate credentials.

2. Click **Elements** > **Routing** > **SIP Entities**.

3. On the SIP Entities page, click **New**.

4. On the SIP Entity Details page, in the **General** area, do the following:

   a. In the **Name** field, type a name for the Session Manager SIP entity.

   b. In the **IP Address** field, type the Security Module IP address of Session Manager.

   c. In the **SIP FQDN** field, type the Security Module FQDN of Session Manager.

   d. In the **Type** field, click Session Manager.

5. In the **Entity Links** area, click **Add** and do the following to create a SIP entity link between Session Manager and Communication Manager:

   a. In the **Name** field, type a name for SIP entity link between Session Manager and Communication Manager.

   b. In the **SIP Entity 1** field, specify the Session Manager SIP entity.

   c. In the **Protocol** field, click the protocol that you want to use for the Session Manager SIP entity.

    d. In the **Port** field, type the port number of the Session Manager SIP entity.

    e. In the **SIP Entity 2** field, specify the Communication Manager SIP entity.

    f. In the **Port** field, type the port number of the Communication Manager SIP entity.

    g. In the **Connection Policy** field, click the connection policy that you want to use for the SIP entity link.

6. In the **Listen Ports** area, click **Add** and do the following:

    a. In the **Listen Ports** field, type the Communication Manager listening port for endpoints that use the protocol and that are in the domain that you specify in the corresponding fields.

    b. In the **Protocol** field, click the protocol that the Session Manager SIP entity uses.

    c. In the **Default Domain** field, click the domain of the Session Manager SIP entity.

    d. Select the **Endpoint** check box to allow Session Manager to forward the registration requests, that are received from endpoints in this domain, to the appropriate primary or secondary Session Manager and use the appropriate Communication Manager listening port.

    e. In the **Notes** field, type any additional note for your reference.

7. Click **Commit**.

Configuring a single node Avaya Breeze® platform cluster

About this task

Use the following procedure to configure a single node Avaya Breeze® platform cluster.

✳ **Note:**

For every Avaya Breeze® platform server running Avaya Device Adapter Snap-in, an additional SIP Entity of the **Endpoint Concentrator** type must be defined. A number of Entity links between the SIP Entity and one or more Avaya Aura® Session Managers must also be defined. The Entity links must have a Connection Policy set to Endpoint Concentrator. An Avaya Aura® Session Manager Communication Profile must also be defined for every user or endpoint.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

2. Click **New**.

3. Select the **Cluster Editor** page.

4. Select the **Core Platform** cluster profile.

5. Enter the cluster attributes.

> ✳ **Note:**
>
> The cluster name must be unique.

> ❗ **Important:**
>
> Do not assign a Cluster IP address to a single node cluster.

6. Select **Enable Cluster Database**.

> ✳ **Note:**
>
> Device Adapter cannot be installed if the cluster database is disabled.

7. Select **Should calls be allowed on the cluster**.

8. Select values for the **Minimum TLS Version for Non-SIP Traffic** and **Minimum TLS Version for SIP Call Traffic**.

9. Deselect **Use secure signaling for platform initiated SIP calls** to allow unsecured calls.

10. Enter the SIP domain in the **Default SIP Domain** field.

11. Select the **Servers** tab.

12. Assign servers to the cluster.

> ✳ **Note:**
>
> All servers in a cluster must have the same Avaya Breeze® platform version.

13. Select the **Services** tab.

14. Assign the Device Adapter service.

15. Click **Commit**.

    The **Service Install Status** field on the **Cluster Administration** page displays a green tick symbol after all the assigned snap-ins are successfully installed on all the servers in the cluster.

Next steps

Click **Show** to display the cluster details. Click the **Service Install Status** field of each server to see the detail of services.

Configuring a multiple node Avaya Breeze® platform cluster

About this task

Use the following procedure to configure a multiple node Avaya Breeze® platform cluster. Multiple node clusters are used to deploy a High Availability (n+1) configuration. For more information about High Availability configurations, see Chapter 9 in the *Deploying Avaya Breeze® platform* guide.

SIP high availability enables the ability to route users of a service to the cluster rather than a specific Avaya Breeze® platform server. In this deployment scenario, the Cluster IP field of the

cluster needs to be populated and the Load Balancer enabled. The users of the Device Adapter service are pointed to the cluster through the Cluster IP.

> ✳ **Note:**
>
> For every Avaya Breeze® platform server running Avaya Device Adapter Snap-in, an additional SIP Entity of the **Endpoint Concentrator** type must be defined. A number of Entity links between the SIP Entity and one or more Avaya Aura® Session Managers must also be defined. The Entity links must have a Connection Policy set to Endpoint Concentrator. An Avaya Aura® Session Manager Communication Profile must also be defined for every user or endpoint.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

2. Click **New**.

3. Select the **Cluster Editor** page.

4. Select the **Core Platform** cluster profile.

5. Enter the cluster attributes.

   > ✳ **Note:**
   >
   > The cluster name must be unique.

   > ❶ **Important:**
   >
   > For multi-node clusters, assign the Cluster IP and enable the Load Balancer.
   >
   > Consider using the previous CS 1000 Node IP as the value of the Cluster IP Address field of the cluster. This will enable performing a migration that will move all endpoints in one step. Do not do this if you are performing a phased migration.

6. Select **Enable Cluster Database**.

   > ✳ **Note:**
   >
   > Device Adapter cannot be installed if the cluster database is disabled.

7. Select **Should calls be allowed on the cluster**.

8. Select values for the **Minimum TLS Version for Non-SIP Traffic** and **Minimum TLS Version for SIP Call Traffic**.

9. Deselect **Use secure signaling for platform initiated SIP calls** to allow unsecured calls.

10. Enter the SIP domain in the **Default SIP Domain** field.

11. Select the **Servers** tab.

12. Assign servers to the cluster.

    > ✳ **Note:**
    >
    > All servers in a cluster must have the same Avaya Breeze® platform version.

13. Select the **Services** tab.

14. Assign the Device Adapter service.

15. Click **Commit**.

    The **Service Install Status** field on the **Cluster Administration** page displays a green tick symbol after all the assigned snap-ins are successfully installed on all the servers in the cluster.

16. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

17. Click **Show** beside the cluster name.

18. Identify the active and standby database servers in the Cluster Database field.

    ✳ **Note:**

    The server marked Active is the primary server. The server marked Standby is the secondary server. All other servers in the cluster should be marked as Idle.

    ❗ **Important:**

    TPS node is active only when one of the two servers: Active and Standby servers are active and running. TPS node is inactive when both Active and Standby servers are not running even if the other servers in cluster are active.

About service attributes

You can use the Device Adapter service attributes that are available on System Manager to apply Device Adapter-specific configuration at a cluster level or a global level. If you set the service attributes at a global level, the configuration is applied to all the Avaya Breeze® platform clusters that have the Avaya Device Adapter Snap-in installed within the Avaya Aura® network. For example, you can specify the port number for RTP/RTCP and also specify whether you want to use this port number at a cluster level or at a global level.

To access service attributes, on System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

Whether the cluster uses the default values or user-defined values for service attributes is determined by whether you select or clear the **Override default** check box. That is:

• If you select the **Override default** check box for an attribute at a cluster level, specify a custom value for the attribute, the cluster uses this value for the attribute instead of the default value or the global level value.

• If you select the **Override default** check box for an attribute at a global level, specify a custom value for the attribute, the change is applied to all the Avaya Breeze® platform clusters that have the Avaya Device Adapter Snap-in installed within the Avaya Aura® network.

    Device Adapter considers this global value as the default value for the cluster level. Hence, if you select the **Override default** check box and set the service attributes at a global level instead of a cluster level, the attribute values are applied at a global level.

However, if you select the **Override default** check box and specify a custom value for an attribute at a cluster level, the cluster level value of the attribute overrides the global level value of the attribute.

• If you clear the **Override default** check box at both cluster level and global level, the cluster uses the default values of the service attributes.

✳ **Note:**

Some service attributes, if modified, require you to stop and start Device Adapter for the changes to take effect. Avaya recommends that you stop and start Device Adapter during the maintenance window to minimize the impact on endpoint registration and call handling.

Service attributes

The following table lists the service attributes that must be configured for Device Adapter.

You can apply the attributes at a cluster level or a global level. For more information, see About service attributes on page 156.

Attribute	Description	Default value	Device Adapter Restart Required
Default Group			
Supplier Id	Avaya provided supplier ID.	10000000	No
IP Telephony Node			
Node ID	Node ID for the Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed. Valid values are 0 through 9999.	None	Yes
System ID	System ID for the Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.	None	Yes
IP Telephony Node / Codecs / Companding Law			
For more information, see Setting the Pulse Code Modulation companding law for endpoints that are migrated to Device Adapter on page 204.			
Companding law	Pulse Code Modulation companding law for the system.	A-law	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
G.729 Voice Activity Detection	Option to enable voice activity detection for G.729 codec.	On	Yes
IP Telephony Node / Codecs / G.723.1			
For more information, see [Configuring G.711, G.722, G.729, and G.723.1 codec settings for Device Adapter](#) on page 204.			
G.723.1 Preference order	The G.723.1 codec preference order in the initial offer.	4 (Lowest)	Yes
G.723.1 Supported voice payload size	Payload sizes supported by Device Adapter for G.723.1 codec. You cannot modify the value of this attribute.	30 milliseconds per frame	Not applicable
G.723.1 Voice Activity Detection	Option to enable voice activity detection for G.723.1 codec.	On	Yes
IP Telephony Node / Quality of Service (QoS)			
For more information, see [Enabling VoIP monitoring](#) on page 205.			
VoIP Monitoring Enabled	Option to enable VoIP monitoring on the Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.	No	No
VoIP Monitoring Reporting Interval	Duration of time after which Device Adapter must run the VoIP monitoring report. Valid values are 30 seconds through 300 seconds.	30 seconds	No
VoIP Monitoring Manager IP address	The IP address of the VMM.	None	No
VoIP Monitoring Manager Port	The port number of the VMM. Valid values are 1 through 65535.	5005	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
Enable VLAN Tagging (802.1Q support)	Option to enable VLAN tagging to support the 802.1Q networking standard.	No	Yes
IP Telephony Node / LAN			
For more information, see Configuring the port number for RTP/RTCP on page 206.			
RTP/RTCP starting port	Port number used by the RTP packets. The port number has two sequential numbers: one for RTP and the other for RTCP. The subsequent port number is used for RTCP.	5200	Yes
IP Telephony Node / DTLS			
For more information, see Security configuration on page 197.			
DTLS policy	Option to enable the DTLS policy to secure communications between endpoints and Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.	Best-effort	Yes
Enable client authentication	Option to enable endpoint authentication.	No	Yes
Call Logs			
For more information, see Enabling Personal Directory support on page 207.			
Enable Callers and Redial List	Option to enable caller and redial list with PD contacts	No	No
Default incoming call log mode	Option to configure the Callers List to log all incoming calls or only the unanswered incoming calls.	Unanswered	No
Contacts			
For more information, see Configuring Corporate Directory support on page 201.			

Table continues…

Comments on this document? infodev@avaya.com

Attribute	Description	Default value	Device Adapter Restart Required
Enable Corporate Directory	Option to enable Corporate Directory.	No	Yes
Enable Personal Directory	Option to enable Personal Directory	No	Yes
Avaya Aura Device Services (AADS) FQDN	The FQDN of the AADS server.	None	Yes
Avaya Aura Device Services (AADS) Port	The port number of the AADS server. Valid values are 1 through 65535.	8443	Yes
Network Address Translation (NAT) For more information, see Configuring time period for NAT mapping on page 209.			
NAT Mapping Keep Alive Timeout	Duration of time, in seconds, after which the audio and signaling port mapping is refreshed. Valid values are 20 seconds through 600 seconds.	30 seconds	No
IP Security (IPSec) The IP Security (IPSec) attributes are available only on the **Service Globals** tab. For more information, see Configuring IP security on page 131.			
Enable IPSec for Media Gateways	Option to enable IP security on a Device Adapter to Media Gateway signaling link.	No	No
Pre-Shared Key for IPSec	Pre-shared key that is used by IP security for data cyphering. Key must be 16 to 32 characters in length and can contain only numbers and letters.	No	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
PreShared key value for IPSec	Pre-shared key that is used by IP security for data cyphering. Key must be 16 to 32 characters in length and can contain only numbers and letters.	None	No
Media Security For more information, see [Setting the media security policy](#) on page 657.			
Media security policy	Option to set the media security policy.	Best-effort	No
Secured number of packets (NKEY)	The number of packets secured. Expressed in power of two (2^x). Valid values are 16 through 31.	31	No
Session key validity time (TKEY)	The session key validity time in hours. Valid values are 8 hours through 168 hours.	24 hours	No
Secure Link Access The attributes in the **Secure Link Access** group are available only on the **Service Clusters** tab. For more information, see [Enabling SSH access for Device Adapter](#) on page 209.			
Enable SSH access on Secure Link	Option to enable SSH access, on a Secure Link interface, to the Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.	No	No
Miscellaneous Parameters For more information, see [Configuring the display text, country, dial tone timeout, interdigit timeout, and busy/overflow timeout for Device Adapter endpoints](#) on page 210.			
Idle set display	The text to display on an idle set.	Avaya	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
Country	The country where the endpoints are located. The tones, cadences, and loss plan that are used depends on the country that you select.	USA	Yes
Dial tone timeout	Duration of time the dial tone is played without the user entering a digit. After the time elapses, the call attempt fails. Valid values are 1 second through 60 seconds.	20 seconds	No
Inter-digit timeout	Duration of time to wait for another digit before attempting the call. After the time elapses, if the number has no conflicts in the PPM Dial Plan data, the call is attempted. Otherwise, the call is rejected. When the prefix of the digit string matches one entry and the total length matches the expected length, the call is attempted. Valid values are 1 second through 10 seconds.	5 seconds	No

Table continues…

Avaya Device Adapter Snap-in Reference

Attribute	Description	Default value	Device Adapter Restart Required
Busy/overflow timeout	Duration of time the busy tone and call failure tone are played. Even if the user does not disconnect the call before the time elapses, Device Adapter completes the call clearing. Valid values are 5 seconds through 999 seconds.	30 seconds	No
Media Gateway			
For more information, see [MGC installation, upgrade, and registration process](#) on page 125.			
Enable legacy loadware upgrades	Option to replace an existing MGC or add an additional new MGC from the factory.	No	No
Media Gateway Accounts			
For more information, see [Setting passwords for the admin2 and pdt2 MGC accounts](#) on page 655.			
admin2 Password	The password for the admin2 account.	None	No
pdt2 Password	The password for the pdt2 account.	None	No
Peripheral Equipment / Analog Set Timers			
For more information, see [Configuring timers for analog endpoints](#) on page 211.			
Minimum Switchhook Flash	Minimum Switchhook Flash timer in milliseconds for 500/2500 sets.	500 milliseconds	No
Maximum Switchhook Flash	Maximum Switchhook Flash timer in milliseconds for 500/2500 sets.	896 milliseconds	No
Off Hook Validation	Off-hook validation timer for Extended Flexible Analog Line Card (XFALC).	250 milliseconds	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
Dial Pulse	Minimum time for dial pulse for Extended Flexible Analog Line Card (XFALC).	15 milliseconds	No
Interdigit	Interdigit time for Extended Flexible Analog Line Card (XFALC).	150 milliseconds	No
Dial Pulse On	Maximum time for dial pulse for Extended Flexible Analog Line Card (XFALC).	150 milliseconds	No
Post Flash	Post Flash timer for Extended Flexible Analog Line Card (XFALC).	200 milliseconds	No
Daylight Saving Rules			
For more information about configuring phones in different time zones to the main site, see Setting time zones and DST for endpoints in a different time zone on page 329.			
Daylight saving enabled	Option to enable daylight saving.	No	No
Start weekday	The first weekday on or after the start date.	Sunday	No
Start day	The date after which the offset time must be applied. The date must be in MM/DD format.	03/08	No
Start time	The time after which the offset time must be applied. The time must be in HH:MM format.	2:00	No
Stop weekday	The first weekday on or after the stop date.	Sunday	No
Stop day	The date after which the offset time must be removed. The date must be in MM/DD format.	11/01	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
Stop time	The time after which the offset time must be removed. The time must be in HH:MM format. VO session should be ended for DVLA phones for a configured period of time by Device Adapter. When the DVLA logout timer expires, the user is asked whether to accept logout. Failure to reply (or selecting "yes") results in a logout. Entering "no" restarts the logout timer.	2:00	No
Offset	The time offset in hours from local standard time. The supported values are 1 and 2.	1	No
Virtual Office/Emergency calls			
For more information, see Emergency Dialing for Virtual Office on page 680.			
TN range for emergency calls from Logged out sets	The range of TNs that will be used for temporary registration of VO logged out sets for making emergency calls.	None	No
SIP domain for emergency calls from Logged out sets	The domain used for making emergency calls from VO logged out sets.	None	No
TN range for DVLA sets	The range of DVLA TNs that will be used for temporary registration of Default Virtual Office Logged out sets.	None	No

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
Idle time interval for DVLA set	The time interval which defines maximum time for DVLA phones, VO logged in to another extensions, to be in the idle state before automatic VO logout (1 - 1440 minutes, or 0h 1m - 24h 0m).	None	No
Voicemail			
For more information, see [Configuring context-sensitive soft keys for voice mail on Device Adapter endpoints](#) on page 411.			
Voicemail Telephony User Interface	The Voicemail Telephony User Interface system that you want to use.	Avaya Aura® Messaging	Yes
Custom dialing sequence: Play	The dialing sequence to play the voice mail message.	4	Yes
Custom dialing sequence: Delete	The dialing sequence to delete the voice mail message.	7	Yes
Custom dialing sequence: Call	The dialing sequence to call the party that left the voice mail message.	88	Yes
Custom dialing sequence: Stop	The dialing sequence to stop playing the voice mail message.	#	Yes
Custom dialing sequence: Reply	The dialing sequence to reply to the voice mail message.	8	Yes
Custom dialing sequence: Compose	The dialing sequence to compose a message and send the message to one or more users.	2	Yes
Custom dialing sequence: Forward	The dialing sequence to forward the voice mail message to another user's mailbox.	6	Yes

Table continues…

Attribute	Description	Default value	Device Adapter Restart Required
Custom dialing sequence: Goodbye	The dialing sequence used for the following: • If pressed from a sub-menu of the main menu, exit from the sub-menu. • If pressed from the main menu, disconnect from the voice mail system.	*	Yes
Remote Cluster For more information, see Configuring the Remote Cluster feature on page 596.			
Remote Cluster configuration enabled	This option enables Remote Cluster configuration. SBC IP addresses below should correspond to configured SIP Entity links to SBC.	No	No
Primary SBC IPv4 Address	One of the IP addresses is mandatory - Primary IPv4 or IPv6. If both are set - IPv4 will be used by default.	None	No
Primary SBC IPv6 Address	One of the IP addresses is mandatory - Primary IPv4 or IPv6. If both are set - IPv4 will be used by default.	None	No
Secondary SBC IPv4 Address	This IP address is optional.	None	No
Secondary SBC IPv6 Address	This IP address is optional.	None	No

Chapter 5: Avaya Device Adapter Snap-in deployment

Snap-in deployment checklist

Use the following checklist for deployment of the snap-in.

No.	Task	Description	Notes	✔
1	Load the snap-in.	See Loading the snap-in on page 169.		
2	Install the snap-in.	See Installing the snap-in on page 170.		
3	Verify deployment.	Use Avaya Breeze® to verify successful deployment.		

File information

Device Adapter is distributed as an SVAR file similar to other Avaya Breeze® platform snap-ins. The SVAR file contains all the components required for deployment of Device Adapter on an Avaya Breeze® platform server.

The Device Adapter file name is in the format of `DeviceAdapter-x.x.x.x.x.svar` where `x.x.x.x.x` represents the major and minor versions of the application. For example, a distribution file is called `DeviceAdapter-8.1.2.x.x.svar`. This distribution file must be signed by Avaya or it cannot be installed on the Avaya Breeze® platform server.

Loading the snap-in

About this task

Use this procedure to load a snap-in into System Manager.

> **Important:**
>
> Pre-loaded snap-ins do not require this step. Pre-loaded snap-ins are available in the Avaya Breeze® platform Element Manager in System Manager. Pre-loaded snap-ins that have been removed by the administrator must be reloaded.

Procedure

1. Log on to System Manager by using the appropriate credentials.

2. Click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

3. Click **Load**.

4. Browse to the location of the snap-in SVAR file.

5. Select the file.

6. Click **Open**.

7. Click **Load**.

8. Click **Accept**.

   > **Important:**
   >
   > You must accept the End User License Agreement (EULA) to use the snap-in.

9. Verify the snap-in is in a state of **Loaded** when the process completes.

Installing the snap-in

About this task

Use this task to install the snap-in to a specific cluster.

> **Note:**
>
> For .svar files larger than 50 MB, schedule snap-in installation during a maintenance window.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

2. Select the snap-in that you want to install.

3. Click **Install**.

4. Select the cluster(s) where you want the snap-in to reside, and click **Commit**.

5. To see the status of the snap-in installation, click the **Refresh Table** icon located in the upper-left corner of the **All Services** list.

   Installed with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze® platform servers in the cluster. **Installing** with a yellow exclamation

mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.

6. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for an Avaya Breeze® platform server.

   The Service Status page displays the installation status of all the snap-ins installed on that server.

7. **(Optional)** Designate the Preferred Version.

   To designate a snap-in as the preferred version, you must administer the user profile. If you want to designate the snap-in as the preferred version, do the following:

   a. Verify that the snap-in is in the **Installed** state for the targeted cluster(s) by opening the System Manager web console, and clicking **Elements** > **Avaya Breeze®** > **Service** > **Management** > **Services**.

   b. From the **All Services** list, select the version of the snap-in you want to mark as Preferred.

   c. Click **Set Preferred Version**.

   d. Select the cluster(s) for which you want this to be the preferred version, and click **Commit**.

Avaya Breeze® platform server administration

For information and procedures about server administration, see "Cluster Administration" in the *Administering Avaya Breeze® platform* guide.

Avaya Breeze® platform cluster administration

For information and procedures about cluster administration, see "Cluster Administration" in the *Administering Avaya Breeze® platform* guide.

✱ **Note:**

Ensure that the **Core Platform** profile is used.

Chapter 6: Avaya Breeze® platform and Avaya Device Adapter Snap-in upgrade

Overview of Avaya Breeze® platform and Avaya Device Adapter Snap-in upgrade

This chapter contains information about the upgrade process for Avaya Breeze® platform and Avaya Device Adapter Snap-in.

The Avaya Device Adapter Snap-in is one component of a much larger Avaya Aura® customer solution. If the Avaya Aura® platform also requires an upgrade, then depending on the release that you want to upgrade from and to, there is an order in which you have to upgrade the different Avaya Aura® components.

Generally, you should upgrade System Manager, Session Manager, and Communication Manager before upgrading the Avaya Breeze® platform and the Avaya Device Adapter Snap-in.

> ✳ **Note:**
>
> Unless the Release Notes for the Avaya Breeze® platform or Device Adapter indicate a different requirement, the Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the other components, such as Session Manager, Communication Manager, and Application Enablement Services, within the Avaya Aura® solution.

For information about the upgrade order for various Avaya Aura® components, see the Release Notes for the specific releases that you want to upgrade from and to.

You may want to upgrade the following:

- Only the Avaya Breeze® platform.
- Only the Avaya Device Adapter Snap-in.
- Both the Avaya Breeze® platform and the Avaya Device Adapter Snap-in.

If both the Avaya Breeze® platform and the Avaya Device Adapter Snap-in require an upgrade, the upgrades are performed as separate procedures. In almost all cases, there is no specific upgrade order required; however, refer to the Release Notes of the specific release that you are upgrading to ensure that there is no specific upgrade order required.

Planning for Avaya Breeze® platform and Device Adapter upgrades

The topics in this section provide information about planning the Avaya Breeze® platform and Device Adapter upgrades to minimize outages during the upgrade process.

The following two deployment models minimize the down-time during Avaya Breeze® platform upgrade:

- N+1

  The N+1 server model allows one Avaya Breeze® platform server to be unavailable, provided the remaining N servers have the required capacity to provide service to the endpoints that got unregistered from the +1 node.

  You can use the rolling upgrade method in an N+1 model to upgrade the Avaya Breeze® platform server. Rolling upgrade method minimizes end-user impact during the upgrade because the endpoints fail over to the active Avaya Breeze® platform servers that are either already upgraded or will be upgraded after the current platform node is upgraded.

- Geo-redundancy

  In a geo-redundant model, two data centers provide service to the endpoints. Every device has a Server 1 and a Server 2 that provide geo-redundancy in an event when there is an outage at one data center.

  The time required by an endpoint or an MGC of an endpoint to fail over during upgrading the Avaya Breeze® platform server in a geo-redundant model is generally more as compared to the N+1 model. This is because the endpoints or MGC of the endpoints try to fail over to the primary server (S1) first. If S1 does not have the required capacity or if S1 is not reachable, the endpoints or MGC of the endpoints try to fail over to the alternate server (S2).

When you upgrade a Device Adapter Snap-in on an Avaya Breeze® platform cluster, the Device Adapter snap-in is upgraded on all the nodes within that cluster. The Device Adapter Snap-in upgrade process is service impacting. Unlike Avaya Breeze® platform, the Device Adapter Snap-in cannot be upgraded as a rolling upgrade.

Fail-over scenarios for UNIStim endpoints during the upgrade

UNIStim endpoint fail over when a registration failure is detected

UNIStim endpoints monitor the registration by using the "time to live" monitoring, but health checks in the registration allow the endpoints to detect a registration failure faster. When an endpoint detects a registration failure, the endpoint restarts and attempts a re-registration.

UNIStim endpoint fail over due to loss of service during call-related signaling

A UNIStim endpoint may detect registration failure. In an event when a registration failure occurs and the call is still active, Device Adapter and the UNIStim endpoint maintain the media path to avoid loss of call. But, a user operation during the call, such as call modification or call release, might result in the call being lost.

If the user is on a call, Device Adapter and the UNIStim endpoint maintain the media path. However:

- If the user tries to modify the media path during an active call and if the endpoint detects the registration failure, the endpoint restarts and attempts a re-registration.

- If the user tries to modify the media path during an active call and if the endpoint has still not detected the registration failure, the endpoint restarts only after Device Adapter fails to respond to a service request made by the endpoint. The endpoint then attempts a re-registration.

Depending on the deployment model, if the endpoint cannot reregister to the same node or cluster, the endpoint tries to fail over to an alternate node or cluster that has the required capacity.

Fail-over scenarios for digital and analog endpoints during the upgrade

Digital and analog endpoint fail over when a registration failure is detected

The MGCs monitor the registration of the endpoints by using the "time to live" monitoring, but health checks in the registration allows the MGC to detect a registration failure faster. After detecting the registration failure, the MGC tries to re-register the endpoint.

Digital and analog endpoint fail over due to loss of service during call-related signaling

The MGC may detect registration failure. This failure could be because of a user action, such as call modification or call release, during the call, which might result in the call being lost.

If the user is on a call, Device Adapter and MGC maintain the media path. However:

- If the user tries to modify the media path during an active call and if the MGC detects the registration failure, the MGC immediately attempts re-registration on behalf of the endpoint.

- If the user tries to modify the media path during an active call and if the MGC has still not detected the registration failure, then the MGC attempts re-registration on behalf of the endpoint only after Device Adapter fails to respond to a service request made by the endpoint.

Depending on the deployment model, if the MGC cannot re-register the endpoint to the same node or cluster, the MGC tries to fail over to an alternate node or cluster.

Rolling upgrade method to upgrade Avaya Breeze® platform in an N+1 model

The N+1 node cluster configuration model supports the rolling upgrade method for upgrading the Avaya Breeze® platform servers within the cluster.

To use the rolling upgrade method, ensure the following:

- All nodes within that cluster are currently functional.

- The cluster must be provisioned such that if one node out of the N+1 nodes is out of service, the remaining nodes within that cluster have enough capacity to support the Device Adapter endpoints that got unregistered from the unavailable node.

The rolling upgrade procedure is as follows:

- Stop the service at the node where you want to upgrade Avaya Breeze® platform. The endpoints on this node register with the remaining nodes within the cluster.

- Upgrade Avaya Breeze® platform on the node where the service is stopped.

- When the upgrade is complete, put the node back into service.

- Similarly, upgrade the other nodes within the cluster.

Caveats

In an N+1 node cluster configuration, if one or more nodes are either not functional or are not reachable, the rolling upgrade method would not reduce the end-user impact because of the following reason:

- If one node is out of service, the cluster is effectively an N node cluster. The remaining nodes do not have the capacity to support all the endpoints that were served by the node that became unavailable.

UNIStim endpoint fail over during Avaya Breeze® platform upgrade in an N+1 model

When the UNIStim endpoints detect a server failure, the UNIStim endpoints restart and try to re-register with the primary server (S1) – the load balancer of cluster 1. Typically, the load balancer assigns the registration to one of the Device Adapter nodes and registration completes. If S1 does not respond, the endpoints wait briefly and retry the registration.

If the cluster is configured for N+1 along with geo-redundancy and if S1 does not respond, the UNIStim endpoints try to register with the secondary server (S2). If S2 does not respond, the endpoints wait briefly and retry the registration to S1.

In an N+1 model, the UNIStim endpoint try to fail over to the primary server first.

If the primary cluster is sized to have enough capacity to support the endpoints within that cluster, the outage is usually short and may not be detected by an end user, unless the user tries to use the endpoint during the fail over.

Depending on factors such as network speed and Session Manager resiliency, the fail-over time for the endpoint to register to a Device Adapter node is typically five minutes or less after an endpoint detects a registration failure.

However, even a short interval for detecting registration failure and failing over may be noticed by the users. Hence, even a very fast switch-over may be noticed by the users.

Analog and digital endpoint fail over during Avaya Breeze® platform upgrade in an N+1 model

Analog and digital endpoints do not restart to fail over to an alternate server. However, the MGC of the analog and digital endpoint detects the registration failure and attempts the re-registration on behalf of these endpoints.

The MGC provides the services that allows the MGC to detect a Device Adapter failure. After the failure is detected, the MGC tries to re-register the endpoints to the primary server. The primary server is analogous to the S1 in case of UNIStim endpoints. If the primary server does not respond and if no alternate servers are programmed, the MGC waits briefly and retries the registration.

If the cluster is configured for N+1 along with geo-redundancy and if S1 does not respond, the MGC tries to register the endpoints to the first alternate server (Alt 1). If the Alt 1 server is unavailable and if a secondary alternate server (Alt 2) is programmed, the MGC tries to register the endpoints to the Alt 2, which is a local backup server. However, if Alt 2 is also not available, the MGC waits for a brief period and tries to register the endpoints to the primary server.

Regardless of whether geo-redundancy is configured, N+1 fail over occurs when the MGC attempts to find capacity in the primary server first.

If the primary cluster is sized to have enough capacity to support the endpoints within that cluster, the outage is usually short and may not be detected by an end user, unless the user tries to use the endpoint during the fail over.

Depending on factors such as network speed and Session Manager resiliency, the fail-over time for the endpoint to register to a Device Adapter node is typically five minutes or less after an endpoint detects a registration failure.

However, even a short interval for detecting the registration failure and failing over may be noticed by the users. Hence, even a very fast switch-over may be noticed by the users.

Avaya Breeze platform upgrade in a geo-redundant model

UNIStim endpoint fail over during Avaya Breeze® platform upgrade in a geo-redundant model

When a UNIStim endpoint detects a server failure, the UNIStim endpoint does the following:

1. The UNIStim endpoint restarts and tries to re-register with the primary server (S1). This is the N+1 failover.
2. If an alternate geo-redundant cluster is configured and if the reregistration attempt to S1 fails, the UNIStim endpoint tries to register with the secondary server (S2).
3. If S2 is not available, the endpoint waits for configured time interval and reattempts the registration to S1.

In a geo-redundant model, the UNIStim endpoints try to fail over within the primary load balancing server first.

However, if the primary cluster has insufficient capacity to support the fail over or if the S1 does not respond, then in a geo-redundant model, the outage time is the sum of the outage time caused during the initial registration failure and the time required to register to the geo-redundant cluster. The outage time is usually short and may not be detected by an end user, unless the user tries to use the endpoint during the fail over.

Depending on factors such as network speed and Session Manager resiliency, the fail-over time for the endpoint to register to a Device Adapter node is typically five minutes or less in addition to the time required to detect the geo-redundancy failure.

However, even a short interval for detecting the registration failure and failing over may be noticed by the users. Hence, even a very fast switch-over may be noticed by the users.

Analog and digital endpoint fail over during Avaya Breeze® platform upgrade in a geo-redundant model

Analog and digital endpoints do not restart to fail over to an alternate server. However, the MGC of the analog and digital endpoint detects the registration failure and attempts the reregistration on behalf of these endpoints.

The MGC provides the services that allows the server to detect a server failure. After the failure is detected, the MGC does the following:

1. The MGC tries to reregister the endpoints to the primary server.

2. If cluster is configured for geo-redundancy and if primary server cluster load balancer does not respond, the MGC tries to register the endpoints to the first alternate server cluster load balancer (Alt 1).

3. If the Alt 1 server is unavailable, the MGC tries to register the endpoints to the second alternate server cluster load balancer (Alt 2), which is a local backup server.

4. If Alt 2 is also not available, the MGC waits for the configured time interval and reattempts the registration to the primary server cluster load balancer.

The MGC attempts to find capacity in the primary server first.

However, if the primary cluster has insufficient capacity to support the fail over, then in a geo-redundant model, the outage time is the sum of the outage time caused during the initial registration failure and the time required to register to the geo-redundant cluster. The outage time is usually short and may not be detected by an end user, unless the user tries to use the endpoint during the fail over.

Depending on factors such as network speed and Session Manager resiliency, the fail-over time for the MGC to register the endpoint to a Device Adapter node is typically five minutes or less in addition to the time required to detect the geo-redundancy failure.

However, even a short interval for detecting the registration failure and failing over may be noticed by the users. Hence, even a very fast switch-over may be noticed by the users.

UNIStim endpoint fail over process in an N+1 and a geo-redundant model

Procedure

1. The following are the two scenarios in which a UNIStim endpoint fails over:

   • When the endpoint detects a registration failure, the UNIStim endpoint restarts and attempts to fail over.

   • A loss of service can occur during call-related signaling. For example, during an active call, the user performs an operation that modifies the media path. In this scenario, the UNIStim endpoint restart and fail over is triggered by the following events:

     - If the endpoint detects the registration failure, the endpoint restarts and fails over.

     - If the endpoint does not detect the registration failure, the endpoint restarts after Device Adapter does not respond to the service request by the endpoint.

2. The following are the fail-over processes:

   • In case of an N+1 deployment model:

     - If the N+1 cluster has enough capacity, the load balancer passes the endpoint registration request to the node that has the capacity to accept this registration. The registration succeeds.

     - If no capacity is available on the N+1 cluster and if an alternate geo-redundant cluster is not configured, the endpoint waits for the configured time interval and reattempts the endpoint registration.

   • In case of a geo-redundant model:

     - If the load balancer does not find the required capacity on S1, it passes the registration request to S2.

     - If S2 has the required capacity, it accepts the registration request.

Analog and digital endpoint fail-over process in an N+1 and a geo-redundant model

Procedure

1. The following are the two scenarios in which the MGC attempts the fail over on behalf of a digital or analog endpoint:

   • When the MGC detects the endpoint registration failure, the MGC attempts the fail over on behalf of the endpoint.

- A loss of service can occur during call-related signaling. For example, during an active call, the user performs an operation that modifies the media path. In this scenario, fail over is triggered by the following events:

  - If the MGC detects the endpoint registration failure, the MGC tries to re-register the endpoint.

  - If the MGC does not detect the registration failure, MGC attempts the endpoint re-registration after Device Adapter does not respond to the service request by the endpoint.

2. The following are the fail over processes:

   - In case of an N+1 model:

     - If the N+1 cluster has enough capacity, the load balancer passes the endpoint registration request to the node that has the capacity to accept this registration. The registration succeeds.

     - If no capacity is available on the N+1 cluster and if an alternate geo-redundant cluster is not configured, the MGC waits for the configured time interval and reattempts the endpoint registration.

   - In case of a geo-redundant model:

     - If the load balancer does not find the required capacity on the primary server, it passes the registration request to the secondary server.

     - If the secondary server has the required capacity, it accepts the registration request.

Guidelines to minimize outages when upgrading Avaya Breeze® platform

This topic provides guidelines that help minimize outages when upgrading Avaya Breeze® platform in both an N+1 model and a geo-redundant model.

> **Note:**
>
> Avaya recommends that you use the rolling upgrade method to upgrade the Avaya Breeze® platform server during a low traffic maintenance window.
>
> Use the rolling upgrade method in a geo-redundant model as well, even though the geo-redundant model allows you to upgrade the entire cluster at one time.

The following are the guidelines to minimize outages when upgrading Avaya Breeze® platform:

1. Perform the upgrade when the cluster is experiencing very low traffic. For example, after business hours.

   Because fewer users use the phones during such hours, the probability of dropped calls is minimized.

2. Use the rolling upgrade method to upgrade the Avaya Breeze® platform server.

For more information, see [Rolling upgrade method to upgrade Avaya Breeze platform in an N+1 model](#) on page 174.

Unless there is a specific requirement to use another upgrade method to upgrade an Avaya Breeze® platform server, use the rolling upgrade method to upgrade the Avaya Breeze® platform servers, within the cluster, one node at a time.

For more information, see the *Upgrading Avaya Breeze® platform* guide.

Guidelines to minimize outages when upgrading both Device Adapter Snap-In and Avaya Breeze® platform

When you upgrade a Device Adapter Snap-in on an Avaya Breeze® platform cluster, the Device Adapter Snap-in is upgraded on all the nodes within that cluster. The Device Adapter Snap-in upgrade process is service impacting.

Unlike Avaya Breeze® platform, the Device Adapter Snap-in cannot be upgraded as a rolling upgrade.

Hence, Avaya recommends that you use the geo-redundant model to minimize the outages. The geo-redundant node can handle the endpoints that fail over during the Device Adapter Snap-In upgrade.

For more information, see [Avaya Breeze platform and Device Adapter snap-in upgrade in a geo-redundant model](#) on page 186.

If you are using an N+1 model, Avaya recommends the following:

1. Perform the upgrade when the cluster is experiencing very low traffic. For example, after business hours.

   Because fewer users use the phones during such hours, the probability of dropped calls is minimized.

2. If both Device Adapter and Avaya Breeze® platform need to be upgraded, upgrade the Avaya Breeze® platform servers first. Avaya Breeze® platform upgrade requires more time as compared to the Device Adapter Snap-In upgrade.

   For more information, see [Guidelines to minimize outages when upgrading Avaya Breeze platform](#) on page 179.

3. Ensure the all the Avaya Breeze® platform nodes are functioning properly.

4. Upgrade the Device Adapter Snap-In.

   For more information, see [Avaya Device Adapter Snap-in upgrade](#) on page 184.

   After you upgrade the Device Adapter Snap-In, the new version of the Snap-In is downloaded to the cluster and the cluster uses the new Snap-in.

   The Device Adapter Snap-In upgrade requires less time and can be completed during the maintenance window. However, to minimize the service impact, ensure that the cluster is fully functional before upgrading the Device Adapter Snap-in.

Checklist for upgrading the Avaya Breeze® platform for a Device Adapter snap-in

The following table contains a checklist for upgrading the Avaya Breeze® platform for a Device Adapter snap-in.

The upgrade method is referred to as a rolling upgrade in the Avaya Breeze® platform upgrade documentation. In a rolling upgrade, you can remove the Avaya Breeze® platform servers from service one at a time, upgrade Avaya Breeze® platform, and then put the server back in service. This method allows the traffic to run on the remaining servers, which avoids down time.

In this topic, instructions to upgrade the Avaya Breeze® platform are modified to meet the requirements of the Device Adapter snap-in.

For more information about upgrading the Avaya Breeze® platform, see the *Upgrading Avaya Breeze® platform* guide.

Step	Task	Notes
1	Refer to the Release Notes of the specific Avaya Breeze® platform release to which you want to upgrade. For certain "source" and "destination" combinations, it may be necessary to upgrade the Device Adapter snap-in before you upgrade System Manager and Session Manager.	Typically, an administrator should upgrade the following servers in the following order before upgrading the Avaya Breeze® platform: • System Manager • Session Manager ✱ **Note:** Unless the Release Notes for the Avaya Breeze® platform or Device Adapter indicate a different requirement, the Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the other components, such as Session Manager, Communication Manager, and Application Enablement Services, within the Avaya Aura® solution.
2	Take a backup of the Cluster DB. Store the backup copy of the Cluster DB at a secure location because the Cluster DB of Device Adapter Release 8.1.1 and earlier contains the Personal Directory data.	For more information, see the *Administering Avaya Breeze® platform* guide.

Table continues…

Step	Task	Notes
3	Do the following to identify the active and standby servers: 1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**. 2. Click **Show** corresponding to the cluster name. The **Cluster Database** field displays whether a server is an active, standby, or idle cluster database server. 3. On the Cluster Administration page, identify the cluster that you want to upgrade.	
4	For clusters with multiple servers, determine the sequence in which you want to upgrade the servers.	Avaya recommends the following upgrade sequence: 1. Upgrade all idle servers one at a time. 2. Upgrade the standby server. 3. Switch the active server to be the standby server. This makes the standby server the new active server. 4. Upgrade the new standby server.
5	If required, download the ISO file and patch file of the Avaya Breeze® platform from PLDS. Do the following: 1. Run the checksum comparisons to confirm that the files are complete, and then compare the resulting value to the value on the PLDS page. 2. If the files are correct, copy the ISO file and the patch file to each Avaya Breeze® platform server that you want to upgrade.	For information about downloading the ISO file and patch file from PLDS, see the *Upgrading Avaya Breeze® platform* guide.
6	Verify that the enrollment password for the Avaya Breeze® platform has not expired. ✳ **Note:** If the enrollment password has expired, replication and upgrade cannot finish.	For information about verifying the enrollment password status, see the *Upgrading Avaya Breeze® platform* guide.

Table continues…

Step	Task	Notes
7	Run the following command to change the state of the node that you want to upgrade to **Deny New Service**: `dasrvstart stop all` The preceding command stops the Device Adapter snap-in and the underlying applications, and forces all sets and MGCs to register to another node.	For more information, see the *Upgrading Avaya Breeze® platform* guide.
8	If the next node is an active node, change the status of the active node to standby.	For information about verifying and changing the cluster database server status, see the *Upgrading Avaya Breeze® platform* guide.
9	Take a snapshot of the current VM. This is useful in case you want to revert to the original version.	This task is not required if you are using the Solution Deployment Manager method to upgrade Avaya Breeze® platform.
10	Run the following command to upgrade the Avaya Breeze® platform software: `upgradeCE <isofilename>` After you run the upgrade command, the Avaya Breeze® platform server restarts automatically.	For more information about upgrading the Avaya Breeze® platform by using the ISO file method, see the *Upgrading Avaya Breeze® platform* guide. For information about upgrading the Avaya Breeze® platform by using the Solution Deployment Manager method, see the *Upgrading Avaya Breeze® platform* guide.
11	If required, install the patch file by using the following command: `patchCE`	For more information, see the *Upgrading Avaya Breeze® platform* guide.
12	Upgrade the mandatory snap-ins.	
13	Verify data replication between System Manager and Avaya Breeze® platform.	For more information, see the *Upgrading Avaya Breeze® platform* guide.
14	On System Manager, run maintenance tests for the Avaya Breeze® platform server.	For more information about running maintenance tests, see the *Administering Avaya Breeze® platform* guide. For information about resolving errors shown by the maintenance tests, see the *Maintaining and Troubleshooting Avaya Breeze® platform* guide.

Table continues…

Comments on this document? infodev@avaya.com

Step	Task	Notes
15	Do the following: 1. On System Manager, click **Elements > Avaya Breeze® > Server Administration**. 2. On the Server Administration page, verify the following for the upgraded Avaya Breeze® platform server: • The **Service Install Status** is a green checkmark. • The **Security Module** is Up. • The **License Mode** is a green checkmark. • The **Version** displays the correct release.	
16	Change the state of the upgraded Avaya Breeze® platform node to **Accept New Service**.	For more information about changing the state of the Avaya Breeze® platform node, see the *Upgrading Avaya Breeze® platform* guide.
17	Verify the Avaya Breeze® platform SIP Entity Link with Session Manager.	For more information, see the *Upgrading Avaya Breeze® platform* guide.
18	Repeat Steps 7 through 17 for each server that you want to upgrade.	
19	Delete the snapshots that you no longer need.	

Avaya Device Adapter Snap-in upgrade

You can upgrade the Device Adapter snap-in on an Avaya Breeze® platform cluster by using System Manager. When you upgrade a Device Adapter snap-in on an Avaya Breeze® platform cluster, the Device Adapter snap-in is upgraded on all the nodes within that cluster. The Device Adapter snap-in upgrade process is service impacting.

Unlike Avaya Breeze® platform, the Device Adapter snap-in cannot be upgraded as a rolling upgrade. The Device Adapter snap-in upgrade process takes approximately 6 to 8 minutes. During the upgrade, all IP sets that are on active calls work properly; however, new calls cannot be made or received on these sets. The MGCs restart during the upgrade and active TDM calls are lost.

As part of the Device Adapter snap-in upgrade process, new firmware for the MGCs may be present. In this case, the MGCs upgrade automatically. The MGCs restart during the upgrade process, which results in an additional down time.

> **✴ Note:**
>
> You must disable IP security (IPSec) before upgrading the Device Adapter Snap-in.

Upgrading the Device Adapter Snap-in

Before you begin

- Ensure that you have upgraded Avaya Breeze® platform to a release that is compatible with the Device Adapter Snap-in Release 8.1.2.

- You must disable IP security before upgrading the Device Adapter Snap-in.

  To disable IP security, set the **Enable IPsec for Media Gateways** service attribute to **No**. For more information, see "Service attributes."

  If you do not disable IP security before upgrading the Device Adapter Snap-in, the MGCs and MGXPECs cannot register to the TPS service after the Device Adapter Snap-in is upgraded.

Procedure

1. Upload the new Device Adapter.

   For more information, see

   Avaya recommends that you do not delete the snapshot of Device Adapter snap-in Release 8.1.1 without verifying the working of Device Adapter snap-in Release 8.1.2.

2. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration** .

3. On the Cluster Administration page, select the cluster on which you want to upgrade the Device Adapter snap-in, and then click **Edit**.

   > **✴ Note:**
   >
   > CS 1000 and Device Adapter snap-in Release 8.1.1 and earlier saves the imported contacts in the cluster database where as Device Adapter snap-in Release 8.1.2 saves the contacts in the PPM.

4. On the Cluster Editor page, click the **Services** tab.

5. In the **Assigned Services** area, click **Uninstall / Force Uninstall** corresponding to the existing Device Adapter snap-in to remove the snap-in.

   You must uninstall an existing Device Adapter snap-in because only one Device Adapter snap-in can remain installed at one time.

6. In the **Available Services** area, click the plus sign (**+**) corresponding to the Device Adapter snap-in that you uploaded in Step 1.

   The Device Adapter snap-in is shown in the **Assigned Services** area.

7. Click **Commit**.

   Clicking the **Commit** button uninstalls the old snap-in and installs the new snap-in, which is service impacting.

The sets unregister during this procedure. MGCs restart and TDM calls are lost. However, existing UNIStim calls remain intact.

The down time for the Avaya Breeze® platform server is approximately 6-8 minutes.

8. Verify that the Device Adapter snap-in is installed correctly and calls can be made on both UNIStim and TDM sets.

Next steps

Migrate the Personal Directory data from the Cluster database of Device Adapter Release 8.1.1 and earlier to the PPM of Device Adapter Release 8.1.2.

For more information, see Migrating the Personal Directory data from Device Adapter 8.1.1 and earlier to 8.1.2 on page 189.

Related links

Service attributes on page 157

Avaya Breeze® platform and Device Adapter snap-in upgrade in a geo-redundant model

You can configure and deploy two Avaya Breeze® platform clusters. You can use this deployment model for either geographic redundancy or for an extra layer of redundancy if required. In a geographical redundant model, you can perform upgrades with minimal impact on services.

To configure geo-redundancy, you must create two identical clusters, each with its own Cluster IP. For IP sets, configure S1 (primary server) to point towards the primary cluster IP, and S2 (secondary server) to point towards the geo-redundant cluster. For more information about configuring geo-redundant Avaya Breeze® platform clusters for an IP set, see the IP server settings of that particular IP set.
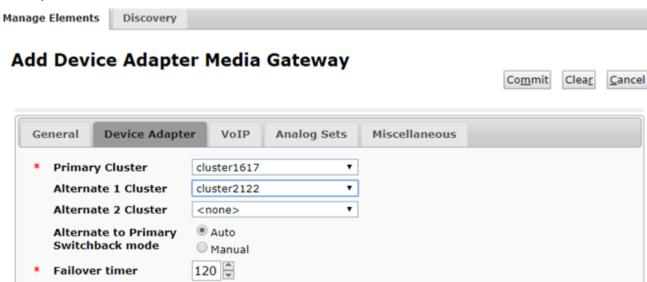
The MGCs require a similar configuration. For more information, see Configuring geo-redundant Avaya Breeze platform clusters for MGCs on page 186.

Configuring geo-redundant Avaya Breeze® platform clusters for MGCs

Procedure

1. Create two identical clusters, each with its own Cluster IP.

   For more information, see "Cluster Administration" in the *Administering Avaya Breeze® platform* guide.

2. On System Manager, click **Services** > **Inventory** > **Manage Elements**.

3. On the Manage Elements page, click **New**.

4. On the New Elements page, on the **General** tab, in the **Type** field, click **Device Adapter Media Gateway**.

5. On the Add Device Adapter Media Gateway page, on the **Device Adapter** tab, in the **Primary Cluster** field, click the primary cluster.

6. In the **Alternate 1 Cluster** field, click a geo-redundant cluster for the primary cluster.

7. Click **Commit**.

Example

Checklist for upgrading the Avaya Breeze® platform and Device Adapter snap-in in a geo-redundant model

Step	Task	Notes
1	On the geo-redundant cluster, stop the DSA services. Stopping the DSA services prevents the traffic from being directed to this node during the upgrade. Traffic continues to run on the primary cluster.	
2	Upgrade the Avaya Breeze® platform on the geo-redundant cluster.	For more information, see Checklist for upgrading the Avaya Breeze platform for a Device Adapter snap-in on page 181.
3	Upgrade the Device Adapter snap-in on the geo-redundant cluster.	For more information, see Upgrading the Device Adapter Snap-in on page 185.

Table continues…

Step	Task	Notes
4	Do the following: 1. On System Manager, click **Elements** > **Avaya Breeze®** > **Server Administration**. 2. On the Server Administration page, verify the following for the upgraded Avaya Breeze® platform server: • The **Service Install Status** is a green checkmark. • The **Security Module** is Up. • The **License Mode** is a green checkmark. • The **Version** displays the correct release.	
5	After the Avaya Breeze® platform and Device Adapter snap-in are upgraded on the geo-redundant cluster, stop the DSA services on the primary cluster. Stopping the DSA services prevents the traffic from being directed to this node during the upgrade. Traffic continues to run on the geo-redundant cluster.	❋ **Note:** This task is service impacting. The MGCs restart and register with the geo-redundant cluster (alternate 1). The sets timeout and register to S2 (secondary server). PPM is not available when the traffic runs on the geo-redundant cluster.
6	Upgrade the Avaya Breeze® platform on the primary cluster.	For more information, see Checklist for upgrading the Avaya Breeze platform for a Device Adapter snap-in on page 181.
7	Upgrade the Device Adapter snap-in on the primary cluster.	For more information, see Upgrading the Device Adapter Snap-in on page 185.

Table continues…

Comments on this document? infodev@avaya.com

Step	Task	Notes
8	After the upgrade is complete, do the following to switch the traffic from the geo-redundant cluster to the primary cluster: • Restart the MGCs. You must have administrative rights to restart an MGC. Restarting an MGC re-registers all the digital and analog sets on the MGC, with up to 160 set re-registrations at one time. • Restart the UNIStim phones. • Stop the DSA services on the geo-redundant cluster to force the sets and MGCs to register back to the primary cluster. You must have administrative rights to stop the DSA services.	

Migrating the Personal Directory data from Device Adapter 8.1.1 and earlier to 8.1.2

About this task

Prior to Device Adapter Release 8.1.2, the Personal Directory data was stored in the cluster database of Avaya Breeze® platform.

In Device Adapter Release 8.1.2, the Personal Directory data is stored in the PPM for Data Privacy.

Use the following procedure to migrate the Personal Directory (PD) data from the cluster database of Device Adapter Release 8.1.1 and earlier to the PPM of Device Adapter Release 8.1.2.

For Data Privacy, you must delete the Personal Directory data from the cluster database.

The migration procedure does not include redial lists and caller lists.

Procedure

1. Log in to System Manager by using the appropriate administrative credentials.

2. On the System Manager web console, change the state of the cluster database to **Deny New Service**. For more information, see the *Upgrading Avaya Breeze® platform* guide.

3. Uninstall Device Adapter Snap-in Release 8.1.1 and earlier and then load and install Device Adapter Snap-in Release 8.1.2. For more information, see Upgrading the Device Adapter Snap-in on page 185.

   PD contacts are still saved in the cluster database.

Avaya recommends that you do not delete the Device Adapter Snap-in Release 8.1.1 without verifying the working of Device Adapter Snap-in Release 8.1.2.

4. Log in to Avaya Breeze® platform server by using SSH and the appropriate credentials.

5. Run the following command to generate the XML file of the PD contacts:

```
pdExport <full_path_to_pd.xml_file>
```

CS 1000 and Device Adapter Snap-in Release 8.1.1 and earlier save the imported contacts in the cluster database, where as Device Adapter Snap-in Release 8.1.2 saves the contacts in the PPM.

6. Run the following command to import data from `pd.xml` file of Device Adapter Snap-in Release 8.1.1 and earlier to the PPM of Device Adapter Snap-in Release 8.1.2:

```
pdImport <full_path_to_pd_xml_file>
```

7. Change the state of the cluster database to **Accept New Service**.

The PD contacts are now available to the Device Adapter endpoints through PPM.

8. After the successful importing of PD data to PPM, run the following command to remove PD information from the cluster database:

> ❗ **Important:**
>
> Before deleting the Personal Directory data from the cluster database, ensure that Device Adapter Release 8.1.2 is working properly. Because, after you delete the Personal Directory data from the cluster database, you cannot downgrade Device Adapter from Release 8.1.2 to Release 8.1.1 without losing the PD data.

```
pdRemove <yes>
```

9. Delete the Device Adapter Snap-in Release 8.1.1 from System Manager.

10. Log out of the Avaya Breeze® platform server.

Related links

Considerations before downgrading Device Adapter from Release 8.1.2 to Release 8.1.1

Consider the following before downgrading Device Adapter from Release 8.1.2 to Release 8.1.1:

- In Device Adapter Release 8.1.2, the Personal Directory data is stored in the Avaya Breeze® platform PPM for Data Privacy. Prior to Release 8.1.2, the Personal Directory data was stored in the Avaya Breeze® platform cluster database.

  In Device Adapter Release 8.1.2, you must migrate the Personal Directory data from the cluster database of Device Adapter Release 8.1.1 and earlier to the PPM. For Data Privacy,

you must delete the Personal Directory data from the cluster database. However, if you delete the Personal Directory data from the cluster database, you cannot downgrade Device Adapter from Release 8.1.2 to 8.1.1 without losing the PD data.

For more information, see Migrating the Personal Directory data from Device Adapter 8.1.1 and earlier to 8.1.2 on page 189.

• Before downgrading Device Adapter from Release 8.1.2 to 8.1.1, ensure that the call center agents are logged out of the CC phones.

For more information, see Incorrect name and extension displayed on a CC phone after downgrading Device Adapter from Release 8.1.2 to Release 8.1.1 on page 297.

Chapter 7: Administration

Avaya Device Adapter Snap-in service administration

The Avaya Device Adapter Snap-in installs on an Avaya Breeze® platform cluster using Avaya Breeze® platform Service Management.

For information and procedures, see "Chapter 5: Avaya Device Adapter Snap-in deployment" in this document as well as "Breeze Service Management" in the *Administering Avaya Breeze® platform* guide.

Device Adapter administration in System Manager
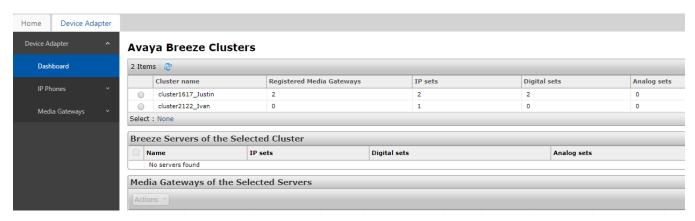
This section describes the Device Adapter elements that can be administered in System Manager. Select **Elements** > **Device Adapter** from the System Manager menu to access the administration screens.

Dashboard

The **Dashboard** screen displays summary information about registered Media Gateway Controllers per cluster and server. Select **Elements** > **Device Adapter** > **Dashboard** from the menu to access this screen.

You can do the following on the Dashboard page to manage the Media Gateway Controllers (MGC):

- Reboot the MGC.
- Re-register the MGC to the primary cluster.
- Force upgrade the MGC to the latest loadware.
- Downgrade the MGC to CS 1000 loadware.
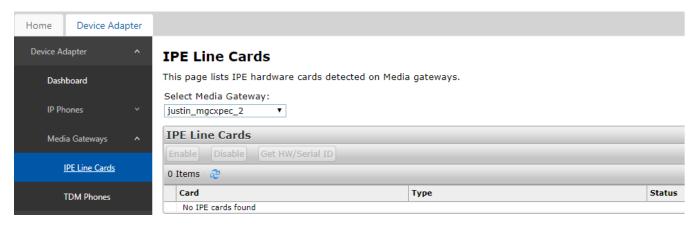
Maintenance and Reports

The **Maintenance and Reports** screen provides a set of IP phone maintenance commands on a selected Avaya Breeze® platform server. Select **Elements** > **Device Adapter** > **IP Phones** > **Maintenance and Reports** from the menu to access this screen.

IPE Line Cards

The **IPE Line Cards** screen provides commands to administer the IPE cards detected on a registered Media Gateway. Cards can be enabled or disabled and the HW/Serial ID retrieved. Select **Elements** > **Device Adapter** > **Media Gateways** > **IPE Line Cards** from the menu to access this screen.

TDM Phones

The **TDM Phones** screen provides commands to administer the TDM endpoints detected on a registered Media Gateway. Endpoints can be enabled or disabled, have the Personal Directory password reset, upgrade the firmware, and retrieve the Serial ID. Select **Elements** > **Device Adapter** > **Media Gateways** > **TDM Phones** from the menu to access this screen.

Related links

[Device Adapter IU commands for IP phones](#) on page 332

Managing IPE line cards on a Media Gateway Controller

Procedure

1. On the System Manager web console, navigate to **Elements** > **Device Adapter** > **Media Gateways** > **IPE Line Cards**.

2. On the IPE Line Cards page, in the **Select Media Gateway** field, click the Media Gateway Controller.

3. In the **IPE Line Cards** area, select the IPE line card that you want to manage.

4. Do one of the following:

   a. Click **Enable** to enable the IPE line card.

b. Click **Disable** to disable the IPE line card.

c. Click **Get HW/Serial ID** to get the hardware information and serial ID of the IPE line card.

Managing TDM phones on a Media Gateway Controller

Procedure

1. On the System Manager web console, navigate to **Elements** > **Device Adapter** > **Media Gateways** > **TDM Phones**.

2. On the TDM Phones page, in the **Select Media Gateway** field, click the Media Gateway Controller.

3. In the **Select IPE Card** field, click the IPE line card.

4. In the **TDM Phones** area, select the TDM phone that you want to manage.

5. Do one of the following:

   a. Click **Enable** to enable the TDM phone.

   b. Click **Disable** to disable the TDM phone.

   c. Click **Get Serial ID** to view the serial ID of the TDM phone.

   d. Click **Reset PD Password** to reset the Personal Directory password.

   e. Click **Upgrade Firmware** to upgrade the firmware.

Starting a snap-in

About this task

The start snap-in functionality is required when you:

- Upgrade the Device Adapter snap-in.
- Change some port assignments for snap-ins.
- Change the capacity of clusters.
- Change some configuration parameters of a snap-in. You must restart the snap-in for the configuration change to take effect.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

2. On the Service Management page, select the snap-in that you want to start.

3. Click **Start**.

4. In the Confirm Start Service dialog box, select the cluster or clusters in which you want to start the snap-in.

5. Click **Start**.

   On the Service Management page, the status of the **Service Install Status** changes to **Starting** and then to **Installed**.

   Restarting the Avaya Breeze® platform server does not affect the snap-in install status.

Stopping a snap-in

About this task

The stop snap-in functionality is required when you:

- Upgrade the Device Adapter snap-in.
- Change some port assignments for snap-ins.
- Change the capacity of clusters.
- Change some configuration parameters of a snap-in. You must restart the snap-in for the configuration change to take effect.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze**® > **Service Management** > **Services**.

2. On the Service Management page, select the snap-in that you want to stop.

3. Click **Stop**.

4. In the Stop Service dialog box, select the cluster or clusters where you want to stop the snap-in.

5. Click **Stop**.

   The **Service Install Status** field changes to **Stopping** and then **Stopped**.

Automatic provisioning

Automatic provisioning is supported by some UNIStim IP phones using:

- 802.1ab Link Layer Discovery Protocol (LLDP)
- Dynamic Host Configuration Protocol (DHCP)
- Configuration files
- UNIStim

UNIStim IP Phones support the following type of provisioning:

- Avaya 1110 IP Deskphone

- Avaya 1120E IP Deskphone

- Avaya 1140E IP Deskphone

- Avaya 1150E IP Deskphone

- Avaya 1165E IP Deskphone

- Avaya 2007 IP Deskphone

- Avaya 1220 IP Deskphone

- Avaya 1230 IP Deskphone

For information about performing this type of provisioning, see "Automatic provisioning" in *Appendix B: Provisioning the IP Phones* of *Avaya Communication Server 1000 IP Deskphones Fundamentals (NN43001-368)* .

Manually adding users and endpoints

It may be necessary during the configuration of Device Adapter to manually add and configure users and endpoints. Manually adding and configuring users and endpoints can also be a useful validation tool before large scale migrations.

Refer to the following documents for information on performing these tasks:

- Adding and configuring Session Manager users

  - *Administering Avaya Aura® Session Manager*

- Adding and configuring Communication Manager users and endpoints

  - *Administering Avaya Aura® Communication Manager*

All documents are available on the Avaya Support site at https://support.avaya.com/.

Security configuration

Device Adapter enables secure communications between endpoints and the Device Adapter cluster using Datagram Transport Layer Security (DTLS). DTLS usage requires both server-side and endpoint actions to be taken.

The DTLS policy service attribute controls the mode of DTLS operation. There are three possible values for this service attribute:

- **Off**

  DTLS is not used. Communications are not secure.

- **Best-effort**

  DTLS is used where possible and supported to secure communications.

- **Always**

  DTLS is always used to secure communications.

Overall solutions can have three levels of security that depend on the solution architecture and the endpoint devices in use:

- **Basic**

  Basic level security uses the **Best-effort** setting of the DTLS policy service attribute. Endpoints are configured with an action byte of 1 and port 4100. There is a brief period of insecure signaling at the beginning of endpoint registration.

- **Advanced**

  Advanced level security uses the **Best-effort** setting of the DTLS policy service attribute. DTLS-capable endpoints are configured with an action byte of 7 and port 4101. All other endpoints are configured with an action byte of 1.

- **Complete**

  Complete level security uses the **Always** setting of the DTLS policy service attribute. All endpoints in use must be DTLS-capable. They are configured with an action byte of 7 and port 4101. Insecure registrations are not permitted.

Additionally, the CA root certificate must be installed on each endpoint. See for information on distributing the certificate to endpoints in the solution.

⭐ **Note:**

If you set the **Enable client authentication** attribute to **Yes**, then the Client Identity Certificate must be installed on the phone.

Mutual DTLS authentication is supported only on the 11xx and 12xx UNIStim endpoints. If the Device Adapter cluster contains any other endpoint; for example, 200x IP UNIStim endpoint, then do not enable client authentication.

The 11xx and 12xx series IP phones are FIPS 140-2 compliant. Ensure that the Client Identity Certificates that are installed on these phones have a key length of at least 2048 bit. This is required for the FIPS compliance process.

You can install the Client Identity Certificate on the 11xx and 12xx UNIStim endpoints by doing any of the following:

- Use SCEP.
- Download the PKCS#12 file that is specified in the [DEV_CERT] configuration section of the *UNIStim Software Release 4.3 for IP Deskphones* Release notes.

For more information about installing the Client Identity Certificate on the 11xx and 12xx UNIStim endpoints, see the *UNIStim Software Release 4.3 for IP Deskphones* Release notes.

Configuring DTLS policy to secure communications between phones and Device Adapter cluster

About this task

⁂ **Note:**

> Mutual DTLS authentication is supported only on the 11xx and 12xx IP UNIStim phones. If the Device Adapter cluster contains any other phone; for example, 200x IP UNIStim phone, then do not enable client authentication.

If you set the **Enable client authentication** attribute to **Yes**, then you must install the Client Identity Certificate on the 11xx and 12xx IP UNIStim phones. During registration, the IP phones send this certificate to Device Adapter for mutual authentication.

The 11xx and 12xx series IP phones are FIPS 140-2 compliant. Ensure that the Client Identity Certificates that are installed on these phones have a key length of at least 2048 bit. This is required for the FIPS compliance process.

You can install the Client Identity Certificate on the 11xx and 12xx UNIStim phones by doing any of the following:

- Use SCEP.
- Download the PKCS#12 file that is specified in the [DEV_CERT] configuration section of the *UNIStim Software Release 4.3 for IP Deskphones* Release notes.

For more information about installing the Client Identity Certificate on the 11xx and 12xx UNIStim phones, see the *UNIStim Software Release 4.3 for IP Deskphones* Release notes.

Procedure

1. Log on to System Manager by using administrative credentials.

2. Navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to configure the DTLS policy at a cluster level or a global level, do one of the following:

   - Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.
   - Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **IP Telephony Node / DTLS** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **DTLS policy** field, in **Effective Value**, click the DTLS policy that you want to use to secure communications between phones and Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.

8. In the **Enable client authentication** field, in **Effective Value**, click **Yes** to enable client authentication.

9. Click **Commit**.

Related links

Distributing the root certificate

About this task

Use the following procedure to distribute the root CA certificate to endpoints in the solution. Certificate distribution is a mandatory part of creating a secure communications solution. For more information, see Security configuration on page 197.

Procedure

1. Log on to System Manager by using the appropriate credentials.

2. Navigate to **Services** > **Security** > **Certificates**.

3. Click **Authority**, and then click **CA Structure & CRLs**.

4. Select **Download PEM file**.

5. Export the certificate file to a local or network drive.

6. Incorporate the certificate file into a group configuration file.

7. Place the group configuration file in a TFTP server the endpoints can access.

    ✱ **Note:**

    Configure a TFTP server for the endpoints if one has not already been included in the endpoint configuration.

8. Restart or re-register the endpoint so it will download the group configuration file.

    ✱ **Note:**

    Refer to the individual UNIStim IP Phone documentation suites for information and procedures on installing the certificate file if installation must be performed manually.

    ❗ **Important:**

    The CA root certificate should be installed in **Trusted Root Certification Authorities** > **Local Machine** for the i2050 software endpoint on Microsoft Windows. Certificate Manager attempts to install it in **Trusted Root Certification Authorities** > **Registry** by default.

    - For additional information if the certificate must be installed manually on an i2050 endpoint, go to HTTPS://SUPERUSER.COM/QUESTIONS/647036/VIEW-INSTALL-CERTIFICATES-FOR-LOCAL-MACHINE-STORE-ON-WINDOWS-7.

    - For additional information about certificate handling, go to Certificate handling on page 70.

Configuring XPORT 9408

About this task

Use the following procedure to configure XPORT 9408. XPORT 9408 is used to support features such as Hotline, Speed Dial, Multiple Appearance DN, and Short Hunt.

Procedure

1. Log in to Communication Manager with the appropriate administrative credentials.
2. Create a new endpoint.
3. Select **9408_DEFAULT_CM_8_0** in the **Template** field.
4. Confirm the value X is populated into the **Port** field.
5. Enter an appropriate value in the **Extension** field.
6. Click **Commit**.
7. Select the **CS1K-IP** endpoint.
8. Select the **Button Assignment** tab.
9. Go to a blank line in the **Button Configurations** section.
10. Select **brdg-appr** in the **Button Feature** column.
11. Enter a in the **Argument-1** column.
12. Enter the extension number used earlier in this procedure in the **Argument-2** column.
13. Enter n for the silent ring option or r for the audible ring option in the **Argument-3** column.
14. Select the **General Options** tab.
15. Enter the mnemonics in the **Features** field that correspond to the feature being configured.
16. Click **Commit**.

Configuring Corporate Directory support

About this task

Corporate directory allows UNIStim and 39xx endpoints to display and access a corporate-wide telephone directory.

Before you begin

Corporate Directory support requires the use of Avaya Aura® Device Services (AADS). Ensure that AADS is available in your Avaya Aura® solution prior to performing this procedure.

Procedure

1. On the endpoints, set CLS to CRPA.

2. Log on to System Manager by using administrative credentials.

3. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

4. Click **Attributes**.

5. Depending on whether you want to configure the Corporate Directory support at a cluster level or a global level, do one of the following:

   • Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   • Click the **Service Global** tab and select the service as **DeviceAdapter**.

6. On the Attributes Configuration page, navigate to the **Contacts** group and do the following:

   a. In the **Enable Corporate Directory** field, in **Effective Value**, click **Yes** to enable Corporate Directory support.

   b. In the **Avaya Aura Device Services (AADS) FQDN** field, in **Effective Value**, type the FQDN that you want to use to access the AADS server.

   c. In the **Avaya Aura Device Services (AADS) Port** field, in **Effective Value**, type the port number that you want to use to access the AADS server.

      The default port is 8443 or 443.

   d. Click **Commit**.

7. Click **Services** > **Inventory** > **Manage Elements**.

8. On the Manage Elements page, on the **Manage Elements** tab, click **New** and configure AADS.

   For more information, see Avaya Aura® Device Services documentation.

9. Do the following to assign Session Manager to a data center and pair the assigned data center with Avaya Aura® Device Services:

   a. On the System Manager web console, navigate to **Elements** > **Session Manager** > **System Status**.

   b. Click **User Data Storage**.

   c. On the User Data Storage page, click the **Data Center** tab.

   d. Select the data center for which you want to assign the Session Manager and click **Edit**.

   e. In the **Data Center** field, click the configured data center and click **Commit** to save the changes.

   f. Click the **Backup and Restore** tab.

   g. Click **Configure Backup** and enter the required details of the backup server.

   h. Click **Test Connection** to check the connectivity of the data center and Session Manager and click **OK** to exit the dialog box.

      i. On the System Manager web console, navigate to **Elements** > **Session Manager** > **Session Manager Administration**.

      j. Click the **Session Manager Instances** tab.

      k. Select the Session Manager instance that you want to pair with Avaya Aura® Device Services and click **Edit**.

      l. In the **Data Center** field, click the configured data center assigned to Session Manager.

      m. In the **Avaya Aura Device Services Server Pairing** field, select the available and configured Avaya Aura® Device Services for pairing.

      n. Click **Commit** to save the changes.

10. Do the following to generate and export the SIP certificate:

      a. On the System Manager web console, navigate to **Services** > **Inventory**

      b. Click **Manage Elements**, and then select the Avaya Breeze® platform server.

      c. Click **More Actions** > **Manage Identity Certificates**.

      d. In the Manage Identity Certificates window, click the SIP certificate, and then click **Export**.

11. On AADS server, import the certificate that you generated in Step 10 to add the FQDN of Avaya Breeze® platform to the trusted hosts.

     If Avaya Breeze® platform, Session Manager, and AADS are on the same System Manager, then AADS can register itself on the System Manager to get the certificates automatically. You can also import System Manager root CA to the AADS server.

     For more information, see the Avaya Aura® Device Services documentation.

12. Create users on the LDAP server. For corporate directory to function, only one LDAP user is required. The login name of the user must match the FQDN of the Avaya Breeze® platform Asset Interface.

     For more information about LDAP server configuration, see *Deploying Avaya Aura® Device Services* guide.

13. Add the CS 1000 users to the System Manager UPM. Device Adapter updates the Corporate Directory data with the System Manager UPM data.

     Do the following for various CS 1000 releases:

- If you run CS 1000 release 6.0 or earlier or releases 7.0 through 7.5, and use a simple CSV file import, do a bulk import into UPM according to the CSV format that UPM supports. For more information, see the *Administering Avaya Aura® System Manager* guide.

- If you run CS 1000 release 7.0 through 7.5 and sync the user accounts for Corporate Directory from LDAP, import the LDAP users into UPM. For more information, see *Administering Avaya Aura® System Manager* guide.

- If you run CS 1000 release 7.6, which is integrated with System Manager, you need not do anything.

  For CS 1000 release 7.6, all users are included in the Corporate Directory, regardless of whether you enable or disable the CS 1000 Endpoint Communication Profile option and select or clear the **Include in Corporate Directory** check box.

Setting the Pulse Code Modulation companding law for endpoints that are migrated to Device Adapter

Procedure

1. Log on to System Manager by using administrative credentials.
2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.
3. Click **Attributes**.
4. Depending on whether you want to set the companding law at a cluster level or a global level, do one of the following:
   - Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.
   - Click the **Service Global** tab and select the service as **DeviceAdapter**.
5. On the Attributes Configuration page, navigate to the **IP Telephony Node / Codecs / Companding Law** group.
6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.
7. In the **Companding law** field, in **Effective Value**, click the companding law that you want to use for the endpoints on the Device Adapter node.
8. Click **Commit**.

Related links

Configuring G.711, G.722, G.729, and G.723.1 codec settings for Device Adapter

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze**® >
   Configuration.

3. Click **Attributes**.

4. Depending on whether you want to configure the codec settings at a cluster level or a
   global level, do one of the following:

   • Click the **Service Clusters** tab, select the cluster, and then select the service as
     DeviceAdapter.

   • Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, do the following:

   a. To configure the G.711 settings, configure the service attributes in the **IP Telephony
      Node / Codecs / G.711** group.

   b. To configure the G.722 settings, configure the service attributes in the **IP Telephony
      Node / Codecs / G.722** group.

   c. To configure the G.729 settings, configure the service attributes in the **IP Telephony
      Node / Codecs / G.729** group.

   d. To configure the G.723.1 settings, configure the service attributes in the **IP Telephony
      Node / Codecs / G.723.1** group.

6. Click **Commit**.

Related links

[Service attributes](#) on page 157

Enabling VoIP monitoring

About this task

VoIP monitoring monitors the Quality of Service (QoS) of voice calls. When you enable VoIP
monitoring, Device Adapter monitors the following QoS parameters: packet count, RTT, jitter buffer
delay, maximum jitter, payload type, source and destination IP addresses, and port numbers.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze**® >
   Configuration.

3. Click **Attributes**.

4. Depending on whether you want to enable VoIP monitoring at a cluster level or a global
   level, do one of the following:

   • Click the **Service Clusters** tab, select the cluster, and then select the service as
     DeviceAdapter.

- Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **IP Telephony Node / Quality of Service (QoS)** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **VoIP Monitoring Enabled** field, in **Effective Value**, click **Yes** to enable VoIP monitoring on the Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.

8. In **VoIP Monitoring Reporting Interval** field, in **Effective Value**, type the duration of time after which Device Adapter must run the VoIP monitoring report.

9. In the **VoIP Monitoring Manager IP address** field, in **Effective Value**, type the IP address of the VoIP Monitoring Manager (VMM).

10. In the **VoIP Monitoring Manager Port** field, in **Effective Value**, type the port number of the VMM.

11. In **Enable VLAN Tagging (802.1Q support)** field, in **Effective Value**, click **Yes** to enable VLAN tagging to support the 802.1Q networking standard.

12. Click **Commit**.

Related links

[Service attributes](#) on page 157

Configuring the port number for RTP/RTCP

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to configure the port number at a cluster level or a global level, do one of the following:

   - Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   - Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **IP Telephony Node / LAN** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **RTP/RTCP starting port** field, in **Effective Value**, type the port number used by the RTP packets.

   The port number must have two sequential numbers: one for RTP and the other for RTCP. The subsequent port number is used for RTCP.

8. Click **Commit**.

Related links

Enabling Personal Directory support

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to enable Personal Directory support and call logging at a cluster level or a global level, do one of the following:

   • Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   • Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Contacts** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **Enable Personal Directory** field, in **Effective Value**, click **Yes** to enable Personal Directory functionality on the Device Adapter endpoints.

8. Click **Commit**.

Next steps

Enable callers list, redial list and call information logging for Personal Directory.

Related links

Enabling callers list, redial list, and call information logging for Personal Directory

About this task

An administrator can enable callers list and redial list with Personal Directory contacts by using the following procedure.

Before you begin

Ensure that Personal Directory functionality is enabled on the Device Adapter endpoint.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to enable callers list, redial list, and call logging at a cluster level or a global level, do one of the following:

   - Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   - Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Call Logs** group.

6. In the **Enable Callers and Redial List** field, in **Effective Value**, click **Yes** to enable callers list and redial list with Personal Directory contacts on the Device Adapter endpoints.

7. In the **Default incoming call log mode** field, in **Effective Value**, click an option depending on whether you want the Callers List to log all incoming calls or only the unanswered incoming calls.

8. Click **Commit**.

Next steps

After you enable Personal Directory, callers list, and redial list, you must select **Enable Centralized Call History?:** check box in **Session Manager Profile** to retain the call history for callers list and redial list after a station reboot. For more information, see *Administering Avaya Aura® Session Manager* document.

Related links

[Enabling Personal Directory support](#) on page 207

Enabling SSH access for Device Adapter

About this task

The **Enable SSH access on Secure Link** option is available only on the **Service Clusters** tab. You can enable SSH access only at a cluster level.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Secure Link Access** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **Enable SSH access on Secure Link** field, in **Effective Value**, click **Yes** to enable SSH access, on a Secure Link interface, to the Avaya Breeze® platform cluster where the Device Adapter snap-in is deployed.

8. Click **Commit**.

Related links

[Service attributes](#) on page 157

Configuring time period for NAT mapping

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to configure time period for NAT mapping at a cluster level or a global level, do one of the following:

   • Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   • Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Network Address Translation (NAT)** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **NAT Mapping Keep Alive Timeout** field, in **Effective Value**, type the duration of time, in seconds, after which you want to refresh the audio and signaling port mapping.

8. Click **Commit**.

Related links

Configuring the display text, country, dial tone timeout, interdigit timeout, and busy/overflow timeout for Device Adapter endpoints

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to configure the display text, country, dial tone timeout, interdigit timeout, and busy/overflow timeout at a cluster level or a global level, do one of the following:

    • Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

    • Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Miscellaneous Parameters** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **Idle set display** field, in **Effective Value**, type the text that you want to display on the idle endpoints.

8. In the **Country** field, in **Effective Value**, click the country where the endpoints are located.

9. In the **Dial tone timeout** field, in **Effective Value**, type the duration of time the dial tone is played without the user entering a digit.

10. In the **Inter-digit timeout** field, in **Effective Value**, type the duration of time to wait for another digit before attempting the call.

11. In the **Busy/overflow timeout** field, in **Effective Value**, type the duration of time the busy tone and call failure tone are played.

12. Click **Commit**.

Related links

[Service attributes](#) on page 157

Configuring timers for analog endpoints

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to configure timers for analog endpoints at a cluster level or a global level, do one of the following:

   • Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   • Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, configure the attributes in the **Peripheral Equipment / Analog Set Timers** group.

6. Click **Commit**.

Related links

[Service attributes](#) on page 157

Chapter 8: Administration of call center feature buttons for Device Adapter phones

Overview

This chapter provides information about configuring call center feature buttons for Device Adapter phones that are supported in Call Center Elite environment.

For information about configuring Call Center Elite features, see the *Avaya Aura® Call Center Elite Feature Reference* and *Administering Avaya Aura® Call Center Elite* guides.

Log in and Log out buttons

When you configure the **Log in** button for a CC phone, the **Log out** button is automatically configured for the phone. The **Log in** and **Log out** buttons appear as toggle buttons on the phone.

The phone screen displays the **Log in** button in the following scenarios:

- When an agent is logged out and trying to login.
- Avaya Aura® Call Center Elite has rejected the login request.

> ✱ **Note:**
>
> If you have not configured a password for the agent, then the agent should not enter * or any password digit after entering the agent ID. As password is not required, Communication Manager does not validate the password and considers the digits after * as a valid password and logs the agent in to the phone.
>
> For information about configuring the agent ID and password, and configuring reason code for agent logout, see the *Administering Avaya Aura® Call Center Elite* guide.

For a logged in agent, the phone screen displays the **Log out** button.

In addition, the phone screen displays the **Log out** button in the following scenarios:

- Avaya Aura® Call Center Elite has rejected the logout request.

- An agent is currently on an active call and presses the **Log out** button. The Device Adapter phone moves to the pending logout state and the agent will be logged out only if the active call is ended.

Depending on the login status of an agent, the Device Adapter phone toggles between the **Log in** and **Log out** buttons.

Configuring a Log in and Log out button for a CC phone

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the login button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In the **Button Feature** field corresponding to the button number that you want to configure as a login button, click **agnt-login**.

   b. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a login button, type a name for login label. For example, Login.

      This label appears on the endpoint.

      If you do not specify a label, the default label that appears on the endpoint is **Log in**.

6. Click **Commit** to save the changes.

Configuring logout override button for an agent

About this task

During Forced logout by clock time, Call Center Elite automatically logs the agent out at a predefined time. If the agent is not on an ACD or DAC call, the agent is logged out immediately. If the agent is on an ACD or DAC call, the agent typically hears a tone burst and the pending icon for logout is displayed. While on an ACD or DAC call, if the agent detects a pending logout, the agent can override the logout for the remainder of the shift hours for that shift by using the logout override button. The logout by clock time recurs for the next shift.

If the agent cannot override the logout, provided the Avaya Aura® Call Center Elite does not have the maximum number of registered agents at the time, the agent can log in back again after the logout is successful.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the logout override button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

    a. In another **Button Feature** field, click **logout-ovr**.

    b. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a logout override button, type a name for the label. For example, Logout Override.

       This label appears on the endpoint.

       If you do not specify a label, the default label that appears on the endpoint is **Logout Ovr**.

6. Click **Commit** to save the changes.

Configuring Auto-in button for an agent

About this task

The Auto In work mode enables the agent to go back to the ACD available queue as soon as the agent ends the ongoing call.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the Auto-in button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

    a. In the **Button Feature** field, click **auto-in**.

    b. In the **auto-in Grp** field, enter the split group number for ACD.

    c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as an Auto-in button, type a name for the label. For example, Auto-in.

This label appears on the endpoint.

If you do not specify a label, the default label that appears on the endpoint is **Auto-in**.

6. Click **Commit** to save the changes.

Configuring Manual-in button for an agent

About this task

The Manual-in work mode requires the agent to press the Manual-in button after ending each call in order to make the agent available to service the ACD queue.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the Manual-in button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In the **Button Feature** field, click **manual-in**.

   b. In the **manual-in Grp** field, enter the split group number for ACD.

   c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a Manual-in button, type a name for the label. For example, Manual-in.

   This label appears on the endpoint.

   If you do not specify a label, the default label that appears on the endpoint is **Manual-in**.

6. Click **Commit** to save the changes.

Configuring After Call Work button for an agent

About this task

An After Call Work mode indicates that the agent is performing after call work, such as completing a call-related form, after the agent ends an incoming call.

If you have programmed timed after call work for an agent, then button configuration is not required on the agent's endpoint. The button configuration is required only if you want to show

after call work mode on the agent's phone during transition from one work mode to another or the agent is allowed to extend the after call work time.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the After Call Work button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In the **Button Feature** field, click **after-call**.

   b. In the **after-call Grp** field, enter the split group number for ACD.

   c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a After Call Work button, type a name for the label. For example, After Call Work.

   This label appears on the endpoint.

   If you do not specify a label, the default label that appears on the endpoint is **ACW**.

6. Click **Commit** to save the changes.

Configuring Auxiliary Work button for an agent

About this task

The agent uses the Auxiliary Work mode for reasons such as to take a lunch break.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the Auxiliary Work button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In the **Button Feature** field, click **aux-work**.

   b. To program the default reason code for work mode transition to Auxiliary Work, enter the reason code in the **Reason Code** field that the agent by default uses while using the Auxiliary Work mode button.

       c. In the **Hunt Grp** field, enter the split group number for ACD.

       d. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as an Auxiliary Work button, type a name for the label. For example, Auxiliary Work.

          This label appears on the endpoint.

          If you do not specify a label, the default label that appears on the endpoint is **Aux work**.

6. Click **Commit** to save the changes.

Interruptible Auxiliary work mode

About Interruptible Auxiliary work mode

Using Interruptible Auxiliary work mode, you can either notify or force an agent to move to Auto-in or Manual-in mode to receive an incoming call waiting in the queue.

For Interruptible Auxiliary work mode, you must configure the reason code for the Auxiliary work mode as Interruptible. For more information, see the *Administering Avaya Aura® Call Center Elite* guide.

The configuration of Interruptible Auxiliary work mode depends on the **Reason code** type and **Reserve level** configured for an agent.

For example, if the **Reserve level** is configured as **Notify Interrupt**, then depending on the configuration of **Interruptible Aux Threshold** parameter in **Hunt Group Settings**, Communication Manager notifies an agent that the agent needs to move to the available state to receive the calls waiting in the queue.

Configuring interruptible auxiliary threshold and interruptible auxiliary deactivation threshold

About this task

The threshold can be set to one of the following:

- Number of calls waiting to be served
- Age of the oldest call in the queue
- A service level target

The deactivation threshold is set to coordinate with the activation threshold.

For example, if the notification is set as calls-warning-threshold, a value from 0 to 998 is assigned, and when the total queued calls drops below this value, the interruptible notifications clear. The deactivation threshold must be less than the activation threshold.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Groups**.

3. Click **Hunt Group**.

4. On the Hunt Group page, select the group number for which you want to configure the Interruptible Aux parameters, and then click **Edit**.

5. Click the **Interruptible Aux & RONA Parameters (R)** tab.

6. In the **Interruptible Aux Threshold** field, select one of the following:

   • **calls-warning-threshold**: Use this option to enable the Interruptible Aux feature when the service level drops below the administered percentage of calls within the specified period.

      You can configure the **calls-warning-threshold** value by clicking the **General Options (O)** tab.

   • **service-level-target**: Use this option to enable the Interruptible Aux feature when the number of calls in the queue for a hunt group exceeds the specified number of calls.

      You can configure the **service-level-target** value by clicking the **ACD Parameters (A)** tab.

   • **time-warning-threshold**: Use this option to enable the Interruptible Aux feature when the oldest call in the queue is waiting for longer than the specified number of seconds.

      You can configure the **time-warning-threshold** value by clicking the **General Options (O)** tab.

   • **none**: Use this option if you do not want to administer the Interruptible Aux feature.

7. In the **Interruptible Aux Deactivation Threshold** field, enter one of the following:

   • If you set the value of the **Interruptible Aux threshold** field to **calls-warning-threshold**, the valid entries for the **Interruptible Aux Deactivation Threshold** field are from **0** to **999**.

   • If you set the value of the **Interruptible Aux threshold** field to **service-level-target**, the valid entries for the **Interruptible Aux Deactivation Threshold** field are from **0** to **100**.

   • If you set the value of the **Interruptible Aux threshold** field to **time-warning-threshold**, the valid entries for the **Interruptible Aux Deactivation Threshold** field are from **0** to **999** in seconds.

   • If you set the value of the **Interruptible Aux threshold** field to **none**, the system does not display the **Interruptible Aux Deactivation Threshold** field.

8. Click **Commit**.

Configuring Agent Reserve Level

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Call Center**.

3. Click **Agents**.

4. Select the agent and click **Edit**.

5. Click the **Agent Skills (S)** tab.

6. In the **Reserve Level** field, select:

   - **Auto In Interrupt**: To change to Auto-In when the notification timer expires.

   - **Manual In Interrupt**: To change to Manual-In when the notification timer expires.

   - **Notify Interrupt**: To provide notification only.

7. Click **Commit**.

   > **Important:**
   >
   > If auto-answer is enabled on the agent's phone, then Avaya Aura® Call Center Elite will always set the **Reserve Level** as **Notify Interrupt** irrespective of the **Reserve Level** set by the administrator.
   >
   > This is because if auto-answer is enabled and the **Reserve Level** is set to **Auto In Interrupt** or **Manual In Interrupt**, the call will be placed on the agent's phone automatically. And if the agent is not present at the desk or does not want to answer the call, the call will not be completed and will be considered as a lost call.

Configuring interruptible auxiliary notification timer

About this task

If the **Reserve Level** is set to **Auto In Interrupt** or **Manual In Interrupt**, and if Auto-Answer is not enabled, Call Center Elite can interrupt the Aux work mode of an agent and present the call to the agent. The interruptible auxiliary notification timer ensures that the agent is not immediately made available to receive calls. Instead, the notification timer provides a brief period to an agent already in the interruptible Auxiliary mode before that agent is made available automatically.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Parameters**.

3. Click **System Parameters - Features**.

4. In the **Interruptible Aux Notification Timer (sec)** field, enter the number of seconds the notification and the flashing lamp or tone are presented before agent is put in Auto-in or Manual-in mode.

   The default value is 3.

5. Click **Commit**.

Set default work mode upon agent login

You can set the default work mode that the agent must be placed in after the agent logs in to the phone as a Call Center Elite agent.

For example, you might want the agent to be placed in the Auto-in work mode as soon as the agent logs in. The Auto-in work mode automatically makes an agent available to receive incoming call center calls.

If you do not set a default work mode, Call Center Elite uses the Aux work mode as the default work mode upon agent login.

For information about setting the default work mode upon agent log in, see the *Administering Avaya Aura® Call Center Elite* guide.

Configuring button labels for a CC phone

About this task

If you do not specify a button label for a CC feature button, then the label name in the **Button Feature** field is used as the default label for the button on the phone.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure a button label, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

6. In the **Button Label** field corresponding to the button number, type a name for the button label.

   This label appears on the endpoint.

An administrator can configure up to 100 characters in the **Button Label** field, but the phone screen displays maximum of 10 characters.

7. Click **Commit** to save the changes.

An administrator can revert back to the default **Button Label** by clearing the value in the **Button Label** field and saving it by clicking on the **Commit** button.

Vector Directory Number return destination

An agent can end a call on a VDN specified destination using Vector Directory Number (VDN). A call ends on a VDN destination only if an agent releases the call and the incoming call is from an active VDN.

A use case of using a VDN return destination is that a supervisor can schedule a survey for the customers by configuring the Vector Directory Number (VDN) return destination. After configuring the VDN destination number, a caller can rate the call, based on the caller's interaction with the agent.

For more information about VDN return destination, see the *Administering Avaya Aura® Call Center Elite* guide.

For information about scheduling a customer survey, see the documentation for your IVR system.

Configuring VDN return destination

Before you begin

Ensure that the incoming call is from an active VDN, that is, the call must be an ACD call.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Call Center**.

3. Click **Vector Directory Number**.

4. On the Vector Directory Number page, select the CC endpoint for which you want to configure the VDN return destination, and then click **Edit**

5. On the Edit Vector Directory Number page, click the **Basic Information** tab.

6. In the **Return Destination +** field, type the VDN return destination number.

7. Click **Commit** to save the changes.

Configuring the MWI feature for a CC phone

About this task

You can configure the Message Waiting Indicator (MWI) feature to alert a call center agent about a new incoming voice mail message or any unopened voice mail message from any of the following:

- Depending on the agent login status, the voice mail box of the call center agent or the voice mail box of the station extension.

- The voice mail box of the station extension only.

> ✱ **Note:**
>
> If you configure MWI for the agent ID, then a lit message waiting indicator lamp on the phone indicates any one of the following:
>
> - If the agent is logged in to the phone as a call center agent, the message waiting indicator is for the voice mail box of the agent.
>
> - If the agent is logged out of the phone, the message waiting indicator is for the voice mail box of the station extension.

For information about listening to the voice mail messages, see the *Avaya Device Adapter User Guide for Avaya Aura*® *Call Center Elite*.

Before you begin

Ensure that the voice mail accounts for both agent ID and station extension are configured on the Voice Messaging Service.

Procedure

1. Log on to System Manager by using administrative credentials.

2. Do the following to specify the voice mail box for which message waiting indicator should be displayed:

   a. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Parameters**.

   b. Click **System Parameters — Features**.

   c. On the System Parameters — Features page, in the **Select device(s) from Communication Manager List** area, click the Communication Manager instance that provides service to the endpoints.

      The MWI configuration is applied to the endpoints that are served by the Communication Manager instance that you select.

   d. In the **System Parameters — Features List** area, click the button corresponding to the system parameters features list that is associated with the Communication Manager instance, and then click **Edit**.

   e. On the change system-parameters features page, navigate to the page that contains the **Message Waiting Lamp Indicates Status For:** field.

f. In the **Message Waiting Lamp Indicates Status For:** field, do any one of the
following:

- To configure MWI for an agent ID, click **loginID**.

  If you select the **loginID** option, a lit message waiting indicator LED on the phone
  indicates any of the following:

  - If an agent is logged in to the phone as a call center agent, a lit message waiting
    indicator LED on the phone along with **MWI: Agent** displayed on the phone
    screen indicates that there are one or more unopened voice mail messages in
    the voice mail box of the agent.

  - If an agent is logged out of the phone as a call center agent, a lit message
    waiting indicator LED on the phone along with **MWI: Station** displayed on the
    phone screen indicates that there are one or more unopened voice mail
    messages in the voice mail box of the station extension.

- To configure MWI for the station extension only, click **station**.

  If you select the **station** option, then irrespective of whether an agent is logged in
  or logged out of the phone, a lit message waiting indicator LED on the phone along
  with **MWI: Station** displayed on the phone screen indicates that there are one or
  more unopened voice mail messages in the voice mail box of the station extension.

  However, if the agent is logged in to the phone, **MWI: Station** is displayed on the
  phone only when the agent is in the Aux work mode after logging in.

  By default, MWI is set to **station**.

3. Administer the MWA (Message Waiting Allowed) mnemonic.

Related links

Configuring call queue status key for a CC phone

About this task

Use this procedure to do the following:

- Configure the **q-calls** button for the CC phone.
- Configure the **Queue Parameters** for the hunt group.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication
   Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the call queue status key, and then click **Edit**.

5. Do the following to configure the **q-calls** button for the endpoint:

   a. On the Edit Endpoint page, click the **Button Assignment** tab.

   b. In the **Button Feature** field corresponding to the button number that you want to configure as the **q-calls** button, click **q-calls**.

   c. In the corresponding **q-calls Grp** field, type the skill group number of the queue which is assigned to the agent.

   d. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure for queue calls information, type a name for the queue calls information button. For example, queue-calls.

      This label appears on the endpoint.

      If you do not specify a label, the default label that appears on the endpoint is **Queue Stat**.

   e. Click **Commit** to save the changes.

6. Do the following to configure the **Queue Parameters** for the assigned queue group:

   a. Navigate to **Elements** > **Communication Manager** > **Groups**.

   b. Click **Hunt Group**.

   c. On the Hunt Group page, select the group number for which you want to configure the **Queue Parameters**.

   d. Click the **General Options** tab.

   e. In the **Queue Parameters**, type the appropriate values in the following fields:

      • **Queue Limit**

      • **Calls Warning Threshold**

      • **Time Warning Threshold**

   f. Click **Commit** to save the changes.

Enable the display of UUI information on a CC phone

You must perform the following configuration in System Manager to enable the display of User-to-User (UUI) information during an ACD call on a CC phone:

• In the Class of Restriction (COR) number that you want to use, set the **Station-Button Display of UUI IE Data?** COR parameter to Yes.

• Assign this COR number to the endpoint and configure the **UUI Info** button for the phone.

Administering COR to enable the display of UUI information on a CC phone

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **System**.

3. Click **Class of Restriction**.

4. On the Class of Restriction (COR) page, click the COR number that you want to modify, and then click **Edit**.

5. Navigate to the page that contains the **Station-Button Display of UUI IE Data?** COR parameter, and set this parameter to **y(es)**.

Next steps

Assign this COR number to the CC endpoint.

Configuring the UUI Info button and assigning the COR number to the CC endpoint

About this task

The call center agent uses the **uui-info** button to view the UUI information during an active ACD call.

Use this procedure to do the following:

- Configure the **uui-info** button for the CC endpoint.
- Assign the COR number that has the **Station-Button Display of UUI IE Data?** COR parameter set to Yes to the CC endpoint.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the **uui-info** button and assign the COR number, and then click **Edit**.

5. Do the following to assign the COR number to the endpoint:

   a. On the Edit Endpoint page, click the **General Options** tab.

   b. In the **Class of Restriction (COR)** field, type the COR number that has the **Station-Button Display of UUI IE Data?** COR parameter enabled.

6. Do the following to configure the **UUI Info** button for the endpoint:

   a. On the Edit Endpoint page, click the **Button Assignment** tab.

   b. In the **Button Feature** field corresponding to the button number that you want to configure as the **UUI Info** button, click **uui-info**.

   c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure for UUI information, type a name for the UUI info button. For example, UUI_Info.

   This label appears on the endpoint.

   If you do not specify a label, the default label that appears on the endpoint is **UUI info**.

7. Click **Commit**.

Result

The **UUI info** button appears on the CC phone.

Configuring call work code button for an agent

About this task

Device Adapter for Avaya Aura® Call Center Elite allows an agent to enter a call work code. Call work codes are digit sequences of up to 16 digits. You can use call work codes to track customer-defined events. A call work code depends on a Call Center usage, for example, a call work code can be a social security number or an agent's account code.

A use case of call work codes in Call Centers can be tracking state of an agent for accounting purpose. In this case, an agent must enter a call work code (account code in this case) before changing the work mode from ACW to Auto-in or Manual-in.

Call work codes can be optional or forced.

If an agent enters a call work code during a call, then it is an optional work code. If you have programmed forced call work code, then the agent has to enter the call work code after the completion of a call, even if the agent has entered the work code during the call.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the call work code button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In another **Button Feature** field, click **work-code**.

   b. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a work code button, type a name for call work code label. For example, WorkCode.

      This label appears on the phone.

      If you do not specify a label, the default label that appears on the phone is **CWC**.

6. Click **Commit** to save the changes.

Configuring the Supervisor Assist feature for a CC phone

About this task

An agent can request assistance from a supervisor by using the Supervisor Assist feature.

When the supervisor answers the call, the agent do one of the following:

- Establish a conference call among the agent, caller, and the supervisor.
- Transfer the call to the supervisor.
- End the call with the supervisor.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the Supervisor Assist feature, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In **Button Feature** field, click **assist**.

   b. In the corresponding **assist Grp** field, type the hunt-group number assigned to the logged in agent.

   c. Navigate to **Groups** > **Hunt Group**.

   d. Select the hunt group assigned to the **assist Grp** field and click **Edit**.

   e. Click the **ACD Parameters (A)** tab.

   f. In the **Supervisor Extension** field, type the extension number of the supervisor.

   g. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a supervisor assist number, type a name for the supervisor assist button label. For example, Supervisor.

This label appears on the phone.

If you do not specify a label, the default label that appears on the phone is **Assist**.

6. Click **Commit** to save the changes.

MCT as Emergency for a call center

Components for configuring Malicious Call Trace as Emergency for call center

You must configure the following elements to use the MCT feature as Emergency:
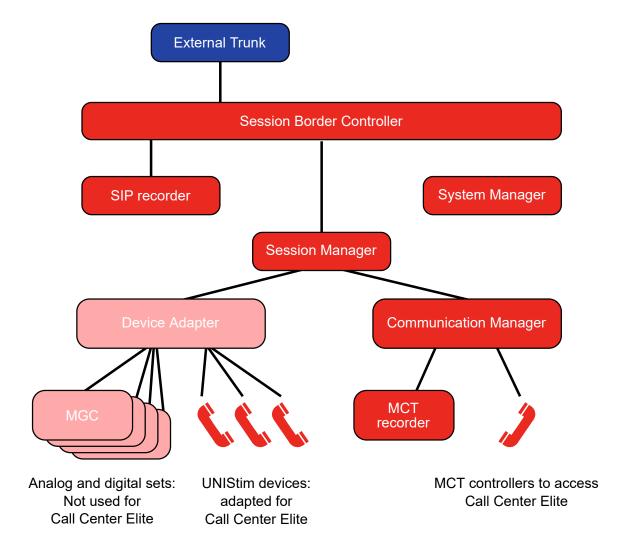
Mandatory elements:

- Configure base MCT on Communication Manager.
- Configure one or more MCT controller stations. Only H.323 or Communication Manager digital stations are supported, unless you are using attendant consoles as controllers.

  SIP endpoints are not supported as controllers.
- Use the CS1K_IPCC station definition to define the applicable Device Adapter agent endpoints and configure the **mct-act** key for these endpoints.
- Define the location where MCT reports can be stored or printed.

Optional elements:

- Other Avaya Aura® SIP devices, if required. These devices can have the **mct-act** key.
- A recording trunk group to record malicious calls.

  In a Call Center Elite environment, the call center records all calls in most cases. Device Adapter does not record calls directly, so the general call recorder is usually configured on the Session Border Controller. Therefore, having a separate call recorder for emergency calls connected to Communication Manager might be considered optional.

External Trunk

Session Border Controller

SIP recorder

System Manager

Session Manager

Device Adapter

Communication Manager

MGC

MCT recorder

Analog and digital sets:
Not used for
Call Center Elite

UNIStim devices:
adapted for
Call Center Elite

MCT controllers to access
Call Center Elite

Configure MCT as Emergency for a call center

General configuration for MCT as Emergency

Ensure that the following components can process calls:

- Session Border Controller
- Session Manager
- Communication Manager

    If you need to process ACD calls, you must configure Avaya Aura® Call Center Elite on
    Communication Manager.

Ensure that these components can process basic and ACD calls.

Configuration on Communication Manager for MCT as Emergency

This section provides a summary of Communication Manager MCT as Emergency programming. For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation* and *Administering Avaya Aura® Communication Manager*.

Pre-work

You must ensure that:

- The optional MCT feature is enabled.
- Classes of restriction for users that may use MCT must have the **Access to MCT** option enabled.

  This is the default setting.
- Feature Access Codes (FAC) for activating and deactivating MCT are configured.

  Avaya Aura® Call Center Elite requires FACs to process calls. However, Avaya SIP phones cannot use FACs for Avaya Aura® Call Center Elite. A Device Adapter agent cannot activate a feature by using the FAC.

Attendant consoles

H.323 and digital (DCP) attendant consoles support the MCT controller functionality.

SIP attendant consoles do not support the MCT controller functionality.

You must ensure that:

- The desired Communication Manager digital (DCP) and H.323 attendant consoles are programmed with MCT activation or controller key or with both of them, depending on the role of each attendant.
- Any SIP attendant consoles are programmed with the MCT activation key if the attendant needs to report an emergency. SIP attendant consoles cannot be MCT controllers.

Stations — controllers

You must specify which extensions can be programmed with the MCT controller key and then program the phones. You can use H.323 or DCP endpoints. SIP endpoints, including Device Adapter digital endpoints, are not supported.

- Enter the extensions of those phones on the Communication Manager "change mct-group-extensions" form.
- Program the DCP or H.323 stations to include the **mct-contr** key.

You must perform both these steps. If you skip any step, the MCT functionality will be unavailable. You can perform these steps in any order.

Stations — non-Device Adapter SIP endpoints used for MCT activation

Program the stations to include the **mct-act** key.

Recording trunks

You must assign a correctly configured recording device to record a malicious call. For more information, see documentation for Communication Manager and Avaya Aura® Call Center Elite.

You can also configure a delay between an ISDN DISCONNECT message received from outside and the subsequent RELEASE message. This prevents too fast call clearing. For example, a user

might have left the call, but the call will remain active for 0, 10, 20, or 30 seconds, allowing to trace the call.

Optionally, you can program the system so that only the controller receives an audio notification that the call is recorded.

Configuring the Emergency button for a Device Adapter endpoint

About this task

Configuring the **Emergency** button for Device Adapter endpoints is similar to configuring the **mct-act** key on UNIStim stations. For this key, you must use the **Emergency** label or its localized equivalent.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the **Emergency** button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In the **Button Feature** field corresponding to the button number that you want to configure as a login button, click **mct-act**.

   b. In the **Button Label** field corresponding to the button number that you want to configure as the Emergency button, type **Emergency**.

      This label appears on the endpoint.

6. Click **Commit**.

Configuring Add/Remove skill button to manage skill set of an agent

Procedure

1. Log on to System Manager by using administrative credentials.

2. Do the following to enable **Add/Remove Agent Skills?** field for changing the skill set for an agent:

   a. Navigate to **Elements** > **Communication Manager** > **System**.

   b. Click **Class of Restriction**.

   c. On the Class of Restriction (COR) page, click the COR number that you want to modify, and then click **Edit**.

   d. Navigate to the page that contains the **Add/Remove Agent Skills?** and set it to **y(es)**.

   e. Click **Enter** to save the changes.

3. Navigate to **Elements** > **Communication Manager** > **Endpoints**.

4. Click **Manage Endpoints**.

5. On the Endpoints page, select the CC endpoint for which you want to configure the **Add/Remove** button, and then click **Edit**.

6. Do the following to configure the **add-rem-sk** button:

   a. On the Edit Endpoint page, click the **Button Assignment** tab.

   b. In the **Button Feature** field corresponding to the button number that you want to configure for changing the agent's skill set, click **add-rem-sk**.

   c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure for adding or removing skill set of an agent, type a name for the skill set button. For example, add_rem_ss.

      This label appears on the phone.

      If you do not specify a label, the default label that appears on the phone is **Chng Skill**.

   d. Click **Commit** to save the changes.

Configuring the Service Observe feature for a CC phone

About this task

The Service Observe feature allows a supervisor to observe an incoming call. The incoming call can be an ACD call, a DAC call or a call to the station's extension.

The available service observing modes are:

  • Listen mode: Listen mode allows a supervisor to only listen to the conversation between the caller and the agent. A supervisor cannot talk in this mode.

    When the administrator programs the **sip-sobsrv** button and enables it for the supervisor, then listen mode is the default service observing mode.

  • Talk mode: Talk mode allows a supervisor to listen and talk to the caller and the agent. A supervisor can use this mode to assist an agent.

  • Coach mode: Coach mode allows a supervisor to talk to the agent without the caller hearing the conversation between the agent and the supervisor.

Procedure

1. Log on to System Manager by using administrative credentials.

2. Do the following to enable the service observing related parameters in the assigned **Class of Restriction**:

   a. Navigate to **Elements** > **Communication Manager** > **System**.

   b. Click **Class of Restriction**.

   c. On the Class of Restriction (COR) page, click the COR number that you want to modify, and then click **Edit**.

   d. Navigate to the page that contains the **Can Be Service Observed?** and **Can Be A Service Observer?** COR parameters, and set these parameters to **y(es)**.

   e. Click **Enter** to save the changes.

3. Navigate to **Elements** > **Communication Manager** > **Endpoints**.

4. Click **Manage Endpoints**.

5. On the Endpoints page, select the CC endpoint for which you want to configure the service observing, and then click **Edit**.

6. Do the following to configure the **sip-sobsrv** button and service observing mode for the endpoint:

   a. On the Edit Endpoint page, click the **Button Assignment** tab.

   b. In the **Button Feature** field corresponding to the button number that you want to configure for the service observing feature, click **sip-sobsrv**.

   c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure for service observing feature, type a name for the service observation button. For example, ser_obs.

      This label appears on the endpoint.

      If you do not specify a label, the default label that appears on the endpoint is **Svc Obsrv**.

   d. In the corresponding **Listen-only?** and **Coach?** field, do one of the following to configure the service observing mode for a supervisor:

      • Listen mode without coaching: Set **Listen-only?** as **y** and **Coach?** as **n** to program the listen mode as the only mode for the supervisor.

      • Listen and Talk mode without coaching: Set both the fields **Listen-only?** and **Coach?** as **n** to allow a supervisor to toggle between the listen mode and listen and talk mode.

      • Listen mode with coaching: Set both the fields **Listen-only?** and **Coach?** as **y** to allow a supervisor to toggle between the listen mode and coach mode.

      • Listen and Talk mode with coaching: Set **Listen-only?** as **n** and **Coach?** as **y** to allow a supervisor to change from one mode to another mode. The available modes for listen and talk mode with coaching are listen mode, listen and talk mode and coach mode.

e. Click **Commit** to save the changes.

Configuring DAC calling on the supervisor's phone

About this task

When a supervisor calls an agent, the call is a Direct Agent Call (DAC). A supervisor can call an agent directly by pressing the feature key pre-configured with the agent ID or by dialing the agent ID.

Before you begin

Ensure that Supervisor phone has an idle call appearance to call an agent.

Procedure

1. Log on to System Manager by using administrative credentials.

2. Do the following to enable direct agent calling functionality on the Supervisor's phone:

   a. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **System**.

   b. Click **Class of Restriction**.

   c. On the Class of Restriction (COR) page, select the COR number corresponding to CC endpoint for which you want to configure the direct agent calling, and then click **Edit**.

   d. In the **Direct Agent Calling?** field, select **y(es)** to enable direct agent calling for an endpoint.

   e. Click **Enter** to save the changes.

3. **(Optional)** Do the following to configure the agent ID on one of the programmable feature keys:

   a. On the Edit Endpoint page, click the **Button Assignment** tab.

   b. In the **Button Feature** field corresponding to the button number that you want to configure for calling an agent directly, click **autodial**.

   c. In the corresponding **DialNumber**, type the agent ID for a Direct Agent Call.

   d. Click **Commit** to save the changes.

Multiple call handling

Multiple call handling (MCH) allows Call Center Elite to present a call center call on an agent's phone while there is another active call on the agent's phone.

You can use MCH to interrupt an active call that has low precedence and present a call that has high precedence on the agent's phone.

For example:

- Call center calls (ACD and DAC) are more important than station extension calls.

- Calls for one skill, such as sales, might be more important than calls for another skill, such as service.

✱ Note:

MCH is applicable for ACD and DAC calls. MCH is not applicable for station extension calls and bridged appearance calls because these calls are not routed by Call Center Elite.

Multiple call handling options

Option	Description
none	MCH is not allowed on the phone. If there is an active call on a call appearance of the agent's phone, Call Center Elite does not present another call on the agent's phone.
on-request	While on an active call on the phone, the agent can decide to receive an additional call center call. For example, the agent can view the call queue by using the **q-calls** button and decide to answer a queued call. The agent can voluntarily receive an additional call by doing the following: 1. Place the current call on hold. 2. Press the **Auto-in** or **Manual-in** button. Call Center Elite presents the queued call to the agent. 3. Press the call appearance key next to the flashing extension icon and answer the call center call. After the agent releases the call, the agent can retrieve the previous call that is on hold, or press the **Auto-in** or **Manual-in** button again to receive the next queued call.

Table continues…

Option	Description
one-forced	The **one-forced** option allows Call Center Elite to force a call center call (ACD or DAC) on an agent's phone while the agent is on an active non-call center call (station extension call).
	However, the following is the criteria:
	• There is no active, held, or ringing call center call on the agent's phone.
	• The phone has an idle call appearance.
	The agent can do the following to answer the call center call:
	1. Place the current call on hold.
	The agent can skip this step if auto-hold is configured for the agent's phone.
	2. Press the call appearance key next to the flashing extension icon and answer the call center call.
	After the agent releases the call center call, Call Center Elite might force another call center call to the phone if the call routing algorithm determines the agent to be the next available agent for the call. Otherwise, the agent can retrieve the previous non-call center call that is on hold.
one-per-skill	The **one-per-skill** option is similar to the **one-forced** option. The only difference is that the **one-per-skill** option forces up to one call center call per skill group on the agent's phone.
	For example, if the agent is part of two skill groups, such as sales and services, Call Center Elite can force up to one call from each skill group on the agent's phone.
many-forced	The **many-forced** option allows Call Center Elite to force two or more call center calls including calls from the same skill group on an agent's phone while the agent is on an active call. The active call can be a station extension call, or an active or held ACD or DAC call.
	However, the following is the criteria:
	• There is no ringing ACD or DAC call on the agent's phone.
	• The phone has an idle call appearance.
	The agent can do the following to answer the call center call:
	1. Place the current call on hold.
	The agent can skip this step if auto-hold is configured for the agent's phone.
	2. Press the call appearance key next to the flashing extension icon and answer the call center call.
	After the agent releases the call center call, Call Center Elite might force another call center call to the phone if the call routing algorithm determines the agent to be the next available agent for the call. Otherwise, the agent can retrieve the previous call that is on hold.

Configuring multiple call handling

Procedure

1. Log on to **System Manager** by using administrative credentials.

2. Navigate to **Elements** > **Communication Manager** > **Groups**.

3. Click **Hunt Group**.

4. On the Hunt Group page, in the **Select device(s) from Communication Manager List** area, select the Communication Manager instance.

5. In the **Hunt Group List** area, click the check box corresponding to the hunt group for which you want to configure multiple call handling, and then click **Edit**.

6. On the Edit Hunt Group page, click the **ACD Parameters (A)** tab.

7. In the **Multiple Call Handling** field, click the multiple call handling type for the users within the hunt group.

Auto-Answer

Prerequisites for Auto-Answer

The Auto-Answer functionality on a Device Adapter CC phone requires the following criteria:

- The Auto-Answer feature is enabled on the target phone.
- The Hands-Free functionality is enabled on the target phone.
- The phone type is UNIStim.
- An incoming call is on the primary DN.
- Target phone is in idle status or has a held call before the new call.

The target phone plays a buzz tone and automatically answers the call after a short delay. If the foregoing criteria are not met, the phone only plays a buzz tone and displays the name and number for an incoming call, but the phone does not automatically answer the call.

The Auto-Answer feature also requires configuring the appropriate feature keys. The following table specifies what feature keys you must configure for different scenarios:

Scenario	Configuration
Agent handles calls in Auto-In mode.	• The **Auto-In** key is required.
	• The **Aux Work** key is required.

Table continues…

Scenario	Configuration
Agent handles calls in Timed After Call Work mode.	The **After Call Work** key is recommended, but not required. Avaya Aura® Call Center Elite transitions the agent to After Call Work.
Agent needs to move to the After Call Work mode manually.	The **After Call Work** key is required.

> ✳ **Note:**
>
> The Auto-Answer feature is incompatible with the Interruptible Aux Work transitions to Manual-In or Auto-In mode. The transition does not require any agent's actions, and the phone can become available when the agent is not present at the working place. Therefore, with Interruptible Aux Work, an agent who logs in to the phone with Auto-Answer enabled only receives a notification. If the call is force-answered and the agent is not present at the working place, the call is lost.

Related links

Configuring Auto-in button for an agent on page 214
Configuring Auxiliary Work button for an agent on page 216
Configuring After Call Work button for an agent on page 215

Configuring the Auto-Answer feature

Procedure

1. Configure the Hands-Free Allowed (HFA) mnemonic for the endpoint.

   For more information, see Administering a mnemonic on page 339.

2. Configure the Auto-Answer Allowed (AAA) mnemonic for the endpoint.

   The phone displays the `Auto-Answer Activated` message only if the AAA and HFA mnemonics are applied. If the Call Forward feature is activated on the target phone, the `CFWD` message replaces the `Auto-Answer Activated` message.

Call recording

An agent or a supervisor can record calls on an agent's phone using the call recording feature. A supervisor can record a call on an agent's phone for quality purpose and an agent can record a call for data collection or for some other after call work.

Device Adapter cannot record calls. A recording server is required with Device Adapter endpoint to record calls.

Device Adapter does not support on demand call recording. Avaya Aura® Call Center Elite and SIP devices support on demand call recording with the help of a recording server.

Call recording can be triggered by any of the following:

- An agent: An agent can start recording a call before the call starts or during an ongoing call. An agent can use one of the following configurations for the call recording feature:

  - Bulk recording on Avaya Aura® Call Center Elite.

  - Bulk recording by a device such as Avaya SBCE because Avaya SBCE redirects the SIP calls to Avaya Aura® Call Center Elite.

  - Using agent's desktop application: If the agent's extension is controlled by a CTI controlled application on the agent's desktop, then the agent can use that application to start or stop call recording. Device Adapter and the agent's extension will not have any information about the call recording.

- The server: In this case, the agent does not have a button or CTI controlled application to start or stop call recording. The administrator configures the recording server to record each and every call for a specific agent or to record specific calls of an agent. The call recording is handled by Communication Manager and Avaya Aura® Call Center Elite and not by the agent. Call recording server also supports recording on demand which depends on the client SDK.

For more information about call recording, see Avaya Contact Recorder *Planning, Installation and Administration* document.

Chapter 9: CTI controlled phones in call centers

CTI controlled phone in a call center

You can use Computer Telephony Integration (CTI) applications, such as Avaya Workspaces, along with call center applications, such as Avaya Aura® Call Center Elite or Avaya Aura® Contact Center, to perform call-center specific operations such as retrieving the caller's order details from a database.

You can use the Device Adapter UNIStim, analog, and digital phones as CTI controlled SIP phones in Avaya Aura® Contact Center and Call Center Elite. However, analog phones do not have the required capabilities, such as display, feature buttons, and headset, to be used as CTI controlled phones. Therefore, Avaya recommends that you do not use analog phones as CTI controlled phones.

You can use a media-only phone (CS1K_IP or Device Adapter digital phone) or a CC phone (CS1K_IPCC) as a CTI controlled phone in Call Center Elite.

However, Avaya recommends that you use a media-only phone (CS1K_IP or Device Adapter digital phone) as a CTI controlled phone in Avaya Aura® Contact Center. This is because Device Adapter does not support call center operations on CS1K_IPCC phones in Avaya Aura® Contact Center.

Call center-specific features are not available on a media-only phone.

To use a phone as a CTI controlled phone, you must configure the phone as a CTI controlled phone. For more information, see Configuring an endpoint as a CTI controlled endpoint on page 241.

Device Adapter supports the following CTI application with Call Center Elite:

- Avaya Workspaces

Device Adapter supports the following CTI applications with Avaya Aura® Contact Center:

- Avaya Workspaces
- Avaya Aura®Agent Desktop

The Device Adapter endpoint is controlled by Avaya Aura®Agent Desktop or Avaya Workspaces by using the Application Enablement Services Computer Telephone Integration feature.

For more information about CTI controllers, see "Administering Application Enablement Services" in the *Administering Avaya Aura® Application Enablement Services* guide.

For the latest and most accurate compatibility information, see https://support.avaya.com/CompatibilityMatrix/Index.aspx on the Avaya Support website.

Recommendations for configuring buttons for CTI controlled CC phones

Avaya recommends the following for configuring buttons for CTI controlled CC phones:

For every call center-specific feature on the CTI application, you must configure the corresponding feature button on the CC endpoint.

However, the user experience of using these options may be different on the CTI application and the endpoint.

> ✳ **Note:**
>
> Failure to configure the buttons on the endpoint may result in feature operation failure in the CTI application. For example, if the CTI application supports the Transfer feature and if the Transfer button is not configured in the station definition of the endpoint, a transfer request from the CTI application fails. Avaya Aura® provides a response informing the user that the request failed.

Configuring an endpoint as a CTI controlled endpoint

About this task

You can use a media-only phone (CS1K_IP or Device Adapter digital phone) or a CC phone (CS1K_IPCC) as a CTI controlled phone, regardless of the call center application that you use.

However, if you are using Call Center Elite, Avaya recommends that you use CC phones as CTI controlled phones. In an event when connection to the CTI application is lost, the agent can log in to the CC phone as a Call Center Elite agent and use the phone to perform call center-specific operations.

For more information about Call Center Elite-compatible phone types, see:

- [Supported phone types in an Avaya Aura Call Center Elite environment](#) on page 55
- [Station compatibility for Sequential Registration of CTI controlled endpoints in a call center environment](#) on page 556

Use this procedure to enable an endpoint to be CTI controlled.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the endpoint that you want to configure as a CTI controlled endpoint, and then click **Edit**.

5. On the General Options tab, in the **Type of 3PCC Enabled** field, click **Avaya**.

6. Click **Commit**.

CTI controlled phones in Call Center Elite

Call Center Elite with Avaya Workspaces as the CTI controller

Avaya Aura® Call Center Elite supports using Avaya Workspaces client as the CTI controller application. Avaya Workspaces provides a multimedia call center experience.

A system administrator might configure the phone as a UC phone or a CC phone. An agent can use these phones as CTI controlled phones with Avaya Workspaces only if the system administrator has configured CTI control for these phones.

However, if the agent is using a CC phone, the agent can log in to only one device at a time by using the agent ID. This is because registrations are exclusive in Call Center Elite.

Hence, ensure that you deny MDA for CS1K_IPCC phones by setting **Max. Simultaneous Devices** to 1.

The agent can use the phone to perform UC or CC operations depending on the following:

- If the agent is using a UC phone along with Avaya Workspaces, then the agent can use the phone to perform only UC operations irrespective of the following:

  - Connection to Avaya Workspaces is proper or lost.

  - The agent is logged in or logged out of Avaya Workspaces as the Call Center Elite agent.

- If the agent is using a call center-capable (CC) phone along with Avaya Workspaces, and:

  - If connection to Avaya Workspaces is proper and if the agent is logged in to Avaya Workspaces as Call Center Elite agent, then the agent can use the phone to perform UC operations. Although, the phone might display some call center features, such as the **q-calls** key to view the call queue, Avaya recommends using Avaya Workspaces to perform the call-related and call center-related operations.

  - If connection to Avaya Workspaces is lost or if the agent is logged out of Avaya Workspaces as a Call Center Elite agent, then the agent can log in to the phone as a Call Center Elite agent. The call center features that are configured for the phone are now available on the phone. The agent can now use the phone to perform the call center operations.

> ✱ **Note:**
>
> - If the phone is CTI controlled by Avaya Workspaces, then irrespective of whether the phone is a UC or CC phone, Avaya recommends that you use Avaya Workspaces to perform the call-related and call center-related operations. This is because Device Adapter does not support shared control between Avaya Workspaces and the phone.

- Avaya recommends that you use a phone that is configured as a CC phone with Avaya Workspaces CTI controller for Call Center Elite. In an event when connection to Avaya Workspaces is lost, you can use the phone to perform call center-specific operations.

  For example, if connection to Avaya Workspaces is lost, and if the phone is configured as a CC phone, the agent can log in to the phone as a Call Center Elite agent. The phone takes over the control from Avaya Workspaces and operates as a CC phone. Call center-specific features now become available on the phone. The agent can then use the phone to perform call center-specific operations.

Supported operations and limitations on a UC phone with Avaya Workspaces as the CTI controller

If you are using a UC phone along with Avaya Workspaces, then you can use the phone to perform only UC phone operations irrespective of whether connection to Avaya Workspaces is proper or lost.

😊 **Note:**

Call Center Elite can acquire and CTI control a UC phone only if the UC phone is registered to Session Manager.

Supported operations on Avaya Workspaces

If you are logged in to Avaya Workspaces as a Call Center Elite agent, you can perform the following operations by using Avaya Workspaces:

- Agent login and logout.

- Change work mode to Auto-In or Manual-In.

- Receive, answer, modify (for example, transfer and conference), and end ACD calls, DAC calls, and calls to the station extension.

- Place outgoing calls either by using the agent ID or the station extension.

- The supervisor can perform Supervisor Assist and other supervisory functions by using Avaya Workspaces.

Supported operations on the UC phone irrespective of the connection to Avaya Workspaces

Depending on the display capabilities of the UC phone, you can use the UC phone to:

- View the progress of the call center calls:

  - View the received call center calls on the call appearance buttons (flashing lamp and icon), in addition to the caller identity information.

  - View the call center calls that were answered on the call appearance buttons (lit lamp and icon), in addition to the caller identity information.

  - View call modification operations, such as transfer and conference, and other related information for the call center calls.

  - View whether the station is idle after you release the call center call.

- Receive, modify, and place station extension calls.

Limitations

- The UC phone does not support call center-operations such as, agent login, logout, and set work modes.

- Whether a UC operation can be performed on the phone depends on the provisioning on Communication Manager. If Communication Manager does not allow an operation, the operation is blocked.

- Call center functions that cannot be carried out by Avaya Workspaces are not supported.

- If your phone is CTI controlled by Avaya Workspaces, Avaya recommends that you use Avaya Workspaces even to perform call-related UC operations. This is because Device Adapter does not support shared control between Avaya Workspaces and the phone.

- If you are using a media-only (UC) phone for multi-device access (MDA), the CTI controller controls only the most recently registered media-only (UC) phone.

Supported operations and limitations on a CC phone when connection to Avaya Workspaces is proper

Call Center Elite can acquire and CTI control a CC phone only if the CC phone is registered to Session Manager.

Supported operations on Avaya Workspaces

If you are logged in to Avaya Workspaces as a Call Center Elite agent, you can perform the following operations by using Avaya Workspaces:

- Agent login and logout.

- Change work mode to Auto-In or Manual-In.

- Receive, answer, modify (for example, transfer and conference), and end incoming ACD calls, DAC calls, and calls to the station extension.

- Place outgoing calls either by using the agent ID or the station extension.

- The supervisor can perform Supervisor Assist and other supervisory functions by using Avaya Workspaces.

Supported operations on the CC phone when connection to Avaya Workspaces is proper

Depending on the display capabilities of the CC phone, you can use the CC phone to:

- View the progress of the call center calls:

  - View the received call center calls on the call appearance buttons (flashing lamp and icon), in addition to the caller identity information.

  - View the call center calls that were answered on the call appearance buttons (lit lamp and icon), in addition to the caller identity information.

  - View call modification operations, such as transfer and conference, and other related information for the call center calls.

  - View whether the station is idle after you release the call center call.

- Receive, modify, and place station extension calls.

Avaya Device Adapter Snap-in Reference

Limitations

- If connection to Avaya Workspaces is proper and if you are logged in to Avaya Workspaces as Call Center Elite agent, the phone might still display some call center features, such as the **q-calls** key to view the call queue. However, Avaya recommends that you use Avaya Workspaces to perform the call-related and call center-related operations. This is because Device Adapter does not support shared control between Avaya Workspaces and the phone.

- Call center functions that cannot be carried out by Avaya Workspaces are not supported.

Supported operations and limitations on a CC phone when connection to Avaya Workspaces is lost

Supported operations on Avaya Workspaces

When connection to Avaya Workspaces is lost, you cannot use Avaya Workspaces to perform call center-specific operations.

Supported operations on the CC phone when connection to Avaya Workspaces is lost

If call center-specific features are configured for the phone, these features are available on the phone only after you log in to the phone as a Call Center Elite agent.

You can perform the following operations by using the phone:

- Agent login and logout.

- Change work mode to Auto-In or Manual-In.

- Receive, answer, modify (for example, transfer and conference), and end incoming ACD calls, DAC calls, and calls to the station extension.

- Place outgoing calls either by using the agent ID or the station extension.

- The supervisor can perform Supervisor Assist and other supervisory functions by using Avaya Workspaces.

Limitations

- Call center functions that are supported by Avaya Workspaces but not by the CC phone are not supported on the phone.

Call Center Elite with CTI monitoring for metadata retrieval

Device Adapter cannot provide metadata directly to Call Center Elite. It sends the information to Communication Manager and Application Enablement Services to allow Call Center Elite to use the metadata for any operations.

CTI controlled phones in Avaya Aura Contact Center

Avaya Aura® Contact Center with Avaya Aura® Agent Desktop as the CTI controller

> **✳ Note:**
>
> - You can use only a UC endpoint (CS1K_IP and Device Adapter digital phone) as a CTI controlled endpoint in Avaya Aura® Contact Center.
>
> - Avaya Aura® Contact Center can acquire and CTI control a UC phone only if the UC phone is registered to Session Manager.

Supported operations on Avaya Aura® Agent Desktop

If you are logged in to Avaya Aura® Agent Desktop as an Avaya Aura® Contact Center agent, you can perform the following operations by using Avaya Aura® Agent Desktop:

- Agent login and logout.

- Change work mode to Auto-In or Manual-In.

- Receive, answer, modify (for example, transfer and conference), and end ACD calls, DAC calls, and calls to the station extension.

- Place outgoing calls either by using the agent ID or the station extension.

- The supervisor can perform Supervisor Assist and other supervisory functions by using Avaya Aura® Agent Desktop.

Supported operations on the UC phone irrespective of whether connection to Avaya Aura® Agent Desktop is proper or lost

Depending on the display capabilities of the UC phone, you can use the UC phone to:

- View the progress of the call center calls:

  - View the received call center calls on the call appearance buttons (flashing lamp and icon), in addition to the caller identity information.

  - View the call center calls that were answered on the call appearance buttons (lit lamp and icon), in addition to the caller identity information.

  - View call modification operations, such as transfer and conference, and other related information for the call center calls.

  - View whether the station is idle after you release the call center call.

- Receive, modify, and place station extension calls.

Limitations

- If connection to Avaya Aura® Agent Desktop is lost, you cannot perform any call center-related operations. Because the phone is a UC phone, you can use the phone to perform only UC operations. Call center operations are not supported on this phone.

- The agent operation depends on the provisioning at Communication Manager. If Communication Manager does not allow an operation, the operation is blocked.

- Call center functions that cannot be carried out by Avaya Aura® Agent Desktop are not supported.

- If your phone is CTI controlled by Avaya Aura® Agent Desktop, Avaya recommends that you use Avaya Aura® Agent Desktop even to perform call-related UC operations. This is because Device Adapter does not support shared control between Avaya Aura® Agent Desktop and the phone.

- If you are using a media-only (UC) phone for multi-device access (MDA), the CTI controller controls only the most recently registered media-only (UC) phone.

Avaya Aura® Contact Center with Avaya Workspaces as the CTI controller

> ✳ **Note:**
>
> - You can use only a UC endpoint (CS1K_IP and Device Adapter digital phone) as a CTI controlled endpoint in Avaya Aura® Contact Center.
>
> - Avaya Aura® Contact Center can acquire and CTI control a UC phone only if the UC phone is registered to Session Manager.

Supported operations on Avaya Workspaces

If you are logged in to Avaya Workspaces as an Avaya Aura® Contact Center agent, you can perform the following operations by using Avaya Workspaces:

- Agent login and logout.

- Change work mode to Auto-In or Manual-In.

- Receive, answer, modify (for example, transfer and conference), and end ACD calls, DAC calls, and calls to the station extension.

- Place outgoing calls either by using the agent ID or the station extension.

- The supervisor can perform Supervisor Assist and other supervisory functions by using Avaya Workspaces.

Supported operations on the UC phone irrespective of whether connection to Avaya Workspaces is proper or lost

Depending on the display capabilities of the UC phone, you can use the UC phone to:

- View the progress of the call center calls:

  - View the received call center calls on the call appearance buttons (flashing lamp and icon), in addition to the caller identity information.

  - View the call center calls that were answered on the call appearance buttons (lit lamp and icon), in addition to the caller identity information.

  - View call modification operations, such as transfer and conference, and other related information for the call center calls.

  - View whether the station is idle after you release the call center call.

- Receive, modify, and place station extension calls.

Limitations

- If connection to Avaya Workspaces is lost, you cannot perform any call center-related operations. Because the phone is a UC phone, you can use the phone to perform only UC operations. Call center operations are not supported on this phone.

- The agent operation depends on the provisioning at Communication Manager. If Communication Manager does not allow an operation, the operation is blocked.

- Call center functions that cannot be carried out by Avaya Workspaces are not supported.

- If your phone is CTI controlled by Avaya Workspaces, Avaya recommends that you use Avaya Workspaces even to perform call-related UC operations. This is because Device Adapter does not support shared control between Avaya Workspaces and the phone.

- If you are using a media-only (UC) phone for multi-device access (MDA), the CTI controller controls only the most recently registered media-only (UC) phone.

Avaya Aura® Contact Center with CTI monitoring for metadata retrieval

Device Adapter cannot provide metadata directly to Avaya Aura® Contact Center. It sends the information to Communication Manager and Application Enablement Services to allow Avaya Aura® Contact Center to use the metadata for any operations.

Chapter 10: Maintenance

Avaya Breeze® platform server maintenance

Avaya Device Adapter Snap-in supports the following maintenance activities through the Avaya Breeze® platform Server Maintenance interface.

- Server shut down and restart
- Server Accept and Deny mode
- Server status

For information and procedures about conducting these activities, see the *Administering Avaya Breeze® platform* guide.

Avaya Breeze® platform cluster maintenance

Avaya Device Adapter Snap-in supports the following maintenance activities through the Avaya Breeze® platform Cluster Maintenance interface.

- Cluster backup and restore
- Cluster Accept and Deny mode
- Cluster status

See *Administering Avaya Breeze® platform* for information and procedures for conducting these activities. This document is available on the Avaya Support web site.

Uninstalling and deleting Avaya Device Adapter Snap-in

Uninstall and delete Avaya Device Adapter Snap-in by using the Avaya Breeze® platform Service Management interface.

For information and procedures about conducting these activities, see the *Administering Avaya Breeze® platform* guide.

Alarm maintenance

Alarm maintenance is performed in the Avaya Aura® System Manager Events interface. For more information about alarm definitions, see [Alarm definitions](#) on page 260.

Viewing the list of Device Adapter maintenance and troubleshooting commands

Procedure

Run the following command at the Avaya Breeze® platform CLI command prompt:

daHelp

Result

A list of Device Adapter-specific maintenance and troubleshooting commands appears in the Avaya Breeze® platform CLI interface.

Related links

[Maintenance commands](#) on page 250
[Troubleshooting commands](#) on page 257

Maintenance commands

This section contains information about the Avaya Breeze® platform commands available for maintaining Device Adapter. All commands in this section require `suser` privileges.

System Manager also provides administration and maintenance of Device Adapter. Refer to [Device Adapter administration in System Manager](#) on page 192 for a list of the available screens.

> **🛈 Important:**
>
> You must not use the **dasrvstart start <app_name | all>** and **dasrvstart stop <app_name | all>** commands in the following conditions:
>
> - For operations related to attribute changes.
> - For operations related to database changes.
>
> You can perform the Device Adapter start and stop operation on the System Manager web interface by navigating to **Elements** > **Avaya Breeze®** > **Service Management** > **Service** and selecting the correct version of Device Adapter. Click **Start** to start an application or **Stop** to stop a running application.

> ⊛ **Note:**
>
> The default user available to run commands is `cust`. The `cust` user has permissions to run maintenance and troubleshooting commands.

Command	Description
`dasrvstart start <app_name	all>`	Starts an individual service or all services.

`dasrvstart stop <app_name	all>`	Stops an individual service or all services.
		
		 🛈 **Important:**
		
		 • The following is the impact on endpoint registration if the `dsa`, `pbx`, `pbxserver`, or `tps` service is stopped on a node:
		
		   - If a load balancer is not configured within the cluster, and if the cluster is a single-node cluster, then stopping any of these services has an impact on endpoint registrations, which results in loss of connection and calls functionality.
		
		   - If the node that has the load balancer configured is running properly, and if any of these services is stopped on any node other than the load balancer node within the cluster, then endpoint registration and re-registration are performed normally.
		
		   - If the cluster is a multi-node cluster, and if any of these services is stopped on the active load balancer node within the cluster, then endpoint registration and re-registration is impacted regardless of the state of other nodes and services within the cluster.
		
		 • Stopping the `csv` service has an impact on the endpoint registration.
		
		 Avaya recommends that you stop and start these services during the maintenance period to minimize endpoint registration and call handling problems.

`dasrvstart status <app_name	all>`	Lists the status of an individual service or all services.
`dsaShow`	Displays statistical information per SDK instance. The **dsaShow** command does not require any parameters. Example: **dsaShow**

Table continues…

Maintenance

Command	Description

`endpointShow <TN | Extension>`	Displays information about the specified endpoint, such as handle, time zone, and Call Forward All Calls destination number configured for the endpoint.
	
	Example:
	
	`endpointShow 112-0-0-1`
	
	`endpointShow 1000003`

`endpointUnlockSCPW <TN | Extension>`	Sends a request to unlock the station control password for the specified TN or extension.
	
	Example:
	
	`endpointUnlockSCPW 3460144`
	
	`endpointUnlockSCPW 112-0-0-1`

Table continues…

Command	Description

`fwUpgrade <TN> <LanguageSet> [<Mode>]`	Where:
	
	• TN must be in the loop-shelf-card-unit format.
	
	• LanguageSet can be set to one of the following:
	
	  - global10: Global 10 Languages (English, French, German, Spanish, Swedish, Italian, Norwegian, Brazilian Portuguese, Finnish, Japanese Katakana)
	
	  - weurope: Western Europe 10 Languages (English, French, German, Spanish, Swedish, Norwegian, Danish, Finnish, Italian, Brazilian Portuguese)
	
	  - eeurope: Eastern Europe 10 Languages (English, French, German, Dutch, Polish, Czech, Hungarian, Russian, Latvian, Turkish)
	
	  - namerica6: North America 6 Languages (English, French, German, Spanish, Brazilian Portuguese, Japanese Katakana)
	
	  - wasia: Spare Group A (English, French, German, Russian, Latvian, Turkish, Ukrainian, Estonian, Lithuanian)
	
	  - spareb: Spare Group B (Not used)
	
	  - Hebrew: Packaged Languages (M3904: English, French, Hebrew, Spanish;
	
	  M3902, M3903 and M3905: English, French, German, Dutch, Polish, Czech, Hungarian, Russian, Latvian, Turkish)
	
	• Mode (optional) can be set to one of the following:
	
	  - normal: This is the default mode.
	
	  - idle: Waits for a busy set to become idle before starting the download.
	
	  - forced: Downloads the set even if it has current firmware or is busy.
	
	Example:
	
	`fwUpgrade 112-0-0-1 global10 idle`
	
	`fwUpgrade 112-0-0-2 hebrew`

Table continues…

Command	Description
`ipeCardDisable <loop-shelf-card>`	Disables IPE card with <loop-shelf-card> TN. All units on this card are disabled and unregistered. Example: `ipeCardDisable 240-1-2`
`ipeCardEnable <loop-shelf-card>`	Enables IPE card with <loop-shelf-card> TN. All units on this card are enabled and try to register. Example: `ipeCardEnable 240-1-2`
`ipeCardGetSerialId <loop-shelf-card>`	Prints the hardware ID, revision, and serial ID of the IPE card with <loop-shelf-card> TN. Example: `ipeCardGetSerialId 240-1-2`

`ipeShow <loop-shelf> or <loop-shelf-card> or <loop-shelf-card-unit>`	Shows the hardware status of the IPE cards or units.
	
	Example:
	
	`ipeShow 240-1`
	
	`ipeShow 240-1-2`
	
	`ipeShow 240-1-2-0`

`ipeUnitDisable <loop-shelf-card-unit>`	Disables the IPE unit with <loop-shelf-card-unit> TN. The unit is unregistered. Example: `ipeUnitDisable 240-1-2-0`
`ipeUnitEnable <loop-shelf-card-unit>`	Enables IPE unit with <loop-shelf-card-unit> TN. Tries to register the unit. Example: `ipeUnitEnable 240-1-2-0`
`ipeUnitGetSerialId <loop-shelf-card-unit>`	Prints the serial ID of the IPE unit with <loop-shelf-card-unit> TN. Example: `ipeUnitGetSerialId 240-1-2-0`
`mgcFailback <loop-shelf>`	Forces an MGC with the given loop and shelf to re-register on its primary cluster. Example: `mgcFailback 112-0`

Table continues…

Command	Description
`mgcReboot <loop-shelf>`	Reboots an MGC with the given loop and shelf. Example: `mgcReboot 112-0`
`mgcShow`	Displays a list and type of media gateway controllers registered on the Avaya Breeze® platform server. The `mgcShow` command does not require any parameters. Example: `mgcShow`

`mgcUpgrade <loop-shelf> <current/legacy> <type>`	Forces MGC upgrade to current or legacy loadware.
	
	Where:
	
	• loop-shelf: Is the loop and shelf of the MGC that you want to upgrade.
	
	• current/legacy: Are optional parameters. The default is current.
	
	  - current: The MGC loadware is upgraded on the MGC load that is injected in the current Device Adapter Snap-In load.
	
	  - legacy: The MGC loadware is upgraded on legacy CS 1000 R7.6 loadware.
	
	• type: Can be one of the following: csp, msp, boot, fpga, app, db1, db2. type is an optional parameter. If you do not specify the type, all loadware is upgraded.
	
	Example:
	
	`mgcUpgrade 4-0 legacy`
	
	`mgcUpgrade 4-0 current csp`

`resetMPMode <digital/analog phone TN>`	Resets the media preservation mode for the given phone along with its linked VGW channel. Example: `resetMPMode 4-0-5-12`

Table continues…

Command	Description

`vgwShow <without parameters> or <loop-shelf> or <loop-shelf-card> or <loop-shelf-card-unit>`	Shows the status of the registered VGW channels. The `vgwShow` command along with the `<loop-shelf-card-unit>` option shows detailed information of one particular channel.
	
	Example:
	
	`vgwShow`
	
	`vgwShow 240-1`
	
	`vgwShow 240-1-11`
	
	`vgwShow 240-1-11-5`

`tnInfo`	Displays a list of TNs of the Device Adapter endpoints that are configured in System Manager.

See *Avaya Communication Server 1000 Software Input Output Reference — Maintenance (NN43001-711)* for a list of maintenance commands. Not all commands listed in this document are supported by Device Adapter.

Related links

Chapter 11: Troubleshooting

Accessing logs

You can access log files from the directory `/var/log/Avaya/services/DeviceAdapter/` in Avaya Breeze® platform. The `DeviceAdapter.log` file contains information specific to Device Adapter. Legacy TPS and PD components continue to use the syslog and write to the `ss_common.log` file. New DSA components use the syslog and write to `dsa.log`.

Troubleshooting commands

The following is a representative list of supported troubleshooting commands. You require `root` or `sroot` privileges to use these commands.

> ✱ **Note:**
>
> Device Adapter does not support the CS 1000 `tcpdump` command for capturing TCP/IP and other packets on the network.
>
> Device Adapter supports only those CS 1000 pcap commands that are mentioned in the following table.

Command	Description
`dasrvstart status all`	Displays the current status of all Device Adapter services.
`tpsShow`	Displays the current Terminal Proxy Server status.
`isetShow`	Displays the currently connected endpoints.
`isetSecShow`	Displays DTLS information for the currently connected endpoints.
`electShow`	Displays the current election status.
`pcapHelp`	Displays the list of available pcap commands.

Table continues…

Command	Description
`pcapStart`	Captures the network packets that are sent and received by the network interfaces of the Avaya Breeze® platform. You can use option **3** of the `pcapConfig` command to specify the network interfaces that you want to monitor. By default, the captured network packets are stored in the `.cap` file that is located at: `/var/log/Avaya/services/DeviceAdapter/pcap` ✱ **Note:** If the `/var` directory is full, Device Adapter automatically deletes the older files from this directory. However, Device Adapter does not delete certain files that are protected from automatic deletion. Hence, to ensure that there is enough disk space in the `/var` directory to store the pcap log files, you might have to manually delete some files from the `/var` directory. You can open and analyze the pcap log file by using Wireshark.
`pcapStop`	Stops capturing the network packets of the network interface.
`pcapStatus`	Displays the current status of packet capturing. For example, started or stopped.
`pcapRestart`	Stops and then starts the packet capturing again. The `pcapRestart` command uses the most recent pcap log file to capture the network packets.
`pcapConfigShow`	Displays the contents of the pcap configuration file. For example, ```[cust@breeze15 ~]$ pcapConfigShow #[PCAP for Linux] [Avaya Breeze] #[Interface] Device=eth Unit=1 #[File System] Folder=/var/log/Avaya/services/DeviceAdapter/pcap FileName=pcap FileNameType=cap FileSize=1000 Files=30 Watermark=100000```

Table continues…

Command	Description

`pcapConfig`	Use the following numbering options with the `pcapConfig` command to configure the pcap settings:
	
	• **0**: Captures the Loopback interface packets.
	
	• **1**: Captures the Management interface packets.
	
	• **2**: Captures the Security Module interface packets.
	
	  This is the default interface for packet capturing.
	
	• **3**: Sets the interface name that needs to be monitored. For example, eth1 for SIP interface.
	
	• **4**: Sets the folder name and path where the pcap log files are to be stored.
	
	  An administrator can create this directory and must set the user to root:easg.
	
	• **5**: Sets the file name for the pcap log file.
	
	• **6**: Sets the file type (extension) for the pcap log file. For example, pcap.
	
	• **7**: Sets the maximum size, in kilobytes, for the pcap log file.
	
	  The maximum supported file size is limited to 100000 KB (100 MB).
	
	  After the file reaches its maximum size, Device Adapter creates a new file to capture the pcap logs.
	
	• **8**: Sets the maximum number of pcap log files that can be created.
	
	  The maximum number of pcap log files supported is limited to 200.
	
	  However, the maximum amount of disk space that Device Adapter allocates for storing the pcap log files is limited to 1 GB. Hence, ensure that the product of the maximum file size and the maximum number of pcap log files that you specify does not exceed 1GB.
	
	  For example:
	
	  - If you specify the maximum file size as 100000 KB (100 MB), the maximum number of pcap log files cannot exceed 10.
	
	  - If you specify the maximum number of pcap log files as 200, the maximum file size per pcap log file cannot exceed 5000 KB (5 MB).
	
	  When the maximum number of files is reached, Device Adapter automatically deletes the oldest pcap file, and creates a new file.
	
	  The pcap log file is stored in the following format:
	
	`pcap_<file number>_<timestamp>.cap`
	
	For example,
	
	`-rw-r-----. 1 cust easg 27272 Aug 23 12:58 pcap_00001_20190823125702.cap`
	
	In the preceding example, the file number is 00001 and the timestamp when the file was closed is 20190823125702.
	
	Where,

Table continues…

Command	Description
	20190823= 23 August 2019
	125702= 12:57:02
	• **9**: Sets the watermark size.
	• **10**: Displays the current pcap configuration.
	• **11**: Loads the pcap configuration file.
	• **12**: Shows the pcap configuration file.
	• **13**: Discards all changes in the pcap configuration file and reverts to the factory default settings.
	• **14**: Saves the changes in the pcap configuration file and quits.
	• **15**: Quits without saving the changes in the pcap configuration file.

For a comprehensive list of supported commands, see *Avaya Communication Server 1000 Software Input Output Reference — Maintenance (NN43001-711)*.

Related links

Alarm definitions

The following table lists the definitions of alarms in the current release.

Table 1: Snap-in alarms

Alarm ID	Description	Error condition
EGC_01	Database query error alarm	• No cluster attribute found • No service attribute list for cluster found • Error getting user data from database • Error getting a parameter from database
EGC_02	Socket error alarm	• Error occurred binding to a port • Error occurred during handling of a client socket <with details>
EGC_03	Thread error alarm	• Error occurred during handling of a client thread <with details>
EGC_04	XML message error alarm	• Error occurred during parsing of an incoming XML message • Error occurred while building an XML response

Table continues…

Alarm ID	Description	Error condition
ITG003	Input \ output file error alarm	• Error occurred while writing a content to a configuration file • Error occurred while reading a content from a configuration file • Error occurred while removing the file-indicator
ITG020	Configuration error alarm	• Invalid format of Terminal Number • Unable to find the user with a provided Terminal Number • Unable to get eth0 IP address • Unable to register for events <with description> • Unexpected cluster attribute value • Error occurred while retrieving HDD parameter • Error occurred while retrieving default gateway from bootp.tap file • Error occurred while retrieving network mask from bootp.tap file • Error occurred while parsing incoming message <with details> • Error occurred while processing a request <with details>

Table 2: DSA alarms

Alarm ID	Description	Error condition
ITG002	Memory allocation error alarm	• Memory allocation failure <with details>
ITG004	Network input \ output error alarm	• Input \ output socket error <with details>

Table continues…

Alarm ID	Description	Error condition
ITG005	Message queue error alarm	• Error occurred while opening PBXLink message queue • Error occurred while opening DSA message queue • Error occurred while opening OMM message queue • Error occurred while sending a message. Message queue is blocked • Error occurred while sending a message. Max number of messages are reached • Error occurred while sending a message. Message queue is closed • Error occurred while reading from a message queue <with details>
ITG012	Module initialization failure alarm	• Unable to start DSA. No Snap-In connection • Unable to start DSA. Endpoint manager initialization failed • EndpointManager initialization failed. Unable to determine eth1 address • EndpointManager initialization failed. Unable to get system data
ITG014	Network interface failure alarm	• Network connectivity lost
ITG020	Configuration error alarm	• Invalid phone type • Not supported set type • Null TN is not allowed • Registration is not allowed in ACF mode • No SIP entity links to a server • Authentication challenge error • Kem type = 24-button doesn't match attached one = <with details> • Endpoint is configured with security-always but a set doesn't support it
ITG030	Media engine error alarm	• Invalid audio capabilities are passed in • Input VoIP session information is not valid for session id= <with details> • Unsupported session type <with details >

Table continues…

Alarm ID	Description	Error condition
ITG031	Certificate error alarm	• Server certificate is not trusted • Trust store initialization failure • Server certificate chain is empty • Some internal errors with details

Table 3: TPS alarms

Alarm ID	Description	Error condition
ITG001	Task spawn failure	• Task spawn failure <with details>
ITG002	Memory allocation error alarm	• Memory <with details>
ITG003	Input \ output file error alarm	• File IO error <with details>
ITG004	Network input \ output error alarm	• Network IO error: <with details>
ITG005	Message queue error alarm	• Message queue error: <with details>
ITG012	Module initialization failure alarm	• Module initialization failure: <with details>
ITG014	Network interface failure alarm	• Ethernet carrier: <with details>
ITG020	Configuration error alarm	• Configuration error: <with details>
ITG036	TPS/DSA communication link alarm	• TPS/DSA communication link: <with details>

Table 4: Troubleshooting actions

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
ITG0001	`Task spawn failure: <taskName>.`	Creation of a Device Adapter task or process failed for some reason.	Critical	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	• Carrier Detection • CSV • PD • TPS • PBX • OMM • TPSElect

Table continues…

Avaya Device Adapter Snap-in Reference
Comments on this document? infodev@avaya.com

ID	Text	Problem Description	Seve rity	Clea red	Critic al to Monit or	SNM P trap	Actions / Proposed Solution	Trigger Component
ITG00 2	`Memory allocati on failure.`	Memory allocation failed. Probable cause is memory leakage.	Maj or	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	• Carrier Detection • CSV • PD • TPS • PBX • OMM • TPSElect • DSA

Table continues…

ID	Text	Problem Description	Seve rity	Clea red	Critic al to Monit or	SNM P trap	Actions / Proposed Solution	Trigger Component
ITG00 3	`File IO error: <fileNam e> <opName> <fd> <errno> <errtext >.`	Some file related input/ output operation (<opName>) for the file (<fileName >) has failed. The operation can be: - file open (<opName> = fopen or <opName> = open) - file read (<opName> = fread) - get file status (<opName> = stat) - ini file open (<opName> = iniFileOpen) - ini section get (<opName> = iniSectionGe t) May be the file does not exist or has incorrect access permissions.	Maj or	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	TPS

Table continues…

Avaya Device Adapter Snap-in Reference
Comments on this document? infodev@avaya.com

ID	Text	Problem Description	Seve rity	Clea red	Critic al to Monit or	SNM P trap	Actions / Proposed Solution	Trigger Component
ITG00 4	`Network IO error: <opName> <fd> <errno> <errtext >.`	Some network related operation (<opName>) has failed. The operation can be: - socket creation (<opName> = socket) - socket bind (<opName> = bind) - set socket options (<opName> = setsocketopt) - socket sending (<opName> = sendto)	Maj or	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	• TPS • TPSElect • DSA

Table continues…

Comments on this document? infodev@avaya.com

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
ITG005	`Message queue error: <opName> <fd> <errno> <errtext>.`	Some message queue related operation (<opName>) has failed. The operation can be: - queue open (<opName> = mq_open) - queue send (<opName> = mq_send) - queue receive (<opName> = mq_receive)	Major	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	• CSV • TPS • TPSElect • OMM • PD

Table continues…

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
ITG012	`Module initialization failure: <moduleName>.`	Failed to initialize and start some programm module. Possible values for moduleName are: - "pbxLinkStartActive - TCP" - failed to start the PBX TCP link to the DSA - "pbxLinkStartPort failed" - PBX link port is not configured - "Problems in ES module" - Echo Server task configuration and initializatin failed	Major	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	• PBX • TPS

Table continues…

ID	Text	Problem Description	Seve rity	Clea red	Critic al to Monit or	SNM P trap	Actions / Proposed Solution	Trigger Component
ITG01 4	`Network interfac e carrier: <ifName> <carrier State>.`	Carrier state for the specified network interface <ifName> changed. Possible values for network interface name (<ifName>) are: - eth0 (Manageme nt interface) - eth1 (Security Module interface) Carrier state can be "LOST" if carrier is lost or "OK" when carrier is restored. The "LOST" state alarms are cleared automaticall y when carrier state becomes "OK". In addition, this alarm can be raised for some internal issues in the Carrier Detection tool. In such case	Criti cal	Yes	Yes	Yes	1. For the "LOST" carrier state, check the ethernet cable connection for the specified interface and connected network equipment. 2. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 3. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 4. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 5. If the alarm continues after replacement hardware has been installed,	Carrier Detection

Table continues…

ID	Text	Problem Description	Seve rity	Clea red	Critic al to Monit or	SNM P trap	Actions / Proposed Solution	Trigger Component
		\<carrierState\> field can be: - "NetLink socket open failed" - failed to open NETLINK socket - "NetLink socket bind failed" - failed to bind NETLINK socket - "EthTool request failed" - failed to check link beating by direct request - "EthTool socket open failed" - failed to open a socket for direct carrier beating requests					contact your next-level technical support for assistance.	

Table continues…

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
ITG0200	Configuration error.	Some configuration error has been detected. Additional data is printed out for the error : - <configFile> - configuration file name, e.g. config.ini; <configVar> - field in the config file that has invalid value; <configValue> - invalid value. Alternatively, the <configFile> <configVar> <configValue> fields can contain just some text information to provide more details about the issue, e.g. "ES2 is assigned the same IP address as default ES1 (TLAN 192.168.96.115). This	Major	Yes (For some cases)	Yes	Yes	1. Potential data configuration error. 2. If the configuration appears to be correct, follow alternate corrective action procedure specified, or contact your next-level technical support.	• TPS • PBX

Table continues…

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
		can cause NAT type detection failure."						
ITG036	`TPS/DSA communication link: <up/down>.`	State of the TPS/DSA PBX link changed. Possible status is "up" or "down". The alarm is cleared automatically when the state becomes "up".	Critical	Yes	Yes	Yes	Intercommunication issue may have caused this alarm. Further analysis is required as described below. 1. Log into device and capture maintenance log (if possible) and send the text to your next-level technical support staff via email. 2. Check statuses for TPS and DSA processes and restart them on the device. Wait for a period of low traffic to minimize risk if possible. For more information, see Maintenance commands on page 250.	PBX

Table continues…

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
EGC_01	`Database query error`	Failed to execute database query. The alarm is cleared automatically when subsequent query operations become successful.	Critical	Yes	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	Snap-in (Java)

Table continues…

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
EGC_02	`Failed to bind socket`	Socket bind network operation failed. Possible reason - network port 15557 is already in use by some other process or service.	Critical	No	Yes	Yes	1. Check that TCP port 15557 is not used by some other process using the command: **# netstat - tnap | grep 15557**. 2. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 3. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 4. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 5. If the alarm continues after replacement hardware has been installed, contact your	Snap-in (Java)

Table continues…

Comments on this document? infodev@avaya.com

ID	Text	Problem Description	Severity	Cleared	Critical to Monitor	SNMP trap	Actions / Proposed Solution	Trigger Component
							next-level technical support for assistance.	
EGC_03	`Unable to shutdown ada snap-in threads`	Failed to shut down some Device Adapter snap-in threads.	Critical	No	Yes	Yes	1. Log into device and capture maintenance Device Adapter log if possible and send the text to your next-level technical support staff through email. 2. Reboot the Avaya Breeze® platform server to restart the software. Wait for a period of low traffic to minimize risk if possible. 3. If the alarm occurs again, install a replacement hardware device and send the failing device to your next-level technical support for further analysis. 4. If the alarm continues after replacement hardware has been installed, contact your next-level technical support for assistance.	Snap-in (Java)

Troubleshooting Device Adapter-related problems

The topics in this section contain information about troubleshooting Device Adapter-related problems.

General troubleshooting

About this task

The first step in troubleshooting any issue with an endpoint or feature not working, or not working correctly, is to consult the log files of the various solution elements. This section contains information on the various log files that are helpful in troubleshooting issues. The Device Adapter core dump is also a useful source of information. Access the Avaya Breeze® platform server through SSH and navigate to `/var/crash/`. The presence of core dump files in this folder indicate application crashes. These files contain debug information for every crash.

The following is the logical progression of information through the Device Adapter solution:

Procedure

1. The endpoint sends data to Device Adapter.

2. The TPS element of Device Adapter sends the data to the DSA element through the PBX link.

3. The DSA element sends the data on to the CSDK element.

4. The CSDK element sends the data on to Avaya Aura® and awaits a response.

5. The response is passed back from Avaya Aura® in the opposite direction.

Result

Device Adapter logs, traces that originate from the endpoint, and traces that originate from Avaya Breeze® platform are useful in following information through the data flow. It can also be helpful to use a CS 1000 solution to validate behaviors.

Set log levels

Avaya recommends configuring the logging levels for the following solution elements:

- Device Adapter
- DSA component
- CSDK

Setting the log level for TPS and PD components of Device Adapter

About this task

The TPS and PD components of Device Adapter use the tps, tpselect, csv, carrdtct, pbx, pbxserver, and pd processes. Any of these processes can generate log messages that are

handled by the rsyslogservice process. All log entries for these processes are routed into the /var/log/Avaya/services/DeviceAdapter/ss_common.log file.

The default logging level of INFO prevents the logging of debug messages. Use the command syslogLevelSet to change the logging level. Logging levels are not reset to default after a service has been restarted. Using the DEBUG level on tps and dsa tasks can cause an outage.

Use the syslogShow command to print current log levels. For example, to show the log levels for the tps process, use the command syslogShow tps.

Use the syslogLevelSet command to adjust log levels for different tasks within one process. For example, use the command syslogLevelSet tps tVTM 7 to set the level of the tVTM task of tpsprocess.

All logging levels map to the following scale:

- -1 = NONE
- 0 = EMERG
- 1 = ALERT
- 2 = CRIT
- 3 = ERROR
- 4 = WARNING
- 5 = NOTICE
- 6 = INFO
- 7= DEBUG

Procedure

Set the logging level to ALL by selecting **Elements** > **Avaya Breeze®** > **Logging** in System Manager and selecting ALL in the Log Level field for the Device Adapter service.

Setting the log level for DSA component

About this task

The DSA component supports logging levels using the commands described for the TPS and PD components. The DSA component supports ERROR, WARNING, INFO, and DEBUG logging levels. The logs are written to the `/var/log/Avaya/services/DeviceAdapter/dsa.log` file located on Avaya Breeze® platform.

Procedure

Run the following command on the Avaya Breeze® platform CLI command prompt to enable DSA level debug logging:

`syslogLevelSet dsa tDSA DEBUG`

Setting the log level for CSDK component

About this task

The CSDK component supports logging levels using the commands described for the TPS and PD components. The CSDK component supports ERROR, WARNING, INFO, and DEBUG logging

levels. The logs are written to the `/var/log/Avaya/services/DeviceAdapter/dsa.log` file located on Avaya Breeze® platform.

Procedure

Run the following command on the Avaya Breeze® platform CLI command prompt to enable CSDK level debug logging:

`syslogLevelSet dsa tCSDK DEBUG`

Setting the filter for DSA log components

About this task

The DSA component displays the log messages only if the DSA component supports the following filter commands:

- dsaLogFilter <String1> <String2>
- dsaLogFilterClear
- dsaLogFilterShow
- To set DSA log filtering, run the following command at the Avaya Breeze® platform CLI command prompt:

    `dsaLogFilter <String1> <String2>`

    For example, dsaLogFilter 112-0-0-1

- To disable DSA log filtering, run the following command at the Avaya Breeze® platform CLI command prompt:

    `dsaLogFilterClear`

- To display active DSA log strings, run the following command at the Avaya Breeze® platform CLI command prompt:

    `dsaLogFilterShow`

Log collection

Use the following information to collect logs from the elements of the Device Adapter solution.

Collecting logs for DSA, TPS, PD, and CSDK components

Procedure

1. Log in to the Avaya Breeze® platform server as the sroot user and using EASG authentication.

2. Use the command zip -r messages.zip /var/log/message*.

3. Use the command zip -r adasnapin.zip /var/log/Avaya/services/DeviceAdapter.

4. Download the messages.zip and adasnapin.zip files from the Avaya Breeze® platform server.

5. Provide the files to the requestor or attach them to the support ticket.

Collecting logs for Core dump

Procedure

1. Log in to the Avaya Breeze® platform server as the sroot user and using EASG authentication.

2. Use the command zip -r crashes.zip /var/crash/ -9.

3. Download the crashes.zip file from the Avaya Breeze® platform server.

4. Provide the file to the requestor or attach them to the support ticket.

Collecting logs for Avaya Breeze® platform

Procedure

1. Log in to the Avaya Breeze® platform server as the sroot user and using EASG authentication.

2. Use the command ce-report.

3. Download the log archive file /var/tmp/cereport-<breeze_server>-<date_time>.tgz from the Avaya Breeze® platform server.

4. Log in to the System Manager server.

5. Use the command collectLogs.

6. Download the /swlibrary/LogsBackup_********.tar.gz from the System Manager server.

7. Provide the files to the requestor or attach them to the support ticket.

Collecting debug logs for Device Adapter and Avaya Breeze® platform

About this task

The following command generates debug logs of Device Adapter and Avaya Breeze® platform for the customers. Customers use these debug logs to provide additional information for a support ticket to Avaya.

Procedure

1. Log in to the Avaya Breeze® platform server as the sroot user and using EASG authentication.

2. Run the following command to generate debug logs for Device Adapter and Avaya Breeze® platform:

```
ada-report
```

Avaya Breeze® platform saves the debug logs in a zip file which contains the following information:

- sar reports

- mgmt log which displays CPU snapshot every 30 seconds

- Core dumps for Terminal Proxy Server (TPS)
- Additional information from `/var/log/Avaya/services/DeviceAdapter` file

3. Download the `/var/tmp/adareport-<breeze_server>-<date_time>.tgz` log archive file from Avaya Breeze® platform server.

The traceSM utility

The traceSM utility is an interactive perl script on Session Manager that allows an administrator to capture, view, and save call processing activity. While not as powerful or versatile as the Wireshark utility, traceSM is essential when working with Avaya SIP. It allows you to view SIP messages even if they have been encrypted with TLS; which cannot be done with Wireshark. The traceSM utility can also display Avaya-specific data such as Personal Profile Manager (PPM) messages and Session Manager call flows.

To run traceSM you must Telnet into the active Session Manager. Only one traceSM instance can be running on a Session Manager at any given time by default. To use multiple instances, it must be run with the -m option. Avaya advises against running multiple instance of traceSM in a production environment as it may cause performance problems.

traceSM should be accessible through the default path. It is located in /opt/Avaya/contrib/bin.

The traceSM utility is a real-time capture tool. You cannot start traceSM to see SIP packets that were sent prior to launching the tool. The capture begins when the application starts and you instruct the application to start capturing logs.

The utility capture buffer is limited to 10,000 packets. Packet collection stops after the buffer is filled. Clear the buffer using the provided commands to continue with capture.

UNIStim trace analysis

A plug-in is available to add the UNIStim protocol to trace analysis performed by Wireshark. The Wireshark analysis tool is available at https://www.wireshark.org/download/win64/all-versions/. The UNIStim plug-in is available at https://kb.avaya.com/kb/index?page=content&id=SOLN264179&actp=SEARCH&actp=search&viewlocale=en_US&searchid=1448611447501 in the "Restricted Solutions Elements" section. You must have an Avaya account to access the plug-in.

Firmware upgrade issues

Condition

TFTP is not supported by TPS for firmware upgrades. UFTP can be used instead.

If it is required to adjust UMS policies for some reason, this should be done on all servers one by one.

The following issue may be encountered when attempting to upgrade i2007 endpoints:

An i2007 endpoint with a legacy 3.x firmware reboots after registering on a CS 1000 system. The endpoint displays a message about a firmware upgrade to a newer firmware provided by a signaling server and reboots without an actual upgrade. This continues until the UMS policy is adjusted to prevent further upgrades. Attempts to upgrade the endpoint over TFTP fails as well.

Cause

A two-step upgrade may be required for upgrading from legacy 3.x releases to 5.x. This is applicable to the i2007 because of changes in the memory structures. An intermediate 3.2+ firmware must be used for this upgrade.

Solution

1. Install C6R firmware for the i2007 on the appropriate signaling server.

2. Upgrade the endpoint C6R. Install C96 or newer firmware the i2007.

3. Upgrade the i2007 to the latest firmware.

    • C6R firmware — ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/www142.nortelnetworks.com/software/i/ipphones/2007/0621C6R.zip

    • C96 firmware — ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/11001200/02282017/0621C96.bin

    • Readme for C96 firmwares — https://downloads.avaya.com/css/P8/documents/101036621

Endpoint registration issues

Procedure

Verify the following items to diagnose issues with endpoint registration:

• Node ID configured.

• System ID in the endpoint and Cluster correspond.

• TN and System ID are not duplicated.

• System Manager, Session Manager, and Communication Manager configurations are valid.

• Trace information on all components.

• Ensure all required ports are available.

System ID configuration issues

About this task

The endpoint System ID must correspond with the Cluster System ID. The following System Manager areas should be checked if an error in the System ID is suspected. The System ID must be consistent across all three of these areas. If they are not, return to the incorrect areas and update the System ID.

Procedure

1. Cluster:

   a. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes** > **Service Clusters** from the menu. Click the Cluster in question and then the Device Adapter Service. Note the System ID attribute.

   b. Click **Elements** > **Avaya Breeze®** > **Service Management** > **Services** from the menu. Click the Device Adapter snap-in. Note the System ID attribute.

2. Endpoint:

   Click **Elements** > **Avaya Breeze®** > **Communication Manager** > **Endpoints** > **Manage Endpoints** from the menu. Click an endpoint. Note the System ID attribute on the General Options tab.

Next steps

You must restart the snap-in service and register the endpoint again for changes to take effect.

System infrastructure (Linuxbase) issues

- Snap-in installation

  Some components of the snap-in are deployed as binary executables with required auxiliary files. Some additional settings in the Linux base OS are also required to make the applications work properly. These tasks are performed during snap-in installation by the `setup.sh` script. Logs from the script are output to `/var/log/messages`. They can be filtered using the `DA setup.sh` pattern.

  If snap-in installation fails, the `/var/log/Avaya/sm/deploy.log` file should be checked. Logs in the file can point to the error.

- Network ports

  The following UDP ports must be open and available for endpoint registration:

  - 4100, 5100, 8300 if DTLS is not used

  - 4101, 5101, 8301 if DTLS is used

  The following additional ports must also be open and available for endpoint registration:

  - TCP - 15000,15060

  - UDP - 5105, 10000, 16540, 16550

Personal Directory issues

Procedure

1. Do the following to verify the PD configuration:

   a. System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

   b. Click on the **Service Clusters** tab.

   c. Select the applicable **Cluster** and Device Adapter service.

   d. On the Attributes Configuration page, navigate to the **Contacts** group.

   e. To enable Personal Directory, select the **Override Default** field and set the **Effective Value** field as **Yes**.

2. Increase the logging level for tDSA, tCSDK, tWAP and tSET to DEBUG by using the following commands:

   syslogLevelSet dsa tDSA DEBUG

   syslogLevelSet dsa tCSDK DEBUG

   syslogLevelSet tps tWAP DEBUG

   syslogLevelSet tps tSET DEBUG

Next steps

The following issues are possible during the PD migration process:

- An error while importing the `pd.xml` file to Avaya Breeze® platform.
- Space before the very first <xml...> tag on the top of file. Delete the space and save the file.

ProVision issues

Condition

The following issues may be encountered while using ProVision:

- Data rows are not transferred to or from the server or any errors during transfer.
- Data is migrated incorrectly during Nortel Migration Tool conversion.

Solution

1. ProVision has the following screens for tracking the transfer process:

   - **View** > **Event Log Viewer**
   - **View** > **Communication Monitor**
   - **View** > **Transaction Viewer**

2. The trace level for the Event Log can be set to DEBUG by editing the ProVision registry settings. Open the Registry Editor as administrator and locate the `HKEY_CURRENT_USER`

`\Software\Avaya\ProVision\ASMSpecial` registry key. Set the `ASMSpecial` value to `dword:00000001`. Save and close the Registry Editor. Run ProVision and open the Event Log Viewer. There should now be an increased level of logging.

The Nortel Migration Tool provides an Excel format of Logs and Reports during the migration process. The Log and Report buttons on the progress window provides this information.

Quality of Service (QoS) issues

About this task

QoS implementation allows for the propagation of RTCP packets received from endpoints to Avaya VoIP Monitoring Manager (VMM). If there are no RTCP statistics available, ensure that QoS monitoring is enabled on System Manager.

> **Important:**
>
> Troubleshooting QoS related problems may require stopping and starting the `tps` service, which might have an impact on endpoint registration and call handling. For more information, see Maintenance commands on page 250.
>
> Avaya recommends that you stop and start the `tps` service during the maintenance period to minimize endpoint registration and call handling problems.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration**.
2. Click **Attributes**.
3. Navigate to the **IP Telephony Node / Quality of Service (QoS)** area and do the following:
   a. In the **VoIP Monitoring Enabled** field, in **Effective Value**, click **Yes**.
   b. Ensure that the **VoIP Monitoring Reporting Interval** field is not set to zero.
   c. In the **VoIP Monitoring Manager IP address** field, in **Effective Value**, type the VMM IP address.
   d. In the **VoIP Monitoring Manager Port** field, in **Effective Value**, type the VMM port number.

      The default port is 5005.
4. Log in to Avaya Breeze® platform server by using SSH and the appropriate credentials.
5. Open the `/opt/Avaya/da/shared/config/mamcfg.xml` file.

   Ensure the `QoS` section contains the same `SAMPLEPERIOD` value as configured for reporting interval on System Manager.
6. If there are problems in the `mamcfg.xml` file, stop and start the `tps` service by using the following commands:

   dasrvstart stop tps

```
dasrvstart start tps
```

7. Verify that the `omm` process is running by using the **`dasrvstart status omm`** command.

8. Set the log level to DEBUG for tVTM by using the **`syslogLevelSet tps tVTM DEBUG`** command to verify that RTCP statistics are sent from the TPS side.

9. Verify that the following log is printed periodically:

   ```
   RTCP statistics is generated for set <IP address of the phone>
   ```

Security issues

About this task

ℹ️ **Important:**

After you modify the DTLS settings of a cluster, you must stop and start the tps and csv services. Stopping and starting these services results in a brief outage interval because the nodes change operation and the UNIStim sets are re-registered. This might have an impact on endpoint registration and call handling. For more information, see

Avaya recommends that you stop and start these services during the maintenance period to minimize endpoint registration and call handling problems.

Procedure

1. SIP TLS:

   a. Confirm there is a separate SIP Entity of type Endpoint Concentrator. Verify in System Manager by selecting **Elements** > **Routing** > **SIP Entities** from the menu and viewing the information.

   b. Confirm there is a TLS link configured between the SIP entity and Session Manager. The Connection Policy should be endpt conc.

   c. Confirm the Avaya Breeze® platform server has a valid SIP identity certificate. Verify in System Manager by selecting **Services** > **Inventory** > **Manage Elements** from the menu and selecting the element. Select **More Actions** > **Manage Identity Certificates**.

2. DTLS:

   a. Confirm DTLS settings have been propagated to TPS. Check `/opt/Avaya/da/shared/config/config.ini`.

   ```
   [UNIStimDTLS]
   TPS_DTLS=1                                          // 0 – Off, 1 – Best
   effort, 2 - Always
   DTLSClientAuthentication=0
   ```

> ✱ **Note:**
>
> The TPS and CSV applications must be stopped and started again after changing the attribute.

b. Confirm DTLS ports are open for CSV and TPS.

```
netstat -unap | grep -E "4101|5101|8301"
udp 0 0 192.168.96.115:8301 0.0.0.0:* 9190/tps
udp 0 0 192.168.96.115:4101 0.0.0.0:* 15320/csv
udp 0 0 192.168.96.115:5101 0.0.0.0:* 9190/tps
```

c. If you have made keystore and truststore certificate changes after snap-in installation, the following commands should be executed from the Avaya Breeze® platform CLI as root.

```
cd /opt/Avaya/da/
./avaya_securitymodule_pki_toolinitda dausersm_pki_descriptor_da.txt
```

d. If no other issues are found, reset the endpoint to factory defaults to delete the previous CA certificate on it. Reinstall the current root CA certificate again.

e. The CA certificate for an i2050 software endpoint must be installed in **Trusted Root Certification Authorities** > **Local Machine**. The Certificate Manager attempts to install it in **Trusted Root Certification Authorities** > **Registry** by default.

SNMP issues

For debug purposes, SNMP alarm requests sent by the TPS applications are logged in the `/var/log/Avaya/services/DeviceAdapter/DeviceAdapter.log` file. The log level should be FINE or above. The following is an example of such an entry. The type of request is RaiseAlarmRequest.

```
42018-03-07 09:46:13,962 [pool-21-thread-11] DeviceAdapterFINE -
DeviceAdapter-99.0.0.1.9999 - Received 236 bytes :

4<?xml version="1.0" encoding="UTF-8" standalone="yes"?><RaiseAlarmRequestid="1"
needResponse="false"><AlarmIDITG050</AlarmID<Clear>false</Clear><DisplayTextThe
application Server is not configured</DisplayText</RaiseAlarmRequest>
```

Configuring Message Waiting

About this task

Use this procedure to configure the Message Waiting functionality of Avaya Aura® Messaging (AAM). This configuration may be necessary if you are experiencing issues with connecting to AAM.

Procedure

1. Log on to System Manager by using the appropriate credentials.

2. Navigate to **Elements** > **Routing**.

3. Click **SIP Entities**.

4. Add a new SIP Entity with the following information:

   - **Name** — The name of the AAM server.

   - **IP Address** — The IP address of the AAM server.

   - **Location** — Select the appropriate location from the list. This was previously configured on the **Routing** > **Locations** screen.

   - **Time Zone** — Select the appropriate time zone.

   - Configure all other attributes as appropriate for your solution configuration.

5. Add a new Entity Link with the following information:

   - **SIP Entity 1** — Previously configured Session Manager link.

   - **SIP Entity 2** — Messaging link configured in the previous step.

      - **Port** — 5060 — If TLS is not enabled.

      - **Port** — 5061 — If TLS is enabled.

   - **Protocol** — TCP — If TLS is not enabled.

   - **Protocol** — TLS — If TLS is enabled.

   - **Connection Policy** — Trusted

6. Click **Commit**.

7. Select **Routing** > **Routing Policy** from the menu.

8. Add a new Routing Policy with the following information:

   - Name — Enter an appropriate descriptive name.

   - Click **Select** in the **SIP Entity as Destination** section. Select the SIP Entity you created in the previous step.

9. Click **Commit**.

10. Select **Routing** > **Dial Patterns** from the menu.

11. Add a new Dial Pattern for the Messaging Access Number with the following information:

    ⊛ **Note:**

       The Messaging Access Number was previously configured on Avaya Aura® Messaging in **Administration** > **Messaging** > **Sites**.

    - **Pattern** — Dialed number or prefix.

    - **Min** — The minimum length of dialed number.

    - **Max** — The maximum length of dialed number.

    - **SIP Domain** — The solution domain.

12. Click **Add** in the **Originating Locations and Routing Policies** section.

13. Select the appropriate Location and Routing Policy from the list.

14. Leave the remaining fields with default values.

15. Click Commit.

16. Repeat steps 9 to 14 for the Auto Attendant Number.

   ⭐ **Note:**

   The Auto Attendant Number was previously configured on Avaya Aura® Messaging in **Administration** > **Messaging** > **Sites**.

17. Select **Inventory** > **Manage Elements** from the menu.

18. Add a new Managed Element with the following information:

   • **Name** — A descriptive name for the element.

   • **Type** — Messaging

   • **Node** — The IP address of the AAM server.

19. Select the **Attributes** tab.

20. Enter the following attributes:

   • **Login** — The System Manager administrative user.

   • **Password** / **Confirm Password** — The System Manager administrative password.

   • **Messaging Type** — AURAMESSAGING

   • **Version** — 6.3

   • **Port** — 636

21. Click **Commit**.

22. Log in to the SAT interface using the appropriate credentials.

23. Enter the following commands:

```
> save translation
> reset system 4
> add media gateway
```

24. Use the command change **private-numbering 0** to change the private number configuration.

25. Add the Ext Code 1100000 to Ext Len 7.

   The entry should appear like the example below.

Ext Len	Ext Code	Trk Grp	Private Prefix	Total Len
7	1100000	2		7

Comments on this document? infodev@avaya.com

> **❋ Note:**
>
> The trunk group should already be configured. Use the command `list trunk-group` to view trunk groups.

26. Use the command `change route-pattern 1` to change the route pattern.

27. Enter the following information:

    - Grp No: 2

    - FRL: 0

    - 1: DgtsFormat Subaddress: unk-unk

28. Use the command `change aar analisys 0` to change Automatic Alternate Routing (AAR).

29. Add Messaging Access Number 1100000.

30. Use the command `add hunt-group 1` to add a hunt group.

31. Enter the following information:

    - Group Name: <A descriptive group name.>

    - Group Extension: 1100000

    - ISDN/SIP Caller Display: mbr-name

    - Coverage Path: 1

      > **❋ Note:**
      >
      > This is configured below. Use the command `list coverage path` command to list all configured coverage paths.

32. Go to the second page of Hunt Group configuration.

33. Enter the following information:

    - Message Center: sip-adjunct

    - Voice Mail Number: 1100000

    - Voice Mail Handle: 1100000

    - Routing Digits: 8

34. Use the command `change feature-access-code` to change the feature access code.

35. Enter 8 in the Auto Alternate Routing (AAR) Access Code field.

36. Use the command `add coverage path 1` to configure the coverage path.

37. Enter the following information:

    - Point1: Use h1 to indicate hunt-group 1 created above.

    - Rng: 2

38. Perform the following configuration for each endpoint.

    a. Use the command **add station <extension_number>**.

    b. Enter the following information:

       • Type: <station type as applicable: CS1k-IP/CS1k-39xx/CS1k-1col/CS1k-2col/CS1k-ana>

       • Coverage path: 1

       • Page 6 SIP Trunk: aar

39. Use the command **save translation** to save all changes.

40. Return to System Manager.

41. Add the same User in AAM User Management.

42. Select **Inventory** > **Synchronization** > **Communication System** from the menu.

43. Select **Incremental Sync data for selected devices**.

44. Click **Now**.

   > ❗ **Important:**
   >
   > Before adding the mailbox on System Manager it should have already been created on AAM and synchronized.

45. Select **User Management** > **Manage Users** from the menu.

46. Update the created Identity screen with the following information:

    • **Login** — User login ID.

      > ✴ **Note:**
      >
      > Check that Session Manager and CM Endpoint Profiles are filled in.

    • Select **Messaging Profile**.

    • **System** — The messaging system.

    • Select **Use Existing Subscriber on System**.

    • **Mailbox Number** — Enter or select the mailbox number.

    • **Template** — Use the default template name associated with the Avaya Aura® infrastructure.

    • **Password** — User password.

47. Click **Commit**.

FIPS 140-2 compliance problems

Procedure

Verify if the 11xx and 12xx series IP phones can register to TPS. If the phones cannot register to TPS, do any of the following:

- Examine the `dsa.log` file for server connection problems.

- Ensure that the Session Manager identity certificates key length is at least 2048 bit.

- If mutual DTLS authentication is enabled, ensure that the Client Identity Certificate that is installed on the phone has a key length of at least 2048 bit.

    For more information, see Security configuration on page 197.

- Examine the following log files for any error messages related to FIPS compliance:

    - `/var/log/Avaya/services/DeviceAdapter/dsa.log`

    - `/var/log/Avaya/services/DeviceAdapter/ss_common.log`

- Report the problem to Avaya Support.

Presence notification problems

Procedure

Run the traceSM utility to trace SIP PUBLISH messages for Presence notification that are generated by Device Adapter.

Ring Again problems

Procedure

Run the traceSM utility to collect and examine the `dsa tDSA tCSDK` debug logs.

Malicious call trace problems

Procedure

Do the following:

a. Run the traceSM utility to collect the `tDSA tCSDK` debug logs.

b. Examine the `/var/log/Avaya/services/DeviceAdapter/dsa.log` file.

Busy Indicator problems

Procedure

Do the following:

    a. Run the traceSM utility to collect the `tDSA tCSDK` debug logs.

    b. Examine the `/var/log/Avaya/services/DeviceAdapter/dsa.log` file.

Hotline one-way problems

Procedure

Run the traceSM utility to collect and examine the `dsa tDSA` debug logs.

Forward button for call forwarding all calls does not appear on the UNIStim or M3900 series digital desk phone

Condition

The **Forward** button that is used to Call Forward All Calls (CFW) does not appear on the UNIStim or M3900 series digital desk phone even after an administrator has configured button number 19 as the **call-fwd** button for the user's endpoint in System Manager.

In System Manager, button number 19 is reserved for configuring a **call-fwd** button for the user's endpoint. The default label that appears on the endpoint for this button is **Forward**. A user can use this **Forward** button to CFW all inbound calls on the user's extension to another extension.

Cause

An administrator has specified an extension number in the **Extension** field corresponding to the **call-fwd** button on button number 19.

Ensure that the **Extension** field corresponding to this **call-fwd** button is blank. If you specify an extension number in this **Extension** field, the **Forward** button does not appear on the endpoint.

Solution

1. Log on to System Manager by using administrative credentials.
2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.
3. Click **Manage Endpoints**.
4. On the Endpoints page, select the endpoint, and then click **Edit**.
5. On the Edit Endpoint page, click the **Button Assignment** tab.
6. Depending on the endpoint type, click the **Feature Buttons** or **Button Modules pages** tab.

7. In button number 19, delete the extension number in the **Extension** field corresponding to **call-fwd** button.

8. Click **Commit**.

Related links

[Configuring an endpoint for Busy Indicator and call forwarding on behalf of another user station](#) on page 435

Multi-device access and Sequential Registration problems

About this task

Multi-device access (MDA) allows a minimum of 2 up to a maximum of 10 concurrent device registrations.

Because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint. If a user wants to share the same user identity for two or more UNIStim endpoints, you must use Sequential Registration to ensure that only one UNIStim endpoint is registered at one time.

For Sequential Registration, set the maximum number of concurrently registered devices to 1.

Procedure

1. If call failure occurs when two or more Device Adapter UNIStim endpoints are configured, do the following:

   a. Ensure that **Max. Simultaneous Devices** is set to 1.

   Any environment where multiple Device Adapter UNIStim endpoints try to register must be configured for Sequential Registration. Multi-Device Access is not supported.

   b. If you have allowed new registrations when the maximum number of registrations is reached, ensure that Session Manager ends an already existing registration if a new registration request is received.

2. If call failure occurs for digital or analog endpoints, do the following:

   a. Ensure that **Max. Simultaneous Devices** is set to 1.

   b. Ensure that the **Block New Registration When Maximum Registrations Active** check box is selected.

3. In case of a slow recovery after a network failure, do the following:

   a. If you have allowed new registrations when the maximum number of registrations is reached, ensure that Session Manager ends an already existing registration if a new registration request is received.

   Otherwise, a network failure between an endpoint and Device Adapter or Device Adapter and Session Manager retains the original registration until the keep-alive signaling detects the network failure. UNIStim endpoints can register only after the failure is detected.

    b. Ensure that Session Manager 1 and Session Manager 2 are configured correctly, and that the destinations are valid Device Adapter clusters, that is, primary and backup.

    c. Ensure that Device Adapter is correctly configured for primary and backup Session Managers.

4. To troubleshoot MDA and Sequential Registration problems in Device Adapter, run the TraceSM utility on Session Manager to collect and examine the `tDSA tCSDK` debug logs.

Virtual Office configuration issues

Condition

Virtual Office Login Allowed (VOLA) attributes are set, but virtual key does not appear during configuration.

The cause for the Virtual Office configuration issue can be one of the following:

- VOLA attributes are in the second line of features in Communication Manager endpoint configuration.
- Key maps take a long time to update.

Solution

1. Check Avaya Breeze® platform for the latest version.
2. Move VOLA attributes to the first line of features in Communication Manager endpoint configuration.
3. If moving VOLA attributes to the first line of features in Communication Manager endpoint configuration fails, then reboot the UNIStim endpoint and retry.
4. If rebooting of UNIStim endpoint fails, then collect DSA (syslogLevelSet dsa tDSA 7) and TPS (syslogLevelSet tps tSET 7) DEBUG logs during registration to analyze and fix the issue.

Troubleshooting voice mail problems

Condition

Display of context-sensitive soft keys for voice mail on the phone is enabled on System Manager. Depending on the configuration, System Manager uses either the default or custom values of the Voicemail attributes.

However, the user still encounters the following problems:

- A user is unable to log in to the voice mail.
- Context-sensitive soft keys for voice mail are not working on the phone.
- Context-sensitive soft keys for voice mail are not displayed on the phone when the user presses the **Messages/Inbox** key or manually dials the voice mail access number on the phone.

⊛ **Note:**

The solution to this problem might require a Device Adapter restart. If a Device Adapter restart is required, Avaya recommends that you stop and start Device Adapter during the maintenance window to minimize the impact on endpoint registration and call handling.

Cause

- The values configured for the Voicemail attributes in System Manager do not match the ones used by Device Adapter.

- The administrator has not restarted Device Adapter after modifying the values of the Voicemail attributes in System Manager.

Solution

1. In the `config.ini` file, examine the `Voicemail` section and ensure that the dialing sequence values for the voice mail soft keys are present and match the ones configured on System Manager.

   If the dialing sequence values are not present or do not match the ones configured on System Manager, re-configure the Voicemail service attributes on System Manager and restart Device Adapter.

   The `config.ini` file is located at `/opt/Avaya/da/shared/config/` on Avaya Breeze® platform.

   If this does not resolve the problem, go to Step 2.

2. If the dialing sequence values are correct in the `config.ini` file, but the voice mail soft keys are not displayed on the phone, restart Device Adapter.

   If this does not resolve the problem, go to Step 3.

3. Do the following to enable log traces and set the log level:

   a. Run the following commands on the Avaya Breeze® platform CLI command prompt to enable the dsa, tps, and pbx log traces:

      - syslogLevelSet dsa tDSA 7

      - syslogLevelSet tps tDSET 7

      - syslogLevelSet pbx tMAM 7

   b. On the System Manager web console, do the following to set the log level:

      a. Navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

      b. Click **Logging**.

      c. In the **Cluster** field, click the Avaya Breeze® platform cluster that has the Device Adapter Snap-In installed.

      d. In the **Server** field, click the server where the cluster resides.

      e. In the **Service** field, click **DeviceAdapter**.

      f. In the **Log Level** field, click **ALL**.

      g. Click **Set Log Level**.

4. Make a test call.

5. Examine the `dsa.log`, `DeviceAdapter.log`, and `ss_common.log` files located at `/var/log/Avaya/services/DeviceAdapter/`.

6. In the dsa.log log file, find the `ProcessSystemDataNotify` message and examine the value of VoiceMailSystem in the message. Do the following:

   a. Ensure that the Voicemail Telephony User Interface system is the same as the one configured on System Manager.

   b. Ensure that the dialing sequence is correct. If the dialing sequence is incorrect, rectify it by using the Voicemail attributes in System Manager.

7. Verify that during an active call to the voice mail, the following message is logged in the dsa.log file:

   ```
   There is call to VoiceMail server.
   ```

Incorrect name and extension displayed on a CC phone after downgrading Device Adapter from Release 8.1.2 to Release 8.1.1

Condition

Incoming call name and extension is displayed incorrectly on a call center phone after downgrading Device Adapter from Release 8.1.2 to Release 8.1.1.

Cause

Device Adapter Release 8.1.2 supports Call Center Elite to provide support for call center operations on CS1K_IPCC phones. Whereas, Device Adapter Release 8.1.1 supports only UC phones (CS1K_IP). Device Adapter Release 8.1.1 does not support Call Center Elite.

If an agent is logged in to the phone as a Call Center Elite agent and if you downgrade Device Adapter from Release 8.1.2 to Release 8.1.1, the agent's status remains as logged in on Communication Manager.

Call Center Elite too maintains the agent's registration status till the registration subscription period expires. The registration status includes the agent's login status. This is part of the high availability capability of Call Center Elite, which allows the agent station to remain available in an event of a temporary signaling failure or phone restart.

If you downgrade Device Adapter to Release 8.1.1 while an agent is still logged in, Device Adapter does not support any call center operations on the phone, including the SIP registration.

However, until the registration period expires and the re-registration attempt fails, Communication Manager and Call Center Elite continue to present calls to the phone as per the Call Center Elite call routing algorithms.

Because the display format of a UC phone and a CC phone is different, the incoming call name and extension is displayed incorrectly on such CC phones.

Solution

Before starting the process to downgrade Device Adapter from Release 8.1.2 to Release 8.1.1, ensure that all agents are logged out of the CC phones as Call Center Elite agents.

> 😊 **Note:**
>
> This procedure is not required for the following phones:
>
> - Phones that are configured as UC phones (CS1K_IP).
> - CTI controlled phones that operate as UC phones and are used for media purposes only.

Related links

[Considerations before downgrading Device Adapter from Release 8.1.2 to Release 8.1.1](#) on page 190

System Manager user creation problem

Condition

Sometimes when creating a user on System Manager, the following error occurs:

```
Endpoint "200802" could not be added on CM "cm" and association of
endpoint to user "200802@<domain name> " failed.
```

Cause

com.avaya.iptcm.cm.controller.exceptions.CmControllerException: 3 4654ff00 5bc5 subtype "3901 " is an invalid entry.

Solution

1. On System Manager, create an endpoint profile by using the correct template in **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.

2. Do the following to link this endpoint to a user:

   a. On System Manager, navigate to **Users** > **User Management** > **Manage Users**.

   b. Select the user, and then click **Edit**.

   c. On the **Communication Profile** tab, enable the **CM Endpoint Profile** option.

   d. Select the **Use Existing Endpoints** check box.
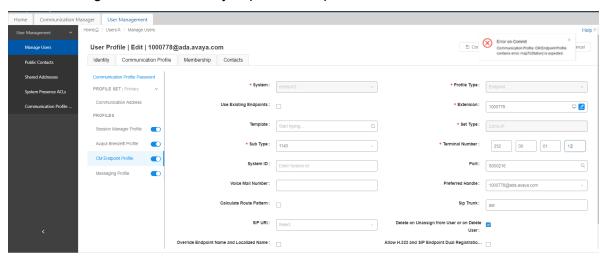
    e. In the **Extension** field, specify the extension.

3. If the following error occurs after you perform step 2, click the extension editor.

4. Click **Commit** on the Endpoint editor.

Element Manager pages are blank

Condition

The Element Manager pages on **System Manager** > **Elements** > **Device Adapter** are blank.

Solution

1. Examine the Device Adapter IU installation logs on System Manager:

   `/opt/Avaya/install_logs/ADA_patch_log_*.txt`

2. Run the following command to verify that the correct System Manager patch is installed:

   > swversion | tail -20

3. Run the following command to verify that System Manager IU is installed:

   **> ls /opt/Avaya/JBoss/wildfly-10.1.0.Final/avmgmt/deployments/
   cs1kmgw.ear***

   The preceding command displays two files: `cs1kmgw.ear` and
   `cs1kmgw.ear.deployed`.

   If the preceding command displays the `cs1kmgw.ear.failed` file instead of
   `cs1kmgw.ear.deployed` file, System Manager IU deployment has failed.

   The `cs1kmgw.ear.failed` file contains the reason for the deployment failure.

4. Examine the following log files on System Manager:

   `/var/log/Avaya/jboss/log/server.log`

   `/var/log/Avaya/jboss/log/quantum.log`

Verifying data replication between System Manager and Avaya Breeze® platform

About this task

System Manager and Avaya Breeze® platform have separate databases. Verify data replication.
Verify that the data is sent properly to DSA and Device Adapter Snap-in level from System
Manager.

Procedure

Do the following on System Manager to verify that all attributes are properly stored in the database
on System Manager:

a. mgmtia

b. Run the following command to get the element type ID:

   select * from rts_applicationsystemtype where resourcetype='CS1KMGW'

c. Run the following command to get the Media Gateway ID:

   select * from rts_applicationsystem where appsystemtypeid=1329

d. Run the following command to get the custom element values:

   select * from rts_attribute where appsystemid=901

Troubleshooting system ID mismatch between Avaya Breeze® platform and Communication Manager user profile for UNIStim endpoints

Condition

UNIStim endpoint registration is rejected and the endpoint displays the following error message:

```
Unequipped
```

A UNIStim endpoint displays only the node ID and Terminal Number (TN), and not the system ID. Hence, the error message that is displayed by the UNIStim endpoint does not indicate the system ID mismatch between the Avaya Breeze® platform attribute and Communication Manager user profile.

Cause

A Communication Manager station representing a Device Adapter UNIStim endpoint associates the station with a unique system ID and TN combination.

A Communication Manager user profile that is administered with the Set Type of CS1k-xxxx has the **System ID** and **Terminal Number** fields. These two values form a unique combination at the solution level for every station representing a Device Adapter UNIStim endpoint.

A Device Adapter cluster is administered with a node ID and system ID in the Avaya Breeze® platform attributes. When a Device Adapter UNIStim endpoint tries to register, it submits the node ID and the TN. Device Adapter locates the Communication Manager station that contains the same unique combination of the cluster system ID and the TN value submitted by the endpoint.

If the TN is the same, but the system ID does not match between the Avaya Breeze® platform attribute and Communication Manager user profile, endpoint registration fails and the endpoint displays the following error message:

```
Unequipped
```

Solution

1. On the Avaya Breeze® platform, examine the `DeviceAdapter.log` file that is located at the following location for a warning message related to system ID mismatch:`/var/log/Avaya/services/DeviceAdapter/DeviceAdapter.log`

2. If there is a mismatch in the system IDs, do any one of the following on System Manager:

   • Do the following to modify the Avaya Breeze® platform **System ID** attribute to match it with the one that is configured in the Communication Manager user profile:

      a. Click **Elements** > **Avaya Breeze®** > **Configuration**.

      b. Click **Attributes**.

      c. Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

      d. On the Attributes Configuration page, navigate to the **IP Telephony Node** group.

      e. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

f. In the **System ID** field, in **Effective Value**, type the system ID.

g. Click **Commit**.

- Do the following to modify the system ID that is configured in the Communication Manager user profile to match it with the one that is configured in the Avaya Breeze® platform **System ID** attribute:

a. Click **Users** > **User Management**.

b. Click **Manage Users**.

c. Select the check box corresponding to the user, and then click **Edit**.

d. Click the **Communication Profile** tab.

e. In **Profiles**, enable **CM Endpoint Profile**.

f. In the **System ID** field, modify the system ID.

g. Click **Commit**.

Troubleshooting MGC-related problems

General commands to verify the MGC configuration

```
ldb> swversionshow

ldb> mgcinfoshow

ldb> mspversionshow

ldb> ethportshow

ldb> sockShow

ldb> inetstatShow

ldb> iosFdShow
```

Enable Media Gateway Controller trace analysis

Use the topics under this section to enable and disable the Media Gateway Controller (MGC) traces for various problem scenarios. Avaya recommends enabling these logs when the traffic level is low. High traffic might log more log entries, which might cause difficulty in tracking the cause.

Enabling and disabling data collection for DSP tVGW-related problem on MGC

Procedure

Do one of the following:

- Run the following command to enable data collection on MGC for DSP tVGW-related problem:

  ```
  > syslogLevelSet tVGW,7
  ```

- Run the following command to disable data collection on MGC for DSP tVGW-related problem:

  ```
  > syslogLevelSet tVGW,6
  ```

Enabling and disabling data collection for tone-related problem on MGC

Procedure

Do one of the following:

- Run the following command to enable data collection on MGC for tone-related problem:

  ```
  > syslogLevelSet tTncTask,7
  > syslogLevelSet tVapiTask,7
  ```

- Run the following command to disable data collection on MGC for tone-related problem:

  ```
  > syslogLevelSet tTncTask,6
  > syslogLevelSet tVapiTask,6
  ```

Enabling and disabling data collection for CardLan problem on MGC

Procedure

Do one of the following:

- Run the following command to enable data collection on MGC for CardLan problem:

  ```
  > syslogLevelSet tCLanLayer3,7
  ```

- Run the following command to disable data collection on MGC for CardLan problem:

  ```
  > syslogLevelSet tCLanLayer3,6
  ```

Enabling and disabling data collection for A31 messaging failure on MGC

Procedure

Do one of the following:

- Run the following command to enable data collection on MGC for A31 messaging failure:

  ```
  > syslogLevelSet tA31Poll,7
  ```

- Run the following command to disable data collection on MGC for A31 messaging failure:

  ```
  > syslogLevelSet tA31Poll,6
  ```

Troubleshooting MGC connection problems

About this task

🛈 **Important:**

Troubleshooting MGC connection related problems may require stopping and starting MGC and `pbxserver` service, which might have an impact on endpoint registrations and call handling.

For more information about the impact on endpoint registrations after stopping and starting the `pbxserver` service, see [Maintenance commands](#) on page 250.

Avaya recommends that you stop and start MGC and `pbxserver` service during the maintenance period to minimize endpoint registration and call handling problems.

Procedure

1. After MGC starts, MGC tries to establish RUDP connection with Device Adapter by using UDP port 15003.

   Run the following command at the MGC CLI command prompt to ensure that the ELAN and TLAN cables are plugged into MGC:

   `ldb> ethportshow`

   An output similar to the following, with two active ports, appears:

   `... Carrier detected on ports:6 ,7`

   If not, then the problem might be with the cables or ethernet link and not because of socket error.

2. Do the following to verify that the pbxserver process listens on UDP port 15003:

   a. Run the following command on the Avaya Breeze® platform CLI command prompt to verify that the pbxserver process listens on UDP port 15003:

   `netstat -putanel | grep 15003`

   A message similar to the following appears:

   `udp 0 0 192.168.96.164:15003 0.0.0.0:* 700 894624883 26820/`
   `pbxserver`

   If pbxserver is not shown, go to Step 2 b.

   b. Run the following command on the Avaya Breeze® platform CLI command prompt to verify the pbxserver status:

   `[root@breeze6 ~]# dasrvstart status pbxserver`

   A message similar to the following appears:

   `? pbxserver.service - PBX Server for Avaya Device Adapter Snap-`
   `in`
   `Loaded: loaded (/etc/systemd/system/pbxserver.service;`

```
enabled; vendor preset: disabled)
Active: active (running) since Thu 2018-11-15 16:56:08 MSK; 4
days ago
Main PID: 1934 (pbxserver)
CGroup: /system.slice/pbxserver.service
L-1934 /opt/Avaya/da/shared/bin/pbxserver
Nov 15 16:56:08 breeze6 systemd[1]: Started PBX Server for
Avaya Device Adapter Snap-in.
Nov 15 16:56:08 breeze6 systemd[1]: Starting PBX Server for
Avaya Device Adapter Snap-in...
```

c. Run the following commands on the Avaya Breeze® platform CLI command prompt to stop and start the pbxserver service:

[root@breeze6 ~]# dasrvstart stop pbxserver

[root@breeze6 ~]# dasrvstart start pbxserver

Repeat Steps 2 and 2 a. If it does not give the expected result, go to Step 2 d.

d. Run the following commands on the Avaya Breeze® platform CLI command prompt to enable debug logs for DSA and pxbserver:

[root@breeze6 ~]# syslogLevelSet dsa tDSA DEBUG

Run the following command to ensure that log level changes are applied:

syslogShow

e. Do the following on System Manager to enable debug logs for Device Adapter snap-in:

a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.

b. Select the appropriate cluster and server.

c. In the **Service** field, click **Device Adapter**.

d. In the **Log Level** field, click **DEBUG**.

f. After enabling the debug log, go to Step 2 c and collect logs for 5 to 10 minutes, and then do the following to extract logs from the Avaya Breeze® platform:

collect /var/log/Avaya/services/DeviceAdapter/DeviceAdapter.log

collect /var/log/Avaya/services/DeviceAdapter/dsa.log

collect /var/log/Avaya/services/DeviceAdapter/ss_common.log

g. Run the following commands on the Avaya Breeze® platform CLI command prompt to investigate error logs:

**[root@breeze6 ~]# cat /var/log/Avaya/services/DeviceAdapter/
DeviceAdapter.log | grep -i "error\|warn"**

**[root@breeze6 ~]# cat /var/log/Avaya/services/DeviceAdapter/
dsa.log | grep -i "error\|warn"**

```
[root@breeze6 ~]# cat /var/log/Avaya/services/DeviceAdapter/
ss_common.log | grep -i "error\|warn"
```

3. Do the following to verify that port 15003 and 15000 are open:

   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   b. In Cluster State, ensure that the cluster state is set to "Accept" corresponding to Avaya Breeze® platform cluster that you are working on.

   c. Run the following command to verify that port 15003 is open:

      ```
      [root@breeze6 ~]# ce fwall show 15003/udp
      ```

      The following message appears:

      ```
      15003/udp on
      ```

   d. If port 15003 is disabled, run the following command to enable port 15003:

      ```
      [root@breeze6 ~]# ce fwall on 15003/udp
      ```

   e. Run the following command to verify that port 15000 is open:

      ```
      [root@breeze6 ~]# ce fwall show 15000/tcp
      ```

      The following message appears:

      ```
      15000/tcp on
      ```

   f. If port 15000 is disabled, run the following command to enable port 15000:

      ```
      [root@breeze6 ~]# ce fwall on 15000/tcp
      ```

4. Do the following to verify that packets from MGC reach the Avaya Breeze® platform server:

   a. Log in to Avaya Breeze® platform as root user and run tshark.

      Ensure that there are no "administratively prohibited" or "host unreachable" messages. These messages appear in situations such as the ports are closed or if there is a firewall problem.

   b. Run the following command, and then restart MGC:

      ```
      [root@breeze6 ~]# tshark -i any "host 192.168.23.24"
      ```

      Where the IP address is MGC ELAN IP.

      The following message appears:

      ```
      1 0.000000000 192.168.23.24 -> 192.168.96.178 UDP 62 Source
      port: 15003  Destination port: 15003
      2 0.000218436 192.168.96.178 -> 192.168.23.24 UDP 50 Source
      port: 15003  Destination port: 15003
      ```

      The following message appears in case of dropped packets:

      ```
      1 0.000000000 192.168.127.91 -> 192.168.96.178 UDP 62 Source
      port: 15003  Destination port: 15003
      ```

```
2 0.000078870 192.168.96.178 -> 192.168.127.91 ICMP 78
Destination unreachable (Port unreachable)
```

If you do not see packets at all, there might be a network problem.

If you see "administratively prohibited" packets, then do the following to put the Avaya Breeze® platform cluster to Deny, and then to Accept mode.

    a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

    b. In **Cluster State**, verify the state of the Avaya Breeze® platform cluster.

c. Verify that the custom firewall rule is set to Off on MGC.

Custom firewall rule might be On if previously the custom firewall rule was set by the CS 1000 call server. Do the following:

    a. Run the following command to verify the port access status:

    ldb> portAccessStatus

    If the following message appears, go to Step b:

```
Global status: custom
Local state: custom
```

    b. Run the following command to turn off custom firewall rule:

    ldb> portAccessOff

5. Do the following to verify the rudp connection status on Avaya Breeze® platform and MGC:

    a. Run the following command on the Avaya Breeze® platform CLI command prompt to verify the rudp connection status:

    [root@br3937 ~]# vxShell pbxserver rudpShow

    The following message appears if the connection is proper:

```
RUDP for Call Server Application
RUDP Port Summary
Port ID       Src IP     Src Port
0xf4428300 192.168.39.38  15003
RUDP Connection Summary
Src IP        Src Port  Connect ID   Dst IP        Dst Port   Status        Msg rcv   Msg sent  Retries
+------------+--------+----------+-------------+--------+------------+--------+--------+------+
192.168.39.38 15003    0xf4428538 192.168.39.49  15003      ESTABLISHED <->  3         132        0
192.168.39.38 15003    0xf4428fb0 192.168.39.37  15002      ESTABLISHED <->  1         129        0
```

    The following message appears if the system cannot find the pbxserver process:

```
value = 0xf56fe080 (4117749888)
```

    To troubleshoot the problem, repeat Steps 2 b through 2 g.

    b. Run the following command on the MGC to verify the rudp connection status:

    ldb> rudpShow

    The following message appears if the connection is proper:

```
Src IP          Src Port   Connect ID    Dst IP        Dst Port  Status       Msg rcv  Msg sent  Retries
+---------------+----------+-------------+-------------+---------+------------+--------+---------+-------+
0.0.0.0          15001     0x84d1f2a0   192.168.96.164 15003      DUDP            0        0        0
192.168.128.144  15003     0x84d1f3a0   192.168.96.164 15003      ESTABLISHED <-> 2       23        1
```

If a message similar to the following appears, verify the IPSEC status on Device Adapter and MGC:

```
Src IP          Src Port   Connect ID    Dst IP        Dst Port  Status          Msg rcv  Msg sent  Retries
+---------------+----------+-------------+-------------+---------+---------------+--------+---------+------+
0.0.0.0          15001     0x84d1f250   10.102.104.31 15003      DUDP                0        0       0.
10.102.103.194   15003     0x84d1f350   10.102.104.31 15003      NOT ESTABLISHED     0       113      102
```

6. Verify if FIPS mode is enabled and MGC runs old loadware from Avaya Device Adapter Snap-in. The old MGC version does not support the strong ciphers that FIPS mode requires.

   - Temporarily disable FIPS mode.

   - Upgrade MGCs to updated loadware lineup and enable FIPS mode.

7. Verify if IPSec is enabled on both the MGC and Avaya Device Adapter Snap-in side.

   On MGC issue `isssShow` command:

   ```
   ldb> isssShow
   ```

   On Avaya Device Adapter Snap-in side:

   - In the **Enable IPsec for Media Gateways** field, in **Effective Value** is set to **Yes**.

   - The **ipsec status** command displays on Breeze® server.

     ```
     [root@breeze5 ~]# ipsec status
     whack: Pluto is not running (no "/run/pluto/pluto.ctl")
     ```

   If IPSec is disabled on both the Breeze® server and Avaya Device Adapter Snap-in then go to the next chapter. Otherwise, perform the following troubleshoot steps:

   - Manually synchronize the IPSec configuration if:

     - IPSec is disabled on MGC but enabled on Avaya Device Adapter Snap-in.

     - IPSec configuration is not synchronized on the MGC or changed on Avaya Device Adapter Snap-in side while MGC was down.

   - Make sure that the Primary Server IP (through `mgcinfoshow`) command corresponds to what is configured in SMGR for the MGC:

     - On System Manager, click **Services** > **Inventory** > **Manage Elements**.

     - On the **Device Adapter** tab, make sure you select the correct cluster.

   - Make sure that if the Avaya Device Adapter Snap-in cluster is Cluster IP (two or more servers) then MGC **Primary Server IP** is set to **Cluster IP**. If Avaya Device Adapter Snap-in cluster consists of a single server, then MGC **Primary Server IP** is set to **SecureLink IP address (eth1)**.

- Verify if the FIPS mode is enabled on the Breeze® server. Do the following:
    - Avaya Device Adapter Snap-in version must be 8.1.3 or later.
    - MGC loadware version should match with ADA 8.1.3 lineup.
        - On MGC, perform `swVersionShow` command.
        - On Breeze® server, verify the loadware files in "`ls -l /opt/Avaya/da/mgc/loadware/current/`".
    - Compare the Avaya Device Adapter Snap-in versions.

    If any of the above values is true, then MGC fails to connect with Avaya Device Adapter Snap-in. Upgrade Avaya Device Adapter Snap-in to 8.1.3 version.

8. After RUDP the link is established, MGC sends the "call server info request" message over the rudp link.

    This is indicated with the following message in the logs:

    `Sending message to Call Server to get csinfo.`

    If MGC receives a response, the following message appears:

    `Successfully got call server information from Primary.`

    a. Run the following command to enable dsa debug logs and verify if dsa receives messages in the dsa log when `Sending message to Call Server to get csinfo.` messages appear on MGC:

    `syslogLevelSet dsa tDSA 7 ; tail -f /var/log/Avaya/services/DeviceAdapter/dsa.log`

    The following example error message indicates that SSK keys between MGC and Avaya Breeze® platform are not generated:

    `Nov 16 12:03:36 greenedpeccm dsa: ERROR: [13077] CSSHClient::Connect(): authentication to host 135.20.225.84 failed with error code -16, message:`

    b. Go to Step 5 to verify the network connectivity and rudp link.

9. After a response to the request in Step 8 a is received, MGC establishes TCP link on port 15000 with Device Adapter.

    Upon successful connection, the following message appears:

    `SYS: PBX TCP link established with ..`

    Run the following command on the Avaya Breeze® platform CLI command prompt to verify the TCP link:

    `[root@breeze5 ~]# vxShell pbxserver tcpLinkShow`

    The following message appears for a successful connection:

    `192.168.128.144 |0xf4228fb0|18 |0 |0 | Link OK`

If the "Failed to open TCP network connection to CS" message appears, do the following:

    a. Verify that the TCP packets reach Avaya Breeze® platform as in Step 4.

    b. Run the following command on the Avaya Breeze® platform CLI command prompt to enable debug logs and contact Avaya Support:

[root@breeze5 ~]# syslogLevelSet pbxserver tRUDP 7

[root@breeze5 ~]# syslogLevelSet pbxserver tvtServer 7

[root@breeze5 ~]# syslogLevelSet pbxserver tvtServerRx 7

10. After TCP link is up, MGC sends a ServerOnline message. Device Adapter responds with a ServerStatus message.

   Run the following mgcShow command to verify that Device Adapter has added MGC to the server list:

   root@breeze14 DeviceAdapter]# mgcShow

   If you receive the following message, the `Received server status for link Primary with status 0` log entry appears on MGC:

```
[root@breeze14 ~]# mgcShow

Registered media gateways:

 # | Loop-Sh |    Conn ID | MGC ELAN IP | TYPE | BOOT |  APP |  CSP |  MSP | FPGA |      DB1 |  DB2 | UPG STATUS |

----+---------+------------+-------------+------+------+------+------+------+------+----------+------+------------+

 1 |    64-0 | 4095903064 | 10.10.10.100 |  MGC | BA18 | NA09 | NB06 | AB02 | AA22 | DSP1AB07 | NONE |     Idle |
```

   You might not receive the preceding message if MGC is not configured on System Manager.

   Do one of the following:

   • Verify the MGC configuration in **Services** > **Inventory** on System Manager.

   • If MGC is configured properly, restart the Device Adapter Snap-In.

   • Examine the dsa tDSA debug logs.

11. After the ServerStatus message is received, MGC waits for Device Adapter to upload the `mgcdb.xml` file to `/u/db/` over SFTP and send a FileUploaded message upon completion.

   After this, dsa logs the following debug log entry:

   `CServerController::SendServiceFileUpdated()`

   MGC shows the following messages for companding law and loop/shelf.

```
09/10/2018 15:21:11 LOG0006 tMgcVgwAppStart: Loop/shelf is set to
0-009/10/2018 15:21:11 LOG0006 tMgcVgwAppStart: Companding law is
set to a-law
```


If Device Adapter cannot upload the `mgcdb.xml` file, it shows the following message and raises an alarm:

```
Cannot transfer XML config file to MGC.
```

Examine the log entries to investigate the reason. The most common reason is that MGC does not have the login set to admin2 and password set to 0000.

MGC waits for `FileUploaded` message for 75 seconds. After that, MGC tries to read the existing `/u/db/mgcdb.xml` file on the disk. Otherwise, MGC restarts.

When the `FileUploaded` message is received, MGC reads the `mgcdb.xml` file to retrieve loop/shelf. MGC uses loop/shelf to further register the DSP channels, IPE cards, and units.

12. MGC detects IPE cards and units.

   The following is an example of log messages on MGC:

```
09/10/2018 15:21:12 LOG0006 CLAN: Slot: 3, Card Type: XMLC (24),
Signaling Type: A10 (2), Map Type: 3
```

   The following is an example of a debug log message in dsa.log:

```
CIPECardManager::OnIPECardPlugged(): 0-0-3
```

   The dsa log message is for loop and shelf that MGC retrieves from the `mgcdb.xml` file.

   a. Run the following command to verify the card and unit detection status on Device Adapter:

   ipeShow <loop>-<shelf>

   The following message appears:

```
[root@breeze5 ~]# ipeShow 0-0
Detected IPE cards for media gateway: 0 0
Card Slot  |    Type   | Status  |
-----------+-----------+---------+
      3 |       MLC |      ok |
```

   b. Do one of the following if the **ipeShow** command does not show any cards, even though the MGC logs show the detected cards:

   • MGC might lose and then re-establish pbxlink. In this case, the card and unit status is not synced with Device Adapter.

   • Unplug and plug in the card again.

   When Device Adapter receives a card detection message, it sends initialization messages and turns off the red LED on the faceplate.

   A red LED indicates that the card is currently not recognized by Device Adapter.

   ALC card is also initialized with a companding law.

Avaya Device Adapter Snap-in Reference

13. MGC starts the VGW application that initializes the DSP daughterboards and starts registering channels.

    a. Run the following command to verify VGW channel registration status on Device Adapter:

vgwShow <loop>-<shelf>

The following message appears:

```
[root@breeze5 ~]# vgwShow 0-0
VGW TN     |       IP        | Port  |  Phone TN
---------------|----------------+--------|-------------
000-00-11-00 |192.168.128.146 |   5392 |000-00-03-00
000-00-11-01 |192.168.128.146 |   5394 |
000-00-11-02 |192.168.128.146 |   5396 |
```

    b. If there are no listed channels, run the following command on MGC to force register the channels:

vgwRegisterAll

Device Adapter sends tone channel initialization messages. One of its parameters is companding law that is used to init TNC device.

When ALC card is detected, Device Adapter tries to register all its 16 units.

14. DLC card units are detected individually. Run the following command to verify the DLC card units:

ipeShow <loop>-<shelf>-<card>

If a DLC unit shows as detected but the set is not working, verify if the DLC unit is configured in System Manager and Communication Manager station.

15. Run the following commands to verify the set registration status:

dsaShow

endpointShow

The endpointShow command can take TN or extension.

An output similar to the following appears:

```
[cust@breeze8 ~]$ endpointShow 240-00-02-21
Extension: 200921
Handle: 200921@men.ru
CS1K Type: 2001
Primary/Secondary/Branch SMs: 192.10.10.10 /  /
Features: VOLA VOUA HFA
Number of Button Modules: 0, Buttons per module: 0
MSEC: MSBT
SMGR Language: en_US
TimeZone: 3:00

CFAC status: Disabled

There are no calls
```

Related links

Troubleshooting MGC registration problems

About this task

Digital or analog set requires provisioning in System Manager.

ⓘ Important:

Troubleshooting MGC registration related problems may require stopping and starting MGC and the `dsa` service, which might have an impact on endpoint registrations and call handling.

For more information about the impact on endpoint registrations after stopping and starting the `dsa` service, see Maintenance commands on page 250.

Avaya recommends that you stop and start MGC and the `dsa` service during the maintenance period to minimize endpoint registration and call handling problems.

Before you begin

On System Manager, ensure that the following fields have appropriate values:

- TN: The loop shelf card unit. Ensure that the loop shelf card unit matches the loop shelf of MGC.
- SystemId: Ensure that the system ID matches the system ID that is configured in the Avaya Breeze® platform attribute.
- Type (for digitals): Ensure the type matches the actual set type. For example, if you configure an endpoint type 2616, ensure that the actual physical phone is of type 2616.

Procedure

1. If the digital set appears as not registered, run the following command to verify if Device Adapter has detected the digital set:

> ***** **Note:**
>
> Analog units cannot be detected. Hence, Device Adapter tries to register all 16 units.

ipeShow

A message similar to the following appears:

```
ipeShow 0-0-3
```

The corresponding unit should appear as online.

2. If the digital set is online, run the following command to verify the registration status:

   endpointShow <loop>-<shelf>-<card>-<unit>

   If the output displays that the endpoint is not logged in, go to Step 3.

3. Run the following command and examine the output to verify if there are any registered and available unallocated VGW channels:

   vgwShow <loop>-<shelf>

   The following output appears:

```
[root@breeze5 ~]# vgwShow 0-0
 VGW TN       |       IP          | Port  |   Phone TN
 000-00-11-00 |192.168.128.146 |   5392 |000-00-03-00
 000-00-11-01 |192.168.128.146 |   5394 |000-00-03-01
 000-00-11-02 |192.168.128.146 |   5396 |000-00-03-02
 000-00-11-03 |192.168.128.146 |   5398 |000-00-03-03
```

4. If the phone does not appear in the Phone TN column and there are no more available channels, verify if more than one VGW channel is assigned to the same phone TN. If yes, then do one of the following:

   • Run the following commands to stop and start the dsa service:

     dasrvstart stop dsa

     dasrvstart start dsa

   • Restart MGC.

   • Report the problem to Avaya Support.

   • Provide more DSPs on the MGC. Upgrade or plug the second DSP DB into MGC to provide more DSPs. Switch from 32 to 96 DSP daughterboard.

5. If your phone has a linked VGW channel or if there are free channels or if your phone appears in the list after you run the **endpointShow** command, then do the following:

   a. Unplug the set.

   b. Enable the dsa tDSA tCSDK debug logs.

   c. Run traceSM.

   d. Plug in the set.

e. Analyze the traceSM output of both SIP and PPM.

f. Provide the dsa.log and traces logs to Avaya Support.

Troubleshooting MGC tone problems

About this task

DSA does the following when applying the dialtone, ringback, and fastbusy tones:

- Allocates a TNC channel number by using the following fixed formula:

(card-1) * 16 + unit + 1

The maximum number of TNC channels is 255.

- Establishes one-way speech between the TNC channel and the set.

- Configures the TNC channel to play the required tone.

You can replace the ringback tone with early media. For example, provide RTP music and announcement instead of local ringback tone.

Procedure

1. Do the following if you hear silence or unexpected media:

   a. Analyze SIP signaling by using traces.

   b. Collect and analyze the RTP traces.

   c. Use G711 for a call. By default, G711 is enabled on Device Adapter. Ensure that G711 is enabled on Communication Manager.

   d. Use the port mirroring feature of MGC to obtain RTP logs.

   e. Use the following commands on the Avaya Breeze® platform:

      `mgcShow -> ipeShow -> vgwShow -> endpointShow`

2. If a dial tone is played with distorted sound, it might be because of companding law mismatch between the TNC device and the set. Do the following:

   - Restart MGC or report the problem to Avaya Support.

3. Do the following if the played dial tone follows incorrect standards:

   a. Verify the Country attribute.

      Device Adapter uses the Country MGC ME attribute to apply country-specific tones.

   b. Verify that the MGC bootup log contains the following log message:

      `LOG0006 TNC: tone table set successfully for USA countryelow.`

4. If the Country attribute is set properly but log message shows another value, MGC might be using an old mgcdb.xml file. This is because Device Adapter could not upload the new mgcdb.xml file. Do the following:

- Verify dsa.log for errors. The login is not set to admin2 and the password is not set to 0000.

- Manually download the /u/db/mgcdb.xml file, edit the Country value, and upload the file. Run the following command on MGC:

ldb> toneTableSet

A message similar to the following appears:

LOG0006 TNC: tone table set successfully for Sweden country

Verify the tone and if it is still incorrect, report the problem to Avaya Support.

Chapter 12: Resources

Documentation

The following table lists the related documents for the Avaya Device Adapter Snap-in. These documents are available on the Avaya Support web site.

Title	Description	Audience
Avaya Device Adapter User Guide for Avaya Aura® Call Center Elite Agents	Describes user operations that can be performed on Device Adapter phones in Avaya Aura® Call Center Elite.	Avaya Aura® Call Center Elite agents and supervisors.
Administering Avaya Aura® Call Center Elite	Describes the procedures to administer Avaya Aura® Call Center Elite features.	Services and support personnel System administrators
Administering Avaya Aura® Session Manager	Describes the routing administration and management of Avaya Aura® Session Manager instances.	Services and support personnel System administrators
Administering Avaya Aura® System Manager	Describes the administration and management of Avaya Aura® System Manager.	Services and support personnel System administrators
Deploying Avaya Aura® System Manager	Describes how to deploy Avaya Aura® System Manager in a virtualized environment using VMware.	Services and support personnel System administrators
Administering Avaya Breeze® platform	Describes the procedures for administering Avaya Breeze® platform and for installing and administering snap-ins running on Avaya Breeze® platform.	Services and support personnel System administrators
Deploying Avaya Breeze® platform	Describes the procedures to deploy and administer Avaya Breeze® platform.	Services and support personnel System administrators
Avaya Aura® Communication Manager Feature Description and Implementation	Describes the procedures to administer the features of Avaya Aura® Communication Manager.	Services and support personnel System administrators
Administering Avaya Aura® Communication Manager	Describes the procedures to administer Avaya Aura® Communication Manager.	Services and support personnel System administrators

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.

2. At the top of the screen, type your username and password and click **Login**.

3. Click **Support by Product** > **Documents**.

4. In **Enter your Product Here**, type the product name and then select the product from the list.

5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.

6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.

7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.

2. Log on to the Avaya website with a valid Avaya user ID and password.

3. On the Avaya Support page, click **Support by Product** > **Documents**.

4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.

5. In **Choose Release**, select the required release number.

6. In the **Content Type** filter, select one or both the following categories:

   • **Application & Technical Notes**

   • **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.

7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

> ⓘ **Important:**
>
> For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.

- Click **Languages** (⊕) to change the display language and view localized documents.

- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.

- Add content to your collection by using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.

- Send feedback on a section and rate the content.

> **Note:**
>
> Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Training

The following courses are available on the Avaya Learning web site. Enter the course code in the **Search** field, and click **Go** to search for the course.

Course Code	Course Title
20970W	Introducing Avaya Device Adapter

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

  > **Note:**
  >
  > Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips

- Information about service packs

- Access to customer and technical documentation

- Information about training and certification programs

- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press Enter.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: CS 1000 class of service and Avaya Aura® feature field mapping

CS 1000 CoS and Avaya Aura® feature field mapping

The following table lists the Avaya Aura® feature field values supported that are mapped from CS 1000 phone Class of Service (CoS) values.

CS 1000 Class of Service (CoS)	Feature name/Description	Default value
ADD	• ADD: Automatic Digit Display for digital and UNIStim endpoints. • DDS: Delay Display calling party information after the call is answered. • TDD: Tandem Digit Display for all digital endpoints except 2006, 2008, 2216, and 2616. • NDD: No Digit Display.	The default value in CS 1000 depends on the station type: • ADD for 2x16 and 2008. • TDD for digital 39xx. • NDD for 2006.
CCSA/CCSD	• CCSA: Controlled Class of Service Allowed • CCSD: Controlled Class of Service Denied	Controlled Class of Service Denied
CNDA/CNDD	• CNDA: Call Number Display Allowed • CNDD: Call Number Display Denied	Call Party Name Display Allowed
CRPA/CRPD	• CRPA: Corporate Directory Allowed • CRPD: Corporate Directory Denied	Corporate Directory Denied

Table continues…

Comments on this document? infodev@avaya.com

CS 1000 Class of Service (CoS)	Feature name/Description	Default value
CNUD/CNUS/ CNUA/CNAA	• CNUD: CLASS Calling Number Multiple Data Format CLID and Message Waiting Lamp for analog CLASS sets Denied. • CNUS: CLASS Calling Number Single Data Format Allowed Display calling number along with date and time in single data message format for analog CLASS sets. • CNUA: CLASS Calling Number Multiple Data Format Display calling number along with date and time in multiple data message format for analog CLASS sets. • CNAA: CLASS Calling Name Multiple Data Format Applies along with CNUA. Display calling number, calling name, and date and time in multiple data message format for analog CLASS sets.	CLASS Calling Number Multiple Data Format
CRA/CRD	• CRA: Continues Ringing Allowed for analog sets. • CRD: Continues Ringing Denied for analog sets.	Continues Ringing Denied
GRLA/GRLD	• GRLA: Group Listening Allowed • GRLD: Group Listening Denied	Group Listening Denied
HFA/HFD	• HFA: Hands-Free Allowed • HFD: Hands-Free Denied The CS 1000 Hands-Free Allowed provides the speakerphone capability.	Hands-Free Denied

Table continues…

CS 1000 Class of Service (CoS)	Feature name/Description	Default value
HTL	HTLxx<HTL-specific parameters> Mnemonics for Hotline buttons emulated using the brdg-app (Hotline 2-way) or autodial (Hotline One-way) buttons. Depending on your requirements, you can use any of the four possible mnemonics: • HTLxxNyyy • HTLxxMkNyyy • HTLxxLyEzzz • HTLxxMkLyEzzz Where: xx - key number (from 0) on button module (or main module), y - button module number 1/2/3, yyy - destination number, y - AD List number in CM station - 1/2/3, zzz - corresponding AD List entry number. • For example: HTL2N100123 – assign Hotline key on button 2 of main button module, with target number 100123 • For example: HTL4M1N15132288888 – assign Hotline key on button 4 of button module 1, with target number 15132288888 • For example: HTL5M0L1E01 - assign Hotline key on button 5 of main button module, with target number set to CM station Abbreviated Dialing List#1 entry 01.	No hotline key

Table continues…

CS 1000 Class of Service (CoS)	Feature name/Description	Default value
HTLI	HTLIxx<HTLI-specific parameters>

Mnemonic to implement the CS 1000 Hotline Intercom feature in Device Adapter. Use the bridged appearance and the HTLI mnemonic to implement the Hotline Intercom feature.

Depending on your requirements, you can use any of the eight possible mnemonics:

• HTLIxxNyyyy

• HTLIxxNyyyyFffff

• HTLIxxMmNyyyy

• HTLIxxMmNyyyyFffff

• HTLIxxLaEbbb

• HTLIxxLaEbbbFffff

• HTLIxxMmLaEbbb

• HTLIxxMmLaEbbbFffff

The format is:

HTLIxx[Mm][Nyyyy][LaEbbb][Fffff]

Where,

• xx: Is the button number.

• m: Is the optional Key Expansion Module (KEM) number.

• yyyy: Is the Hotline number.

• a and bbb: Are the list and entry number if you want to use Abbreviated Dialing.

• ffff: Is for an optional filter to filter the inbound calls by CLID.

  The CLID of an inbound call is considered a match if it contains the string that you specify in ffff.

  For example, CLID 12345678 is considered a match for the filter 2345.

  If you configure the CLID filter in the HTLI mnemonic, then:

  - For an inbound call that has a matching CLID, Device Adapter provides a single buzz tone and auto-answers the call. | No hotline intercom key |

Table continues…

CS 1000 Class of Service (CoS)	Feature name/Description	Default value

	- For an inbound call that does not have a matching CLID, Device Adapter provides a ring tone but does not auto-answer the call.
	
	If you do not configure the CLID filter in the HTLI mnemonic, Device Adapter auto-answers all inbound calls.
	
	The following is an example of a boss/secretary intercom scenario using the HTLI mnemonic:
	
	• Phone A: ext1001, button 2 – bridg-app to X-port 2001
	
	  mnemonic: HFA HTLI2N2002F2002
	
	• Phone B: ext1002, button 2 – bridg-app to X-port 2002
	
	  mnemonic: HFA HTLI2N2001F2001
	
	For more information, see "Hotline Intercom" in "Appendix H: Call processing features and services."	

LNA/LND	• LNA: Last Number Redial Allowed • LND: Last Number Redial Denied	Last Number Redial Denied
LPA/LPD	• LPA: Lamp Allowed Message Waiting Lamp allowed for analog non-CLASS sets. • LPD: Lamp Denied Message Waiting Lamp denied for analog non-CLASS sets.	Lamp Denied
MUTA/MUTD	• MUTA: Mute Allowed • MUTD: Mute Denied	Mute Denied
MWA/MWD	• MWA: Message Waiting Allowed • MWD: Message Waiting Denied	Message Waiting Denied

Table continues…

CS 1000 Class of Service (CoS)	Feature name/Description	Default value

SCK / SCB	• SCK: Speed dial soft key
	
	• SCB: Speed dial feature key
	
	Mnemonics for Speed Call soft keys and feature keys.
	
	• To assign a Speed dial soft key, assign SCK[UC]X where U stands to Speed Call User, C - Speed Call Controller, X - AD List number in CM station - 1/2/3.
	
	  For example: SCKU2
	
	• To assign a Speed dial feature key, assign SCBxx[UC]z or SCBxxMy[UC]z where U stands to Speed Call User, C - Speed Call Controller, xx - key number (from 0) on button module (or main module), y - button module number 1/2/3, z - AD List number in CM station - 1/2/3.
	
	  - For example: SCB10U2 – assign speed call user key on button 10 of main button module, linked to CM station Abbreviated Dialing List #2
	
	  - For example: SCB5M2C3 – assign speed call controller key on button 5 of button module 2, linked to CM station Abbreviated Dialing List #3
		No speed dial key

VOLA/VOLD	• VOLA: Virtual Office Login Allowed Setting VOLA enables the Virtual soft key on the phone. • VOLD: Virtual Office Login Denied Setting VOLD disables the Virtual soft key on the phone. ✳ **Note:** If VOLA is present in the features, then it will be On automatically. To turn VOLA off from CS 1000 configuration, use VOLD. For Device Adapter, you have to delete VOLA from the phone programming.	The default value in CS 1000 is VOLD because the absence of VOLA means login is not allowed. Device Adapter does not use VOLD.

Table continues…

CS 1000 Class of Service (CoS)	Feature name/Description	Default value
VOUA/VOUD	• VOUA: Virtual Office User Allowed Setting VOUA allows the extension to use as user ID for Virtual Office operation. • VOUD: Virtual Office User Denied Setting VOUD does not allow an extension to use as user ID. ✱ **Note:** If VOUA is present in the features, then it will be On automatically. To turn VOUA off from CS 1000 configuration, use VOUD. For Device Adapter, you have to delete VOUA from the phone programming.	The default value in CS 1000 is VOUD because the absence of VOUA means user ID is not allowed for Virtual Office operation. Device Adapter does not use VOUD.
WTA/WTD	• WTA: Warning Tone Allowed • WTD: Warning Tone Denied	Warning Tone Allowed

Appendix B: Set time zone and DST for endpoints

Setting time zones and DST for endpoints in a different time zone

About this task

Use this procedure to set a time zone and daylight saving time (DST) on each endpoint that is physically in a different time zone to the main site.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Service Profiles**.

2. Click **New**.

3. In the **Identity** section, do the following:

   a. In the **Name** field, enter a descriptive name for the Service Profile.

   b. In the **Description** field, enter a description for the Service Profile.

4. In the **Available Service to Add to this Service Profile** list next to the **Name** of the service, do one of the following:

   • To add the latest version of the service, click the plus **+** sign.

   • To add an alternate version of the service, click **Advanced**. In the **Add Service-Advanced** dialog box, in the **Service Version** field, select the version, and then click **Add**.

5. Click **Commit**.

6. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

7. On the **Services Profiles** tab, do the following:

   a. In the **Profile** field, click the required profile.

   b. In the **Service** field, click **DeviceAdapter**.

8. In the **Media Security** area, do the following:

   a. Select the **Override default** check box.

      b. In **Effective Value**, click the appropriate SRTP level based on the location security requirement.

9. In the **Daylight Saving Rules** area, do the following:

      a. In the **Daylight saving enabled** field, select the **Override default** check box.

      b. In **Effective Value**, click **Yes**.

      c. In the **Start weekday**, **Start day**, **Start time**, **Stop weekday**, **Stop day**, **Stop time**, and **Offset** fields, select the corresponding **Override default** check box.

      d. In **Effective Value** corresponding to these fields, configure the daylight saving settings that applies to the country the endpoint is located in.

10. Click **Commit**.

11. On System Manager, click **Users** > **User Management** > **Manage Users**.

12. Select the user profile in the list, and then click **Edit**.

    The snap-in displays the User Profile page.

13. Click the **Communication Profile** tab and do the following:

      a. Click **Avaya Breeze® Profile**.

      b. In the **Services Profile** field, select the same service profile name as selected in Step 4.

14. Click the **Identity** tab and do the following:

      a. In the **Time Zone** field, click the required time zone.

      b. Click **Commit**.

Example

The following is an example on how Device Adapter applies the daylight saving offset time.

In the following screen shot, the **Start weekday** is set to **Sunday**, the **Start day** is set to March 24, and the **Start time** is set to 2:00 AM.

Device Adapter applies the daylight saving offset time for the endpoint that is located in the time zone that you specified in the **Time Zone** field as follows:

- If this day is March 24, Sunday in the given time zone, then Device Adapter applies the daylight saving offset time on this day after 2:00 AM.

- If March 24, Sunday is already past in the given time zone, then Device Adapter applies the daylight saving offset time on the next Sunday.

Daylight Saving Rules

8 Items			
Name	**Override Default**	**Effective Value**	**Description**
Daylight saving enabled	✔	Yes ⌄	
Start weekday	☐	Sunday ⌄	The first weekday on or after start date.
Start day	✔	03/24	The date after which to apply the offset. Supported format: MM/DD.
Start time	☐	02:00	The time after which to apply the offset. Supported format: HH:MM.
Stop weekday	☐	Sunday ⌄	The first weekday on or after stop date.
Stop day	✔	10/24	The day after which to remove the offset. Supported format: MM/DD.
Stop time	✔	03:00	The time after which to remove the offset. Supported format: HH:MM.
Offset	☐	1	The time offset in hours from local standard time. Supported values: 1-2.

Appendix C: Device Adapter Integration Unit commands

Device Adapter IU commands for IP phones

The topics in this section provide information about the Device Adapter Integration Unit (IU) commands that you can use to manage IP phones.

Related links

[Device Adapter administration in System Manager](#) on page 192

IP phones Maintenance and Reports page command descriptions

This topic contains information about the IP phones maintenance commands that are available on the Maintenance and Reports page. The Maintenance and Reports page is available on the System Manager web interface in **Elements** > **Device Adapter** > **IP Phones** > **Maintenance and Reports**.

Phone related

Command name	Description
isetCount	Shows the total number of registered sets based on the query that you run.
isetFWGet	Shows a list of IP phones firmware based on the query that you run.
isetGet	Shows a list of IP phones based on the query that you run.
isetNATShow	Shows general information for all sets behind a NAT router or given IP | TN.
isetReset	Resets the registered IP set.
isetResetAll	Resets all registered IP sets.
isetSecGet	Shows a list of IP phones based on the query that you run.
isetSecShow	Shows UNIStim encryption related information for all registered sets or IP | TN.
isetSecShowByIP	Shows UNIStim encryption related information for all registered sets, sorted by IP.

Table continues…

Command name	Description
isetSecShowByTN	Shows UNIStim encryption related information for all registered sets, sorted by TN.
isetSecUpdate	Re-configures S1/S2 ports and action bytes on the phones based on the query that you run.
isetShow	Shows general information for all registered sets or given IP | TN.
isetShowByIP	Shows general information for all registered sets, sorted by IP.
isetShowByTN	Shows general information for all registered sets, sorted by TN.
isetInfoShow	Shows the DHCP configuration and iset information for the specified IP set.
isetFWShow	Shows general information about firmware of all registered sets.
cookieRegShow	Shows the cookie registry information.
cookieShowByName	Shows the list of sets with a particular cookie set.
cookieShowByTN	Shows the cookie list for a set specified by TN.
dsetDelayHookswitchSet	Sets the Type value. For example, 2004P2, 2050PC, and 2004P1.

Maintenance

Command name	Description
disTPS	Line TPS gracefully switches the registered sets to the other servers located in the same cluster.
disiTPS	Line TPS gracefully switches the registered idle sets to the other servers located in the same cluster.
enlTPS	Enables the line TPS application and accepts set registrations.
itgAlarmTest	Generates ITGXXXX test alarms.
forcedisTPS	Forces to unregister all registered sets (on local server) and disables TPS.
loadBalance	Line TPS application attempts to balance the registration load of sets between this server and the rest of the cluster servers.
tpsSOCmdStatusShow	Shows the TPS Service Switch Over Command status.
echoServerShow	Shows general information about the Echo Servers that are used for NAT traversal feature, including the number of requests sent by this system.
elmShow	Shows the list of supported languages.
itgCardShow	Displays the card role, TLAN IP addresses, system information and location, status, and up time.
tpsInfoShow	Shows the status of the TPS.
tpsShow	Shows the TPS information.

Security

Command name	Description
tpsReloadCrls	Reloads the certificate revocation lists used by the TPS Service.
tpsShowCrls	Shows the certificate revocation lists used by the TPS Service.
csvReloadCrls	Reloads the certificate revocation lists used by the CSV Service.
csvShowCrls	Shows the certificate revocation lists used by the CSV Service.

Remote phone diagnostics

Command name	Description
eStatShow	Shows the Ethernet statistics for the specified IP set.
RTPStatShow	Shows the most recent RTCP statistics information for given IP | TN.
RTPTraceShow	Shows the RTCP statistics information periodically for the number of polling period. If this parameter is not specified, the default is until the end of the call.
RTPTraceStop	Stops the previously run RTPTraceShow command for an IP set.
rPing	Requests the IP set to ping an IP address. The count parameter of this command indicates the number of successful attempts the set should initiate.
rPingStop	Requests the specified IP set to stop pinging.
rTraceRoute	Requests the specified IP set to trace route an IP address.
rTraceRouteStop	Requests the IP set to stop tracing route an IP address.
RUDPStatShow	Shows RUDP/UNIStim statistics for specified IP set.

Firmware download

Command name	Description
umsPolicyShow	Displays the current upgrade policy.
umsUpgradeAll	Upgrades all registered sets according to the policy and firmware file at a given time. Example for time format is 14:00.
umsUpgradeTimerCancel	Cancels the scheduled upgrade.
umsUpgradeTimerShow	Shows the upgrade schedule.
umsCreatePolicy	Creates a new policy.
umsDeletePolicy	Deletes a policy.
umsSetPolicy	Assigns policy for the particular firmware.
umsSetPolicyProtocol	Sets protocol for a policy.
umsSetPolicyRetries	Sets the number of retries for a policy.
umsSetPolicyUpgradeType	Sets the upgrade type for a policy. Upgrade type can be: UPGRADE, DOWNGRADE, REFRESH, NEVER, FULLVERSION, and ANY.
uftpAutoUpgradeTimeoutSet	Sets a user response time out for postponed firmware upgrade.

Table continues…

Command name	Description
uftpNodeShow	Shows the IP telephone firmware download summary of a node.
uftpRunTimeDataReset	Resets the run-time data field in the UFTP data block.
uftpShow	Shows the IP telephone firmware download information.
uftpSpeedLimitSet	Configures the bandwidth parameters for firmware download by using the UFTP protocol.
uftpSpeedLimitShow	Shows the current bandwidth parameters for firmware download by using the UFTP protocol.
uftpTurboModeShow	Shows the firmware download Turbo Mode information.
uftpTurboMode	Schedules the Turbo Mode.
uftpTurboModeTimeoutSet	Sets the firmware download Turbo Mode idle time out for this SS. It automatically exits the Turbo Mode if there are no active upgrade jobs during MM minutes. Where SS and MM are the abbreviations from the following format:

Time Format	Template	Example
MTIME	MM:SS.ss	91:17.01
TIME	hh:MM:SS.ss	01:31:17.01
DTIME	DD HH:MM:SS.ss	00 04:31:17.01

UNIStim

Command name	Description
usiGetPhoneRudpSettings	Gets the RUDP Max Retries Counts and RUDP Timeout values for all IP set types.
usiSetPhoneRudpRetriesByITType	Sets the RUDP Max Retries Count for IP sets of the specified \"SetType\" to [Value].
usiSetPhoneRudpTimeoutByITType	Sets the RUDP Timeout value for IP sets of specified \"SetType\" to [Value] in milliseconds.

Loss plan

Command name	Description
UKLossPlanClr	Sets the IP Phone's loss plan to default values.
UKLossPlanSet	Sets the IP Phone's loss plan to UK specific values.
lossPlanClr	Sets the IP Phone's loss plan to default values.
lossPlanPrt	Prints the offsets and current values for handset, headset, and handsfree RLR and SLR.
lossPlanSet	Adjusts the levels of a given transducer by using the given RLR and SLR offsets.

Appendix D: Remote IPE cabinets

Fiber Remote IPE and Carrier Remote IPE

Floor-standing Fiber Remote IPE cabinet

You can install an MG-XPEC card on a floor-standing Fiber Remote IPE cabinet. The MG-XPEC card allows users served by a floor-standing Fiber Remote IPE cabinet to connect to Device Adapter. The MG-XPEC card replaces the Fiber Controller card on the floor-standing Fiber Remote IPE cabinet.

Wall-mounted Fiber Remote IPE cabinet

You cannot retrofit a wall-mounted Fiber Remote IPE cabinet with an MG-XPEC card.

Avaya recommends a G4XX gateway solution to allow users of a wall-mounted Fiber Remote IPE cabinet to connect to Device Adapter.

Floor-standing Carrier Remote IPE cabinet

You can install an MG-XPEC card on a floor-standing Carrier Remote IPE cabinet. The MG-XPEC card allows users served by a floor-standing Carrier Remote IPE cabinet to connect to Device Adapter. The MG-XPEC card replaces the Remote Carrier Interface card on the floor-standing Carrier Remote IPE cabinet.

Wall-mounted Carrier Remote IPE cabinet

You cannot retrofit a wall-mounted Carrier Remote IPE cabinet with an MG-XPEC card.

Avaya recommends a G4XX gateway solution to allow users of a wall-mounted Carrier Remote IPE cabinet to connect to Device Adapter.

Mini-Carrier Remote IPE cabinet

You can replace the Remote Mini-carrier Interface (RMI) card with the CS 1000E Media Gateway Controller (MGC) card to allow the users of the remote site to connect to Device Adapter.

Trunk cards, such as the Universal Trunk card, are not supported. You can use G4xx gateway solution to meet the local trunk requirements.

Related links

Appendix E: Mnemonics and button labels

Mnemonics

This section provides the Mnemonics that are used in Device Adapter. These mnemonics are mostly used for the features (CS 1000; classes of service).

The following Mnemonics, except POA and POD, are entered in the **Features** field. For more information, see Administering a mnemonic on page 339.

They may also have a specific assigned button for the service, which is configured separately. The remainder map directly to a Communication Manager feature or service.

Generic Station Mnemonics

Mnemonic	Name	Comments
CCSA CCSD	Controlled Class of Service Allowed. Controlled Class of Service Denied.	
CNDA CNDD	Calling / Called Number Display Allowed. Calling / Called Number Display Denied.	Only valid on a CLASS analog station or digital and UNIStim stations. Implicit: If names are configured, Calling/called Party Name Display parallels CNDA/CNDD.
FNA FND	Call Forward No-answer Allowed. Call Forward No-answer Denied.	
HTA HTD	Hunting Allowed. Hunting Denied.	Call forward on busy to the Hunt extension.
MWA MWD	Message Waiting Allowed. Message Waiting Denied.	This station is allowed voice mail. The mailbox extension needs to be configured.

Table continues…

Comments on this document? infodev@avaya.com

Mnemonic	Name	Comments
PUA DPUA GPUA	Call PickUp Allowed. Used for calls to users in the group. Directory number Call PickUp Allowed. Used to pick up calls at a specific extension. Group Call PickUp Allowed. Used to pick up calls from a nearby group.	
WTA WTD	Warning Tone Allowed. Warning Tone Denied.	

Analog Station Mnemonics

Mnemonic	Name	Comments
CNUA CNUS CNAA CNUD	CLASS Calling Number Multiple Data String Format Allowed. CLASS Calling Number Single Data String Format Allowed. CLASS Calling Name Multiple Data String Format Allowed. CLASS display denied.	
DIP DTN	Dial Pulse Digit Tone - DTMF digits	Analog station digit transmission.
LPA LPD	Lamp Allowed. Lamp Denied.	
MCRA	Multiple Call Arrangement Allowed.	Analog stations are by default Single Call Arrangement, but this class of service over-rides that setting.
XFA (XFD) (XFR)	Transfer Allowed. Transfer Denied. The absence of XFA on Device Adapter implies XFD. Transfer Restricted by feature incompatibility.	

Digital and UNIStim Station Mnemonics

Mnemonic	Name	Comments
AAA	Auto-Answer Allowed.	

Table continues…

Mnemonic	Name	Comments
ADD	Automatic Digit Display.	
DDS	Delay Display until call is answered.	
TDD	Tandem Digit Display. Allow redirection information.	
NDD	No Digit Display. Only applicable for digital or UNIStim stations without a display.	
CRPA	Corporate Directory Allowed.	
CRPD	Corporate Directory Denied.	
HFA	Hands-free Allowed. If a headset is configured, headset is also allowed.	
HFD	Hands-free Denied.	
LNA	Last Number redial Allowed.	
LND	Last Number redial Denied.	
POA	Privacy Over-ride Allowed. Turn off privacy for the active call.	
(POD)	Privacy Over-ride Denied. Implicit in Device Adapter without the POA feature.	

Administering a mnemonic

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the endpoint for which you want to administer the mnemonic, and then click **Edit**.

5. On the Edit Endpoint page, click the **General Options** tab.

6. In the **Features** field, type the mnemonic that you want to administer.

   You can specify up to 20 feature attribute strings. Use a space to separate each feature attribute string.

7. Click **Commit**.

Button labels

The Device Adapter user is familiar with the CS 1000 names and acronyms, and the underlying Communication Manager feature button name may be confusing. The feature button names and the corresponding Communication Manager names are translated in part by Device Adapter, but the names can be over-ridden by System Manager. This allows customized labels in multiple languages.

The button names and mapping of these names from CS 1000 to Communication Manager are described in the following table.

Mnemonic	Button name
NUL	CS 1000: No feature assigned
MWK	CS 1000: Message Waiting key
TRN	CS 1000: Transfer
	Communication Manager button: transfer
AO3	CS 1000: 3-party conference key
AO6	CS 1000: 6-party conference key
	Communication Manager button: conference
CFW	CS 1000: Call Forward key
	Communication Manager button: call-fwd
RGA	CS 1000: Ring Again key
	Communication Manager button: auto-cback
PRK	CS 1000: Call Park key
	Communication Manager button: Snap-in: park & page
RNP	CS 1000: Ringing Number pickup key
	Communication Manager button: call-pkup
SCU	CS 1000: Speed Call User
SSU	CS 1000: System Speed Call User
SCC	CS 1000: Speed Call Controller
SSC	CS 1000: System Speed Call Controller NP, NUL
	Communication Manager button: Autodial used, with the underlying Abbreviated Dialing Group list.
PRS	CS 1000: Privacy Release key
	Communication Manager button: exclusion

Table continues…

Mnemonic	Button name
SCA	CS 1000: Single Call Arrangement
	Only one call is allowed across all users and bridging into the call is allowed.
	Communication Manager button:
	• If the number is used on a single station only, the number should be a call appearance.
	• Otherwise, it is a bridged appearance of a specific line appearance.
MCA	CS 1000: Multiple Call Arrangement
	Every button can have its own call but bridging into the call is not allowed.
	Communication Manager button: This is a bridged appearance button with the parameter indicating "any line appearance."
SCN, MCN	CS 1000: SCA and MCA, non-ringing
SCR, MCR	CS 1000: SCA and MCA, ringing
	Communication Manager button: The button is configured as a call appearance or bridged appearance based on the SCA versus MCA option. Use the Active Station Ringing flag.

Appendix F: Infrastructure features and services

Endpoint registration

★ **Note:**

This section is applicable to UNIStim IP endpoints only.

Endpoint registration feature description

When an endpoint may power up, reboot, or carry out another operation requiring it to register to the Device Adapter, the following occurs:

- The endpoint tries to register.
  - The registration request is only sent if the set has a node ID and TN configured, and some mechanism to reach the servers. This may use DHCP or provisioned IP addresses.
  - The endpoint initiates UNIStim registration with the "Server 1".
  - If it is unable to register there and "Server 2" is configured on the endpoint, it will attempt to register with "Server 2".
  - If it has not yet registered, it waits a period and retries, starting with "Server 1".
- The Device Adapter load balancer assigns the request to a selected Device Adapter instance, based on keeping as even a loading as possible on the cluster.
- The Device Adapter instance initiates SIP registration with the Session Manager on behalf of the endpoint.
- The Session Manager registers the endpoint and sends the configuration information of the endpoint (key map, etc.) to the Device Adapter.
- The Device Adapter accepts the data and completes the UNIStim registration with the endpoint.

The Device Adapter follows the CS 1000 endpoint handling.

Password protection using the Node password (IP Phone Installer Password) controls who can change the TN on the IP Phone. The IP Phone Installer Password protection controls registration with a virtual line TN on the Call Server. The password can be set on the Device Adapter through

CLI commands such as nodePwdSet. The password is stored as plain text on the CS 1000 disk but encrypted on the Device Adapter.

When password protection is not enabled, a UNIStim IP Phone displays the node ID and Terminal Number (TN) of the IP Phone for five seconds as the IP Phone starts. When the password protection is enabled on the Device Adapter (or IP Line Gateway in the CS 1000), the node and password are displayed. If the data was already set, the phone waits for 5 seconds, and if the user does not begin changing anything, the registration proceeds.

The user may choose to configure the IP connectivity, Node ID, and TN of the endpoint during registration. If the Node is to be changed, the user does so. Otherwise, the user may change the TN.

If the control password is enabled, the user must enter that before changing the TN; on successful password entry the TN can change. If the password is disabled, the TN can be changed immediately.

If the Node password is configured on the Signaling Server, once the endpoint logs in the **IP Phone Telephone Options** > **Set Info** menu does not display the Set IP Information or Ethernet Information options.

❉ Note:

The Avaya Aura® SIP phone user enters an extension number and password during registration. It does not have a node and TN.

Prerequisites for endpoint registration on Device Adapter

The CLI commands `nodePwdSet`, `nodePwdEnable`, and `nodePwdDisable` are implemented on the **Avaya Breeze®** platform server to control the Node password. If the Node password is configured, the **IP Phone Telephone Options** > **Set Info** menu does not display the Set IP Information or Ethernet Information options. Unlike with the CS 1000, the password is stored hashed on the Device Adapter, and not as plain text.

It is assumed that the Device Adapter has been configured, as have the balance of the Aura network. Furthermore, the users have been configured in the Communication Manager and System Manager. Refer to the following for more information about the server-side operations:

- "Chapter 3: Migration from CS 1000 to Device Adapter"

  This applies for the migration of users from a CS 1000 to Device Adapter.

- "Chapter 5: Avaya Device Adapter Snap-in deployment"

  This applies for all cases of deploying the Device Adapter.

- "Chapter 7: Administration"

  This applies for administration of the Device Adapter itself and adding users to the Device Adapter.

User administration for endpoint registration

Except for provisioning the user on System Manager and ensuring that Session Manager and Communication Manager are correctly set up, there is no requirement for user administration specifically for endpoint registration.

However, ensure that the user is correctly configured in System Manager with the correct identity and Terminal Number (TN), allowing Session Manager to match the login request to the right station definition and route the handling as required to Communication Manager.

Registering the endpoint

About this task

The Device Adapter follows the CS 1000 registration process. The user may be required to configure the IP connectivity, Node ID, and TN of the endpoint during registration, or may choose to change the values already on the endpoint. This information is protected by the Node password if the password is enabled.
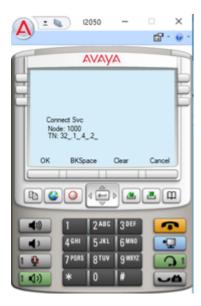
The UNIStim station typically is not a new install. It will have already been set up to run within the CS 1000 IP Line service. Therefore, the "change a node ID and TN" procedure is shown here. None the less, the same general procedure applies for a newly installed UNIStim endpoint.

A 2050 soft client is used for the illustrations; an endpoint with a smaller display may require switching across pages to carry out the same operations.

Procedure

1. Bring up the connection service data entry screen. Use one of the following:

   a. The station reboot password.

   b. Power cycling the endpoint. (For a 2050 soft client, close the application and re-open.)

   c. Disconnecting the endpoint from the LAN long enough to reboot.

   If the password is not required, the **Connect Svc** screen appears for 5 seconds.

Otherwise, the password is displayed instead of the TN.

2. Use the left arrow or right arrow to access the correct field to edit. For example, pressing the right arrow puts the cursor at the right-hand side of the first field (Node). Pressing the left arrow puts the cursor at the end of the "unit" of the TN.

3. Add the node ID if it is not available or edit the node ID if it is incorrect. **BKSpace** clears the last character, **Clear** will clear all characters, and **OK** accepts whatever is currently in the fields.

4. If required, enter the password and press **OK**.

5. If the password is not required, or the password was accepted, edit the TN. The field is formatted with the sub-fields aaa.bb.cc.dd. When the sub-field needs less than the full number of characters (for example, the "loop" 32 in the three character loop field), enter the data as mentioned earlier.

6. Press **OK** to log in. Several screens will slash in the display area as the different UNIStim and SIP messages are passed, but finally registration completes.

   The user's UNIStim endpoint is registered.

Media Gateway controller registration

⊛ **Note:**

This section is only applicable to digital and analog endpoints connected to a Media Gateway controller.

Media Gateway controller registration feature description

Use of the mnemonic MGC implies use of MGXPEC. Although the form factors are different, the handling is the same.

Registration of the MGC with Device Adapter is invisible to the end user. Registration with Session Manager is also invisible.

However, if the MGC fails to register or if a specific endpoint fails SIP registration, it is visible to the user.

Normally, the MGC registers with the server S1. If the registration fails, it tries to register to server S2. This continues until registration succeeds. However, until the registration succeeds, the endpoints are unable to do any call processing or service operations, unless those operations are totally within the station firmware.

The station is physically attached to the MGC and does not need to register with the MGC. Subsequently, Device Adapter attempts SIP registration on behalf of all possible Terminal Numbers (TN) on the MGC. The MGC does not know what has been provisioned, and therefore, Device Adapter cannot know. Device Adapter sends a request for the information.

If the SIP registration succeeds, then the endpoint at that TN exists in the programming. The details sent by PPM are transmitted to the station as applicable. For example, 39xx endpoints may get display information, but all stations that are time and date compatible will receive the time of day. Note that analog and digital 200X endpoints do not have button labels generated by programming. The analog stations do not have feature buttons and the digital 200X stations have paper labels.

If SIP registration for a TN fails, the most probable reason is that no station has been defined for that TN. If the station exists and System Manager has a station defined for that TN and the registration fails, the logs can indicate the reason for the failure. This can include having an invalid station type versus endpoint type. A digital endpoint cannot be programmed as an analog endpoint and vice versa. Further, a 39XX cannot be programmed as a 2616 or 2008, and so forth.

In all cases, if the registration is expected to succeed but fails, it typically means either a network failure or a configuration problem. If all endpoints fail to register, the network is the most probable problem. But, whenever a subset of the stations successfully registers while others do not, verify the endpoint configuration on System Manager or Communication Manager.

The registration depends on values in EEPROM of the MGC. It is easier to migrate by putting the original call server IP address on Device Adapter than to change the programming on the MGC. After initialization, the MGC establishes its proprietary communication path (PBX-link) towards the primary Device Adapter Cluster IP written in EEPROM (mgcsetup). The primary Device Adapter Cluster IP should be the former Call Server IP.

IPSec is used to secure the traffic.

MGC supports triple registration, that is, with a primary server, a secondary server, and usually a local back-up tertiary server. MGC always tries to register first to the primary. If that fails, it registers to the secondary (alternate 1) or tertiary (alternate 2). Typically, if the MGC is registered

to an alternate and the primary recovers or the link recovers, MGC re-registers to the primary. For Device Adapter, the server is the Device Adapter cluster and not a specific server.

After the PBX-link is established, Device Adapter performs load balancing to spread the endpoints as evenly as possible across Device Adapters in the cluster. If the Device Adapter load balancer decides that the MGC should be registered to another server, the MGC closes the PBX link connection and opens a new one with the Avaya Breeze® platform server IP provided to it.

MGC sends its loadware lineup to Device Adapter. Device Adapter may trigger a loadware upgrade at the MGC, to ensure that all devices are running current versions.

MGC then triggers configuration data upload. Device Adapter sends configuration files over SFTP and sends various parameters by using the PBX Link messages.

Later, if an administrator changes the configuration; for example, Attributes, Device Adapter sends the updated files to the registered MGCs and informs the MGCs about the update.

Unlike the UNIStim endpoints, MGC registers all its VGW (Voice Gateway DSP) channels with Device Adapter. As opposed to CS 1000, Device Adapter doesn't require VGWs to be pre-configured.

After this, the Status and Signaling Device (SSD) module is initialized. This permits signaling between Device Adapter and the physical endpoints to be complete. By using the SSD signaling, the CardLAN module starts detecting digital line cards (DLC) and analog line cards (ALC).

Device Adapter adopts the CS 1000 call server CardLan functionality:

- Enable or disable card or unit
- Card or unit parameter download

Device Adapter provides a way to enable or disable individual cards and units through Device Adapter Element Manager. The enabled status is stored on the MGC. Hence, it survives re-registration to another cluster.

If any card type other than ALC or DLC is detected, it will be ignored and an alarm is generated.

Related links

[Configuring Media Gateway Controllers](#) on page 126

Media Gateway Controller registration feature operation

There are no user visible feature operations. The device acts as an intermediary between the endpoint and Device Adapter, which modifies the endpoint handling to conform to a suitable SIP endpoint model.

Feature key labels feature description

Stations with paper labels

A subset of the endpoints with programmable buttons such as most digital stations, do not support downloading labels to the endpoints. The existing labels may be reused for most of the services and features. New labels may be required for others.

Stations with endpoint programmable, not downloadable labels

A small percentage of endpoint types such as 3903 and 3904 stations, allow a user to specify the language on the set, overriding the configuration passed down from the System Manager. This can change the displayed button labels, based on the labels provided with the selected language.

The selected language, if supported in the endpoint firmware, will translate a button label into the default label interpretation for that language. If the configured language changes to another of the languages supported by the firmware, the label changes to the default in the new language.

However, these endpoints typically also allow you to locally change the label on a button. For example, "Auto-dial 13035381357" can be relabeled as "George", and other labels can also be changed.

Refer to the user guide for any endpoints supporting this capability; for example, the *Avaya 3901, 3902, 3903, and 3904 Digital Deskphones User Guide* includes a section "Change a Feature Key label (M3902)" for the 3902, and "Change a Feature Key label (M3903 and M3904)" for the 3903 and 3904. The procedures are similar, but not identical.

Note that the 3901 is effectively a "paper label" station type. The user has a fixed feature button which is activated by pressing **Feature** and a feature number. These are recorded on a paper "Feature Card" on the front of the phone. Therefore, Transfer may be "<Feature> 1", Conference may be '<Feature> 2", Autodial 13035381357 may be "<Feature> 3", and so on.

About customizing stations from System Manager

The feature key label area displays a 10-character string for each of the feature keys. Each feature key includes the key label and an icon. The icon state can be on, off, or flashing. A telephone icon displays the status of the configured DN. Key labels are left-aligned for keys on the left side of the screen, and right-aligned for keys on the right side of the screen. To change the feature key label, press the Services key to access **Telephone Options** > **Change Feature** key label option. For more information about changing the feature key label, see the applicable *IP Deskphone User Guide*.

If a label is longer than 10 characters, the last 10 characters are displayed, and the excess characters are deleted from the string.

The endpoint requires localized data for the stations:

1. With programmable feature buttons, and

2. With the programmable buttons not using "paper labels".

Localization is at least partially outside the scope of the Device Adapter in this respect, as the custom labels are administered on the System Manager and passed down to the Device Adapter and endpoint. A Unicode label can successfully be sent to any station that has the correct firmware; sending a Chinese label, for example, to an endpoint whose firmware does not support Chinese will not work. Endpoints supporting Chinese have a reduced number of call information lines, allowing them to use "taller" characters. However, a custom label in Chinese may be loaded on a station that supports the Chinese language.

Supported CS 1000 endpoints

All buttons can have a customized label. The UNIStim phone screen displays 10 characters per label, 9 characters for 12xx sets. If no label has been defined, TPS provides default, localized labels.

★ **Note:**

This effectively includes only 11xx and 12xx UNIStim endpoints. 200X endpoints do not support feature key labels. 39XX endpoints store feature key labels locally.

Supported Communication Manager endpoints

Avaya Aura® SIP phones support custom button labels. The labels can be set on the phone interface, or by an administrator in the System Manager.

Administering feature key labels

About this task

Refer to the user guide for each phone type for on-endpoint administration of custom button labels for that station. The procedure to administer feature key labels for Device Adapter is same as that of CS 1000.

Consider the following conditions:

• Changing feature key labels for the prime DN (key 0 or button 1) is not supported. This aligns with the CS 1000 experience.

• It is possible to add labels from Communication Manager with the appropriate language set.

• Auto-dial buttons with no number programmed cannot be assigned a custom label.

• Speed call feature key is configured as an Auto-dial button in the Communication Manager station. If no number is configured for the button, the user cannot assign a custom label to the key.

Refer to System Manager administration documentation for the mechanisms used to relabel a service or feature name on a button. Note that this permits any feature key to be labeled internally

as the underlying Communication Manager button type, while maintaining the user visible label with the CS 1000 naming convention.

Procedure

1. Access the **Telephone Options** menu and select **Change FKL** (Change Feature Key Label).

   A message appears to select a key.

2. Type the new label text.

3. Click **Select** to confirm the new label.

Configuring feature key labels

About this task

Refer to the user guide for each phone type for on-endpoint operations using custom button labels for that station.

Device Language Support

Device language support feature description

Each station with an alphanumeric display can display words as well as numbers. Setting the language allows the station to display the correct button labels, date display, and other information in the local language.

The languages available on CS 1000 include the following:

Arabic	Czech	Simplified Chinese	Traditional Chinese
Danish	Dutch	English	Finnish
French	German	Greek	Hebrew
Hungarian	Italian	Japanese Kanji	Japanese Katakana
Swedish	Korean	Latvian	Norwegian
Polish	Portuguese	Russian	Spanish
Turkish			

These are packaged in groups of up to 10. However, languages depending on pictograms may not be supported on all stations, as they reduce the number of display lines available from three lines to two. Endpoints with two or less lines may be unable to provide a display.

Some of these languages are Unicode and are available only on certain supported sets. There is no change in support when used with a CS 1000.

Some Avaya Aura® languages are not supported by Device Adapter. These are Spanish (Latin America) and French (Canada). If one of these languages is configured for the user in System Manager, Device Adapter maps it to the supported Spanish or French language respectively.

Configuring the station language in System Manager

About this task

Unless migrated by the ProVision tool, the default language is English. Even though the language can be controlled by an administrator, options built into the firmware of the stations that support multiple language displays allow the user to change the language on the station.

The system administrator can change the language used on the station in either System Manager or Communication Manager.

Some Avaya Aura® languages are not supported by Device Adapter. These are Spanish (Latin America) and French (Canada). If one of these languages is configured for the user in System Manager, Device Adapter maps it to the supported Spanish or French language respectively.

Before you begin

Verify that the desired language is supported on the station. The IP and 39xx phones support a subset of the languages available in each firmware version.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.

2. On the Endpoints page, select the endpoint for which you want to configure the language, and then click **Edit**.

3. On the **Profile Settings** tab, in the **Language and Region** area, do the following:

   a. In the **Language** field, click the language that you want to configure for the endpoint.

      The **User Preferred Language** is set to the same language as specified in the **Language** field.

   b. In the **Language File In Use** field, click the language file.

4. Click **Commit**.

Device language support feature operation

This feature sets the default language for soft keys, time and date displays. For example, the word used as a name for a month.

Device language support feature interaction

The programmable button labels in Communication Manager and System Manager may change the name of a button from the default for that language. This interaction existed in CS 1000 as well, where the user can have a custom label for many keys.

Station types

This section contains information about the station types.

UNIStim stations

The following are the three families of UNIStim stations:

- IP 200X
- IP 11XX
- IP 12XX

IP 200X phones

These are the oldest UNIStim stations supported on Device Adapter. They may have different phases, but only the phases listed in this section are supported with Device Adapter. The earlier phases do not support RFC 2833; and therefore, cannot perform end-to-end digit transmission.

UNIStim 2001 phase 1 and 2 phones

Comments on this document? infodev@avaya.com

This phone is intended as the entry level UNIStim phone. It has the following capabilities:

- LCD display (2 line).

  - Information display (idle display and display during the call) as the top display line.

  - Four context-sensitive soft keys, with labels as the bottom display line.

- A single green Line key at bottom right.

- Volume bar, Release key, and Hold key.

- Message and Service keys.

- Message waiting lamp.

- Visual ringing indicator.

- Speaker. But there is no speaker button. Handsfree is done by pressing the line key while on hook.

UNIStim 2002 phase 1 and 2 phones

This is a more capable phone. It has the following capabilities:

- Four programmable feature keys.

- The station also allows the user to customize feature key labels with limitations.

- Four context-sensitive soft keys that provide access to a maximum of 10 features.

- LCD Display

  - The top two lines provide labels for the programmable buttons.

  - The second line from the bottom either shows the idle display or call information.

- The bottom line shows the current feature name for the soft key under the label.

• Hold, Release, Mute, Headset, and Speaker keys.

• Volume control bar

• Handsfree

- Speakerphone

- Headset port and headset key

• Six specialized fixed keys

- Quit

- Directory (Personal Directory)

- Message (Inbox)

- Services

- Expand to PC

• Integrated Ethernet Switch. Only one network port is required for phone and PC.

• Message Waiting Lamp and visual ring indicator.

The 2002 phone supports attaching one or more expansion modules to add the following:

• 24 additional buttons (one module).

• 48 additional buttons (two modules).

• The shift button does not control the expansion module. Each one has a single page.

UNIStim 2004 phase 0, 1, and 2 phones

This UNIStim phone is intended for professional worker. It is very similar in terms of capability to the 1140 UNIStim phone. Programmable line (DN) and feature key labels appear beside the key. Context-sensitive soft key labels appear directly above the key.

It has the following capabilities:

- Twelve programmable feature keys: Six (physical) user-defined feature key labels and six lines or features accessed by pressing the Shift key.

  - Because it has effectively twelve programmable keys, it is capable of multiple lines (up to twelve).

- The station also allows the user to customize feature key labels with limitations.
- Four context-sensitive soft keys that provide access to a maximum of 10 features.
- Large LCD Display (8x24 character).

  - The top three lines provide labels for the programmable buttons.
  - The next three lines show either the idle display or call information.
  - The bottom line shows the current feature name for the soft key under the label.

- Handsfree

  - Speakerphone
  - Headset port and headset key

- Volume control bar
- Hold, Release, Handsfree (Speaker), Mute, and Expand to PC keys.
- Six specialized fixed keys

  - Quit
  - Directory (Personal Directory)
  - Message (Inbox)
  - Shift or Outbox
  - Services
  - Copy

- Message Waiting Lamp and visual ring indicator

The 2004 supports attaching one or more expansion modules to add the following:

- 24 additional buttons (one module)
- 48 additional buttons (one module with the shift button or two modules)

UNIStim 2007 phones

Comments on this document? infodev@avaya.com

This phone is basically a 2004 phone with a touch screen for all buttons except the hold, release, mute, headset, speaker, and volume buttons. The navigation arrows were merged into a single rocker control.

Expansion Module for 200X UNIStim phones

The IP Phone Key Expansion Module (KEM) is a hardware component that connects to IP Phone 2002 and IP Phone 2004 and provides additional line appearances and feature keys.

Up to two IP Phone KEMs can be connected to an IP Phone 2002 or IP Phone 2004. The IP phones themselves support a maximum of 48 additional line or feature keys, which can be attained by using a single 24-key KEM and a shift key on the IP phone, or by using two IP Phone KEMs.

IP Phone 2002

The Shift key of the IP Phone 2002 is not functional for the KEMs. With one KEM, the IP Phone can have up to 24 additional line/feature keys. With two IP Phone KEMs, the IP Phone can have up to 48 additional line/feature keys.

IP Phone 2004
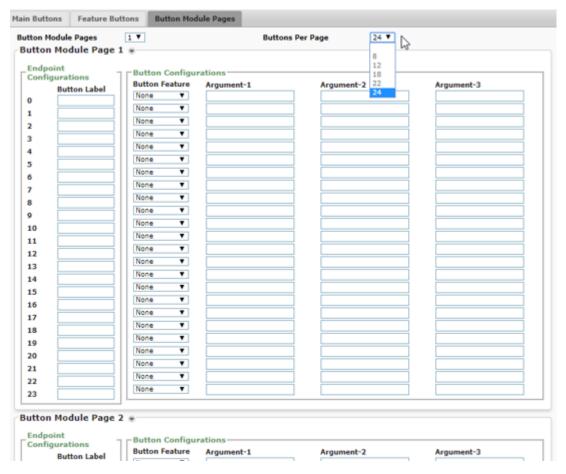
The IP Phone 2004 can have up to 48 additional line/feature keys by using a 24-key KEM and the Shift key functionality. With two IP Phone KEMs, the Shift key functionality does not affect the IP Phone KEMs because the maximum number of line/feature keys is already available.

Expansion Module: 24-key LCD KEM for 20xx series endpoints

- Up to 24 additional keys:
    - 2002: one KEM
        - CM endpoint configuration:
            - CS1000-Type=2002
            - Button Module Pages=1
            - Buttons-per-Page=24
    - 2004: one KEM
        - CM endpoint configuration:
            - CS1000-Type=2004
            - Button Module Pages=1. The Shift will still allow the KEM to have two pages.
            - Buttons-per-Page=24
- 25 to 48 additional keys:
    - 2002: two KEMs
        - CM endpoint configuration:
            - CS1000-Type=2002
            - Button Module Pages=2
            - Buttons-per-Page=24
    - 2004: one KEM, using Shift
        - CM endpoint configuration:
            - CS1000-Type=2004
            - Button Module Pages=2
            - Buttons-per-Page=24

                Note that the CM requires the second module page for the shifted module entries even though only one KEM is used.
    - 2004: two KEMs, if not using Shift
        - CM endpoint configuration:
            - CS1000-Type=2004
            - Button Module Pages=2
            - Buttons-per-Page=24

Note that each module is predefined with a size of 24 buttons, numbered 0 to 23 on the module.

Specify the data on the **Button Module Pages** tab:

- Page use:
  - The first KEM always uses data from Button Module Page 1. If the endpoint is a 2004 endpoint, it may also use a second page.
  - If two modules are used, the second KEM uses the data from Button Module Page 2.
  - If the station is a 2004 station that can use the Shift button and only one physical KEM is used, and when the KEM is shifted, the KEM uses the data from Button Module Page 2. Both modules must be configured.
- Button Label: Any custom label name.
- Button Feature: Select a compatible Communication Manager feature.
- Argument-1 through Argument-3: Provide the additional data as specified in the Communication Manager feature documentation.

IP 11XX phones

These are the most current UNIStim phones supported on Device Adapter, except for the 12xx series, which are intended to be a cost improvement. They may have different phases, but all phases support RFC 2833; and therefore, can provide end-to-end digit transmission.

UNIStim 1110 phone

*Note: If supported by your server, the Feature Status Lamp provides a user-defined alert. Contact your system administrator to find out if this feature is available for you.

This is a single line station, similar to an IP 2001 phone.

The following are the common features between 1110 and 2001 phones:

- LCD Display (2 line)
  - Information display (idle display and display during the call) as the top display line.
  - Four context-sensitive soft keys, with labels as the bottom display line.
- A single green Line key.
- Volume keys rather than volume bar. The volume keys perform the same function as the volume bar.
- Release key and Hold key.
- Message and Service keys.
- Message waiting lamp.
- Visual ringing indicator.
- Speaker. However, there is no speaker button. Handsfree is performed by pressing the line key while on hook.

In addition to the preceding features, the 1110 phone has the following capabilities:

- The navigation function with its up, down, left, and right navigation rocker provides improved menu options. The 2001 phone has only up and down. Both can scroll through the display.
- The feature status lamp. This has a narrow range of services for which it can be used and active.
- The Enter button at the center of the navigation rocker.

- The Expand to PC button.

UNIStim 1120 phone

The following are the common features between 1120 and 2002 phones:

- Four programmable feature keys.

- The station also allows the user to customize feature key labels, with limitations.

- Four context-sensitive soft keys that provide access to a maximum of 10 features.

- LCD Display

  - The top two lines provide labels for the programmable buttons.

  - The second line from the bottom shows either idle display or call information.

  - The bottom line shows the current feature name for the soft key under the label.

- Handsfree

  - Speakerphone

  - Headset port and headset key

- Volume keys rather than volume bar. The volume keys perform the same function as the volume bar.

- Hold, Release, Handsfree (Speaker), Headset, Mute, and Expand to PC keys.

- Six specialized fixed keys:

  - Quit

  - Directory (Personal Directory)

  - Message (Inbox)

  - Services

- Copy (not present on the 2002)

- Message Waiting Lamp and visual ring indicator

In addition to the preceding features, the 1120 phone has the following capabilities:

- Integrated Gigabit Ethernet Switch. Only one network port is required for phone and PC.

- USB port for accessories such as wireless headset, mouse, or keyboard.

- Wide-band audio if a third-party headset or handset that supports wide-band is connected.

- Most fixed keys with an LED indicator integrate that into the button, rather than having it elsewhere on the station.

- An Enter key at the center of the navigation rocker.

- The feature status lamp. This has a narrow range of services for which it can be used and active.

The 1120 supports attaching one or more expansion modules to add the following:

- 18 additional buttons (one module without Shift).

- 36 additional buttons (one module with Shift or two modules without Shift).

- 54 additional buttons (three modules without Shift).

UNIStim 1140 phone

* If supported by your server, the Data waiting message indicator provides a data alert.
Contact your system administrator to find out if this feature is available for you.

> **⁕ Note:**
>
> The 2050 soft client looks and acts effectively the same as the 1140 UNIStim phone. However, as a soft client it has an interconnection to the PC to consider. For example, unless the application is opened, it cannot process calls.

The 1140 phone has six programmable feature buttons with Shift, allowing twelve to be programmed, similar to the IP 2004 phone.

The following are the common features between 1140 and 2004 phones:

- Twelve programmable feature keys: Six physical lines or feature keys, and six lines or features accessed by pressing the Shift key.

  - Because it has effectively twelve programmable keys, it is capable of multiple lines up to twelve.

- The station also allows the user to customize feature key labels, with limitations.

- Four context-sensitive soft keys that provide access to a maximum of 10 features

- Large LCD Display (7x24 character)

  - The top three lines provide labels for the programmable buttons.

  - The next three lines show either idle display or call information.

  - The bottom line shows the current feature name for the soft key under the label.

- Handsfree

  - Speakerphone

  - Headset port and headset key

- Volume keys rather than volume bar. The volume keys perform the same function as the volume bar.

- Hold, Release, Handsfree (Speaker), Headset, Mute, and Expand to PC keys.

- Six specialized fixed keys:

  - Quit

  - Directory (Personal Directory)

  - Message (Inbox)

  - Shift or Outbox

  - Services

  - Copy. This not present on the 2004 phone.

- Message Waiting Lamp and visual ring indicator.

In addition to the preceding features, the 1140 phone has the following capabilities:

- Integrated Gigabit Ethernet Switch. Only one network port is required for phone and PC.

- USB port for accessories such as wireless headset, mouse, or keyboard.

- Wide-band audio if a third-party headset or handset that supports wide-band is connected.

- Most fixed keys with an LED indicator integrate that into the button, rather than having it elsewhere on the station.

- An Enter key at the center of the navigation rocker.

- The feature status lamp. This has a narrow range of services for which it can be used and active.

The 1140 supports attaching one or more expansion modules to add the following:

- 18 additional buttons (one module without Shift).

- 36 additional buttons (one module with Shift or two modules without Shift).

- 54 additional buttons (three modules without Shift).

UNIStim 1150 phones

The 1150 phone is optimized for call center use. As such, it can be used on Device Adapter, but until the call center capability is provided by Device Adapter, its use is limited.

UNIStim 1165 phones

* If supported by your server, the Feature Status Lamp provides a user-defined alert.
Contact your system administrator to find out if this feature is available for you.

The 1165 station has eight programmable feature buttons with Shift, allowing sixteen to be programmed. It has the same intent as the IP 2007 phone to provide an improved display (color) and access. However, it maintains the physical buttons instead of relying on a touch-sensitive screen.

The 1165 phone has the following capabilities:

- Sixteen programmable feature keys: Eight physical lines or feature keys, and eight lines or features accessed by pressing the Shift key.

  - Because it has effectively sixteen programmable keys, it is capable of multiple lines up to twelve.

    Note that the shifted set of programmable feature buttons appears on the feature keys list on Communication Manager and System Manager.

- The station also allows the user to customize feature key labels, with limitations.

- Four context-sensitive soft keys that provide access to a maximum of 10 features.

- Large high-resolution graphical color display. Nine lines of 24 characters as the normal display:

  - The top four lines provide labels for the programmable buttons.

  - The next three lines show either idle display or call information.

  - The bottom line shows the current feature name for the soft key under the label.

- Handsfree:

  - Speakerphone

  - Headset port and headset key

- Volume keys instead of the volume bar. The volume keys perform the same function as the volume bar.

- Hold, Release, Handsfree (Speaker), Headset, Mute, and Expand to PC keys.

- Six specialized fixed keys:

  - Quit

  - Directory (Personal Directory)

  - Message (Inbox)

  - Shift or Outbox

  - Services

  - Copy. This not present on the 2004 phone.

- Message Waiting Lamp and visual ring indicator.

- Two Integrated Gigabit Ethernet Switch ports. Only one network port is required for phone and PC.

- USB port for accessories such as wireless headset, mouse, or keyboard.

- Wide-band audio if a third-party headset or handset that supports wide-band is connected.

- Most fixed keys with an LED indicator integrate that into the button, rather than having it elsewhere on the station.

- An Enter key at the center of the navigation rocker.

- The feature status lamp. This has a narrow range of services for which it can be used and active.

Expansion Module for 11XX phones

On CS 1000, the expansion module (Graphical Expansion Module (GEM)), is supported on the following IP Phones:

- IP Phone 1120E

- IP Phone 1140E

- A soft client edition exists for the IP Soft Client 2050

The expansion module is a hardware accessory that connects to an IP Phone to provide additional line and feature keys. The module is a graphical expansion module with 18 self-labeling keys.

1140E with one GEM   1140E with two GEMs

The supported IP Phone 1100 series phones can support a maximum of three expansion modules at one time. This allows the IP Phone 1120E and IP Phone 1140E to have a maximum of 54 additional line or feature keys.

The phones support a maximum of 54 added keys. The following are the options:

- 1-18 keys added:

  - Single 18-key GEM with nothing programmed against the shifted page.

- 19-36 keys added:

  - Single 18-key GEM with the Shift key and a shifted page.

  - Two 18-key GEMs. The Shift key will have no effect.

- 37-54 keys added: Three 18-key GEMs. The Shift key will have no effect.

Expansion Module: 18-Key GEM for 11xx Series Endpoints

- Up to 18 additional keys:

  - Use one GEM.

- CM endpoint configuration:
  - CS1000-Type=1120, 1140
  - Button Module Pages=1
  - Buttons-per-Page=18

Because the administrator defined only the first 1 to 18 buttons, Shift will not provide any added buttons.

- 19 to 36 additional keys:
  - Using one GEM and Shift.
    - CM endpoint configuration:
      - CS1000-Type=1120, 1140
      - Button Module Pages=2
      - Buttons-per-Page=18

      CM requires the second module page for the shifted module entries. It is unaware that the second page is a shifted GEM page.

      Because this is a single GEM, the shifted key total is less than the maximum number of keys available.
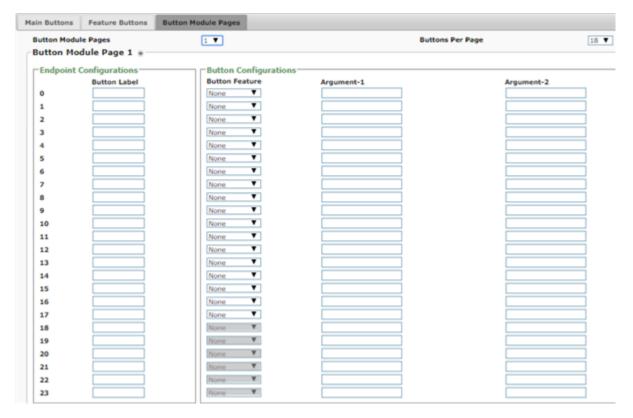
  - Using two GEMs.
    - CM endpoint configuration:
      - CS1000-Type=1120, 1140
      - Button Module Pages=2
      - Buttons-per-Page=18

      The Shift will not provide any added buttons. CS 1000 cannot use Shift on both GEMs because that exceeds the maximum button count for the station, and it cannot shift only one GEM.

- 37 to 54 additional keys:
  - Use three GEMs.
    - CM endpoint configuration:
      - CS1000-Type=1120, 1140
      - Button Module Pages=3
      - Buttons-per-Page=18

      The shift will not provide any added buttons.

The following image shows the button module page. The screen shows 24 buttons. However, only 18 out of the 24 buttons are available, which are buttons 0 through 17. The rest of the buttons are unavailable.

Note that each module screen is predefined with a size of 24 buttons, numbered 0 to 23 on the module. This represents the largest supported module size in Avaya Aura®. The buttons that are unavailable for use appear dimmed on the screen.

To navigate to the **Button Module Pages** tab, on System Manager, click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**, and then edit an endpoint. Click the **Button Assignment** tab.

Specify the data on the **Button Module Pages** tab:

- Page use:
  - The first GEM always uses data from Button Module Page 1. If more buttons than the base 18 are needed, the second page can be used.
  - If two modules are used, the second GEM uses the data from Button Module Page 2.
  - If the station can use the Shift button and only one GEM is used, and when the GEM is shifted, the GEM uses the data from Button Module Page 2. Although only one physical GEM is configured, Communication Manager considers them as two separate modules.
- Button Label: Any custom label name.
- Button Feature: Select a compatible Communication Manager feature.
- Argument-1 through Argument-3: Provide the additional data as specified in the Communication Manager feature documentation.

IP 12XX phones

The IP 12XX series is intended to be a cost reduction for customers, providing the same general service as the 11XX series, but more economically.

Some limitations apply. However, most limitations will not be noticed by the users. For more information, see the documentation for the 12XX series.

UNIStim 1210 phone

This station is basically the same as the 1110 phone, but with simpler and less expensive body, simplified button locations, four discrete direction arrows for navigation, and a number of other simplifications.

The Conference key which is a soft key on the 1110 phone is a fixed key on the 1210 phone.

The following are the common features between the 1210 and 1110 phones:

- LCD Display (2 line)

  - Information display (idle display and display during the call) as the top display line.

  - Four context-sensitive soft keys, with labels as the bottom display line.

- Volume keys

- Release key and Hold key

- Message and Service keys

- Message waiting lamp

- Visual ringing indicator

• Speaker

However, the 1210 phone has the following changes:

- The navigation function with its up, down, left, and right buttons replaces the navigation rocker.

- The Enter button is at the center of the navigation buttons and not at the center of the rocker.

- The Expand to PC button is labelled as Applications.

- Mute, Handsfree (speaker), and Headset keys are added.

- The single green Line key from the 1110 phone is omitted. The Handsfree and Headset keys perform the role when the user chooses to not use the handset.

UNIStim 1220 phone

This station is basically the same as the 1120 phone, but with simpler and less expensive body, simplified button locations, four discrete direction arrows for navigation, and a number of other simplifications.

The following are the common features between the 1220 and 1120 phones:

- Four programmable feature keys.

- The station also allows the user to customize feature key labels, with limitations.

- Four context-sensitive soft keys that provide access to a maximum of 10 features

- LCD Display

  - The top two lines provide labels for the programmable buttons.

  - The second line from the bottom shows either idle display or call information.

- The bottom line shows the current feature name for the soft key under the label.

- Handsfree

  - Speakerphone

  - Headset port and headset key

- Volume keys

- Hold, Release, Handsfree (Speaker), Headset, Mute, and Expand to PC (labelled as Applications) keys.

- Five specialized fixed keys:

  - Quit

  - Directory (Personal Directory)

  - Message (Inbox)

  - Services

  - The Copy key is omitted. The user must use the context-sensitive soft key instead.

- Message Waiting Lamp and visual ring indicator.

- Wide-band audio if a third-party headset or handset that supports wide-band is connected.

- Fixed keys with an LED indicator integrate that into the button.

However, the 1220 phone has the following changes:

- The navigation function with its up, down, left, and right buttons replaces the navigation rocker.

- The Enter button is at the center of the navigation buttons and not at the center of the rocker.

- Integrated 10/100 Mbps Ethernet Switch. Only one network port is required for phone and PC.

- The Conference key which is a soft key on the 1120 phone is a fixed key on the 1220 phone.

The 1220 phone supports attaching an expansion module to add up to 24 additional buttons (one module with Shift).

UNIStim 1230 phone

This station is somewhat of a hybrid of the 1140 and 1165 phones, with simpler and less expensive body, simplified button locations, four discrete direction arrows for navigation, and a number of other simplifications. However, it has ten programmable feature buttons, allowing up to 20 buttons to be programmed.

The 1230 phone has the following capabilities:

- Twenty programmable feature keys: Ten physical line or feature keys, and ten lines or features accessed by pressing the Shift key.

  - Because it has effectively twenty programmable keys, it is capable of multiple lines up to twenty.

- The station also allows the user to customize feature key labels, with limitations.

- Four context-sensitive soft keys that provide access to a maximum of 10 features.

- Large LED display. Eight lines of 24 characters:

  - The top five lines provide labels for the programmable buttons.

  - The next two lines show either idle display or call information.

  - The bottom line shows the current feature name for the soft key under the label.

- Handsfree

  - Speakerphone

  - Headset port and headset key

- Volume keys

- Hold, Release, Handsfree (Speaker), Headset, Mute, and Expand to PC (labelled as Applications) keys.
- Five specialized fixed keys:
  - Quit
  - Directory (Personal Directory)
  - Message (Inbox)
  - Shift or Outbox
  - Services
  - The Copy key is omitted. The user must use the context-sensitive soft key instead.
- Message Waiting Lamp and visual ring indicator.
- Wide-band audio if a third-party headset or handset that supports wide-band is connected.
- Fixed keys with an LED indicator integrate that into the button.

However, the 1230 phone has the following changes:

- The navigation function with its up, down, left, and right buttons replaces the navigation rocker.
- The Enter button is at the center of the navigation buttons and not at the center of the rocker.
- Integrated 10/100 Mbps Ethernet Switch. Only one network port is required for phone and PC.
- The Conference key which is a soft key on the 1110 phone is a fixed key on the 1230 phone.

The 1230 supports attaching an expansion module to add up to 24 additional buttons (one module with shift).

Expansion Module for 12XX phones

Including setups with the BCM, the 1200 series has two Key Expansion Modules (KEM). One has 12 keys and the other has 18 keys. CS 1000 supports only the 12 key model.

The 12-key module provides soft labels that are based on the registered configuration.

On CS 1000, the expansion module is supported on the following IP Phones:

- IP Phone 1220E
- IP Phone 1230E

The 12 key KEM can provide 12 keys without Shift or 24 keys with Shift. It is soft labelled.

12 Key KEM

The supported 1200 series IP phones can support a maximum of three expansion modules at one time. This allows the IP phones to have a maximum of 36 additional line or feature keys with up to three expansion modules.

On Device Adapter, the phones support a maximum of 36 added keys. The following are the options:

- 12 Key KEM:

    - 1-12 keys added: Single 12-key KEM, with nothing programmed against the shifted page.

    - 13-24 keys added: Single 12-key KEM, with Shift.

    - 13-24 keys added: Two 12-key KEMs, with nothing programmed against the shifted page.

    - 25-36 keys added: Three 12-key KEMs, with nothing programmed against the shifted page.

    - CS 1000 supports up to four modules and 48 buttons, but Communication Manager allows only three pages of button module buttons.

Expansion Module: 12-Key KEM for 12xx Series Endpoints

- Up to 12 additional keys:

    - Use one KEM.

        • The Shift will not provide any added buttons.

        • CM endpoint configuration:

            - CS1000-Type=1220, 1230

            - Button Module Pages=1

            - Buttons-per-Page=12

- 13 to 24 additional keys:
  - Using two KEMs
    - The Shift will not provide any added buttons.
    - CM endpoint configuration:
      - CS1000-Type=1220, 1230
      - Button Module Pages=2
      - Buttons-per-Page=12
  - Using one KEM and Shift
    - CM endpoint configuration:
      - CS1000-Type=1220, 1230
      - Button Module Pages=2
      - Buttons-per-Page=12

  Communication Manager requires the second module page for the shifted module entries. It is unaware that the second page is a shifted KEM page.

  Because this is a single KEM, the shifted key total is the same as the maximum number of keys available.

- 25 to 36 additional keys:
  - Use three KEMs
    - The Shift will not provide any added buttons.
    - CM endpoint configuration:
      - CS1000-Type=1220, 1230
      - Button Module Pages=3
      - Buttons-per-Page=12
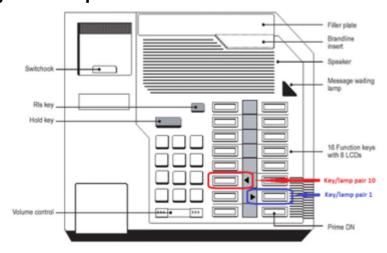
Digital stations

The digital stations include the following:

- The following sets are referred as the digital 200X stations. However, they are not all numbered 200x:
  - 2006, 2008, and two European variants – one column of keys with lamp indicators.
  - 2216, 2616, and a European variant – two columns of keys with lamp indicators.
- The following sets are referred as the 39XX stations:
  - 3901

- 3902

- 3903

- 3904

- 3905

Digital 200X phones

The 2XXX digital phones supported by Device Adapter were usually referred to as M2XXX phones because they were modular in design allowing the phone to be configured with and without different optional parts.

The most commonly added option was the display, which could present the time and date on one line, and the caller information on a second line. This was the only available display option. This option is not available in the 2006 phone.

When the station has the display module configured, the station is automatically assigned a specific key as a Program key. This Program key permits the user to change set features such as the display contrast.

The Meridian Communications Adapter can be used instead of the display, allowing other capabilities such as Group 4 fax. It requires the Program key.

 Note:

Fax is not supported on Device Adapter endpoints.

The fixed location buttons are limited to the following:

- Hold

- Disconnect (Release). This could also be used to abort an operation such as entering an autodial number.

- Volume up and down

All stations have the following:

- Message waiting lamp
- Speaker

For the lamps, the following LCD states are applied:

LCD state	Function
Off	The key or function is idle.
On (steady)	The key or function is active. If this is a line appearance for an outgoing call, the call may not yet have completed.
Flash (1 per second)	In progress; ringing.
Fast flash (2 per second)	1. Call is on hold. 2. Programming associated with this key is still in progress. 3. The feature key was pressed, but the required action is incomplete.

The LCD is shaped like a triangle pointing right for single column stations. Stations with two columns have a single LCD display between the columns of buttons, with the indicator LCD pointing towards the associated button.

Digital 2006 phone

The M2006 station is a single-line telephone with six programmable function keys.

The preceding picture shows an M2006 digital phone without the optional Meridian Communications Adapter. If the adapter is present, then the top key must be for the Program key. The Program key sets options for the adapter such as fax settings.

The 2006 phone has the following features:

- Six programmable keys:
  - The bottom right key (key 0) is the line appearance (DN) for this station.

- The remaining five key/lamp pairs can be assigned any feature that is not considered a DN such as Transfer, Call Forward, or Conference.

  - If a second key is assigned with any function associated with an extension, such as SCA, MCA, and two-way hotline, the station is disabled until this is rectified.

  - If the station has a display, key 5 is reserved for the Program key. Key 5 is the top key in the column.

- Optional Meridian Communications Adapter, permitting access by an RS-232-D interface.

- Volume bar

- Release key

- Hold key

- Speaker

- Message waiting lamp. This indicates voice mail status even without a mailbox key. It may be necessary to manually call into the voice mail system to retrieve messages.

Digital 2008 phones

The M2008 is a multi-line telephone with eight programmable function keys. The M2008HF contains an integrated Handsfree unit.

The picture in this topic shows an M2008 digital phone with the optional display. If the display or a Meridian Communications Adapter is present, then the top key on the right-hand button column (key 7) must be for the Program key. The Program key allows to set display options.

The 2008 phone had two variants: M2008 and M2008HF. The two variants are based on the presence (M2008HF) or absence (M2008) of handsfree.

The 2008 phone has the following features:

- Eight programmable keys:

    - The bottom right key, which is key 0, is normally the line appearance for this station.

    - The remaining seven key/lamp pairs can be assigned any feature such as Transfer, Call Forward, or Conference.

    - Optionally, one or more of the remaining seven key/lamp pairs can be assigned a DN.

    - If the station has a display or Meridian Communications Adapter, key 7 is reserved for the Program key. Key 7 is located at the top in the column.

- Optional display (2 line)

- Volume bar

- Release key

- Hold key

- Speaker

- Message waiting lamp. This indicates voice mail status even without a mailbox key. It may be necessary to manually call into the voice mail system to retrieve messages.

Digital 3110 (European) phone

The M3310 station is similar to the 2008 phone, but without handsfree.

The M3110 digital telephone supports the following features:

- On-Hook Dialing and Group Listening

- Dedicated Release and Hold keys

- Message Waiting and Mute Indicators

- Headset Socket

- 2 x 24 character display

- Eight feature keys including:

  - Program key

  - Seven system programmable keys:

    - The bottom right key, which is key 0, is normally the line appearance for this station.

    - The lower six of the remaining seven key/lamp pairs can be assigned any feature such as Transfer, Call Forward, or Conference.

    - Optionally, one or more of the six key/lamp pairs can be assigned a DN.

    - If the station has a Meridian Communications Adapter, key 7 is used for the Program key. Key 7 is located at the top in the column.

- Speaker for listening only

- Mute key

- Volume control for:

  - Handset

  - Ringing Tone

  - Buzz Tone

  - On-Hook Dialing and Group Listening

- Support for the following set options:

  - MCA data option to provide integrated voice and data.

  - External Alerter for high-ambient noise environments.

- This uses A-law and not mu-law by default.

Digital 3310 phone

The M3310 station is similar to the 2008HF (handsfree) with display.

The M3310 digital telephone supports the following features:

- Handsfree, On-Hook Dialing, and Group Listening

- Dedicated Release and Hold keys

- Message Waiting and Speaker/Mute Indicators

- Headset Socket

- 2 x 24 character display

- Eight feature keys including:

  - Program key

  - Seven system programmable keys:

    - The bottom right key, which is key 0, is normally the line appearance for this station.

    - The lower six of the remaining seven key/lamp pairs can be assigned any feature such as Transfer, Call Forward, or Conference.

    - Optionally, one or more of the six key/lamp pairs can be assigned a DN.

    - If the station has a Meridian Communications Adapter, key 7 is used for the Program key. Key 7 is located at the top in the column.

- Speaker key. This can be enabled or disabled.

- Mute key. This can be enabled or disabled.

- Volume control for:

  - Handset/Headset

  - Ringing Tone

  - Buzz Tone

  - On-Hook Dialing and Group Listening

  - Handsfree

- Support for the following set options:

  - MCA data option to provide integrated voice and data.

  - External Alerter for high-ambient noise environments.

  - Wall-mount ability.

- This uses A-law and not mu-law by default.

Digital 2216 phone

The preceding picture is of an M2216 digital phone with the optional display. If the display is present, then the top key on the right-hand button column (key 7) must be for the Program key. The Program key allows to set the display options. Note that the 2216 phone is intended for the call center environment and has a plug-in-headset that can be used for agent login and logout. Inserting or removing the headset logs in and logs out the agent at this station.

It has 16 keys (buttons) that can be configured as any of a number of features.

The bottom button, which is key 0, is always assigned as the call center extension and position ID. The other fifteen buttons can have any feature desired. However, normally one is transfer and another is conference. Some of the remaining keys are assigned call center functions such as call supervisor.

The LCD lamp beside the key shows nothing to indicate Off. A lit triangle pointing at the button indicates On. A flashing triangle is for different events such as ringing. The lamps are between the buttons, so half the triangles point left (the ones to the right of their buttons), while the other half point right.

The 2216 phone supports attaching one or more expansion modules to add the following:

• 22 additional buttons (one module)
• 44 additional buttons (two modules)

Digital 2616 phone

The preceding picture is of an M2616 digital phone with the optional display. If the display is present, then the top key on the right-hand button column (key 7) must be for the Program key. The Program key allows to set the display options. The 2616 phone is not intended for the call center environment, but can still be used in the call center environment.

If the 2616 phone is used in a call center environment, the call center position ID button can be used for agent login and logout. The station has a normal handset, so the call center option of logging in by using a headset is not available.

It has 16 keys (buttons) that can be configured as any of the number of features.

For call center operations, the bottom button (key 0) is always assigned as the call center extension and position ID. The other fifteen buttons can have any feature desired. However, normally one is transfer and another is conference. Some of the remaining keys are assigned call center functions such as call supervisor.

If the 2616 phone is not used for call centers, key 0 is the station extension and no call center feature buttons are configured.

The LCD lamp beside the key shows nothing to indicate Off. A lit triangle pointing at the button indicates On. A flashing triangle is for different events such as ringing. The lamps are between the buttons, so half the triangles point left (the ones to the right of their buttons), while the other half point right.

The 2616 phone supports attaching one or more expansion modules to add the following:

- 22 additional buttons (one module)
- 44 additional buttons (two modules)

Digital 3820 phone

The 3820 station is similar to the 2616 phone with display.

The M3820 Meridian digital telephone supports the following features:

- Handsfree, On-Hook Dialing, and Group Listening
- Dedicated Release and Hold keys
- Message Waiting and Speaker/Mute Indicators
- Headset Socket
- 2 x 24 character display
- 16 Feature keys including:
    - Store/program key located at key/lamp 7
    - 13 system programmable keys
        - Key 1 is typically the primary extension line appearance button.
        - Any or all of the remaining 12 keys can be line appearances.
    - Handsfree/speaker key can be enabled or disabled.
    - Mute key can be enabled or disabled.
- Volume control for:
    - Handset/Headset
    - Ringing Tone
    - Buzz Tone
    - On-Hook Dialing and Group Listening
    - Handsfree
- Directory/Caller's List with 9 dedicated keys namely:
    - Directory key: Located at the position that is usually occupied by the LCD for Key 0 at the bottom right column.
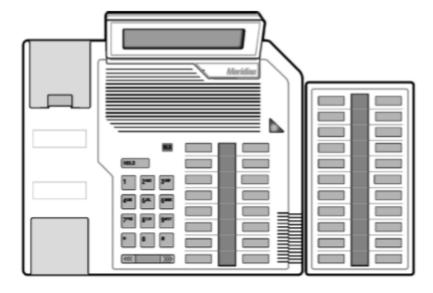
- Caller's List key: Located at the position that is usually occupied by the LCD for Key 8 at bottom left column.

- Delete key: Located at the position of Key 0 at the bottom right column.

- Edit key: Located at the position of Key 8 at the bottom left column.

- 4 cursor

- Dial: Located at the right of the navigation buttons.

• Support for the following terminal options:

- MCA data option to provide integrated voice and data.

- External Alerter for high-ambient noise environments.

- Wall-mount ability.

The 3820 supports attaching one or more expansion modules to add the following:

• 22 additional buttons (one module)

• 44 additional buttons (two modules)

These are functionally the same as the module attached to the 2616 phone, but are a different hardware variant intended for the European market.

Expansion Modules for 200X digital phone

Only the 16 key stations (2216, 2616, and 3820) support expansion modules. The model for the expansion module used on the M3820 differs from the 2x16 model number, but the user experience and programming are the same.

The supported expansion module, called the 22-key AOM or 22-key Add-On Module, has 22 key/ lamp pairs. It has paper labels or pre-printed button caps, with triangular LCD indicator in the strip between the two columns of keys indicating the state of the specific key.

M2216, M2616, and M3820 can support up to two of these modules, with up to 44 added keys.

The following are the options:

- 22 Key AOM:

  - 1-22 keys added: Single 22-key AOM

  - 23-44 keys added: Two 22-key AOMs

Expansion Module: 22-Key AOM for Aries Series Endpoints
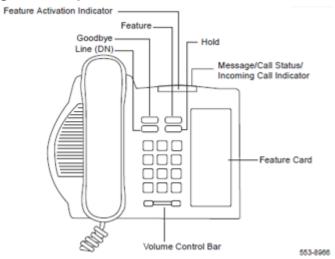
- Starting Key Number on first module: 16

- Up to 22 additional keys:

  - Use one AOM

  - CM endpoint configuration:

    - CS1000-Type=2216|2616|3820

    - Button Module Pages=1

    - Buttons-per-Page=22

- 23 to 44 additional keys:

  - Use two AOMs

  - CM endpoint configuration:

    - CS1000-Type=2216|2616|3820

    - Button Module Pages=2

    - Buttons-per-Page=22

Digital 39XX phones

The 3905 phone is supported. However, similar to the IP 1150 phone, the 3905 phone is created for the call center environment. Without the call center support by Device Adapter, its function and relevance is limited.

However, as with the 3904 phone, it supports the expansion modules to provide an increase in the number of usable buttons.

Digital 3901 phone

M3901 is a telephone with a single line key.

The M3901 phone operates in a different way than the other M3900 series digital phones. The M3901 phone supports five programmable features that are administered as keys: 1 through 5. Key 0 is the line key. The user activates the features by pressing the M3901 Feature Key, and then pressing the dial pad number key for that feature.

The system administrator programs the features for each M3901 phone. There is a feature card placed on the phone, which lists the features and instructions. The feature card is shown on the right-hand side of the phone in the preceding picture.
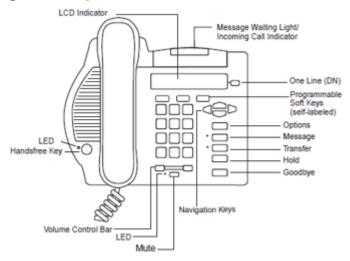
The M3901 phone has the following fixed keys:

- The line button (station extension or call appearance)
- Goodbye button
- Hold button
- Feature button (used as <feature + 1..5> to activate programmed feature
- Volume control bar

It has a feature activation indication lamp to inform the user that the feature is active. It also has a lamp for call states or idle state and for message waiting indication.

Most CS 1000 services can be provisioned against the five features. For example, the administrator can program the station with autodial, conference, transfer, call forward, and access to a speed call list. Line appearances are not allowed.

Digital 3902 phone

The M3902 phone has one Line (DN) Key and three Programmable Soft Keys (self-labeled).

The M3902 phone has the following fixed keys:

- The line button (station extension or call appearance)
- Goodbye button
- Hold button
- Mute button with an LED.
- Transfer button with an LED. This can be configured as either transfer or conference. These are the only features allowed on this button.
- Message waiting indication button and indicators.
- Handsfree button with an LED.
- Volume control bar
- Options button and navigation arrows
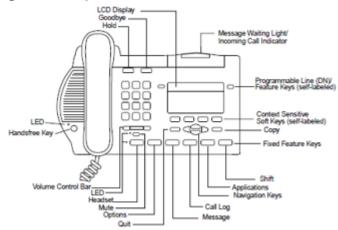
The three soft keys are configured by the administrator and are not context-sensitive.

The station also has an LCD display. This has two lines. The top line is used for the call information during a call or for idle station when idle. The bottom line shows the three features assigned to the soft keys.

The labels on the soft keys are set based on the firmware translation of the button function. It says autodial if the station's language is English, but it will change to another language supported for the station if administered by the system administrator or if the Options key is used to change the language.

However, the 3902 phone does not support receiving custom labels from System Manager.

Digital 3903 phone

The M3903 phone has two Programmable Line (DN)/Feature Keys (self-labeled) with two features or lines configured on each key. It also has four context-sensitive soft keys (self-labeled).
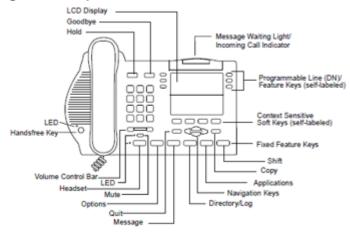
The M3903 has the following fixed keys:

- Two line or feature buttons, including for the station extension or call appearance, with a Shift button accessing two more buttons.

- Shift button

- Goodbye button

- Hold button

- Mute button with an LED

- Four context-sensitive soft keys

- Message waiting indication button and indicator

- Handsfree button with an LED

- Headset button with an LED

- Call Log button. The call log is internal and is not stored on Device Adapter.

- Copy button for moving callers to the personal directory.

- Quit button to terminate the call log related activities.

- Volume control bar

- Applications button

- Options button and navigation arrows

The station includes a four-line display. The top line indicates the currently active buttons from the programmable feature and line buttons. The middle two lines provide idle display and caller and called party information. The bottom line provides the soft key labels.

Call Join allows a user to create a conference with an existing caller and a second, incoming call. Note that the user requires a second line appearance on this station. Place the first call on hold, answer the second, and then create the conference.

Digital 3904 phone

The M3904 phone has six Programmable Line (DN)/Feature Keys (self-labeled), with two features or lines configured on each key. It also has four context-sensitive soft keys (self-labeled).

The M3904 phone has the following fixed keys:

- Six line or feature buttons, including for the station extension or call appearance, with a shift button accessing six more buttons.

- Shift button

- Goodbye button

- Hold button

- Mute button with an LED.

- Four context-sensitive soft keys.

- Message waiting indication button and indicator.

- Handsfree button with an LED.

- Headset button with an LED.

- Directory/Log button. Personal directory and call log are internal and are not stored in Device Adapter.

- Copy button to move callers to the personal directory.

- Quit button to terminate call log related activities.

- Volume control bar

- Applications button

- Options button and navigation arrows

The station includes a seven-line display. The top three lines indicate the currently active buttons from the programmable feature and line buttons. The middle three lines provide idle display, and caller and called party information. The bottom line provides the soft key labels.
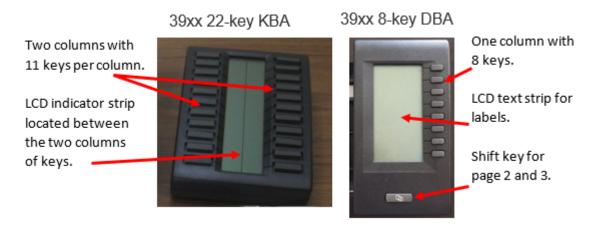
Call Join allows a user to create a conference with an existing caller and a second, incoming call. The user requires a second line appearance on this station. The user must place the first call on hold, answer the second, and then create the conference.

This station supports expansion modules.

The 3904 phone supports attaching one or more expansion modules to add:

- 24 additional buttons. One module with 8 keys and a Shift button paging through three screens.

- 22 additional buttons. One module with 22 keys.

- 44 additional buttons. Two modules with 22 keys each.

Expansion Module for 39XX digital phones

Only the 3904 and 3905 phones support the expansion modules.

The 22-key Key-Based Accessory (KBA) provides an additional 22 buttons per module. These use the same style as the AOM for the M2x16 and M3820, with the triangular icon to indicate feature status. The Shift is not used.

However, the smaller 8-key Display-Based Accessory provides only 8 physical buttons per module, but these buttons are soft labelled. This allows them to have three pages of entries, for 24 total added keys per module.

These modules can be configured for the 3904 and 3905 phones. Up to two KBA or one DBA expansion modules may be used. But they may not be mixed. Either Key-based modules or Display-based module must be used for all modules.

## Expansion Module: 22-Key KBA for 39XX series endpoints

- Starting Key Number on first module: 32

- Up to 22 additional keys:
    - Use one KBA.
    - CM endpoint configuration:
        - CS1000-Type=3904|3905
        - Button Module Pages=1
        - Buttons-per-Page=22
- 23 to 44 additional keys:
    - Use two KBAs.
    - CM endpoint configuration:
        - CS1000-Type=3904|3905
        - Button Module Pages=2
        - Buttons-per-Page=22

Expansion Module: 8-Key DBA for 39XX series endpoints

- The shift key is on the expansion module itself.
- Starting Key Number on first module: 32
- Up to 24 additional keys:
    - Use one DBA.
    - CM endpoint configuration:
        - CS1000-Type=3904|3905
        - Button Module Pages=3
        - Buttons-per-Page=8

Analog stations

Analog stations typically have either rotary dial digit entry or have a keypad. When they have the keypad, they may be provided with a switch to toggle between dial pulse and DTMF. Rotary dial phones are limited to dial pulse only.

CLASS sets typically have a display for caller information. Other sets may have a small display for dialed digits, but this is not universal.

These sets may be wall hanging or desk-top. These sets may be with or without visual indicators or a flash button, which sends a properly timed switch hook flash rather than relying on the user's hand speed, or with displays for the CLASS sets. They do not have feature buttons and expansion modules.

Appendix G: Generic station operations

Generic station operations

The following operations apply to different subsets of the CS 1000 stations handled as Device Adapter endpoints. Each button type must be taken in context, as not all stations have soft keys, or programmable hard keys.

* Note:

All endpoints support the dial pad, and all except a very specialized subset allow the cradle or switch hook to act as a line selector/line release mechanism by off-hook and on-hook.

Generic station button operation

The operation for each of these buttons apply to all endpoints supporting the button. If the button or service is not supported, it might still be available using the Flexible Feature Code (FFC) operations.

The FFC is the same functionally as a Feature Access Code (FAC) of Communication Manager. To the endpoint user, the name change from FFC on CS 1000 to FAC on Communication Manager is invisible, although knowing it is configured as the FAC is crucial for the administrator.

Fixed Feature Keys

The following fixed feature buttons are supported for the endpoints, which were built with the button:

- Release key to disconnect a call
- Hold and retrieve
- Mute
- Headset
- Speaker on/off
- Shift
- Message waiting key and indicator for voice mail

Unless indicated in the section describing the fixed feature key, these buttons are not administered.

Release key

The **Release key** button is available on all Device Adapter endpoints except the analog endpoints.

Release key feature description

The **Release key** button functions like the **Call Drop** button found on several of the traditional Communication Manager endpoints. Pressing this button ends the call.

The button can also be used on CS 1000 (and to a limited extent on the Device Adapter endpoints) to end some on-endpoint provisioning or service operations.

This button cannot be removed or assigned any different function.

Terminating a call using the Release key button

About this task

When you are active in a call on the headset, speakerphone, or the handset, use the following procedure to release from a call.

Procedure

Press the **Release** button.

The call terminates as though the user was using the handset and was off hook and went on hook.

Hold and retrieve

This button is available on all Device Adapter endpoints except the analog endpoints. These will use the hook-flash.

Hold and retrieve feature description

The **Hold** button allows the current call to be held, so that another call can be answered, or modified, for example, transferred or conferenced.

When a call is held, for all endpoints with a visible indicator for the line in use the lamp or icon flashes for the line appearance (which may be a call appearance button or a bridge appearance). Other lamps or icons match the states of whatever operation is carried on for that button.

To retrieve the call, press the line appearance button with the flashing icon that was the line appearance of the held call.

The **Hold** button cannot be removed or assigned any different function.

Placing a call on hold

About this task

When you are active in a call on the headset, speakerphone, or the handset, use the following procedure to place the call on hold.

Procedure

1. Press the **Hold** button.

   The system places the call on hold.

   • The icon or lamp beside the button flashes.

   • The user is no longer in two-way speech.

   • If announcement is configured, the system plays the music to the party on hold.

2. Further actions depend on the user configuration and availability of other line keys.

Retrieving a call from hold

About this task

The user has a call on hold and decides to take the call off hold.

• The icon or lamp is flashing for the line appearance in question.

• The user and party on hold have no speech path.

• The party on hold may be receiving music on hold.

Procedure

Press the **line appearance** button.

The user may do this while on hook and receive the call on the speakerphone with the button lighting, on the headset of the headset is present.

Alternatively, if it becomes active on the speakerphone, the user may use another mechanism to change to another I/O device.

If the user went off hook and then pressed the line appearance, the handset is used instead of the speakerphone or headset.

The system activates the call.

• The icon or lamp beside the button stops flashing and is lit.

• The user has a two-way speech with the party that was on hold.

Mute

Mute feature description

Note that analog endpoints will typically never have the **Mute** button. Specific third-party analog endpoints that may be used with the CS 1000 might have the button, but CS 1000 analog endpoints do not have it.

The **Mute** button is a **set audio for receive only/set audio for send and receive** toggle. The CS 1000, Communication Manager, and Device Adapter handling is identical.

Muting a call

About this task

When you are active in a call on the headset, speakerphone, or the handset, use the following procedure to mute the call.

If present, the lamp beside the mute button is dark.

Procedure

Press the **Mute** button.

The media path changes such that the outgoing media path is blocked.

• The icon or lamp beside the hold button lights (if the lamp is present).

• Media from the muted party is blocked.

• Media to the muted party continues.

Unmuting a call

About this task

The user has a call on mute and decides to un-mute the call.

    • If present, the icon or lamp is lit for the hold button.

    • Media from the muted party is blocked.

    • Media to the muted party continues.

Procedure

Press the **Mute** button.

The media becomes bidirectional, and if a lamp is present it goes dark.

Headset button and headset

Headset button and headset feature description

The headset button is only available with a subset of digital endpoints, and UNIStim endpoints except for the 2004 and 1110. For endpoints supporting this button, the button will always be present but may not be enabled in provisioning.

The **headset** button allows users to:

- select the first available line appearance and use the headset
- switch to using the headset from whatever mode of audio was previously in use.

The button acts as **turn on headset audio, turn off any other audio** only. The user must use another button to release the call. For example, the release button, the switch hook, another line button if auto-hold is not used and the hold was not pressed.

A station with a handset, headset, and speakerphone may switch from either the speakerphone or handset to using the headset this way; there is no button to return to the handset.

Prerequisites for operating headset button and headset

1. Set the endpoint feature in Communication Manager or System Manager to include Hands Free Allowed (HFA) to enable the handsfree.
2. Connect the headset to the correct connector on the endpoint.

Operating the headset

About this task

Operations from the user perspective are unchanged from CS 1000 operations.

- To answer a call using the headset, press the headset key (⌨).

  The Headset LED indicator, located on the Headset key, lights to indicate that the headset is in use.

  Audio is provided by the headset.

- To change the media for a call, to switch to the headset, press the headset key (⌨).

  The Headset LED indicator, located on the Headset key, lights to indicate that the headset is in use.

  Audio is provided by the headset.

- To switch a call from the handset or handsfree to the headset, press the headset key (⌨).

  The Headset LED indicator, located on the Headset key, lights to indicate that the headset is in use.

  Audio is provided by the headset.

Switching from headset to handset

Procedure

1. Put the call on hold.

2. Push the flashing line appearance button used for the call.

   The Headset LED indicator, located on the headset key (🎧), goes dark to indicate that the headset is no longer in use.

Speaker and speakerphone

Speaker and speakerphone feature description

The **speaker** button is only available with a subset of digital endpoints, and with all UNIStim endpoints except for the 1110. For endpoints supporting this button, the button will always be present but may not be enabled in provisioning.

The 1110 can use handsfree and therefore implicitly use the speaker as a speaker phone by pressing the line appearance button without going off hook.

The **speaker** button allows users to:

- Select the first available line appearance and use the speaker in a hands-free mode.
- Switch to using the speaker and handsfree from whatever mode of audio was previously in use.

The button acts as **turn on speakerphone audio, turn off any other audio** only. The user must use another button to release the call. For example, the release button, the switch hook, another line button if auto-hold is not used and the hold was not pressed.

A station with a handset, headset, and speakerphone may switch from either the headset or handset to using the speakerphone this way; there is no button to return to the handset.

Pressing a line appearance while the handset is on the cradle will permit handsfree on some digital sets that do not have a **speaker** button.

For information about the exact subset of endpoints supporting this, see the endpoint documentation.

Prerequisites for operating speaker and speakerphone

Set the endpoint feature in Communication Manager or System Manager to include Hands Free Allowed (HFA) to enable the handsfree.

Speaker and speakerphone feature operation

Operating the speaker key using the Speaker fixed key

About this task

Operations from the user perspective are unchanged from CS 1000 operations. The following are the operations using the Speaker fixed key.

- To answer a call using the speaker, press the Speaker key (▣ ◁))).

  The Speaker LED indicator, located on the Speaker key, lights to indicate that the speaker is in use.

  Audio is provided by the speaker.

- To change the media for a call, to use the speaker, press the Speaker key (▣ ◁))).

  The Speaker LED indicator, located on the Speaker key, lights to indicate that the speaker is in use.

  Audio is provided by the speaker.

- To place a call, press the Speaker key (▣ ◁))) on an idle station

  The Speaker LED indicator, located on the Speaker key, lights to indicate that the speaker is in use.

  Audio is provided by the speaker.

Switching from speaker to handset using the Speaker fixed key
Procedure

1. Put the call on hold.

2. Push the flashing line appearance button used for the call.

   The Speaker LED indicator, located on the Speaker key (▣ ◁))), goes dark to indicate that the speaker phone is no longer in use.

Operating the speaker key without the Speaker fixed key

About this task

The following are the operations available for speakerphone without using the Speaker fixed key. The handsfree service must be supportable on the endpoint.

- To answer a call, do the following:

  1. Ensure that the station is ringing, and the handset is in the cradle.

  2. Press the programmable button for the ringing line appearance to answer a call using the speaker.

     The line indicator, located by the appearance, lights to indicate that the line is in use.

     If the endpoint has a speaker key, it lights as well.

     Audio is provided by the speaker.

- To switch to the Speaker phone, do the following:

    1. Ensure that the user is active on a call in some other mode (headset, handset).

    2. Place the call on hold

        The lamp or icon for the line appearance is winking and the media is stopped.

    3. Put the handset in the cradle.

    4. Press the line appearance.

        The line indicator, located by the appearance, lights to indicate that the line is in use.

        If the endpoint has a speaker key, it lights as well.

        Audio is provided by the speaker.

- To place a call, press the line appearance button.

    If the endpoint has a speaker key, it lights as well.

    Audio is provided by the speaker.

Switching from speaker to handset without the Speaker fixed key

Procedure

1. Put the call on hold.

2. Push the flashing line appearance button used for the call.

    If the endpoint has a speaker key, it goes dark to indicate that the speaker phone is no longer in use.

Page Shift

Page Shift feature description

The **page shift** button is only available with a subset of digital and UNIStim endpoints that have a certain number of physical programmable buttons but allow the user to toggle between different pages to access another set of buttons. The 1140 UNIStim endpoint is an example.

The 1140 has 6 programmable buttons on the endpoint. By default, an 1140 endpoint shows the first page of 6 button labels: buttons 1 through 6. Pressing the **shift key** changes these to buttons 7 through 12.

The administrator typically configures the 12 buttons so that the 6 most common are on page 1, and the rest are on page 2.

Certain phones use a printed **Shift** button label on the shift button, while others use a printed symbol. For information about the applicable labelling, see the station user guide.

This is an automatic function for any endpoint that supports the button and has feature keys configured on the second page of the display.

Page Shift feature administration

Not applicable. This is an automatic function for any endpoint that supports the button and has feature keys configured on the second page of the display.

Viewing pages

Procedure

1. While viewing the first page of the buttons and labels, press the **shift** button.

   The system displays the second page.

2. While viewing the second page of the buttons and labels, press the **shift** button.

   The system displays the first page.

Message waiting key and indicator for voice mail

Analog sets rely upon a special dial tone. Typically, CS 1000 uses a stuttered dial tone, where three short bursts of dial tone are followed by normal dial tone to tell the user a message is waiting. The user needs to manually dial into voice mail to retrieve the message. This is also used if voice mail is assigned to a non-analog endpoint which does not have an assigned Message waiting key or lamp.

Therefore, this section applies to all endpoints that have a **Message Waiting Indicator** button and visible indicator lamp or icon.

Message waiting key and indicator for voice mail feature description

This button is a fixed feature key for certain endpoint types, while a being a programmable feature key for others.

- A subset of the digital endpoints supporting a **Message Waiting** button use a programmable key for this button. These include the digital 2xxx stations. The administrator configures the station to have the **Message Waiting Indicator** button and lamp assigned to a specific key (button) number.

- Note that even though the station type of a 2xxx IP station is 2xxx, the IP 2xxx (UNIStim) stations use fixed location buttons and indicators.

Prerequisites for message waiting key and indicator for voice mail

- Configure the mailbox on the voice mail system. See the voice mail system administration guide for the procedure to configure this data.

- Configure Message Waiting Allowed (MWA) class of service for the endpoint.

- If the endpoint has buttons for Message Waiting or supports it on a fixed button location, configure **Message Waiting Indicator** on the appropriate button for the endpoint.

Message waiting key and indicator for voice mail feature operation

The location of the lamp and button differ based on the station type. See the application-specific endpoint documentation to determine the location of the button and indicator.

When a voice mail message is ready to be retrieved for endpoints:

- With a button and lamp, the indicator lights.

- Without a button and lamp, the special dial tone is provided.

Viewing a message on a station

Before you begin

The voice mail system must receive a message on the station.

Procedure

The voice mail system sends a message to Device Adapter.

The message waiting indicator is lit.

Retrieving the message for a station with the button and indicator

About this task

The message can be retrieved as follows, for a station with the button and indicator:

Procedure

1. To select a line appearance, perform one of the following:

   - Using the line buttons. If the handset is off hook, this uses the handset.

     If the handset is on hook and the speaker is available, this activates hands-free.

   - Lifting the handset.

   - Using the **headset** button, if the button is available and if the headset is connected.

   - Using the **speakerphone** button, if the endpoint supports the speaker and button.

2. Press the correct voicemail button for the station type.

3. Follow the prompts to log in.

4. Use the voicemail menu to listen to, forward, answer, delete, or otherwise handle the message.

   When all messages are heard, the message waiting indicator turns off. This might take several seconds, based on the traffic at the voicemail and network traffic.

Retrieving the message for a station without the button and indicator

Procedure

1. The user will have already selected a line appearance, as the user needed to hear the special dial tone. Until the appearance was chosen, no special dial tone can be received.

2. Enter the user access number for the voice mail server.

3. Follow the prompts to log in.

4. Use the voicemail menu to listen to, forward, answer, delete, or otherwise handle the message.

   When all messages are heard, the message waiting indicator turns off. This might take several seconds based on the traffic at the voicemail and network traffic.

Navigation Buttons

Navigation buttons feature description

The navigation usually includes five buttons and can include more. The 3902 has four, though, as the **enter** button in the center is missing.

In general, all station types have an up, down, left, and right arrow. This moves the cursor in the applicable screen. For example, this is used when changing the Node ID and TN in the UNIStim registration data.

Most stations have a **quit** button (sometimes with the image of a stop sign on it, instead of words). This allows the user to exit an active application, such as scrolling through the personal directory, without ending an active call.

⚠️ **Warning:**

The **release** button can also close the application (as can any soft keys that may be available at the time), but the **release** button will end active calls if one exists and is best avoided when closing applications during a call.

In addition, many IP stations include an **enter** button in the center of the navigation arrows. This can be used instead of the **Select** soft key, when the **Enter** fixed key is present.

Navigation buttons feature administration

Not applicable. This is native to the endpoints with the capability.

Navigation buttons feature operation
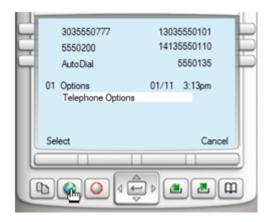
While in a suitable menu or screen, use the **up** and **down** buttons to scroll up or down, and the **left** and **right** to move to the left or right.

Use the **enter** or **quit** buttons as an alternative to the soft keys when in the menus.

Options Menu

Options Menu feature description

The **Options Menu** button opens a menu to select and modify options on the phone. You can click on the **Options** button as shown below to access the menu.

You can select Telephone Options by pressing the **Select** soft key or **Enter** in the middle of the navigation buttons to access a set of menu choices.

In this case, we can change the language to any other currently loaded in the station firmware, change the date and time, change information about the set including custom labels.

See the user guide for the specific station type to carry out any Options menu handling.

When the user leaves the **Options** menu or a sub-menu sitting idle for 30 seconds, the station cancels the operation.

This feature is native to the endpoints with the capability, and the menu is controlled only by the presence or absence of a subset of features configured on the endpoint, the firmware. For example, if the firmware does not support Spanish, the option cannot be used in **Languages**.

Options menu feature administration

Not applicable. This is native to the endpoints with the capability, and the menu is controlled only by the presence or absence of a subset of features configured on the endpoint, firmware, and so on. For example, if the firmware does not support Spanish, the option cannot be used in Languages.

Accessing Options Menu

Procedure

Select the option for the topic and press **Select**.
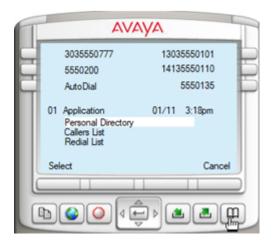
Volume Control

This is a simple **volume up** and **volume down** control for tones and audio.
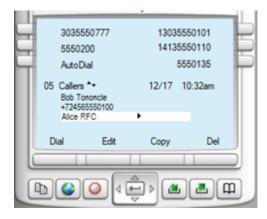
Personal Directory, Redial List, and Callers List

Personal directory, redial list, and callers list feature description

This button allows the user to access their personal directory, check the callers list (possibly calling someone on the list), or redial one of the previously called parties.

When a list is selected, the user can scroll up or down, shift right to see more details, or shift left to return to the display.

This shows a callers list accessed through this menu, scrolled partway down (the "05 Callers" indicates we are looking at the fifth element in the callers list), and the upward facing and downward facing triangles indicate we can scroll up or down. Beside the highlighted name is a right facing triangle, indicating we can use the right navigation button to see more details.

The soft keys indicate options we can carry out with this entry:

- **Dial:** Call the user.
- **Edit:** Edit the information, which allows the user to remove "Bob Tononcle" from the top entry shown.
- **Copy:** Copy the entry to add to Personal Directory.
- **Del:** Delete the entry

Prerequisites for personal directory or redial list or callers list

To configure the endpoint:

- Add the feature Last Number redial Allowed (LNA) to the features list to enable redial.
- Calling Party Name Display must be enabled.

The Personal Directory information must be extracted using the ProVision tool.

Normal administration for call data is done by the endpoint itself, see the endpoint user guide for details.

Personal directory or redial list or callers list feature operation

For information, see the endpoint-specific documentation.

Other Buttons

All other buttons either were used for other products such as the CS 2100, or are very specialized. For example, the **Copy** button, used only in Personal Directory to copy entries from the Caller's List or Redial List.

There is a context sensitive **copy** soft key on the endpoint for all endpoints that support the Personal Directory, making the **copy** key redundant

Programmable Feature Keys

This provides a station with feature key access to services and features (that is, access to the feature is not FFC based), and provides identities to use while calling (call appearance buttons, bridged appearance buttons). It does not apply to analog CS 1000 stations, though a **flash** button may be provided to give a reliable switch hook flash.

Buttons available as soft keys on certain station types may need to be configured as fixed keys on older station types.

For example, 3904 has context sensitive soft keys, but 2616 does not. Therefore, when the soft key is provisioned on the 3904, the transfer feature becomes available on a soft key when the user is active in a call and can use the soft key to complete a transfer. On the other hand, 2616 has no soft keys, and therefore requires the Transfer feature button provisioned.

However, even with the presence of soft keys, many other buttons, such as line appearances, auto-dial buttons are valid for provisioning on all set types with programmable keys.

Context-sensitive soft keys
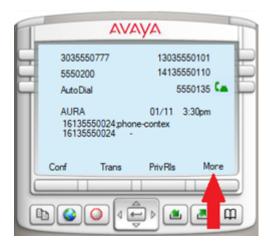
Context-sensitive soft keys feature description

Context-sensitive soft keys depend on the call state, station state, and services available.

The display has four buttons with labels. If there are less than four soft keys in a specific state, all the buttons are shown:

If there are four or more, up to three of the buttons are displayed, with the fourth button indicating **More**, allowing the user to access the additional soft keys:

The soft keys vary based on the current endpoint state and can vary when the options are used. Note that the soft key may not be visible, **Conf** location is fixed for the ad hoc Conference, and if the administrator used No Hold Conference and omitted the normal **Conference** button, the display leaves **Conf** position blank:

Context-sensitive soft keys feature administration

Context-sensitive soft keys are programmed against the specific feature button for the set, as defined in the default data model. That is, if a station supports the transfer soft key, it can be provisioned on key 17. It cannot be programmed on any other button, and no other feature can be programmed. However, the button can also be left with no feature or service programmed.

Context-sensitive soft keys feature operation

For information, see the endpoint-specific documentation.

IP Phone dedicated context-sensitive soft key assignment

NUL indicates that no key is assigned to this index. Keys 17 to 26 are soft keys. Key 16 is the fixed position message waiting key.

IP Phone key number	Responses Allowed
Key 16	MWK, NUL
	MWK: Message Waiting key
Key 17	TRN, NUL
	TRN: Call Transfer key
Key 18	AO3, AO6, NUL
	AO3: 3-party conference key
	AO6: 6-party conference key
Key 19	CFW, NUL
	CFW: Call Forward key
Key 20	RGA, NUL
	RGA: Ring Again key

Table continues…

IP Phone key number	Responses Allowed
Key 21	PRK, NUL
	PRK: Call Park key
Key 22	RNP, NUL
	RNP: Ringing Number pickup key
Key 23	SCU, SSU, SCC, SSC, NUL
	SCU: Speed Call User
	SSU: System Speed Call User
	SCC: Speed Call Controller
	SSC: System Speed Call Controller
Key 24	PRS, NUL
	PRS: Privacy Release key
Key 25	CHG, NUL
	CHG: Charge Account key
Key 26	CPN, NUL
	CPN: Calling Party Number key

Context-sensitive soft keys for voice mail on Device Adapter endpoints

You can use System Manager to configure context-sensitive soft keys for voice mail on UNIStim IP desk phones and 3900 series digital desk phones. Context-sensitive soft keys for voice mail are supported only on phones which support context-sensitive soft keys.

Users can use these context-sensitive soft keys on their phones to perform various operations, such as play, reply, and delete voice mail, on their voice mail messages.

The following list provides information about whether these phones support context-sensitive soft keys:

- CS 1000 CS1K-1col and CS1K-2col digital phones do not support context-sensitive soft keys.
- A subset of the 39xx phones supports context-sensitive soft keys.
  - M3901 digital phone does not support soft keys.
  - M3902 supports programmable soft keys, but these soft keys are not context-sensitive.
  - M3903, M3904, and M3905 phones support context-sensitive soft keys.
- Most of the lower-end UNIStim IP desk phones support programmable soft keys, but only few of these phones support context-sensitive soft keys.
  - UNIStim i2001 and i2002 desk phones support programmable soft keys, but these soft keys are not context-sensitive. UNIStim IP desk phones display only those soft keys that are relevant to the current context. You can press the **More** key to view all soft keys.

    However, configuration on the call server overrides which soft keys are displayed on these phones.

- The UNIStim 1120 phone supports programmable soft keys that are context-sensitive.

You can use the **Voicemail Telephony User Interface** attribute on System Manager to specify the Voicemail Telephony User Interface system that the customer uses.

Device Adapter supports the following Voicemail Telephony User Interface systems:

- Avaya Aura Messaging
- CallPilot
- Custom

Voicemail Telephony User Interface systems use dialing sequence to determine the action that the voice mail system must perform on a specific key press. For example, pressing Play plays the voice mail message.

Each Voicemail Telephony User Interface system has its own default dialing sequence for voice mail operations, such as play message, delete message, and call sender, during an active voice mail call. You can use System Manager to specify custom values for these dialing sequence attributes.

The valid value for a dialing sequence can contain digits 0 through 9 and can include special characters * and #. For example, *5343#. The maximum length of a dialing sequence is 32 characters.

Device Adapter passes these attribute values to the TPS component by using the `config.ini` file, which is available at `/opt/Avaya/da/shared/config/`.

For example, you set the **Custom dialing sequence: Play** attribute to `3`. When a user presses the **Play** soft key on the phone, Device Adapter uses the TPS service to pass the value 3 to the voice mail system, which in turn plays the voice mail message.

⊛ **Note:**

After you modify the Voicemail attributes, you must stop and start Device Adapter for the changes to take effect. Avaya recommends that you stop and start Device Adapter during the maintenance window to minimize the impact on endpoint registration and call handling.

You can also use the **Voicemail Telephony User Interface** attribute to enable or disable the display of context-sensitive soft keys for voice mail on the phones. By default, context-sensitive soft keys for voice mail is enabled.

You can use the context-sensitive soft keys for voice mail on these phones only for outgoing calls to the voice mail system and only when you are logged in to the voice mail box.

If you disable the **Voicemail Telephony User Interface** attribute, then the voice mail context-sensitive soft keys are not displayed on the phone. Instead, the phone displays the usual soft keys, such as **Conf** and **Trans**, while it is connected to the voice mail service.

The following table provides information about the context-sensitive soft keys for voice mail that are displayed on the phone. A user can press the **More** key to navigate to the next display. For example, if a user is on the Page 1 display, the user can press **More** to navigate to the Page 2 display.

Page	First soft key	Second soft key	Third soft key	Fourth soft key
1	**Play**	**Delete**	**Call**	**More**
2	**Stop**	**Conf**	**Reply**	**More**
3	**Comp**	**Forward**	**Bye**	**More**

> ✱ **Note:**
>
> Context-sensitive soft keys for voice mail on Taurus M39xx series digital phones are displayed only if you select **CallPilot Default** as the Voicemail Telephony User Interface system.
>
> If you select any other Voicemail Telephony User Interface system for the M39xx series digital phones, the context-sensitive soft keys for voice mail are displayed incorrectly these phones.

The display of the context-sensitive soft keys for voice mail is different on the Taurus M39xx series digital phones as compared to other phones.

The following table provides information about the context-sensitive soft keys for voice mail that are displayed on the Taurus M39xx series digital phones:

Page	First soft key	Second soft key	Third soft key	Fourth soft key
1	**Play**	**Stop**	**Last**	**More**
2	**Next**	**Delete**	**Skip >**	**More**
3	**Skip <**	**Quit**	Not applicable	**More**

Configuring context-sensitive soft keys for voice mail on Device Adapter endpoints

About this task

Use this procedure to specify the Voicemail Telephony User Interface system and the dialing sequences that the customer uses for context-sensitive soft keys for voice mail.

Voicemail Telephony User Interface systems use dialing sequence to determine the action that the voice mail system must perform on a specific key press. You can use either the default values or specify custom values for dialing sequence.

The valid value for a dialing sequence can contain digits 0 through 9 and can include special characters * and #. For example, *5343#. The maximum length of a dialing sequence is 32 characters.

Whether Device Adapter uses custom or default values for the dialing sequence depends on whether you select or clear the **Override Default** check box and whether you specify custom values for the dialing sequence attributes.

- If you select the **Override Default** check box and:
  - Leave the dialing sequence attributes as blank, context-sensitive soft keys for voice mail are not displayed on the phone for the dialing sequences that are left blank.
  - Specify custom values for the dialing sequence attributes, context-sensitive soft keys for voice mail are displayed on the phone. Device Adapter uses the custom values for dialing sequence.

> ✱ **Note:**
>
> Ensure that the values that you specify match the dialing sequence values on the voice mail server.

- If you clear the **Override Default** check box, Device Adapter uses the default dialing sequence values associated with the Voicemail Telephony User Interface system that you have selected, that is, **CallPilot Default**, **Avaya Aura Messaging Default**, or **Custom**. Device Adapter ignores the blank fields and the values that you specify for dialing sequences.

  The default dialing sequence values for the **Custom** Voicemail Telephony User Interface system are the same as those of the **Avaya Aura Messaging Default** Voicemail Telephony User Interface system.

Depending on whether you configure these attributes at a cluster level or a global level, these attributes are applied at a cluster or global level. For more information, see <u>About service attributes</u> on page 156.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

3. Click **Attributes**.

4. Depending on whether you want to configure the voice mail attributes at a cluster level or a global level, do one of the following:

   - Click the **Service Clusters** tab, select the cluster, and then select the service as **DeviceAdapter**.

   - Click the **Service Global** tab and select the service as **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Voicemail** group.

6. To override the default value of an attribute, select the **Override Default** check box corresponding to the attribute.

7. In the **Voicemail Telephony User Interface** field, in **Effective Value**, click the Voicemail Telephony User Interface system that you want to use.

   To disable the display of the context-sensitive soft keys for voice mail on the phones, click **Disabled**.

8. In the **Custom dialing sequence: Play** field, in **Effective Value**, type the dialing sequence to play the voice mail message.

9. In the **Custom dialing sequence: Delete** field, in **Effective Value**, type the dialing sequence to delete the voice mail message.

10. In the **Custom dialing sequence: Call** field, in **Effective Value**, type the dialing sequence to call the party that left the voice mail message.

11. In the **Custom dialing sequence: Stop** field, in **Effective Value**, type the dialing sequence to stop playing the voice mail message.

12. In the **Custom dialing sequence: Reply** field, in **Effective Value**, type the dialing sequence to reply to the voice mail message.

13. In the **Custom dialing sequence: Compose** field, in **Effective Value**, type the dialing sequence to compose a message and send the message to one or more users.

14. In the **Custom dialing sequence: Forward** field, in **Effective Value**, type the dialing sequence to forward the voice mail message to another user's mailbox.

15. In the **Custom dialing sequence: Goodbye** field, in **Effective Value**, type the dialing sequence that can be used for any of the following:

   • If pressed from the sub-menu of the main menu, exit from the sub-menu.

   • If pressed from the main menu, disconnect from the voice mail system.

Next steps

After you modify the Voicemail attributes, you must stop and start Device Adapter for the changes to take effect.

⊛ **Note:**

   Avaya recommends that you stop and start Device Adapter during the maintenance window to minimize the impact on endpoint registration and call handling.

Related links

[Service attributes](#) on page 157

Dialing a number

Dialing a number feature description

The user seizes a call appearance (selecting a line appearance, going off hook) and enters the number to call a desired party or service. Typically, this is done on a digit by digit basis for digital or analog phones and can be done this way for UNIStim phones.

Depending on the destination state, the far end indicates a ringing state (or some other intermediate state enroute to success), call failure (with an applicable indication), reaches an interactive voice response menu to navigate, or is automatically answered.

Eventually, the call is answered (if it did not fail) and is cleared.

On the CS 1000, all dialed digits are handled by the Call Server, which completes the dialing phase after the digits match an internal extension or dial plan rule. UNIStim and 39XX phones support a Predial state where the user can modify the number before sending it to a call server.

With the Communication Manager, 96x1 Avaya Aura® SIP phones use en-bloc dialing. This type of dialing analyzes digits by using information received from the PPM Dial Plan Data section. Client SDK does the same. However, to the user the number can be digit by digit or "enter all digits and then send the data"; the en-bloc dialing occurs between the SIP client on the 96x1 and the

Session Manager, which is analogous to doing the same in the digit collection code of a CS 1000 call server.

Prerequisites for Avaya Aura®

The following needs to be done in the Aura network:

1. The Communication Manager, Session Manager, and any other devices must be deployed and configured to communicate.

2. The desired digit translations must be entered in the System Manager. This downloads the information as applicable to route the calls through the Session Manager and Communication Manager. In addition, the call may route through a media gateway or IP connection to the external environment. This must be set up correctly.

3. The Device Adapter must be deployed and configured.

4. The Device Adapter endpoints must be deployed and configured on the Session Manager and Communication Manager.

No routing decisions are configured in the Device Adapter. Effectively, the Device Adapter converts the endpoints it services into "96x1-like" endpoints registering through the Session Manager to the controlling Communication Manager. Once the endpoints can register with the Session Manager, the endpoints should be able to place calls successfully, provided all the translations and destinations are correctly configured.

However, the Device Adapter has three timer values administered:

• Dialtone: Determines how long dialtone is to be played without the user entering a digit. On expiry, the call attempt is failed.

• Interdigit: Determines how long to wait for another digit before attempting the call. On expiry, if the number has no conflicts in the PPM Dial Plan data, the call is attempted. Otherwise the call is rejected.

> ☀ **Note:**
>
> As soon as there is a valid match (prefix to the digit string matches one entry, and the total length matches the expected length), the call is attempted.

• Busy/overflow: Busy tone and call failure tone are played out for a specific maximum duration. If the user does not disconnect before the timer expires, the Device Adapter completes call clearing anyway.

These are included in the Attributes of the Device Adapter in the System Manager.

Dialing a number feature operation

Dialing normal numbers

About this task

Use this procedure for normal dialing.

Procedure

1. The user selects a line appearance on the endpoint (including going off hook with analog stations).

2. The user enters digits.

3. Device Adapter analyzes dialed digits against the dial plan obtained in the same way as Avaya Aura® SIP phones.

4. When a match is found (digit pattern plus correct number of expected digits, where the minimum and maximum number of digits is the same):

    a. The Device Adapter initiates the call with the Session Manager and Communication Manager.

    b. Call progress conforms to SIP call handling (speech path cut through, tones, etc.).

    c. If the call is failed at this point:

       • Appropriate messaging and tones are provided to the caller.

       • When the caller clears the call, the user endpoint is idle.

    d. Else if the called party does not answer:

       • If the far end fails the call, appropriate messaging and tones are provided to the caller.

       • When the caller clears the call, the user endpoint and any remaining call attempt artifacts are cleared or idled, as applicable.

    e. Else:

       • When the call is answered, features supported at that time are available.

       • When either party clears the call, the user endpoint is idle.

5. When a match is found (digit pattern plus correct number of expected digits, where the minimum number of digits is the less than the maximum number of digits):

    a. The Device Adapter continues waiting for more digits.

    b. If the interdigit timer expires (indicating no more digits), the user indicates end of dial, or the number of digits reaches the maximum allowed, the Device Adapter initiates the call with the Session Manager and Communication Manager.

    c. Call progress conforms to SIP call handling (speech path cut through, tones, etc.).

    d. If the call is failed at this point:

       • Appropriate messaging and tones are provided to the caller.

       • When the caller clears the call, the user endpoint is idle.

    e. Else if the called party does not answer:

       • If the far end fails the call, appropriate messaging and tones are provided to the caller.

- When the caller clears the call, the user endpoint and any remaining call attempt artifacts are cleared or idled, as applicable.

    f. Else:

- When the call is answered, features supported at that time are available.

- When either party clears the call, the user endpoint is idled.

6. When no match exists (invalid digit string), the Device Adapter indicates failure to the user.

- Appropriate messaging and tones are provided to the caller.

- When the caller clears the call, the user endpoint is idled.

Predialing state for UNIStim and 39XX phones

About this task

Device Adapter supports the Predial state for UNIStim and 39XX phones.

Procedure

1. The user enters digits at the keypad; the Device Adapter collects them.

2. When the user selects a line appearance, the Device Adapter analyzes dialed digits against the dial plan obtained in the same way as Avaya Aura® SIP phones.

3. When a match is found (digit pattern plus a valid number of digits, greater than or equal to the minimum number of digits and less than or equal to the maximum number of digits):

    a. The Device Adapter initiates the call with the Session Manager and Communication Manager.

    b. Call progress conforms to SIP call handling (speech path cut through, tones, etc.).

    c. If the call is failed at this point:

- Appropriate messaging and tones are provided to the caller.

- When the caller clears the call, the user endpoint is idled.

    d. Else if the called party does not answer:

- If the far end fails the call, appropriate messaging and tones are provided to the caller.

- When the caller clears the call, the user endpoint and any remaining call attempt artifacts are cleared or idled, as applicable.

    e. Else:

- When the call is answered, features supported at that time are available.

- When either party clears the call, the user endpoint is idled.

4. When no match exists (invalid digit string), the Device Adapter indicates failure to the user.

- Appropriate messaging and tones are provided to the caller.

- When the caller clears the call, the user endpoint is idled.

Dialing a number feature interaction

None identified specific to the Device Adapter. The reader may have interactions with feature operations on the Communication manager.

Display capabilities

Display capabilities feature description

Device Adapter phones, except for analog phones without display and several digital and UNIStim phones without display, show caller information and other data. A subset also provides soft keys, and a largely overlapping subset provides labels for the provisioned programmable buttons.

The display updates at various stages while the user is involved in calls. In particular, it changes when:

- Making a basic call.
- Receiving a basic call.
- Receiving information about changes in the far end while making or receiving a basic call.
- Answering a basic call.
- Receiving an answer indication for a basic call.
- Releasing a basic call.
- Receiving the clearing from the other party releasing a basic call.

The topics above include:

- Context-sensitive key access:
  - Idle call state.
  - Off hook call state.
  - Dialed call state.
  - Ringing remotely call state.
  - Ringing locally call state.
  - Active call state.
- Time and date, call timer, and other similar set display features.
- Display of calling or called numbers.
  - This includes not displaying the far end user information if the station is configured to not display caller information.

In addition, the following are also included in the station displays capable of them:

- Labels for the fixed feature keys.
- Message waiting key and indicator for voice mail.

Prerequisites of services configured in System Manager

The Device Adapter requires the following classes of service configured in the System Manager:

- Features:
  - Digit Display:
    - Typically one of:
      - DDS (Digit Display Standard)
      - ADD (automatic digit display)
    - A "Tandem Digit Display" configuration includes both ADD and DDS.
    - The NDD class of service (No Digit Display) will prevent digits from being shown on the screen. However, if an endpoint has no digit display hardware, NDD is the correct choice for that endpoint.
  - Name Display:
    - CNDA (Call party Name Display Allowed)
    - The CNDD (Call party Name Display denied) applies for endpoints unable to display names.
    - The CNDA/CNDD is a bidirectional flag:
      - Outgoing calls will show the called party name if received.
      - Incoming calls will show the calling party name if received.
- If calling party privacy is to be enabled, the user must use either the "Calling Party Number Block" FAC or have a Communication Manager button assigned. Refer to Communication Manager documentation to configure these.

Display capabilities feature operation

About this task

There is no user operation specific to the display on the user station. When the information is received it is displayed.

😊 **Note:**

If a call is received without a name but with a number, the number is displayed; when a call is received with presentation restricted for the information, the "anonymous caller" display is provided.

Display capabilities feature interaction

Activating a feature key during a call may obscure the information displayed for the call. As an example, during a call transfer, the press of the transfer button or soft key will provide an "outgoing call" screen. If cancelled, the original information is displayed.

End-to-End Signaling

End-to-End signaling feature description

When a caller wishes to access an interactive menu, using digits to select the desired option, it is necessary to send the digit information to the far end. The CS 1000 refers this as End-to-End Signaling.

With many TDM resources this is possible using direct media through the audio path. A PRI call using 64 Kbps in E1 countries or using 56 kbps in T1 countries for 3.1 KHz audio provides a reliable media path for digit transmission.

However, IP is a lossy medium where packets can be lost and is subject to data compression which means the exact frequencies can be lost. Sending DTMF over G.729 for digit menus will fail. Therefore, End to End Signaling relies on DSPs in the MGC and in the UNIStim endpoints detecting the digits and using RFC 2833 transmission of digit packets. These indicate start a digit x, continue a digit x and end of digit x reliably.

The packets indicating the digit are detected and the tone reconstituted at the receiving end. Therefore, the digit is transmitted cleanly. Both CS 1000 and Communication Manager use RFC 2833 to provide reliable digit transmission. As the Device Adapter is entirely IP based, this suffices for End to End Signaling in the Device Adapter.

Prerequisites for End-to-End signaling

RFC 2833 support must be enabled at the MGC or UNIStim endpoint. Support for RFC 2833 packetized digit transmission to the far end is determined by the data in the SDP received from the far end. If the far end did not indicate support for RFC 2833 in the SDP offer or answer, the Device Adapter cannot send the digit packets to the far end. However, this is under control of the far end; the Device Adapter always permits end to end transmission of digits using RFC 2833.

Feature operation of End-to-End signaling

The feature operation of End-to-End signaling is invisible to the user. An example of End-to-End signaling is calling a customer care number of a company and receiving a menu option list. The

menu option list can be, Press 1 for sales or Press 2 for support. A user can proceed by selecting a choice from the menu options .The process of user selection uses RFC 2833 technology.

Other services which use the End-to-End signaling feature are voice mail, automated attendants etc.

Flexible Feature Codes

Feature description of flexible feature codes

CS 1000 supports Flexible Feature Codes (FFCs). The earliest model in the Northern Telecom digital Private Branch Exchange (PBX) explained special prefix digit string used to trigger special handling on a website. Later fixed feature code were introduced to request the desired feature. This approach was found to be limited in some cases. A digit pattern that was acceptable in one region was unacceptable in another region. So flexible feature codes feature was introduced to overcome this problem.

The Malicious Call Trace feature will be used as an example to explain the flexible feature codes:

The original CS 1000 Malicious Call Trace signaling used the special prefix, followed by the feature code 83. Rather than using the fixed digit pattern with CS 1000 FFCs, the user dials the digit pattern associated with the Malicious Call Trace (MTRC) FFC. The call trace is carried out.

The Communication Server has a similar model, with a call trace capability. It supports an FFC equivalent called as Feature Access Codes (FAC).

When CS 1000 FFC is mapped to the Communication Manager FAC, an analog endpoint user will not detect any difference. At the same time, digital and UNIStim endpoints can be assigned a Malicious Call Trace button, and when you press this button then FFC is not required. However, even digital and UNIStim endpoints can initiate transfer, enter the FFC, and carry out the trace. The ProVision tool extract the FFCs and map the respective FFC with the applicable FACs on the Communication Manager.

Prerequisites for configuring flexible feature codes

Ensure that you have the ProVision tool to retrieve the information of flexible feature codes while upgrading your system.

Making calls using flexible feature codes or feature access codes

About this task

You can enter Flexible Feature Code (FFC) or Feature Access Code (FAC) after pressing the line appearance key or after activating the call transfer.

Procedure

1. To use FFC or FAC before making the call operation for example, for accessing a speed dial list, do the following:

   a. Select a line appearance.

   b. Enter the applicable FFC or FAC at the station dial pad. For example, enter the digit string for the speed call list.

   c. Enter any additional information required at the station dial pad, based on the requested service. For example, the index for the desired speed dial list destination.

2. To use FFC or FAC in the middle of a call operation; for example, for flagging a call as malicious, do the following:

   a. Determine that the service is required, for example, deciding that an active call needs to be flagged as malicious.

   b. Initiate transfer.

   c. Enter the applicable FFC or FAC at the station dial pad. For example, enter the digit string for Malicious Call Trace.

   d. The user will be reconnected to the other party. But, this depends on the purpose of the service. For example, for malicious call trace the user is reconnected to allow the system to trace. When the public network supports a malicious call trace request from the system, the request may be processed on that side of the network, which may involve actions as determined by the national policing and security organizations.

Tone and cadence

Tone and cadence settings feature description

General

Different tones – ring tone, ring-back, overflow, dial, and so forth – vary on a country by country basis. The Device Adapter provides the ability to change the tones provided to the end user.

The CS 1000 and Communication Manager have different approaches to the tones and cadences, in part because the CS 1000 provides tones based on a "stimulus device" basis, which provides additional options. However, the SIP stations are more dependent on the endpoint, and therefore the tones are configurable by country, but not as modifiable.

CS 1000 endpoints

Tone and cadences are administered in Overlay 56 as FTC tables.

There are no predefined country tables except North American. Therefore, the administrator needed to be able to set the tones to match the country in question.

Communication Manager endpoints

Avaya Aura® SIP phones use the COUNTRY field in the Settings file to provide country specific tones. This removes the requirement to change the tones and cadences to conform to the current country.

Tone and cadence feature administration

All Device Adapter endpoints use the country setting of Device Adapter to determine the tones and cadences used.

Tone and cadence feature operation

Provided the endpoints and the Device Adapter are configured to provide the correct country setting for each endpoint, the endpoints receive the in-band tones either from the remote side (typically as audio in the RTP stream) or as locally generated tones from the Device Adapter.

⊛ **Note:**

Device Adapter does not support media tones through Avaya Aura® Media Server. The tones are generated either by the MGC resources or by the endpoint itself.

Key Expansion Modules

Key Expansion Modules feature description

A modular unit with different numbers of keys (based on the specific expansion module) can be attached to 16-key 2xxx digital phones, specific 39xx digital desk phones, and most UNIStim IP phones. Note that a specific station may have more than one possible choice of key expansion module, but some modules are limited to a subset of the stations supporting the added modules.

The extra keys can be assigned to any combination of lines and features. You can typically add more than one expansion modules to a single telephone, providing an increase in line/feature keys.
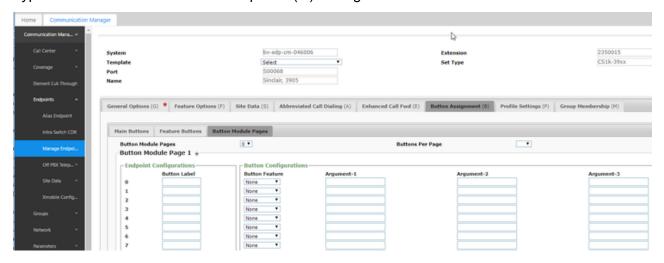
You will need a separate footstand for the module(s). The modules do not use the same base as the station itself.

The Key Expansion Module connects to the telephone through a ribbon cable running from the base of the telephone. It is physically connected to the telephone by the footstand, which attaches to the footstand of the station.

For more information about the specific expansion modules supported on Device Adapter, see the user guides for the supported endpoints.

Key Expansion Modules feature administration

The Communication Manager Endpoint Administration has some new attributes for CS 1000 endpoints behind the station administration screens. The following example is based on the Set Type: CS1k-39xx and the General Options (G) setting for the set as 3905:

CS 1000 Endpoint Type

Two important pull-down values on the preceding System Manager screen provide the ability to tailor a station definition to the hardware.
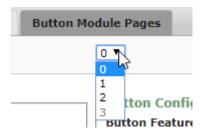
- Number of Expansion Module Pages – "Button Module Pages". This allows the administrator to determine how many expansion modules are attached to the station. When this is non-zero, one or more of the subsequent button module "pages" can be programmed. If the "pages" value is set to 1, then only the first module can be administered.

- Number of Keys/Buttons per Page – "Buttons per Page". This allows setting the pages for the correct module type for any endpoint with two different expansion modules. For example, the 12xx stations can use a 12 or an 18-button expansion module.

Note that the values of the buttons per page and number of pages can be confusing. The underlying logic can be obscure.
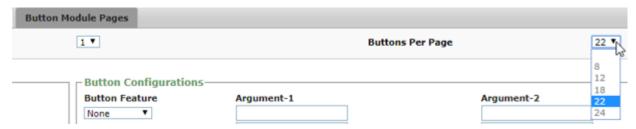
One module per page

The original 22-key add-on module (AOM) did not support a Shift operation because the station itself did not have soft keys or Shift inherently. As such, these are very straight forward.

The Button Module Pages allow 0,1, or 2.

A non-zero number of pages provides a fixed number of buttons per page of 22:

Fewer buttons on Communication Manager for specific expansion modules

Communication Manager provides three additional button pages that can be programmed. If a fourth page is needed, the page will not be available. Therefore, a CS 1000 endpoint with the extra page will have fewer buttons after migrating.

CS 1000 had inconsistent numbers of available buttons based on the number of modules. For example, modules with a total button count, including the shifted values, lower than the maximum might be able to use a Shift. If the total count exceeds the maximum, all modules could become un-shifted. Therefore, the next step up from three modules with Shift could be seven modules without Shift.

Mapping this into Communication Manager, Device Adapter uses a fixed page size, which may or may not be on one module. For example, if 18 buttons exist per module, and the module can have up to two pages, then there will be two pages for a shifted module.

As a result, in certain cases the total number of expansion modules or the total number of possible buttons decreases with Communication Manager.

- The 12 button LCD KEM for the 12XX has two pages when you have a single module, using the 12XX shift key to access the second page.

  - This yields an effective increase of up to 24 added buttons.

    Two Communication Manager module button pages are used.

    - Number of pages: 2
    - Buttons per page: 12
    - Number of physical modules: 1

  - However, the 12XX stations are limited by Communication Manager button limitations to no more than 36 added buttons (three pages at 12 buttons per page). Hence, if you add a second KEM, you get 36 as the maximum added number of buttons. Unlike the 11XX KEM, the first KEM can use the Shift key, but the second KEM cannot use the Shift key.

Three module button pages are used.

- Number of pages: 3

- Buttons per page: 12

- Number of physical modules: 2

- A user can also have three KEM modules without Shift. Three module button pages are used.

- Number of pages: 3

- Buttons per page: 12

- Number of physical modules: 3

However, in CS 1000, the user can access the fourth page of buttons on the second module in a two-KEM setup (assuming two were used). The user can also access the fourth page by having four expansion modules.

This is not supported with Device Adapter.

Modules with or without Shift

The 12-key LCD and other expansion modules allow the Shift button under some circumstances but deny it in others.

- The 12-button LCD KEM for the 12XX was mentioned above.

  - If there is a single module, it supports Shift on Device Adapter.

    - This requires two pages.

    - If there are two modules, Device Adapter allows the first KEM to have 24 buttons, as two pages of buttons, but the second KEM cannot be shifted. Communication Manager allows only three pages.

      - This requires three pages, but the first two are used by the first module and Shift.

    - If there are three KEMs, none of them can Shift.

- The 18-button KEM for the 11XX has two pages when you have a single module, using the 11XX shift key to access the second page.

  - This yields an effective increase of up to 36 buttons. Two module button pages are used.

    - Number of pages: 2

    - Buttons per page: 18

    - Number of physical modules: 1

  - However, because the 11XX stations are limited to no more than 54 added buttons, if you add a second KEM, you also get 36 as the maximum added number of buttons. The first KEM cannot use the Shift because the second KEM cannot use the Shift.

Again, two module button pages are used.

- Number of pages: 2
- Buttons per page: 18
- Number of physical modules: 2

- If a user wants to have between 37 and the maximum 54 additional buttons, then three KEM modules are needed, without Shift. Three module button pages are used.

  - Number of pages: 3
  - Buttons per page: 18
  - Number of physical modules: 3

- The 18-button soft KEM for the 2050 soft client is treated the same as the 18–button KEM for the 11XX.

- The 24-button KEM for the 200X has two pages when you have a single module, using the 200X Shift key to access the second page.

  - This yields an effective increase of up to 48 buttons. Two module button pages are used.

    - Number of pages: 2
    - Buttons per page: 24
    - Number of physical modules: 1

  - However, since the 200X stations are limited to no more than 48 added buttons on Device Adapter, if you add a second KEM, you also get 48 as the maximum added number of buttons. Neither KEM can use a Shift because that would require an additional page on Communication Manager.

    Again, two module button pages are used.

    - Number of pages: 2
    - Buttons per page: 24
    - Number of physical modules: 2

Modules with Shift handled as multiple pages

Because certain modules allow more than a single Shift, there is an added "pages versus buttons per module" aspect.

Modules with more than two pages in the hardware are mapped as using three pages in Communication Manager. However, as the modules were "one expansion module per station," this does not change the available number of buttons. Administrators must consider this.

- The 8-button DBA for the 39XX with the Shift key integrated into the module is physically a single-page 24 button module, and not an 8 button three-page module. However, the administration of the expansion module uses three pages of 8 buttons.

  - Number of pages: 3

- Buttons per page: 8

Key Expansion Modules feature operation

The user presses the feature buttons on the key expansion module in the same way he or she would on the set itself.

Comments on this document? infodev@avaya.com

Appendix H: Call processing features and services

Auto-Answer

Prerequisites for Auto-Answer on a UC phone

The Auto-Answer functionality on a Device Adapter UC phone requires the following criteria:

- The Auto-Answer feature is enabled on the target phone.
- The Hands-Free functionality is enabled on the target phone.
- The phone type is UNIStim or digital.
- An incoming call is on the primary DN.
- Target phone is in idle status or has a held call before the new call.

The target phone plays a buzz tone and automatically answers the call after a short delay. If the foregoing criteria are not met, the phone only plays a buzz tone and displays the name and number for an incoming call, but the phone does not automatically answer the call.

Configuring Auto-Answer for a UC phone

Procedure

1. Configure the Hands-Free Allowed (HFA) mnemonic for the phone.

   For more information, see [Administering a mnemonic](#) on page 339.

2. Configure the Auto-Answer Allowed (AAA) mnemonic for the phone.

   The phone displays the `Auto-Answer Activated` message only if you configured AAA and HFA mnemonics. If the Call Forward feature is activated, the phone displays the `CFWD` message instead of `Auto-Answer Activated`.

Autodial

Autodial feature description

Autodial has two main sub-topics:

- Administering the autodial number
- Using the stored autodial number.

Administration can be done by the:

- System administrator, who might prevent the user from changing the destination number
- User

To use the autodial key, typically the user selects a line appearance, receives dial tone, and presses the autodial button. At that time, the call server processes the digits to route the call.

A subset of users may use the autodial button for different purposes, though. Certain users program the autodial button to send digits when prompted for some operation. As an example, the system may have some routes classified as "expensive", and the user needs to enter an authorization code.

Background information

CS 1000 endpoint configuration

The **autodial** button is not programmed with a predefined number.

Users program the **Autodial** keys by using the on-hook method. When the phone is idle, the user presses on the required **autodial** key. The screen enters the programming mode.

The user edits the number and presses the **autodial** key to complete the change.

Communication Manager endpoint configuration

The following are two types of Autodial buttons with same feature button type autodial:

- The destination number is configured in Communication Manager for the station. This is read-only Autodial. The user cannot change the number.
- Read-write Autodial is programmed by the user.

Autodial feature configuration

The normal provisioning for a Device Adapter endpoint is provided by ProVision and the Nortel Migration Tool. To add an **autodial** button to an existing set, or to add one to a set being configured:

Configuring autodial on Communication Manager
Procedure

1. On the Communication Manager command line interface, type the `change station <extension>` command.

   The command can be abbreviated to the shortest unique entry.

   For example, to change station 5552345, the following is acceptable: cha sta 5552345

2. Navigate to the button definition pages.

3. Select an empty button that exists on the endpoint and type `Autodial`.

   Do not specify an autodial destination number if you want to the user to configure the autodial number on the endpoint. If you specify a destination number, the number appears as read-only on the endpoint and the user cannot modify the number.

4. Type `#`.

Configuring autodial on System Manager
Procedure

1. Log on to the System Manager web console.

2. Click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.

3. To edit an existing device, click on the selection box beside the correct set name, and click **Edit**.

4. Make changes or additions on the **General options** tab.

5. Select the **Button Assignment** tab.

6. Select an unused button and select the **autodial** option from the pull-down.

   Do not enter any digits if the user is to be able to enter an autodial number.

Autodial feature operation

Provisioning the Autodial number

About this task

The Device Adapter maps the CS 1000 Autodial to the Communication Manager Autodial read-write buttons.

The CS 1000 does not allow migration of Autodial destination numbers when migrating from CS 1000 to Device Adapter. You need to reprogram Autodial numbers after upgrading to Device Adapter.

Autodial programming scenario:

Procedure

1. Press the **Autodial** key while in the idle state.

2. At the prompt, type the destination number.

3. Press Autodial again to save the changes.

   The number cannot be programmed if the **Autodial** button is configured with a predefined number by the administrator.

Using the Autodial button

About this task

A free call appearance is required at the time of completing the programming dialog, if the user wishes to use the **autodial** button. Furthermore, an autodial button must have had the user data entry completed and Device Adapter must have performed a programming call to Communication Manager.

Autodial dialing scenario:

Procedure

1. When the user goes off-hook, it automatically selects the prime DN key.

   This is the button referred to by CS 1000 users as key 0, which corresponds to a Communication Manager endpoint button 1

   Alternatively, on sets with headsets, or hands-free, pressing these keys also selects key 0. Pressing any other line key selects that line key. This is the same behavior as CS 1000.

2. Press an Autodial key.

   This differs from Communication Manager where pressing Autodial automatically selects a call appearance.

3. As mentioned above, a user may also press Autodial key when the RTP stream offer for the call is answered. The stored number is output as RFC 2833 events.

   The dialing scenario using the RFC 2833 is not supported on phones with no RFC 2833 support, such as the i2050v2 or less.

Autodial feature interaction

If the destination is SIP but not RFC 2833 capable, end-to-end signaling is not possible. TDM endpoints can do end-to-end signaling provided there is an intervening SIP to TDM gateway that can provide the capability.

Busy Indicator

Busy Indicator feature description

> ✳ **Note:**
>
> Device Adapter supports the Busy Indicator feature for UNIStim and digital phones.

The Busy Indicator (BI) feature provides multi-appearance telephone users and attendants with a visual indicator of the busy or idle status of a phone. This feature is typically used in a boss-secretary scenario.

The Busy Indicator feature of Device Adapter is similar to the Busy Forward Status (BFS) feature of CS 1000, but with some variations.

In Device Adapter, the Busy Forward Status (BFS) key is linked to the BI feature on the secretary's phone.

The default label for the Busy Indicator button is BusyFwd on the secretary's phone and provides the following capabilities:

- The BusyFwd key lamp provides a visual indicator of the boss's phone state:
  - Lit: If the boss's phone is busy.
  - Dark: If the boss's phone is idle.
- When the secretary presses the BusyFwd button, Device Adapter automatically dials the boss's number. This functionality is similar to the Hotline one-way feature.
- The secretary can use the BusyFwd button to transfer a call to the boss.

The BusyFwd key is not supported on the boss's phone. The boss can use the Call Forward feature to redirect the calls to the secretary.

Because the BusyFwd key is not supported on the boss's phone, the BusyFwd button on the secretary's phone cannot monitor the Call Forward All Calls (CFW) status on the boss's phone.

Call Forwarding on behalf of a monitored extension:

Device Adapter supports the Communication Manager operation of managing Call Forward All Calls (CFW) from a user extension on behalf of another user extension.

For example, phone A is the secretary's phone and phone B is the boss's phone.

Phone A user wants to turn on or off CFW on behalf of phone B. Phone A user can use the Call Forward All Calls feature along with the Busy Indicator feature to manage the CFW status of phone B.

Phone A user can activate CFW and specify the CFW destination number on behalf phone B. The inbound calls on phone B are forwarded to the CFW destination number.

To do this, on System Manager, an administrator must first configure station A to permit station A to manage CFW on behalf of station B. For more information, Configuring an endpoint for Busy Indicator and call forwarding on behalf of another user station on page 435.

After the preceding configuration:

- Phone A displays a Call Forward button that is configured for the extension number of phone B. The default label for this button is **Forward**, which is received from PPM.

- Phone A displays the call forward status of the phone B by using the key lamp or icon for the **Forward** button.

  The following indicates the lamp or icon status:

  - Lit: Call forward is active on phone B.

  - Dark: Call forward is not active on phone B.

- Phone A user can activate CFW on behalf of phone B, set the CFW destination number on behalf of phone B, and cancel CFW on behalf of phone B.

  - If phone A has the capability to display the Forward button, phone A displays the regular call forward prompt. The phone A user can enter the CFW destination number on behalf of phone B at this call forward prompt.

    The default destination number is the extension number of the user activating the call forward, which is phone A in this example.

  - After CFW is active, Device Adapter saves the destination number in the PPM parameter, the same way that it does for regular CFW. Each Forward button can have a different destination number saved.

  - Device Adapter and the phone use the saved destination number as the default number for the Forward button the next time the user activates CFW.

  - If Call Forward is activated for the extension of phone B, and phone A has the capability to display the Forward button for phone B, phone A can cancel CFW on behalf of phone B.

Prerequisites for activating Call Forward All Calls on behalf of another user station

Determine which extensions require call forwarding to be handled by another user station

In most cases where an administrative assistant needs to monitor multiple extensions, the administrative assistant does not require the Call Forward feature for all the user extensions that are being monitored. If the administrative assistant is monitoring the call forward status for multiple user extensions, then configuring a **call-fwd** button for all the associated Busy Indicator buttons can result in having insufficient buttons on the administrative assistant's station.

Before configuring a **call-fwd** button for an associated Busy Indicator button, a system administrator must confirm the user extensions for which an administrative assistant must both monitor the status and manage call forward. A system administrator must configure a **call-fwd**

button only for those user extensions on behalf of which an administrative assistant wants to manage call forwarding. This is a manual process.

For migrated endpoints, a system administrator can analyze the logs for the Busy Indicator buttons that are mapped by ProVision and determine which Busy Indicator buttons would require an associated Forward button.

Configure the Call Forward capability

The Busy Indicator button on an endpoint might be configured by using any of the following methods:

- ProVision was used to define the stations based on the CS 1000 programming.

  A system administrator can make changes to the station definition after the mapping is done by using ProVision and before the configuration is migrated to System Manager. This allows a system administrator to modify the station definition before the sets are defined in System Manager and Communication Manager.

- The sets were configured by using some other method, such as manual configuration.

Assume that phone A is the secretary's phone and phone B is the boss's phone. The system administrator has determined that the phone A user must manage CFW on behalf of phone B extension.

The following are the prerequisites for allowing phone A to activate Call Forward All Calls (CFW) on behalf of phone B:

- By using System Manager, an administrator must configure a **call-fwd** button for phone A. The extension number for this **call-fwd** button must be that of phone B. For more information, see

  After the administrator performs the preceding configuration, a Forward button using a programmable feature key for phone B extension appears on phone A.

- Phone A user must assign a call forward destination number for phone B by using this Forward programmable feature key.

Verifying the Call Forward All Calls status of an extension by using the Avaya Breeze® platform CLI

About this task

Before configuring a user station to allow the user station to activate CFW on behalf of another user extension, an administrator must first verify the Call Forward status of the user extension for which CFW is to be activated. That is, whether Call Forward is enabled or disabled, and the destination number that is configured for the call forward.

The CFW status is displayed only for an extension that can be forwarded by another user. If the only station that can execute CFW is the one on which the extension is the call appearance, the line is not displayed.

This means that:

- There must be at least one station configured that can manage CFW on behalf of this extension. The station can monitor the CFW status and manage the target CFW destination number if CFW is active for this extension.

- If no extension can manage CFW on behalf of this extension, CFW status is not displayed.

You can also use this procedure to troubleshoot CFW problems.

Procedure

1. Log into the Avaya Breeze® platform CLI by using administrative credentials.

2. Run the following command:

   endpointShow <extension>

   Where, *<extension>* is the extension number on behalf of which CFW is to be configured. That is, extension number of the boss.

   For example, **endpointShow 1000234**

3. Examine the output.

   The output contains information about the call forward status and the CFW destination number that is configured for the extension.

   For example:

   - CFAC Status: Enabled, Number: 1225755

   - CFAC Status: Disabled

Configuring an endpoint for Busy Indicator and call forwarding on behalf of another user station

About this task

A system administrator can use this procedure to configure Busy Indicator and enable a user station to Call Forward All Calls (CFW) on behalf of another user station.

⊛ **Note:**

- CS 1000 and the station firmware of CS 1000 stations have fixed button numbers, which are presented as context-sensitive soft keys, for certain features, such as the **call-fwd** button that is used to manage call forwarding on behalf of another user extension. Device Adapter maintains this end user experience. As a result, System Manager maintains this user experience by providing programming capabilities for these buttons.

- Therefore, in System Manager, some buttons, such as the **call-fwd** soft key on button number 19 for endpoints with soft keys, are reserved for configuring **call-fwd** for the user's endpoint, that is, the secretary's phone. The secretary can use this button to forward the inbound calls that are received on the secretary's phone to another user extension. Ensure that you do not specify an extension number in the **Extension** field that corresponds to this **call-fwd** button. For more information, see Forward button for

[call forwarding all calls does not appear on the UNIStim or M3900 series digital desk phone](#) on page 293.

You can configure one or more of the remaining feature buttons as Forward buttons to enable CFW on behalf of another user extension, that is, the boss's phone. You must specify the extension number of the boss in the **Extension** field that corresponds to this **call-fwd** button. A secretary can use this Forward button to manage CFW on behalf of the boss's extension.

- If you are configuring the **call-fwd** button for a digital or UNIStim endpoint to allow a user to call forward all calls on behalf of another extension, Avaya recommends that you do not use the CS1k-1col and CS1k-2col template types. If you use these template types and if the user does not use the optional display module that was available for purchase with these endpoints, the user cannot view the information that is being entered. Even with the display, the user might have to use paper labels to label the buttons on the endpoint to indicate the CFW destination on behalf of another extension.

- Call forwarding on behalf of another extension feature is not supported on 2001 and 3901 endpoints.

The user who is managing call forwarding on behalf of another extension is generally an administrative support person such as a receptionist, secretary, office administrator, or any person who provides support to the other parties.

This user might want to manage Call Forward All Calls on behalf of more than one user extension. In this scenario, an administrator must configure a separate **call-fwd** button for each extension that the user wants to manage.

Before you begin

Before configuring a user station to allow the user station to activate CFW on behalf of another user extension, an administrator must verify the Call Forward status of the user extension for which CFW is to be activated. For more information, see [Verifying the Call Forward All Calls status of an extension by using the Avaya Breeze platform CLI](#) on page 434.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the secretary's endpoint for which you want to configure Busy Indicator and CFW for another user extension, and then click **Edit**.

5. Depending on the endpoint type, click the **Feature Buttons** or **Button Modules pages** tab.

   ✱ **Note:**

   This assigns the feature to a programmable feature key and not to a reserved soft key.

6. On the Edit Endpoint page, click the **Button Assignment** tab.

7. Do the following to configure the Busy Indicator button:

   a. In the **Button Label** field corresponding to the button number that you want to configure as Busy Indicator, type a name for the Busy Indicator button label. For example, BI.

      This label appears on the endpoint along with the destination number.

      The default label is BusyFwd on the secretary's phone.

      * **Note:**

      Avaya recommends that you use the default label. If you use a label other than the default label and if an endpoint uses a language other than English, Device Adapter cannot translate the label to the other language.

   b. In the corresponding **Button Feature** field, click **busy-ind**.

   c. In the **TAC/Ext** field, type the extension number of the boss.

   * **Note:**

   If the ProVision tool is used to configure the Busy Indicator button, you can skip this step. However, verify the button label and the status of the monitored extension.

8. Do the following to configure a Forward button that the secretary can use to manage CFW on behalf of the boss's phone:

   a. In the **Button Label** field corresponding to the button number that you want to configure as a Forward button, type a name for the Forward button.

      The Forward button appears with this name on the secretary's phone.

      Because the secretary might be managing CFW on behalf of two or more extensions, Avaya recommends that you provide a button name that the secretary can easily identify. For example, the name of the party on behalf of whom the secretary would be managing CFW.

   b. In the corresponding **Button Feature** field, click **call-fwd**.

   c. In the corresponding **Extension** field, type the extension number of the boss.

   * **Note:**

   This step is manual because ProVision cannot distinguish between extensions that require only monitoring and extensions that require CFW in addition to monitoring.

9. Click **Commit**.

Remote call forward handling on a destination number where CFW is enabled

> ✱ **Note:**
>
> Ensure that **Chained Call Forwarding** is enabled on Communication Manager.

Call forward on an extension can interact with remote CFW in the following ways:

- If a Phone A initiates CFW to phone B, and phone B is remotely CFW to phone C, then inbound calls on phone A are forwarded to phone C.

- If phone A is remotely CFW to phone B, and phone B initiates CFW to phone C, then inbound calls on phone A are forwarded to phone C.

- If a user locally initiates CFW, a remote CFW overrides the local CFW.

Enabling remote call forwarding

About this task

For example, if phone A has set the extension number of phone B as CFW destination number, and phone B has set the extension number of phone C as the CFW destination number, then to enable the inbound calls on phone A to be forwarded to phone C, you must enable the **Chained Call Forwarding** feature on Communication Manager.

Before you begin
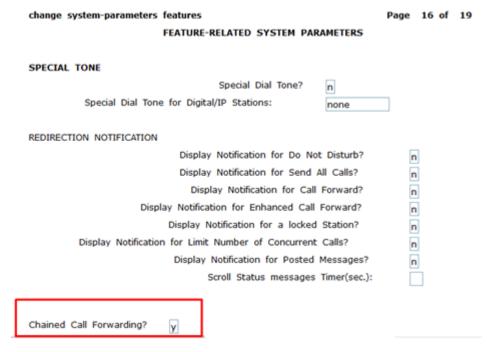
You must have administrative rights to access the Communication Manager CLI.

Procedure

1. At the Communication Manager CLI command prompt, run the following command:

   ```
   change system-parameters features
   ```

2. On page 16, select the **Chained Call Forwarding** check box.

```
change system-parameters features                          Page  16 of  19
                    FEATURE-RELATED SYSTEM PARAMETERS


SPECIAL TONE
                                  Special Dial Tone?    n
                Special Dial Tone for Digital/IP Stations:    none


REDIRECTION NOTIFICATION
                      Display Notification for Do Not Disturb?        n
                      Display Notification for Send All Calls?        n
                        Display Notification for Call Forward?        n
               Display Notification for Enhanced Call Forward?        n
                      Display Notification for a locked Station?      n
           Display Notification for Limit Number of Concurrent Calls? n
                      Display Notification for Posted Messages?       n
                          Scroll Status messages Timer(sec.):



Chained Call Forwarding?    y
```

Busy Indicator feature operation

Dialing the boss's phone number from the secretary's phone
Procedure

While the boss's phone is in an idle state, on the secretary's phone, press the Busy Indicator button that is configured to monitor the boss's extension.

The default label for this button is BusyFwd.

Device Adapter dials the BI number of the boss.

Transferring a call from the secretary's phone to the boss's phone
Procedure

1. While on the call on the secretary's phone, press the Transfer button.

2. Press the BusyFwd button.

3. Press the Transfer button.

   Device Adapter transfers the call to the BI number of the boss.

Redirecting a call from the boss's phone to the secretary's phone

Procedure

Use the Call Forward feature to redirect a call from the boss's phone to the secretary's phone.

The BusyFwd key is not supported on the boss's phone.

Call Forward All Calls on behalf of the boss's extension feature operation

The user operation to manage Call Forward All Calls (CFW) on behalf of the boss's extension might differ depending on the endpoint type.

If the secretary's phone has a Forward key configured for the secretary, then the user operation might differ for this Forward key and the CFW soft key which is configured to manage CFW on behalf of the boss's phone.

Depending on the specific station type, the soft keys and button labels may differ between the Forward button that is configured for the secretary's extension and the Forward button that is configured to manage CFW on behalf of the boss's extension. This can have an impact on a subset of the other operations.

Specifying a new CFW destination number on behalf of the boss's extension from UNIStim and digital phones

Procedure

1. On the secretary's phone, press the Forward button that is configured for the boss's extension.

2. Type the CFW destination number on behalf of the boss's phone.

3. Press the Forward button again to activate CFW on behalf of the boss's phone.

Result

- If the destination number resolves to a valid number, or a valid routing to the number such as a valid country code, area code, and local exchange prefix:
  - The lamp or icon state for the Forward button indicates active.
  - Inbound calls on the boss's extension are forwarded to the specified destination number.
  - Device Adapter saves the specified destination number and uses the same destination number when the CFW is reactivated.
  - The forwarded extension indicates the forwarded status.
- If the destination number resolves to an invalid number:
  - The phone displays **release and try again** briefly, and then reverts to the idle state.
  - Inbound calls on the boss's extension are not forwarded.
  - Device Adapter generates error logs in the `dsa.log` file that is located at:

```
/var/log/Avaya/services/DeviceAdapter/dsa.log
```

Deactivating CFW on behalf of the boss's extension from UNIStim and digital phones

Before you begin

An administrator must configure your station with an additional **call-fwd** button by using the feature key. This **call-fwd** button must be assigned the extension number on behalf of which you want to manage CFW, that is, the boss's extension.

For more information, see [Configuring an endpoint for Busy Indicator and call forwarding on behalf of another user station](#) on page 435.

You can deactivate CFW on behalf of the boss's phone only if CFW is active for the boss's phone, and inbound calls on the boss's extension are forwarded to the destination number.

Procedure

When the Forward button that is configured for the boss's phone is an active state, press the Forward button.

Result

The call forwarding is cancelled:

- The lamp or icon state for the Forward button indicates inactive.
- Inbound calls on the boss's extension are no longer forwarded to the destination number.

Reactivating the most recent CFW destination number on behalf of the boss's extension from UNIStim and digital phones

Before you begin

Inbound calls on the boss's extension must have been successfully forwarded to the destination number in the past. Currently, CFW on behalf of the boss's extension must be in an inactive state.

Procedure

1. On the secretary's phone, press the Forward button that is configured for the boss's extension.
2. To reuse the existing CFW destination number, press the Forward button again.

Result

CFW is activated on behalf of the boss's phone.

If the destination number resolves to a valid number, or a valid routing to a number such as a valid country code, area code, and local exchange prefix:

- The lamp or icon state for the Forward button indicates active.
- Inbound calls on the boss's extension are forwarded to the destination number.
- The forwarded extension indicates the forwarded status.

Note:

Because call forward to the destination number was successfully activated in the past, reactivation should succeed. However, there might be some administrative changes done in between the time deactivation and reactivation was done. For example, the number was another extension in this environment and that station is deleted. Therefore, in such cases, reactivation fails.

Verify the CFW destination number on behalf of the boss's phone when CFW is active

Prerequisites for verifying the CFW destination number when CFW is active on the boss's phone

An administrator must configure the secretary's station with an additional **call-fwd** button by using the feature key. This **call-fwd** button must be assigned the extension number on behalf of which the secretary wants to manage CFW, that is, the boss's extension.

For more information, see [Configuring an endpoint for Busy Indicator and call forwarding on behalf of another user station](#) on page 435.

CFW on behalf of the boss's extension must be active on the secretary's phone, and inbound calls on the boss's extension must be forwarded to the destination number.

Verifying whether calls are forwarded on behalf of another extension

About this task

Note:

In Device Adapter, you cannot use the soft keys on a 39xx or UNIStim phone to verify whether calls are forwarded on behalf of another extension, that is, the boss's extension. These soft keys are reserved for CFW of the station itself, that is, the secretary's extension.

However, the icon of the CFW button that is configured for the boss's extension indicates the current CFW status.

Procedure

On the secretary's phone, verify the lamp state of the Forward button that is configured for the boss's extension.

Result

- If lamp is lit, CFW is activated on behalf of the boss's phone.
- If lamp is dark, CFW is not activated on behalf of the boss's phone.

Verifying the CFW destination number on behalf of another extension

About this task

Note:

In Device Adapter, you cannot use the soft keys on a 39xx or UNIStim phone to verify the CFW destination number on behalf another extension, that is, the boss's phone.

However, the icon of the CFW button that is configured for the boss's extension indicates the current CFW status. As a workaround you can deactivate and re-activate CFW to verify the CFW destination number.

Use the following procedure to verify the CFW destination number by deactivating, and then reactivating CFW.

Procedure

1. On the secretary's phone, press the Forward button that is configured for the boss's extension.

   The current CFW is cancelled.

2. Press the Forward button that is configured for the boss's extension again.

3. Do any one of the following:

   • To reuse the existing CFW destination number, verify that the existing CFW destination number is correct, and then press the Forward button again.

   • To change the CFW destination number, enter the new CFW destination number, and then press the Forward button again.

Result

CFW is activated on behalf of the boss's phone.

• If the destination number resolves to a valid number, or a valid routing to a number such as a valid country code, area code, and local exchange prefix:

   - The lamp or icon state for the Forward button indicates active.

   - Inbound calls on the boss's extension are forwarded to the specified destination number.

• If the destination number is invalid:

   - The lamp or icon state for the Forward button indicates idle.

   - Inbound calls on the boss's extension are not forwarded.

Call forward

Call Forward feature description

The three basic options supported for Call forward are:

• Call Forward, All Call: Call Forward All Calls (CFW) automatically forwards incoming calls to another destination, within or outside the system. Only calls to the station extension (Prime DN on CS 1000) or any single-appearance secondary number on the telephone are forwarded. Numbers shared with other users cannot be forwarded in this manner. Outgoing calls can still be placed from the telephone when Call Forward is active.

- Call Forward, No Answer: Call Forward No Answer automatically forwards unanswered calls to another destination. The customer can specify the number of rings before the system invokes Call Forward No Answer. CS 1000 supports a default of four rings.

- Call Forward, Busy User: Call Forward Busy (CFB) automatically routes calls to a target when a telephone is busy.

These options allow the calls to be treated differently based on the call type. This permits calls from internal parties to receive a different treatment than external parties.

An option also exists to allow or deny a user to call forward to an external number.

⊛ **Note:**

The **Call Forward Busy** and **Call Forward No Answer** are configured to terminate at the same destination.

Prerequisites for call forwarding

The ProVision and Nortel Migration Tool provide the path to configure migrating endpoints. The migration operation discards all class-of-service codes. If there is an applicable class-of-service and configuration on the station, the migration tools create the coverage path data and assign it to the endpoint. The class-of-service is not migrated to the features.

To manually configure the service, refer to "Call Forwarding administration" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

The key aspects are:

- Call Forward All Calls is a button or FAC related action. Ensure that the stations and FACs are defined correctly.

- Ensure that the **call-fwd** button for the user extension is configured properly in System Manager.

  For more information, see .

- For Call Forward No Answer and Call Forward Busy, ensure that a coverage path exists that matches the desired target. If it does not already exist, create a new coverage path.

- The station must use the identified coverage path.

- Analog stations must use the FAC model.

⊛ **Note:**

Communication Manager supports the **Call Forward Busy/No Answer** button to allow a user to enable or disable the service from the endpoint. This was not supported for the CS 1000 endpoints. To use this service, the administrator must follow the procedures in "Call Forwarding administration" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide. This button is not migrated and any use of the button must conform to the Communication Manager handling.

Feature operation for Call Forwarding

Call Forward No Answer and Call Forward Busy can be administered on the station through System Manager. Call Forward All Calls can be activated and deactivated by user operations.

Call forward on stations without a Call Forward key

Some stations, such as analog stations, do not have feature buttons. Other stations might be configured without a Call Forward button, but allow to activate or deactivate call forwarding by using feature access codes.

Activating call forward by using Feature Access Code
Procedure

1. Go off hook.
2. Dial the Feature Access Code (FAC) for **Call Forwarding Activation All**.
3. Listen for a dial tone.
4. Dial the extension number of the destination.
5. Disconnect the telephone after you hear three-beep tone.

Deactivating call forward by using Feature Access Code
Procedure

1. Go off hook.
2. Dial the Feature Access Code (FAC) for Call Forwarding deactivation.
3. Disconnect the telephone after you hear the three-beep tones.

Call forward on stations with a Call Forward button or soft key

Some digital and UNIStim stations provide a soft key to perform call forwarding operations. You can program this soft key as unused or call forwarding only.

Other stations use a programmable feature key, which is configured as the call forwarding key.

You can use the call forwarding button or soft key to activate or deactivate call forwarding, and verify the destination for call forwarding.

Activating call forward by using call forward feature key
Procedure

1. Press the **Call Forward** feature soft key (where applicable) or button.
2. If the desired destination is not already present, enter the extension number of the destination.
3. Press the **Call Forward** feature soft key or button again.

Verifying destination for call forwarding by using call forward feature key

About this task

Not all endpoints provide a **check the forward value** option. The following applies only to endpoints that can display the current value.

The display must indicate that the call is forwarded, by text in the display and/or icon/lamp states with the **Forward** button or soft key.

Procedure

1. Press the **Call Forward** feature soft key (where applicable) or button.

2. Verify the destination. If the destination is correct, do the following:

   a. For endpoints without the **Ok** and **Cancel** soft keys, press the **Call Forward** feature soft key (where applicable) or button. Press the soft key or button once to activate call forward and twice to return to the inactive state.

   b. For endpoints with the **OK** and **Cancel** soft keys, press the **Cancel** soft key.

Deactivating call forward by using call forward feature key

About this task

The display must indicate that the call is forwarded, by text in the display and/or icon/lamp states with the **Forward** button or soft key.

Procedure

1. Press the **Call Forward** feature soft key (where applicable) or button.

2. For endpoints presenting the options **OK** and **Cancel**, press the **Cancel** soft key.

Feature interaction of call forwarding

Call Forward All Calls will over-ride **Call Forward Busy/No Answer**.

⊛ **Note:**

Only the system administrator handles the CS 1000 administration functions, a user can not change the call forward busy or call forward no answer destination on CS 1000. This is not a CS 1000 function.

The feature that allows a user to change the call forward busy and call forward no answer destination is an Avaya Aura® function.

To change the **Call Forward Busy/No Answer** destination from an internal telephone, refer to Communication Manager documentation.

Call Pickup

Call Pickup feature description

Use the Call Pickup feature to answer calls for one another.

The normal Call Pickup feature requires that users be members of the same pickup group.

With the related Extended Call Pickup capability (Group Pickup), users in one pickup group can answer the telephones for users in another pickup group.

With the related Directed Call Pickup capability (Directory Number Pickup), users can specify what other telephone they want to answer. Pickup groups are not needed with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this capability.

Prerequisites for Call Pickup

The ProVision and Nortel Migration Tool provide the path to configure migrating endpoints.

By detecting the class, the applicable pickup group data is created (the group or extended group) and the class of restrictions data is created and assigned for a DN pickup. After the data has been created and the button assigned, the class of service values are discarded.

For information about manually configuring the service, see Call Pickup administration in *Avaya Aura® Communication Manager Feature Description and Implementation*.

Ensure that the following are configured:

- System Parameters Features for extended and direct Call Pickup must be enabled, to use the Group Pickup or DN Pickup capabilities.
- Call pickup groups and extended call pickup groups are configured.
  - An extended call pickup group provides the scope within which a user in one group may do a group pickup from another group.
  - Extended groups support only 25 groups within the extended group.

Endpoints

- The stations are configured with buttons corresponding to the Communication Manager nomenclature. However, the button display will conform to CS 1000 displays.
  - Normal call pickup: **call-pkup**.
  - Call pickup from another group: **ext-pkup**.
  - Directed (Directory Number) Call Pickup: **dir-pkup**.
- Features:
  - A group must either exist or be created, the user assigned to the pickup group, and the pickup key assigned to the group, if the user is to be able to pick up calls within the user's group.

- A simple extended group and its internal groups must be created, the user assigned to one of the groups, and the extended group pickup button (ext-pkup) assigned to the set, if the user is to be able to pick up calls within another group.

- A class of restriction must be assigned permitting the user to pick up calls based on extension, the user assigned this class of restriction, a second class of restriction defined to allow users to be picked up, the class of restriction assigned to the set to be picked up, and a direct pickup (dir-pkup) button assigned to the station of the user doing the call pickup, if the user is to be able to pick up calls at a specific extension.

• Stations without class PUA can still have other users pick up calls from this station, provided the station belongs to a call pickup group.

Ringing number pickup within your group

Procedure

1. Select a line appearance.

2. Press the **Pickup** key.

Ringing number pickup within another group

About this task

Call to a user in a pickup group within a shared extended group can be picked up either by a user in the same pickup group, or by a user in any other group within the extended group. However, a pickup group outside the extended group cannot retrieve group calls from any group within the extended group.

The group numbers on CS 1000 may differ from the group indexes after migration. In this case, inform the users about the indices for the groups within the extended group.

Procedure

1. Select a line appearance.

2. Press the **Group Pickup** key.

3. Dial the group index number for the call to be picked up from the other group.

4. Press **#**.

Directory number pickup within your group

Procedure

1. Select a line appearance.

2. Press the **Directory Number Pickup** key.

3. Dial the extension number that you want to pick up.

4. Press **#**.

Call Pickup feature interaction

For information about interactions between the Call Pickup and other features, see the Communication Manager documentation.

Call Waiting

Call Waiting feature description

Call Waiting notifies a telephone user on an established call (internal or external) that an external call is waiting to be answered.

Call Waiting feature for analog stations

If two or more users share the extension (bridged and call appearance), the call waiting indication will not apply.

In CS 1000, the user can enable or disable call waiting by using the FFC (equivalent to the FAC in the Communication Manager configuration). There is no corresponding FAC, so the feature is completely controlled by class of service values.

While on a call, the user may receive a second call; an audible indication is provided. The user can toggle between the two calls using a switch hook flash, although the user cannot conference the two together.

✱ Note:

The Call Waiting feature for CS 1000 analog stations is implemented in software on the Device Adapter; SIP endpoints are handled as multi-appearance endpoints, and therefore any analog endpoint on the Device Adapter appears to be multi-appearance to the Communication Manager. The user experience is that of an analog endpoint, though.

Call Waiting for multi-line capable stations

On the CS 1000 endpoint, Call Waiting notifies a telephone user on an established call on a Single Call Arrangement DN button (both internal or external calls), that an external call is waiting to be answered. When an external call comes, and the user is on a call, the Call Waiting lamp flashes and a buzz sounds through the speaker.

With the Communication Manager, the endpoints have more than one line appearance for the calls, and the call is presented to the second, third, or fourth appearance button.

The Device Adapter uses the added call appearance button to provide call waiting. Bridged appearance buttons (shared with other users) do not get call waiting.

Call Waiting feature administration general

The ProVision and Nortel Migration Tool provide the path to configure migrating endpoints.

To manually configure the service, refer to the following two procedures for the analog stations and for digital and UNIStim stations.

Call Waiting feature administration for analog stations

Before you begin

⊛ **Note:**

This may be created in the Communication Manager or on the System Manager.

Procedure

1. Carry out administration tasks required to edit an existing station or create a new one, based on the mechanism used.

2. Ensure the features include:

   a. WTA – Warning Tone Allowed (to receive the audio indication of a waiting call)

   b. CWA – Call Waiting Allowed.

3. Ensure a second line appearance is present in the button assignment.

Call Waiting feature administration for digital and UNIStim stations

Before you begin

This may be created in the Communication Manager or on the System Manager.

Procedure

1. Carry out administration tasks required to edit an existing station or create a new one, based on the mechanism used.

2. Ensure at least one additional call appearance is present in the button assignment. This would be places where the call waiting key was placed on the CS 1000 endpoint.

3. If the user is to be able to switch between the two calls without using the "hold" button explicitly, configure "auto-hold".

Call Waiting feature operation

Procedure

1. The user is busy on the call appearance DN key.

2. A call is placed to this DN number.

3. The second call appearance key flashes.

4. If the user presses the ringing line appearance:

   a. Auto-hold: The current call is placed on hold and a new call is established with the incoming request. The user can switch between the calls by pressing the appearance buttons.

   b. No auto-hold: Answering the second call releases the first call. Alternatively, the user can place the current call on hold and press the second call appearance button. A connection is established to the new call and the user can switch between the two using the Hold method.

Call Waiting feature interaction

Refer to the Communication Manager documentation for Considerations for Call Waiting Termination, Interactions for Call Waiting Termination, Interactions for Call Pickup, Interactions for Hold, Interactions for Conference.

Callers list

Callers List feature description

Personal Directory (PD), Callers List, and Redial List are intertwined within the digital stations that support this capability (redial and callers only on the 3903, but redial, callers, and directory on the 3904 and 3905) or PD data on PPM (UNIStim).

The Callers List is a call log feature. The content of the list is generated during call processing. You cannot modify this content. However, you can delete or, in some cases, copy entries to the Personal Directory.

The 3903 phone has a greatly reduced capacity for storing this data. The following is the Callers List size:

- 3903 phones: 10 entries

- All other phones: 100 entries

Callers List support the following for devices that support Personal Directory:

- Maximum entries = 100 (20 for the 3903 phone)

- Maximum characters in name = 24

- Maximum characters in DN = 31

- Multiple actions:

    - Dial DN of an entry.

    - Edit the digits of an entry.

    - Copy the information of an entry and add it to the Personal Directory, allowing details to be modified.

    - Delete an entry.

- Password protection to control access to the Callers List.

- One-minute time out to exit if the user is idle.

PPM stores the most recent 100 call log entries, which are saved in the format of one entry per one call format. When the device is logged in, the saved call log entries are separated into Callers and Redial list.

This is invisible to Communication Manager. It is handled either by the telephone itself (3904) or Device Adapter (UNIStim).

Callers List is an automatic feature of some digital and UNIStim stations.

Stations with a display and the Directory/Log button can provide a trail of the called and calling parties and can copy entries from either the called (Redial List) or calling party (Callers List) lists into a Personal Directory. This process is independent of any corporate directories.

The 39xx stations that have this capability handle it internally in the phone. For added robustness, the UNIStim stations that support the Callers List feature, provide the callers list by using PPM as the data warehouse. This permits the PPM call history to survive a reboot of the station.

★ **Note:**

New callers information will be lost after the station reboot.

If primary Session Manager fails and secondary Session Manager becomes available, then after a station reboot some of the Callers list entries can be lost.

For information about changing the station control password to protect the callers list data, see

Dialing a number from a callers list

About this task

The callers list is populated when the call is received. This is the earliest that a name is available. However, there may not be a name present.

You can access the callers list from the soft keys of an idle endpoint.

Procedure

1. Do one of the following to access the callers list:

   a. On an idle endpoint, press the **Callers** soft key.

   b. On an idle endpoint, do the following:

      a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

      b. Scroll down to select the Callers List from the options.

      c. Press Select.

2. Use the up and down arrows to scroll through the stored entries.

   You may need to select between Old entries and New entries first.

   Calls that provide name information display the calling-party name. Otherwise, no name is present.

3. When you select an entry, a triangle facing to the right is present. Use the right arrow to view more details.

   You can use the right arrow when a number is displayed. Clicking the right arrow shows the number saved as the name as well as being saved as the number.

4. Use the left arrow to return to the list.

5. Press dial to call the party.

Editing a Callers List entry

About this task

You cannot edit a name in the callers list. You can edit a number, as it may not be successfully dialed in the form it was received. For example, the number received is a short form such as 5550111 of the number 1-555-555-0111.

Procedure

1. Do one of the following to access the callers list:

    a. On an idle endpoint, press the **Callers** soft key.

    b. On an idle endpoint, do the following:

        a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

        b. Scroll down to select the Callers List from the options.

        c. Press Select.

2. Use the up and down arrows to navigate to the entry that you want to edit.

    You may need to select between Old entries and New entries first.

3. Press Edit to edit the number.

4. If the number is not the same as any existing entry, the number is saved.

    If the edited number is the same as an existing entry, the number is not saved.

5. Press dial to call the party.

Copying an entry from the Callers List to the Personal Directory

About this task

This procedure is similar to the procedure of copying an entry from the redial list.

Procedure

1. Do one of the following to access the callers list:

    a. On an idle endpoint, press the **Callers** soft key.

    b. On an idle endpoint, do the following:

        a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

        b. Scroll down to select the Callers List from the options.

        c. Press Select.

2. Use the up and down arrows to navigate to the entry that you want to copy.

3. Press **Copy** to copy the entry.

    Use the dial pad to modify the name if necessary.

4. Press the **Next** soft key.

    Use the dial pad to modify the phone number if necessary.

5. Press the **Done** soft key.

6. Exit by clicking on the stop sign or by waiting for the one-minute inactivity timer to expire.

7. Enter the Personal Directory.

   The new entry is present in the Personal Directory. You can edit, delete, or modify the entry.

Deleting a Callers List entry

Procedure

1. Do one of the following to access the callers list:

   a. On an idle endpoint, press the **Callers** soft key.

   b. On an idle endpoint, do the following:

      a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

      b. Scroll down to select the Callers List from the options.

      c. Press Select.

2. Use the up and down arrows to navigate to the entry that you want to delete.

3. Press Del to delete the entry.

   You can also delete the entire list by pressing Del without selecting an entry.

4. Confirm the deletion.

5. Press Yes to delete the entry.

6. Exit by clicking on the stop sign or by waiting for the one-minute inactivity timer to expire.

Callers List feature interaction

Calling-party privacy requested by any intervening system or network may prevent the caller from being called. Because of services enroute, the calling-party number may be anonymous. Therefore, the number is not callable.

The caller may have routed through the originating network with an abbreviated caller ID, and then transited to the local system without having the number made fully qualified. Because of this, the calling number received may be formatted invalidly; and therefore, unreachable.

The caller may have a number that cannot be dialed directly. Because of this, the calling number received may be unreachable.

Conference (Ad hoc conference)

Users with endpoints capable of end-to-end signaling can access conference bridges by dialing in to the bridge and entering any necessary bridge code and password.

Conference (Ad hoc Conference) feature description

UNIStim and Digital Stations

Use the Conference feature, with the associated **conf** button, to create a conference without the assistance of an attendant.

A user with a multiple appearance telephone with a **conf** button can create a conference with as many as six participants.

A user with a single-line telephone can create a conference with as many as three participants.

Each of these three participants can then add another participant. Thus, a user who has a single-line telephone can create a conference call with as many as six participants.

A **Conference** key configured for UNIStim and 39XX endpoints at a fixed position and 2XXX digital endpoints at a programmable position. Communication Manager considers it as a restricted call appearance that cannot receive any incoming call but can only be used for outgoing calls placed in the process of establishing a conference. Device Adapter will treat this button as a CS 1000 **Conference** key with existing localization.

The CS 1000 TN can be provisioned with either CLS A03 or A06. This means the user can establish a 3-way or 6-way conference. There is no such limitation for a Communication Manager station, all conference buttons are treated as six party conference.

Certain endpoints display **Conference** and a number, for example, CONFERENCE 3. The number displayed with the **CONFERENCE** label on the phone is the number of conference participants other than the current user. For example, if a user was participating in a conference with 2 other participants, the CONFERENCE label would display **CONFERENCE 2**.

Analog Stations

Conferences are made by using a hook flash and subsequent operations.

CS 1000 analog station requires the transfer class-of-service to be permitted in order to do any conferencing because there is no button to program with the transfer or conference function. The absence of the button does not indicate that transfer or conference is denied.

On CS 1000, the transfer service automatically allows three-party conference. To do a transfer, three-party conference must be allowed. On the other hand, for CS 1000, it is necessary to add a class-of-service to permit a six-party conference.

The Transfer function is available only during an active call. The call may be an existing conference, when six-party conferencing is allowed.

When the user does a switch hook flash, the active call, including conferences that are below the maximum size for an ad hoc conference, is put on hold. The user receives a new dial tone and can dial the transfer target number.

After the far-end is reached, the user can either complete the transfer (blind) or wait until the far-end answers the call, and then complete the transfer (consultative). The transfer completion is done by hanging up.

If the user wants to create a conference instead, the user does a switch hook flash after the destination has answered. All parties are now in the call.

Transfer can be cancelled by doing the switch hook flash while the call is ringing.

Conference feature administration

The ProVision and Nortel Migration Tool provide the path to configure migrating endpoints.

See Administering Conference feature parameters for the steps in configuring the Communication Manager to provide conference. Stations are configured differently based on the endpoint type.

Administering endpoints with automatic conference button locations

About this task

Analog stations have a **virtual** feature button 18 configured in the endpoint template as a conference button. Unless this button is removed in the configuration, it will be the button that is used on Communication Manager, and conferencing users will be allowed. Device Adapter maps between the base operation (hook flash) and the button function.

UNIStim, M3903, M3904, and M3905 stations program the conference button as button 18. However, this is a soft key in the context-sensitive map. It is made available only when a call is active.

Procedure

1. Start to administer or create the station.

2. If not already done, select the correct template and model for the endpoint:

   a. CS1k-IP for UNIStim sets.

   b. CS1k-ana for analog sets.

   c. CS1k-39xx for 3903, 3904, and 3905 sets. The 3901 and 3902 do not fit this model as well, see the next section.

3. If this station is to support conference, ensure button 18 is assigned as the conference button. Otherwise, remove any feature definition for this button.

Administering digital endpoints where the conference button is not fixed

About this task

M3902 has the conference or transfer mapped to button 4, a fixed key reserved for either conference or Transfer. It is not usually placed on any other button. Only, the three soft keys are supposed to be configured as programmable buttons. Note that for the 3902, the soft keys are not context sensitive.

M3901 allows the button to be configured as button 1, 2, 3, 4, or 5. It is accessed by pressing the feature key and then 1, …, or 5 as per the configuration.

The remaining stations allow the user to configure the conference service on any programmable button.

Procedure

1. Start to administer or create the station.

2. If not already done, select the correct template and model for the endpoint:

   a. CS1k-1col for non-39xx digital sets with a single key/lamp pair.

   b. CS1k-2col for non-39xx digital sets with a pair of keys surrounding the lamp pair.

   c. CS1k-39xx for the 3901 or 3902.

3. If not already done, select the correct type in the general options for the endpoint. Refer to the list of supported digital endpoints.

4. If this station is to support conference, program the applicable button as the conference button:

   a. 3901: ensure one of the buttons 1-5 is assigned as the conference button.

   b. 3902: ensure button 4 is assigned as the conference button.

   c. 2xxx digital sets: ensure one of the valid buttons is assigned as the conference button.

Administering conference button for analog endpoints

About this task

The classes on CS 1000 analog stations are XFA/XFD, and C6A/C6D:

- XFA – Transfer Allowed: The user can initiate transfer in the manner appropriate for the endpoint. A three-party conference is also allowed.

- XFD – Transfer Denied: The user cannot request a transfer. This class is superfluous in Device Adapter, as absence of permission to transfer is the same as forbidding it.

- C6A – Six-Party Conference Allowed: The user can expand a conference to include up to six parties.

- C6D – Six-Party Conference Denied: The user can only create a three-party conference.

When the migration detects the XFA class-of-service, the tools automatically assign the analog station a conference button at position 18. The class-of-service is not carried over.

This virtual button is used as the basis for the SIP signaling during the feature activation. If needed, this button can be manually added in the features buttons for the CS1k-ana station by using System Manager or Communication Manager to carry out the configuration.

Procedure

1. Start to administer or create the station.

2. If not already done, select the correct template for the endpoint.

   CS1k-ana for the analog stations.

3. If this station is to support conference, program feature button 18 as the conference button.

Setting up conference for UNIStim and digital endpoints

About this task

To create or expand a conference, use the following procedures to add maximum of six parties in the conference. You can also add an incoming call to an existing conference.

Device Adapter does not support merging one conference to another. As an example, if you are already on a conference call using ad hoc conference feature, you cannot merge and join another meet me conference call.

Procedure

1. Do the following to put all current parties on hold:

   a. All except 3901: Press the **conference** key while on an active call.

   b. 3901: Put the call on hold using the **hold** button.

   c. Press the **Feature** button.

   d. Enter the index for the conference feature.

2. When dial tone is provided, dial the number of the party to be added.

3. If the party is not reachable, do the following:

   a. Press **Release** to end the attempt to add the third party.

   b. Press the **line appearance** button to rejoin the second party or second parties.

4. Do the following to complete the conference:

   a. All except 3901, 3903, or 3904: Press the **conference** key again to complete the conference.

   b. 3901: Press the **Feature** button.

   c. Enter the index for the conference feature.

d. 3903, 3904: Press the **Connect** soft key to create the conference.

Setting up a conference for analog endpoints

About this task

To create or expand a conference, carry out the following steps until a maximum of six parties are in the conference. This can be used to add an incoming call to an existing conference.

Device Adapter does not support merging one conference to another. As an example, if you are already on a conference call using ad hoc conference feature, you cannot merge and join another meet me conference call.

Procedure

1. Start with a simple call or a small conference.

2. Begin the conference request by putting all current second parties on hold. Do a switch hook flash.

3. When dial tone is provided, dial the number of the party to be added.

4. Do one of the following

   • If the party is not reachable, end the attempt by doing a switch hook flash.

   • After the called party answers, complete the conference by doing a switch hook flash.

Conference feature interaction

No specific interactions have been identified based on Device Adapter, but interactions between the call transfer on Communication Manager and other services there are described in Communication Manager documentation.

No Hold Conference

Conference (No Hold Conference) feature description

Communication Manager handles all the call operations in the no hold conference feature.

If you are on an active call, then using the no hold conference feature you can establish a conference call without interrupting the current conversation or putting the current caller on hold.

No hold conference feature works with or without a pre-configured destination.

If an endpoint is controlled by a CTI application then a feature key for **Noholdconf** is not required for that endpoint.

If you abort the no hold conference process the original call will remain active.

Configuring No Hold Conference without a pre-configured destination

About this task

The no hold conference feature allows an agent to set up a conference call without interrupting the current conversation.

For example, if an agent presses the no hold conference feature button and then dials an extension the participant that answers the call joins the no hold conference.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the UC endpoint for which you want to configure the no hold conference feature, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In another **Button Feature** field, click **no-hld-cnf**.

   b. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a no hold conference, type a name for the no hold conference button label. For example, No_hld_cnf.

      This label appears on the endpoint.

      If you do not specify a label, the default label that appears on the endpoint is **Noholdconf**.

   If the destination is not pre-configured, an agent can dial the required destination number to add as a participant in no hold conference during an active call.

6. Click **Commit** to save the changes.

Configuring No Hold Conference with a pre-configured destination

About this task

The no hold conference feature allows an agent to set up a conference call without putting the active call on hold.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the UC endpoint for which you want to configure the no hold conference feature, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In another **Button Feature** field, click **no-hld-cnf**.

   b. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a no hold conference, type a name for the no hold conference button label. For example, No_hld_cnf.

      This label appears on the endpoint.

      If you do not specify a label, the default label that appears on the endpoint is **Noholdconf**

6. In the corresponding **Ext** field, type the extension number as the participant of the conference.

   Device Adapter dials the number immediately after pressing the **Noholdconf**

7. Click **Commit** to save the changes.

Creating a No Hold Conference for UNIStim and digital endpoints

About this task

You can set up a conference call without interrupting the current conversation using the no hold conference feature.

Communication Manager handles all the call operations for no hold conference feature.

Device Adapter does not support merging one conference to another. As an example, if you are already on a conference call using no hold conference feature, you cannot merge and join another meet me conference call.

Before you begin

Ensure that you are on an active call and the administrator has programmed **Noholdconf** on one of programmable feature keys or on the expansion module.

If you are a call center agent logged in to a CC phone with an incoming call as ACD or a DAC call, then ensure that you are in the manual-in or auto-in mode to answer the incoming call. For a logged out agent the phone operates as a normal Unified Communications (UC) phone, which does not depend on your login status.

Procedure

1. Do one of the following:

    • During an active call, press the **Noholdconf**

    If an extension number is pre-configured for no hold conference, pressing the **Noholdconf** key dials the pre-configured extension number directly.

    • If the extension number is not pre-configured, do the following:

    - Press the **no-hld-cnf** key.

    - Dial the required number followed by delimiter #.

    Expiry of the inter-digit timer also indicates that the dialing is complete. The inter-digit timer is five seconds after the last digit was entered.

    > ✴ **Note:**
    >
    > The destination number can be an extension number or an external number which you can dial using a PSTN trunk. The destination must not be the Vector Directory Number.
    >
    > You must not press the following feature keys after pressing the **Noholdconf** key to dial a number directly. Pressing these keys will abort the No Hold Conference feature:
    >
    > • Hotline two-way using an abbreviated dialing list
    >
    > • Speed Call

    An active call between you and the caller will continue as long as you dial the number of the participant or until the participant for no hold conference answers the call.

    When the destination number answers the call, a three-way conference is established between you, the caller, and the destination number (pre-configured or a new number).

2. Repeat the previous step to add participants to the existing no hold conference.

    You can add maximum of six participants.

Next steps

Press the **Release** button or place the handset on hook to end the active call.

No Hold Conference feature interaction

No specific interactions have been identified based on Device Adapter, but interactions between the call transfer on Communication Manager and other services there are described in Communication Manager documentation.

Flexible Feature Codes

Flexible Features Codes feature description

The CS 1000 documentation defines Flexible Features Codes (FFCs) as follows:

Flexible Feature Codes (FFCs) are user-defined numbers of up to four digits that can be used in place of existing Special Prefix (SPRE) codes. With DN Expansion (DNXP) package 150, Flexible Feature Codes (FFCs) can be up to seven digits long. The Flexible Feature Code (FFC) feature allows customers to define different dialing codes for different features. There is no limit to the number of FFCs per prompt as long as each one is unique.

This feature allows the use of digits 0 through 9, and the asterisk (*) and octothorpe (#) to activate features. Special Prefix (SPRE) dialing feature is still supported, with or without the FFC feature enabled. However, the Special Prefix (SPRE) must be assigned in LD 15 in order for FFCs to operate for those features that also use SPRE codes.

The *Avaya Aura® Communication Manager Feature Description and Implementation* guide defines Feature Access Codes as follows:

A Feature Access Code (FAC) must contain from one to four characters. These characters can be digits or a combination of digits and a character such as an asterisk (*) or a pound sign (#). If you use a character, you must position this character first in the FAC.

The asterisk (*) and pound sign (#) characters are often used in pairs. You can use one of these characters and digits to activate a feature and the other character and the same digits to deactivate the feature. For example, if you use the asterisk (*) and the digits 2 and 9 to activate the Posted Messages feature, then you can use the pound sign (#) character and the digits 2 and 9 to deactivate the Posted Messages feature.

In practical terms, the implementation is identical, but there may be specific FFCs that do not have a corresponding FAC and vice versa.

Any such gaps are discussed in this section.

Assigning Feature Access Codes to features

Procedure

1. Log in to Communication Manager as administrator and type: `change feature-access-codes`

2. In the field corresponding to the feature to which you want to assign the FAC, type the FAC that conforms to your dial plan.

   You can scroll through the Feature Access Code (FAC) screen to locate the telephone feature that you want.

Some features require more than one FAC. Type an FAC in each required field. For example, type a separate FAC in the **Call Forwarding Activation Busy/DA**, **All**, and **Deactivation** fields.

3. Press Enter to save the changes.

Next steps

Ensure that you notify all users about the assigned FACs.

Modifying or deleting Feature Access Codes that is assigned to a feature

Procedure

1. Log in to Communication Manager as administrator and type: `change feature-access-codes`

2. Navigate to the field corresponding to the feature for which you want to modify or delete the FAC and do one of the following:

   a. To modify the FAC, type a new FAC that conforms to your dial plan.

   You can scroll through the Feature Access Code (FAC) screen to locate the telephone feature that you want.

   Some features require more than one FAC. Type an FAC in each required field. For example, type a separate FAC in the **Call Forwarding Activation Busy/DA**, **All**, and **Deactivation** fields.

   b. To remove an FAC, delete the FAC.

3. Press Enter to save the changes.

Next steps

Ensure that you notify all users about the assigned FACs.

Flexible features codes feature operation

Feature Access Codes (FACs) are used as a mechanism to access the feature. For example, the FAC for Last Number Dialed, which has a corresponding FFC: Last Number Redial, is used as per the description of that feature. The user goes off-hook and dials the FAC.

Flexible features codes feature interactions

No feature interaction is identified for the feature access code that handles itself. There may be interactions on a per-feature basis.

Group Paging

Group Paging feature description

Group paging allows users to call a paging group and make announcement on the speakers of the phones that are within the paging group. Group paging announcements cannot be done on external speakers.

If a group paging call cannot be established with all the members of the paging group, for reasons such as the member phones are off hook, then the user who initiates the group paging hears a busy tone.

To create a paging group, you must:

1. Create a paging group.

2. Assign extensions that you want to add as members of the paging group.

3. Assign an identifying extension for the paging group. Other users and members of the paging group can dial this extension to establish a group page call with the members of the paging group.

4. Assign a Class of Restriction (COR) to the paging group. Users who want to page this group must have the permission to call this COR.

For more information about creating a paging group, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

When a user dials the extension of the paging group, a group page call is presented to all the phones within the group. The group page call is auto-answered by using the speakerphone. Paging is one-way communication. Group members can hear the user who initiates the page, but cannot respond directly.

Limitations of Group Paging

Device Adapter does not support group paging in the following cases:

- Group paging is not supported on bridged appearances. A bridged appearance of a group member does not receive any indication of a call when the page arrives. The bridged appearance cannot bridge onto the page.

- A group paging call is not presented on the phone in the following cases:

  - The group member has an active or a ringing call, or if the extension is off-hook.

  - Send All Calls (Make Set Busy) feature is activated on the phone.

- The user who initiated the group page can put the page on hold, but other group members cannot put the page on hold.

- Group page call cannot be conferenced, transferred, or forwarded to other extensions.
- When using a Device Adapter CC phone in Call Center Elite, supervisors cannot use the Service Observe feature to observe an agent when a group page call is active on the agent's phones.

Group Paging feature administration

Procedure

1. Configure the Hand-Free Allowed (HFA) mnemonic for the endpoint that is a member of the paging group.

   For more information, see Administering a mnemonic on page 339.

   If the HFA mnemonic is not configured for the endpoint, the call is not auto-answered and rings until the call is answered manually.

2. Create a paging group.

   For more information about creating a paging group, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

Hotline two-way

Hotline two-way feature description

Hotline is not a truly native stand-alone feature for the Communication Manager; instead, it is a subset of the Abbreviated Dialing feature. When implemented. To the user it is functionally indistinguishable from CS 1000 hotline.

On the CS 1000, several variants on hotline were defined.

- For digital and UNIStim endpoints, a button was pressed that provided an "auto-dial" to a destination. This may allow options such as "conference/hotline", but when an appearance was selected (or the user pressed the conference or transfer), the system automatically called the hotline destination.
- Analog stations with the basic analog handling called the programmed hotline target by going off-hook.
- One-way and two-way hotline existed:

  - Hotline buttons combine the autodial function with at least the outgoing call capability of a line appearance. One-way hotline can only place outgoing calls from the line appearance key, while two-way allows calls to be received as well as originated from the key.

  - One-way hotline used the key to call a specific destination. The user pressed the programmed hotline key, and the programmed destination (which can be either a number or a speed call list entry) is dialed.

The one-way hotline has no information for call-back; it is an un-callable extension. Therefore, if the CS 1000 endpoint had a prime directory number (an extension assigned to key 0), that was used for the calling party information for the hotline call. Otherwise, the call was anonymous.

- Two-way hotline combines the hotline key and a bi-directional line appearance of a specific DN. It extends the one-way hotline to allow incoming calls to the key, which requires an assigned extension.

As with the one-way hotline, pressing this button selects the line and dials the destination as a single operation. However, as the dialable number for the hotline key is available, the far end user will see the hotline key's extension number and can uses it to call back to the near end hotline key. The two-way hotline service is supported on Device Adapter.

- A hotline destination may be a hotline list entry or a specific extension as the target.

- The Device Adapter provides the ability to automatically dial the hot line target using a line appearance and HTL feature mnemonic. This includes having the call automatically dial on the analog station going off hook.

Hotline two-way feature administration

Typically, the ProVision tools will migrate this capability. If the admin needs to create a station with hotline capability or modify an existing station with hotline capability, it is necessary to note that the buttons indicated in the mnemonics are using the Communication Manager procedure of starting button numbering at 1, and not 0. However, CS 1000 key 0 corresponds to Communication Manager button 1.

Hotline feature mnemonic for digital and UNIStim stations

Feature Mnemonic Legend:

- HTLxxMkNxxxxxxx

    - HTL: Hotline feature.

    - xx: Button number, where the lowest button is 1.

    - Mk: Optional module information.

        - If the button is on the station and not an expansion module, this may be omitted.

        - Otherwise, k is the module number (1, 2, or 3, within the limits of the station's permissible expansion modules).

        - M0 is also allowed to indicate a button on the station.

    - Nxxxxxxxx: The target of the hotline call. This is used for the autodial, and in theory, may be an internal number or an external number such as a cell phone number, possibly with additional content such as authorization codes. The digits are used as a dialed digit string.

    This is always a destination number that other parties can call. Device Adapter receives the hotline's extension from the Session Manager PPM.

- HTLxxMkLyEzzz

    - HTL: Hotline feature.

    - xx: Button number, where the lowest button is 1.

    - Mk: Optional module information.

        - If the button is on the station and not an expansion module, this may be omitted.

        - Otherwise, k is the module number (1, 2, or 3, within the limits of the station's permissible expansion modules).

        - M0 is also allowed to indicate a button on the station.

    - Ly: The list number as configured on the station (abbreviated dial list 1, 2, or 3).

    - Ezzz: The entry in the list.

Administering a digital or UNIStim station with the hotline target as a digit string

About this task

This topic provides information about administering a digital or UNIStim station with the hotline target as a digit string:

Procedure

1. Create the X-Port with the call appearance required for the hotline. The same X-Port is used for both sides of the hotline.

2. Edit or create the station with the "Hotline" button.

    a. Define a bridged appearance button for the hotline. The Device Adapter will provide a localized label "Hotline" for the button. The extension number of the bridged appearance button becomes the Hotline number in terms on CS 1000 Hotline two-way feature.

    b. For a hotline to a specific destination, add the HTL (Hotline) N (number) mnemonic: HTLxxMkNxxxxxxx or HTLxxNxxxxxxx where:

        - HTLxx: xx is the key number (starting with the lowest button numbered as 1). HTL08 would indicate CS 1000 key 7 (the eight button on the phone or expansion module).

        - HTLxxMk: k is the button module number. The value for k may be 0 if the button is on the station itself, or it may be omitted:

            - HTL08M0N: Two-way hotline to the indicated number, using button 8 (CS 1000 key 7), on the phone itself.

            - HTL08N: Two-way hotline to the indicated number, using button 8 (CS 1000 key 7), on the phone itself. The M0 for the module (indicating "not on a module") is implicit.

            - HTL08M1N: Two-way hotline to the indicated number, using button 8 (CS 1000 key 7), on the module 1. Depending on the station this may be set to 1, 2, or 3. Note that the numbering is "per module", as the starting button number changes based on the module used, and the station using the module. "Button 8" is

always button 8 on a module, but whether the first button is 16, 24, or 32 means button 8 may be button 24, button 32, or button 40 on a station, depending on the station type.

- HTLxxMkNxxxxxxx, HTLxxNxxxxxxx: xxxxxxx is the destination number or extension. It may include digits, "*", or "#".

Administering a digital or UNIStim station with hotline lists

About this task

This topic provides information about administering a digital or UNIStim station with hotline lists.

Procedure

1. Define or modify an abbreviated dial list with the desired destination as an entry.

2. Create the X-Port with the call appearance required for the hotline.

3. Define the FAC codes for any Abbreviated Dialing List required. This could include List 1, List 2, and List 3. If only List 1 is used in stations, then the FAC for List 1 suffices, but any list that is used must have the FAC defined.

4. Edit or create the station with the "Hotline" button. Do the following:

   a. Define a bridged appearance button for the hotline. Device Adapter provides a localized label "Hotline" for the button.

   b. Specify required abbreviated list number in CM station's Abbreviated Dialing List 1, List 2 or List 3 fields.

   c. Add the HTL (Hotline) L (list) mnemonic:

   HTLxxMkLyEzzz

   where:

   - xx is the key number (starting with the lowest button numbered as 1) HTL08 would indicate key 7 (the eight button on the phone or expansion module).

   - k is the button module number. K may be 0 if the button is on the station itself, or Mk may be omitted for the station itself. For indicating the modules, k is the button module number 1-3, depending on the station and module type.

   - Ly is list y: L1, L2, or L3.

   - Ezzz Is entry zzz in list y.

Hotline feature mnemonic for analog stations

Analog stations do not have programmable buttons (xx) or modules (Mk). Therefore, the button and module related HTLxxMkNnnnn feature mnemonic for a digital or UNIStim endpoint simplifies to HTLNnnnn on an analog endpoint.

Similarly, the lack of buttons and modules simplifies the HTLxxMkLyEzzz digital or UNIStim hotline list mnemonic to HTLLyEzzz on an analog endpoint.

Administering an analog station with the hotline target as a digit string

Procedure

Do the following to edit or create a station with the Hotline feature:

    a. Ensure that a call or bridged appearance is defined on key 0 and 1.

    b. Add the HTL (Hotline) N (number) mnemonic - HTL*y*Nxxx-xxxx for a hotline to have a specific destination.

       In the mnemonic, y is set to either 0 or 1 and xxx-xxxx is the destination number.

Because an analog phone has two feature buttons (0 and 1), when configuring the hotline feature, it is important to define which button is to be set as the hotline key. For example, hotline call to number xxx-xxxa should be set to key 0 and hotline call to number xxx-xxxb should be set to key 1, where xxx-xxxa and xxx-xxxb are different destination numbers.

Also, when the phone is in an off-hook state, set hotline key to 0 (line-0). However, when the phone is in a call (line-0), set hotline key to 1 and press Flash key one time to either transfer the current call or to connect to a conference call.

> ⓘ **Important:**
>
> When using two feature buttons, ensure that the same configuration type is used for all keys such as Call-App and Bridge-App.

Administering an analog station with hotline lists

Procedure

1. If you are using a hotline list, define or modify an abbreviated dial list with the desired destination as an entry.

2. Define the FAC codes for any Abbreviated Dialing List required.

   This can include List 1, List 2, and List 3. If only List 1 is used in stations, then the FAC for List 1 suffices, but any list that is used must have the FAC defined.

3. Edit or create the station with the Hotline feature. Do the following:

       a. Ensure that a call or bridged appearance is defined on key 0 and 1.

       b. For a hotline that uses a list entry, do the following:

           a. Specify the required Abbreviated list number in CM station's Abbreviated Dialing List 1, List 2, or List 3 fields.

           b. Add the HTL (Hotline) L (list) feature: HTLLyEzzz

             Where:

              • Ly is the list number stored on the station: L1, L2, or L3.

              • Ezzz is the entry zzz in list y.

Managing hotline calls on digital or UNIStim stations

Procedure

Do any of the following:

a. To make a hotline call on a digital or UNIStim station, press the Hotline button.

b. To answer a hotline call on a digital or UNIStim station, press the Hotline button.

c. To clear a hotline call on a digital or UNIStim station, press the Release button or go on-hook.

Managing hotline calls on analog stations

Procedure

Do any of the following:

a. To make a hotline call on an analog station, go off-hook.

b. To answer a hotline call on an analog station, go off-hook.

c. To clear a hotline call on an analog station, go on-hook.

Hotline two-way feature interaction

Do not assign a bridged appearance to the same X-port call appearance to any station other than those involved in the two-way hotline. It may lead to a situation where the hotline key indicates busy with a special icon because another phone is using it.

Incoming calls on hotline buttons may ring visibly and audibly. The audible status is controlled by its bridge-app setting in the Communication Manager station by using the same approach as for the regular bridged appearance keys.

Hotline one-way

Hotline one-way feature description

✳ **Note:**

Device Adapter supports the Hotline one-way feature for UNIStim and digital phones.

Hotline one-way allows an administrator to set a number as an autodial number for a Device Adapter endpoint.

Prior to Device Adapter Release 8.1, the CLID of the X-port number was presented to the far end and a call to the x-port extension was used to ring the user's hotline key.

Since Device Adapter Release 8.1, the following applies for Hotline one-way:

• Configuration of X-port extension for each hotline is not required. Hence, additional endpoint license is not needed.

• Configuration of mnemonic is not required. Instead, Hotline one-way uses the autodial button feature with the number configured on the Communication Manager station.

The CLID of the station along with the Hotline button appears on the endpoint.

✱ **Note:**

The Hotline one-way feature requires a call appearance. If all call appearances are busy and if a user presses the Hotline button, the call attempt fails.

Configuring an endpoint for Hotline one-way

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the endpoint for which you want to configure Hotline one-way, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab and do the following:

   a. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a hotline one-way, type a name for the hotline button label. For example, Hotline.

      This label appears on the endpoint along with the destination number that you configure as the hotline one-way autodial number.

      If you do not specify a label, hotline one-way autodial number appears as the default label on the endpoint.

   b. In the corresponding **Button Feature** field, click **autodial**.

   c. In the **DialNumber** field, type the destination number that you want to configure as the hotline one-way autodial number.

   d. Click **Commit**.

Hotline one-way feature operation

Procedure

The user presses the Hotline button on the phone. Device Adapter does one of the following:

- If a call appearance is available, the call is attempted.
- If all call appearances are busy, the call attempt fails.

Hotline Intercom

Hotline Intercom feature description

> ✱ **Note:**
>
> Device Adapter supports the Hotline Intercom feature for the UNIStim and digital phones.

The Hotline Intercom feature adds an additional capability to the existing Hotline two-way feature that allows a call to be auto-answered after providing a single buzz tone.

Hotline Intercom uses a bridged appearance on the X-port and the enhanced HTLI mnemonic to auto-answer inbound calls and auto-dial the hotline number that is configured for the Device Adapter endpoint. Administrators can use the HTLI mnemonic to the specify the Caller ID (CLID) for which auto-answer must be enabled.

The CLID of an inbound call is considered a match if it contains the string that you specify in the CLID filter of the HTLI mnemonic. For example, CLID 12345678 is considered a match for the filter 2345.

If you configure the CLID filter in the HTLI mnemonic, then:

- For an inbound call that has a matching CLID, Device Adapter provides a single buzz tone and auto-answers the call.
- For an inbound call that does not have a matching CLID, Device Adapter provides a ring tone but does not auto-answer the call.

If you do not configure the CLID filter in the HTLI mnemonic, Device Adapter auto-answers all inbound calls.

If the endpoint is busy on another call, then the current call is put on hold.

A user can answer the intercom call through handsfree or headset, which requires the HFA mnemonic. A user can also answer this call by using the handset.

Configuring an endpoint for Hotline Intercom

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the endpoint for which you want to configure Hotline Intercom, and then click **Edit**.

5. On the Edit Endpoint page, on the **General Options** tab, in the **Features** field, configure the HTLI mnemonic for Hotline Intercom.

   For example, LNA HFA HTLI2N2002F2002.

   You can configure the CLID filter in the HTLI mnemonic to auto-answer calls that have the matching CLIDs.

   If you do not configure the CLID filter, Device Adapter auto-answers all inbound calls.

   For more information about the HTLI mnemonic, see CS 1000 CoS and Avaya Aura feature field mapping on page 322.

6. Click the **Button Assignment** tab and do the following:

   a. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a Hotline Intercom number, type a name for the hotline intercom button label. For example, Hotline.

      This label appears on the endpoint along with the destination number.

      If you do not specify a label, the default label that appears on the endpoint is **Hotline**.

   b. In another **Button Feature** field, click **brdg-appr**.

   c. In the **Button** field, type the button appearance of the X-port where you want to bridge the call.

7. In the **Ext** field, type the extension of the X-port where you want to bridge the call.

8. Repeat Step 4 through Step 7 for the destination phone that you want to pair with this phone for Hotline Intercom.

9. Click **Commit**.

Hotline Intercom feature operation

About this task

This topic explains how a hotline intercom call is handled in a boss and secretary environment.

For example, phone A is the boss's phone and phone B is the secretary's phone. The following HTLI mnemonic is configured on phone A and phone B:

- Phone A: ext1001, button 2 – bridg-app to X-port 2001. Mnemonics: HFA HTLI2N2002F2002
- Phone B: ext1002, button 2 – bridg-app to X-port 2002. Mnemonics: HFA HTLI2N2001F2001

Procedure

1. Phone A user presses button 2.
2. Call arrives on phone B which provides a single buzz tone, activates handsfree, and establishes a speech path.
3. Boss and secretary can speak now.
4. Either party presses the Release button to end the call.
5. Phone B user performs the same operation to call phone A.

Last Number Redial

Last Number Redial feature description

Last Number Redial (LNR), which is defined on a customer and a telephone basis, allows the last number dialed by a user to be automatically stored.

The stored number can be redialed by pressing the primary extension line appearance twice ("double DN/Line Key press"), or by dialing the feature access code on analog telephones.

The number is stored whether the call rings, is busy or answered, or a valid access code is dialed with the number.

Only one number, of up to 24 digits, can be stored at any one time. The new number overwrites the previously stored number.

Note that the Communication Manager and the CS 1000 support the "Last Number Redial" button, but it was used much less frequently than the double key press.

Last Number Redial feature administration

About this task

Refer to the Communication Manager Feature Description and Implementation document for information on configuring the Feature Access Codes.

Before you begin

The endpoint is configured with the last number redial feature configured as a set feature.

Procedure

1. Start to administer or create the station.

2. Program the station Feature with the class of service LNA (Last Number Redial Allowed). Dialed digits are stored in PPM.

Last Number Redial feature operation

About this task

The Device Adapter supports following methods of activating Last Number Redial for stations with line keys (that is, other than analog stations):

Procedure

1. Select a line appearance:

   • Press on a line key.

   • Go offhook.

   • Press the speaker button to go handsfree.

   • Press the headset button.

2. The prior step selected a line appearance. Press the active line appearance a second time.

   The 1210 set only is set up to allow the user to go offhook and press Last Number Redial softkey; the Device Adapter does not support the CS 1000 Last Number Redial feature keys.

Optional 1210 procedure

Procedure

1. Select a line appearance:

   • Press on a line key.

   • Go offhook.

   • Press the speaker button to go handsfree.

   • Press the headset button.

2. Press the Last Number Redial soft key.

Analog Procedure

Procedure

1. Go off hook.

2. Dial the "Last Number Dialed" Feature Access Code.

Last Number Redial Feature Interactions

Refer to the Communication Manager Feature Description and Implementation document for information on feature interactions.

Loudspeaker paging

Loudspeaker paging feature description

Loudspeaker paging allows a user to access the paging resources by dialing the TAC code of the paging zone and make announcements on customer-supplied loudspeakers and radio paging equipment.

Loudspeaker paging feature administration

About this task

For a user experience similar to CS 1000, Avaya recommends that you configure the TAC to match the FFC that is used on CS 1000.

Before you begin

- Ensure that Voice Paging is set up for the Avaya Aura® system. Refer to the *Avaya Aura® Communication Manager Feature Description and Implementation* guide to do the following:

    - Prepare to administer Loudspeaker Paging.

    - Set up Voice Paging over loudspeakers.

- Ensure that you are using an MM711 card for loudspeaker paging.

Procedure

1. Log in to System Manager by using administrative credentials.

2. Click **Elements** > **Communication Manager** > **Element Cut-Through**.

3. Click the Communication Manager instance for which you want to configure the Loudspeaker paging.

4. On the Element Cut Through page, in the **Command** field, type the following command:

    ```
    change paging loudspeaker
    ```

5. Click **Send**.

6. On the Loudspeaker Paging page, do the following:

   a. In the **Port** field corresponding to the zone number, type the physical port number of the paging trunk for this zone.

   b. Under **Voice Paging**, in the **TAC** field, type the TAC code to access the speakers in the corresponding paging zone.

   c. In the corresponding **COR** field, type the class of restriction number that you want to assign to the paging zone for voice paging.

      Valid values are 0 to 995.

   d. In the corresponding **TN** field, type the tenant partition number for voice paging if tenant partitioning is used.

      Valid values are 1 to 100.

7. Click **Done**.

Make Set Busy

Make Set Busy feature description

The Make Set Busy feature in CS 1000 had the following functionality:

The Make Set Busy (MSB) feature allows a Meridian 1 proprietary telephone to appear busy to all incoming calls. Outgoing calls can still be made from the telephone. To activate this feature, a separate MSB key/lamp pair must be assigned. Incoming calls to Multiple Appearance Directory Numbers (MADNs) in the MSB mode are still signified by the indicator next to the Directory Number (DN) key and can be answered even while MSB is active. Calls to any Single Appearance Directory Number on the telephone receive a busy indication.

In the details, the MSB feature provides coverage treatment. For example, if the call to the station would result in redirection to voicemail, when MSB was active the call redirected to voicemail. If no redirection was configured, the caller got busy treatment.

The MSB feature corresponds to the **Send All Calls** feature and button on the Communication Manager system. The **Send All Calls** button is configured as using a coverage path to provide the desired capability.

Administering make set busy

About this task

The Communication Manager analog to Make Set Busy is the **Send All Calls** key. Calls immediately go to Coverage when you press this key. To allow a user to use the Send All Calls

key as Make Set Busy, the administrator must ensure the Coverage script has the same criteria for Send All Calls and Make Set Busy.

Coverage criteria for bridged call appearances are based entirely on the criteria of the primary extension that is associated with the bridged call appearance. If a telephone user activates **Send All Calls** on the primary extension, incoming calls still ring bridged call appearances of that extension, provided a simulated bridged appearance of the call is maintained at the primary extension.

For information about configuring Coverage and Send All Calls, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

The administrator will follow the procedure below:

Procedure

1. Extract the user busy handling for the CS 1000 user, to determine the coverage requirement.

   a. Does the call redirect to voice mail?

      This is the most frequently used case.

   b. Does the call redirect to another user?

      This is used frequently for users in a support group; typically, they redirect to a group hunt list.

   c. Is a secondary call forward used?

      This is uncommon, and usually means the call forwarded to another user, and if the user was unavailable, the call went to voice mail.

   d. Is the call provided busy treatment?

      This is the original handling, but as voice mail got more common, this option became correspondingly less common.

2. On Communication Manager or System Manager, determine whether a new coverage path definition is needed.

   a. If an existing path suffices, reuse that path.

   b. Otherwise, the coverage path is defined.

3. On Communication Manager or System Manager, the **Send All Calls** button is defined for the station, providing the link allowing the user to trigger coverage for all incoming calls.

   The administrator has the option to provide a custom label and will typically label the button as "MakeSetBsy", the label on a 3903 or 3904 endpoint.

Activating or deactivating Send All Calls or Make Set Busy

Before you begin

Ensure that the **Send All Calls**/**Make Set Busy** button is configured.

- To activate **Send All Calls**/**Make Set Busy**, perform the following:

  1. The lamp or icon associated with the button is dark.

  2. Press the **Send All Calls** button, typically, labelled to indicate **Make Set Busy**.

     The lamp or icon lights, and calls redirect as per the coverage defined.

- To deactivate **Send All Calls**/**Make Set Busy**, perform the following:

  1. The lamp or icon associated with the button is lit.

  2. Press the **Send All Calls** button, typically, labelled to indicate **Make Set Busy**.

     The lamp or icon goes dark, and calls no longer redirect as per the coverage defined, unless the applicable service such as Call Forward on Busy applies (the user is active on a call, and no call appearances are available).

Next steps

For information about the Send All Calls feature, see the Communication Manager documentation .

Malicious Call Trace

Malicious Call Trace feature description

A digital or UNIStim phone is assigned a Malicious Call Trace (MCT) button. During an active call, the user presses the **MCT** button, if the call is malicious.

A Feature Access Code (FFC in CS 1000) can be defined to initiate MCT from an analog phone. To trigger the MCT trace on an analog phone, initiate a transfer (do a switch hook flash) and dial the FAC. The user is then placed back in the call with the malicious caller. This can be done with digital and UNIStim phones that do not have an **MCT** button but do have a **transfer** button.

The call is then logged on the server side, including a screen display which is visible to administrator. A limited subset of trunking interfaces to the public network also permit sending the Malicious Call Trace to the PSTN or ISP.

The MCT key is mapped to the Communication Manager button mct-act (MCT Activation). The feature description on CS 1000 and Communication Manager is functionally identical. Device Adapter treats the **mct-act** button as the legacy MCT key providing the default localized label as per the endpoint firmware or reusing the "paper label" for endpoints without label firmware.

Malicious Call Trace feature administration

Common administration for Malicious Call Trace

For information about MCT FAC and configuring the system and trunks for MCT, see *Avaya Aura®
Communication Manager Feature Description and Implementation*.

ProVision Migration administration for Malicious Call Trace

During the migration of the information for the endpoints, if a specific TN being migrated has the
class of service MCTA (MCT Allowed) and an **MCT** button, then the Communication Manager
station being created based on the TN information is assigned an **mct-act** button (MCT Activation)
at same position. Analog stations do not have the button, relying on the FAC, and therefore will not
have a button allocated.

The class of service MCTA is not migrated to the Communication Manager station Features. It
suffices to define the button.

Creating a new station or adding MCT to the existing station

About this task

The norm will be to use ProVision to migrate. However, an administrator might need to create a
station using Communication Manager station programming or might need to add the capability to
an existing endpoint.

Procedure

1. Do one of the following:

   • Create the new station, if required.

   • Otherwise, change an existing station.

2. Make any other data changes required for the station, such as, fill new fields, change
   existing field values.

3. If the station is analog, use the FAC.

   No configuration steps apply for MCT.

4. If the station is digital or UNIStim:

   a. If a button is available, assign an **mct-act** button for the MCT feature.

      No lamp or icon is required for the button, although one is recommended.

   b. Otherwise, ensure the user has documentation regarding activation of MCT by FAC.

Malicious Call Trace feature operation

During an active call, if the user presses the **MCT** key, Device Adapter generates the corresponding SIP FNU for the malicious call trace feature. The FAC is processed at Communication Manager by using transfer handling.

To specify the MCT deactivation FAC and release all MCT resources, at least one non-SIP endpoint is required as an MCT controller. This non-SIP endpoint can be a Communication Manager H.323 or digital endpoint. For more information about the configuration and operation of the H.323 or digital endpoint, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

MCT deactivation FAC is mandatory.

Tracing a malicious call from an analog phone

About this task

This procedure can also be used for digital or UNIStim phones without the MCT key.

Before you begin

Ensure that you are on a malicious call.

Procedure

1. Initiate transfer or conference.

    a. On Analog stations: Flash the switch hook.

    b. Others: Press the **Transfer** or **Conference** button or soft key.

       A special dial tone signifies that the call is on hold.

2. Enter the FAC.

    A success tone is heard. The user is reconnected to the call.

Tracing a malicious call from digital and UNIStim phones

Before you begin

Ensure that the call is a malicious call.

Procedure

Press the **CallTrace** key.

A success tone is heard. The user is reconnected to the call.

Message Waiting and Voice Mail

Message Waiting and Voice Mail feature description

The Message Waiting service provides either of the following:

- A visual indicator (lamp and/or icon) and a button to access the voice mail server
- A special audible dial tone that requires the user to call in to the voice mail service.

A limited subset of analog endpoints may have an indicator but not have the button to access voice mail.

The commands that are available at the voice mail server differ based on the user's corporate policies and the desired actions, as it is uncommon for a site to use all available options. The following are the commonly present options:

- Get the **help** menu.
- Listen to an unheard message.
- Listen to a message that was already heard.
- Delete a message.
- Save a message you heard.
- Skip forward in the mailbox.
- Skip backward in the mailbox.
- Change settings such as the user's password or greeting, provide out of office alerts, etc.
- Log out of the mailbox.

Other options may be present, and options listed above can be omitted (for example, if the mailbox automatically saves all messages for 14 days, there is usually no need to save the message).

Administration of Message Waiting and Voice Mail

> ⚠ **Warning:**
>
> Custom Local Area Signaling System (CLASS) sets are analog sets with some additional modem circuitry for enhanced signaling. This circuitry is susceptible to high voltages, up to -150 Volts, and is used by many Message Waiting line cards. Hence, for a CLASS endpoint, you must define the CLASS station with message waiting lamp as Lamp Denied (LPD) if you do not use at least one of the CLASS display features, that is, CNUA, CNUS, or CNAA.
>
> The Lamp Allowed (LPA) feature is used for analog stations for basic message waiting lamp. Do not enable the LPA feature for analog CLASS endpoints without enabling at least one of

the CLASS display features, that is, CNUA, CNUS, or CNAA, because it causes a significant health and safety hazard.

However, if you provision the CLASS set correctly with at least one of the CLASS display features, that is, CNUA, CNUS, or CNAA, the Message Waiting line cards handle the LPA feature correctly by signaling the lamp state over the modem and not by voltage.

Device Adapter supports the following:

- Voicemail Message Waiting indication for analog sets equipped with a lamp controlled by applied voltage.

- Voicemail Message Waiting indication for analog CLASS sets equipped with a lamp.

⚠ **Warning:**

Do not use applied voltage for analog CLASS sets.

The configuration of the voice mail server is outside the scope of this document.

The following options are configured as a part of the station definition in Communication Manager, either through the Communication Manager administration screens or by using System Manager.

- Coverage options, to route the call to the voice mail.

- Analog station classes of service for message waiting:

  - Analog stations with a basic message waiting lamp requires the Lamp Allowed (LPA) feature.

    ✱ **Note:**

    For analog CLASS endpoints, if you use the LPA station definition feature, ensure that you enable at least one of the CLASS display features, that is, CNUA, CNUS, or CNAA.

  - Analog CLASS stations require the Message Waiting Allowed (MWA) feature. These will also require the following features:

    - CNUS (CLASS Calling Number Single Data String Format Allowed),

    - CNUA (CLASS Calling Number Multiple Data String Format Allowed), or

    - CNAA (CLASS Calling Name Multiple Data String Format Allowed).

      ✱ **Note:**

      Using the MWA feature requires at least one CLASS display feature to be used. If the CNUA, CNUS, or CNAA CLASS display feature is not assigned, the MWA feature may be non-functional.

      ⚠ **Warning:**

      For analog CLASS endpoints, if you use the LPA station definition feature, ensure that you enable at least one of the CLASS display features, that is, CNUA, CNUS, or CNAA. Using the LPA feature for an analog CLASS endpoint without using any of

the CLASS display features is a health and safety hazard. Note that the endpoint does not notify the line card or server that it is an analog CLASS endpoint. This is determined during the programming.

Therefore, using the LPA feature without using the CLASS display feature for a station which has a CLASS modem is not supported and is potentially hazardous.

- If the LPA feature is not provided for an analog endpoint, when the Communication Manager indicates a message is waiting, Device Adapter uses the special (stuttered) dial tone.

- Button allocation on the endpoints supports the Message Waiting lamp and button. The button has a fixed location on the UNIStim and most 39xx stations (key 5 on the 3902, and key 16 on the 3903, 3904, 3905, and other UNIStim endpoints). The 3901, 1 column and 2 column 2xxx digital stations may have the button assigned on any unassigned buttons.

These features may be configured either using the Communication Manager or using the System Manager. Refer to the *Communication Manager Feature Description and Implementation* document for steps involved with each aspect.

Operations of Message Waiting and Voice Mail

Managing voice mail messages on analog phones or digital and UNIStim phones without the Message Waiting Indication key and lamp

About this task

This procedure may be used by analog phones or digital and UNIStim phones without the Message Waiting Indication key and lamp.

Procedure

1. To detect a voice mail message received, do the following:

   a. The user goes off hook (including handsfree and using the headset).

   b. A visual display is also be present.

      - A CLASS station may include an indicator in the display that a voice mail message is present.

      - Other analog stations with a lamp for voice mail indications may have the indicator show that a voice mail message is present.

2. To log in and retrieve messages received, do the following:

   a. The visual display (text in the screen, LED, or lamp) will indicate when a voice message is present.

   b. While offhook, enter the access extension number for the voice mail server.

   c. Log in, using the credentials that is applicable for the server. This may include entering the mail box number and password, or may be the password only, depending on the voice mail system and configuration.

d. The user is logged in and will use the Telephony User Interface options as configured on the voice mail system.

e. The user may log out; if all messages are received, the indicator lamp or icon changes to indicate no messages are present.

Managing voice mail messages for analog phones or digital and UNIStim phones with the Message Waiting Indication key and lamp

About this task

This procedure may be used by analog phones or digital and UNIStim phones with the Message Waiting Indication key and lamp.

Procedure

1. To detect a voice mail message received, do the following:

    The visual indicator is lit may also be present.

    • Some endpoints use the same lamp when the user is on a call or on hold as they use for Message Waiting. In that case, the lamp will only have meaning for voice mail when the station is idle.

    • Other stations will have the lamp lit as long as a voice mail message is unheard. The station has a second lamp to indicate status (typically, a lamp with a different color).

2. To log in and retrieve messages received, do the following:

    a. The LED or lamp is lit when a voice message is present.

    b. Select a line appearance (the one associated with the mailbox).

    c. Press the voice mail **Inbox** button.

    d. Log in using the credentials that is applicable for the server. This may include entering the mail box number and password, or may be the password only, depending on the voice mail system and configuration.

    e. The user is logged in and will use the Telephony User Interface options as configured on the voice mail system.

    f. The user may log out; if all messages are received, the indicator lamp or icon changes to indicate no messages are present.

Feature Interactions of Message Waiting and Voice Mail

On stations where the lamp for Message Waiting is also used for "incoming call alerting" or "outgoing call in progress", "active in a call", or "on hold", the Message waiting indication is only valid while idle. As soon as the user initiates a call or receives an incoming call, the lamp state applies to calls on the station. Until no calls remain active on the station, the lamp applies to call states and not to voice mail.

Mobile Extensions (Mobile X) using EC500

Refer to the *Avaya Extension to Cellular User* Guide for information and procedures associated with this feature. This document is available on the Avaya Support portal.

Multiple Appearance Directory Number (MADN)

Multiple Appearance Directory Number feature description

In the most accurate sense, Multiple Appearance Directory Number (MADN) applies both to a Single Call Arrangement and to a Multiple Call Arrangement, when at least two buttons for the number exist in the network.

The following are all MADN:

- One user with two or more call appearance buttons on his or her station.
- At least two users with a single line appearance button for a specific call appearance. There is a call appearance button positioned either on one of the two endpoints or on a virtual set, depending on the specific desire behavior.
- A mix of users have two or more buttons while other users have a single button for line appearances.

MADN has two variants:

- Only one call can exist at a time on any of the stations. For example, if User 1 has a call on a line appearance for 235-5801, other users cannot create a new call. This is "Single Call Arrangement".
- Every line appearance button can have its own call. This is "Multiple Call Arrangement".

With MADN, a Single Call Arrangement (SCA) may be private or non-private; that is, the call may or may not use exclusion.

- If exclusion is enabled, no other user may use the extension until the user releases the call or puts the call on hold with non-exclusive call retrieval. If Alice had an exclusive call and put it on hold, Bob could pick the call up and have exclusive "ownership" of the call.
- If exclusion is disabled or not configured, other users may "conference into the call", using the line button.
- The lamp state indicates either idle, "available" (flashing), or "in exclusive use by someone else" (lit).
- SCA is not recommended for analog stations, as they are unable to use any other appearances to place calls while the SCA number is active.
- The 1210 UNIStim phones cannot bridge a call. Hence, Avaya recommends that you do not configure SCA on 1210 UNIStim phones. If SCA is configured on a 1210 UNIStim phone and

if the SCA number is active, the user cannot use any other appearances on the 1210 phone to place a call or join another call. This limitation of the 1210 UNIStim phone is the same in both CS 1000 and Communication Manager.

A Multiple Call Arrangement (MCA) call is significantly different.

- If there are 30 users, there may be at least 30 calls in progress at one time.

- If a user has 10 appearances, the user may have up to one call in progress (ringing, being placed, or active) and all other appearances may be on hold.

- No user may bridge into the appearance being used by another user.

- The lamp state for the button is for the current call only; if a call is ringing, any user with an idle button can answer it (flashing). However, buttons already in use indicate that they are in use (lit), and as soon as the call is answered or released, all parties not already in a call have the button go dark, available for the next call.

The Device Adapter provides both user experiences, depending on how the button is configured.

If configured for SCA:

- If one user has a single call appearance button and all others have a bridged appearance button for this appearance, no more than one incoming call is allowed, and only the user on the call can access the "outbound" appearance for call transfer and conference associated with the transfer or conference key.

- The setting of the exclusion determines whether others can bridge in.

- A **privacy** button is available to toggle from not private to private. This is the reverse of the logic on the CS 1000, where the toggle is from private to not-private, but otherwise the behavior is identical.

- Both incoming and outgoing calls can consume the single call appearance available for calls. However, transfer and conference is still available.

If configured for MCA:

- Typically, an X-Port (virtual station) is defined with sufficient call appearances to allow all users to have a single call for this extension.

- The stations are defined with a specialized Bridged Appearance, which has the "a" (any) parameter. This matches the MADN approach:

  - For an incoming call, all idle MCA buttons indicate the incoming call.

  - When the call is answered, only the party answering is on the call. All other fringing buttons go idle.

  - If a user uses the button to call out, the caller information for the call is that of the MCA extension.

  - Outgoing calls are not visible to any other users.

  - Each user can transfer or conference the call but cannot do this to the extension in use.

- All calls are private. The user must add anyone (conference or transfer).

October 2020   Avaya Device Adapter Snap-in Reference   489
Comments on this document? infodev@avaya.com

For more information, refer "Per Button Ring Control" section, where the call appearance variants SCA and MCA split into ringing (SCR and MCR) and non-ringing (SCN and MCN).

Prerequisites to configure Multiple Appearance Directory Number

Administrator must ensure that all users on Session Manager are configured with Multiple Device Access set to allow only one endpoint to register, and a new registration to override an existing registration.

The norm is to use ProVision to migrate. This includes mapping analog stations with the MCA Denied (MCRD) class-of-service into an SCA model, or analog stations with MCA Allowed (MCRA) into the MCA model. However, an administrator may need to create a station using by Communication Manager station programming or may need to add the capability to an existing endpoint.

For more information, see "Creating a bridged call appearance on a single-line telephone" (analog endpoints) section and "Creating a bridged call appearance on a multi-appearance telephone" (other endpoints) section in the *Avaya Aura® Communication Manager Feature Description and Implementation* document for SCA handling.

Create appearances for MCA as follows:

- Ensure that a virtual station (X-Port) is defined with the correct extension, and sufficient call appearances to provide enough call support. The extension is administered without hardware being assigned (making it a virtual station), and has the "Port" field set to x. For creating a new station, see the Communication Manager documentation.

- Define the applicable button as a bridged appearance:

  - MCA: Ensure that it has the "a" parameter assigned as parameter 1, and the extension as parameter 2.

  - SCA: Ensure that it has the parameter for call appearance 1 assigned to the lowest indexed button as parameter 1, and the extension as parameter 2.

- If the call is an SCA, and the administrator wants to allow changing the privacy settings for the call, the administrator defines an exclusion button on the station, typically labelled as Privacy.

Ensure that only the programmable buttons on any endpoint can be configured as line appearances (either call appearance or bridged appearance). This should be invisible to the person coming from CS 1000, as the additional "programmable" keys have fixed uses. For example, the speed call soft key can be one of four variants, but can only be a speed call key. If an administrator mis-programs a station to put the appearance on an invalid button, Device Adapter ignores this button.

Multiple Appearance Directory Number feature operation

Answering a call on a single line

About this task

The user will answer the call in the same manner as the user would if the call is not shared with other users.

Procedure

When a call rings, go off hook

If this is an SCA line with privacy (exclusion) enabled, no other user may access this extension. Otherwise, all other users may "bridge in" (join the call).

Answering a call on a multiple line

Procedure

1. The applicable call appearance button is alerting on all users with an idle button.

2. Select the line appearance. Do one of the following:

   - To answer on the headset, press the headset button.

   - To answer on speakerphone, do one of the following:

     - Press the line appearance that is ringing with the handset on the cradle.

     - Press the **Speaker** button.

   - To answer with the handset, do one of the following:

     - If the handset is in the cradle, go off hook.

     - If the phone is already off hook, press the line appearance.

   If this is SCA, the lamp state on all other users indicates the exclusion state.

   If this is MCA, the indicators on all other ringing users' stations become idle.

Making a call on a single line

About this task

The user will initiate the call in the same manner as the user would if the call was not shared with other users.

Procedure

When you want to make a call, go off hook.

If this is an SCA line with privacy (exclusion) enabled, no other user may access this extension. Otherwise, all other users may "bridge in" (join the call) after it is answered.

Making a call on a multiple line

Procedure

Select the line appearance:

- To originate a call on the headset, press the headset button.

- To originate a call on speakerphone, do one of the following:

    - Press the line appearance that is ringing with the handset on the cradle.

    - Press the **Speaker** button.

- To originate a call with the handset, do one of the following:

    - If the handset is in the cradle, go off hook.

    - If the phone is already off-hook, press the line appearance.

If this is SCA, the lamp state on all other users indicates the exclusion state.

If this is MCA, the indicators on all idle user stations remain idle.

Changing the privacy

About this task

You can change the exclusion (privacy) to enabled or disabled.

Procedure

To change the privacy, press the **exclusion** button.

Placing the call on hold and retrieving the call

About this task

Placing a call on hold allows another user to pick up the call, or the original user to pick it up at another phone, even when privacy was invoked.

A user cannot place the call on hold, except to initiate transfer or conference, on an analog phone. The user does a hook flash.

Procedure

A digital or UNIStim phone of a user may or may not have multiple lines. In either case, do the following:

a. To place a call on hold, press the **Hold** key.

   The lamp flashes on all stations.

   User may move to another station.

b. The user or another user may retrieve the call by pressing the **Line appearance** button.

Multiple Appearance Directory Number feature interaction

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Multi-Device Access

The topics in this section provide information about the general behavior, limitations, and configuration of the Multi-Device Access (MDA) feature for UC phones.

In addition to the MDA information documented in this section, there are additional MDA limitations and configurations specific to a call center environment. For more information, see Sequential Registration and MDA in a Call Center Elite environment on page 539.

Multi-Device Access feature description

> ✳ **Note:**
>
> - Device Adapter supports Multi-Device Access (MDA) only for UNIStim endpoints.
> - Avaya Aura® supports MDA on the SIP phones that are capable of supporting the MDA feature.
>
>   The J-series 3PCC phones do not support the Avaya Aura® SIP messaging that is required for MDA. If a J-Series 3PCC phone registers to a Device Adapter station definition for MDA, the buttons do not map correctly. This leads to a major loss of function. Hence, Avaya recommends that you do not use a J-series 3PCC phone for MDA.
>
>   However, MDA is supported on a J-Series Avaya Aura® phone.

Multi-Device Access is defined in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide as follows:

"With the Multi-Device Access (MDA) feature, a SIP user can register more than one SIP device with a single extension. For example, a user has 96X1 at the desk, 96X1 in the lab, and Avaya one-X® Communicator on the laptop. All these devices are registered with the same extension 123456. When a call arrives at extension 123456, all the devices are alerted. The user can answer the call from any one of the devices. If required, the user can bridge on to the call from one of the idle devices by using the Simulated Bridge Appearance (SBA) feature. Therefore, the call can be handed off between devices without parking the call."

An administrator must configure MDA based on the topology requirements of the user.

Depending on how an administrator has configured MDA for an Avaya Aura® user, the Avaya Aura® user can register up to 10 SIP devices with the same extension. However, if you configure

MDA to include Device Adapter UNIStim endpoints in addition to other traditional Avaya Aura® SIP endpoints, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint. This is because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA. If a node with the least load receives this registration request, but already has this TN registered, the registration attempt fails. The attempt to register the second or subsequent endpoint may fail because only one instance of a TN can register per node.

* **Note:**

> For MDA, ensure that all Avaya Aura® SIP endpoints that are registered concurrently with UNIStim endpoint connect to Session Manager by using secure connection (TLS).

Till Device Adapter Release 8.1.1, the administrator must also clear the **Block New Registration When Maximum Registrations Active** check box to ensure timely fail-over support. If the **Block New Registration When Maximum Registrations Active** check box was selected, fail over was delayed because Device Adapter waits for the existing registration to be declared failed by Session Manager. Hence, the **Block New Registration When Maximum Registrations Active** check box must be clear to support MDA and fail over in case of network problems.

In Device Adapter Release 8.1.2, enhancements in fail over handling removes this restriction. For more information, see .

This is a true MDA environment where two or more endpoints are registered concurrently with Session Manager.

For more information, see .

Concurrently registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA. Because the other Avaya Aura® SIP endpoints do not register to Device Adapter, fail-over is not a problem for the Avaya Aura® SIP endpoints. Therefore, having one Device Adapter UNIStim endpoint and nine 96x1 endpoints, all registered concurrently is permissible. But, having just two Device Adapter UNIStim endpoints register concurrently might lead to service failure.

The intent of MDA is to allow a single user to move to another part of the office and use a SIP endpoint in that location just like the user's desk phone. After the SIP endpoint is registered, the endpoint is a local copy of the user's phone. Therefore, even if the maximum number of simultaneously registered devices is set to more than one and if more than one endpoints are registered, only one endpoint is in use at a time because a single user is supposed to use this service.

For example, the user has two or more sets registered in the MDA user station definition. When a call arrives, all registered stations are alerted. When the user answers at one station, the other stations end the alerting, but will show the call status in the icon or lamp associated with the call appearance. The user cannot place other calls from the same call appearance on any of the other endpoints that are registered for MDA, until the call ends. But, if the user switches phones or asks someone else to join the call at one of the other endpoints that the user registered for MDA, the other endpoints can join the call as Simulated Bridge Appearances (SBA). This behavior is similar to the SCA feature of CS 1000, except that CS 1000 does not support MDA. For CS 1000, the calls are made to different user stations and the true bridged appearances are applicable.

> **✳ Note:**
>
> Because these are two instances of a single extension joining a call, Avaya Aura® neither considers it as a conference nor indicates that a conference exists.

With MDA, you can define a single user station of any normal endpoint type. Prior to Device Adapter, this could be a variant of either the 96x1 or J-series phone. With Device Adapter, you can configure MDA for the CS 1000 IP stations.

Other stations may or may not be able to register as this user station based on whether the endpoint type has a mapping function on System Manager to correctly map feature button types. The mapping function allows the buttons to be defined. The service is provided to all endpoints that can register as this user as per the button definition of the user station. For example, 96X1, J-Series, or CS1K-IP can register as a CS1K-IP endpoint.

Note that different CS1K-IP endpoints may not have the same number of programmable feature buttons. Using an endpoint with fewer buttons results in loss of these feature buttons.

If a user SIP registers with station types that differ from the station definition, then to avoid loss of keys, Avaya recommends that you use an endpoint with the least number of keys as the primary station.

In addition, the CS1K-IP endpoints and Avaya Aura® SIP endpoints have not only different number of buttons, but many features that use a Feature Key in CS 1000 use an item from the Feature List on the Avaya Aura® SIP endpoint. As a result, an exact mapping between the CS 1000 endpoints and Avaya Aura® SIP endpoints may not be possible.

However, even if the appropriate buttons defined on the station definition are not available or cannot be mapped on a station type, you can use the appropriate FACs to perform the function of these missing buttons, and register the endpoint as the user station.

> **✳ Note:**
>
> If a user who is on a call by using a device that is configured for MDA tries to join the call by using another device that is configured for MDA, Communication Manager verifies the status of the Exclusion feature for the device. If the Exclusion feature is enabled for the device, then the other device cannot join the call until the user who enabled the Exclusion feature disables the Exclusion feature in Communication Manager.

For information about MDA and Sequential Registration in Call Center Elite, see "Sequential Registration and MDA in a Call Center Elite environment" in "Appendix H: Call processing features and services."

MDA limitations

The following are the limitations of MDA in Device Adapter:

- Device Adapter uses the hardware ID of the UNIStim phone, from CS 1000, to register the UNIStim phone. This hardware ID must be unique in CS 1000. Whereas, MDA uses the user identity to register the UNIStim phone.

During phone registration, Device Adapter uses the TN of the phone to map the hardware ID and user identity.

The TN is nothing but the physical port ID of a phone on CS 1000. For a UNIStim phone, the TN is a logical port ID of the UNIStim phone because the UNIStim phone does not have a physical shelf. For digital and analog phones, the TN is the physical port ID to which the phone is physically connected by wires.

The following are the registration differences in different infrastructure scenarios when two or more UNIStim endpoints, with the same TN, try to register:

- In a single-node cluster, the registration always fails.

- In geo-redundant clusters, including two single-node clusters, a second registration succeeds.

- In all other cases, the registration may or may not succeed depending on the current registrations.

Therefore, registering two or more UNIStim phones with the same TN is non-deterministic in MDA.

Hence, registration of a UNIStim endpoint is non-deterministic in an MDA configuration where the maximum number of concurrent registrations is set to two or more, and out of these endpoints more than one endpoint is a UNIStim endpoint.

Avaya recommends that if your MDA configuration contains two or more phones, ensure that only one phone out of these phones is a UNIStim phone.

- The primary station definition must be that of a UNIStim endpoint because the intent is to migrate the CS 1000 endpoints and its users to Avaya Aura®. Registering an existing UNIStim endpoint to a new 96x1 station definition is contradictory. Device Adapter does not support using a non-UNIStim station definition for a UNIStim endpoint that is registering for MDA.

  You must use the CS1K_IP station template to define the station definition for a UNIStim phone that will be used as a UC phone.

  You must use the CS1K_IPCC station template to define the station definition for a UNIStim phone that will be used as a call center-capable phone.

- Digital and analog endpoints do not support MDA. These endpoints use the physical device access port (loop, shelf, card, unit) or Terminal Number (TN) to identify the set. This is a physical port of these devices and cannot be modified by the user. Only UNIStim endpoints that use a virtual TN, allow the user to modify the TN. Note that after the user modifies the TN, the user must restart the endpoint. For more information, see MDA limitations for digital and analog endpoints on page 497.

  However, you can use the Sequential Registration fail-over configuration to configure fail-over support for digital and analog endpoints. For more information, see Sequential Registration fail-over support for analog and digital endpoints on page 537.

MDA limitations for digital and analog endpoints

MDA is not supported for analog and digital phones because of the following reasons:

- For MDA, the TN must be unique in the cluster:

  For digital and analog endpoints, the TN is the physical port ID of the phone. The first half of the TN indicates the MGC and the other half indicates the port ID of the line card on that MGC. Registering two or more Device Adapter digital or analog endpoints with the same TN is not supported because the TN is an identifier for a single, hardwired connection on a line card.

- A user cannot modify the TN of an analog or digital endpoint:

  Unlike an analog or digital endpoint that have a fixed, physical TN, a UNIStim endpoint has a virtual or logical TN that is used for device tracking. The UNIStim endpoint does not have a physical line card interface point or MGC. This allows a user to modify the TN of a UNIStim endpoint and register as the intended user. Note that after the user modifies the TN, the user must restart the endpoint.

  A system administrator can also modify the station definition for the UNIStim endpoint on Device Adapter and Communication Manager.

  Because the digital and analog endpoints have a fixed TN, a user cannot modify the TN. Hence, there is no mechanism to log in as a different TN or log in again with the same TN.

- Digital and analog endpoints do not have the ability to block re-registration attempts to re-acquire the TN:

  The Device Adapter core software that is shared by all endpoints can block re-registration attempt of an endpoint until the user re-registers the endpoint by manually logging in the endpoint.

  However, for digital and analog endpoints, there is no mechanism to prevent an MGC from immediately trying to re-register a digital or analog endpoint that gets unregistered. If a 96x1 or other SIP device tries to sequentially register, Session Manager unregisters a currently registered digital or analog endpoint. The MGC of this digital or analog endpoint immediately sends a SIP re-registration request to Session Manager, and repeats the re-registration attempt until the registration succeeds. This process unregisters the 96x1 or other SIP device.

Multi-Device Access feature administration

Configuration of maximum number of simultaneous devices that can register concurrently:

For MDA, an administrator can specify a minimum of 2 and maximum of 10 SIP devices that can concurrently register with Session Manager. However, Avaya recommends that out of the 10 SIP

endpoints only one endpoint should be a Device Adapter UNIStim endpoint. This is because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA.

If a user wants to use two or more Device Adapter UNIStim endpoints, then Avaya recommends that you set **Max. Simultaneous Devices** to 1. This is called Sequential Registration and not MDA.

Configuration for how Session Manager should handle new endpoint registration request if maximum registered devices is reached:

Whether Session Manager registers a new endpoint when the maximum number of concurrent registered devices is reached depends on whether an administrator selects or clears the **Block New Registration When Maximum Registrations Active** check box:

- If the configuration is to block the endpoint from registering, the endpoint SIP registration request is rejected.

  If a user wants to register a new device, the user must manually un-register an existing registered device.

- If the configuration is to allow the endpoint to register, the endpoint SIP registration request is allowed. However, Session Manager un-registers an existing device that is registered for the longest period of time before registering the new device.

This configuration is a part of the Session Manager Profile configuration of the user in System Manager. For more information, see Configuring maximum number of devices that can register concurrently for MDA on page 499.

Scenarios when the maximum number of registered devices is reached:

The following are the scenarios if the maximum number of registered devices is reached:

- If the **Block New Registration When Maximum Registrations Active** check box is clear and the maximum number of registered devices is reached, a new registration attempt clears the oldest prior registration.

  Because **Max. Simultaneous Devices** is set to 2 or more, Session Manager selects and un-registers the device that has been registered for the longest period of time from the currently registered devices.

- If the **Block New Registration When Maximum Registrations Active** check box is selected, and if the maximum number of registered devices is reached, then:

  - Either of the following is applicable if a new registration request is received:

    - Session Manager rejects the new registration request.

    - A user must manually log out of a currently registered device to register a new device.

  - In an event of a network failure, when the endpoint loses connectivity and tries to re-register, then:

    - Till Device Adapter Release 8.1.1, Session Manager processed this as a new registration request. After the keep-live signaling detected a connection failure, Session Manager un-registered the existing registered device and allowed the new SIP registration. However, this caused a delay in fail over.

• In Device Adapter Release 8.1.2, enhancements in high availability and fail over remove this limitation. Session Manager identifies the endpoint by using the device ID and processes the fail over attempt as a re-registration request rather than a new registration request by the endpoint and registers the endpoint.

Configuring maximum number of devices that can register concurrently for MDA

About this task
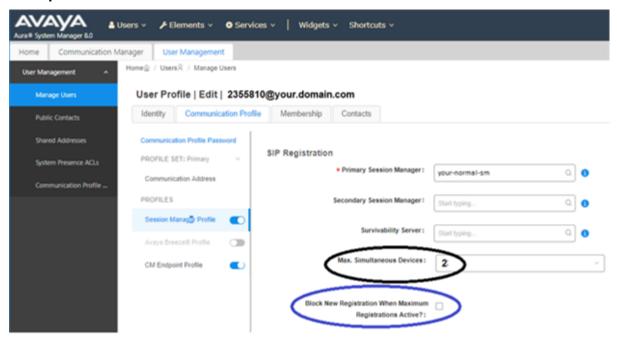
The following procedure shows extension 2355810 in the domain your.domain.com.

The following procedure has only a single Session Manager. You can configure a secondary Session Manager and add a survivable branch Session Manager. The feature handling is still the same.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Click **Users** > **User Management** > **Manage Users**.

3. Select the user, and then click **Edit**.

4. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.

5. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, type the maximum number of devices that can register concurrently.

   You can specify a maximum of 10 SIP devices. However, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint.

   If the user wants to include two or more Device Adapter endpoints, then Avaya recommends that you set the **Max. Simultaneous Devices** field value to 1. This is called Sequential Registration and not MDA.

6. Do one of the following to determine whether Session Manager should allow new registrations when the maximum number of registered devices is reached:

   • Clear the **Block New Registration When Maximum Registrations Active** check box to allow Session Manager to register a new device. Session Manager un-registers an existing device that is registered for the longest period of time before registering the new device.

   • Select the **Block New Registration When Maximum Registrations Active** check box to block new registrations.

   Select this check box only if you want to force a user to manually log out of an already registered device when the maximum number of registered devices is reached and allow a new registration.

7. Click **Commit**.

Comments on this document? infodev@avaya.com

Example

In the preceding example, **Max. Simultaneous Devices** is set to 2. Which means, only two devices can register at a time. If a third device tries to register, then based on whether you have selected or cleared the **Block New Registration When Maximum Registrations Active** check box, the new device registration is either blocked or a current device that is registered for the longest period of time is un-registered to allow the new registration. In the preceding example, the device that registered first is un-registered to allow the new registration.

Next steps

You can further configure the station definition for the MDA user extension in Communication Manager or System Manager. For more information, see Configuring the station definition for the MDA user extension on page 500.

Configuring the station definition for the MDA user extension

About this task

The template type that you use to define the station definition depends on whether you want to configure the phone as a UC, call center (CC), or a CTI controlled phone:

Phone type	Station definition template
Unified Communications phone	CS1K_IP
Call center (CC) phone in Call Center Elite	CS1K_IPCC
Phone in Avaya Aura® Contact Center	CS1K_IP

Table continues…
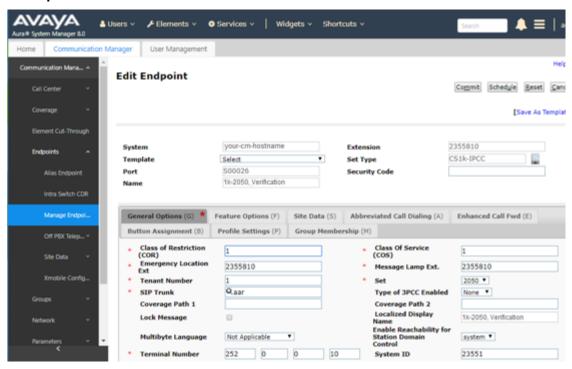
Phone type	Station definition template
CTI controlled phone along with Call Center Elite	• CS1K_IPCC if you want to use the phone as a CC phone if connection to the CTI controller is lost. However, if connection to the CTI controller is proper, the phone functions as a UC phone. Note that only a subset of the CS 1000 endpoints can be used as CS1K_IPCC phones. For more information, see Supported phone types in an Avaya Aura Call Center Elite environment on page 55. • CS1K_IP if you want to use the phone as a UC phone. However, if connection to the CTI controller is lost, call center operations cannot be performed from this phone.
CTI controlled phone along with Avaya Aura® Contact Center	CS1K_IP

Procedure

Do any one of the following to configure the station definition for the MDA user extension:

• Configure the station definition at the Communication Manager CLI command prompt.

For more information, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

• On System Manager, click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** and configure the station definition.

Example

The preceding screen shot shows the endpoint defined as a 2050 soft client. An endpoint that has the appropriate feature content mapping to the 2050 soft client can SIP register at this extension.
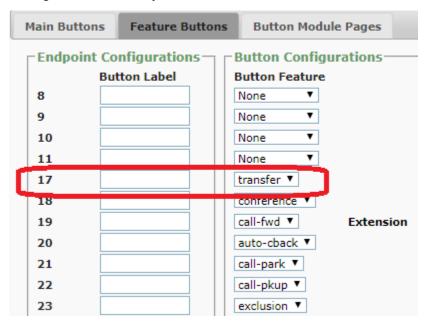
However, a 96x1, a J-Series, or a non-CS 1000 soft client has a moderately different *user experience* as compared to the Device Adapter endpoint.

The Transfer button is an example of this difference:

- The Transfer button on both UNIStim endpoint and Avaya Aura® SIP endpoint appears as a context-sensitive soft key. This Transfer soft key is available only when the user is on a call and has the resources to transfer the call.

- Device Adapter maps the Transfer soft key to include the call appearance and the Transfer function in a single button. Device Adapter sends the applicable message for the current context.

  The following screen shot shows a programmed Transfer soft key at position 17 on the **Feature Buttons** tab.

  The Transfer soft key configuration is for a 1140 phone that is on Device Adapter. Device Adapter considers this as both a Transfer soft key and a call appearance button. In the following example, buttons 0 through 11 are programmable feature keys and buttons 17 through 23 are soft keys.

- An Avaya Aura® SIP endpoint uses the Transfer soft key, which puts the current call on hold and selects a second call appearance.

  The following screen shot on the left shows the screen of a 96x1 phone and the screen shot on the right shows the screen of a UNIStim phone.

  On the 96x1 phone, the fourth button labeled **transfer** is an additional call appearance. This **transfer** button is mapped to the Transfer soft key on the UNIStim station.

  The Transfer soft key appears at the bottom of both the UNIStim and 96x1 endpoint screens only during an active call. The user must press the Transfer soft key to initiate the transfer and enter the destination number. The user must then press the Complete soft key to complete the transfer.

The Avaya Aura® SIP endpoint moves all the call appearances to the first screen, which is the Phone screen, with the call appearance for the Transfer button placed last.

Note that all feature buttons on the CS 1000 station appear on the second screen, which is the Features screen, on the 96x1. For example, the Forward feature button.

MDA with one Device Adapter UNIStim endpoint and one or more Avaya Aura® SIP endpoints registered concurrently

Device Adapter allows concurrent registrations of a minimum of 2 up to a maximum of 10 SIP endpoints for MDA. However, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint. One or more Avaya Aura® SIP stations can register at the same time along with the UNIStim endpoint.

✱ Note:

> For MDA, ensure that all Avaya Aura® SIP endpoints that are registered concurrently with UNIStim endpoint connect to Session Manager by using secure connection (TLS).

If the endpoints are in a public area and other users can access the endpoints, then retaining a 96x1 or other SIP station in a registered state when the user is not at the desk is possibly a security risk. However, if you do not allow multiple devices to register concurrently, the user cannot transfer the call between devices.

If the user wants to use some other devices or application; for example, Expert Client or 96x1, in addition to the Device Adapter UNIStim endpoint, then out of the permissible number of registered devices, which is 10:

- Avaya recommends that only one endpoint should be a Device Adapter UNIStim endpoint. This is because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA.

- There can be more than one other traditional Avaya Aura® SIP endpoints, such as 96x1, J-series, and Avaya soft clients.

- The maximum number of endpoints that can register is 10.

For example, the user may have two Avaya Aura® SIP devices, such as a 96X1 and a J-series, in addition to a Device Adapter UNIStim 1140 endpoint. The **Max. Simultaneous Devices** is set to 2. If the 96X1 and J-series endpoints are registered and the 1140 endpoint tries to register, Session Manager terminates the registration of the device that is registered for the longest period of time to register the Device Adapter UNIStim endpoint. That is, either the J-Series or the 96x1 SIP phone. However, the operation of the J-series and 96x1 is different from that of the 1140 and the user experience is not the same.

This is especially true for soft keys on Device Adapter. For example, a Transfer soft key on a Device Adapter UNIStim endpoint has a call appearance or bridged appearance attached to it. Device Adapter maps the user's pressing of the Transfer soft key to the equivalent of a 96X1 user seizing a call appearance for a call transfer, including the call being on hold. Device Adapter then sends any transfer key specific SIP messages that are sent by a 96x1.

Therefore, the additional call appearance appears on the 96x1 and can be used in the Avaya Aura® user experience model.

You must also consider the number of keys for the 96x1 that uses the Device Adapter station profile. If the Avaya Aura® SIP endpoint has more programmable buttons, then the endpoint remains functional, but the key expansion modules do not map appropriately. An 18 button Key Expansion Module does not map to a 12 or 24 button Key Expansion Module.

Prerequisites for configuring MDA for one Device Adapter endpoint and one or more Avaya Aura® SIP endpoints registered concurrently

You must configure the station definition, which normally represents the primary station that the user uses. Because the intent of Device Adapter is to migrate the CS 1000 endpoints and users to an Avaya Aura® environment, the CS 1000 station definition already exists. For more information, see

The 96x1 may have fewer added button modules or modules with different number of buttons. If the user uses divergent station types, then to avoid loss of keys, Avaya recommends that you use an endpoint with the least number of keys as the primary station.

For more information, see

The station data that is sent to Device Adapter is according to the template that is generated by the station definition. Device Adapter modifies the information to ensure maximum compatibility with the endpoint that is being registered, although, there might be some loss of keys. The 96x1 and other SIP endpoints use a similar data conversion for compatibility with the CS1K-IP SIP stations.

Caveat

- There will be some user experience differences if the user switches between the migrated CS 1000 endpoint and the Avaya Aura® SIP endpoint.

Configuring MDA support for one Device Adapter endpoint and one or more Avaya Aura® SIP endpoints registered concurrently

Procedure

Do one of the following:

- Configure the CS1K_IP station in Communication Manager.

- Do the following to configure the CS1K_IP station in System Manager:

    a. Log on to System Manager by using the appropriate administrative credentials.

    b. Click **Users** > **User Management** > **Manage Users**.

    c. Select the user, and then click **Edit**.

    d. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.

    e. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, click **2** or more devices based on the number of concurrent devices you want to register.

       You can specify a maximum of 10 SIP endpoints. Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint.

    f. Do one of the following:

       - Clear the **Block New Registration When Maximum Registrations Active** check box to allow Session Manager to terminate an existing endpoint's SIP registration when a new registration request is received.

       - Select the **Block New Registration When Maximum Registrations Active** check box to allow Session Manager to retain an existing endpoint's SIP registration and reject the new registration request.

    g. Click **Commit**.

MDA with one Device Adapter endpoint and one or more Avaya Aura® SIP endpoints registered concurrently feature operation

About this task

For example, a user has a 1140 at the desk and a 96x1 in the lab. The user goes to the lab, and then goes home and registers by using the Expert Client on the computer. The next day the user goes to the office and uses the 1140. The user then gets another 96x1 phone and registers.

The user's identity is extension 2355777, which uses node 1050 and TN 32-0-6-1.

The **Max. Simultaneous Devices** is set to 3 or more.

Procedure

1. The user is registered at 1140.

2. The user goes to the lab and logs in by using the 96x1 as 2355777.

   a. The user can log in.

   b. The 96x1 can place and receive calls.

   c. The 1140 remains available for calls.

3. The user goes home and logs in by using the Expert Client as 2355777.

   a. User can log in.

   b. The Expert Client can place and receive calls.

   c. The 1140 remains available for calls.

      If the **Max Simultaneous Devices** was set to 2, Session Manager would have unregistered the 1140. However, because the **Max Simultaneous Devices** is set to 3 in this example, the 1140 remains registered.

   d. The 96X1 remains available for calls.

4. User goes to the office the next day and switches to the 1140.

   a. The 1140 is already registered and can place and receive calls.

   b. If the user has not logged out of the 96x1 the previous night, the 96x1 can still place and receive calls. This may be a security or access capability violation in some environments.

   c. If the user has not logged out of the Expert Client the previous night, the Expert Client can still place and receive calls. This may be a security or access capability violation in some environments.

5. The user logs in to another 96x1.

   a. Session Manager terminates the oldest registered device, which is the 1140.

   b. The 1140 can no longer place and receive calls.

   c. The new 96x1 endpoint can place and receive calls.

   d. If the user has not logged out of the 96x1 the previous night, the 96x1 can still place and receive calls. This may be a security or access capability violation in some environments.

   e. If the user has not logged out of the Expert Client the previous night, the Expert Client can still place and receive calls. This may be a security or access capability violation in some environments.

Park and page

CS 1000 style Park and Page functionality is available when Device Adapter is paired with the Call Park and Page Snap-in. The Call Park and Page Snap-in must be deployed in a dedicated Avaya Breeze® platform cluster to enable this functionality.

Refer to the *Call Park and Page Snap-in Reference* for additional information and procedures associated with this snap-in.

Basic and Per Button Ring Control

Ring control

Individual buttons may have the line set to ring or to alert silently. This is "per button ring control."

Alternatively, bridged appearances may provide or block audible ring tone for all bridged appearances, although traditionally call appearances were "always ringing" without per button ring control.

In all cases, the lamp will flash, but audible ringing is enabled or disabled in this manner.

Ring control feature administration

Enabling bridged appearance ringing options
Procedure

Set the **Bridged Call Alerting** flag to enable audible ringing.

Enabling active station (Off-Hook) ringing options
Procedure

Set the **Active Station Alerting** flag to enable audible ringing.

- Single: provide a single tone burst only

- Continuous: Provide normal ring cycles.

- If-busy-single: If idle, provide normal ring cycles. Otherwise, provide a single ring burst.

- Silent: Do not provide audible ringing.

Enabling per button ring control options

About this task

These are available only for bridged appearances prior to Aura 8.1, and are assigned "per key". As an example, four call appearances may each have a different option. This is not highly recommended. However, it is not uncommon to have the first appearance selected provide normal ring cycles, and the others to provide another option.

Procedure

Set the **ringing** field to enable the desired ringing.

- **r**— Ring: Provide normal ring cycles.
- **n**— No-ring: Silent ringing.
- **a**— Abbreviated: Provide ringing for a short period and then stop.
- **d**— Delayed: Wait for a few ring cycles and then ring.

Only the first two choices map to normal CS 1000 behaviors. However, the abbreviated tone can provide a tone burst, which is useful while in a call.

Ring control feature operation

Ring control feature works as follows:

- A call is received on a line appearance configured as "silent."

  No audible ringing is heard, although the lamp flashes.

- A call is received on a line appearance configured as "ring."

  No ringing is heard and the lamp flashes.

- A call is received on a line appearance configured as "abbreviated."

  No ringing is heard briefly, although the lamp flashes until the call is answered.

- A call is received on a line appearance configured as "delayed."

  No audible ringing is heard initially, although the lamp flashes. After a short period, normal ringing commences

Ring Control feature interaction

For ring control feature interactions, see *Avaya Aura® Communication Manager Feature Description and Implementation* document.

Personal Directory

Personal Directory feature description

The Personal Directory, Callers List, and Redial List are intertwined within the digital stations that support this capability (redial and callers only on the 3903, but redial, callers, and directory on the 3904 and 3905) or PD data on PPM (UNIStim).

Personal Directory allows you to enter or copy names in a personal directory, delete entries, or delete the entire list. You can also edit the name or number of an entry in the list. For example, if you want to dial some additional access code (trunk, feature, and so on) to place a call, you can edit the number in the directory to include the missing prefix or prefixes.

The Callers List and Redial List are call log features. The content of these lists is generated during call processing. You cannot modify this content. However, you can delete, or in some cases, copy entries or lists. You can also call (Callers List) or redial (Redial List) parties in these lists.

Password protection is available to control access to a user's Personal Directory, Callers List, and Redial List.

Digital stations

Digital stations of type 3903 and 3904, and 3905 call center stations, store list information on the station. The phase 3 stations allow a three-letter search of the directory.

If you want to dial someone from the directory, redial a previously called destination or call back a caller. You can perform this function on the endpoint and the endpoint simulates an outgoing call to the target.

The 3903 phone has a greatly reduced capacity for storing this data. It supports only the callers and redial lists.

- Directory size:

    - 3903: Not available. Callers list and redial list are available.

    - 3904: 100 entries

- Callers list size:

    - 3903: 10 entries

    - 3904: 100 entries

- Redial list size:

    - 3903: 5 entries

    - 3904: 20 entries

UNIStim station

UNIStim stations use the lists that are stored in the system, allowing the same capacity as the 3904:

- Directory size: 100 entries

- Callers list size: 100 entries
- Redial list size: 100 entries

The Personal Directory, Callers List, and Redial List use PPM to store directory data and user profile options.

PPM stores the most recent 100 call log entries, which are saved in the format of one entry per one call format. When the device is logged in, the saved call log entries are separated into Callers and Redial list.

Personal Directory supports the following for devices that support personal directory:

- Maximum entries = 100
- Maximum characters in name = 24
- Maximum characters in DN = 31
- Multiple actions:
    - Add new entry.
    - Edit an entry.
    - Delete an entry.
    - Delete contents of directory.
    - Copy an entry from Callers List to Personal Directory.
    - Copy an entry from Redial List to Personal Directory.
    - Dial DN of an entry.
- Password protection to control access to Personal Directory.
- One-minute time out to exit if the user was idle.

This is invisible to Communication Manager. It is handled either by the telephone itself (3904) or by Device Adapter (UNIStim).

Personal Directory feature administration
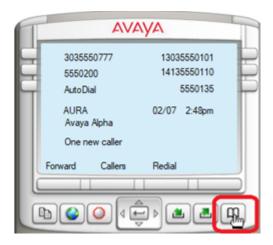
To enable the Personal Directory capability, you must configure the Calling and Called Party Name Display (CPND) feature.

For information about changing the station control password to protect the Personal Directory data, see Changing the station control password on page 522.

Adding a new Personal Directory entry

Procedure

1. Press the Directory/Log button.

2. Select Personal Directory.

3. Use the up and down arrows to scroll through the stored entries.

4. Depending on the endpoint, select Add or AddNew to add a new entry.

5. Enter a name.

6. Press the Next soft key.

7. Enter a phone number.

   ⊛ **Note:**

   If the new phone number matches an existing saved phone number in System Manager, then PPM merges the new contact information with the already existing contact information in System Manager. The resulting contact is known as an associated contact.

   An associated contact overwrites a user defined contact name with the contact name saved in the System Manager.

   The phone screen displays the associated contact information in the following scenarios:

   - After the network recovery

   - After a station re-registration

   - If the administrator has updated a field value for the station using System Manager web console

   A user cannot edit an associated contact, it can only be edited by the administrator.

8. Press the Done soft key.

9. Exit by pressing the stop sign or by waiting for the one-minute inactivity timer to expire.

Editing a Personal Directory entry

Procedure

1. Press the Directory/Log button.

2. Select Personal Directory.

3. Use the up and down arrows to navigate to the entry that you want to edit.

   Use the right arrow to see more details of the entry. Use the left arrow to return to the list.

4. Select Edit to edit the entry.

5. Edit the name, and select Next.

6. Edit the phone number.

   Some characters may not be valid for the name and phone number.

   ⊛ **Note:**

   If the edited phone number matches an existing saved phone number in System Manager, then PPM merges the edited contact information with the already existing contact information in System Manager. The resulting contact is known as an associated contact.

   An associated contact overwrites a user defined contact name with the contact name saved in the System Manager.

   The phone screen displays the associated contact information in the following scenarios:

   • After the network recovery

   • After a station re-registration

   • If the administrator has updated a field value for the station using System Manager web console

   A user cannot edit an associated contact, it can only be edited by the administrator.

7. Press the Done soft key.

8. Exit by pressing the stop sign or by waiting for the one-minute inactivity timer to expire.

Deleting a Personal Directory entry

Procedure

1. Press the Directory/Log button.

2. Select Personal Directory.

3. Use the up and down arrows to navigate to the entry that you want to delete.

4. Press Del to delete the entry.

   You can also delete the entire list by pressing Del without selecting an entry.

5. Confirm the deletion.

6. Press Yes to delete the entry.

   Pressing No aborts the procedure. The No button is the same soft key as the Del. Therefore, the cursor on the 2050 phone is on No as soon as you press Del.

7. Exit by clicking on the stop sign or by waiting for the one-minute inactivity timer to expire.

Dialing a number from Personal Directory

Procedure

1. Press the Directory/Log button.

2. Select Personal Directory.

3. Use the up and down arrows to navigate to the number that you want to dial.

4. Press Dial.

Privacy

Privacy feature description

Privacy (more specifically, the Privacy Release button) allows a user to toggle between a call being "single user only" to "anyone can bridge in" and vice versa. The basic provisioning for the stations will control whether the call is by default private or publicly accessible.

An MCA bridged appearance is always private, and no other user can bridge in. Therefore, the Device Adapter provides this capability only with bridged and call appearances mapped as SCA. Further, as the analog set has no privacy release button, it will not support making or receiving private calls.

The 1210 UNIStim phones cannot bridge a call. Hence, Avaya recommends that you do not configure SCA on 1210 UNIStim phones. If SCA is configured on a 1210 UNIStim phone and if the SCA number is active, the user cannot use any other appearances on the 1210 phone to place a call or join another call. This limitation of the 1210 UNIStim phone is the same in both CS 1000 and Communication Manager.

CS 1000 endpoint user experience

By using the Single Call Arrangement functionality, any user sharing the SCA DN can bridge into the call by pressing the corresponding SCA DN key unless the user has invoked privacy or privacy was invoked by default.

A call is private by default. If the user presses the Privacy Release soft key, the call toggles into the non-exclusive mode and all DN appearances on all phones blink. Any user sharing the DN can press the DN button to join in. This turns the call into a conference. Only one user can bridge in for each Privacy Release key press.

Communication Manager endpoint user experience

The Exclusion feature is similar. It is activated in the following ways:

- Manual Exclusion: Users turns the feature on or off by using the Exclusion button.

- Automatic Exclusion: The feature is activated when a user makes a call. Users must manually deactivate it.

- Buttonless Automatic Exclusion: The feature is activated when a user makes a call and deactivate when the call ends.

Administering privacy

About this task

The norm will be to use ProVision to migrate. However, an administrator may need to create a station using Communication Manager station programming or may need to add the SCA capability to an existing endpoint.

The station requires its default setting. However, unless exclusion is enabled for the system, the station cannot be set in this manner.

Procedure

In the change system-parameters features pages on either the System Manager or in the Communication Manager, shortly before the last page, set the **Automatic Exclusion by COS** to **yes**.

Before doing any further steps, give some time for data replication to occur if you are using the System Manager.

If you are using the Communication Manager, you can proceed immediately. However, it will take some time for the data to replicate with the System Manager.

Adding the exclusion button to the stations

About this task

Stations that have the automatic exclusion flag and have a button can receive automatic exclusion. Change the Class of Service Group to allow Automatic Exclusion.

Procedure

1. To enable or disable Automatic Exclusion for the group, change the cos-group or Class of Service Group for the group number intended.

2. Do the following:

   - To enable exclusion, click on the Automatic Exclusion box if not filled. Members of the COS group will now have automatic exclusion available.
   - To disable exclusion, click on the Automatic Exclusion box if filled. Members of the COS group will now have automatic exclusion unavailable.

   The exclusion button can now be provided to the stations in the group.

3. For every station that requires the ability to remove exclusion, add the exclusion button.

Turning off privacy

About this task

To activate privacy, an endpoint with the Automatic Exclusion Class of Service simply initiates or answers a call.

To activate public accessibility, an endpoint without the Automatic Exclusion Class of Service simply initiates or answers a call.

To turn off privacy, the user with Automatic Exclusion and the Exclusion (Privacy) button does the following:

Procedure

1. Pressing the Privacy Release (Exclusion) button toggles the Exclusion state.

2. When Exclusion is off, the corresponding DN lamp blinks (U-Hold icon). Other users on bridge appearances do not receive the blink indication when Exclusion is off.

3. When Exclusion is on, the lamp returns to the original state.

   All conference participants must press Privacy Release to allow others to join the conference.

   If the station with call appearance is on hold, turning off Exclusion and bridge could replace call appearance on the call.

Configuring privacy on an endpoint

About this task

To activate privacy, an endpoint with the Automatic Exclusion Class of Service initiates or answers a call.

To activate public accessibility, an endpoint without the Automatic Exclusion Class of Service initiates or answers a call.

To turn off privacy, the user with Automatic Exclusion and the Exclusion (Privacy) button will do the following.

> ✳ **Note:**
>
> All conference participants must press Privacy Release to allow others to join the conference. If the station with call appearance is on hold, turning off Exclusion and bridge could replace call appearance on the call.

Procedure

Press the **Privacy Release (Exclusion)** button.

Exclusion state toggles.

When Exclusion is off, the corresponding DN lamp blinks (U-Hold icon). Other users on bridge appearances do not receive the blink indication when Exclusion is off.

When Exclusion is on, the lamp returns to the original state.

Privacy feature interaction

For privacy feature interactions, see *Avaya Aura® Communication Manager Feature Description and Implementation* document.

Private Line Service

Private line service feature description

The Private Line Service feature allows a CS 1000 or a Meridian 1 proprietary endpoint to access reserved PSTN trunks, if the administrator has assigned some of the PSTN trunks as private trunks to the endpoint.

The available functionalities with the Private Line Service feature are:

- Making outgoing calls: You can make outgoing calls using the reserved trunks. Internal calls cannot be made using the private line service feature, the calls must be routed through the public network.

  Outgoing calls can be made only if the administrator has configured a private line button on your endpoint. The private line buttons can be configured as one of the following:

  - Private Line Ringing (PVR)
  - Private Line Non-ringing (PVN)

- Routing incoming calls: If reserved trunks are assigned to your endpoint, then Communication Manager routes all the incoming calls using the reserved trunk to that particular endpoint only.

  For the incoming calls, Private Line Service feature supports bridged call appearance in the SCA mode, which means that only one call is allowed across all the users and bridging into the call is allowed.

- Supported features: You can use following features on your endpoint with the configured Private Line Service feature:

  - Automatic Dialing.

  - Automatic Preselection

  - Call Pickup

  - Call Transfer

  - Call Status

  - Conference

  - Common Audible Signaling

  - Hold

  - Multiple Appearance Single Call Arrangement

  - Prime Directory Number as the calling party number for making outgoing calls using the PVR or PVN key

  - Privacy

  - Privacy Release

  - Release

  - Transfer

Prerequisites for Private Line Service

Ensure that you have bridged call appearance configured on your endpoint for Private Line Service feature operation. Bridged call appearance must be of Single Call Arrangement (SCA) mode, which means that only one call is allowed across all users and bridging into the call is allowed.

Administering endpoints for making outgoing calls using the Private Line Service feature

About this task

If the administrator has assigned some of the PSTN trunks as private trunks to the endpoint, the Private Line Service feature allows a CS 1000 or a Meridian 1 proprietary endpoint to access these reserved PSTN trunks to make outgoing calls.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Element Cut-Through**.

3. In the **Element Name** field, select the Communication Manager for which you want to configure the PVR or PVN key to make an outgoing call.

4. On the change system parameters – special applications page, set the **Customizations for CO Trunks and Busy Indicators?** field to **y(es)**.

5. Navigate to **Network** > **Trunk Group**.

6. On the Trunk Group page, select the trunk group name for which you want to configure the private line service feature to make outgoing calls.

7. On the Edit Trunk Group page, click the **Parameter Options (P)** tab and do the following:

   a. Select the **Cut-Through** check box.

      Any change in the **Cut-Through** field will be applicable to the system only if the **Customizations for CO Trunks and Busy Indicators?** field is set to **y(es)**.

      If the **Customizations for CO Trunks and Busy Indicators?** field is set to **n(no)** and you make any change in the **Cut-Through** field. Then, the user interface will show the updated value of the **Cut-Through** field but this value will not affect the system programming and outgoing call will fail.

   b. Clear the **Detect Far End Dialtone?** check box.

      Detect Far End Dialtone? field is visible on the user interface only if the **Cut-Through** check box is selected. If you select the **Detect Far End Dialtone?** check box, then outgoing calls through the private trunks will fail.

   c. Click **Commit** to save the changes.

8. On the Edit Trunk Group page, click the **General Option (G)** tab and do the following:

   a. In the **TAC** field, type the trunk access code of the CO trunk.

      Device Adapter does not support special characters for the trunk access code, trunk access code must be a number.

   b. Click **Commit** to save the changes.

9. Configure the **Hotline** button and define the TAC code as the auto dial number. For more information, see .

   You can directly make an outgoing call by dialing a number using the **Hotline** button. The hotline button will access the reserved trunk for the endpoint and dial the number by dialing the TAC code followed by the external number.

Administering endpoints for receiving incoming calls using the Private Line Service feature

About this task

Using the **Private Line Service** feature, Communication Manager routes the incoming call to an endpoint using the private trunks assigned to that endpoint.

Incoming calls are routed to the endpoints using bridged appearances of the X-port.

Procedure

1. Configure X-Port with the bridged appearances in Single Call Arrangement (SCA) mode on the endpoints for which you want to configure the Private Line Service feature. For more information, see [Configuring XPORT 9408](#) on page 201.

2. Log on to System Manager by using administrative credentials.

3. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **System**.

4. Click **Class of Restriction**.

5. In the Class Of Restriction (COR) that you want to use, set the **CALLING PERMISSION** field for a specific COR to **y**.

   The trunk group can route the incoming calls to the endpoint only if the updated COR with calling permissions enabled is assigned to the endpoint.

6. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Network**.

7. Click **Trunk Group**.

8. On the Trunk Group page, select the trunk group name for which you want to configure the private line service feature for routing the incoming calls to the endpoint.

9. On the Edit Trunk Group page, click the **General Option (G)** tab and do the following:

   a. Assign the updated **COR** to the trunk group.

   b. In the **Group Type** field, select **CO** to edit the CO trunk parameters.

   c. In the **TAC** field, type the trunk access code of the CO trunk.

      Device Adapter does not support special characters for the trunk access code, trunk access code must be a number.

   d. In **Incoming Destination** field, type the X-port extension number or the range of extension numbers on which the incoming calls will be routed.

      Bridged appearance for the private line key will be configured on these extensions for answering the incoming calls.

   e. Click **Commit** to save the changes.

Making an outgoing call using Private Line Service feature

About this task

If some of the PSTN trunks are assigned as private trunks to your endpoint, the Private Line Service feature allows a CS 1000 or a Meridian 1 proprietary endpoint to access these reserved PSTN trunks to make outgoing calls.

Before you begin

Ensure that:

- You have required configurations related to the CO trunk and trunk groups to make an outgoing call using the private trunks.
- You have the **Hotline** button configured on your endpoint with the TAC code programmed as the auto dial number.
- **Hotline** button is labelled as **PVR** or **PVN** on your endpoint.

Procedure

1. Press the **PVR** button to make an outgoing call.

   The **PVR** button will access the reserved trunk for the endpoint.

2. Dial the number using the dial pad.

   If the called party is available and answers the call, an active call is established between you and the called party.

3. Press the **Release** button or place the handset on hook to end an active call.

   Either you or the caller can end an active call.

Answering an incoming call using Private Line Service feature

About this task

Using the **Private Line Service** feature, Communication Manager routes the incoming call to an endpoint using the private trunks assigned to that endpoint.

When you receive an incoming call, the programmed appearance on your endpoint flashes.

Before you begin

Ensure that:

- You have required configurations related to the CO trunk and trunk groups to route the incoming calls to your endpoint.
- You have bridged appearance of X-port configured on your endpoint to receive the incoming call.
- Bridged appearances are configured in the Single Call Arrangement (SCA) mode.

Procedure

1. Answer the incoming call by pressing the bridged appearance key programmed for answering outgoing calls.

   By using the SCA functionality, you or any other user who is sharing the appearance key can bridge into the call by pressing the corresponding bridged appearance key unless the user has invoked privacy.

2. Press the **Release** button or place the handset on hook to end an active call.

   Either you or the caller can end an active call.

Redial list

Redial list

Personal Directory (PD), Callers list, and Redial list are intertwined within the digital stations that support this capability (redial and callers only on the 3903, but redial, callers, and directory on the 3904 and 3905) or PD data on PPM (UNIStim).

The Redial List is a call log feature. The content of the list is generated during call processing. You cannot modify this content. However, you can delete or, in some cases, copy entries to the Personal Directory.

The 3903 phone has a greatly reduced capacity for storing this data. The following is the Redial list size:

- 3903 phones: 5 entries
- All other phones: 100 entries

Redial List supports the following for devices that support Personal Directory:

- Maximum entries = 100 (5 for the 3903)
- Maximum characters in name = 24
- Maximum characters in DN = 31
- Multiple actions:
  - Dial DN of an entry.
  - Edit the digits of an entry.
  - Copy the information of an entry and add it to the Personal Directory, allowing details to be modified.
  - Delete an entry.
- Password protection to control access to the Redial List.
- One-minute time out to exit if the user is idle.

PPM stores the most recent 100 call log entries, which are saved in the format of one entry per one call format. When the device is logged in, the saved call log entries are separated into Callers and Redial list.

This is invisible to Communication Manager. It is handled either by the telephone itself (3904) or Device Adapter (UNIStim).

Redial lists are an automatic feature of certain digital and UNIStim stations. Stations with a display and the **Directory** or **Log** button can provide a "trail" of called and calling parties and can copy entries from either the called (Redial list) or calling party (Callers list) lists into a personal directory. This application is completely independent of any corporate directories.

Note that 39xx stations with this capability handle it completely internal to the phone. For added robustness, the UNIStim stations supporting this provide it using the PPM as the data warehouse. This permits the PPM call history to survive a reboot of the station.

> *** Note:**
>
> If primary Session Manager fails and secondary Session Manager becomes available, then after a station reboot some of the Redial list entries can be lost.

Changing the station control password

About this task

The norm will be to use ProVision to migrate, for passwords and any other elements. However, an administrator may need to create a station using Communication Manager station programming or may need to add the capability to an existing endpoint. To secure the data, a station control password is required. This is administered on the station data initially. Use this procedure to program the password data for a Device Adapter that was already migrated.

> *** Note:**
>
> The password is user administrable. User can change the password to prevent even the systems administrator from knowing the password.

Procedure

1. Edit a station that supports the capability.

2. Change the station password.

   Further password operations are carried out from the station.

Dialing a number from the redial list

About this task

The redial list is populated when the destination replies. This is the earliest that a name is available. The redirected call might change some data in the list.
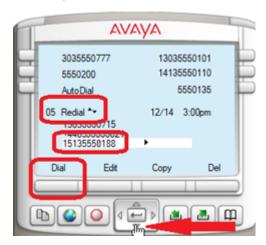
You can access the redial list from the soft keys of an idle endpoint.

Procedure

1. Do one of the following to access the redial list:

   a. On an idle endpoint, press the **Redial** soft key.

   b. On an idle endpoint, do the following:

      a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

      b. Scroll down to select the Redial List from the options.

    c. Press Select.

2. Use the up and down arrows to scroll through the stored entries.

   You may need to select between Old entries and New entries first.

   Calls to destinations that provide name information display the calling-party name. Otherwise, no name is present.

3. When you select an entry, a triangle facing to the right is present. Use the right arrow to view more details.

   You can use the right arrow when a number is displayed. Clicking the right arrow shows the number saved as the name as well as being saved as the number.

4. Use the left arrow to return to the list.

5. Press dial to call the party.

Editing a redial list entry

About this task

You cannot edit a name in the redial list. You can edit a number, as it may have been incorrectly dialed.

The redial list is populated when the destination replies. This is the earliest that a name is available. The redirected call might change some data in the list.

Procedure

1. Do one of the following to access the redial list:

   a. On an idle endpoint, press the **Redial** soft key.

   b. On an idle endpoint, do the following:

      a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

      b. Scroll down to select the Redial List from the options.

      c. Press Select.

2. Use the up and down arrows to navigate to the entry that you want to edit.

   You may need to select between Old entries and New entries first.

   Calls to destinations that provide name information display the called-party name. Otherwise, no name is present. This is especially true for invalid numbers, as the caller cannot be reached.

3. Press Edit to edit the number.

4. If the number is not the same as any existing entry, the number is saved.

   If the edited number is the same as an existing entry, the number is not saved.

5. Press dial to call the party.

Coping an entry from the redial list to the Personal Directory

About this task

This procedure is similar to the procedure of copying an entry from the callers list.

Procedure

1. Do one of the following to access the redial list:

   a. On an idle endpoint, press the **Redial** soft key.

   b. On an idle endpoint, do the following:

         a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

         b. Scroll down to select the Redial List from the options.

         c. Press Select.

2. Use the up and down arrows to navigate to the entry that you want to copy.

3. Press **Copy** to copy the entry.

   Use the dial pad to modify the name if necessary.

4. Press the **Next** soft key.

   Use the dial pad to modify the phone number if necessary.

5. Press the **Done** soft key.

6. Exit by clicking on the stop sign or by waiting for the one-minute inactivity timer to expire.

7. Enter the Personal Directory.

   The new entry is present in the Personal Directory. You can edit, delete, or modify the entry.

Deleting a redial list entry

Procedure

1. Do one of the following to access the redial list:

   a. On an idle endpoint, press the **Redial** soft key.

   b. On an idle endpoint, do the following:

      a. Press the Directory/Log button. This may show an icon or label. For more information, see the user guide for your station type.

      b. Scroll down to select the Redial List from the options.

      c. Press Select.

2. Use the up and down arrows to navigate to the entry that you want to delete.

3. Press Del to delete the entry.

   You can also delete the entire list by pressing Del without selecting an entry.

4. Confirm the deletion.

5. Press Yes to delete the entry.

6. Exit by clicking on the stop sign or by waiting for the one-minute inactivity timer to expire.

Redial lists feature interaction

When a call is redirected, the name returned will be that of the redirected destination. As a result, the user must confirm the number is to the party he or she wished to call prior to making the call.

Further, redirections may also end up in modified digits in the called number data. The Device Adapter has no control over routing decisions outside the Device Adapter.

Ring Again

Ring Again feature description

For Avaya Aura® deployment, the **Ring Again** feature is called the Automatic Call Back feature. The call-back operation is often referred to as Ringout or Ringout call.

For UNIStim endpoints, the **Ring Again** feature key is mapped to the **Auto Callback** key at a fixed position key. This fixed position key maps to a context-sensitive soft key and is active only when the capability is needed and applicable. Device Adapter treats it as a legacy RGA button and provides localization for UNIStim and all 39xx endpoints, except the 3901 endpoints.

For digital M3903, M3904, and M3905 endpoints, the **Ring Again** feature key is mapped to the **Auto Callback** key at a fixed position in the soft keys, in the same way it is done for the UNIStim endpoints. Other digital sets must have the **Auto Callback** key assigned to one of the available programmable keys. Device Adapter treats the **Auto Callback** button as a legacy RGA button, and provides localization for the M3902 set that has programmable soft keys, and for the M3903, M3904, and M3905 sets.

Analog sets can invoke **Ring Again** by using the Communication Manager Automatic Call Back Feature Access Code. Device Adapter treats it as a Flexible Feature Code equivalent.

✳ **Note:**

CS 1000 and Device Adapter does not support **Ring Again** feature on the PSTN trunks. **Ring Again** feature is supported only for local and private trunks.

Ring Again, Busy Destination

This feature works in the following manner:

- A user makes a call, which terminates on a busy destination. The phone displays the **Ring Again** key or soft key.

  ✳ **Note:**

  The phone does not display the **Ring Again** key if the call was made using a PSTN trunk.

- The user decides to activate Ring Again and be informed of the called party becoming idle and presses the **Ring Again** key.

- The user's phone screen returns to an idle state with the **Ring Again** key indicating it is active.

- The user can cancel the Ring Again request by pressing the **Ring Again** key before a callback offer is received. A callback offer is received when Avaya Aura® presents the Ringout call invitation.

- Eventually, the called-party station goes idle and is now available for a return call. When the endpoint receives a callback offer, the **Ring Again** key flashes and an audible tone is heard to indicate that a callback offer is received.

- The user answers this Ringout call like a normal call by off-hook or by selecting the ringing call appearance.

- The Ring Again feature can be activated for calls made from any line DN key.

Ring Again on No Answer

A corresponding variant is available for Ring Again on No Answer (RANA). For RANA, the same button is used, but the behavior is different.

Upon encountering a station that does not answer, a station with the Ring Again capability can activate RANA by pressing the Ring Again key. Later, when the desired station goes off-hook to make or receive a call, and then goes on-hook, the station that activated Ring Again receives a buzz through the telephone's loudspeaker while the lamp flashes if that station is idle. The station user can dial the desired station by lifting the handset or pressing a DN key, and then pressing the Ring Again key.

This feature works as follows:

- User A calls user B. User A receives a ring-back tone.

- The user waits long enough to decide to activate RANA.

- User A presses the Ring Again (RGA) key. The RGA key indicator turns on steadily.

- User A either goes on-hook or presses the Release (RLS) key. The indicator associated with RGA key remains on and user A is now free to receive or make other calls.

- User B goes off-hook to make a call, and then goes on-hook. User A is given a short ring through the loudspeaker and the indicator associated with the RGA key flashes.

- User A either picks up the handset or presses a DN key. User A receives dial tone.

- User A presses the RGA key. The user against which the Ring Again was placed is rung and the indicator associated with the RGA key is turned off.

Caveats

The user who requested the Ring Again service must accept the offer in a timely manner. That is, in a duration of six ring cycles. If the user does not answer the call-back request from the Ring Again service, the request is cancelled. This has implications when the Ring Again requesting party is on a fully busy station. If no appearances are available at the time of the Ring Again call-back offer, the request is cancelled.

The called party may go back off-hook before the user requesting Ring Again completes the retry of the original call. This is uncommon but may occur when the Ring Again target ends one call and starts a second immediately. If the user that requested the Ring Again accepts the Ring Again call-back request, the user may encounter a Ring Again, Busy case.

Analog endpoints encountering a busy destination are offered a choice of options rather than a button. They can enter a service code as provided by the server and activate Ring Again.

If the user attempts Ring Again to another target station, the initial Ring Again is cancelled. Users can only have one active Ring Again.

Ring Again feature administration

For information about configuring system-wide parameters, see the Communication Manager and System Manager documentation.

The endpoint is programmed to support the Ring Again service by either configuring the automatic call-back FAC or by adding the auto-cback key to the station. This can be done in either System Manager or Communication Manager.

Device Adapter maps the name auto-cback to the correct soft label on stations that are capable of using soft labels.

Ring Again feature operation

This feature is used in the following ways:

- When the destination is busy and the user presses the **Ring Again** key, Device Adapter subscribes to a Ringout call. The **Ring Again** key with an arrow now appears on the idle screen.

  The user can cancel the Ring Again request by pressing the **Ring Again** key before a callback offer is received. A callback offer is received when Avaya Aura® presents the Ringout call invitation.

- When the user receives an incoming indication that the target is idle, Device Adapter flashes the **Ring Again** key and provides audible indications, which can be a normal or priority ring tone.

  - The Ringout call is answered if the user takes the phone off-hook or selects a call appearance. If the user does not answer within a programmed period of time, Ring Again is cancelled. The programmed period of time is usually six ring cycles.

  - When Ringout call is presented by Communication Manager, the user receives an incoming call on a free call appearance and Ring Again soft key flashes indicating that this is a Ringout call. If there are no free appearances, the call cannot be presented.

  - When the **Ring Again** key flashes to present the callback offer, the user can press the **Ring Again** key to ignore the offer. The **Ring Again** key becomes dark and the audible tone stops. Pressing the **Ring Again** key only ignores the callback offer and does not cancel it. The offer automatically times out after the time-out period is reached.

    This behavior is similar to the Ignore option on the Avaya Aura® SIP endpoints. When a callback offer is presented on an Avaya Aura® SIP endpoint, the **Ignore** soft key appears on the endpoint. The user can press the **Ignore** soft key to ignore the callback offer.

- The user answers this Ringout call like a normal call by off-hook or by selecting the ringing call appearance.

> ✳ **Note:**
>
> There is a difference in configuration between Device Adapter and Communication Manager phones. Device Adapter phones have one call appearance by default and Communication Manager phones have two call appearances. Additionally, Communication Manager phones cannot deactivate Ring Again (Automatic Callback) when both call appearance lines are busy. The same behavior is applicable to a Device Adapter phone.

If both lines become busy, users cannot use Ring Again unless they restart their phone.

Example

The following is an example of the preceding scenario on Device Adapter phones:

- User A calls User B. User B answers.
- User C calls User A, but User A does not answer. User C presses Ring Again to call User A later.

- User D calls User C and User C answers.
- User A and User B end their call.
- The Ring Again is cancelled because there is only one call appearance.
- User C and User D end their call. Ring Again does not happen.

Avaya recommends that you configure a second call appearance for Device Adapter phones to overcome this limitation.

Ring Again feature interaction

The following limitations exist in Communication Manager implementation when compared with CS 1000:

- Users cannot activate Automatic Callback from a bridged call appearance.
- If a user activates Automatic Callback from a primary extension number, the return call notification rings at all bridged call appearances.

❗ Important:

A wait time of 32 seconds is required before attempting a second Ring Again to the same phone as the previous, over the same network.

For more information, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

Sequential Registration

The topics in this section provide information about the general behavior, limitations, and configuration of the Sequential Registration feature for UC phones.

In addition to the Sequential Registration information documented in this section, for information about Sequential Registration specific to a call center environment, see .

Sequential Registration feature description

Device Adapter uses the Sequential Registration feature to provide fail-over support for endpoints.

In Sequential Registration, only one endpoint can register at one time.

If a new registration request is received, Session Manager terminates an existing registration to register the new device. Sequential Registration is crucial for providing endpoint fail-over support and other useful operations.

> ✳ **Note:**
>
> - Device Adapter supports Sequential Registration only for UNIStim endpoints.
>
> - Avaya Aura® supports Sequential Registration on the SIP phones that are capable of supporting the Sequential Registration feature.
>
>   The J-series 3PCC phones do not support the Avaya Aura® SIP messaging that is required for Sequential Registration. If a J-Series 3PCC phone registers to a Device Adapter station definition for Sequential Registration, the buttons do not map correctly. This leads to a major loss of function. Hence, Avaya recommends that you do not use a J-series 3PCC phone for Sequential Registration.
>
>   However, Sequential Registration is supported on a J-Series Avaya Aura® phone.

Sequential Registration provides the following fail-over and operational support:

- An endpoint can re-register without waiting for the original SIP registration to fail. This fail-over mechanism minimizes the recovery time.

  Sequential Registration is supported for UNIStim endpoints.

  Sequential Registration also provides fail-over support for analog and digital endpoints that are on an MGC in an event of a network failure.

  When the MGC detects a registration failure, then depending on the deployment model, the MGC tries to re-register the endpoint either on the same cluster or alternate cluster. Because the device ID is the same, Session Manager considers this request as a re-registration request rather than a new request and registers the endpoint.

  However, the Sequential Registration feature itself is not supported for analog and digital endpoints.

  For more information, see [Sequential Registration fail-over support for analog and digital endpoints](#) on page 537.

- Sequential Registration allows two or more UNIStim endpoints to act as a single user device. If one device is registered and another device tries to register, Session Manager terminates the registration of the first device and registers the second device. For example, the user can log in at a desk phone, then log in with the 2050 client on the laptop. Later, the user can log in by using the desk phone or use some other device. With every new registration, Session Manager terminates the previous registration.

- Sequential Registration allows adding Avaya Aura® SIP phones. But, the user experience on these phones might be different than the Avaya Aura® user experience.

- Sequential Registration allows a user to perform a Virtual Office login at a UNIStim endpoint since Device Adapter Release 8.1.1.

  For more information, see [Virtual Office](#) on page 718.

To configure Sequential Registration, set the MDA configuration fields to the following:

- Set the **Max. Simultaneous Devices** value to 1.

- Clear the **Block New Registration When Maximum Registrations Active** check box to allow new registrations. Session Manager terminates the registration of an existing device to register the new device.

  > ✱ **Note:**
  >
  > However, selecting the **Block New Registration When Maximum Registrations Active** check box is the preferred method to provide fail-over support for digital and analog endpoints. Selecting this check box prevents an Avaya Aura® SIP device from trying to register sequentially to an analog or digital device.
  >
  > For more information, see

Sequential Registration with two or more Device Adapter UNIStim endpoints but without Avaya Aura® SIP endpoints

CS 1000; and therefore, Device Adapter identifies each UNIStim station by a hardware port ID or Terminal Number (TN). In CS 1000, all TNs must be unique. No two devices can share a TN, although, they can share MADN numbers, feature key definitions, and so on.

If you want to allow a user to use two or more Device Adapter UNIStim endpoints by using Sequential Registration, you must set the **Max. Simultaneous Devices** MDA configuration field value to 1. If you set the **Max. Simultaneous Devices** value to more than one, redundancy and call processing problems occur.

- The endpoints may fail over to a geographic redundancy cluster and the Device Adapter cluster cannot recognize that the other endpoint exists.

- Device Adapter does not correctly handle call-related messages. Hence, the call processing fails.

As a result, if you want to have a 1140 and a 2050 share a user extension and station definition, then only one of these endpoints can be active. Hence, the **Max. Simultaneous Devices** value must be set to 1. Any other value is not supported if you want to configure Sequential Registration and allow two or more Device Adapter UNIStim endpoints.

Therefore, whenever a 1140 UNIStim station is the active station for a user, the user receives the CS 1000 user experience for the 1140 UNIStim station, if:

- The user station is configured as 1140.

- The user is logged in and registered with a 1140 UNIStim station.

In addition to the 1140, if the user also has a 2050 soft client, the user can log in by using the same user identity. But, because the node and TN are the same, Device Adapter cannot register both the endpoints concurrently. If **Max. Simultaneous Devices** is set to 1, the Session Manager that receives the SIP REGISTER message terminates the registration of the 1140 endpoint and registers the 2050 soft client.

Because the 2050 and 1140 have the same basic layout, there is no difference in the base feature handling. However, if the 1140 has expansion modules, the station definition includes these modules. If 2050 does not have the modules, the extra keys are lost when the user uses the 2050.

Note that allowing the 2050 to register by terminating the 1140 registration was inherently unstable in releases prior to Device Adapter Release 8.1. From the messages received, Device Adapter is aware that Session Manager has ended the UNIStim set registration. Device Adapter prevents re-registration without deliberate user operations.

However, if the endpoint loses network service, the endpoint restarts and tries to register to a new server. The new server might be in a geographic redundancy cluster; and hence, does not have access to the information in the prior device.

To resolve this problem, since Release 8.1, Device Adapter stores the registration termination status within the endpoint. Thereby, preventing the endpoint from registering with Session Manager until the user chooses to do so. Hence, the endpoint does not try to re-register automatically.

Sequential Registration with two or more Device Adapter UNIStim endpoints and one or more Avaya Aura® SIP endpoints

If you have some other device or application; for example, Expert Client or 96x1, in addition to two or more Device Adapter UNIStim stations, the same general feature interaction applies as when you configure Sequential Registration for multiple UNIStim endpoints without the Avaya Aura® endpoints.

- If the user wants to use two or more Device Adapter UNIStim endpoints, then you must set the **Max. Simultaneous Devices** value to 1 to limit the maximum number of registered devices to one. Only one Device Adapter UNIStim endpoint can register at one time.

- If the user wants to use a mixture of SIP endpoints and multiple Device Adapter UNIStim endpoints, then you must set the **Max. Simultaneous Devices** value to 1.

Furthermore, if a Device Adapter station definition is used as the primary station definition and an Avaya Aura® SIP endpoint uses this station definition, the user experience on the Avaya Aura® SIP endpoint differs.

For example, a user has a 1140, a 2050 soft client, and a 96x1 SIP phone. The user may register with the Avaya Aura® SIP device, terminating the registration of the Device Adapter endpoint, which can be either the 1140 hard client or the 2050 soft client. However, the operation of the 1140 and the 96x1 are different, most feature buttons on the Device Adapter station map to the feature list on the 96x1, and the user experience of the feature buttons that are on both the CS 1000 endpoint and the Avaya Aura® endpoint is not the same.

This is especially true for the definition and handling of some context-sensitive soft keys on Device Adapter. For example, a Transfer soft key on a Device Adapter UNIStim endpoint has a call

appearance or bridged appearance attached to it. Device Adapter maps the action of the user pressing the key to the equivalent of:

- Placing the current call on hold.

- Seizing a new call appearance.

- Sending any transfer key-specific SIP messages that are sent by a 96x1.

Conversely, a 96x1 or any other Avaya Aura® SIP phone that uses this station definition has one or more additional call appearance buttons. The additional call appearance behind the transfer soft key on the UNIStim phone appears as a new call appearance, with the button labeled **transfer**. This provides the line appearance that is crucial for allowing the transfer to be carried out.

This button is configured to reserve a call appearance for outgoing calls used for Transfer and Conference. Therefore, the additional call appearance appears on the 96x1 and can be used in the Avaya Aura® user experience model. No visible button exists on the Device Adapter UNIStim phone.

You must also consider the number of keys for the 96x1 that uses the Device Adapter station profile. If the Avaya Aura® SIP endpoint has more programmable buttons, then the endpoint remains functional. But, if the UNIStim endpoint has key expansion modules, the key expansion modules do not map appropriately. An 18 button Key Expansion Module does not map to a 12 or 24 button Key Expansion Module.

Some feature buttons on the Device Adapter endpoint are included in the feature list on the 96x1 and other Avaya Aura® SIP endpoints. You can access this feature list by using the scrollable menu on the 96x1 and the Avaya Aura® SIP endpoints. Therefore, a feature that uses a feature button on the 1140 potentially uses a corresponding entry in the feature list of the 96x1 and other Avaya Aura® SIP endpoints to obtain a similar service operation whenever the CS1K-IP definition maps to a 96X1, J-series, or Expert Client.

Caveat for allowing two or more Device Adapter UNIStim endpoints to register

Setting the **Max. Simultaneous Devices** value to 1 allows a user using any UNIStim station to register by using a 2050 soft client, without requiring additional licenses. This configuration is also a practical option if a user wants to use a UNIStim endpoint for emergency purposes, and the other available stations have fewer feature buttons.

You can allow any UNIStim endpoint type to share a single user definition. If you use a less capable endpoint (with fewer feature buttons) that has a simple definition as your primary station for Sequential Registration, and then register a more capable endpoint (with more buttons), then:

- All feature function buttons that are configured on the primary station are available on the more capable station.

- Additional buttons on the more capable station are undefined and cannot be used.

For example, a user wants to use a 1120 and a 1140 endpoint sharing the same station definition and user profile.

The station definition for a 1120 endpoint has eight programmable buttons, which are 0 through 7. These buttons include the four physical buttons (0 through 3) on page 1, and four buttons (4 through 7) on page 2, which are obtained by using the Shift key. There are no additional buttons on the **Feature Buttons** tab.

The station definition for a 1140 endpoint allows up to 12 programmable buttons, plus one or more expansion modules. In addition to the eight buttons (0 through 7) on the base button page, there are four additional buttons on the **Feature Buttons** tab.

If you set the 1120 station definition as the primary definition, the 1140 endpoint can log in to the 1120 station definition and access buttons 0 through 7. This allows all feature functions of the 1120 on the 1140, but the four additional feature buttons on the 1140 are lost.

Conversely, if you set the 1140 station definition as the primary definition, and when the user registers on the 1120 by using the station definition of the 1140, then buttons 8 through 11 and any expansion modules on the 1140 are lost. Only the eight lowest numbered buttons are available. The lost buttons and expansion modules may contain feature functions, which are also lost.

For more information, see Recommendations when configuring Sequential Registration support for two or more Device Adapter UNIStim endpoints on page 534.

Recommendations when configuring Sequential Registration support for two or more Device Adapter UNIStim endpoints

You must configure the station definition, which normally represents the primary station that the user uses. Normally, this is the CS1K-IP station for a UC phone and CS1K_IPCC station for a CC phone.

Avaya recommends the following when you want to configure Sequential Registration support for two or more Device Adapter UNIStim endpoints:

- Use the same CS1K_IP or CS1K_IPCC station definition for endpoint types with similar capabilities only. For example, a 12 feature key station definition should only be used with the 12 feature key endpoint devices.

  However, you can use the same station definition with endpoint types that have different capabilities for emergency purposes, provided that you configure the lowest indexed button as a call appearance button.

  When the endpoint has fewer buttons or display lines than the station definition, these buttons and the associated services along with the display lines are lost on the endpoint.

- When you want to use stations with divergent capabilities, then to avoid loss of keys, Avaya recommends that you use an endpoint with the least number of keys as the primary station. Ensure that you configure the most crucial features and at least one call appearance for the buttons available on the primary station.

  The station data that is sent to Device Adapter is according to the template that is generated by the station definition. Device Adapter modifies the information to ensure maximum

compatibility with the endpoint that is being registered, although, there might be some loss of keys. The 96x1 and other SIP endpoints use a similar data conversion for compatibility with the SIP stations.

For more information, see [Sequential Registration with two or more Device Adapter UNIStim endpoints and one or more Avaya Aura SIP endpoints](#) on page 532.

- Ensure that the endpoint supports the programmable feature buttons that you have defined in the CS1K_IP or CS1K_IPCC station definition.

- Ensure that the expansion module supports the same number of feature buttons that you have defined in the CS1K_IP or CS1K_IPCC station definition.

- Avoid configuring essential buttons on the expansion modules.

Caveats

- Capability mismatch due to changes in the number of available buttons is beyond the scope of Device Adapter. Avaya recommends that you register the migrated CS 1000 endpoints to user stations with equal number of programmable buttons. If necessary, the user can register and have fewer buttons, but that is a limitation of the device used.

- There might be some user experience differences if the user switches between the migrated CS 1000 endpoint and the Avaya Aura® SIP endpoint. For example, some feature buttons on the Device Adapter endpoint are included in the feature list of the 96x1 and other Avaya Aura® SIP endpoints. You can access this feature list by using the scrollable menu on the 96x1 and Avaya Aura® SIP endpoints. Therefore, a feature that uses a feature button on the 1140 uses a corresponding entry in the feature list of the 96x1 and other Avaya Aura® SIP endpoints to obtain a similar service operation.

- Legacy Avaya Aura® SIP devices have fewer significant caveats, although there might be an extra call appearance for the Transfer key. However, buttons on expansion modules may be lost in legacy Avaya Aura® SIP devices.

Configuring Sequential Registration support for two or more Device Adapter UNIStim endpoints

Procedure

Do one of the following:

- Configure the CS1K_IP station in Communication Manager.

- Do the following to configure the CS1K_IP station in System Manager:

    a. Log on to System Manager by using the appropriate administrative credentials.

    b. Click **Users** > **User Management** > **Manage Users**.

    c. Select the user, and then click **Edit**.

    d. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.

    e. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, click **1**.

f. Clear the **Block New Registration When Maximum Registrations Active** check box.

g. Click **Commit**.

Sequential Registration with two or more Device Adapter UNIStim endpoints feature operation

About this task

For example, a user has 1140 at the desk, a 2050 soft client on the computer, and a 96x1 in the lab. The user goes to the lab, and then goes home and registers by using the computer. The next day the user goes to the office and uses the 1140.

The user's identity is extension 2355777, which uses node 1050 and TN 32-0-6-1.

Procedure

1. The user is registered at 1140.

2. The user goes to the lab. The user logs in with the 96x1 in the lab as 2355777.

   a. The user can log in. The user experience and set display is similar to a 96X1 station.

   b. When Session Manager terminates the 1140 SIP registration, the 1140 displays the following messages:

   ```
   Registration is on hold.

   Press RESET to continue.
   ```

   c. A Reset soft key is displayed at the 1140.

   d. The 96x1 can place and receive calls.

3. User goes home and starts 2050.

   a. The 2050 soft client offers TN 32-0-6-1 and node 1050 as the station.

   b. Session Manager terminates the SIP registration of the 96x1. The user is logged out.

   c. The 2050 can place and receive calls.

4. User goes to the office the next day and switches to 1140.

   a. The user presses the Reset soft key on the 1140.

   • The user does not shut down the 2050.

      a. When Session Manager terminates the SIP registration, the 2050 displays the following messages:

      ```
      Registration is on hold.

      Press RESET to continue.
      ```

      b. The 2050 displays a Reset soft key.

   • The user shuts down the 2050.

Because the 2050 is shut down, the 2050 attempts to re-register only when the user starts it again. As this is a deliberate user action, it is acceptable.

b. The 1140 can place and receive calls.

Sequential Registration fail-over support for analog and digital endpoints

You can configure the Sequential Registration fail-over support for Device Adapter analog and digital endpoints, that are on an MGC, in an event of a network failure either by allowing new registration requests or blocking new registration requests.

Fail-over support for analog and digital endpoints by blocking new registration requests

You can configure fail-over support for analog and digital endpoints by setting **Max. Simultaneous Devices** to 1 and selecting the **Block New Registration When Maximum Registrations Active** check box, which blocks any new registration request.

This configuration prevents another device from using the Device Adapter station registration through Sequential Registration. Hence, the Device Adapter station need not recover the station identity.

Till Device Adapter Release 8.1.1, the preceding configuration caused a delay when the SIP connectivity between the MGC and Device Adapter or between Device Adapter and Session Manager was lost, and endpoint registration failed over. The registration was delayed till the time the keep-alive signaling detected a connectivity loss, and Session Manager un-registered the current SIP registration and allowed a new SIP registration.

In Device Adapter Release 8.1.2, Session Manager identifies an endpoint for registration by using the device ID. If the MGC detects a registration failure, then depending on the deployment model, the MGC tries to re-register the endpoint either on the same cluster or alternate cluster. Because the device ID is the same, Session Manager processes this request as a re-registration request rather than a new request and registers the endpoint. This results in faster fail over.

Avaya recommends that you use this method to provide fail-over support for analog and digital endpoints.

Fail-over support for analog and digital endpoints by allowing new registration requests

Use the Sequential Registration configuration, that is, allow new registration requests, to provide fail-over support for analog and digital endpoints.

Depending on where the outage occurred either the MGC fails over to an alternate Device Adapter instance within the same cluster or Device Adapter may register to an alternate cluster.

The following are the scenarios:

- In an N+1 cluster, if a Device Adapter instance on a primary cluster (primary Avaya Breeze® platform) loses connectivity, the endpoints fail over to another Device Adapter instance within the same cluster.
- In an N+1 cluster, if the one cluster loses connectivity, the MGC on that cluster fails over to the Alternate 1 cluster.

- If the connectivity between the primary cluster and Session Manager is lost, every MGC on the primary cluster fails over to the Alternate 1 cluster.

However, the use of Sequential Registration to provide fail-over support for analog and digital endpoints is not recommended because of the following reasons:

- If a digital or analog endpoint gets unregistered, the MGC of this digital or analog endpoint immediately tries to re-register the endpoint. There is no mechanism to prevent the MGC from immediately trying to re-register a digital or analog endpoint that gets unregistered.

  Because the configuration is to allow new registration request, if a 96x1 or other SIP device tries to sequentially register, Session Manager unregisters a currently registered digital or analog endpoint. The MGC of this digital or analog endpoint immediately sends a SIP re-registration request to Session Manager, and repeats the re-registration attempt until the registration succeeds. This process unregisters the 96x1 or other SIP device.

- Sequential Registration verifies station compatibility to a limited extent to prevent a user from logging in at an incompatible station definition.

  When a user uses analog or digital endpoints, the user cannot log in with the same user identity at any other device, that is, Avaya Aura® SIP endpoint or UNIStim endpoint.

Configuring fail-over support for analog and digital endpoints by blocking new registration requests

About this task

Use the Sequential Registration configuration fields to configure fail-over support for analog and digital endpoints by blocking new registration requests.

Selecting the **Block New Registration When Maximum Registrations Active** check box restricts an Avaya Aura® SIP device from trying to register sequentially to an analog or digital endpoint.

✴ **Note:**

Avaya recommends that you use this method to provide fail-over support for analog and digital endpoints.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Click **Users** > **User Management** > **Manage Users**.

3. Select the user, and then click **Edit**.

4. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.

5. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, click **1**.

6. Select the **Block New Registration When Maximum Registrations Active** check box.

7. Click **Commit**.

Configuring fail-over support for analog and digital endpoints by allowing new registration requests

About this task

Use this procedure to configure fail-over support for analog and digital endpoints by using Sequential Registration. This configuration allows new registration requests.

However, this fail-over method is not recommended.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.
2. Click **Users** > **User Management** > **Manage Users**.
3. Select the user, and then click **Edit**.
4. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.
5. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, click **1**.
6. Clear the **Block New Registration When Maximum Registrations Active** check box.
7. Click **Commit**.

Sequential Registration and MDA in a Call Center Elite environment

In addition to the general MDA and Sequential Registration information, the topics in this section provide information specific to MDA and Sequential Registration in a Call Center Elite environment.

Related links

[Multi-Device Access](#) on page 493
[Sequential Registration](#) on page 529

MDA and Sequential Registration support for Call Center Elite

MDA support

MDA support in a Call Center Elite environment depends on the station type:

- MDA is supported on a UC phone (CS1K_IP) irrespective of whether the phone is CTI controlled or not.
- MDA is not supported on a call center-capable phone (CS1K_IPCC).

> *️⃣ **Note:**
>
> Ensure that you deny MDA for CS1K_IPCC phones by setting **Max. Simultaneous Devices** to `1`.

Sequential Registration support

Both Call Center Elite and Device Adapter support Sequential Registration of CC phones irrespective of whether an agent is logged in or logged out of the phone as a Call Center Elite agent.

> *️⃣ **Note:**
>
> • The J-series 3PCC phones do not support the Avaya Aura® SIP messaging that is required for Sequential Registration. If a J-Series 3PCC phone registers to a Device Adapter station definition for Sequential Registration, the buttons do not map correctly. This leads to a major loss of function, especially call center functions. Hence, Avaya recommends that you do not use a J-series 3PCC phone for Sequential Registration.
>
>   However, Sequential Registration is supported on a J-Series Avaya Aura® phone.
>
> • For the reasons mentioned in the preceding Note, Avaya recommends that you do not use a J-series 3PCC phone for MDA when using a phone as a UC phone in a call center.

MDA and Sequential Registration support for CTI controlled endpoints

Call centers generally use Computer Telephony Integration (CTI) applications, such as Avaya Workspaces, along with Avaya Aura® Call Center Elite to perform call-center specific operations such as retrieving the caller's order details from a database.

Depending on the endpoint configuration, you can use the endpoint as a media-only (CS1K_IP) endpoint or a CC endpoint (CS1K_IPCC) with the CTI application. Call center-specific features are not available on a media-only endpoint.

MDA support for CTI controlled phones

MDA is supported only on a CTI controlled UC endpoint (CS1K_IP) irrespective of whether connection to the CTI application is proper or lost.

> *️⃣ **Note:**
>
> • Ensure that you deny MDA for CS1K_IPCC phones by setting **Max. Simultaneous Devices** to `1`.
>
> • Avaya recommends that you use an endpoint that is configured as a CC endpoint (CS1K_IPCC) with a CTI application in Call Center Elite. In an event when connection to the CTI application is lost, the agent can use the phone to perform call center-specific operations.
>
>   For example, if connection to Avaya Workspaces is lost, and if the phone is configured as a CC phone, the agent can log in to the phone as a Call Center Elite agent. The phone takes over the control from Avaya Workspaces and operates as a CC phone. Call center-

specific features now become available on the phone. The agent can then use the phone to perform call center-specific operations.

- A CTI controlled call center-capable phone can be used to perform call center-specific operations in the event of a connection failure to the CTI application only in a Call Center Elite environment. If you are using a call center application other than Call Center Elite; for example, Avaya Aura® Contact Center, you can use only a UC endpoint (CS1K_IP) as a CTI controlled endpoint. Hence, Avaya recommends that you use the CS1K_IP station type as a CTI controlled endpoint in a call center other than Call Center Elite.

Sequential Registration support for CTI controlled phones

Device Adapter supports Sequential Registration for both UC and CC phones.

Only a small subset of endpoints can function as CC endpoints. You can use the other endpoints as media-only endpoints with the CTI application. However, you cannot use these endpoints to perform call center-specific functions in the event of a CTI connection failure. For more information about the supported CC phone types that you can use to perform call center-specific operations in a Call Center Elite environment in the event of a CTI connection failure, see Supported phone types in an Avaya Aura Call Center Elite environment on page 55.

MDA limitations when using CTI applications with Call Center Elite

* **Note:**

     MDA is supported only on UC phones (CS1K_IP) in a Call Center Elite environment.

The functionality offered by the CTI applications is limited to the station capabilities. In addition to the general MDA limitations, the following are the MDA limitations when you use a UC phone with a CTI application in a Call Center Elite environment:

- CTI applications can control the digital, UNIStim, and analog endpoints for media only.

- If digital or UNIStim endpoints are controlled by a CTI application, then these endpoints provide only UC functions. Note that the endpoints must have the required buttons and display. Analog endpoints do not have buttons and only CLASS analog sets provide a display. Hence, an agent can perform only "hook-flash and code" operations on an analog endpoint.

    Therefore, MDA is not supported on analog phones.

- For a CTI controlled UC phone, ensure that you use the CS1K_IP station template to define the station definition for the phone:

    Registering an existing UNIStim endpoint to a new 96x1 station definition is contradictory. Device Adapter does not support using a non-UNIStim station definition for a UNIStim endpoint that is registering for MDA.

- UC endpoints do not support call center-specific features and operations.

- In a Device Adapter endpoint avoid MDA when mixing CTI controlled UC endpoints (CS1K_IP) with CTI controlled CC endpoints (CS1K_IPCC).

Avaya recommends that you use Sequential Registration in this case.

For more information, see MDA and Sequential Registration support for CTI controlled endpoints on page 540.

- For CTI controlled media-only (UC) phones, CTI controls only the most recently registered device. The following is an example when the maximum number of simultaneous devices is set to 3:

  - A user logs in to device A and this device is acquired by a CTI controller.

  - The user logs in to device B:

    • Device A remains registered and usable.

    • Device B registers and becomes usable.

    • CTI control at device A ends. Only device B is CTI controlled.

  - The user logs in to device C:

    • Device A remains registered and usable.

    • Device B remains registered and usable.

    • Device C registers and becomes usable.

    • CTI control at device B ends. Only device C is CTI controlled.

  - The user logs in to device D:

    The maximum number of concurrently registered devices is exceeded.

    • Device A is unregistered.

    • Device B remains registered and usable.

    • Device C remains registered and usable.

    • Device D registers and becomes usable.

    • CTI control at device C ends. Only device D is CTI controlled.

  - If the user unregisters device D and if no other device is registered, the last device that was CTI controlled and is still registered becomes CTI controlled. That is, device C becomes CTI controlled.

    If the user wants device B to be CTI controlled, the user must unregister device B and log in to device B again. Device B becomes CTI controlled. Device C is no longer CTI controlled.

Minimum features required on a CTI controlled endpoint for MDA and Sequential Registration

Some endpoints may not have enough feature keys and/or soft keys to support full function of a station definition. Whereas, other endpoints may provide display using alternate display lines. In

either case, even the most limited UNIStim endpoint supports minimal functions, provided the necessary service or button type is configured for the endpoint.

The CTI controlled endpoints used for MDA and Sequential Registration should support at a minimum the following services consistent with the Communication Manager handling:

- One or more call appearances

- Remote-party information display capabilities

- Fixed-purpose keys such as:
    - Release
    - Volume
    - Hold

- Common programmable feature buttons and soft keys such as:
    - Transfer
    - Conference
    - Call Forward
    - Voice Mail

Recommendations for identifying phones for Sequential Registration in a call center environment

User experience when switching between endpoints by using Sequential Registration is consistent when the station definitions of these endpoints provide the same features and options. For a consistent user experience when switching between the endpoints, ensure the following:

- Identity the station types that provide similar capabilities.

- The supported stations must have one or more feature keys available.

- The stations must have at least one button defined for call appearance.

Some stations, such as the 1150, have additional feature keys, which are dedicated to specific CS 1000 applications. These buttons can be used when the endpoint is used as a call center endpoint. However, these buttons are unusable when the endpoint is used as a UC endpoint.

Any station definition, with or without the supported expansion module, allows a user to register with an endpoint that supports minimal service, provided key 0 of the station is defined as a call appearance button if you are using a single key phone.

However, for full compatibility between station types, ensure the following:

- An endpoint that is sequentially registering to a station that has multiple feature buttons must provide at least the matching number of buttons.

    Having fewer buttons on the endpoint results in loss of service associated with the missing buttons.

However, you can use the same station definition with endpoint types that have different capabilities for emergency purposes, provided that you configure the lowest indexed button as a call appearance button.

• An endpoint that is sequentially registering to a station that has expansion modules must provide the same number of expansion modules and buttons per module.

In Sequential Registration, loss of certain buttons when switching between endpoints results in degradation of the user experience. For example, if the user's primary station has 12 buttons, then sequentially registering a station that has 4 buttons results in loss of the upper 8 buttons.

To maintain a consistent user experience, Avaya recommends that you use stations with similar capabilities for Sequential Registration.

Station compatibility matrix for Sequential Registration of UC phones in a call center environment

Identify compatible station types for Sequential Registration of UC phones

The following are the considerations when identifying compatible station types for Sequential Registration of UC phones in a call center environment:

• If the primary station definition is a single feature key (or line) button endpoint, then:

- Any UNIStim endpoint can sequentially register with no loss of feature.

• If the primary station definition has 4 feature key buttons and has no expansion modules, then:

- Sequentially registering any endpoint that has 4 or more feature key buttons results in no loss of features.

- Sequentially registering an endpoint that has a single feature button retains key 0, but key 1, key 2, and key 3 are lost.

• If the primary station definition has 4 feature key buttons and has at least one expansion module, then:

- Sequentially registering any endpoint that has 4 or more feature key buttons and an equal or greater number of expansion modules, each with an equal or greater number of feature buttons, results is no loss of features.

- Sequentially registering an endpoint that does not have expansion modules or has expansion modules with fewer buttons results is loss of the missing buttons on those expansion modules.

- Sequentially registering an endpoint that has a single feature button retains key 0, but key 1, key 2, and key 3 are lost.

- If the primary station definition has 10 feature key buttons and does not have expansion modules, then:
  - Sequentially registering any endpoint that has 10 feature key buttons results in no loss of features.
  - Sequentially registering an endpoint that has fewer feature buttons results in loss of the missing buttons.
- If the primary station definition has 10 feature key buttons and has at least one expansion module, then:
  - Sequentially registering any endpoint that has 10 or more feature key buttons and an equal or greater number of expansion modules, each with an equal or greater number of feature buttons, results is no loss of features.
  - Sequentially registering an endpoint that does not have expansion modules or has expansion modules with fewer buttons results is loss of the missing buttons on those expansion modules.
  - Sequentially registering an endpoint with fewer feature buttons results in loss of the missing buttons.

Station definitions with a single line appearance key

Any station can register using the TN of a single line appearance station. All UNIStim endpoints have 1, 4, 10, or 12 feature keys and support single line appearance. Further, all stations have at least as many display lines as the station definition.

Note that these stations do not support expansion modules.

The following table provides compatibility matrix for Sequential Registration of station definitions that have a single line appearance key with other station types:

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
2001	Not applicable	Any	Not applicable	No capability loss.
1110	Not applicable	Any	Not applicable	No capability loss.
1210	Not applicable	Any	Not applicable	No capability loss.

Station definitions with up to four programmable feature keys

An endpoint with station definition of four or more buttons loses the highest three buttons when this endpoint sequentially registers with an endpoint that has only a single line appearance. All other stations do not lose feature keys.

The following are the scenarios when a lesser capable endpoint tries to sequentially register with a 1120 station definition that has one or more of the 18 button expansion module:

- If an endpoint with fewer expansion modules sequentially registers to the 1120 endpoint, then the lesser capable endpoint loses all buttons that are configured on the additional expansion modules on the 1120 endpoint.

- If the expansion modules of any endpoint have fewer buttons as compared to the 1120, the additional buttons are lost. For example, if you define buttons 0 to 17 on page 1 of the 1120 expansion module, and if you sequentially register the 1230 endpoint to the 1120 endpoint, buttons 12 to 17 of the 1120 endpoint are lost because the 1230 endpoint has a twelve-button expansion module.

✱ **Note:**

The 2050 soft phone is functionally the same as the 1140 phone and is grouped in the following table.

The following table provides compatibility matrix for Sequential Registration of station definitions that have up to four programmable feature keys with other station types:

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
2002	Not applicable	2001, 1110, or 1210	Not applicable	Only key 0 is maintained. Display is available.
		Any other including SIP	Not needed	No capability loss.
1120	When no expansion module is used	2001, 1110, or 1210	Not applicable	Only key 0 is maintained. Display is available.
		Any other including SIP	Not needed	No capability loss.
1120	18, 36, or 54 added buttons	2001, 1110, or 1210	Not applicable	Only key 0 is maintained. Expansion module buttons are lost. Display is available.
		2002 or 2007	Not applicable	Any expansion modules are lost. Otherwise, there is no capability loss.
		1120, 1140, or 1150 (2050)	0, 18, 36, or 54 buttons	No capability loss, unless there are fewer expansion modules.

Table continues…

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
		1220 or 1230	0, 12, 24, or 36 buttons	Only the first 12 buttons (0-11) of the 1120 expansion module are available. Otherwise, there is no capability loss, unless there are fewer expansion modules.
		2004	0, 24, or 48 buttons	Top 6 buttons (buttons 18 to 23) of the 2004 expansion module are unavailable. Third expansion module is lost. Otherwise, there is no capability loss, unless there are fewer expansion modules.
		Avaya Aura® SIP device	As applicable	No capability loss, unless there are insufficient button pages and buttons per page.
1220	When no expansion module is used	2001, 1110, or 1210	Not applicable	Only key 0 is maintained. Display is available.
		Any other	Not applicable	No capability loss.
1220	12, 24, or 36 buttons	2001 or 1210	Not applicable	Only key 0 is maintained. Expansion module buttons are lost. Display is available.

Table continues…

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
		1110	0, 18, 36, or 54 buttons	Only key 0 is maintained. Expansion module buttons may be maintained if present, but the highest 6 buttons of the 1110 expansion module are not used. Display is available. Otherwise, there is no capability loss, unless there are fewer expansion modules.
		1120, 1140, or 1150 (2050)	0, 18, 36, or 54 buttons	No capability loss, unless there are fewer expansion modules. Highest 6 buttons of the 11xx expansion module are not used.
		1220 or 1230	0, 12, 24, or 36 buttons	No capability loss, unless there are fewer expansion modules.
		2002 or 2007	Not applicable	Expansion modules are lost.
		2004	0, 24, or 48 buttons	Top 12 buttons of the 2004 expansion module are unavailable. The third expansion module is lost. Otherwise, there is no capability loss, unless there are fewer expansion modules.
		Avaya Aura® SIP device	As applicable	No capability loss, unless there are insufficient button pages and buttons per page.

Station definitions with ten or more programmable feature keys

An endpoint with station definition of ten or more buttons loses the highest nine (or eleven) buttons when this endpoint sequentially registers with an endpoint that has only a single or four line appearances. All other stations do not lose feature keys.

The following are the scenarios when a lesser capable endpoint tries to sequentially register with a station definition that has ten or more programmable feature keys and one or more expansion modules:

- If an endpoint with fewer expansion modules sequentially registers, all buttons on the additional expansion modules of the more capable endpoint are lost.

- If the expansion modules of any endpoint have fewer buttons, the additional buttons on the more capable endpoint are lost. For example, if you define buttons 0 to 17 on page 1 of the 1140 expansion module, and if you sequentially register the 1230 endpoint to the 1140 endpoint, buttons 12 to 17 of the 1140 endpoint are lost because the 1230 endpoint has a twelve-button expansion module.

> ✳ **Note:**
>
> The 2050 soft phone is functionally the same as the 1140 phone and is grouped in the following table.
>
> The 1230 station is an exception because it has ten programmable feature keys.

The following table provides compatibility matrix for Sequential Registration of station definitions that have ten or more programmable feature keys with other station types:

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
2004, 2007, 1140,2050, 1150, 1230	When no expansion module is used	2001, 1110, 1210	Not applicable	Only key 0 is maintained. Display is available one line at a time.
		2002	Not applicable	Only keys 0 to 3 are maintained.
		1120	Not needed	
		1220	Not applicable	
		2004, 2007, 1140, 2050, 1150, 1230, Avaya Aura® SIP device	Not needed	No capability loss.
2004	24, 48 buttons	2001, 1110, 1210	Not applicable	Only key 0 is maintained. Expansion modules are lost. Display is available one line at a time.

Table continues…

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
		2002	Not applicable	Only keys 0 to 3 are maintained. Expansion modules are lost.
		1120	0, 18, 36, (or 54) buttons	Only keys 0 to 3 are maintained. The 2004 expansion modules lose top 6 buttons. If the 1120 has a third expansion module, the third expansion module is not usable.
		1220	0, 12, 24, (or 36) buttons	Only keys 0 to 3 are maintained. The 2004 expansion modules lose top 12 buttons. If the 1220 has an extra expansion module, the expansion module is not usable.
		2004	0, 24, or 48 buttons	No capability loss, unless there are fewer expansion modules.
		2007	Not applicable	Expansion modules are lost.
		1140, 2050, 1150	0, 18, 36, (or 54) buttons	The 2004 expansion modules lose top 6 buttons. If the 1140 has a third expansion module, the third expansion module is not usable.
		1230	0, 12, 24, (or 36) buttons	The 2004 expansion modules lose top 12 buttons. If the 1230 has a third expansion module, the third expansion module is not usable.

Table continues…

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
		Avaya Aura® SIP device	As applicable	No capability loss, unless there are insufficient button pages and buttons per page.
1140, 2050, 1150	18, 36, or 54 buttons	2001, 1110, 1210	Not applicable	Only key 0 is maintained. Expansion modules are lost. Display is available one line at a time.
		2002	Not applicable	Only keys 0 to 3 are maintained. The 1140 and 2050 expansion modules are lost.
		1120	0, 18, 36, (or 54) buttons	Only keys 0 to 3 are maintained. No other capability loss, unless there are fewer expansion modules.
		1220	0, 12, 24, (or 36) buttons	Only keys 0 to 3 are maintained. The 1140 and 2050 expansion modules lose top 6 buttons. No other capability loss, unless there are fewer expansion modules.
		2004	0, 24, or 48 buttons	No capability loss, unless there are fewer expansion modules. Top 6 buttons on the 2004 expansion modules are unused.
		2007	Not applicable	Expansion modules are lost.
		1140, 2050, 1150	0, 18, 36, or 54 buttons	No capability loss, unless there are fewer expansion modules.

Table continues…

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
		1230	0, 12, 24, or 36 buttons	The top 2 buttons on the 1140, 2050, and 1150 are lost. The 1140 and 2050 expansion modules lose top 6 buttons. Otherwise, there is no capability loss, unless there are fewer expansion modules.
		Avaya Aura® SIP device	As applicable	No capability loss, unless there are insufficient button pages and buttons per page.
1230	12, 24, or 36 buttons	2001, 1110, 1210	Not applicable	Only key 0 is maintained. The 1230 expansion modules are lost. Display is available one line at a time.
		2002	Not applicable	Only keys 0 to 3 are maintained. The 1230 expansion modules are lost.
		1120	0, 18, 36, or 54 buttons	Only keys 0 to 3 are maintained. Top 6 buttons on the 1120 expansion modules are unused. Otherwise, there is no capability loss, unless there are fewer expansion modules.
		1220	0, 12, 24, or 36 buttons	Only keys 0 to 3 are maintained. Otherwise, there is no capability loss, unless there are fewer expansion modules.

Table continues…

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
		2004	0, 24, or 48 buttons	No capability loss, unless there are fewer expansion modules on the 1230 station definition. Top 12 buttons on the 2004 expansion modules are unused.
		2007	Not applicable	Expansion modules are lost.
		1140, 2050	0, 18, 36, or 54 buttons	Top 6 buttons on the 1140 and 2050 expansion modules are unused. Otherwise, there is no capability loss, unless there are fewer expansion modules than those defined in the station definition.
		1230	0, 12, 24, or 36 buttons	No capability loss, unless there are fewer expansion modules.
		Avaya Aura® SIP device	As applicable	No capability loss, unless there are insufficient button pages and buttons per page.

Station compatibility matrix for Sequential Registration of call center phones without CTI control

This section provides information about the station compatibility matrix for Sequential Registration of call center phones that are used without CTI control, and all call center operations are performed by using the phone. Note that any endpoint that supports call center-specific features can also be CTI controlled. However, many endpoints that support CTI control in a call center do not support call-center specific features. However, these endpoints can be used as media-only endpoints.

Device Adapter supports the following call center-specific features on the supported CC endpoints. These features are consistent with Call Center Elite handling.

- Login and logout

- One or both of the following buttons that an agent can use to become available to receive incoming call center calls:

  - Auto-In

  - Manual-In

- One or both of the following buttons to set the agent work mode:

  - After Call Work (ACW)

  - Auxiliary Work (Aux Work)

  Note that the agent is unavailable to receive incoming call center calls in these work modes.

- One or more call appearance buttons.

- Three line display to provide call center-related information to the agent.

- Line appearances:

  - To receive incoming station extension calls and call center calls (ACD and DAC).

  - To make calls by using the station extension.

  - To modify existing calls.

- Additional bridged appearances for shared service.

- Generic service buttons that are used in call centers such as:

  - Transfer

  - Conference

  - Call Forward

  - Voice Mail

- Call center-specific buttons:

  - Buttons used by call center agents such as:

    - Supervisor Assist

    - Emergency Call

  - Buttons used by call center supervisors such as:

    - Agent Observe

    - Change Agent Skills (move agents from one queue to another)

Most UNIStim endpoint types support most, but not all, of the preceding features because they either do not have enough feature keys and/or soft keys, or do not have the required display capability.

Station definitions with less than ten programmable feature keys

Although station definitions with less than ten programmable feature keys cannot normally be used as call center agent stations, they may be used for media only with a CTI controller. These station definitions have insufficient feature buttons, which results in loss of buttons. You cannot

access the features associated with the lost buttons. Because CS 1000 stations do not have a Feature menu, you cannot access these features from the Feature menu as well.

- Single line stations cannot be used as call center stations because single line stations require a call appearance button and do not have any extra buttons to provide even the basic call center capability of agent login.

- Four button stations can provide a call appearance and a login/logout button.

Assume that Call Center Elite provides the following capability in a call center:

- Forces the agent into the Auto-In work mode after the agent logs in.

- Provides Timed After Call Work (TACW).

- Requires agent logout instead of supporting the Aux Work mode.

- Does not allow any other capability such as Supervisor Assist and displaying the queue status.

If preceding example, the endpoints with less than ten programmable feature keys might be able to provide enough feature buttons to be used. However, these endpoints lack the required display capability.

Hence, Avaya recommends that you use stations with less than ten feature key buttons as CTI controlled media-only endpoints. These endpoints are not recommended when an agent wants to log in to the endpoint as a Call Center Elite agent and use the endpoint to perform the call center operations when connection to the CTI application is lost.

Station definitions with twelve or more programmable feature keys and three display lines

You can use stations with twelve or more programmable feature keys and three display lines as call center endpoints because these endpoints have enough buttons and display lines for call center operations. However, stations with fewer buttons and display lines cannot sequentially register to call center stations that have twelve or more buttons programmed and have three display lines.

> ✳ **Note:**
>
> The 1230 phone has enough buttons, but has insufficient display capability. Hence, using the 1230 station to sequentially register with a station that has twelve or more programmable feature keys and three display lines is not recommended if you want to use the highest two buttons to configure essential CC feature buttons such as login/logout and work mode selection.

The following table provides compatibility matrix for Sequential Registration of station definitions that have twelve or more programmable feature keys and three display lines, with other station types. The 2050 soft phone is functionally the same as the 1140 phone and is grouped in the following table.

Primary station definition	Expansion module buttons	Station used for sequential registration	Expansion module buttons	Result
1140, 2050, or 1150	When no expansion module is used	1140, 2050, or 1150	Not needed	No capability loss.
		Avaya Aura® SIP device	Not needed	No capability loss.
	18, 36, or 54 buttons	1140, 2050, or 1150	0, 18, 36, or 54 buttons	No capability loss, unless there are fewer expansion modules.
		Avaya Aura® SIP device	As applicable	No capability loss, unless there are insufficient button pages and buttons per page.

Station compatibility for Sequential Registration of CTI controlled endpoints in a call center environment

If you are using a CTI application to perform call center-specific operations, you can use the CTI controlled endpoint as a media-only endpoint. You cannot use the endpoint to perform call center-specific operations, even if the endpoint is configured as a call center-capable (CS1K_IPCC) endpoint.

However, if the connection to the CTI application is lost, then depending on the configuration and the endpoint type, you can use the endpoint as either a media-only endpoint or a call center endpoint.

You can use the following types of endpoints with a CTI application:

- Media-only endpoint (CS1K_IP):

  You can use the CTI controlled endpoint for media only if call center-specific features are not required on the endpoint. This is because all call center operations are performed on the CTI application and the endpoint is used for media only. In this case, a station with less capability is acceptable for sequentially registering to this endpoint. Hence, a single call appearance button on the endpoint may suffice.

  However, you cannot perform call center-specific operations from the endpoint in an event when connection to the CTI application is lost.

- Call center endpoint (CS1K_IPCC):

  If you want to perform call center-specific operations on the CTI controlled endpoint in an event when connection to the CTI application is lost, then you must use an endpoint that is capable of providing call center-specific features and configure the station definition accordingly. When connection to the CTI application is lost, you can log in to the phone as a Call Center Elite agent and perform call center-specific operations.

Hence, Avaya recommends that you use a CS1K_IPCC endpoint with a CTI application.

However, if any specific programmable call center button is not available on endpoint, that service will not be available on the endpoint, even if the CTI application provides the service.

For more information, see Supported phone types in an Avaya Aura Call Center Elite environment on page 55.

For more information, see MDA and Sequential Registration support for CTI controlled endpoints on page 540.

Identify endpoints that can be used as CTI controlled media-only endpoints

The following are the recommendations for identifying endpoints that be used as CTI controlled media-only endpoints:

- An endpoint with display capability is recommended, although not necessary.

  An agent can use the display to verify that the media of the current call aligns with the CTI controller requirements.

- The endpoint must have at least one call appearance key that can be used to terminate calls on the endpoint.

- The endpoint must have an additional call appearance to allow basic UC calls, such as 911 calls, when the agent is not logged in to the CTI application and the endpoint is not CTI controlled. The endpoint may have other UC keys that are required for the associated UC feature handling.

The following table provides information about whether the mentioned endpoints types can be used as CTI controlled media-only endpoints:

Endpoint type	Whether usable as CTI controlled media-only endpoint
Analog	You cannot use an analog endpoint as a CTI controlled media-only endpoint.
Digital	You can use a digital endpoint that has display capability as a CTI controlled media-only endpoint. However, a digital endpoint without display capability is not recommended. Digital endpoints do not support any call center-specific features without a call center client acting as the CTI controller. These endpoints provide a speech path with the CTI controller.
UNIStim	In theory, you can use any UNIStim endpoint as a CTI controlled media-only endpoint. While on a call center call, call center agents typically use a PC to perform operations such as retrieving the order details of a customer. Headset capability is needed. Any headset that can connect to the handset jack suffices.

Identify endpoints that can be used as CC endpoints when connection to the CTI application is lost

You can use an endpoint that is capable of providing Call Center Elite agent function as a CC endpoint along with the CTI application.

The endpoint provides media-only capability when connection to the CTI application is proper. However, in the event of a connection failure to the CTI application, the configured call center-specific features are available on the phone when the agent logs in to the phone as a Call Center Elite agent. The agent can then use the phone to perform call center-specific operations.

Call centers may use their own simplified CTI application to interface with AES and send the appropriate messages to Communication Manager, allowing the calls to be presented and accepted at the endpoint. However, the CTI applications typically have no media capability. The endpoint provides the media.

Therefore, when the network and all applications function correctly, the endpoint is used for media only. The network connection between the CTI application and the endpoint permits the CTI controller to exercise control.

However, if connection to the CTI application is lost due to reasons such as network issues or power failure, the CTI control is lost. The endpoint reverts to being a station connected to Communication Manager. All user interface control can be performed from the endpoint.

The following are the recommendations for identifying endpoints that be used as call center endpoints in the event of a connection failure to the CTI application:

- Use a CS1K_IPCC endpoint with a CTI application.

- The station definition must be programmed such that in the event of a CTI application connection failure, the agent can log in to the endpoint as a Call Center Elite agent.

- Communication Manager and Call Center Elite must provide call center capability, including supporting the agent login feature.

- The station must be a Call Center Elite compatible station. The appropriate call center mode and feature buttons must be configured for the endpoint. Ideally, there should be a feature-by-feature alignment, although the user interface of the endpoint and the CTI application may differ.

> ⊛ **Note:**
>
> A CTI controlled call center-capable phone (CS1K_IPCC) can be used to perform call center-specific operations in the event of a connection failure to the CTI application only in a Call Center Elite environment. If you are using a call center application other than Call Center Elite; for example, Avaya Aura® Contact Center, the endpoint can be used only as a media-only endpoint. Hence, Avaya recommends that you use the CS1K_IP station type as CTI controlled endpoint in a call center other than Call Center Elite.

The following table provides information about whether the mentioned endpoints types can be used as CC endpoints in the event of a connection failure to the CTI application in Call Center Elite:

Endpoint type	Whether usable as CC endpoints in case of a CTI application connection failure
Analog	Analog endpoints do not support Call Center Elite functions. Hence, you cannot use analog endpoints as CC endpoints.
Digital	Digital endpoints do not support Call Center Elite functions. Hence, you cannot use digital endpoints as CC endpoints.

Table continues…

Endpoint type	Whether usable as CC endpoints in case of a CTI application connection failure
UNIStim	• CS1K_IP stations: CS1K_IP stations provide limited support for CTI with Sequential Registration. They do not support the necessary handling for call center features in the event of a CTI application connection failure. • CS1K_IPCC stations: You can use the CS1K_IPCC station for CTI with Sequential Registration, provided the station is configured as a Call Center Elite station and the necessary buttons and features are configured.

MDA and Sequential Registration configuration for CTI controlled endpoints

Prerequisites for configuring MDA and Sequential Registration for CTI controlled endpoints

Depending on the configuration, an endpoint can be used as either a CTI controlled media-only endpoint or a CTI controlled call center endpoint. For more information, see Station compatibility for Sequential Registration of CTI controlled endpoints in a call center environment on page 556.

Before you configure MDA or Sequential Registration for CTI controlled endpoints, ensure the following:

- Configure the endpoint as a CTI controlled endpoint.

  For more information, see Configuring an endpoint as a CTI controlled endpoint on page 241.

- The CTI server is configured. This configuration depends on the CC server type. This configuration is not in scope of discussion in this document.

- The CTI flags are correctly set on the endpoint.

- The CTI control is programmed. CTI control programming depends on the type of the CTI controller. For example, Agent Desktop, Equinox, and Workspaces are significantly different. For more information, see the documentation of the respective CTI controller.

Configuring MDA for CTI controlled media-only endpoints

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Click **Users** > **User Management** > **Manage Users**.

3. Select the user, and then click **Edit**.

4. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.

5. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, type the maximum number of devices that can register concurrently.

You can specify a maximum of 10 SIP devices. However, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint.

If the user wants to include two or more Device Adapter UNIStim endpoints, then Avaya recommends that you set the **Max. Simultaneous Devices** field value to 1. This is called Sequential Registration and not MDA.

6. Clear the **Block New Registration When Maximum Registrations Active** check box to allow Session Manager to accept new registration request.

Configuring Sequential Registration for CTI controlled CC endpoints

About this task

Use this procedure to configure Sequential Registration for CTI controlled endpoints that can be used as CC endpoints. In an event when connection to the CTI application is lost, an agent can log in to the phone and use the phone to perform call center-specific operations.

Procedure

1. Log on to System Manager by using the appropriate administrative credentials.

2. Click **Users** > **User Management** > **Manage Users**.

3. Select the user, and then click **Edit**.

4. On the User Profile: Edit: <user name> page, on the **Communication Profile** tab, click **Session Manager Profile**.

5. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, type 1.

6. Clear the **Block New Registration When Maximum Registrations Active** check box to allow Session Manager to accept new registration request.

Selecting the **Block New Registration When Maximum Registrations Active** check box causes a delay in fail over in the event of a network failure.

MDA and Sequential Registration support when using Avaya Expert Client and UNIStim endpoint

Avaya Expert Client and UNIStim endpoint used as UC endpoints in a Call Center Elite environment

Both MDA and Sequential Registration are supported if both Avaya Expert Client and a Device Adapter UNIStim endpoint are used as UC endpoints in a Call Center Elite environment. Ensure that the station definition used for these endpoints is a CS1K_IP station. The Device Adapter UNIStim endpoints cannot assign feature list settings to feature key buttons and do not have a Features list.

The behavior and limitations of MDA and Sequential Registration are the same as those for other Avaya Aura® SIP devices.

Avaya Expert Client and UNIStim endpoint used as CC endpoints in a Call Center Elite environment

Only Sequential Registration is supported if both Avaya Expert Client and a Device Adapter UNIStim endpoint are used as CC endpoints in a Call Center Elite environment. Ensure that the station definition used for these endpoints is a CS1K_IPCC station. The Device Adapter UNIStim endpoints cannot assign feature list settings to feature key buttons and do not have a Features list.

The behavior and limitations of Sequential Registration are the same as those for other Avaya Aura® SIP devices.

Avaya Expert Client and UNIStim endpoint as CTI controlled endpoints in a Call Center Elite environment

When you use both Avaya Expert Client and a Device Adapter UNIStim endpoint in a Call Center Elite environment, only one of these endpoints can be SIP registered at one time. Therefore, the CTI application will control either Avaya Expert Client or the UNIStim endpoint.

The endpoint supports MDA only when it is not registered as a CC endpoint. Device Adapter supports both digital and UNIStim endpoints as CTI controlled endpoints.

CTI controlled UNIStim endpoints support both MDA and Sequential Registration. Therefore, with CTI control, Avaya Expert Client and UNIStim endpoint that are used as UC endpoints can coexist. However, the CTI controller identifies the most recently registered endpoint to perform operations such as answer a call, release a call, and transfer a call. Even with MDA, the CTI controller controls only the most recently registered endpoint, even though both the endpoints are capable of carrying out UC functions.

Device Adapter does not support MDA and Sequential Registration for a digital endpoint. However, you can use the Sequential Registration configuration to provide fail-over support for digital endpoints. For more information, see Sequential Registration fail-over support for analog and digital endpoints on page 537.

Send All Calls

Send All Calls when the presence status is set as DND feature description

You can redirect all calls to a configured extension using Send All Calls (SAC) feature. SAC feature works only if the presence status is set as Do Not Disturb.

Configuring Send All Calls when the presence status is set as DND

About this task

You can redirect all incoming calls to a configured extension when the presence status is set as DND using the Send All Calls (SAC) feature.

Before you begin

Ensure that you have activated DND on your extension.

For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation* and *Administering Avaya Aura® Communication Manager* document.

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the UC endpoint for which you want to configure the SAC feature, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

   a. In another **Button Feature** field, click **send-calls**.

   b. In the corresponding **Extension** field, type the extension number to redirect the calls.

   c. **(Optional)** In the **Button Label** field corresponding to the button number that you want to configure as a SAC feature, type a name for the SAC button label. For example, SendCalls.

      This label appears on the endpoint.

      If you do not specify a label, the default label that appears on the endpoint is **send-calls**.

6. Click **Commit** to save the changes.

Redirecting all calls when the presence status is set as Do Not Disturb

About this task

You can redirect all calls to a configured extension when the presence status is set as DND on your extension using Send All Calls (SAC) feature. Device Adapter does not support a DND presence status.

If you set your status as DND on the Avaya Aura® SIP endpoint and use sequential registration to register on a Device Adapter endpoint. The Device Adapter endpoint can activate or deactivate the Send All Calls (SAC) when the presence status is set as DND feature but the already set presence status (DND in this case) will not change on the Device Adapter endpoint.

If you are registered on a Device Adapter endpoint using sequential registration, then you cannot change your status from DND to active or available from the Device Adapter endpoint. You can change your presence status from the SIP endpoint only. Avaya recommends that you always change your presence status to available before registering to any other endpoint. For more information, see the *Using Avaya 9608/9608G/9611G IP Deskphones SIP* document.

Before you begin

Ensure that:

- You have activated DND on your extension.
- The administrator has programmed **send-calls** on one of the programmable feature keys or on the expansion module.

If you are a call center agent, ensure that you are logged in with your agent ID and agent password, if configured.

For a logged out agent the phone operates as a normal Unified Communications (UC) phone, which does not depend on your login status.

Procedure

1. When you set your status as DND, press **send-calls** key to redirect all calls to a configured extension.

   If the configured destination extension answers the call, an active call is established between you and the configured destination.

   If the called extension is busy then depending on the configuration, the call will either be routed to the voice mail or will not be completed at that time.

2. Press the **Release** button or place the handset on hook to end an active call.

   When you change your status from DND to any other status then SAC feature will be disabled automatically and the active icon of the **send-calls** feature button will no longer be available on the screen.

Send All Calls when the presence status is set as DND feature interaction

Send All Calls feature works only if the presence status is set as DND on the extension. If you deactivate DND from your extension then Send All Calls functionality of this feature will be disabled automatically.

Speed Dial

Speed Dial feature description

The Speed Dial and Speed Call feature names are effectively synonymous in this context.

Speed Call on CS 1000 allows you to place calls by dialing a one-digit, two-digit, or three-digit code. You can use Speed Call for both internal and external calls. To use Speed Call, CS 1000 digital and UNIStim phones must have a Speed Call key/lamp pair.

Analog telephones can activate Speed Call by using the Special Prefix (SPRE) or Flexible Feature Codes (FFC) on the CS 1000.

CS 1000 phones are designated as a Speed Call Controller (SCC) or a Speed Call User (SCU). SCCs can program the numbers to be stored (Speed Call codes) and use the Speed Call list. SCUs do not program Speed Call codes. They only use the Speed Call lists.

Each stored number is assigned a Speed Call code from the Speed Call list. Each list on CS 1000 can contain up to 1000 telephone numbers (entries). The maximum number of digits of the telephone number that can be stored in each entry is specified by the customer. Speed Call entries can be 4, 8, 12, 16, 20, 24, 28, or 31 digits long.

Device Adapter maps the CS 1000 Speed Call to the Communication Manager Abbreviated Dialing list feature. An administrator can configure the abbreviated dialing list as per the requirements of a specific system size. For example, an administrator can configure a small Communication Manager setup to allow a maximum of 12,000 total entries in all abbreviated dialing lists, per system. If the administrator configures 2,400 abbreviated dialing lists, each list can contain a maximum of 5 entries.

- There are four types of Abbreviated Dialing Lists:

  - System: One list exists per Communication Manager, with no more than 100 entries.

    The administrator can define one system list for the entire organization.

    Most administrators assign this list to each telephone and allow everyone in the organization to use the list.

    If the administrator allows everyone to use the system list, the administrator must include only those numbers that anyone in the organization has permission to call. For example, the administrator might want to add an emergency telephone number or telephone numbers of other office locations to this list.

    The system list can contain up to 100 entries and can be changed by a system administrator.

  - Group: Shared among a group of users, with no more than 100 entries.

    The administrator can define group lists for groups or departments where members of the group frequently dial the same numbers. The administrator determines which users have access to group lists.

Each user can access up to three group lists. The administrator can program the list or can designate a user in each group to program the list. The administrator can specify this designated user on the Abbreviated Dialing Group List screen.

- Personal: Up to three lists per station, with no more than 100 entries.

Personal lists are used for users who need their own set of stored numbers. The administrator determines which users have access to a personal list and the size of each list.

A personal list is created automatically when the administrator assigns the list to an individual telephone.

Each user can have as many as three personal lists, depending on whether the user also has access to a system or group list. Either the administrator or the user can assign telephone numbers to personal lists.

- Enhanced: Up to two lists, with no more than 1000 entries.

The administrator can use enhanced lists for users who need more list entries than the number of entries allowed in group-number and system-number lists.

Two enhanced-number lists are allowed per system, in addition to the system-number list. The enhanced list can contain any number or dial-access code.

The administrator creates the enhanced lists and determine which users can access the lists.

- Phones can have access to a maximum of three lists of any type. They are assigned as Abbreviated Dialing List 1, 2, and 3 in the Communication Manager station fields.

- A phone user can program Communication Manager personal lists. Only one dedicated extension is allowed to program a Communication Manager group list. This normally restricts access to a single phone user.

For more information, see "Abbreviated Dialing" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

Based on the SCB / SCK feature mnemonic programmed against the station, Device Adapter presents the **Autodial** Communication Manager feature button to the sets as:

- **Speed Call User** key (SCU)

- **Speed Call Controller** key (SCC)

Only Abbreviated Dialing lists of group type can be programmed by using the SCC button. To program personal lists, use the Program FAC. Refer to sections with analog sets below.

This can be presented as either a soft key on stations supporting the capability, or a programmable feature key, on any station with a programmable feature key available.

Analog sets activate the Abbreviated Dialing feature by using Abbreviated Dialing FACs with no adaptation by Device Adapter. UNIStim and digital sets can also activate the Abbreviated Dialing feature directly by using FACs.

Speed Dial feature administration

The speed call list keys are configured as soft keys on certain station types, or as programmable feature keys. Note that digital and UNIStim stations with soft keys and buttons have a soft key reserved for speed call (23) but may have speed call programmed at other locations. A station may have access up to three available speed call list, although this is less common than having a single list.
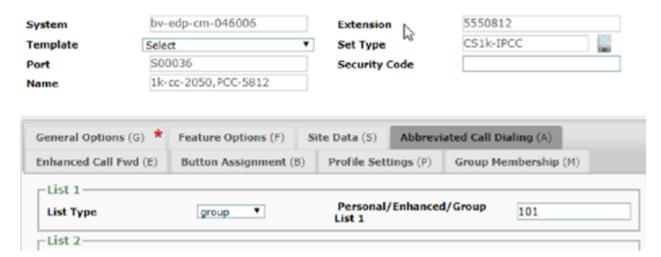
Device Adapter endpoint provisioning on the Communication Manager and System Manager does not assign the capability to key 23. Instead, the provisioning indicates the desired feature mnemonic, and the Device Adapter maps the feature mnemonic used for the soft key to have the soft key enabled.

The mnemonics shown include a parameter x. This is the number 1, 2, or 3 of the Abbreviated list configured in the station. On the other hand, the list number stored as the station's "abbreviated list 1" will be a numeric value as defined in the Communication Manager list creation and can be in triple digits.

For example, the following image shows a group list 101:

```
display abbreviated-dialing group 101
                    ABBREVIATED DIALING LIST


           Group List:    101       Group Name: Sample
      Size (multiple of 5):    15    Program Ext:           Privileged?    n
DIAL CODE
    01: 5550115
    02: 5551114
    03: 5550112
    04: 5551811
    05:
    06:
```

It can be assigned as abbreviated dial list 1 on a station:

Avaya Device Adapter Snap-in Reference

Therefore, in the mnemonic use 1, and not 101.

Program a Soft Key as Speed Call

There is no Module option. Soft keys are always present on the station .

Legend:

- SCKUx:
    - SC: speed call
    - K: key (soft key)
    - U: user
    - X: 1–3 (Abbreviated list 1, 2, or 3)
- SCKCx:
    - SC: speed call
    - K: key (soft key)
    - C: controller
    - X: 1–3 (Abbreviated list 1, 2, or 3)

Configuring Speed Call User for Soft Keys
Procedure

1. Define the Abbreviated Dialing list to be used.

   For the procedure to create the list, see "Abbreviated Dialing" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

2. Define the FAC codes for any list required.

3. Do the following, while creating or changing the station:

   a. Set the Abbreviated Dialing list as station's abbreviated dialing list 1, 2, or 3.

For the procedure to allow a station to use the list, see "Assigning telephones for group lists" in "Chapter 4: Abbreviated Dialing", in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

b. Add the feature mnemonic SCKUx, where x is the abbreviated dial list number (1–3) on the station.

⊛ **Note:**

Unless this is a personal list, the user can only use the list and cannot edit the list.

Configuring Speed Call Controller for Soft Keys

About this task

This procedure is applicable only for group lists. System and enhanced lists require administrator programming. Users can always modify personal lists.

Procedure

1. Define the Abbreviated Dialing group to be used.

   For the procedure to create the list, see "Abbreviated Dialing" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

2. Specify the phone extension as Program Ext in the Abbreviated Dialing group list. Note that only one dedicated extension can program a group list.

```
display abbreviated-dialing group 123
                         ABBREVIATED DIALING LIST


            Group List:    123       Group Name: demo
      Size (multiple of 5):   5      Program Ext:   555-0812
   DIAL CODE
      01: 5550811
      02: 5551114
      03: 5550115
```

3. Define the Abbreviated Dial Prgm_Group_List FAC.

```
change feature-access-codes
                         FEATURE ACCESS CODE (FAC)
      Abbreviated Dialing List1    Access Code: [      ]
      Abbreviated Dialing List2    Access Code: [      ]
      Abbreviated Dialing List3    Access Code: [      ]
   Abbreviated Dial - Prgm Group List    Access Code: [      ]
```

4. Do the following, while creating or changing the station:

    a. Set the Abbreviated Dialing list as the station's abbreviated list 1, 2, or 3.

        For the procedure to allow a station to use the list, see "Assigning telephones for group lists" in "Chapter 4: Abbreviated Dialing", in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

    b. Add the feature mnemonic SCKCx where x is the abbreviated dial list number (1–3) on the station.

        ✱ **Note:**

        This user can both change and use the list. Only one controller can be defined per group abbreviated dial list.

Program a Feature Key as Speed Call

An optional part of the mnemonic describes the device providing the soft key. If the module indicator M is present, either a module 0 indicates the button is on the station itself, or the number indicates the button page on which it is found.

If the module indicator M is not present, the button is on the station and not a module.

Legend:

- SCBbbMmUx:

    - SC: speed call

    - B: feature button

    - bb: button number (00 to max on station or on extension module)

    - M: expansion module, when an expansion module is to provide this button

    - m: module number (1, 2, or 3; optionally, 0 can be used to indicate the actual station)

    - U: user

    - x: 1–3 (Abbreviated list 1, 2, or 3)

- SCBbbUx:

    - The absence of the Mm indicates that this is on the station itself and not a n expansion module

    - SC: speed call

    - B: feature button

    - bb: button number (00 to max on station or on extension module)

    - U: user

    - x: 1–3 (Abbreviated list 1, 2, or 3)

    - Mm is omitted because this button is not on a button module.

- SCBbbMmCx:

  - SC: speed call

  - B: feature button

  - bb: button number (00 to max on station or on extension module)

  - M: expansion module, when an expansion module is to provide this button

  - m: module number (1, 2, or 3; optionally, 0 can be used to indicate the actual station)

  - C: controller

  - x: 1–3 (Abbreviated list 1, 2, or 3)

- SCBbbCx:

  - SC: speed call

  - B: feature button

  - bb: button number (00 to max on station or on extension module)

  - C: controller

  - x: 1–3 (Abbreviated list 1, 2, or 3)

  - Mm is omitted because this button is not on a button module.

Configuring Speed Call User for Feature Keys
Procedure

1. Define the Abbreviated Dialing list to be used.

   For the procedure to create the list, see "Abbreviated Dialing" in the *Avaya Aura®
   Communication Manager Feature Description and Implementation* guide.

2. Define the FAC codes for any list required.

3. Do the following, while creating or changing the station:

   a. Set the Abbreviated Dialing list as the station's abbreviated dialing list 1, 2, or 3.

      For the procedure to allow a station to use the list, see "Assigning telephones for
      group lists" in "Chapter 4: Abbreviated Dialing", in the *Avaya Aura® Communication
      Manager Feature Description and Implementation* guide.

   b. Add the feature mnemonic SCBbbMmUx or SCBbbUx, where:

      - bb is the button (entered as two digits; 08 and not 8).

      - Mm is the expansion module number. This is not needed when the button is on the
        station, which is why the SCBbbUx mnemonic exists.

      - U indicates a user.

      - x is the abbreviated dial list number (1-3) on the station.

> ⊛ **Note:**
>
> Unless this is a personal list, the user can only use the list and cannot edit the list.

   c. Add an autodial button feature.

Configuring Speed Call Controller for Feature Keys
Procedure

1. Define the Abbreviated Dialing group list to be used.

   For the procedure to create the list, see "Abbreviated Dialing" in the *Avaya Aura®
   Communication Manager Feature Description and Implementation* guide.

2. Specify the phone extension as Program Ext in the Abbreviated Dialing group list. Note
   that only one dedicated extension can program a group list.

```
display abbreviated-dialing group 123
                    ABBREVIATED  DIALING  LIST


              Group List:    123        Group Name:  demo
        Size (multiple of 5):    5      Program Ext:   555-0812
 DIAL CODE
        01:  5550811
        02:  5551114
        03:  5550115
```

3. Define the Abbreviated Dial Prgm_Group_List FAC.

```
change feature-access-codes
                           FEATURE  ACCESS  CODE  (FAC)
       Abbreviated  Dialing  List1    Access  Code:  [    ]
       Abbreviated  Dialing  List2    Access  Code:  [    ]
       Abbreviated  Dialing  List3    Access  Code:  [    ]
  Abbreviated  Dial  -  Prgm  Group  List    Access  Code:  [    ]
```

4. Do the following, while creating or changing the station:

   a. Set the Abbreviated Dialing list as the station's abbreviated dialing list 1, 2, or 3.

      For the procedure to allow a station to use the list, see "Assigning telephones for
      group lists" in "Chapter 4: Abbreviated Dialing", in the *Avaya Aura® Communication
      Manager Feature Description and Implementation* guide.

   b. Add the feature mnemonic SCBbbMmCx or SCBbbCx, where:

      • bb is the button (entered as two digits; 08 and not 8).

- Mm is the expansion module number. This is not needed when the button is on the station, which is why the SCBbbCx mnemonic exists.
- C indicates a controller.
- x is the abbreviated dial list number (1-3) on the station.

> ✳ **Note:**
>
> This user can both change and use the list. Only one controller can be defined per group abbreviated dial list.

c. Add an autodial button feature.

Programming Analog Station Speed Call User

About this task

There are no buttons for analog stations. Hence, these stations can only use FAC codes.

Procedure

1. Define the Abbreviated Dialing list to be used.

   For the procedure to create the list, see "Abbreviated Dialing" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

2. Define the FAC codes for any list required.

3. While creating or changing the station, set the Abbreviated Dialing list as the station's abbreviated dialing list 1, 2, or 3.

   For the procedure to allow a station to use the list, see "Assigning telephones for group lists" in "Chapter 4: Abbreviated Dialing", in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

   The user can only use the list and cannot edit the list.

Programming analog station Speed Call Controller

About this task

Analog sets do not have buttons. Hence, access the Abbreviated Dialing programming feature by using FAC codes.

Procedure

1. Define the Abbreviated Dialing list to be used.

   For the procedure to create the list, see "Abbreviated Dialing" in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

2. Specify the phone extension as Program Ext in the Abbreviated Dialing group list. Note that only one dedicated extension can program a group list.

3. Define the Abbreviated Dial Prgm_Group_List FAC.

4. While creating or changing the station, set the Abbreviated Dialing list as the station's abbreviated dialing list 1, 2, or 3.:

For the procedure to allow a station to use the list, see "Assigning telephones for group lists" in "Chapter 4: Abbreviated Dialing", in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

> **✱ Note:**
>
> The user can both change and use the list. Only one controller can be defined per group abbreviated dial list.

Speed Dial feature operation

The speed call user and speed call controller can both be used to place calls using the list.

When the user activates either an **SCU** key or soft-key or an **SCC** key or soft-key, the Device Adapter handles all operations until sufficient information has been entered to make the call attempt.

Following noticeable user experience changes can be observed :

- Pressing the **speed call user** button does not reset the dial tone timeout. That is, if a user goes offhook, waits for 7 seconds, and presses the **SCU**, the call will expire in 2 seconds. This is not the case for CS 1000.

- If the user enters a wrong or not configured entry, an audible tone is played by AMS while the screen remains in the active call state. In CS 1000, reorder tone with **Release and try again** screen is given.

Using speed dial on digital and UNIStim phones
Procedure

1. The user goes off hook or selects a line appearance.

2. The user presses the **speed call user** or **speed call controller** button or soft key.

3. In **response to the request (dial tone)** at the prompt, the user must enter the two-digit list entry number (01, 02, 03, .., 10, ..), except for the following:

   - For personal list that contains up to 10 entries, the user must enter the one-digit list entry number (1#, 2#, ..., 0# equals to 10).

   - For enhanced list, the user must enter the three-digit list entry number.

4. Based on dial tone, Device Adapter originates an outgoing call (as if the **autodial** button is used) with the dialed list information to allow Communication Manager to call the number:

   - FAC for the abbreviated dialing list 1, 2, or 3, based on the list indicated with the feature mnemonic: SCBbbUn, SCKUn, SCBbbCn, or SCKCn, where n is the list number 1, 2, or 3.

   - The one, two or three digits for the entry in the list, as provided by the user.

Using speed dial on analog phones

Procedure

1. The user goes off hook.

2. The user enters the FAC for the abbreviated dialing list 1, 2, or 3.

3. In **response to the request (dial tone)** at the prompt, the user must enter the two-digit list entry number (01, 02, 03, .., 10, ..), except for the following:

   • For personal list that contains up to 10 entries, the user must enter the one-digit list entry number (1#, 2#, ..., 0# equals to 10).

   • For enhanced list, the user must enter the three-digit list entry number.

4. Based on dial tone, the Device Adapter originates an outgoing call (as if the **autodial** button is used) with the dialed list information to allow the Communication Manager to call the number:

   • FAC for the abbreviated dialing list 1, 2, or 3.

   • The one, two or three digits for the entry in the list, as provided by the user.

Modify the Speed Call List

When the user activates an **SCC** key or soft-key, it is up to the Device Adapter to determine whether this is for programing or calling purposes. If done without selecting a line appearance, this is intended for programming. Otherwise, the user wants to use the list.

Speed dial programming requires the use of a call appearance to make a "programming" call. If no free **call appearance** button is available, the programming fails. It also means the programming can fail due to other call related reason.

Changing the Group Lists on digital and UNIStim phones

Procedure

1. The user presses the **SCC** key or soft key while on-hook (i.e. in the "Idle" state); Device Adapter assumes the controller/programing mode. Dial tone is provided.

2. The user enters the 2-digit list entry number. Dial tone is provided.

3. The user enters the target number to be used to program the entry.

4. The user presses the **SCC** key.

Result

Device Adapter originates an outgoing call (as if the **autodial** button has been used) with the following dialed number:

• Starting with FAC for "Abbreviated Dial - Prgm Group List".

• Followed by the 4-digit list number - the list number is indicated in the associated feature mnemonic (SCBbbCl or SCKCl) and the station settings.

• Followed by the 2-digit list entry number - as entered by the user.

• Followed by the target number - as entered by the user.

The list is programmed and the user gets confirmation.

Changing Group list on analog phones

Procedure

1. The user goes off hook. Dial tone is presented.
2. The user dials the FAC for "Abbreviated Dial - Prgm Group List".
3. The user enters the 4-digit list number.
4. The user enters the 2-digit list entry number.
5. The user enters the target number to be used to program the entry.
6. The user enters #.
7. The user goes on hook.

Changing Personal list on analog phones

About this task

The user is the only party using this list; therefore, he or she only needs to know whether this is a personal list associated with the "list 1", "list 2", or "list 3" on the user's station. Group lists can only be changed if this user is the group list controller, and the system and enhanced lists are controlled by the administrator.

Procedure

1. The user goes off hook. Dial tone is presented.
2. User dials the "Program Access Code" FAC.
3. User dials the '1' or '2' or '3' that corresponds to Personal list #1, #2 or #3 to program.
4. User dials the 1-digit list entry code (Personal list consists of max 10 entries).
5. User dials the target number to be used to program the entry.
6. User dials the **#**.
7. On-hook.

Speed Dial feature interaction

Speed call dialing by FAC is NOT supported on phones which do not support RFC2833, such as the 2050v2, or 2004 phase 0 and phase 1 stations.

Programming the abbreviated dialing list by FAC is not supported on phones which do not support RFC2833, such as the 2050v2, or 2004 phase 0 and phase 1 stations.

Speed call dialing requires Avaya Aura® Media Server to collect the dialed entry code.

Refer to Communication Manager documentation for possible interactions on the Communication Manager.

Transfer — blind or consultative

Transfer — blind or consultative feature description

In both the CS 1000 and the Communication Manager, transfer is implemented by placing an existing call on hold, seizing a new appearance, dialing to the target destination, and then either completing the transfer while ringing (blind transfer), or completing the transfer after the destination answers (consultative transfer).

Digital and IP endpoints usually request and complete transfer using a dedicated button to request the transfer. Analog endpoints, which do not have the button, request the transfer by using a hook flash to put the current call on hold and request a new line, and typically by hanging up the call to complete the transfer. This model is not used for CS 1000 digital or UNIStim stations, and will not be supported for these stations on the Device Adapter.

CS 1000 endpoint user experience for UNIStim and Digital Stations

Call transfer is made using a transfer feature key (TRN) which is predefined for UNIStim and 39XX endpoints as a soft key at a fixed position, but may be disabled (removing transfer capability). For digital 200X endpoints the button may be defined at an unfixed programmable position.

The Transfer soft key is available only on the phone screen during an active call. For digital 200X stations, the button is always present, but it does not function unless there is a call. In practice, it is present, but behaves as though it was not there until an active call exists on the station.

The active call may be on any line appearance (both the user's extension and any auxiliary or shared numbers programmed on the station). On activation of the transfer key, the active call is put on hold, and the user receives a new dial tone when it is pressed. After the far-end is reached, the user can either complete the transfer (blind) or wait until the far-end answers the call and then complete the transfer (consultative). The transfer completion is done by pressing the Transfer key again.

The transfer call is made on behalf of an active DN key. For example, phone A has a primary DN 2000 on key 0, DN 2001 on key 1. When there is an active call with key 1, the user initiates a transfer to another set B. Set B rings and displays DN 2001 as the caller number, not the primary DN of set A.

A transfer using the conference function is also available. The user creates a conference and hangs up.

CS 1000 endpoint user experience for Analog Stations

Call transfer is made by using a hook flash and subsequent operations.

The analog station requires the transfer class-of-service to be permitted because there is no button to program with the transfer function. The absence of the button does not indicate that transfer is denied.

The transfer service automatically allows three-party conference. On CS 1000, it is necessary to add a class-of-service to permit a six-party conference.

The Transfer function is available only during an active call. The call may be an existing conference, when six-party conferencing is allowed.

When the user does a switch hook flash, the active call, including conferences that are below the maximum size for an ad hoc conference, is put on hold. The user receives a new dial tone and can dial the transfer target number.

After the far-end is reached, the user can either complete the transfer (blind) or wait until the far-end answers the call, and then complete the transfer (consultative). The transfer completion is done by hanging up.

Transfer can be cancelled by doing the switch hook flash while the call is ringing.

Communication Manager endpoint user experience

The corresponding transfer operation for Communication Manager is the "Pull Transfer". The Communication Manager documentation description begins as follows: "With Pull Transfer, either the transferring party or the transferred-to party can press the Transfer button to complete the transfer operation."

What button is used depends on the endpoint. It may be a soft key, or a fixed button. However, from the user experience, the mode used by the CS 1000 user has an almost exact match in Communication Manager. Note, though, that additional supplementary options vary; a large overlap exists, but some elements are not identical.

It should be noted that the H.323 endpoints on Communication Manager have an even closer correlation than the 96x1 and J-series SIP stations. As with the CS 1000, the transfer key "hides" a virtual call appearance underneath the transfer button. Pressing the button simultaneously requests the "spare" call appearance and requests the transfer service. SIP endpoints may do this if configured to do so. However, the call may also be put on hold, a new line appearance selected, and the transfer initiated at that point.

Transfer — blind or consultative feature administration

The classes on the analog stations are XFA/XFD:

- XFA – Transfer Allowed: The user can initiate transfer in the manner appropriate for the endpoint.

- XFD – Transfer Denied: The user cannot request a transfer. This class is superfluous in Device Adapter, as absence of permission to transfer is the same as forbidding it.

When the migration detects the XFA class-of-service, the tools automatically assign the analog station a conference button at position 18. This virtual button is used as the basis for the SIP signaling during the feature activation. If needed, this button can be manually added in the features buttons for the CS1k-ana station by using System Manager or Communication Manager to carry out the configuration.

The class-of-service is not propagated to Device Adapter. The presence or absence of the conference button suffices.

Digital and UNIStim endpoints require the Transfer button or soft key to be programmed. Soft keys have a fixed location as position 17. The UNIStim and digital 200X station programmable buttons do not. Note that 3901 has the feature assigned to a button at position 1 to 4, but the user presses the feature button and enters the digit aligning to the button. The 3902 stations must have either conference or transfer configured at position 4 and cannot assign it elsewhere. This is also done

on the System Manager or the Communication Manager configuration pages, but the type of station must be the appropriate station family: CS1k-IP, CS1k-39xx, CS1k-1col or CS1k-2col.

Transfer — blind or consultative feature operation for UNIStim and Digital Stations

About this task

Device Adapter will treat this button as a CS 1000 Transfer key with existing localization. Both consultative and blind (transfer a ringing call) transfers are supported.

The CS 1000 end user behavior is retained with following differences:

- When a user presses the Transfer or Conference key during an active call, a simple dial tone is given as opposed to a special stuttered dial tone as in CS 1000.

- A consultative call is made using the Transfer or Conference key which provides an outgoing call appearance. That means the far end will always see the phone extension as CLID.

  This differs from the CS 1000 behavior where a consultative call is made on behalf of the DN key of the original call. This should be taken into consideration when making an original call from a bridged appearance:

Procedure

1. Set A key 0 - brdg-app to Set B.

2. Set A calls Set C from key 0. Set C sees extension of Set B.

3. Set A presses Transfer and calls Set D. Set D sees extension of Set A, not Set B.

Transferring a call from UNIStim and digital phones by using the Transfer feature

Procedure

1. The user is on an active call.

2. The user decides to carry out a transfer.

3. The user presses the transfer button.

   a. The original party is placed on hold, and the lamp beside the line appearance button flashes.

   b. Dial tone is provided to the user doing the transfer.

4. The user dials the destination. The destination rings.

5. To carry out a blind transfer the user presses the transfer button again while the call is still ringing. The transfer completes on ringing.

6. To carry out a consultative transfer the user presses the transfer button again after the transfer target answers. The transfer completes after a brief consultation call.

Transferring a call from UNIStim and digital phones by using the Conference feature

Procedure

1. The user is on an active call.

2. The user decides to create a conference (typically knowing that he or she will drop out shortly, changing the conference to a transfer).

3. The user creates a conference. For more information, see Conference (Ad hoc conference) on page 456.

4. To complete the transfer the user drops out of the call.

   To cancel a transfer and return to the original call, the user presses the line appearance button beside the flashing lamp. The call attempt aborts and the user rejoins the original call.

Transfer blind or consultative feature operation for Analog Stations

Device Adapter ignores the hook flash when the conference button is not configured in the station definition.

Both consultative and blind (transfer a ringing call) transfers are supported.

CS 1000 end-user behavior is retained with following differences:

- There is no six-party conference differentiation. Rather than a default three-party conference that can be service changed to allow up to six, all users with the capability allow a six-party conference.

Transferring a call from analog phones

Procedure

1. The user is on an active call.

2. The user decides to carry out a transfer.

3. The user does a switch hook flash.

   a. The original party is placed on hold.

   b. Dial tone is provided to the user doing the transfer.

4. The user dials the destination. The destination rings.

5. To carry out a blind transfer the user hangs up while the call is still ringing. The transfer completes on ringing.

6. To carry out a consultative transfer the user hangs up after the transfer target answers. The transfer completes after a brief consultation call.

Transferring a call from analog phones by using the Conference feature
Procedure

1. The user is on an active call.

2. The user decides to create a conference (typically knowing that he or she will drop out shortly, changing the conference to a transfer).

3. The user creates a conference. For more information, see [Conference (Ad hoc conference)](#) on page 456.

4. To complete the transfer the user drops out of the call.

   To cancel a transfer and return to the original call, the user does a switch hook flash while the call is ringing. The call attempt aborts and the user rejoins the original call.

Transfer — blind or consultative feature interaction

No specific interactions are identified based on the Device Adapter. However, interactions between the call transfer on the Communication Manager and other services there are described in the Communication Manager documentation are identified.

Virtual Office

Virtual Office feature description

Device Adapter supports Virtual Office (VO) only for UNIStim endpoints with the following terminologies:

• Home set: The home set is the default set that is programmed with the user identity. However, logging in by MDA and Sequential Registration might change the home user identity.

• Guest set: The guest set is used to log in using the home user identity.

• Home button: The home button is a soft key used to regain the programmed identity of the set.

• Virtual button: The virtual button is used to change the current station identity to another.

With the Virtual Office (VO) feature functionality on CS 1000, you can log in to the phone that is configured to support VO on a different Communication Server (CS) on the network by using a user ID and password. The user ID can be one of the following:

• A local DN for Terminal Number (TN) on the same CS.

• A complex number, if TN exists on another CS.

- Coordinated Dial Plan (CDP) number: CDP is a private network dial plan that is used within a local cluster of CS 1000 servers.
- Uniform Dial Plan (UDP) number: UDP is a private network enterprise canonical dial plan that expands the CDP local network to a global network with multiple local networks. A global network can make calls between local networks using the private dial plan.
- Transferable DN (AC + HLOC + DN): UDP number with the network prefix added to it. Network prefix is the numbering plan access code.

When you log in to the virtual office at a guest station, the endpoint takes over the identity of the home station, which means that the endpoint logs out from the local station. When you log out from the guest station, the endpoint reverts to its original identity.

> ✱ **Note:**
>
> - Terminal Number (TN) is a unique hardware ID for a phone that is registered with Device Adapter, which means that there is a unique TN available per ADA node.
> - Virtual Office also supports Emergency Dialing.

Virtual Office functionality for UNIStim phones on Device Adapter

Device Adapter provides the following functionality of Virtual Office feature for UNIStim phones:

- Supports station configuration by allowing you to log in by using VO credentials at the guest station. When you log in at the guest station by using a virtual key, the station using the user identity at that time (that is either home station or another VO guest station) logs out. You must press the Home key to log into the home station again. Pressing the Home key logs you out of the current guest station.
- Uses SIP handle plus SIP domain as user ID.
- Supports home station configuration by allowing you to log in by using VO credentials at the home station.
- Supports normal functionality of a station when you log in by using VO credentials and a normal user presses the Home key.
- Supports login using alphanumeric characters.

Virtual Office, Sequential Registration, and Multi-device access features comparison

In MDA and Sequential Registration features, change of registered user requires a TN change. For example, you are logged into a set as TN xxx xx xx xx. Another user does an MDA or Sequential Registration login on the same set as TN yyy yy yy yy. If you log out and try to register again on the same set, then the set will not return to its original identity, that is TN xxx xx xx xx. But, the set will register as the changed TN yyy yy yy yy.

In case of Virtual Office, you can program certain user devices to act as a home device. This device corresponds to the device on which the user initially logged in to, assuming the user carries out Sequential Registration. The VO feature works as follows:

- The VO user initially uses the home device as per Sequential Registration.
- The user logs in at a guest device using the login identity and not the TN, which is used for Sequential Registration. The guest device takes the home device identity.
- The original device is VO logged out. To return to the original home device identity, user presses the Home soft key.

- If user exits the home device or performs some action to return to the home device or does VO login on any other device, the guest device will regain its original identity.

The following are the limitations of Virtual Office in Device Adapter:

- If during the registration process the home station and guest station have different TN (hardware port ID) but same hardware device ID, then registration fails.

- If during the registration process the home station and guest station have the same TN but different hardware ID, then VO works as Sequential Registration.

- If the request comes from the same Avaya Breeze® platform, then the oldest registration gets unregistered by the cluster and the latest one gets registered.

- If the request comes from different Avaya Breeze® platform nodes, then the setting for **Max Simultaneous User** and the **Block new registrations** on the Session Manager determines the configuration.

Migration of Virtual Office related CoS values and attributes using ProVision tool

Use the ProVision tool to migrate Virtual Office Login Allowed (VOLA) and Virtual Office User Allowed (VOUA) CoS values of TN block of CS1k–IP endpoint to the feature mnemonics of Communication Manager endpoint.

You cannot use ProVision tool to migrate the VOLO attributes, **TN range for emergency calls from Logged out sets** and **SIP domain for emergency calls from Logged out sets**. You must configure them manually.

Prerequisites for Virtual Office

For VO configuration, you must configure entity links between all Avaya Breeze® platform and Session Managers. You must configure the station to support either or both of the following:

- VO home phone function

- VO guest home function

⊛ **Note:**

A station can work as both home phone and a guest phone, but only one function can be active at a time. That is, if a user is using the home phone and walks away, another user can use the phone as a guest phone. Also, a home phone with the virtual soft key that is logged out by a remote user can also use the virtual key to log in as a guest phone.

You must have one or both of the following Class of Service attributes for the Virtual Office feature configuration in the station features list for home and guest phone:

- VO Login Allowed (VOLA): If VOLA is programmed as a feature on a station, then you can use the station as a home phone as well as other stations can also log in to this station. If VOLA is not programmed, then login to the station from a guest phone is denied. Note that, using VOLA does not mean that the station can be used as a guest phone. If VOLA is not available, then VO Login will be denied.

- VO User Allowed (VOUA): If VOUA is programmed as a feature on a station, then you can use the station as a guest station only and it cannot use VO credentials to login at any other station. If VOUA is not available, then VO user will be denied.

Prerequisites for making emergency calls from a VO logged out device

- A VO logged device will not have any assigned user, as another device will be using the user identity. As a result, any VO logged out phone can attempt an emergency call without user authentication.

- For making emergency calls such as 911,112 and so on without any user authentication, ensure that you have selected the **Allow Unauthenticated Emergency Calls** check box on Session Manager.

- For making emergency calls from a VO logged out phone, both **TN range for emergency calls from Logged out sets** and **SIP domain for emergency calls from Logged out sets** attributes in **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes** must be defined in System Manager.

- Administrators must confirm that the configuration is correct. The correct configuration should allow the logged out phone to make an emergency call to PSAP. This includes at least one successful test call.

VO DVLA timer
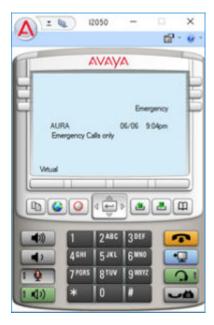
A DVLA phone using the Virtual Office (VO) functionality either returns to the idle state when there is no active call on a DVLA phone with a VO login, or the phone user have not pressed any buttons on the phone. When the phone returns to the DVLA state, it re-registers.

At the same time, re-registration does not happen if the DVLA set does not use VO login operation or performs VO login operation but the user of the set actively works on the logged in set.

For example, if a user on a DVLA phone with VO login makes a call and does not perform any further actions during the configured DVLA idle time interval, then the timeout is not applied to the phone as the phone is still in the call and not inactive.

To invoke the Emergency calls feature, a user should register an IP phone with a TN from the DVLA TN range defined in System Manager. Emergency domain must be configured in the System Manager. The **Emergency** button is now displayed on the phone screen.

The following is an example of an emergency call display if the emergency domain is configured in System Manager:

The following is an example where the emergency call button is not available as the emergency domain is not configured in System Manager:

DVLA logout timer

The VO session should be ended for DVLA phones for a configured period by Device Adapter. When the DVLA logout timer expires, the device adapter displays the message to logout. In case you do not act upon or select Yes, then the system logs out. If you select No, the system restarts the logout timer.

DVLA timer reset

The timer can be reset by performing one of the following actions:

- Pressing a button
- Active call

⊛ **Note:**

The timer restarts after the active call is dropped.

Difference between VOLO and DVLA phones

When a Unistim phone unregisters, it gets a VOLO TN to make emergency calls. A phone is unregistered because of the following two reasons:

- When another phone tries to log in to its TN, or
- When another phone VO logs in to its account.

Unregistered (VOLO) phones can use Virtual Office login feature to log in to another phone. A VOLO phone user can press the appropriate key to request the phone to register again to its TN and continue to work as a regular Unistim phone.

However, DVLA phones are not designed to make calls similar to that of a normal phone. They can only be used to VO login to other phones. Also, emergency calls can be made from DVLA phones.

Configuring Virtual Office support for Device Adapter UNIStim endpoint

Before you begin

Device Adapter requires the following class of service attributes to configure Virtual Office feature:

- Virtual Office Login Allowed (VOLA)
- Virtual Office User Allowed (VOUA)

Procedure

1. Do one of the following:

   - Configure the CS1K-IP station in Communication Manager. For more information, see Communication Manager documentation.

   - Do the following to configure the CS1K-IP station in System Manager:

      a. Log in to System Manager by using the appropriate administrative credentials.

      b. Click **Users** > **User Management** > **Manage Users**.

      c. Select the user, and then click **Edit**.

      d. On the User Profile: Edit: <user name> page, click **Communication Profile** tab and then click **Session Manager Profile**.

      e. In the **SIP Registration** area, in the **Max. Simultaneous Devices** field, click **1**.

      f. Clear the **Block New Registration When Maximum Registrations Active** check box.

      g. Click **Commit**.

2. Configure the applicable CoS from VOLA/VOUA for the Device Adapter. For more information, see [CS 1000 CoS and Avaya Aura feature field mapping](#) on page 322.

3. Do the following to configure the **Idle time interval for DVLA set** field for the DVLA phones:

      a. In the **Idle time interval for DVLA set** field, enter a time interval which defines maximum time for DVLA phones.

      This attribute can be set to values ranging from 1 to 1440 minutes in one of the following formats:

        • Minutes. For example, 5 or 5m.

        • Hours and minutes. For example, 5h 5m.

        • Hours. For example, 5h.

      By default, the value is 0 because this function is considered to be turned off.

      The following error message is displayed when a user tries to set any other non-numeric value:

```
"Service Globals : The attribute Idle time interval for DVLA
set does not contain a valid value based on the attribute type.
Please correct the entry.".
```

      There are no additional logs for tracking incorrectly entered data, as this happens on the Session Manager side and when entering incorrect data, no messages are sent to the Device Adapter side.

      b. Click **Commit**.

Virtual Office with two or more Device Adapter UNIStim endpoints feature operation

About this task

For example, a user has following three endpoints:

- Endpoint device A: SIP registered device with extension number 2000401, TN 100 0 1 2, and user login name alice@mynet.com.

- Endpoint device B: SIP registered device with extension number 2000501, TN 104 0 1 5, and user login name bob@mynet.com.

- Endpoint device C: SIP registered device with extension number 2000502, TN 108 0 1 18, and user login name carol@mynet.com.

The Home soft key is present only on the logged out sets.

Procedure

1. The User performs Virtual Login at device B to device A that is the user presses Virtual soft key on device B and enters the User ID and password of device A. The status of the endpoint devices will be as follows:

   • Endpoint device A: Logged out from the registered extension number and user name. Device A still stores TN 100 0 1 2 as Home TN that the user entered manually during device registration, but this Home TN is not registered on device A.

   • Endpoint device B: Device is registered with extension number 2000401 and takes device A identity that is TN 100 0 1 2. Device B still stores TN 104 0 1 5 as Home TN that the user entered manually during device registration, but this Home TN is not registered on device B.

   • Endpoint device C: SIP registered device with extension number 2000502, TN 108 0 1 18, and user login name carol@mynet.com.

2. The User performs Virtual Login at device C to device A that is the user presses Virtual soft key on device C and enters the User ID and password of device A. The status of the endpoint devices will be as follows:

   • Endpoint device A: Logged out from the registered extension number and user name. Device A still stores TN 100 0 1 2 as Home TN that the user entered manually during device registration, but this Home TN is not registered on device A. Whenever device B logs out by the login at device C, device A must not revert to its original identity. Therefore, manual login using the Home soft key is mandatory.

   • Endpoint device B: Device reverts to its original identity and register itself with the extension number 2000501 and TN 104 0 1 5.

   • Endpoint device C: Device is registered with extension number 2000401 and TN 100 0 1 2. Device C still stores TN 108 0 1 18 as Home TN that the user entered manually during device registration, but this Home TN is not registered on device C.

3. The user presses Home soft key on device A. The status of the endpoint devices will be as follows:

   • Endpoint device A: SIP registered device with extension number 2000401, TN 100 0 1 2, and user login name alice@mynet.com.

   • Endpoint device B: SIP registered device with extension number 2000501, TN 104 0 1 5, and user login name bob@mynet.com.

   • Endpoint device C: SIP registered device with extension number 2000502, TN 108 0 1 18, and user login name carol@mynet.com.

Virtual Office feature interaction

Interaction between VO, Sequential Registration, and MDA

- Identity Recovery:

  You can recover and register to the original identity of the guest device endpoint only if you log in as the new identity by VO (that is by login identity). You can log out either by VO or Sequential Registration.

  If you log in by Sequential Registration (that is by TN or hardware port ID) and log out by either VO or Sequential Registration, the endpoint does not recover its original identity. Sequential Registration changes and stores the TN for later use.

- Reboot:

  A set logged out using MDA, Sequential Registration, or VO, regain its login identity after reboot. That means, the set registers itself using the home TN which was manually entered in the set during registration.

Configuring Session Manager to make emergency calls from a VO logged out phone

About this task

A VO logged out phone can perform the following functions:

- Make emergency calls.

- Use the functionality provided by the Virtual key.

- Return to the previously occupied TN during registration.

You must configure Session Manager with the following changes to make a successful emergency call.

Before you begin

Do the following to let a logged out VO set to make emergency calls such as 911 and 112:

- You must select **Allow Unauthenticated Emergency Calls** check box on Session Manager. If the **Allow Unauthenticated Emergency Calls** check box is clear, then all the emergency calls for phones in the VO logged out state is rejected by the Session Manager.

- You must define system resources on the Device Adapter clusters to provide Virtual Office Logged Out (VOLO) TNs.

- Before configuring the VOLO TN attribute, you must identify a continuous range of unassigned TNs. A VOLO TN must not be a TN already assigned to a Device Adapter endpoint.

Procedure

1. Configure PSAP for the VO logged out phones to test the emergency calls.

2. Log in to System Manager by using administrative credentials.

3. Navigate to **Elements** > **Session Manager** > **Global Settings**.

4. Select the **Allow Unauthenticated Emergency Calls** check box, and click **Commit**.

5. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

6. Click the **Service Clusters** tab.

7. In the **Cluster** field, click the appropriate application cluster.

8. In the **Service** field, click **DeviceAdapter**.

9. Navigate to the **Virtual Office/Emergency Calls** section and do the following:

    a. In the **TN range for emergency calls from Logged out sets** field, enter the TN range for logged out sets.

    The format of TN range is lll-ss-cc-uu:lll-ss-cc-uu, where:

    - "lll" is a multiple of 4.

    - "ss" is 00 or 01.

    - "cc" is 00 to 15.

    - "uu" is 00 to 31.

    - ":" is the delimiter between the lowest and highest TN in the range. For example, 112-00-00-00:112-00-03-31 allocates 4 blocks of 32 instances, for 128 emergency call TNs.

    b. In the **SIP domain for emergency calls from Logged out sets** field, enter the SIP domain.

    The VO logged out phone uses:

    - VOLO TN range to take free VOLO TN from the assigned range.

    - SIP domain to form an anonymous SIP handle during an emergency call.

    c. Click **Commit**.

10. Make at least one successful test call from a VO logged out phone. Confirm that the information is as expected at the PSAP.

Configuring Session Manager to make emergency calls from a DVLA phone

About this task

A DVLA phone can perform the following functions:

- Make emergency calls.

- Use the functionality provided by the Virtual key.

You must configure Session Manager with the following changes to make a successful emergency call.

Before you begin

Do the following to let a default VO logged out set to make emergency calls such as 911 and 112:

- You must select **Allow Unauthenticated Emergency Calls** check box on Session Manager. If the **Allow Unauthenticated Emergency Calls** check box is clear, then all the emergency calls for phones in the DVLA state is rejected by the Session Manager.
- You must define system resources on the Device Adapter clusters to provide Default VO Logged Out (DVLA) TNs.
- Before configuring the DVLA TN attribute, you must identify a continuous range of unassigned TNs. A DVLA TN must not be a TN already assigned to a Device Adapter endpoint.

Procedure

1. Configure PSAP for the default VO logged out phones to test the emergency calls.
2. Log in to System Manager by using administrative credentials.
3. Navigate to **Elements** > **Session Manager** > **Global Settings**.
4. Select the **Allow Unauthenticated Emergency Calls** check box, and click **Commit**.
5. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
6. Click the **Service Clusters** tab.
7. In the **Cluster** field, click the appropriate application cluster.
8. In the **Service** field, click **DeviceAdapter**.
9. Navigate to the **Virtual Office/Emergency Calls** section and do the following:

   a. In the **TN range for DVLA sets** field, enter the TN range for DVLA sets.

      The format of TN range is lll-ss-cc-uu:lll-ss-cc-uu, where:

      - "lll" is a multiple of 4.
      - "ss" is 00 or 01.
      - "cc" is 00 to 15.
      - "uu" is 00 to 31.
      - ":" is the delimiter between the lowest and highest TN in the range. For example, 112-00-00-00:112-00-03-31 allocates 4 blocks of 32 instances, for 128 emergency call TNs.

      The following error message is displayed when a user tries to set a value different from the above format:

      ```
      "Service Globals : The attribute TN range for DVLA sets does
      not contain a valid value based on the attribute type. Please
      correct the entry.".
      ```

    b. Click **Commit**.

10. Make at least one successful test call from a default VO logged out phone. Confirm that the information is as expected at the PSAP.

Dialing an emergency number from a VO logged out phone

About this task

You can dial an emergency number from a Virtual Office phone when the user is not logged in.

Before you begin

You must program all emergency numbers on Communication Manager. For more information about configuring emergency number in the system, refer the Communication Manager documentation.

✱ **Note:**

Depending on the jurisdiction, you might need to define more than one emergency number. For example, many North American jurisdictions have 9-1-1 for emergencies requiring police, fire services, or ambulances, but support 2-1-1 for mental health or emergency housing.

Procedure

1. Press the Emergency feature key or go off hook.

   Going off hook will automatically activate the Emergency feature key.

2. Listen for a dial tone.

3. Dial the appropriate emergency number configured at the station for the specific jurisdiction. For example, 911 for America, 999 and 112 for United Kingdom.

4. Device Adapter analyzes the dialed digits against the dial plan in the same way that it does for Avaya Aura® SIP phones.

5. When a match is found (digit pattern plus correct number of expected digits, where the minimum and maximum number of digits is the same):

   a. Device Adapter initiates the call with Session Manager and Communication Manager.

   b. The emergency call progresses with the SIP call handling procedure.

   c. If the call fails at this point:

      • Appropriate messages and tones are provided to the caller.

      • When the caller clears the call, the user endpoint is idle.

   d. Else, if the PSAP does not answer:

      • If the far end fails the call, appropriate messages and tones are provided to the caller.

      • When the caller clears the call, the user endpoint and any remaining call attempt artifacts are cleared.

e. Else:

- When the call is answered, features supported at that time are available.

- When either party clears the call, the user endpoint is idle.

6. When a match is found (digit pattern plus correct number of expected digits, where the minimum number of digits is the less than the maximum number of digits):

a. Device Adapter initiates the call with Session Manager and Communication Manager.

b. The emergency call progresses with the SIP call handling procedure.

c. If the call fails at this point:

- Appropriate messages and tones are provided to the caller.

- When the caller clears the call, the user endpoint is idle.

d. Else, if the PSAP does not answer:

- If the far end fails the call, appropriate messages and tones are provided to the caller.

- When the caller clears the call, the user endpoint and any remaining call attempt artifacts are cleared.

e. Else:

- When the call is answered, features supported at that time are available.

- When either party clears the call, the user endpoint is idle.

🛈 Important:

Device Adapter does not support call back from PSAP to the caller..

7. When a match is found but the dialed number is not an emergency number, Device Adapter indicates call failure to the user:

- Appropriate messages and tones are provided to the caller.

- When the caller clears the call, the user endpoint is idle.

8. When no match exists (invalid digit string), the Device Adapter indicates failure to the user:

- Appropriate messages and tones are provided to the caller.

- When the caller clears the call, the user endpoint is idle.

Voice mail and Inbox button

This section is a subset of message waiting. It is functionally replaced with the "Message Waiting and Voice Mail" section.

Configuring controlled class of service support

About this task

With this feature, you can configure the password to protect your phone menu items such as Language and Change FeatureKey label.

Procedure

1. Log in to System Manager with the credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoint**.

4. On the Endpoints page, select the endpoint to configure the controlled class of service support.

5. Click **Edit**.

6. Enter the password in the **Security code** field.

   SMGR notifies the user if the password is incorrect. The examples of errors are the following:

   • Entry must be all digits for Security Code. In case the password contains anything other than digits.

   • The minimum length of the Security Code should be 4. In case the password is less than 4 characters.

7. On the Edit Endpoint page, click the **General Options** tab.

8. Add CCSA mnemonic in the **Features** field.

9. Click **Commit**.

Result

When you go to the phone menu in the Language or Change FeatureKey label item, you need to enter the password in the **Security code** field.

Configuring the personal profile manager

About this task

You can change the Session Manager settings for the sites with a big number of endpoints such as 1000 to 5000 endpoints per single Breeze® server.

If the Session Manager Instances are used for Avaya Device Adapter Breeze® server with a big number of Endpoints (1000-5000) connected, configure the following:

• **Maximum Connection per PPM client** to 8

- **PPM Packet Rate Limiting Threshold** to 500

Procedure

1. Log in to System Manager with the credentials.

2. On the System Manager web console, navigate to **Elements** > **Session Manager** > **Session Manager Administration**.

3. In **Session Manager Instances**, select the System Manager from the list.

4. Click **Edit**.

   The System Manager web console displays the Edit Session Manager window.

5. In the Personal Profile Manager (PPM) - Connection Settings, configure the following:

   - Select the **Limited PPM Client Connection** check box.

   - Enter 8 in the **Maximum Connection per PPM client** field.

   - Select the **PPM Packet Rate Limiting** check box.

   - Enter 500 in the **PPM Packet Rate Limiting Threshold** filed.

Appendix I: Avaya SBCE configuration for Device Adapter

Remote Cluster

Use the Remote Cluster feature to configure Avaya SBCE on the Breeze®. The Remote Cluster feature configures both primary and secondary Avaya SBCE IP addresses, that will override user defined Session Manager addresses for all Device Adapter endpoints. All registered endpoints re-register using the newly configured IPs. All new registrations will use defined registration path.

> **✱ Note:**
>
> Only valid IP formats are permitted in all of the four IP addresses fields. If **Remote Cluster** is disabled, then the registered Device Adapter endpoint will be used.

> **✱ Note:**
>
> The following are included in the Avaya SBCE setup that were resolved after changing their configuration:

- To use FAC for Agent work mode through Avaya SBCE and all FACs that require a reason code to work with Avaya SBCE, enable DTMF telephone events on Avaya SBCE codec list in media rules.

  For information about these fields, see Administering Avaya Session Border Controller for Enterprise at https://support.avaya.com/.

- To receive voice mail messages on a Device Adapter set that is configured Avaya SBCE, you must add the G711 codec and enable the MKI and Lifetime fields on the Media Rules page of Avaya SBCE.

  For information about these fields, see Administering Avaya Session Border Controller for Enterprise at https://support.avaya.com/.

- For DTMF, enable DTMF in the codec list of Avaya SBCE media rules and disable the SIP INFO for DTMF field on the messaging server.

  For information about these fields, see Administering Avaya Session Border Controller for Enterprise at https://support.avaya.com/.

  For information about these fields, see Administering Avaya Aura® Messaging at https://support.avaya.com/.

Comments on this document? infodev@avaya.com

Configuring Remote Cluster

About this task

The **Remote Cluster** feature is configured to override user defined System Manager addresses for all Device Adapter endpoints. If the **Remote Cluster** feature is enabled and both primary IP addresses are empty, then the Device Adapter sends SNMP alarms.

Procedure

1. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

2. Depending on whether you want to configure the **Remote Cluster** feature at a cluster level or a global level, do one of the following:

   a. Click the **Service Clusters** tab, select the appropriate application cluster, and then select the service as **DeviceAdapter**.

   b. Click the **Service Global** tab and select the service as **DeviceAdapter**.

3. Navigate to the **Remote Cluster** section and do the following:

   a. In the **Remote Cluster configuration enabled** field, select the check box, and click **Yes** to enable the **Remote Cluster** configuration.

   b. In the **Primary SBC IPv4 Address** field, type the primary SBC IPv4 address.

   c. In the **Secondary SBC IPv4 Address** field, type the secondary SBC IPv4 address.

   ✳ **Note:**

   If both IPv4 and IPv6 addresses are available in the primary and secondary Avaya SBCE, then Device Adapter uses the IPv4 addresses.

Configuring the WebLM server IP address on EMS

Before you begin

- Log on to the EMS web interface to access Avaya SBCE.

- Install the license for Avaya SBCE.

  For information about Avaya SBCE license and installation, see Deploying Avaya Session Border Controller for Enterprise on an Avaya Aura® Appliance Virtualized Platform and Administering Avaya Session Border Controller for Enterprise on the Avaya Support website.

Procedure

1. Login as an administrator to the EMS web interface.

2. In the **Device** drop-down list, click **EMS**.

3. Navigate to the **Device Management** page, and click **Add**.

4. Navigate to the **Add Device** page, enter the following in the **Device Name** and **Management IP** address of the SBC devices:

    a. In the **Device Name** field, enter `SBC`.

    b. In the **Management IP** field, enter the management IP address of the device.

For more information about field descriptions in the Device Management page, see Administering Avaya Session Border Controller for Enterprise on the Avaya Support website.

5. Navigate to **Device Management** > **Licensing**.

6. Perform one of the following:

- For a WebLM server or standalone server installed on System Manager, in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

   The URL format of the WebLM server installed on System Manager is: `https://<SMGR_server_IP>:52233/WebLM/LicenseServer`.

   The URL format of the standalone WebLM server is: `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer`.

- For an external WebLM server, type the link for the external WebLM server in **External WebLM Server URL** and click **Save**.

7. Click **Refresh Existing License** to refresh the existing licenses.

8. On the **Dashboard** screen, check the **License State** field.

   If the configuration is successful, the **License State** field shows **OK**.

Next steps

Configure Avaya SBCE to enable interfaces.

Network information

Network information is required to allocate IP addresses and masks to the interfaces on the Avaya SBCE.

😊 **Note:**

A1 and B1 are the two interfaces used in configuring Avaya SBCE. Each side of the Avaya SBCE can have one interface assigned. Generally, A1 is used for the internal side and B1 is used for the external side.

For more information about the A1 and B1 interface, see Administering Avaya Session Border Controller for Enterprise.

Enabling Avaya SBCE interfaces

Procedure

1. In the **Device** drop-down list, click **SBCE**.

2. In the navigation pane, click **Network & Flows** > **Network Management**.

   The SBC server displays the Network Management page.

3. On the Network Management page, click the **Interfaces** tab.

4. In the **Status** field, click **Enabled** for the **A1** interface name.

5. In the **Status** field, click **Enabled** for the **B1** interface name.

6. Navigate to the **Networks** tab and click **Add**.

7. In the **Gateway**, **Subnet Mask** and **IP Address** fields, enter relevant **A1** interface values.

   For more information about field descriptions in the Networks tab, see Administering Avaya Session Border Controller for Enterprise on the Avaya Support website.

8. Click **Add**.

9. In the **Gateway**, **Subnet Mask** and **IP Address** fields, enter relevant **B1** interface values.

10. Click **Save**.

11. Click **System Management** from the main menu.

12. In the status bar field, click the **Restart Application** icon.

Generating a .PEM certificate for Avaya SBCE

About this task

Use this procedure to provide a certificate and key for Avaya SBCE along with root CA certificate.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **TLS Management** > **Certificate**.

4. Click **Generate CSR**.

   The Generate CSR page is displayed.

5. In the **Country Name** field, enter the country name within which the certificate is created.

6. In the **State/Province Name** field, enter the state or province where the certificate is created.

7. In the **Locality Name** field, enter the locality or city where the certificate is created.

8. In the **Organization Name** field, enter the name of the company creating the certificate.

9. In the **Organizational Unit** field, enter the group within the company creating the certificate.

10. In the **Common Name** field, enter the name used to identify the company or group creating the certificate.

11. In the **Algorithm** field, select the hash algorithm to be used with the RSA signature algorithm.

12. In the **Key Size (Modulus Length)** field, select the certificate key length in bits.

13. In the **Key Usage Extension(s)** field, select the purposes for which the public key is used.

14. In the **Subject Alt Name** field, enter CN with a semicolon followed by an IP address.

15. In the **Passphrase** field, enter a password that is used when encrypting the private key.

16. In the **Confirm Passphrase** field, enter the same value entered in the Passphrase field.

17. In the **Contact Name** field, enter the individual name within the issuing organization acting as the contact point for certificate related issues.

18. In the **Contact E-mail** field, enter the e-mail address of the contact.

19. Click **Generate CSR**.

   For more information on **Generate CSR** field descriptions, see Administering Avaya Session Border Controller for Enterprise.

20. On the home page of System Manager web console, in the Services section, click **Security** > **Certificates** > **Authority**.

21. In the navigation pane, click **Public Web**.

22. In the navigation pane, navigate to the Enroll section and click **Create Certificate from CSR**.

23. In the **Username** field, enter the administrative account user name that is authorized to enroll a certificate.

24. In the **Enrollment code** field, enter the code to identify enrollment of a certificate.

25. In the **Request file** field, click **Browse** and browse to the location of the certificate file.

26. In the **Result type** drop-down field, select **PEM - full certificate chain** and click **OK**.

   You can convert a certificate with a .PEM extension to the .crt extension by renaming the file and changing the PEM extension to .crt.

   ✳ **Note:**

   This configuration generates certificates for inbound and outbound traffic on A1 and B1.

Creating client profiles

About this task

Use this procedure to create client profiles for inbound and outbound traffic.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **TLS Management** > **Client Profiles**.

4. Click **Add**.

   The EMS server displays the New Profile window.

5. Navigate to the TLS Profile section.

6. In the **Certificate** field, enter the certificate number with the .pem extension.

7. Navigate to the Certificate Verification section.

8. In the **Peer Certificate Authorities** field, enter the certificate number with the .crt extension

9. Navigate to the Handshake Options section.

10. In the **Version** field, check the version of Avaya SBCE.

11. Click **Finish** to create a client profile for the inbound traffic.

    The EMS server installs and displays the new TLS client profile.

12. Repeat step 3 through step 11 to create a client profile for the outbound traffic.

    ⊛ **Note:**

    For more information on TLS client profile screen field descriptions, see Administering Avaya Session Border Controller for Enterprise.

Creating server profiles

About this task

Use this procedure to create server profiles for inbound and outbound traffic.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **TLS Management** > **Server Profiles**.

The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.

4. Click **Add**.

   The system displays the Add Server Configuration Profile window.

5. Navigate to the TLS Profile section.

6. In the **Certificate** field, enter the certificate number with the .pem extension.

7. Navigate to the Handshake Options section.

8. In the **Version** field, click all versions of Avaya SBCE.

9. Click **Finish** to create a server profile for the inbound traffic.

10. Repeat step 3 through step 9 to create a server profile for the outbound traffic.

Adding internal and external signaling interface for Avaya SBCE

About this task

Use this procedure to define internal and external signaling interfaces with port number 5061 and 5091 on the Avaya SBCE.

For communication:

- Avaya SBCE and Device Adapter requires port number 5061
- Session Manager and Device Adapter requires port number 5091

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS server displays the Signaling Interface screen.

4. In the content pane, click **Add**.

   The EMS server displays the Add Signaling Interface pop-up window.

5. In the **Name** field, enter a descriptive name for the internal signaling interface.

6. In the **IP Address** field, select an internal signaling interface IP address.

7. In the **TLS Port** field, enter `5061` as the port number for Session Manager.

   The **TLS Profile** field is enabled immediately after the **TLS Port** field is defined

8. In the **TLS Profile** field, select the pre-defined TLS profile.

9. Click **Finish**.

10. In the **Name** field, enter a descriptive name for the external signaling interface.

11. In the **IP Address** field, select an external signaling interface IP address.

12. In the **TLS Port** field, enter `5061` as the port number for Device Adapter.

    The **TLS Profile** field is enabled after the **TLS Port** field is defined.

13. In the **TLS Profile** field, select the pre-defined TLS profile.

14. Click **Finish**.

    > **✱ Note:**
    >
    > To add an internal and external signaling interface with port number 5091, in the **TLS Port** field, type `5091`, and repeat step 4 through step 15.
    >
    > For more information about the Add signaling interface field descriptions, see Administering Avaya Session Border Controller for Enterprise.

    The EMS server displays the new configuration in the Signaling Interface display.

Adding media interface for the Avaya SBCE

About this task

Use this procedure to define internal and external media interfaces on the Avaya SBCE.

Define the details of the RTP, and SRTP port ranges for the internal and external media streams. The IP addresses for the media interface can be the same as those used for the signaling interface.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **Network & Flows** > **Media Interface**.

    The EMS server displays the Media Interface page.

4. In the content pane, click **Add**.

    The EMS server displays the Add Media Interface pop-up window.

5. In the **Name** field, enter a descriptive name for the internal media interface.

6. In the **IP Address** field, select an internal media interface IP address.

7. In the **Port Range** field, enter port ranges for the media path with enterprise end-points.

8. Click **Finish**.

9. In the content pane, click **Add**.

The EMS server displays the Add Media Interface pop-up window.

10. In the **Name** field, enter a descriptive name for the external media interface.

11. In the **IP Address** field, select an external media interface IP address.

12. In the **Port Range** field, enter port ranges for the media path with enterprise end-points.

13. Click **Finish**.

For more information about the Add media interface field descriptions, see Administering Avaya Session Border Controller for Enterprise.

The EMS server displays the new configuration in the Media Interface display.

Adding Server Interworking Configuration Profiles for Avaya SBCE

About this task

Server Interworking is defined for each server connected to the Avaya SBCE. Configuration of interworking includes Hold support, T.38 fax support, and SIP extensions.

Use this procedure to configure server interworking for Avaya SBCE.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **Configuration Profiles** > **Server Interworking**.

4. On the Interworking Profiles screen, click **Add**.

   The EMS server displays the Interworking Profile window.

5. Navigate to the avaya-ru profile, which is a factory setting appropriate for Avaya equipment.

6. Click **Clone Profile**.

   The system displays a Clone Profile pop-up window.

7. In the **Clone Name** field, enter a descriptive name for the Session Manager.

8. Click **Finish**.

9. Navigate to the General tab, click **Edit**, and enter details in the pop-up menu.

10. Select the **T.38 Support** check box and click **Next**.

11. Click **Finish**.

SIP servers

A server definition is required for each server connected to the Avaya SBCE. In Avaya SBCE, Device Adapter is connected as the Trunk Server, and the Session Manager is connected as the Call Server.

Related links

Configuring Session Manager as the call server

About this task

Use this procedure to configure Session Manager as the Call Server.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. To define Session Manager as a Call Server, navigate to **Services** > **SIP Servers**.

4. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.

5. In the **Profile Name** field, enter a descriptive name for the Session Manager and click **Next**.

6. In the **Server Type** drop-down menu, select **Call Server**.

7. In the **IP Address / FQDNs** field, type the Session Manager SIP interface address, the same as the Session Manager SIP Entity.

8. In the **Transport** field, check **TLS**, if TLS is used to signal transport between Session Manager and the Avaya SBCE.

9. In the **Port** field, type `5061` used for theSession Manager.

10. Click **Finish**.

11. Navigate to the Advanced tab.

12. In the **Interworking Profile** drop-down list, select the Interworking Profile for Session Manager.

13. In the **TLS Client Profile** field, select the predefined Avaya TLS client to be used for the server.

14. Click **Finish**.

To generate two SIP profiles for the Session Manager, click the SM profile, on the **Heartbeat** tab, select the **Enable Heartbeat** check box, to communicate with Device Adapter by using TLS.

Clone the previous SM profile and type `5091` in the port number field.

Related links

[SIP servers](#) on page 604

Configuring Device Adapter as a Trunk Server

About this task

Use this procedure to configure Device Adapter as the Trunk Server.

Procedure

1. Navigate to **Services** > **SIP Servers**.

2. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.

3. In the **Profile Name** field, type a descriptive name for the Device Adapter, and click **Next**.

4. In the **Server Type** drop down menu, select **Trunk Server**.

5. In the **IP Addresses / FQDNs** field, type the Device Adapter SIP interface.

6. In the **Transport** field, check **TLS**.

7. In the **Port** field, type `5061` used for the Device Adapter.

8. Click **Finish**.

9. Navigate to the Advanced tab.

10. In the **Interworking Profile** drop-down list, select the Interworking Profile for the Session Manager.

11. Click **Finish**.

Related links

[SIP servers](#) on page 604

Adding Routing Configuration Profiles

About this task

You must add the routing to route to Session Manager on the internal side and Device Adapter on the external side. The IP addresses and ports defined in the procedure are used as the destination for signaling.

> ✱ **Note:**
>
> - Default port number values are assigned for TCP, UDP, and TLS if no port number is specified in the **Next Hop IP Address** field.
>
> - The default port number used for TCP and UDP fields is 5060.
>
> - The default port number used for the TLS field is 5061.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **Configuration Profiles** > **Routing**.

4. In the application pane, click **Add**.

   The application pane displays the Routing Profile pop-up menu, and the Content pane displays the parameters of the selected routing profile.

5. In the **Profile Name** field, enter `Call Server`, a descriptive name for Session Manager and click **Next**.

6. In the **Next Hop Server** field, enter the Session Manager SIP interface address and port number.

7. In the **Transport port** field, click **TLS**.

8. Click **Finish**.

9. To define a route for Session Manager, in the content pane, click **Clone**.

   The EMS server displays the Clone Profile pop-up window.

10. In the **Next Hop Address** field, type `5091` for Session Manager.

11. In the **Transport** field, select **TLS**.

12. Click **Finish**.

13. To define a route for the Device Adapter, in the content pane, click **Clone**.

14. The EMS server displays the Clone Profile pop-up window.

15. In the **Next Hop Address** field, type `5061` for Device Adapter.

16. In the **Transport** field, select **TLS**.

17. Click **Finish**.

Creating a reverse proxy policy

About this task

Use this procedure to create a policy to allow traffic in the Avaya SBCE.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **Configuration Profiles** > **Reverse Proxy Policy**.

   The system displays the Reverse Proxy Policy window.

4. Click **Add**, navigate to General and enter `rule name`.

5. In the **Allow Web Sockets** field, select **Y**.

6. In the **Request Max Body Size** field, type `2 MB`.

   For more information about the Reverse Proxy Policy field descriptions, see Administering Avaya Session Border Controller for Enterprise.

Creating an application rule

About this task

Use this procedure to create an application rule for the Avaya SBCE.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the navigation pane, click **SBCE**.

3. In the navigation pane, click **Domain Policies** > **Application Rules**.

4. Click **Add** to create a new application rule and enter rule name.

   Note:

   Type the number of concurrent sessions required for the customer license. As a best practice, type a number that is higher than the number specified in the customer license.

   For example, if you have a license for 300 concurrent sessions, type 500 for each, audio and video.

5. Enter the required values in the appropriate fields and click **Finish**.

   For more information on the Application Rule screen field descriptions, see Administering Avaya Session Border Controller for Enterprise.

Topology hiding

Topology hiding is used to manage how the source, destination and routing information in SIP and SDP message headers must be substituted or changed to maintain the network integrity. It is also used to hide the topology of the enterprise network from external networks.

The default Replace Action is Auto. This replaces local information with IP addresses, generally the next hop for destination headers and local IP for source headers.

Topology hiding has an advantage of presenting single and multiple Record-Route headers externally from Session Manager. Topology hiding cannot be applied to the Contact header, but IP addresses are translated to the Avaya SBCE external addresses using NAT.

Creating a topology hiding profile for Avaya SBCE

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **Configuration Profiles > Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.

4. Click **Add**.

5. In the **Profile Name** field, enter the profile name and click **Next**.

6. In the **Header** field, enter the name of the header to be changed with topology hiding.

7. In the **Criteria** field, add the criteria that changes with topology hiding.

8. In the **Replace Action** field, add an option that replaces the header.

9. In the **Overwrite Value** field, add a value that overwrites the header.

   For more information about the Topology Hiding Profiles field descriptions, see *Administering Avaya Session Border Controller for Enterprise*

Media rules

Media rules on Avaya SBCE are used to handle any unusual media handling scenarios that a Service Provider encounters.

Creating a media rule for the Avaya SBCE

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the Avaya SBCE you want to administer.

3. In the navigation pane, click **Domain Policies** > **Media Rules**.

   The application pane displays the existing Media Rule sets, and the content pane displays the parameters of the selected Media Rule set.

4. In the applications pane, click **Add** and enter **rule name**.

   The EMS server displays the **Media Rule window**.

5. Navigate to the **Encryption** tab.

6. Navigate to the **Audio Encryption** section and select the preferred format.

7. In the **Encrypted RTCP** field, select the check box.

8. In the **Interworking** field, select the check box.

   Video encryption is not currently offered as part of the solution but do the following so that the conversion to RTP can occur.

9. Navigate to the **Video Encryption** section and select the preferred format.

10. In the **Encrypted RTCP** field, select the check box.

11. In the **Interworking** field, select the check box.

12. Click **Finish**.

13. **(Optional)** To configure audio codec prioritization, navigate to the **Codec Prioritization** tab and click **Edit**.

14. Select the **Codec Prioritization** and **Allow Preferred Codecs Only** check boxes.

15. In the **Preferred Codecs** field, select a single codec or hold down the **Ctrl** key and click to select multiple codecs simultaneously.

16. Click the **Signaling QoS** tab in the content pane.

    The EMS server displays the **Signaling QoS** pop-up window.

17. Edit the appropriate fields and click **Finish**.

    For more information on the Media Rules field descriptions, see *Administering Avaya Session Border Controller for Enterprise*.

Creating an end point policy group for Avaya SBCE

About this task

An end point policy group is required to implement the Media rule.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE that you want to administer.

3. In the navigation pane, click **Domain Policies > End Point Policy Groups**.

   The application pane displays the existing End Policy group sets, and the Content pane displays the parameters of the selected End point policy set.

4. In the application pane, click **Add**.

5. The EMS server displays the first **Group Name** window.

6. In the **Group Name** field, type a name for the new policy group, and click **Next**.

   The EMS server displays the second Policy Group window where you must define the policy group parameters.

7. In the **Application Rule** drop-down list, specify an application rule that defines the type of Avaya SBCE.

8. In the **Media Rule** drop-down list, specify the media rule used to match media packets.

9. Click **Finish**.

   For more information on the End Point Policy Group field descriptions, see *Administering Avaya Session Border Controller for Enterprise*.

Creating a server flow for the Avaya SBCE

Creating a subscriber flow for Session Manager

About this task

Use this procedure to create a subscriber endpoint flow for Session Manager manually.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

Separate tabs display the parameters comprising subscriber endpoint flows and server endpoint flows.

4. Navigate to the **Subscriber Flows** tab.

   The content area displays the existing endpoint flows.

5. Click `Add`.

6. In the **Flow Name** field, type a flow name such as **SM_Flow_5091**.

7. In the **Signaling Interface** field, select the external interface towards the Avaya SBCE, and click **Next**.

8. In the **Media Interface** field, select the internal media interface towards the Avaya SBCE.

9. In the **End Point Policy Group** field, click the created endpoint policy.

10. In the **Routing Profile** field, keep the default value.

11. Navigate to **Optional Settings**.

12. In the **TLS Client Profile** field, select the external TLS profile defined in the Creating a client profile section.

13. Click **Finish** to save.

14. Click **Add** to create another subscriber flow for **SM_Flow_5061**.

    The **SM_Flow_5061** window is displayed. Repeat step 6 through step 13 to configure **SM_Ser_5091**. You need to use the **SM_Ser_5091** name later in the procedure.

Creating a subscriber flow for Breeze®

About this task

Use this procedure to create a subscriber flow for Breeze®.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **Network & Flows > End Point Flows**.

4. Separate tabs display the parameters comprising subscriber endpoint flows and server endpoint flows.

5. Navigate to the **Subscriber Flows** tab.

   The content area displays existing endpoint flows.

6. Click **Add** to create a Breeze Subscriber Flow for **Breeze_flow_5061**.

7. In the **Flow Name** field, type a flow name such as **Breeze_flow_5061**.

8. In the **Signaling Interface** field, select the internal interface towards the Avaya SBCE, and click **Next**.

9. In the **Media Interface** field, select the external media interface towards the Avaya SBCE.

10. In the **End Point Policy Group** field, click the created endpoint policy.

11. In the **Routing Profile** field, keep the default value.

12. Navigate to **Optional Settings**.

13. In the **TLS Client Profile** field, select the internal TLS profile defined in the Creating a client profile section.

14. Click **Finish** to save.

15. Navigate to the **Server Flows** tab.

    The content area displays the existing endpoint flows.

16. Click **Add** to create a server flow for SM_Flow_5091.

    The SM_Flow_5091 window is displayed.

17. In the **Flow Name** field, type a flow name.

18. In the **SIP Server Profile** field, select the Server Configuration Hiding Profile to be used for this Server End Point Flow.

19. In the **Received Interface** field, select the external interface towards the endpoints.

20. In the **Signaling Interface** field, select the internal interface towards the Avaya SBCE.

21. In the **Media Interface** field, select the interface towards the Avaya SBCE.

22. In the **End Point Policy Group** field, click the created endpoint policy.

23. In the **Routing Profile** field, keep the default value.

24. In the **Topology Hiding Profile**e field, keep the default value or select the appropriate topology hiding profile.

25. Click **Finish**.

    Repeat step 17 through step 25 to create flows for **Breeze_flow_5091**, **SM_Ser_5091** and **SM_flow**.

26. To check the configured flows, locate the flow you want to see in the **Server Flows** tab and click **View**.

Creating PPM mapping profile for the Avaya SBCE

About this task

Use this procedure to create a standard Personal Profile Manager (PPM) mapping profile for the Session Manager server.

Procedure

1. Log on as administrator to the EMS web interface.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. Navigate to **DMZ Services > PPM Mapping**.

4. Click the **Add** button that is above the Mapping Profiles list.

5. In the **Profile Name** field, type the profile name.

6. Click **Next**.

7. In the **Server Type** field, select Session Manager.

8. 8. In the **SIP Server Profile** field, select the profile you want to assign to Session Manager.

9. In the **Server Address** field, select the pre-defined IP address and port number of the Session Manager system for which you are creating a profile.

10. In the **Signaling Interface** field, select the external signaling interface used for the profile.

11. In the **Mapped Transport** field, select the transport protocol used for the mapping profile.

12. Click **Finish**.

13. Repeat step 4 through step 12 to create a standard mapping profile for **SM_5091**.

Reverse proxy configuration

Configuring reverse proxy for PPM Session Manager port 5060

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **DMZ Services** > **Relay Services**.

4. On the **Relay Services** page, click **Reverse Proxy** > **Add**.

   The Add Reverse Proxy page is displayed.

5. In the **Service Name** field, enter a name for the reverse proxy profile. For example, **PPM_SM5060**.

6. In the **Enabled** field, select this check box to enable the profile.

7. In the **Listen IP** field, select the IP address of an external Avaya SBCE system.

8. In the **Listen Port** field, enter the port number that the remote workers use for SSO service. For HTTPS, the default value is 443.

9. In the **Listen Protocol** field, select the protocol that the remote workers use for the SSO service.

10. In the **Listen TLS Profile** field, select a configured TLS profile.

11. In the **Server Protocol** field, select the protocol for the IDE server.

12. In the **Server TLS Profile** field, select a configured server profile.

13. In the **PPM Mapping Profile** field, select a configured PPM mapping profile.

14. In the **Reverse Proxy Policy Profile** field, select the number of requests permitted per second.

15. In the **Server Addresses** field, enter the server IP address and port number.

16. Click **Finish**.

Configuring reverse proxy for PPM Session Manager 5091

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **DMZ Services** > **Relay Services**.

4. On the Relay Services page, click **Reverse Proxy** > **Add**.

   The Add Reverse Proxy page is displayed.

5. In the **Service Name** field, enter a name for the reverse proxy profile. For example, **PPM_80_p5091**.

6. In the **Enabled** field, select this check box to enable the profile.

7. In the **Listen IP** field, select the IP address of an external Avaya SBCE system.

8. In the **Listen Port** field, enter the port number that the remote workers use for SSO service. For HTTP, the default value is 80.

9. In the **Listen Protocol** field, select the protocol that the remote workers use for the SSO service.

10. In the **Listen TLS Profile** field, select a configured TLS profile.

11. In the **Server Protocol** field, select the protocol for the IDE server.

12. In the **Server TLS Profile** field, select a configured server profile.

13. In the **PPM Mapping Profile** field, select a configured PPM mapping profile.

14. In the **Reverse Proxy Policy Profile** field, select the number of requests permitted per second.

15. In the **Server Addresses** field, enter the server IP address and port number.

16. Click **Finish**.

Configuring reverse proxy for PPM Session Manager port 5090

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, click the Avaya SBCE you want to administer.
3. In the navigation pane, click **DMZ Services** > **Relay Services**.
4. On the Relay Services page, click **Reverse Proxy** > **Add**.

   The Add Reverse Proxy page is displayed.
5. In the **Service Name** field, enter a name for the reverse proxy profile. For example, **PPM_SM5090**.
6. In the **Enabled** field, select this check box to enable the profile.
7. In the **Listen IP** field, select the IP address of an external Avaya SBCE system.
8. In the **Listen Port** field, enter the port number that the remote workers use for SSO service. For HTTPS, the default value is 443.
9. In the **Listen Protocol** field, select the protocol that the remote workers use for the SSO service.
10. In the **Listen TLS Profile** field, select a configured TLS profile.
11. In the **Server Protocol** field, select the protocol for the IDE server.
12. In the **Server TLS Profile** field, select a configured server profile.
13. In the **PPM Mapping Profile** field, select a configured PPM mapping profile.
14. In the **Reverse Proxy Policy Profile** field, select the number of requests permitted per second.
15. In the **Server Addresses** field, enter the server IP address and port number.
16. Click **Finish**.

Configuring reverse proxy for PPM Session Manager port 80

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, click the Avaya SBCE you want to administer.
3. In the navigation pane, click **DMZ Services** > **Relay Services**.
4. On the **Relay Services** page, click **Reverse Proxy** > **Add**.
5. In the **Service Name** field, enter a name for the reverse proxy profile. For example, **PPM_80**.

6. In the **Enabled** field, select this check box to enable the profile.

7. In the **Listen IP** field, select the IP address of an external Avaya SBCE system.

8. In the **Listen Port** field, enter the port number that the remote workers use for SSO service. For HTTP, the default value is 80.

9. In the **Listen Protocol** field, select the protocol that the remote workers use for the SSO service.

10. In the **Listen TLS Profile** field, select a configured TLS profile.

11. In the **Server Protocol** field, select the protocol for the IDE server.

12. In the **Server TLS Profile** field, select a configured server profile.

13. In the **PPM Mapping Profile** field, select a configured PPM mapping profile.

14. In the **Reverse Proxy Policy Profile** field, select the number of requests permitted per second.

15. In the **Server Addresses** field, enter the server IP address and port number.

16. Click **Finish**.

Configuring Whitelist setting in Firewall for Avaya SBCE

About this task

You can use this procedure to set up whitelist rules to always allow data from specific IP addresses.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the **Device** drop-down list, click the SBCE you want to administer.

3. In the navigation pane, click **DMZ Services** > **Firewall**.

4. On the Whitelist tab, click **Add**.

5. In the **Name** field, enter the name of the whitelist rule.

6. In the **Source Address** field, enter the IP address from which data must be allowed.

7. In the **Destination Address** field, enter the IP address to which sending data must be allowed.

8. Click **Finish**.

   For more information on the Whitelist tab field descriptions, see Administering Avaya Session Border Controller for Enterprise.

Configuring Avaya SBCE on SM

About this task

Use this procedure to add the external IP address (B1) of Avaya SBCE in the virtual Session Manager. Use this task to create entity links between virtual SM and Device Adapter using TLS port 5061 and link between virtual SM and Device Adapter concentrator using TLS port 5091.

Procedure

1. Log on to the System Manager web interface.

2. In the **Elements** section, click **Routing**.

3. In the left navigation pane, click **SIP Entities**.

4. On the **SIP Entities** page, click **New**.

5. Navigate to **SIP Entity Details** > **General**.

6. In the **Name** field, enter the name of the SIP entity.

7. In the **IP Address** field, enter the external IP address of the Avaya SBCE.

8. In the **Type** field, select Session Manager.

9. Navigate to **Entity Links** and click **Add**.

10. Click **Commit**.

11. To create entity links between virtual Session Manager and Device Adapter using TLS port 5061, in the Name field, enter a name of the SIP entity.

12. In the **IP Address** field, enter the IP address of the external Avaya SBCE system.

13. In the Type field, select Breeze®.

14. Navigate to **Entity Links** and click **Add**.

15. Click **Commit**.

16. To create entity links between virtual Session Manager and Device Adapter concentrator using TLS port 5091, in the **Name** field, enter a name of the SIP entity.

17. In the **IP Address** field, enter the IP address of the external Avaya SBCE system.

18. In the **Type** field, select **Endpoint Concentrator**.

19. Navigate to **Entity Links** and click **Add**.

20. Click **Commit**.

21. To configure remote access with internal IP addresses for Avaya SBCE, in the **Elements** section, click Session Manager.

22. In the left navigation pane, click **Network Configuration** > **Remote Access**.

23. In the **Remote Access** page, click **New**.

24. The system displays the **Remote Access Configuration** page.

25. In the **Name** field, enter a remote access configuration name.

26. Navigate to **SIP Proxy Private IP Addresses**.

27. Click **New** to add a new SIP proxy private address to communicate with Session Manager.

28. In the **SIP Private Address (Reference B)** field, type the internal IP address of Avaya SBCE.

29. In the **SBC Type** field, select Avaya SBCE.

30. Select the **Securable** check box.

31. Click **Add**.

Configuring Avaya SBCE on Communication Manager

About this task

Use this procedure in the Communication Manager to ensure Media Encryption maps with media configuration on Avaya SBCE.

Before you begin

Ensure that the **Media Encryption Over IP** field on the system-parameters customer-options screen is set to **y**.

Procedure

1. On the SAT screen, type `change ip-codec-set` n, where n is the number corresponding to the codec set you want to change.

2. In the **Encrypted SRTCP** field, type `best-effort`, if you want Communication Manager to negotiate encrypted SRTCP capability between endpoints.

3. In the **Media Encryption** field, add one or more profiles.

   If the RTP media encryption is set to none, the enforce-encrypted SRTCP rules do not apply to the RTP/RTCP streams.

4. Save and Exit.

   Optional: Do the following to disable the **Enforce SIPS URI for SRTP** on Signaling Group.

5. Enter `change signaling-group` n, where n is the signaling group number.

6. Ensure that the **Group Type** field is set to **SIP**.

7. Set the **Peer Server** field to **SM**.

8. Ensure that the **Enforce SIPS URI for SRTP** is set to **n**.

9. Select **Enter** to save your changes.

   For more information on Setting up the signaling groups, see Avaya Aura® Communication Manager Feature Description and Implementation.

Appendix J: Legacy Avaya Aura® SIP endpoint feature and Communication Manager feature support

Legacy Avaya Aura® SIP endpoint feature support on Device Adapter

A limited number of features that are supported on the 96X1 and J-Series SIP stations are available on Device Adapter supported CS 1000 stations.

> ✱ **Note:**
>
> Device Adapter provides the following user experience for these features:
>
> - User experience similar to that of CS 1000.
>
> - User experience similar to but not identical to that of CS 1000.
>
> - User experience similar to that of Avaya Aura®.

For information about the Communication Manager user experience for the following features, see the Communication Manager feature documentation.

- Abandoned Call Logging

- Abort Transfer

- Authorization Codes

- Automatic Hold

- Calling Party Number Block, Unblock

- Calling Party Number Block, Unblock of Internal Numbers

- Code Calling

- Crisis Alert (Dial/View)

- Directory (Aura Integrated)

- Group Paging

- Hunt Groups
- Idle Line Appearance Select
- Limit Number of Concurrent Calls
- Loudspeaker Paging
- Loudspeaker Paging - Deluxe
- Malicious Call Trace (MCT) - Activation
- MLPP (Multiple Level Precedence and Pre-emption) TDM Trunking
- Multiple Device Access
- Priority Calling
- Simulated Bridged Appearance
- Station On-Hook Dialing
- Temporary Bridged Appearance
- Time of Day Routing
- VIP Calling

Limit Number of Concurrent Calls

The Limit Number of Concurrent Calls (LNCC) feature is accessed on a multiappearance station, and it lets the users receive only one call at a time. If you enable the LNCC feature and the user is busy in another call, the rest of the incoming calls receive a busy tone.

This feature is supported on CS 1000 UNISTIM IP phones.

LNCC allows:

- Outgoing calls, incoming priority calls, and emergency callback for SIP stations.
- Outgoing calls, incoming priority calls, emergency callback, and crisis alert for H.323 and DCP stations.

Configuring LNCC on CS1000

About this task

The Limit Number of Concurrent Calls (LNCC) feature restricts the number of incoming calls to one call at a time. LNCC configuration on CS 1000 IP phones is similar to that of the configuration for SIP phones.

LimitInCalls is a new feature key that must be configured for the CS 1000 phones. Do the following to access the LNCC feature on the CS 1000 phones:

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the CC endpoint for which you want to configure the login button, and then click **Edit**.

5. On the Edit Endpoint page, click the **Button Assignment** tab.

    a. In the **Button Feature** field, select **limit-call**.

    b. (Optional) In the **Button Label** field corresponding to the button number that you want to configure as a **limit-call** button, type a name for the limit-call label. For example, `Limit-call.`

    This label appears on the endpoint.

    If you do not specify a label, the default label that appears on the endpoint is **LimitInCalls**.

6. Press **LimitInCalls** button on the phone to activate the feature.

    ✱ **Note:**

    LNCC feature status - **Limit In Call Activated**, is displayed on the top line of the phone screen and through the feature key lamp to confirm that the feature is activated on the phone.

7. Press **LimitInCalls** button again on the phone to deactivate the future.

    ✱ **Note:**

    No feature status appears on the phone screen to confirm that the feature is deactivated on the phone.

8. Click **Commit** to save the changes.

Communication Manager feature support

Communication Manager provides all feature support on Device Adapter.

The following table indicates whether Device Adapter supports or partially supports the Communication Manager features, along with the type of user experience.

For features listed in the table, Device Adapter provides a user experience similar to that of the following:

- CS 1000
- CS 1000, but with minor differences.

- Avaya Aura®
- Both CS 1000 and Avaya Aura® depending on the feature configuration.

Communication Manager service/feature	Supported	User experience similar to	Comments
Abandoned Call Logging	Yes	CS 1000	The logs are logged in the caller's logs.
Abbreviated Dialing	Yes	Both of the following: • Depending on the configuration, the user experience is similar to CS 1000. • Avaya Aura®	You can configure this feature to simulate several CS 1000 features. Otherwise, the user experience is similar to that of Avaya Aura®.
Abort Transfer	Yes	CS 1000	User operation for this feature is the same as that of CS 1000. For more information, see "Transfer — blind or consultative" in "Appendix H: Call processing features and services."
Account Codes	Yes	CS 1000, with minor differences.	Differences exist in how you administer this feature in CS 1000. But, the user experience is similar to that of CS 1000, with minor differences.
Announcements	Yes	CS 1000, with minor differences.	Differences exist in how you administer this feature in CS 1000. But, the user experience is similar to that of CS 1000, with minor differences.
Authorization Codes	Yes	CS 1000, with minor differences.	The number or length of the authorization codes may differ. But, the user experience is similar to that of CS 1000, with minor differences.
Automatic Callback	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	You can configure this feature to simulate the CS 1000 Ring Again feature. Depending on how you configure this feature, the user experience can be the following: • Avaya Aura® Automatic Callback • CS 1000 Ring Again

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Automatic Dial Buttons	Yes	CS 1000, with minor differences.	For more information, see "Autodial" in "Appendix H: Call processing features and services."
Automatic Exclusion	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	You can use this feature to configure the Privacy Release settings for a CS 1000 user experience.
Automatic Route Selection (ARS)	Yes	Avaya Aura®	You can configure this feature to perform the Network Alternate Route Selection (NARS), Basic Alternate Route Selection (BARS), or Coordinated Dialing Plan (CDP) call routing functions of CS 1000.
Bridged Line (Call) Appearances	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	You can use Bridged Call Appearances for the MADN SCA and MCA features. However, you can configure Bridged Line and Call Appearances to provide an Avaya Aura® user experience.
Button Module	Yes	CS 1000, with minor differences.	Button Modules are supported only on those CS 1000 stations that support button modules. The physical device determines the number of buttons per module, although some modules, with two or more pages, are programmed as though they were two or three smaller modules. Some stations may limit the maximum number of button modules allowed.
Call Coverage (6 levels)	Yes	Avaya Aura®	The CS 1000 second level call forward permits up to two coverage options. Second level call forward means forwarding a forwarded call.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Caller ID (Name and number)	Yes	CS 1000, with minor differences.	Device Adapter provides the CS 1000 user experience for this feature depending on the message contents received. The message contents can differ because of third-party interoperability.
Call Forward (All call, Busy, No answer, Disable)	Yes	CS 1000, with minor differences.	For more information, see "Call forward" in "Appendix H: Call processing features and services."
Call Hold, Resume	Yes	CS 1000	
Call Log Missed/ Answered/Outgoing calls (Call/Delete/Details)	Yes	CS 1000, with minor differences.	Call log uses logs from Personal Directory and other related logs. For more information, see "Appendix H: Call processing features and services."
Call Park, Answer Back	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	If you use the Avaya Breeze® platform Park and Page feature, the user experience is similar to that of CS 1000. Otherwise, the user experience is similar to that of Avaya Aura®.
Calling Party Number Block, Unblock of Internal Numbers	Yes	Avaya Aura®	Parts of this feature support the CS 1000 Privacy service. You can disable CS 1000 Calling Party Privacy setting. However, this is not supported in Device Adapter Release 8.1.2 and Avaya Aura® Release 8.1.2. If you do not modify the configuration of the Communication Manager FAC, CS 1000 FFC, or any other setting of this feature, the user experience for Privacy operations is similar to that of CS 1000. The service itself is the Avaya Aura® service, with all Avaya Aura® capabilities. The key parts for CS 1000 FFC handling are similar to that of the Avaya Aura® model. But, based on the additions, the overall experience is that of Avaya Aura®.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Call Pickup	Yes	CS 1000, with minor differences.	For more information, see "Call Pickup" in "Appendix H: Call processing features and services."
Class of Service (CoS)	Yes	Both of the following: • CS 1000 • Avaya Aura®	A CS 1000 CoS may or may not have a matching Avaya Aura® CoS. The following are the configuration options: • If a CS 1000 CoS matches an Avaya Aura® CoS, the matching Avaya Aura® CoS is available in System Manager. You can configure the Avaya Aura® CoS in System Manager. For more information about the available options in the Avaya Aura® CoS table, see the screen shot that follows this table. • If a CS 1000 CoS does not have a matching Avaya Aura® CoS, a matching Avaya Aura® feature exists on the Device Adapter endpoint. You can configure the Avaya Aura® feature on the Device Adapter endpoint.
Code Calling	Yes	Avaya Aura®	Tone-based loudspeaker paging.
Conference (Ad-hoc six-party)	Yes	CS 1000, with minor differences.	Some CS 1000 sets use three-party conference. Whereas, Device Adapter sets use only six-party conference.
Contacts (Add/Edit/Delete/Details)	Yes	CS 1000, with minor differences.	Uses Personal Directory and related logs.
Core Redundancy	Yes	Avaya Aura®	
Crisis Alert (Dial/View)	Yes	Avaya Aura®	Dial only. This feature provides 911 call paging capability.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Directed Call Pickup	Yes	CS 1000, with minor differences.	Device Adapter maps the Avaya Aura® feature to the CS 1000 PUDN FFC. However, although there are minimal differences visible to the user, CS 1000 requires the user to belong to a pickup group. This is not required in the Avaya Aura® equivalent feature.
Directory (Aura Integrated)	Yes	Avaya Aura®	Uses Corporate Directory.
Exclusion	Yes	CS 1000, with minor differences.	The Exclusion feature of Avaya Aura® and the Privacy feature of CS 1000 are similar. This includes both the station setting, and the Privacy key and Exclusion button function. For more information, see "Privacy" in "Appendix H: Call processing features and services."
Extended Call Pickup	Yes	CS 1000, with minor differences.	Device Adapter maps the Avaya Aura® feature to the CS 1000 Group Call Pickup feature. Depending on the Extended Call Pickup feature configuration, there might be no visible user experience difference. However, Avaya Aura® requires the user's group to belong to an extended pickup group, which is not required in the CS 1000 Group Call Pickup feature.
Extension to Cellular (EC500)	Yes	Both of the following: • CS 1000 • Avaya Aura®	Uses FAC to change state. Neither the CS 1000 station nor the Device Adapter station is aware of the call routing to cellular.
Feature Name Extensions	Yes	Avaya Aura®	Used by EC500.
Forced Entry of Account Codes	Yes	Avaya Aura®	
Hold Recall	Yes	Avaya Aura®	Hold Recall re-rings the station that placed it on hold if the station is idle.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Hotline	Yes	CS 1000, with minor differences.	Uses abbreviated dialing. Two-way hotline user experience is similar to that of CS 1000. One-way hotline uses Autodial after the user selects a call appearance. This is similar to the Avaya Aura® user experience.
Hunt Groups	Yes	Both of the following: • CS 1000 • Avaya Aura®	Linear (direct department calling) and round robin (circular) align with CS 1000 handling of the Hunt Groups feature. However, Avaya Aura® has more alternatives for the Hunt Groups feature.
Idle Line Appearance Select	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	Avaya Aura® allows differentiation between appearances shared by multiple users and private call appearances.
Last Number Dialed	Yes	CS 1000, with minor differences.	Last Number Dialed is generically available for digital and UNIStim stations by doing any of the following: • Press the primary extension line appearance twice. • On the sets that support Redial list, press the appropriate entry in the Redial list. For more information, see "Last Number Redial" in "Appendix H: Call processing features and services."
Limit Number of Concurrent Calls	No	Avaya Aura®	In CS 1000, there is no direct equivalent feature for the Limit Number of Concurrent Calls feature. However, you can configure a single key for the directory number in a CS 1000 station to automatically limit the number of concurrent calls.
Local Survivability with Survivable Remote	Yes	Avaya Aura®	

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Loudspeaker Paging	Yes	Avaya Aura®	By using loudspeaker paging, a CS 1000 user can call the paging trunk.
Loudspeaker Paging – Deluxe	Yes	Avaya Aura®	A corresponding Park & Page feature exists in CS 1000, but the user experience is different.
Malicious Call Trace (MCT) - Activation	Yes	Both of the following: • CS 1000 • Avaya Aura®	MCT activation has the same user experience as that of the CS 1000 user experience. However, deactivating MCT requires a non-SIP station to act as an MCT controller in CS 1000. To Avaya Aura®, all Device Adapter stations are SIP stations.
Meet-Me Conferencing – CM	Yes	Both of the following: • Avaya Aura® • Depending on the configuration, the user experience can be similar to CS 1000.	The user experience may differ from that of CS 1000 based on the specific CS 1000 Meet-Me conference bridge. The user experience depends on how the bridge service handles the conference.
Message Retrieval (one button)	Yes	Avaya Aura®	Message retrieval is part of the Message Waiting feature in CS 1000. Avaya Aura® provides the ability to retrieve system-wide posted messages.
Message Waiting Indication (own number)	Yes	CS 1000, with minor differences.	Message Waiting Indication, including audible indication and lamp state, is part of the Message Waiting feature in CS 1000. In the Avaya Aura® documentation, the Message Waiting feature is also referred to as the Leave Word Calling feature.
Multiple Call Handling, Multiple Lines, Multiple Call Appearances	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	The specific user experience depends on whether the call appearances are implemented as the CS 1000 model of bridged call appearances, or whether the standard Avaya Aura® model is used.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Multiple Device Access	Yes	CS 1000, with minor differences.	Ensure that there is only one device registered at one time. If the number of concurrent devices registered is more than one, problems can occur in case of a network failure. For example, an endpoint that lost connection to Device Adapter, or Device Adapter that lost connection to Session Manager or Communication Manager may be unable to register successfully.
Ringing Control - Bridged Line	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	System Manager or Communication Manager configuration. The Ringing Control - Bridged Line feature aligns with the implementation of the appearances. You can use the following bridged or call appearance options, as applicable, to map the CS 1000 and Device Adapter feature: • SCN (non-ringing) • SCR (ringing) • MCN (non-ringing) • MCR (ringing) Otherwise, the Avaya Aura® model is used.
Send All Calls	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	The station displays the button name as Make Set Busy. If you configure the Send All Calls feature to mimic the Make Set Busy feature, the user experience is similar to that of CS 1000. Otherwise, the user experience is similar to that of Avaya Aura®.
Time of Day Routing	Yes	Depending on the configuration, the user experience is similar to the following: • CS 1000 • Avaya Aura®	Both CS 1000 and Avaya Aura® have Time of Day-based routing. Although, the implementation differs significantly and the user experience depends on the configuration of this feature.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Traffic Measurements	Yes	Avaya Aura®	
Transfer (Attended, Unattended)	Yes	CS 1000, with minor differences.	CS 1000 and Avaya Aura® provide similar transfer handling for specific stations. However, the Avaya Aura® SIP stations differ from the Avaya Aura® H.323 and digital stations. The CS 1000 behavior closely matches the behavior of the H.323 and digital stations. Device Adapter maps the behavior to provide a user experience similar to that of CS 1000.
VIP Calling	Yes	Avaya Aura®	
Automatic Hold	Partially supported	Avaya Aura®	The Automatic Hold feature allows you to switch between the current held party and active party, and vice-versa. Device Adapter does not rely on the configuration parameters in System Manager. The service is always on.
Calling Party Number Block, Unblock	Partially supported	Avaya Aura®	CS 1000 has an equivalent feature for the 911 call center equivalent.
Group Paging	Partially supported	Avaya Aura®	Some CS 1000 station types do not have speakers and cannot receive pages.
Multiple Level Precedence and Pre-emption (MLPP) TDM Trunking	Partially supported	Avaya Aura®	CS 1000 supported MLPP for the Federal market as a server feature. You must follow specific administration procedures to access the software feature documentation. MLPP signaling was provided over applicable ISDN variants and – to a limited extent – over H.323 and SIP trunks in the network. However, CS 1000 Release 5 was the last release that was JITC certified.

Table continues…

Communication Manager service/feature	Supported	User experience similar to	Comments
Priority Calling	Partially supported	Avaya Aura®	• Priority button is not displayed on a Device Adapter phone. • Device Adapter phone is unable to make an abbreviated dialing call as a Priority call using FAC. • The dn-dst key is not available for a Device Adapter phone. • The consult key is not available for a Device Adapter phone.
Simulated Bridged Appearance	Partially supported	Avaya Aura®	Dual-registration does not work for a Device Adapter UNIStim user.
Station On-Hook Dialing	Partially supported	CS 1000	The CS 1000 Predial and Initiate feature is equivalent to the Station On-Hook Dialing feature, but the behavior differs significantly. The Predial and Initiate feature that is used on CS 1000 conforms to Avaya Aura® and is supported. User can predial while on hook, and then initiate in a manner similar to the CS 1000 user experience.
Temporary Bridged Appearance	Partially supported	Avaya Aura®	The term-x-gr button is not included in the template of a Device Adapter phone. As a result, the Device Adapter phone cannot bridge to the call by using the term-x-gr button.

Example

Avaya Aura® CoS in System Manager

View Class Of Service (COS) Data

Edit Done

| System | na-cm03-046006 | Number | 15 |

General Options

- ☐ Ad-hoc Video Conferencing
- ☐ Automatic Callback
- ☐ Automatic Exclusion
- ☐ Buttonless Auto Exclusion
- ☐ Call Forwarding Busy/DA
- ☑ Call Forwarding Enhanced
- ☑ Call Forwarding All Calls
- ☐ Client Room
- ☐ Conference Tones
- ☐ Console Permissions
- ☐ Contact Closure Activation
- ☑ Data Privacy
- ☐ MOC Control
- ☐ Bridging Exclusion Override

- ☐ Extended Forwarding All
- ☐ Extended Forwarding Busy/DA
- ☐ Intra-Switch CDR
- ☐ Masking CPN/Name Override
- ☐ Off-Hook Alert
- ☐ Personal Station Access (PSA)
- ☑ Priority Calling
- ☐ Priority IP Video
- ☐ QSIG Call Offer Originations
- ☑ Restrict Call Fwd-Off Net
- ☐ Trk-to-Trk Transfer Override
- ☐ VIP Caller
- ☐ Match BCA Display to Principal

Edit Done

Comments on this document? infodev@avaya.com

Appendix K: CS 1000 FFC and Communication Manager FAC mapping

CS 1000 FFC and Communication Manager FAC mapping

This section provides a list of CS 1000 FFCs and the closest matches in Communication Manager FACs.

The following conditions do not indicate the absence of a service. The service can be available by using a feature key.

- A CS 1000 service uses an FFC, but a corresponding Communication Manager service is not supported by using an FAC.
- An Avaya Aura® service uses an FAC, but a corresponding CS 1000 service is not supported by using an FFC.

All features available on both CS 1000 and Communication Manager may not be listed in this section because of the following reasons:

- The service may differ significantly in user experience and may not map cleanly. For example, there may be a different number of required FACs versus FFCs, the feature is available but is invoked differently, or the feature has different confirmation responses.
- The service does not have a close enough match.

Example

Analog station autodial is currently not supported on Device Adapter. Therefore, FFCs and FACs are not required for analog stations.

However, both CS 1000 and Communication Manager support an autodial feature button. The configuration differences are not visible to the end user and the user operations are the same. Therefore, digital and IP station autodial is supported on Device Adapter by using the programmable feature button.

Example

Both CS 1000 and Communication Manager allow the user to have both internal and external call forward destinations and verify the settings. Some specific FFCs are defined to support this.

However, Communication Manager groups this under Enhanced Call Forward. The FAC operations to use them are different. The end result is the same, but invocation differs.

In this case, the FFCs and FACs for Call Forward are similar, but not identical.

If an FFC is not listed in this section, the FFC must be presumed to not map to an FAC.

⁎ **Note:**

For analog phones, Avaya Aura® does not have a corresponding FAC for the CS 1000 "Permanent Hold" FFC and the subsequent Retrieve operation. Hence, Device Adapter does not support the Permanent Hold and Retrieve operation on an analog phone. Instead, a user can perform hook-flash to hold and retrieve a call on a Device Adapter analog phone.

However, Device Adapter supports the hold and transfer, hold and conference, and hold and initiate a new call operations on an analog phone.

FFC and FAC comparable features with similar user experience

Specific features provided by FAC on Device Adapter are the same from the user experience perspective as the features provided by FFC on CS 1000. Whether a feature provides a user experience similar to CS 1000 or Avaya Aura® depends on how you configure the feature.

Note that the feature name may differ. For example, Send All Calls sends all calls to the indicated busy user coverage path, which allows the "user busy" tone. Make Set Busy sends all calls to the busy user coverage path or handling. The feature looks the same to the party that invokes the service and to the callers, although Send All Calls permits more forwarding options.

CS 1000 FFC	Matching FAC	Description
DSN Specific FFCs		
For more information, see Multiple Level Precedence and Preemption (MLPP) service in the Communication Manager documentation.		
AFTO	Flash Access Code	DSN flash precedence.
ATVF	Immediate Access Code	DSN immediate precedence.
ATVM	Priority Access Code	DSN priority precedence.
ATVP	Flash Override Access Code	DSN flash override precedence.
AVNR	Routine Access Code	DSN routine call.
Call Forward		
CFDD	Call Forward Deactivation	Call forward destination deactivation.
CFWA	Call Forward Activation All	Call forward all calls activate.
CFWD	Call Forward Deactivation	Call forward all calls deactivate.
Calling Party Privacy		
CPP	Per Call CPBN Blocking	Calling party privacy.
CPPO	Per Call CPBN Unblocking	Calling party privacy override.

Table continues…

CS 1000 FFC	Matching FAC	Description
Electronic Lock		
ELKA	Station Lock Activation	Electronic lock activate.
ELKD	Station Lock Deactivation	Electronic lock deactivate.
Hospitality		
RMST	Six separate FACs	Room status.
Make Set Busy		
MSBA	Send all Calls Activation	Make set busy activated.
MSBD	Send all Calls Deactivation	Make set busy deactivated.
Pickup (Call Pickup variants)		
PUDN	Directed Call Pickup	Pick up directory number.
PUGR	Directed Group Call Pickup	Pick up group.
PURN	Call Pickup	Pick up ringing number.
Redial Variants		
RDLN	Last Number Dialed	Redial last number.
Ring Again		
RGAA	Automatic Callback Activation	Ring again activate.
RGAD	Automatic Callback Deactivation	Ring again deactivate.
Speed Call		
SPCC	Abbreviated Dialing Group Programming	Speed call controller.
SPCE	Abbreviated Dialing Group Programming	Speed call erase.
SPCU	Abbreviated Dialing List 1/2/3	Speed call user.
Ungrouped Flexible Feature Codes		
AUTH	SA9105 Authorization Code Dialing Access Code	Used when entering an authorization code in the CS 1000 predial model.
SCPC	Station Security Code Change	Station control password change.
TFAS	Trunk Answer Any Station	Trunk answer from any station.

FFC and FAC features with some user experience differences

The following table lists the CS 1000 FFCs and the closest matches in Communication Manager FACs.

CS 1000 FFC	Matching Communication Manager FAC	Description
Automatic Wake-up		
AWUA	Automatic Wakeup Call	Automatic wake up activate. The Automatic Wakeup Call FAC is used to both activate and deactivate Automatic Wakeup Call.
AWUD	Automatic Wakeup Call	Automatic wake up deactivate. The Automatic Wakeup Call FAC is used to both activate and deactivate Automatic Wakeup.
AWUV	Verify Wakeup Announcement	Automatic wake up verify.
Call Forward		
CFDD	Call Forwarding Enhanced Deactivation	Call forward destination deactivation.
CFHO	Call Forwarding Enhanced Activation	Call Forward/HUNT override.
CFWA	Call Forwarding Enhanced Activation	Call forward all calls activate.
CFWD	Call Forwarding Enhanced Deactivation	Call forward all calls deactivate.
CFWV	Call Forwarding Enhanced Status	Call forward all calls verify.
ICFA	Call Forwarding Enhanced Activation	Internal call forward activate.
ICFD	Call Forwarding Enhanced Deactivation	Internal call forward deactivate.
ICFV	Call Forwarding Enhanced Status	Internal call forward verify.
Call Park For the closest match, the system uses the Avaya Breeze® platform Call Park and Page. However, an additional service exists on Communication Manager with a similar user experience, driven by FACs. For more information about the Call Park and Page Snap-in, see the Avaya Breeze® platform documentation. For more information about Communication Manager Call Park and parked call retrieval, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.		
CPRK	Call Park Access Code	Park an active call that can then be retrieved from a different station by using the answer back access code. CS 1000 automatically proposes a system Call Park extension to use, and you need not specify an extension on which to park the call. For Communication Manager, you must specify the extension on which to park the call.

Table continues…

CS 1000 FFC	Matching Communication Manager FAC	Description
CPAC	Answer Back Access Code	Retrieve parked calls. If no one answers the call before a system-wide expiration interval expires, the system redirects the call.
Group Hunt		
GHTA	Hunt Group Busy Deactivation	Group hunt termination allowed.
GHTD	Hunt Group Busy Activation	Group hunt termination disallowed.
Mobility features		
Comparable capability exists with the EC500 (Extension to Cellular), with Avaya Aura® Release 8.1.2. If a transfer or conference is initiated with two separate FFCs on CS 1000 and one on Communication Manager, Communication Manager separates the two services on completion by using two separate FACs. This requires the following: • The signaling group must be configured as using DTMF over IP as rtp-payload. • The off-pbx-telephone must be set to include feature invocation by in-call DTMF in the configuration set. • The gateway that provides the trunk for the call must be of an acceptable version.		
MCAN	Cancel current call	Cancel a Transfer or Conference from a mobile phone.
MCFA	Hold and initiate new call	CS 1000: Activate a Conference from a mobile phone.
MCOM	Transfer complete or Conference complete	Complete a Conference or Transfer from a mobile phone. Communication Manager uses two separate FACs to carry out this operation.
MTGL	Toggle with held call	Enables a mobile phone to toggle between the two parties in a Conference or Transfer.
MTRN	Hold and initiate new call	CS 1000: Activate the Mobile Extension transfer feature.
Redial Variants		
RDST	Saved Number Redial	Redial store. Save a specific number for redial later.
RDSN	Saved Number Redial	Redial saved number.

CS 2100

From Avaya Device Adapter Release 8.1.3 onwards, you can use Device Adapter to manage phones migrated from CS 2100 product.

The configuration required for Avaya Aura® and Device Adapter for the phones migrated from CS 2100 product is identical to that of migrated CS 1000 phones. The CS 2100 product supports the following components and these components will be supported on Device Adapter in the same way as CS 1000 after migration.

- IPE shelves
- Digital cards
- Analog cards
- UNISTim devices

Appendix L: Hardware requirements for migration

Hardware requirements for migration

In general, the hardware of a CS 1000M (TDM-based CS 1000) or Meridian 1 (precursor to the CS 1000) can migrate to CS 1000E. CS 1000E is the CS 1000 with entire IP connection between the controlling server and the analog and digital line cards. Devices that migrate to a CS 1000E can migrate to Device Adapter with the caveat that trunking hardware is not needed and a few specific additions, such as the attendant consoles, are not used.

The first two topics in this section provide information about additional hardware, including cables, needed to migrate from the Meridian 1 and CS 1000M to Device Adapter. Note that these hardware elements should already be present in a CS 1000E, although the vintage may need to be changed. That is, if a specific card such as an MG-XPEC is a lower vintage than the supported card, the card must be replaced with the supported card. Any additional associated cards, such as the XSM, or cables need to conform as well.

Large system specific cards to migrate TDM to IP

The following cards, and cables or cable kits are necessary to permit the CS 1000 or Meridian 1 Intelligent Peripheral Equipment (IPE) TDM shelf to migrate to IP. This is an essential requirement to allow the shelf to be controlled through Device Adapter.

> **Note:**
>
> IPE shelves that are already migrated to provide call signaling and media over IP do not need to add additional equipment. It is not necessary to change an existing MG-XPEC because they are all pre-loaded with sufficient DSP ports.

Applicable hardware

Customers with a mix of versions from the supported list can use Device Adapter. The E5 and E6 vintages of certain items are cards or cables that are:

- Made with lead-based solder; and therefore, only partly ROHS compliant (E5).
- Made without lead-based solder; and therefore, fully ROHS compliant (E6).
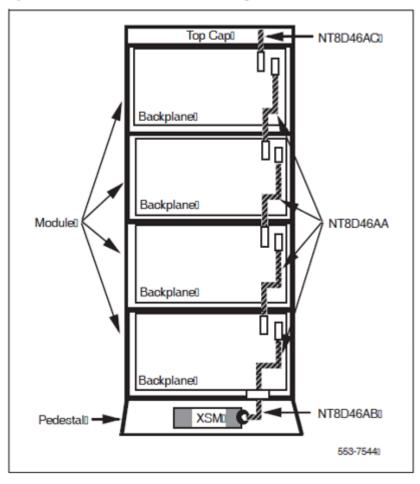
Because there is no functional difference, they can be intermingled successfully. Although, manufacturing of the E5 is discontinued.

Part code	Part description	Status
Parts that are currently available.		
NTDW20AAE6	Media Gateway Extended Peripheral Equipment Controller (MG-XPEC) The MG-XPEC card replaces the NT8D01 XPEC controller card, NT1P62 Fiber XPEC controller card, or NT7R52 Remote Carrier Interface card in the controller slot of an NT8D37 IPE module for CS 1000M. MG-XPEC has two onboard DSP DBs that provide 192 channels.	Available
NTDW25AAE6	MG-XPEC Network and TTY cable kit. The contents include: • Two new IO Panels • Two NTDW26ABE6 TTY Cables (Pin out same as MG1010) • Eight Cat-5e Ethernet cables • Twelve RJ45 couplers • One Card Slot label	Available
NTDW26ABE6	MG-XPEC TTY cable (CABLE, MG-XPEC TTY PORTS) This is included in the NTDW25AAE6 kit.	Available
NTDW26BAE6	MG-XPEC XSM cable (CABLE, MG-XPEC XSM PORT)	Available
NT8D22AEE6	Extended System Monitor (XSM), lead-based solder free.	Available
Parts no longer manufactured, but still supported for Device Adapter.		
NTHU70AA	MG-XPEC AND CABLING KIT Dependent on whether the MG-XPEC version is E5 or E6.	MD
NT8D22AEE5	Extended System Monitor, lead-based solder used.	MRSD
Cables and kits sold with the E5	Lead-based solder used.	MRSD
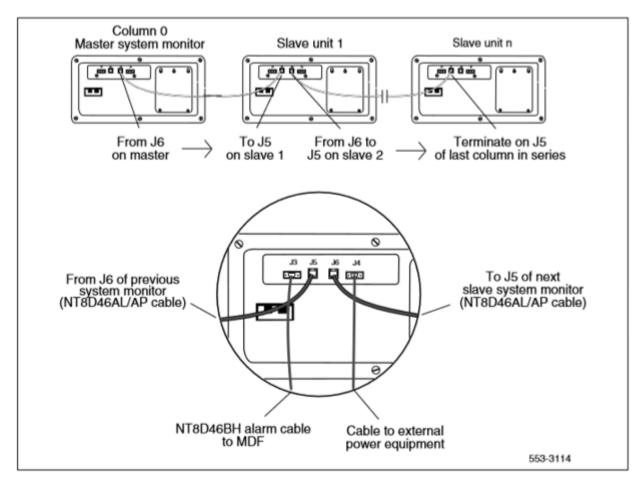
The XSMs in multiple groups on a large CS 1000 typically have a single XSM acting as the master, which is connected to the MG-XPEC. The remainder of the XSMs chain to pass signaling to the master.

The following figure shows cabling within a column. All shelves in the column have their backplanes linked to allow a single XSM in the base to signal faults and alarms.

System monitor module-to-module cabling

The different columns connect in a chain, with the master XSM reporting to the MG-XPEC, the status of itself and the different slave XSMs.

553-3114

Only the master needs to be the indicated vintage. Older XSM subordinate cards at subordinate unit 1 and higher can connect to the master through the J5 to J6 connections, but only the master (NT8D22AEE5 or NT8D22AEE6) can signal to the MG-XPEC and pass alarms and ringing generator messages correctly.

On the NT8D22AE XSM card, ensure the following:

- Switch SW1-1 is set to Off.
- Switch SW2-2 is set to On.

Switches SW1-1 and SW2-2 are on the NT8D22AE XSM card, both E5 and E6.

Device Adapter provides support for sending SNMP traps to System Manager for alarms on the MG-XPEC shelves. Specifically, Device Adapter sends XSM and PSTAT signals to System Manager. Therefore, if some event happens with PSTAT or XSM, the administrator should examine the alarm in System Manager in **Services** > **Events** > **Alarms**.

Related links

MG-XPEC installation

The CS 1000 documentation has detailed procedures to install the MG-XPEC. The *Communication Server 1000E Installation and Commissioning* guide for release 7.6 includes a section on replacing the XPEC (TDM interface) with MG-XPEC.

For more information, see the "Media Gateway Extended Peripheral Equipment Controller (MG XPEC)" section in the *Communication Server 1000E Installation and Commissioning* guide. Specifically, the "Installation and Commissioning" section contains information about the process of connecting the cables and installing the circuit board. This explicitly requires NTDW26BAE6 to connect the new vintage of the NT8D22 XSM to the MG-XPEC.

The circuit card reference (*Circuit Card Reference Avaya Communication Server 1000*) for release 7.6 includes information about the settings of the switches on the cards.

- For information about switch settings on the XSM, see "NT8D22 System Monitor" in Chapter 7: Option Settings. It also contains a short description about daisy chain of XSM cards. For more information about these settings along with additional details, see the *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* guide.

- For more information about MG-XPEC, see "Chapter 37: NTDW20 Media Gateway Extended Peripheral Equipment Controller card." However, MG-XPEC is not configured by switches, so the reference is more for background information and information about the faceplate LED display rather than installation and commissioning.
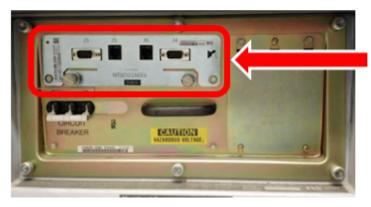
The *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* guide for installation of large systems includes the procedure for the XSM.

- Specifically, see the "Configuring the System Monitor" section for the procedure to configure the system monitor (XSM, NT8D22). This includes the settings of the different switches on the card.

    The following picture shows the back of the pedestal base after it is opened.

Pedestal base, with the cover removed to see the power switch and XSM in proximity

Extended System Monitor card

Related links

[Large system specific cards to migrate TDM to IP](#) on page 639

Cards required to migrate TDM chassis and cabinets to IP

The following cards, and cables or cable kits are necessary to allow the CS 1000M or Meridian 1 small system (Option 11) chassis or cabinet to migrate to Device Adapter.

✴ **Note:**

Chassis or cabinet that is already migrated to provide call signaling and media over IP do not need to add additional equipment. It is not necessary to change an existing MGC, although it may be necessary to add DSP resources if cards are moved in the system. For example, if an administrator replaces four cards used for trunks with four cards for analog or digital stations, there may be an increase in the required DSP ports.

Applicable hardware

Customers with a mix of versions from the supported list can use Device Adapter. The E5 and E6 vintages of certain items are cards or cables that are:

- Made with lead-based solder free; and therefore, not ROHS compliant (E5).

- Made without lead-based solder; and therefore, fully ROHS compliant (E6).

Because there is no functional difference, they can be intermingled successfully. Although, manufacturing of the E5 is discontinued.

Part Code	Part Description	Part Description
Parts currently available.		
NTDW60BAE5	MGC - Gateway Controller Provides a gateway controller for MG1000E IP media gateways in a CS 1000E system. Has two DB expansion sites that can be installed with DB32, DB96, and DB128 boards.	See NTDW98AAE6 later in this section.
NTDW98AAE5 NTDW98AAE6 NTDW98AAGS	MGC w/metal faceplate Provides a gateway controller for MG1000E IP media gateways in a CS 1000E system. Has two DB expansion sites that can be installed with DB32, DB96, and DB128 boards.	MRSD Available Available
NTDW78AAE5 NTDW78AAE6 NTDW78AAGS	MGC DSP Daughterboard 128 ports	MRSD Available Available
Parts no longer manufactured, but still supported for Device Adapter.		
NTDW62AAE5 NTDW62AAGS	MGC DSP Daughterboard 32 ports	End of Sale End of Sale
NTDW64AAE5 NTDW64AAGS	MGC DSP Daughterboard 96 ports	End of Sale End of Sale

Device Adapter provides support for sending SNMP traps to System Manager for alarms on the MGC chassis and cabinets. Specifically, Device Adapter sends XSM and PSTAT signals to System Manager. Therefore, if some event happens with PSTAT or XSM, the administrator should examine the alarm in System Manager in **Services** > **Events** > **Alarms**.

Related links

MGC installation

The CS 1000 documentation has detailed procedures to install the MGC. The *Communication Server 1000E Installation and Commissioning* guide for release 7.6 includes a section on replacing the XPEC (TDM interface) with the MGC.

For more information, see the "Installing and connecting Avaya CS 1000E hardware" chapter. Specifically, the "Installing Server cards and Gateway Controller cards" section, "Gateway Controller installation" subsection includes a procedure ("Procedure 24 Installing the MGC card") that contains information about the process of connecting the cables and installing the circuit board.

The circuit card reference (*Circuit Card Reference Avaya Communication Server 1000*) for release 7.6 includes information about the settings of the switches on some cards, but the MGC does not have physical switches.

- For more information about MGC, see "Chapter 36: NTDW60 Media Gateway Controller Card." However, the MGC is not configured by switches, so the reference is more for background information and information about the faceplate LED display rather than installation and commissioning.

- Information about the NTDW98 MGC is covered in "Chapter 36: NTDW60 Media Gateway Controller Card." The card is functionally identical but has improved EMC containment.

- For information about the DSP daughterboards used on the MGC, see "Chapter 41: NTDW62, NTDW64, and NTDW78 Media Gateway Controller Daughterboards."

Related links

[Cards required to migrate TDM chassis and cabinets to IP](#)

Additional NT8D37 IPE shelf hardware

You can reuse a majority of IPE line cards and hardware from the shelves. For example, CS 1000 supports all versions of the NT5K02 Flexible Analog Line Card. If CS 1000 is using a specific version of NT5K02 Flexible Analog Line Card, then CS 1000 will be incompatible with the earlier versions of the NT5K02 Flexible Analog Line Card. Incompatibility with CS 1000 results in a corresponding incompatibility with Device Adapter.

If you experience any problem while using a specific vintage card, you can fix the problem by using a later version of the card. If you migrate the lower vintage, then the problem will remain on the card after migrating to Device Adapter. This issue potentially applies to any card or cards in the IPE shelf. However, most customers upgrade the hardware to the versions that meet their needs, and the cards in their systems should not have any issues. The cards may not be upgraded to get additional feature content, though.

For Device Adapter, you can use any version of NT8D37 IPE shelf. The existing hardware on the shelf should be sufficient for Device Adapter. but the shelf requires a compatible power equipment. The power equipment may be AC or DC powered, as applicable, and this can affect other cards and devices.

IPE shelves used for Carrier Remote and Fiber Remote have the following caveat:

- If Carrier Remote is using the NT8D37 IPE module, you can migrate the NT8D37 IPE module to Device Adapter. You must replace the Remote Carrier Interface card with MG-XPEC.

Ensure that you install an IP infrastructure instead of the T1 or E1 carrier links. T1 and E1 carrier links that are used in Carrier Remote IPE do not support IP.

- If Fiber Remote is using the NT8D37 IPE module, you can migrate the NT8D37 IPE module to Device Adapter. You must replace the Fiber Controller Card with MG-XPEC.

  Ensure that you install an IP infrastructure instead of the fiber links. Fiber Remote IPE uses an optical fiber connection which may or may not support IP.

You cannot migrate trunk cards, including music and recorded announcement trunk cards, and conference resources to Device Adapter. However, the following line cards can migrate:

Line Card	Comments
NT5K02	Flexible Analog Line Card with high and low voltage Message Waiting lamp option with a number of localized card variants.
NT5K96	Flexible Analog Line Card (XFALC) with a number of localized card variants.
NT5D49AA	Analog Message Waiting Line Card (Brazil).
NT7K20	Global Analog Line Card (GALC) with high and low voltage Message Waiting lamp option.
NT8D09 NT8D09BB	Analog Message Waiting Line Card.
NTRA04AA	Flexible Message Waiting Line Card (China).
NTRA05AA	Flexible Analog Line Card (China).
NTRA08: NTRA08AA NTRA08AB	Flexible Analog Line Card (China).
NT8D02	Digital Line Card supported in CS 1000E, CS 1000M, and Meridian 1.

The following hardware and cards are also reused:

Card and other hardware components	Comments
NT8D21	A ringing generator for AC systems. This ringing generator is required for analog telephones. Any XSP connected directly to the MG-XPEC must be of Release E5 or E6 of the NT8D22AE Extended System Monitor (XSM) card. XSP of any release other than E5 or E6 disables the ringing generator.
NT6D42	A ringing generator for DC systems. This ringing generator is required for analog telephones. Any XSP connected directly to the MG-XPEC must be of Release E5 or E6 of the NT8D22AE Extended System Monitor (XSM) card. XSP of any release other than E5 or E6 disables the ringing generator.
Power Supply	Power supply is regionally dependent and can be AC or DC.
Other hardware components	Pedestals, mount kits, and other hardware that are already in use.

Non-NT8D37 IPE shelf hardware

Generically, systems that do not use the NT8D37 IPE shelf derived from products that used a main cabinet (with the CPU) and added more cabinets as expansion cabinets to provide larger systems. Eventually, rack-mountable variants referred to as main or expansion chassis were created. Although, the main versus expansion description for the cabinet is sometimes functional. The same cabinet hardware can be a main cabinet or expansion cabinet based on its use. However, the chassis serves as a main cabinet, and the chassis expander as an expansion cabinet equivalent.

A majority of IPE line cards and hardware from the chassis and cabinets can be reused. For example, there is no specific version of the NT5K02 Flexible Analog Line Card that is supported. All are supported. If a specific version is indicated, this indicates incompatibility of lower versions with CS 1000, as opposed to with Device Adapter.

Any problem in a specific vintage card that may be fixed in a higher version of the card will remain on the card after migrating to Device Adapter. This applies to the IPE shelf. However, most customers upgrade the hardware to versions that meet their needs. The cards may not have been upgraded to get additional feature content, though.

The systems use a number of cabinets and chassis. However, the following are explicitly not supported:

- NTAK12
- NTDK50

These do not support the MGC and must be replaced by an NTAK11 cabinet if you want to retain the users' stations.

The following chassis and cabinet equivalents, including chassis expanders as applicable, to an NT8D37 IPE shelf are supported:

Chassis and cabinet	Comments and description
NTAK11	Small system cabinet. The most common form factor for small systems. Houses the MGC and 10 IPE cards.
NTC310AAE6	Media Gateway 1010 Chassis. Houses a dedicated MGC slot and slots for 10 IPE cards. The NTC314AAE6 Utility Card is also supported.
NTDK91BB	A four IPE card chassis that supports the MGC and up to four IPE cards. However, the card in slot 4 may be an NTDK16 digital line card, allowing up to 48 stations, emulating digital line cards in slots 4, 5, and 6.
NTDK92 Chassis Expander	Connects to the NTDK91 chassis to provide additional line capacity. NTDK92 supports any IPE cards in slots 7, 8, 9, and 10.
NTDU14CA	Houses the MGC and four IPE line cards.
NTDU15CA Chassis Expander	Provides four additional universal card slots for the NTDU14 chassis for additional capacity.

Trunk cards, including music and recorded announcement, and conference resources are not migrated to Device Adapter. However, the following line cards can migrate:

Line card	Comments
NT5K02	Flexible Analog Line with high and low voltage Message Waiting lamp option with a number of localized card variants.
NT5K96	Flexible Analog Line Card (XFALC) with a number of localized card variants.
NT5D49AA	Analog Message Waiting Line Card (Brazil).
NT7K20	Global Analog Line Card (GALC) with high and low voltage Message Waiting lamp option.
NT8D09, NT8D09BB	Analog Message Waiting Line card.
NTRA04AA	Flexible Message Waiting Line Card (China).
NTRA05AA	Flexible Analog Line Card (China).
NTRA08: NTRA08AA NTRA08AB	Flexible Analog Line Card (China).
NT8D02	Digital Line card supported in CS 1000E, CS 1000M, and Meridian 1.
NTDK16	Digital Line card with 48 ports. Supported in small system Chassis system. Not supported for NT8D37 shelf or NTAK11 cabinet.

The following hardware and cards are also reused:

Card and other hardware components	Comments
NT8D21	A ringing generator for AC systems. This ringing generator is required for analog telephones. It requires Release E5 or E6 of the NT8D22AE Extended System Monitor (XSM) card. Otherwise, the ringing generator is disabled.
NT6D42	A ringing generator for DC systems. This ringing generator is required for analog telephones. It requires Release E5 or E6 of the NT8D22AE Extended System Monitor (XSM) card. Otherwise, the ringing generator is disabled.
Power Supply	Power supply is regionally dependent and can be AC or DC.
Other hardware components	Pedestals, mount kits, and other hardware that is already in use.

NT1R20 Off-Premise Station Analog Line card

About NT1R20 Off-Premise Station Analog Line card

Introduction

The NT1R20 Off-Premise Station (OPS) Analog Line card is an intelligent eight-channel analog line card designed to be used with 2 - wire analog terminal equipment such as analog (500/2500 – type) telephones and analog modems.

The NT1R20 OPS analog line card provides eight full-duplex analog telephone line interfaces. Each line has integral hazardous and surge voltage protection to protect the system from damage due to lightning strikes and accidental power line connections. This card is normally used whenever the phone lines leave the building in which the switch is installed.

The NT1R20 OPS analog line card provides:

- Line supervision
- Hook flash
- Battery reversal

An administrator can install this card in any IPE slot.

Electrical characteristics

Characteristic	Specification
Terminal Impedance (TIMP)	600 ohms, 900 ohms
Balance Impedance (BIMP)	600 ohms, 900 ohms, 3COM, 3COM2

⊛ **Note:**

The default value of TIMP and BIMP is 600 ohms.

The combination of TIMP/BIMP for a default and an invalid configuration is 600/600.

Configuring NT1R20 OPS analog line card

Procedure

1. Log on to System Manager by using administrative credentials.

2. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints**.

3. Click **Manage Endpoints**.

4. On the Endpoints page, select the endpoint for which you want to configure the NT1R20 OPS analog line card, and then click **Edit**.

5. On the Edit Endpoint page, on the **General Options** tab, in the **Features** field, configure the mnemonic for NT1R20 OPS analog line card specifications.

For example, TIMP900 BIMP900 ONS.

The default value of TIMP and BIMP is 600 ohms.

The invalid combinations of TIMP/BIMP are 600/900 and 900/600, all the other combinations of TIMP/BIMP are valid.

The combination of TIMP/BIMP for a default and an invalid configuration is 600/600.

The available options are:

- TIMP600
- TIMP900
- BIMP600
- BIMP900
- BIMP3COM2
- BIMP3COM

6. Click **Commit** to save the changes.

Extended System Monitor support for Device Adapter

Extended System Monitor (XSM) on a CS 1000 system works as follows:

- The CS 1000 system uses MGC-XPEC.
- The serial connection to the XSM modules uses the MGC remote TTY feature.
- The remote TTY feature passes the serial data to the call server through a MGC. The MGC does not have any configuration to process the XSM messages.

On a CS 1000 large system, you must program the XSM interface as a remote TTY on overlay 17. To check the status of XSM on the CS 1000 system, you must put overlay 37 into the background routines or the nightly routine.

XSM on a Device Adapter works as follows:

- Device Adapter does not support remote TTY feature, so MGC-XPEC supports XSM feature but the call server does not support the XSM feature.
- Device Adapter does not support any configuration of MGC-XPEC.
- When you reboot MGC-XPEC, it checks if an XSM device is present. If the device is present, MGC-XPE prints an info message and then automatically starts a background audit.

  MGC-XPEC checks the status of the XSM device every hour by sending a query. When the XSM device responds, Device Adapter receives an SNMP trap and forwards the SNMP trap to System Manager.

- If the XSM device is not present, MGC-XPEC prints an error message and disables all XSM functionality on the XSM card.

> **Note:**
>
> - To add any other XSM device to MGC-XPEC later, you must reboot the MGC.
> - The functionality of the XSM feature on Device Adapter and CS 1000 is the same.

Appendix M: Additional security information for Avaya Device Adapter Snap-in

Certificate management

Device Adapter uses certificates that are installed on Avaya Breeze® platform to establish mutually authenticated TLS/DTLS sessions.

SECURITY_MODULE_SIP identity certificate and trusted CA certificates provide secure communication with the following elements:

- SIP/TLS connections to Session Managers.
- HTTPS connections to Session Managers for PPM services.
- HTTPS connections to Avaya Aura® Device Services.
- DTLS connections from UNIStim endpoints.

SECURITY_MODULE_HTTP identity certificate and trusted CA certificates provide secure communication with the following element:

- HTTPS connections from Device Adapter Element Manager on Session Manager.

Activate a new Identity Certificate

After you activate a new Identity Certificate on Avaya Breeze® platform, you must restart Avaya Breeze® platform. Reinstallation of Device Adapter is not required.

Within 5 minutes after you upload the new certificates for Avaya Breeze® platform on System Manager, Device Adapter automatically applies the new certificates and restarts the dsa, tps, and csv services.

> ✱ **Note:**
>
> This is service impacting. Avaya recommends that you activate the new Identity Certificate and restart Avaya Breeze® platform during the maintenance window to minimize the impact on endpoint registration and call handling.

For information about replacing an Identity Certificate and restarting the Avaya Breeze® platform, see the *Administering Avaya Breeze® platform* guide.

Activate and deactivate trusted CA certificates

After you activate or deactivate trusted CA certificates on Avaya Breeze® platform, you need not restart Avaya Breeze® platform or reinstall Device Adapter.

Within 5 minutes after you activate or deactivate a trusted CA certificate on Avaya Breeze® platform, Device Adapter automatically applies the changes and restarts the dsa, tps, and csv services.

> ✱ **Note:**
>
> This is service impacting. Avaya recommends that you activate or deactivate trusted CA certificates on Avaya Breeze® platform during the maintenance window to minimize the impact on endpoint registration and call handling.

For more information about adding and removing trusted CA certificates on Avaya Breeze® platform, see *Administering Avaya Breeze® platform* guide.

Reinstalling Device Adapter

About this task

Reinstalling Device Adapter impacts the service. Avaya recommends that you allow a maintenance window of approximately 20 minutes to reinstall Device Adapter.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Service Management**.

2. Click **Services**.

3. On the Services page, click the appropriate Device Adapter, and then click **Uninstall**.

4. Click the appropriate Avaya Breeze® platform cluster, and then click **Commit**.

5. Click the Device Adapter that you installed in the preceding step, and then click **Install**.

6. Click the appropriate Avaya Breeze® platform cluster, and then click **Commit**.

Passwords for administrative accounts

Avaya Breeze® platform

Avaya Breeze® platform controls the SSH accounts.

Media gateways

MGC supports only local authentication by using two accounts: admin2 and pdt2. MGC does not support central authentication. MGC does not have an enrollment relationship with System Manager.

Setting passwords for the admin2 and pdt2 MGC accounts

About this task

The default passwords for the admin2 and pdt2 accounts are the same as the CS 1000 passwords. The account name and password information is stored securely on the MGC.

CLI access is done over serial port and SSH. Insecure shells rlogin / telnet are disabled.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

2. Click **Attributes**.

3. On the Attributes Configuration page, click the **Service Clusters** tab.

4. In the **Cluster** field, click the appropriate cluster.

5. In the **Service** field, click **DeviceAdapter**.

6. Navigate to the **Media Gateway Accounts** area.

7. In the **admin2 Password** field, in **Effective Value**, type the password for the admin2 account.

8. In the **pdt2 Password** field, in **Effective Value**, type the password for the pdt2 account.

9. **(Optional)** To override the default values, select the **Override Default** check box.

Phone authentication

Digital and analog phones do not support user authentication. Their physical slot defines the TN that is required to register the phone.

UNIStim phone registers by specifying the node ID and TN number. The node ID can be of maximum four digit length. You can configure the node ID in the **Node ID** attribute on System Manager. In the background, Device Adapter registers the phone as regular SIP endpoint by using the Communication Profile password. The Communication Profile Password is obtained from the System Manager database which has a replica on the Avaya Breeze® platform server. Other SIP stations cannot log in to the same extension until the end user knows the Communication Profile password.

You can protect the Node ID/TN login form with a node pin. You can set the node pin by using the `nodePwdEnable/nodePwdSet` CLI commands. The node pin can be of 6 to 14 digits length. You can run the command at any Avaya Breeze® platform server. Changes apply to all servers in a cluster immediately. The pin is stored in PPM.

You can use the Protection Mode feature to protect access to Personal Directory on UNIStim phone. The Protection Mode feature is accessible through the Phone menu. The entered password is verified against the Communication Manager Station Security Code. Device Adapter supports password guessing protection when access to Personal Directory is locked for one hour if a user enters a wrong password (Communication Manager Station Security Code) three times. The number of attempts and timestamp of the lock is stored in PPM. Administrators can reset the lock by using the **Unlock the user's SCPW** option.

You can also protect Personal Directory for digital M39xx phones with a password. The password is stored in the phone EEPROM. This is a legacy behavior.

Media security

The Media Security feature of Device Adapter is used to secure audio speech path for UNIStim, digital, and analog endpoints by using SRTP.

Media security configuration consists of the following three parts:

- Configuring Communication Manager IP codec set.
- Configuring the **Media security policy** attribute on System Manager.
- Configuring the **Secured number of packets (NKEY)** and **Session key validity time (TKEY)** attributes on System Manager.

Configuring CM IP codec set

About this task

Device Adapter supports only the AES_CM_128_HMAC_SHA1_80 cipher suite, which is implemented in Communication Manager as the 1-srtp-aescm128-hmac80 media encryption option. This is one of the five media encryption options that are currently available on Communication Manager. To permit media security to use the right encryption, the Communication Manager 1-srtp-aescm128-hmac80 media encryption option must be set.

Procedure

1. Set the Media Encryption section to contain: `1-srtp-aescm128-hmac80`

2. Set Encrypted SRTCP to: `enforce-enc-srtcp`

> **Note:**
>
> Device Adapter supports SRTCP with SRTP, and RTCP with RTP. A combination of either SRTP and RTCP or RTP and SRTCP is not supported.
>
> For example, if SRTCP is used with RTP, calls still go through, but RTCP reports do not work.

Setting the media security policy

About this task

You can configure the media security policy at a global, cluster, or service profile level. The service profile level is used to configure the media security policy for a single endpoint or a group of endpoints.

Modifying the media security policy does not require a Device Adapter snap-in restart.

The 2004 phase 0 and phase 1 UNIStim phones do not support Media Security. Hence, registration is rejected if Media security is set to Always for these phones.

The following are the supported protocols for each media security policy type:

- **Off**: SRTP is disabled for endpoints.
- **Best-effort**: SRTP is preferred.
- **Always**: Only SRTP is possible. RTP is disabled.

The **Secured number of packets (NKEY)** and **Session key validity time (TKEY)** attributes define near-end SRTP key lifetime.

The lifetime is presented in SIP SDP offer/answer and expressed in 2^x packets.

For example,

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:32
```

In the preceding example, the key length is 2^20 == 1 048 576 packets

The **Session key validity time (TKEY)** attribute is used to calculate the number of packets (2^x) by using the maximum length of time and a negotiated codec. You can configure the maximum length of time (TKEY attribute) between 8 to 168 hours. The default is 24 hours.

The **Secured number of packets (NKEY)** attribute is used as top margin. It is expressed in 2^x, where x is 16 to 31. The default is 31. If the lifetime calculated by using the **Session key validity time (TKEY)** attribute is greater than NKEY, then the NKEY value is set as the lifetime.

For example,

TKEY = 24 hours

NKEY = 20 (power of 2)

codec = G729A, 30ms

Lifetime based on TKEY and G729/30ms codec is 2 937 600 packets == 2 ^ 21.

NKEY(20) is less than 21, thus the resulting lifetime is 2^20.

When the SRTP key is about to expire during a call, UNIStim phone/VGW channel notifies Device Adapter. Device Adapter sends a new SDP offer with a newly generated master key. The feature is automatic and does not require any provisioning.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

2. Click **Attributes**.

3. Depending on the level for which you want to configure the media security policy, click the **Service Profiles**, **Service Clusters**, or **Service Globals** tab.

4. In the **Service** field, click **DeviceAdapter**.

5. On the Attributes Configuration page, navigate to the **Media Security** group and do the following:

   a. In the **Media security policy** field, in **Effective Value**, click the media security policy.

      The options are: **Off**, **Best-effort**, and **Always**.

      Default value is **Off**.

   b. In the **Secured number of packets (NKEY)** field, in **Effective Value**, type the number of packets secured.

      Valid values are 16 through 31.

      Default value is 31.

   c. In the **Session key validity time (TKEY)** field, in **Effective Value**, type the session key validity time in hours.

      Valid values are 8 through 168 hours.

      Default value is 24 hours.

6. **(Optional)** Select the **Override Default** check box to override the default values.

7. Click **Commit**.

Related links

[Media security feature operation](#) on page 658

Media security feature operation

Media security is obtained using Secure RTP (SRTP) and Secure RTCP (SRTCP). SRTP encrypts the media content based on a secure key and SRTCP provides statistics and control operations.

There is no user-specific action to use SRTP. Device Adapter and intervening servers negotiate a media stream that conforms to the RTP and SRTP requests in the SDP of the INVITE.

- If the SDP in the INVITE is RTP only, then the call either completes as RTP end-to-end or the call fails.

- If the SDP in the INVITE is SRTP only, then the call either completes as SRTP end-to-end or the call fails.

- If the SDP has both SRTP and RTP, the call attempts to complete as SRTP, but falls back to RTP if necessary.

Related links

[Setting the media security policy](#) on page 657

[Media Security (RTP versus SRTP)](#) on page 694

Firewall

Viewing the service ports for Device Adapter snap-in

About this task

Device Adapter snap-in lists the required TCP and UDP ports as the Avaya Breeze® platform service ports.

Additionally, Device Adapter snap-in opens the following ports when the **Enable legacy loadware upgrades** attribute is enabled.

- TCP port 20, 21 for FTP.
- TCP/UDP port 111 for sunrpc.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze®** > **Configuration**.

2. Click **Service Ports**.

3. On the Service Ports page, in the **Service** field, click the Device Adapter service.

4. In the **Cluster** field, click the appropriate cluster.

   The service ports are displayed on the Service Ports page.

Media Gateway port configuration

MGC supports legacy VxWorks-based firewall also known as Port Access Restrictions.

You can administer the feature through CLI commands only. No GUI interface is provided. Use the `portAccessHelp` CLI command to view the Help.

Configuration is done on each MGC. You cannot configure system-wide parameters.

The feature has three states:

- Off: Firewall is not active.
- Default: Firewall runs default configuration.
- Custom: Firewall runs custom configuration.

The default configuration is to allow the following incoming connections:

Protocol	Port number	Service
TCP	22	SSH
TCP	15000	PBX link
UDP	500	IPSec IKE
UDP	15003	RUDP HB

Custom configuration is read from the `/u/db/customport.xml` file, which should be manually uploaded by an administrator.

Upgrade from CS 1000 to Device Adapter MGC loadware does not change the firewall state. If you are migrating MGCs that run a custom firewall configuration, you must allow UDP port 15003.

The DSP ports are handled by the DSP and are not covered by the firewall.

Device Adapter compliance with FIPS 140-2 standard

Device Adapter complies with Federal Information Processing Standards Publication (FIPS) 140-2, Security Requirements for Cryptographic Modules, which specifies the security requirements that are to be met by the cryptographic modules. These cryptographic modules are used within the security system to protect sensitive information within a computer and telecommunications systems, including voice systems.

The TPS and CSV components of the Device Adapter Snap-in SVAR file contain Mocana version 6.5 with FIPS 140-2 compliant Cryptographic module.

The Avaya Breeze® platform Release 3.7, on which, Device Adapter is deployed, uses the OpenSSL Cryptographic Module and OpenSSL itself in FIPS mode. DSA, CSDK, TPS, CSV, and PD use OpenSSL.

Device Adapter supports the following CS 1000 UNIStim IP phones:

- 11xx series: 1110, 1120E, 1140E, 1150E, and 1165E
- 12xx series: 1210, 1220, and 1230
- 2004 phase 0, 1, and 2
- 2007
- i2050 softphone

> ✳ **Note:**
>
> Only the 11xx and 12xx series IP phones on Device Adapter are FIPS 140-2 compliant.

Device Adapter automatically upgrades the firmware to version 5.5.9 on the 11xx and 12xx series phones when these phones first register to Device Adapter. This firmware contains Mocana DTLS library version 6.5, with Cryptographic module, which is FIPS 140-2 compliant. Mocana DTLS library version 6.5 is used by the TPS and CSV applications.

> ✳ **Note:**
>
> MGC does not comply with FIPS 140-2. MGC uses Mocana version 5.1 for IPSec, SSH, and SFTP. Mocana version 5.1 is not FIPS compliant.

Appendix N: Location-based operations

Location-based operations

Avaya Device Adapter Snap-in uses the following features of Avaya Aura® Session Manager to perform tasks:

- Avaya Device Adapter Snap-in is considered a trusted endpoint by Avaya Aura® Session Manager. This means that Session Manager does not challenge SIP requests coming from Avaya Device Adapter Snap-in using end-to-end TLS.

- Avaya Device Adapter Snap-in indicates the signaling location of a call by the IP address located in the **Via** header of the INVITE request. Signaling locations must be administered using IP address patterns.

- Avaya Device Adapter Snap-in indicates the media location of a call by the IP address located in the SDP.

The location referred above has an implication to the personnel performing the migration and maintaining the Device Adapter clusters.

A simple example will illustrate this requirement.

Example

- Assume that subnet `10.138.46.1` is in Miami, Florida, and `10.138.47.1` is in Berlin, Germany.

- All emergency (911 or equivalent) calls need to route to the applicable Public Service Answering Point (or equivalent), regardless of where the user logs in.

- If Alice logs in at the Miami site, any 911 call must go to Miami. If Alice travels to Berlin and logs in there, even if Alice dials 911 and not the German emergency code, the call should route to emergency services in Berlin.

This requires three levels in the hierarchy of configuration:

- Location: The location of the site must be defined in the "locations" data, in order to permit calls to get different routing based on the city in question.

- Network Region: Each location will have one or more network regions. As an example, a university may have multiple campuses, each campus may have multiple buildings, and large buildings may have multiple floors.

- Network address map: Programming depends on the desired granularity. Each IP address in the table maps to a suitable network region.

  The IP address may represent an IP subnet, an MGC or MG-XPEC, or the IP address of a UNIStim phone. Each entry may also include a number allowing calls back from the PSAP.

The System Manager and Communication Manager both permit the administrator to create locations and network regions for the IP phones, permitting the user to access services local to the user station. However, the Communication Manager must be correctly set up with the location service (Multiple Locations) or services (Multiple Locations and Multinational Locations) enabled.

This may require licensing changes for the Communication Manager, although most servers have the service entitlement in the licensing. If the licensing entitles the user to the services, the administrator may log in to the System Management Interface of the Communication Manager and enable the services. Note that only entitled services can be changed; if the services are not licensed, the administrator needs to purchase the new licenses.

Key features that use multiple locations

The two key features that use multiple locations are Enhanced 911 and Multi-Location Dial Plan. For more information, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

- Enhanced 911: Uses the multiple locations to determine the best "911" center routing, and if necessary, it uses a suitable "call-back" address configured in the network map to permit the emergency responders to use the automatic location information database to isolate the caller's location.

- Multi-Location Dial Plan: This service is analogous to the "Zone Based Dialing" service on the CS 1000, where multiple smaller CS 1000 nodes were converted to survivable satellites of a central CS 1000 "master" in a data center. Since the different sites could repeat extensions (for example, a site in Colorado and a site in Texas could both have a 538-2345 number), each specific zone had its own ability to insert and delete prefixes (etc.) to ensure calls routed correctly, and station displays showed the same information after consolidation as they did before consolidation.

For more information and procedures, see "Routing Outgoing Calls" in the *Administering Avaya Aura® Communication Manager* guide. The access to these administration screens is also available on the System Manager, which provides a mechanism to administer the Communication Manager information from the System Manager.

Configuring locations
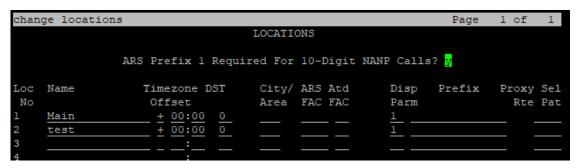
Procedure

1. To define the location:

    a. Enable Multiple location handling on Communication Manager.

       You can use the System Management Interface on Communication Manager to add the capability.

By default, the system has location 1 defined and all stations (etc.) will belong to this location.

b. Ensure that multiple location programming is enabled. Define additional locations as needed to match the geographical areas where the calls must break out to the public domain.

```
change locations                                        Page    1 of    1
                                LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

Loc  Name           Timezone  DST      City/ ARS Atd     Disp    Prefix   Proxy Sel
 No                 Offset             Area  FAC FAC     Parm             Rte Pat
1    Main           + 00:00  0         ___   ___ __      1   _____ _____
2    test           + 00:00  0         ___   ___ __      1   _____ _____
3    _____   _ __:__  __        ___   ___ __      __  _____ _____
4    _____       :    __        ___   ___ __
```

2. To define the network regions, do one of the following:

   a. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Network** > **IP Network Regions**.

   b. Use the Communication Manager SAT interface and type `change ip-network-region` and define the network regions.

   ⭐ **Note:**
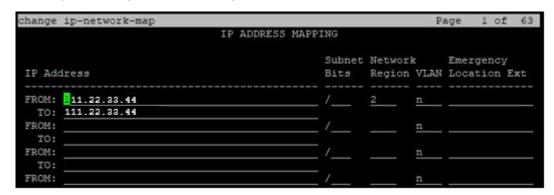
   - The region requires a location to map it to if the calls are to route through a specific gateway.

   - By default, region 1 has location 1, and all endpoints use this region.

   In the following example, location 2 is used for the region 2:

```
change ip-network-region 2                              Page   1 of  20
                          IP NETWORK REGION
   Region: 2        NR Group: 2
 Location: 2        Authoritative Domain: _____
     Name: test region          Stub Network Region: n
 MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: yes
       Codec Set: 1             Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                    IP Audio Hairpinning? n
   UDP Port Max: 3329
 DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
         Audio PHB Value: 46
         Video PHB Value: 26
 802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
         Audio 802.1p Priority: 6
         Video 802.1p Priority: 5      AUDIO  RESOURCE  RESERVATION  PARAMETERS
 H.323 IP ENDPOINTS                               RSVP Enabled? n
   H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

3. To map IP addresses of the SIP endpoints and MGCs or MG-XPECs to different regions, do one of the following:

   a. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Network** > **IP Network Maps**.

   b. Use the Communication Manager SAT interface and enter `change ip-network-map`.

   Configure 911 information whenever the number will not necessarily terminate correctly on the right PSAP. Configure other information as required.

```
change ip-network-map                               Page   1 of  63
                        IP ADDRESS MAPPING

                                      Subnet Network        Emergency
    IP Address                        Bits   Region VLAN Location Ext
    -----------------------------------------  ------ ------ ---- -------------
    FROM: 111.22.33.44                      /__    2     n   _____
      TO: 111.22.33.44
    FROM: _____  /__   ____   n   _____
      TO: _____
    FROM: _____  /__   ____   n   _____
      TO: _____
    FROM: _____  /__   ____   n
```

   The preceding image shows region 2, which maps to location 2. The IP address can be that of the UNIStim endpoint, the IP address of a PC running a 2050 client, an MGC management port IP address, or an MG-XPEC management port IP address.

Result

This enables Communication Manager to route calls from endpoints based on the location of the endpoint. Regions can be created mapping to the default location (that is, to location 1), but this will not affect routing. All calls will still use location 1 settings and gateways for routing calls until location 2 (or greater) is defined and used.

Next steps

Further administration is required to enable the specific service or option for a service requiring location-based origination. Refer to Communication Manager documentation for specific features and the administrative requirements to enable them.

 Note:

> Device Adapter is unaware of the locations and regions to which its stations or MGCs/MG-XPECs belong. This is handled entirely within Communication Manager. However, the administrator needs to be aware of the configuration required to make this work correctly on Communication Manager and must implement the programming required.

Appendix O: User experience differences between CS 1000 and Device Adapter

User experience differences for UC call processing features and services

Analog Station Dialing Options

Analog sets have two different mechanisms for dialing digits:

- A rotary dial mechanism generating 1 to 10 pulses, representing the digits 1 to 9, and 10 pulses representing the digit 0. In CS 1000, this is the Dial Pulse (DIP) class of service.
- A DTMF transmission mechanism using standard DTMF to provide the digits. In CS 1000, this is the Digit Tone (DTN) class of service.

The analog stations have their physical limitations when migrating to Device Adapter. That is, a station that can only do dial pulse still has to do dial pulse signaling, and a station that can only use DTMF has Digit Tone signaling. Stations that can switch between the two based on a switch on the phone can use either, but must use the value corresponding to the switch settings.

This information is needed by Device Adapter to allow it to use the required DTMF detection or dial pulse detection. The class of service values are entered as analog station features. Device Adapter uses the feature to handle the user's digit entry correctly.

- A rotary dial station uses the DIP feature.
- A DTMF station uses the DTN feature.
- If neither is present, then the station should not be analog.

Except for information feedback to the user, there is no user action. However, when the user presses 4, a DIP station does four-timed switch-hook-toggle pulses, to send the digit as pulses. A DTN user may hear tones.

Auto-Answer

- CS 1000 endpoint user experience

  The Auto-Answer Back feature of the CS 1000 is similar to the Auto-Answer feature of Device Adapter.

  The Auto-Answer Back feature auto-answers an incoming call on the hands-free audio device of the phone. An incoming call is auto-answered only if the call arrives at the phone when the phone is in an idle state. A short buzz tone is provided on the phone to alert the called party that the call is answered automatically on the hands-free audio device. If the phone doesn't support hands-free or if hands-free is currently disabled, the Auto-Answer Back feature does not function and the incoming call is presented as usual on the phone, that is, by ringing.

  An incoming call is auto-answered only if the call arrives on the primary DN key.

  In CS 1000, an end user can enable or disable the Auto-Answer Back feature by pressing the AAK key on the phone.

- Device Adapter endpoint user experience

  The functioning of the Auto-Answer feature in Device Adapter is similar to the functioning of the Auto-Answer Back feature in CS 1000.

  The only difference is that, in Device Adapter, an end user cannot enable or disable the Auto-Answer feature. Instead, a system administrator can enable or disable the Auto-Answer feature by using the AAA mnemonic.

Autodial

- CS 1000 endpoint user experience

  By using Autodial, UNIStim and digital 200X users can dial a number by pressing the Autodial feature key (ADL) programmed with a predefined number.

  Users program the Autodial keys by using the on-hook method. When the phone is idle, the user presses on the required autodial key. The screen enters into the programming mode. The user edits the number and presses the autodial key to complete the change.

  Analog endpoint users on the CS 1000 had a partial dial variation. By using the FFC to enable autodial, the endpoint is configured with a digit string or the leading digits of a digit string that allows the user to dial the remaining digits. When the user goes off-hook, on dial tone time out, autodial is executed. This may require additional digits, if partial digit string autodial is used.

- Communication Manager endpoint user experience

The following are two types of Autodial buttons with same feature button type autodial:

- When the destination number is configured in the Communication Manager station. This is read-only Autodial. The user cannot change the number.

- When read-write Autodial is programmed by the user.

• Device Adapter endpoint user experience

The Device Adapter does not support the analog equivalent of autodial.

Device Adapter maps CS 1000 UNIStim and digital 39XX, 2X16, and 200X Autodial to Autodial read-write buttons.

Migration from CS 1000 does not migrate the Autodial destination numbers. Users will have to reprogram Autodial numbers after upgrading to Device Adapter.

Device Adapter maps CS 1000 Autodial to the Communication Manager Autodial button.

Autodial programming scenario:

- User procedure

  1. User presses Autodial key while in the idle state.

  2. A prompt message appears on the screen.

  3. User enters the destination number.

  4. User presses Autodial again to save the changes.

- The number cannot be programmed if the Autodial button is configured with a predefined number by the administrator.

- A free call appearance is required at the time of completing the programming dialog. Device Adapter performs a programming call to Communication Manager.

Autodial dialing scenario:

- User procedure

  1. When the user goes off-hook, it automatically selects the prime DN key (key 0 or button 1). Alternatively, on sets with headsets, or hands-free, pressing these keys also selects key 0. Pressing any other line key selects that line key. This is the same behavior as the CS 1000.

  2. User presses an Autodial key. This differs from Communication Manager where pressing Autodial automatically selects a call appearance.

  3. User may also press Autodial key when call is answered. The stored number is output as RFC 2833 events.

- Dialing scenario after answer is not supported on phones with no RFC 2833 support, such as the i2050v2 or less.

For more information, see "Autodial" in "Appendix H: Call processing features and services."

Basic station display

The various stations with displays are described in their respective user guides. This display includes:

- Time and date information.
- Idle screens, such as a display of the corporate name on stations supporting this capability.
- Soft keys available on an idle station for applicable stations.

The idle set display may not be identical to CS 1000. Not all feature keys are necessarily migrated. However, buttons that were migrated from CS 1000 keys are in the appropriate places, with a name similar enough to make identifying the button easy. Administrators can use System Manager to customize button labels for the stations. As a result, names shown may change due to administrator provisioning choices.

For more information, see "Display capabilities" in "Appendix G: Generic station operations."

Busy Indicator

- CS 1000 endpoint user experience

The Busy Forward Status (BFS) feature of CS 1000 is similar to the Busy Indicator feature of Device Adapter, but with some differences.

BFS provides multi-appearance telephone users and attendants with a visual indicator of the busy or idle status of a phone. This feature is typically used in a boss-secretary scenario.

For example, phone A is secretary's phone and phone B is boss's phone.

Configure the BFS key on phone A. The format is KEY xx BFS <TN of SET B>. Phone A monitors the state of phone B. Depending on the state of phone B, the BFS key on phone A shows the following status:

- Dark lamp: Phone B is idle.
- Lit lamp: Phone B is on a call.
- Flashing lamp: Phone B is call forwarding all calls to phone A.

The phone A user can use the BFS key to transfer the call to phone B. While phone A is on a call with some other party, the phone A user can press the BFS key to call phone B, and then press the BFS key again to transfer the call to phone B.

However, as compared to the Avaya Aura® Busy Indicator (BI) button, the BFS key in CS 1000 has the additional capability to call forward all calls on behalf of another user extension.

In CS 1000, to call forward all calls from phone B to phone A, the phone A user can press the BFS key that is configured to provide busy status indications for the phone B extension.

In Avaya Aura®, a system administrator can configure a **call-fwd** button for phone A. The default label for this button on the phone is Forward. Phone A user can specify the extension

number of phone B for this Forward key, and use this Forward key to manage call forward all calls on behalf of phone B.

- Communication Manager endpoint user experience

Use the Busy Indicator feature to provide multi-appearance telephone users and attendants with a visual indicator of the busy or the idle status of one of the following system resources:

  - An extension number.

  - A trunk group.

  - A terminating extension group (TEG).

  - A hunt group, either direct department calling (DDC) or uniform call distribution (UCD).

  - Any loudspeaker paging zone, including all zones.

A SIP phone can support only another extension.

You can assign extension numbers, trunk group access codes, and loudspeaker paging access codes to a Busy Indicator (BI) button.

The Busy Indicator button provides an attendant or a user with direct access to the extension number, the trunk group, or the paging zone. The Facility Busy lamp indication for a Vector Directory Number (VDN) is not On when the VDN is being used. You can use the associated button to place a call to a VDN.

For example, phone A is secretary's phone and phone B is boss's phone.

After an administrator configures the busy-ind button feature for phone A, phone A monitors the state of phone B.

Depending on the call status of phone B, the BI button lamp on phone A changes to lit or dark. The button function is indication only. User can press the button, but it is ignored by the phone. However, unlike the CS 1000 BFS feature, there is no indication of the forwarded status.

Instead, Communication Manager provides a Call Forward button to forward calls on behalf of the monitored user extension. For example, if a Call Forward button is configured on phone A on behalf of phone B, the phone A user can use this button to manage Call Forward on behalf of phone B.

Separate BI and Call Forward buttons allow a user to use the Busy Indicator and Call Forward features separately.

- Device Adapter endpoint user experience

BFS equivalent capability of monitoring the busy status of a monitored extension and dialing the monitored extension:

The Busy Indicator feature of Device Adapter is similar to the Busy Forward Status (BFS) feature of CS 1000, but with some variations.

The Busy Indicator (BI) button is mapped to the BFS key on the secretary's phone. This button appears as the BusyFwd button on the secretary's phone. This button provides BFS

equivalent capability of monitoring the status of the boss's extension and transferring calls from the secretary's phone to the boss's extension.

For example, phone A is secretary's phone and phone B is boss's phone.

After an administrator configures the busy-ind button feature for phone A, phone A monitors the state of phone B.

Depending on the BI status of phone B that Device Adapter receives from Communication Manager, the lamp state on phone A changes to the following:

- Dark lamp: Phone B is idle.

- Lit lamp: Phone B is on a call.

When the phone A user presses the BusyFwd button in a dialing state, Device Adapter dials the BI number of phone B.

Phone A user can perform the following steps to transfer a call to phone B:

1. While on the call, press the Transfer button.

2. Press the BusyFwd button.

3. Press the Transfer button.

    Device Adapter transfers the call to the BI number of phone B.

When the phone A user presses the BusyFwd button in an idle state, Device Adapter automatically selects the lowest idle line appearance, and dials the BI number of phone B.

BFS equivalent capability of managing Call Forward on behalf of another user extension:

In Device Adapter, unlike CS 1000, the BusyFwd button on phone A does not Call Forward All Calls (CFW) of phone B to phone A. Instead, an administrator can configure another **call-fwd** button for phone A, which the phone A user can use to manage CFW on behalf of phone B.

Although the ProVision tool can provide the Busy Indicator, including the dial capability associated with BFS, the ProVision tool does not automatically provide the call forward handling.

In a CS 1000 environment, the BFS key has three roles. Whether all the three roles apply depends on the following contexts:

- All locations use the ability to monitor the status of the called extension. This allowed departmental administration assistants a mechanism to track the status of the members of the department. This frequently required more than 10 BFS keys.

    In Device Adapter, the Busy Indicator button provides this capability.

- The ability to use the BFS key to transfer calls to the associated extension or to auto-dial the extension programmed at that key. This capability was used only in a few scenarios, such as, the administrative assistant wanted to transfer a call to a target.

    In Device Adapter, the Busy Indicator button provides this capability.

- In a subset of cases in CS 1000, the BFS key can also be used to call forward all calls on behalf of the monitored extension. In some cases, an administrative assistant might have to monitor the status of two or more extensions.

  This function is not available with the Busy Indicator button in Device Adapter. However, in Device Adapter, the programmable **call-fwd** button provides the capability to call forward all calls on behalf of a monitored extension, also referred to as the "CFW controlled" extension. Because this capability is not always used and consumes an extra button, a system administrator must first identity the extensions that an administrative assistant wants to monitor and manually configure the **call-fwd** buttons only for such extensions. ProVision does not map this button.

For more information, see "Busy Indicator" in "Appendix H: Call processing features and services."

Call Forward All Calls

The CS 1000 Call Forward All Calls (CFW) automatically forwards incoming calls to another destination, within or outside the system. Only calls to the station extension, which is the Prime DN on CS 1000, or any single-appearance secondary number on the telephone are forwarded. Numbers shared with other users cannot be forwarded in this manner. Outgoing calls can still be placed from the telephone when Call Forward is active.

This service is available both for digital and UNIStim multi-line stations, and for analog stations or digital single-line stations that use the Flexible Feature Codes on the CS 1000 (Feature Access Codes on the Communication Manager).

With the following provisions, the behavior is unchanged between the CS 1000 and Device Adapter endpoints:

- By default, the basic call forward feature on Communication Manager does not maintain the call forward destination when the call forward is cancelled. CS 1000 maintains this destination information and uses this as a default call forward target.

  To maintain the CS 1000 behavior, Device Adapter saves the current call forward destination and uses it as the default call forward destination the next time the user activates call forward.

- Confirmation tone is a three-beep burst.

For more information, see "Call forward" in "Appendix H: Call processing features and services."

Call Forward Busy

Call Forward Busy (CFB) automatically routes calls to a target when a telephone is busy. This service is provisioned against a station on CS 1000 and cannot be configured.

Communication Manager allows a user to modify the call forward destination. Users who want to use this feature should refer to the Communication Manager documentation for details. This is not

a CS 1000 feature and is provided by Communication Manager that controls the station through Device Adapter.

The equivalent service used in Communication Manager is Coverage and applies to both busy stations and stations where the user did not answer. For more information about the Coverage feature, see the Communication Manager feature documentation.

For more information about the Call Forward feature, see "Call forward" in "Appendix H: Call processing features and services."

Call Forward on No Answer

Call Forward on No Answer (CFNA) automatically routes calls to a target when a telephone rings, but the user does not answer. This service is provisioned against a station on the CS 1000 and cannot be configured.

Communication Manager allows a user to modify the call forward destination. Users who want to use this feature should refer to the Communication Manager documentation for details. This is not a CS 1000 feature and is provided by Communication Manager that controls the station through Device Adapter.

The equivalent service used in Communication Manager is Coverage and applies to both busy stations and stations where the user did not answer. For more information about the Coverage feature, see the Communication Manager feature documentation.

For more information about the Call Forward feature, see "Call forward" in "Appendix H: Call processing features and services."

Call Pickup

Call Pickup can be done within a group. Call Pickup is referred to as Ringing Number Pickup in CS 1000. Picking up a ringing number in another group is referred to as Group Pickup in CS 1000. Picking up a specific ringing destination is referred to as Directed Pickup, DN Pickup, or Directory Number Pickup in CS 1000.

All three have a corresponding Communication Manager equivalent, and the end user experience should have no noticeable differences beyond a potential of the group indices being changed.

Caveats exist around the CS 1000 Group Pickup migration to the Communication Manager Extended Pickup Group. The group sizes may differ. The groups allowed within a group pickup are dependent on the extended group, which is a supergroup enclosing the smaller groups.

The superset group can hold up to 25 groups. The group pickup can only pick up calls within the supergroup to which it belongs. As a result, the group indices may not map 1:1 from CS 1000 to Communication Manager and Device Adapter.

For more information, see "Call Pickup" in "Appendix H: Call processing features and services."

Call Waiting

- CS 1000 endpoint user experience

  Call Waiting notifies a telephone user on an established call, on a Single Call Arrangement DN button (internal or external), that an external call is waiting to be answered. When an external call arrives and the user is on a call, the Call Waiting lamp flashes and a buzz sounds through the speaker.

  Call Provisioning:

  - CLS SWA

  - Call Waiting (CWT) feature key

  User procedure:

  - Phone is busy on a Single Call Arrangement DN key.

  - A call is placed to this DN number.

  - Call Waiting key flashes.

  - If the user presses the Call Waiting key, the current call is placed on hold and a new call is established with the incoming request. Alternatively, the user can place the current call on hold and press the Call Waiting key. A connection is established to the new call and the user can switch between the two using the Hold method.

  - Outgoing calls cannot be made using the Call Waiting key.

  - The Call Waiting indication can be received on any of the line DN keys.

- Communication Manager endpoint user experience

  Communication Manager does not support a Call Waiting feature.

- Device Adapter endpoint user experience

  The database migration tool will create one extra call appearance for the primary extension. Device Adapter adds no special logic. The extra DN key allows the call to be presented to the user even when the first is busy.

For more information, see "Call Waiting" in "Appendix H: Call processing features and services."

Called / Calling Party Display on a Station

Calling and Called party name display is available only on stations with an alphanumeric display. Certain stations, such as M2616, may or may not have a display. The display module is an option on that station. Others either have a display or do not have a display. If they have a display, some older stations may not have name display capability.

The number information is displayed when the user enables the service by using the Automatic Digit Display (ADD) or Digit Display Standard (DDS) feature, although Tandem Digit Display (TDD) exists and includes both of the prior capabilities. For differences between the options, see the CS

1000 documentation. However, the Call Number Display Denied (CNDD) feature forcibly blocks the display, No Digit Display (NDD) applies for endpoints without a display screen.

The station is programmed with the feature (CS 1000: class of service) Call party Name Display Allowed (CNDA) on a station permitting name display. If the feature mnemonic is not provided, the name display is not presented.

Stations with the feature programmed display names and numbers if the display of digits is enabled, provided the station has the capability. For example, if an M2616 without a display is substituted for a station with a display, no name or number information is displayed.

For more information, see "Display capabilities" in "Appendix G: Generic station operations."

Conference using Communication Manager Ad hoc conference

- CS 1000 endpoint user experience

  A Conference key configured for UNIStim and 39XX endpoints at a fixed position and digital 200X endpoints at an unfixed position. This key is available on phone screen during an active call. The active call is put on hold and the user receives a new dial tone when it is pressed. The user completes the conference by pressing Conference key again when the far-end answers.

  The number displayed with the `CONFERENCE` label on the phone is the total number of conference participants. For example, if a user was participating in a conference with 2 other participants, the `CONFERENCE` label would display `CONFERENCE 3`.

  Conferencing on an analog phone functions in a manner similar to the Transfer experience described in the preceding section.

- Device Adapter endpoint user experience

  - Digital and UNIStim stations

    A Conference key configured for UNIStim and 39XX endpoints at a fixed position and digital 200X endpoints at an unfixed position. Communication Manager considers it as a restricted call appearance that cannot receive any incoming call but can only be used for outgoing calls placed in the process of establishing a conference. Device Adapter will treat this button as a CS 1000 Conference key with existing localization.

    The CS 1000 TN can be provisioned with either CLS A03 or A06. This means the user is allowed to establish a three-way or six-way conference. There is no such limitation for a Communication Manager station. On Communication Manager, all stations have a six-party conference capability.

    The number displayed with the `CONFERENCE` label on the phone is the number of conference participants other than the current user. For example, if a user was participating in a conference with 2 other participants, the `CONFERENCE` label would display `CONFERENCE 2`.

  - Analog stations

The analog stations support call transfer on Device Adapter. However, even on CS 1000, the operation was tied to conference.

CS 1000 permitted a user with an analog station having the transfer capability to:

• Do a transfer or create a three-party conference.

• Do a transfer or create a conference of up to six parties.

When the transfer/conference capability is enabled, Device Adapter always allows six-party conferences on a station that is migrated from CS 1000. The transfer is always available if conference is allowed.

To create a conference, the analog station user must be on an active call or have a conference already created with less than six participants.

• The user does a switch hook flash and receives a dial tone.

• The user dials the number of the additional party that is needed in the conference.

• If the user hangs up while the call target is ringing, Device Adapter does a blind transfer. This can transfer an existing conference to the target.

• If the user hangs up after the call to the call target is answered, the transfer is completed as a consultative transfer. This can transfer an existing conference to the target.

• If the user does a switch hook flash while ringing, the conference attempt is cancelled.

• If the user does a switch hook flash after the target has answered, the target party is added to the conference.

This matches the CS 1000 analog station user experience for conference.

Related links
Conference (Ad hoc conference) on page 456

Context-sensitive key access

Context-sensitive soft keys depend on the current state of the call (which includes the station being idle, and therefore, not having a call), the state of the station itself, and services available.
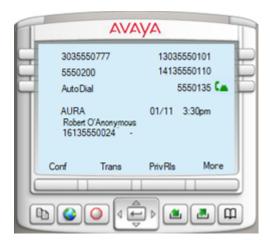
The CS 1000 endpoints that support soft keys typically have a display that includes four buttons with labels.

If there are less than four soft keys that can be used in a specific state, all the buttons are shown.

This example shows an idle endpoint, with a call forward soft key, a Callers List soft key, and a Redial List soft key. For more information, see the Personal Directory section.
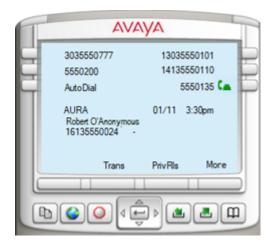
If there are four or more buttons, up to three buttons are displayed. The fourth button indicates More, which allows the user to view the additional soft keys.

This shows an endpoint active in a call, with the Conference, Transfer, and Privacy Release buttons active. The More button allows the user to view a second set of buttons applicable for the current state.

The soft keys vary based on the current endpoint state and can vary when the Options are used.

Note that the soft key may not be visible. The Conf location is fixed for ad hoc Conference, and if the administrator used No Hold Conference and omitted the normal Conference button, the display leaves the Conf position blank.

For more information, see "Context-sensitive soft keys" in "Appendix G: Generic station operations."

Dialing a number

- CS 1000 endpoint user experience

  All dialed digits are handled by the Call Server, which completes the dialing phase after the digits match an internal extension or dial plan rule. UNIStim and 39XX phones support a Predial state where the user can enter and modify the number before sending it to a call server.

- Communication Manager endpoint user experience

  96x1 Avaya Aura® SIP phones use en-bloc dialing. This type of dialing analyzes digits by using information received from the PPM DialPlanData section. CSDK does the same.

- Device Adapter endpoint user experience

  Device Adapter analyzes dialed digits against the dial plan obtained in the same way as Avaya Aura® SIP phones.

  Device Adapter supports the Predial state for UNIStim and 39XX phones. The user can enter the digits prior to accessing a line appearance, possibly correct misdialed digits, and then select the line appearance to make the call.

  Device Adapter supports three timers that are administered through Avaya Breeze® platform service attributes: dialtone, interdigit, and busy/overflow.

For more information, see "Dialing a number" in "Appendix G: Generic station operations."

EC500 (Mobile Extension)

The CS 1000 Mobile Extension (Mobile X) service parallels the Communication Manager Extension to Cellular 500 service. To the user, there is no visible difference in the operation, as the call extends from Communication Manager to the defined cell phone.

Refer to the document *Avaya Extension to Cellular User Guide* for information and procedures associated with this feature. This document is available on the Avaya Support portal. Chapter 1 provides an introduction to this feature and Chapter 4 provides information and procedures on user operations.

Related links

[Mobile Extensions (Mobile X) using EC500](#) on page 488

Emergency Dialing for Virtual Office

- CS 1000 endpoint user experience

  - When a SIP user is logged in to a VO account: CS 1000 supports emergency dialing by allowing Virtual Office users to directly call Public Safety Answering Point (PSAP) for their geographic location. The home server determines the VO login and redirects the emergency call to CS 1000 host. The host CS 1000 uses the ESA location information to receive a call back and sends the location number to PSAP.

  - When a SIP user is logged out from a VO account: CS 1000 supports emergency dialing for making calls and receive call back by allowing Virtual Office users to temporarily register with the Call Server. The registration begins as the user tries to make a call from the logged out phone by going off hook, pressing the primary key, or using the handsfree or headset.

- Communication Manager endpoint user experience

  Communication Manager does not support the Virtual Office feature. Services related to Virtual Office such as Emergency Dialing for Virtual Office do not apply.

- Device Adapter endpoint user experience

  - When a SIP user is logged directly in to the set using normal registration or logged in to a VO account: Device Adapter does not have any specific configuration for providing emergency dialing using Virtual Office. The configuration at Session Manager and ELIN server ensures that the call information is available to PSAP, to identify the caller information, and receive call backs.

  - When a SIP user is logged out from a VO account or the server becomes unregistered: Device Adapter supports emergency dialing for making calls and receive call back by using VOLO attributes that is **TN range for emergency calls from Logged out sets** and **SIP domain for emergency calls from Logged out sets**.

Avaya Breeze® platform cluster attribute VOLO is assigned automatically to the logged out set. The VOLO attribute cannot be used once the phone returns to its normal state or if it loses network or power during the logged out state.

VOLO TN is used to handle emergency calls using CS 1000 components. VOLO TNs are used to register the logged out phone with the Avaya Breeze® platform components.

The logged out phone can only make ESA calls such as 911, 112 and so on. The configured VOLO TNs are expected to be fully restricted, which means the device will not be registered with Session Manager and all the operations other than emergency calling will be rejected. So, that means Session Manager can make an emergency call from an unregistered phone by making a connection of Device Adapter and the device.

User procedure:

- Phone is in logged out state.
- The User goes off hook.
- A VOLO TN is assigned immediately when the phone goes to logged out state

  ⊛ **Note:**

  You can change the default value of allocated TNs and SIP domain assigned for making emergency call by navigating to **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes** from the System Manager web console.

- Emergency number can be dialed from the phone.
- Any other operation cannot be completed using this phone.
- Incoming call from PSAP are not supported.

🛈 **Important:**

VOLO TN is assigned to a logged out phone only during the transition from normal to logged out state. If logged out phone does not get any free VOLO TN during that transition, the phone will remain in logged out state with no additional key or capability to make emergency calls. If a VOLO TN becomes free later, when the phone is already in logged out state, then VOLO TN will not be assigned dynamically and the phone will not be able to make emergency calls.

For more information, see "Virtual Office" in "Appendix H: Call processing features and services."

Endpoint registration

⊛ **Note:**

This section is only applicable to UNIStim IP endpoints.

- CS 1000 endpoint user experience

  The user may be asked to configure the IP connectivity, Node ID, and TN of the endpoint during registration. This information is protected by the Node password if it is enabled.

  If the Node password (IP Phone Installer Password) is configured on the Signaling Server, the **IP Phone Telephone Options** > **Set Info** menu does not display the **Set IP Information**

or **Ethernet Information** options. Password can be set on the Signaling Server through CLI commands such as `nodePwdSet`. The password is stored as plain text on disk.

- Communication Manager endpoint user experience

The Avaya Aura® SIP phone user enters an extension number and password during registration.

- Device Adapter endpoint user experience

Device Adapter follows the CS 1000 registration process. The user may be asked to configure the IP connectivity, Node ID, and TN of the endpoint during registration. This information is protected by the Node password if it is enabled.

The CLI commands `nodePwdSet`, `nodePwdEnable`, and `nodePwdDisable` are implemented on the Avaya Breeze® platform server to control the Node password. If the Node password is configured, the **IP Phone Telephone Options** > **Set Info** menu does not display the **Set IP Information** or **Ethernet Information** options. The password is stored hashed, not as plain text.

Related links

End-to-End Signaling

End-to-end signaling is done in an IP network by using RFC 2833 RTP packets. As a consequence, stations that support RFC 2833 and digital or analog stations using DSP resources on the Media Gateway Controller, can provide end-to-end signaling.

However, the older IP station firmware versions may be unable to do this. The applicable stations are IP Phone 2001 phase 1, and IP Phone 2004 phase 0 and phase 1. The phase 2 IP Phone 200x is the only version of IP Phone 200x that can perform RFC 2833.

Verify that the station is RFC 2833 compatible. Otherwise, it cannot do end-to-end signaling.

For more information, see "End-to-End Signaling" in "Appendix G: Generic station operations."

Feature key labels

- CS 1000 endpoint user experience

All buttons can have a customized label. The UNIStim phone screen displays 10 characters per label, 9 characters for 12xx sets. If no label has been defined, TPS provides default, localized labels.

✱ **Note:**

Digital 200X endpoints do not support feature key labels. 39XX endpoints store feature key labels locally.

- Communication Manager endpoint user experience

  Avaya Aura® SIP phones support custom button labels. The labels can be set on the phone UI or by administrator in System Manager.

- Device Adapter endpoint user experience

  Feature key labels for UNIStim IP phones can be set by the administrator in System Manager and modified by the user similar to the CS 1000 experience.

  The following end user procedure that is currently applicable to CS 1000 is retained for Device Adapter.

  - The user accesses the **Telephone Options** menu and chooses **ChangeFKL**.

  - A message is displayed to select a key.

  - The user types the new label text.

  - The user presses **Select** again to confirm the new label.

  Changing feature key labels for the prime DN is not supported. This is similar to the CS 1000 experience.

  It is possible to add labels from Communication Manager or from System Manager with the appropriate language set.

  Autodial buttons with no number programmed cannot be assigned a custom label.

  Speed call feature key is configured as an Autodial button in the Communication Manager station. If no number is configured for the button, the user cannot assign a custom label to the key.

For more information, see "Feature key labels feature description" in "Appendix F: Infrastructure Features and Services."

Fixed Feature Key Access to Services

The digital and UNIStim stations predominantly rely on fixed buttons, fixed location but programmable buttons, or programmable keys.

Example:

- Fixed buttons: Release and Hold.

- Fixed location but programmable buttons: Conference soft key on an 1140 may or may not be enabled.

- On programmable keys: Line appearances, Autodial, and so on. All feature buttons that are not completely fixed on a subset of digital phones

These buttons allow the user to access services that an analog station user must access by using the Feature Access Codes.

The services configured for the fixed feature keys function is in the same manner as that on the CS 1000 endpoints, or on a multi-line endpoint type such as a SIP 96x1.

Related links

Flexible Feature Code (Feature Access Code) Access to Services

Analog sets do not have fixed feature keys. Instead, they rely on either using the hook-flash; for example, for transfer and conference, or Feature Access Codes.

The administrator must maximize the number of CS 1000 FFCs that are mapped to the FAC of the same digit string. For example, if FFC 4456 and FAC 4456 both trigger Call Park and Page, the user experience remains unchanged.

For more information, see "Flexible Feature Codes" in "Appendix G: Generic station operations" and "Appendix H: Call processing features and services."

Group Paging

The Group Paging feature of Device Adapter does not have an equivalent feature in CS 1000.

Hence, the Device Adapter user experience for group paging is similar to that of Avaya Aura®, except for the following difference:

- On endpoints that are configured in Avaya Aura®, a group paging call is not auto-answered if the user has set the state to Do Not Disturb.

  Whereas, on the Device Adapter UNIStim endpoints in Avaya Aura®, a group paging call is auto-answered even if the user has set the state to Do Not Disturb.

  A user cannot set the state to Do Not Disturb on a Device Adapter UNIStim phone. However, if MDA is allowed, the user can simultaneously log in to an Avaya Aura® phone and set the state to Do Not Disturb.

For more information, see "Group Paging" in "Appendix H: Call processing features and services."

Handsfree and Speaker button

A subset of CS 1000 stations provides the user the ability to use the station in a hands-free manner. Almost all have a speaker button, although a few stations can provide the capability without the button.

CS 1000 users can make calls on hands-free in the following ways assuming the station is able to act as a speakerphone, and the capability is enabled with the Hands Free Allowed (HFA) feature:

- While the handset is in the cradle, press the desired line appearance key. The station seizes the appearance as a handsfree station.

- While using the handset or headset, or while on hook and idle, the user can shift into handsfree by pressing the speaker button. Using while on hook and idle seizes an available line appearance.

This approach is maintained with Device Adapter. The CS 1000 HFA class of service must be programmed as a feature for the station to access the capability.

Leaving handsfree may require putting the call on hold and then taking it off hold by using the handset, if the user wants to do so.

For more information, see "Headset button and headset" and "Speaker and speakerphone" in "Appendix G: Generic station operations."

Hold (and Retrieve)

The Hold button is used to place a call on hold with an on-hold music, if provided. Providing on-hold music is a function of Communication Manager and not of Device Adapter. For more information, see the Communication Manager documentation.

The call can be placed on hold for several reasons, such as to answer another call and to switch from headset to handset or speakerphone to handset.

Retrieving a call is done by pressing the line appearance that is on hold or by pressing the speaker or headset button, if available. If you press the line appearance that is on hold and if the handset is off-hook, the handset becomes active. Otherwise, the speaker phone or headset, if available, becomes active.

Related links

Hotline (Hotline two-way)

Use the Hot Line feature to automatically dial a specific number.

Two-way hotline or hotline two-way is a hotline button where party A can call party B, or party B can call party A. However, Communication Manager has no native function equivalent.

⊛ **Note:**

Note that the destination number for the hotline button must be already configured on the target Communication Manager station.

Because the number is configured on the target Communication Manager station, a user cannot edit the number on a Device Adapter endpoint. Hence, the Hotline two-way number is read-only on the endpoint.

Two-way hotline is created by having two users share bridged appearances of an X-Port, where only these users have this button. The button is labeled as a hotline button, and when the user initiates a call on this button, Device Adapter initiates a call to the extension. As the only other

user with this extension as a bridged appearance is the other party in the two-way hotline, that user is rung.

As a result, to the user, the button follows the behavior of the hotline.

User operation:

- User A and B have a two-way hotline button on their stations.

- User A presses the hotline button to call user B.

    - Device Adapter seizes a call appearance.

    - The target number is dialed.

    - User B rings and ringback is provided to user A.

- User B answers the call. Both parties are in a two-way call.

For more information, see "Hotline two-way" in "Appendix H: Call processing features and services."

Hotline one-way

- CS 1000 endpoint user experience

    The number configured for Hotline one-way appears as a line key on the phone. The user can press this button to dial the number.

    Users cannot receive inbound calls on this line key. The outgoing Caller ID (CLID) is the prime DN. CS 1000 does not reserve an SCN or MCN key for the Hotline one-way key. Hence, if a user dials a hotline one-way number, the call is attempted even if all call appearances are busy.

- Device Adapter endpoint user experience

    Hotline one-way uses the autodial button feature. Hotline one-way allows an administrator to set a number as an autodial number for a Device Adapter endpoint.

    The Hotline one-way button is presented as Autodial on the endpoint with the configured number as the default label. When a user presses this button, Device Adapter selects the lowest available line appearance and autodials the number.

    ✱ **Note:**

    The Hotline one-way feature requires a call appearance. If all call appearances are busy and if a user presses the Hotline button, the call attempt fails.

For more information, see "Hotline one-way" in "Appendix H: Call processing features and services."

Hotline Intercom

- CS 1000 endpoint user experience

  You can use the Hotline Intercom feature in a boss and secretary environment where two people can communicate through the speaker by pressing the Hotline Intercom button.

  Configure phone A with HOT I key and specify the target DN as phone B and a mode; for example, Voice or Ringing. Similarly, configure the target phone B with HOT I key and specify the target DN as phone A.

  When a user presses the Intercom key, the target phone auto-answers the call after providing a ring tone.

  The prime DN is the CLID.

- Communication Manager endpoint user experience

  Automatic intercom is a feature where a button is administered. When a user presses the button, a call is place to a predefined extension. An intercom call makes a unique alerting sound. If the desk phone has an intercom button with a status lamp, the lamp flashes.

  To control which users can make intercom calls to each other, an administrator can add the desk phones of the users to a group called "intercom group." After the administrator adds the desk phones to the group, users can make intercom calls by administering an automatic intercom button on their desk phones.

- Device Adapter endpoint user experience

  The Hotline Intercom feature in Device Adapter adds the auto-answer capability to the existing Hotline two-way feature.

  Configuration and user experience are almost the same as that of CS 1000. Device Adapter provides an additional HTLI mnemonic to auto-answer a call.

  Hotline Intercom uses a bridged appearance and the enhanced HTLI mnemonic to auto-answer inbound calls and auto-dial the hotline number that is configured for the Device Adapter endpoint. Administrators can use the HTLI mnemonic to the specify the Caller ID (CLID) for which auto-answer must be enabled. If the CLID filter is not specified, Device Adapter auto-answers all inbound calls.

  For more information about the HTLI mnemonic, see CS 1000 CoS and Avaya Aura feature field mapping on page 322.

  With Device Adapter, the target phone is provided the CLID of the X-port. In CS 1000, the prime DN is the CLID.

For more information, see "Hotline Intercom" in "Appendix H: Call processing features and services."

Last Number Redial

- CS 1000 endpoint user experience

  The user selects last number redial by making the phone off-hook or selecting a DN key and then using some form of the **Last Number Redial** key.

  - In multi-line sets, the user can double press the prime DN key.

  - In single line sets, and if configured on multi-line sets, the user can take the phone off-hook and select and press the fixed or programmable key.

  - Additionally, 1210 model phones have a **Last Number Redial** key.

  - Finally, analog station users can use the applicable Last Number Redial FFC to redial the last user called.

- Communication Manager endpoint user experience

  The feature is done locally on the set.

- Device Adapter endpoint user experience

  Last Number Redial is implemented in the following way:

  - The feature is administered through LNA/LND mnemonic of Communication Manager station Features field.

  - Device Adapter uses the Features CLS string to set the feature state on the set.

  - Dialed digits are stored in PPM DeviceData.

  Device Adapter supports following methods of activating Last Number Redial:

  - Double-press on a line key

  - Off-hook and press the line key

  - 1210 set only: Off-hook and press Last Number Redial softkey

  - The analog station user can use the Last Number Dialed Feature Access Code in place of the FFC.

Device Adapter does not support any endpoint other than the 1210 using the Last Number Redial feature keys.

For more information, see "Last Number Redial" in "Appendix H: Call processing features and services."

Loudspeaker paging

In CS 1000, paging is available as both part of the Park and Page operation and as a stand-alone feature. The Loudspeaker paging feature is commonly used for this service, but the Avaya Aura® service variant called Voice Paging is effectively identical to the paging on CS 1000.

- CS 1000 endpoint user experience

  The CS 1000 paging description says:

  "The system provides switching access and trunk circuit interface to a customer-supplied speaker or radio paging equipment. Paging equipment is accessed by dial access or a Page key on attendant consoles. Telephones cannot be assigned a Page key and must dial access this feature."

  The paging service is configured to access a paging trunk card that is connected to the speakers or a trunk card that is connected to a radio distribution trunk. An administrator can provision a flexible feature code (FFC) to allow users to access the trunk route.

  To perform the paging, the user does the following:

  1. Goes off hook and enters the feature (FFC) code.

  2. Accesses the page trunk, makes the announcement, and then goes on hook.

  3. Attendant consoles may also use the paging key.

- Communication Manager endpoint user experience

  The Loudspeaker Paging feature of Communication Manager is similar to the paging on CS 1000.

  Like CS 1000, Communication Manager offers other paging options, such as Park and Page. But, paging without an active call provides the same user experience as the paging on CS 1000. That is, the user accesses the paging system and makes an announcement.

  However,

  - Communication Manager uses Trunk Access Code (TAC) to access the paging resources. This has the same appearance as using the FFC and is identical to using the CS 1000 route access code to reach the paging trunk.

  - In addition, you can configure up to 9 paging zones. This requires up to 9 different ports (one port per zone) along with a TAC and class of restriction (COR) group per zone.

- Device Adapter endpoint user experience

  Device Adapter does not support the analog trunk cards that were used on CS 1000 for paging. Instead, like Communication Manager, Device Adapter uses Loudspeaker Paging.

  In Device Adapter, you must provision the Avaya Aura® system with the Voice Paging configuration, and use the MM711 card to perform loudspeaker paging. For more information about configuring paging in Avaya Aura®, see the Communication Manager documentation.

To perform the paging, the user does the following:

1. Goes off hook and dials the TAC of the paging zone.

2. Makes the announcement.

3. Goes back on hook.

⊛ **Note:**

For a user experience similar to CS 1000, Avaya recommends that you configure the TAC to match the FFC that is used on CS 1000.

For more information, see "Loudspeaker paging" in "Appendix H: Call processing features and services."

Make Set Busy

- CS 1000 endpoint user experience

  A feature key that makes a phone appear busy to incoming calls.

  Calls to the number receive a busy treatment as configured for the number. Different options are available if you have multiple users sharing the number.

- Communication Manager endpoint user experience

  The closest Communication Manager analog is the **Send All Calls** key. Calls immediately go to Coverage when you press this key. To use the **Send All Calls** key as Make Set Busy, ensure the Coverage script has the same criteria for Send All Calls and Make Set Busy.

  Coverage criteria for bridged call appearances are based entirely on the criteria of the primary extension that is associated with the bridged call appearance. If a telephone user activates Send All Calls on the primary extension, incoming calls still ring bridged call appearances of that extension, as long as a simulated bridged appearance of the call is maintained at the primary extension.

- Device Adapter endpoint user experience

  Device Adapter maps **Make Set Busy** to **Send All Calls**.

  The CS 1000 endpoint is assigned a send-calls button and one or two coverage paths to specify where incoming calls are routed when Send All Calls is activated. The send-calls button is treated by Device Adapter as CS 1000 Make Set Busy key.

  To use the **Send All Calls** key as Make Set Busy, ensure the Coverage script has the same criteria for Send All Calls and Make Set Busy.

  Pressing the **Make Set Busy** button toggles the **Send All Calls** feature. When the feature is activated, the indicator light near the **Make Set Busy** button is lit and the message `Make set busy activated` appears on the set display. When the feature is cancelled, the indicator light is no longer lit. No special message is displayed on the set.

  See the Communication Manager documentation for specifics of the Send All Calls feature.

For more information, see "Make Set Busy" in "Appendix H: Call processing features and services."

Malicious Call Trace

- CS 1000 endpoint user experience

Administration

CS 1000 is configured to support Malicious Call Traces (MCT). This includes any trunks capable of sending MCT signaling. Options include local recording trunks, logging devices, disconnect delay times, and other items based on national requirements.

FAC capability is defined for analog, digital, and UNIStim users without the trace key. Two primary options exist:

- The system prefix is configured. SPRE + 83 triggers call trace.
- An FFC (equivalent to Feature Access Code) is configured as MTRC (Malicious call TRaCe).

Endpoints are configured to support MCT.

- The MCTA (Malicious Call Trace Allowed) class of service is required. This applies to analog, digital, and UNIStim endpoints.
- Digital and UNIStim endpoints can have a **CallTrace** key provided.
  - The **CallTrace** key cannot be a soft key on an endpoint.
  - The **CallTrace** key does not require a lamp or icon.

User operation

To trace a malicious call from an analog (500/2500-type) phone:

1. User is on a call and determines that the call is malicious.
2. Flash the switchhook. A special dial tone signifies that the call is on hold.
3. Enter SPRE+83 or the FFC. You are reconnected to the call.

To trace a malicious call from a digital or UNIStim phone using Special Prefix (SPRE) code or FFC:

1. User is on a call and determines that the call is malicious.
2. Press Transfer or Conference. A special dial tone signifies that the call is on hold.
3. Enter SPRE+83 or the FFC. You are reconnected to the call.

To trace a malicious call from a digital or UNIStim phone using the **CallTrace** key:

1. User is on a call and determines that the call is malicious.
2. Press the **CallTrace** key. You remain connected to the call.

- Communication Manager endpoint user experience

A user or an attendant can use either a feature button (mct-act) or a Feature Access Code (FAC) to activate MCT. Either the recipient of the call, or another user or attendant, can activate MCT.

The mct-act button is effectively the same as the TRC key on the CS 1000. The MCT FAC is similar in function to the MCT FFC on CS 1000.

- Device Adapter endpoint user experience

Administration

For information about MCT configuration, button administration, and FAC administration, see the Communication Manager documentation.

Both Avaya Aura® and CS 1000 use a digit string to activate Malicious Call Trace on devices that do not have an MCT activation button. Avaya Aura® uses an FAC and CS 1000 uses an FFC (or Special Prefix and a digit code) to configure the MCT activation button. To provide a similar user experience, Avaya recommends that administrators use the same digit string in the Communication Manager FAC as the one that was used in the CS 1000 MCT FFC (MTRC).

Device Adapter presents a "MCT-ACT" CM feature button as the **CallTrace** key on the set. Pressing the **CallTrace** key starts the "Malicious Call Trace" feature.

Avaya Aura® MCT requires a Malicious Call Trace controller to perform any additional operations that are required. To specify the MCT deactivation FAC and release all MCT resources, at least one non-SIP station is required. This non-SIP station can be a Communication Manager H.323 or digital station. MCT deactivation FAC is mandatory.

For more information about MCT controller, see the *Avaya Aura® Communication Manager Feature Description and Implementation* guide.

User operation

To trace a malicious call from an analog (adapted CS 1000 500/2500-type) phone:

1. User is on a call and determines that the call is malicious.

2. Flash the switchhook. Dial tone signifies that the call is on hold.

3. Enter the Malicious Call Trace activation FAC.

4. When completed, a dial tone is heard. Press "#" (or enter your extension) to trace the call. A confirmation tone is given.

5. You are reconnected to the call.

To trace a malicious call from a digital or UNIStim phone by using the Malicious Call Trace activation FAC:

1. User is on a call and determines that the call is malicious.

2. Get a second call appearance (including using Transfer or Conference). Dial tone signifies that the call is on hold.

3. Enter Malicious Call Trace activation FAC.

4. When completed, a dial tone is heard. Press "#" (or enter your extension) to trace the call. A confirmation tone is given.

5. You are reconnected to the call.

To trace a malicious call from a digital or UNIStim phone by using the MCT **CallTrace** key:

1. User is on a call and determines that the call is malicious.

2. Press the **CallTrace** key. You remain connected to the call.

To deactivate MCT by using the MCT deactivation FAC:

1. MCT controller accepts the MCT controller request.

2. Any additional operations are performed as per the MCT controller function.

3. Go off-hook or select a call appearance.

4. Enter the MCT deactivation FAC.

5. A confirmation tone is heard.

6. All resources are released.

For more information, see "Malicious Call Trace" in "Appendix H: Call processing features and services."

Media Gateway Controller registration of digital and analog stations

> *** Note:**
>
> This section is applicable to all endpoints other than the UNIStim IP endpoints.

- CS 1000 endpoint user experience

  The user is typically unaware that the endpoint is connected to a Media Gateway Controller (MGC) registered to a server providing call processing. All services are carried out invisibly, except under:

    - System fault conditions such as network failures.

    - Maintenance or administration operations that take the endpoint off-line.

  The MGC finds its controlling call server and registers itself. CS 1000 has the underlying software required to map messages to and from the units in the MGC correctly.

- Device Adapter endpoint user experience

  The MGC finds its controlling call server and registers itself. However, in this case the controlling server is the Device Adapter, which:

    - Maps each device on the MGC by a Terminal Number or TN (legacy Loop, Shelf, Card, and Unit) into information which can be used to retrieve the station identity.

- Registers the device by its SIP identity with the Session Manager.

- Acts as a configuration retrieval interface with Session Manager and Communication Manager.

- Completes any other aspects of the registration of the endpoint.

Unlike the UNIStim endpoints, the non-IP endpoints historically have not needed to register individually. Doing so allows the endpoints the potential to accept new services and features provided by Communication Manager without reworking the architecture.

Related links

[Media Gateway controller registration](#) on page 345

Media Security (RTP versus SRTP)

Media security is obtained by using Secure RTP (SRTP) and Secure RTCP (SRTCP). SRTP encrypts the media content based on a secure key and SRTCP provides statistics and control operations.

> **☀ Note:**
>
> Media security is not available on the following phones for the G.711 10ms, G.723 10ms, and G.729 10ms payloads.
>
> • 200x series phase 0/1 phones
>
> • IP Desk phones 1210, 1220, and 1230

CS 1000 provided the ability to maintain media security by using Secure RTP (SRTP) and Secure RTCP (SRTCP) instead of the insecure base version. This was controlled by a setting in the CS 1000 configuration as the Media Security System default. This could be done by using either the CLI or Element Manager. In either case the system can be set as:

• Never (MSNV)

• Best effort (MSBT)

• Always (MSAW)

This could also be applied to individual IP endpoints as a class of service, overriding the system default. However, the IP stations can also be set explicitly to use the system default (MSSD), and when that changes, the IP station changes as well.

With the Device Adapter, an equivalent operation exists. The cluster can be set with a cluster attribute. For more information, see [Setting the media security policy](#) on page 657.

When the setting is **Always**, any INVITE generated by Device Adapter is sent with only SRTP requested in the Session Description Protocol data. If the setting is **Never**, only RTP is requested. However, with **Best Effort**, both options are requested.

The endpoint also has the option of using media security different from the system setting, through the **Features** field. Enter the applicable CS 1000 class-of-service mnemonic as a feature.

Related links

[Media security feature operation](#) on page 658
[Media security](#) on page 656

Multiple Appearance Directory Number (MADN)

- <u>CS 1000 endpoint user experience</u>

  A Multiple Appearance Directory Number is a DN number that rings on two or more endpoints. A MADN is created when a number must ring on more than one endpoint.

- <u>Communication Manager endpoint user experience</u>

  Communication Manager implements Single Call Arrangement (SCA) through "regular" bridged appearances.

  The 1210 UNIStim phones cannot bridge a call. Hence, Avaya recommends that you do not configure SCA on 1210 UNIStim phones. If SCA is configured on a 1210 UNIStim phone and if the SCA number is active, the user cannot use any other appearances on the 1210 phone to place a call or join another call. This limitation of the 1210 UNIStim phone is the same in both CS 1000 and Communication Manager.

  Multiple Call Arrangement (MCA) is implemented through "MCA" bridged appearances - brdg-appr with "a" parameter.

- <u>Device Adapter endpoint user experience</u>

  Device Adapter uses the Communication Manager implementation of SCA and MCA to replicate MADN.

  When an analog set migrates to Device Adapter, the station may be SCA or MCA. This can be determined from MCRD (MCA denied, which means the station is SCA) or MCRA (MCA Allowed).

  This determines whether the migration tool maps the station DN to a traditional call appearance, a traditional bridged appearance if the extension is shared, or whether it is using the brdg-appr a (bridged appearance, any). After determining the correct type of line appearance, the class of service value is discarded during the migration.

  There is a limitation for specific digital sets. Specific keys may be unable to process features outside a specific list of permissible features. For example, 3902 has three programmable soft keys, but the fourth feature key can only be conference or transfer.

  CS 1000 rejects allocation of unsupported services on a key during administration. Device Adapter is separated from the configuration. To ensure that only valid requests are made to Communication Manager, any button feature allocation that is not allowed on a specific key is ignored.

> **✳ Note:**
>
> The Multiple Appearance DN capability requires Session Manager to be configured to support Multiple Device Access in a very specific manner.
>
> - The maximum number of devices that can log in as this user must be limited to one.
>
> - A new login attempt must be able to over-ride an existing logged in registration.
>
> This allows an endpoint registered to Device Adapter that reboots or loses network connectivity to Device Adapter to register at any Avaya Breeze® platform in the Device Adapter cluster, or in a server 1/server 2 case, to register with the backup cluster. Otherwise, the new registration would potentially be blocked.
>
> For more information about Multiple Appearance DN handling on Device Adapter, see "Multiple Appearance Directory Number (MADN)" in "Appendix H: Call processing features and services."

Multi-Device Access

The Multi-Device Access (MDA) feature is a capability provided by the Avaya Aura® SIP services.

Multi-Device Access is defined in the *Avaya Aura® Communication Manager Feature Description and Implementation* guide as follows:

"With the Multi-Device Access (MDA) feature, a SIP user can register more than one SIP device with a single extension. For example, a user has 96X1 at the desk, 96X1 in the lab, and Avaya one-X® Communicator on the laptop. All these devices are registered with the same extension 123456. When a call arrives at extension 123456, all the devices are alerted. The user can answer the call from any one of the devices. If required, the user can bridge on to the call from one of the idle devices by using the Simulated Bridge Appearance (SBA) feature. Therefore, the call can be handed off between devices without parking the call."

Depending on the configuration, MDA allows up to 10 SIP endpoints to register concurrently. However, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint. An administrator can use the MDA configuration fields to configure the Sequential Registration feature. Sequential Registration allows one device to be registered at one time. If you configure the MDA feature to allow a new registration when the maximum number of devices registered is reached, Session Manager terminates the oldest registration to allow the new SIP registration. However, in Sequential Registration because registration of only one device is allowed at a time, the devices log in sequentially and not concurrently.

- CS 1000 endpoint user experience

  CS 1000 does not have a feature that aligns to the MDA feature. There were provisioning models that appeared similar, but they did not support user login and the pairing of the phones was permanent.

  Each CS 1000 station was programmed by using a "device physical port" definition or Terminal Number (TN).

Administrators could configure two stations with the same definition and with identical DN keys by using MADN. As the primary DN key (which is key 0) was the same, both stations used the same identity for outgoing calls.

For example, a user has a 3904 desk phone (12 feature keys) and a 2050 soft client (12 feature keys) with the following configuration:

- Configuration of features and class-of-service options is the same on both the endpoints.

- Key 0 would normally be SCA, ringing or non-ringing (although, MCA is also possible). Key 0 is configured for the directory number 555-1212 with the associated name Alice Doe.

- Key 1 can be shared within a department. Key 1 is configured for the directory number 555-2112 with the associated name IETF Docnames. This is normally MCA.

- Keys 2 through 11 can be any other legitimate keys.

- The soft keys matched definitions as well.

The following is the feature experience in CS 1000:

- If Alice dialed from either phone on the prime DN (555-1212), the outgoing call has the identity Alice Doe with the number 555-1212.

- If an inbound call arrives at 555-1212, both phones ring and Alice can answer on either of the phones. If the line was SCA, the other phone shows the call status and can be used to join the call. The called-party information shows Alice Doe with number 555-1212.

- If Alice dialed by using the team number, the configuration option selected determines whether the name and ID of Alice's prime DN key (that is, key 0) is used or whether the information for key 1 is used.

- If an inbound call arrives at 555-2112, all user endpoints with this number would ring. If Alice answers this call, then all other endpoints would show idle. If anyone else answers this call, then Alice's endpoints would show idle.

This is similar to the MDA user experience on the Avaya Aura® SIP endpoints, except the following:

- Login is not needed.

- Logout is not possible.

- Is not limited to IP endpoints.

- Consumes additional licenses because a new set is defined for every new paired device.

• Communication Manager endpoint user experience

Administrators can configure the number of devices that can SIP register simultaneously to Session Manager. A minimum of 1 up to a maximum of 10 SIP devices can register at one time. Administrators can use the MDA-related configuration fields to configure the number of devices for MDA. Allowing two or more SIP endpoints to register concurrently is called MDA. Allowing one endpoint to register at one time is called Sequential Registration as there was no official name for this feature in Device Adapter Release 8.0.1.

For example, a user has a 96x1 at the desk, a 96x1 in the lab, and an Avaya Workplace Client on the laptop. All these devices are registered with the same extension 123456. For MDA, the **Max. Simultaneous Devices** must be set to 2 or higher.

When a call arrives at extension 123456, all three devices are alerted. The user can answer the call from any one of the devices. This consumes the call appearance on all three devices. If a user answers the call on call appearance 1 on Avaya Workplace Client, the other two 96x1 sets show the call appearance 1 as being in use on another device.

If required, the user can bridge on to the call from one of the idle devices by using the Simulated Bridge Appearance (SBA) feature. Therefore, the call can be handed off between devices without parking the call. The user can move from Avaya Workplace Client to 96x1 and take over the call from there.

The preceding MDA user experience is similar to that of SCA ringing a prime DN.

Depending on how an administrator has configured MDA for an Avaya Aura® user, the Avaya Aura® user can register up to 10 SIP devices with the same extension.

In addition, administrators can select or clear the **Block New Registration When Maximum Registrations Active** check box in System Manager to determine how Session Manager handles new registration requests when the maximum number of registrations is reached for the SIP extension.

For example,

- The user has **Max. Simultaneous Devices** set to 2.

- The user uses three devices, which are, 96X1 in the office, 96X1 in the lab, and Avaya Workplace Client on the laptop.

- The user typically uses the 96X1 in the office or Avaya Workplace Client, and both are registered.

- The user is registered at the 96X1 in the office first, and then at Avaya Workplace Client.

If the user tries to register at the 96X1 in the lab, then depending on the configuration, Session Manager does any one of the following:

- If the **Block New Registration When Maximum Registrations Active** check box is selected, Session Manager rejects the registration. The user must manually end the registration of one of the registered devices to allow the new registration.

- If the **Block New Registration When Maximum Registrations Active** check box is cleared, the registration is allowed. However, because only two devices can concurrently register, Session Manager un-registers the device that is registered for the longest period of time, that is, the 96x1 in the office.

The preceding option of terminating a current SIP registration and allowing a new registration is the core of the Sequential Registration feature. Although, the Sequential Registration feature name is not used in the Avaya Aura® documentation, the administrative options allow a user to register the endpoints sequentially.

For example, a user has a 96x1, a J-series, and an Avaya Workplace Client. The initial state has the user logged in to the 96x1 as the user identity.

The user can do the following:

- The user logs in to the J-series. When Session Manager receives the SIP registration request for the J-series, Session Manager terminates the registration of the 96x1.

- The user then logs in to the Avaya Workplace Client. When Session Manager receives the SIP registration request for the Avaya Workplace Client, Session Manager terminates the registration of the J-series.

This sequential registration of endpoints can continue indefinitely.

For more information, see the *Administering Avaya Aura® System Manager* guide.

• Device Adapter endpoint user experience

Multi-Device Access – also called Multiple Device Access in some documents – is a Session Manager capability and configuration that is leveraged by Device Adapter.

MDA allows a minimum of 2 up to a maximum of 10 SIP endpoints to register concurrently as the same user identity. However, Avaya recommends that out of the 10 SIP endpoints only one endpoint should be a Device Adapter UNIStim endpoint. This is because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA. The remaining devices must be other traditional Avaya Aura® devices. These devices can simultaneously register to Communication Manager and can share the same Avaya Aura® license. With Device Adapter, you can have one Avaya Aura® license for a Communication Manager extension. You can use the same license to configure MDA for up to 10 simultaneous SIP devices for the same user.

Administrators can also configure whether Session Manager should allow or block new registrations when the maximum number of devices registered is reached.

However, administrators can set the maximum number of concurrently registered devices to 1. If device 1 is registered and device 2 tries to register, Session Manager terminates the registration of device 1 and registers device 2. This configuration of allowing only one device to register at one time is called Sequential Registration.

Sequential Registration is a crucial part of the capabilities allowing for fail-over and other useful operations. For more information, see

For more information about MDA and the associated limitations, see "Multi-Device Access" in "Appendix H: Call processing features and services."

Mute

In general, Mute and Unmute are automatic functions. However, IP phones have an enhancement that can be configured on a per set basis.

There is one CS 1000 and Device Adapter item where this differs from generic mute. When an IP phone has the Mute key allowed (MUTA) class-of-service, the typical behavior experienced on all other endpoints applies. MUTA is a Device Adapter feature.

However, if the endpoint is configured with the Mute key denied (MUTD) feature, the button is still present. But, instead of muting the call, the button places the call on hold, possibly with an on-hold music.

In a MUTD IP phone, the Mute button can be a toggle, which places the call on hold and retrieves the call.

For more information, see "Mute" in "Appendix G: Generic station operations."

No Hold Conference

- CS 1000 endpoint user experience

CS 1000 supports a conference soft key for UNIStim, 39XX and digital 200X endpoints. The conference key on UNIStim and 39XX endpoints is a fixed key whereas on digital 200X endpoints, the key is not fixed and you can configure it as required.

CS 1000 does not support the no hold conference feature on analog endpoints because the no hold conference feature requires a feature key to perform the feature operation.

No Hold Conference allows you to establish a conference call without placing the current caller on hold. No hold conference feature continue the active call as long as you dial you dial an extension number of the participant or until the participant for no hold conference answers the call. You cannot use ring back feature with the no hold conference feature.

CS 1000 supports following variants of No Hold Conference feature:

- Basic No Hold Conference

  The following is the user procedure for the basic no hold conference feature:

  1. During an active call, the user presses the **NoHoldConf** key.

     The **NoHoldConf** feature key icon is lit, which shows that the feature is active.

  2. The user dials the required extension number followed by **#**.

     If the administrator has pre-configured the extension number, then pressing the **NoHoldConf** key will establish the conference directly.

  3. Depending on the state of the endpoint, the **NoHoldConf** key shows the following status:

     - Flashing lamp (60 ipm): Indicates that the destination extension is ringing.
     - Fast Flashing lamp (120 ipm): Indicates a failed attempt for establishing conference using no hold conference.
     - Dark lamp: Indicates a successful or terminated no hold conference attempt.

  4. If the call is not answered, a user can end the outgoing call by pressing the call appearance DN key.

- No Hold Conference with Autodial: The administrator programs a Conference Autodial (CA) button which combines the NHC feature with the autodial feature programmed with an auto dial number.

The following is the user procedure for no hold conference with the autodial feature:

1. During an active call, the user presses the **CA** key.

   The **CA** feature key icon is lit, which shows that the feature is active.

2. Depending on the state of the endpoint, the **CA** key shows the following status:

   • Flashing lamp (60 ipm): Indicates that the destination extension is ringing.

   • Fast Flashing lamp (120 ipm): Indicates a failed attempt for establishing conference using autodial feature.

   • Dark lamp: Indicates a successful or terminated conference autodial attempt.

3. If the call is not answered, a user can end the outgoing call by pressing the call appearance DN key.

- No Hold Conference with Speed dial: The administrator programs a Conference-Speed Call (CS) button which combines the NHC feature with the speed dial feature programmed with the speed call list.

The following is the user procedure for No Hold Conference with Speed dial:

1. During an active call, the user presses the **CS** key.

   The **CS** feature key icon is lit, which shows that the feature is active.

2. The user enters the index of the desired entry.

3. Depending on the state of the endpoint, the **CS** key shows the following status:

   • Flashing lamp (60 ipm): Indicates that the destination extension is ringing.

   • Fast Flashing lamp (120 ipm): Indicates a failed attempt for establishing conference using speed dial feature.

   • Dark lamp: Indicates a successful or terminated conference speed call feature.

4. If the call is not answered, a user can end the outgoing call by pressing the call appearance DN key.

- No Hold Conference hotline: The administrator programs a Conference Hotline (CH) button which combines the NHC feature with the hotline one-way feature programmed with a destination number.

The following is the user procedure for No Hold Conference with hotline one-way feature:

1. During an active call, the user presses the **CH** key.

   The **CH** feature key icon is lit, which shows that the feature is active.

2. Depending on the state of the endpoint, the **CH** key shows the following status:

   • Flashing lamp (60 ipm): Indicates that the destination extension is ringing.

   • Fast Flashing lamp (120 ipm): Indicates a failed attempt for establishing conference using hotline one-way feature.

   • Dark lamp: Indicates a successful or terminated conference hotline feature.

3. If the call is not answered, a user can end the outgoing call by pressing the call appearance DN key.

The phone screen displays the number of participants in the conference by displaying the number with the feature label. As an example, if the phone screen displays CONFERENCE 3

this means the conference has total three participants which includes the user and other two participants.

- Communication Manager endpoint user experience

Communication Manager supports the no hold conference feature with the help of **no-hld-cnf** feature key. The same button is used in Device Adapter endpoints.

- Device Adapter endpoint user experience

Device Adapter supports the no hold conference for UNIStim and Digital endpoints. The administrator programs a feature key for the no hold conference on one of the feature keys or on the key expansion module.

Device Adapter supports only the basic no hold conference and the conference auto dial feature, the user procedure remains the same. Conference with speed dial list and hotline are not supported on Device Adapter.

Park and Page

CS 1000 style Park and Page functionality is available when Device Adapter is paired with the Call Park and Page Snap-in. The Call Park and Page Snap-in must be deployed in a dedicated Avaya Breeze® platform cluster to enable this functionality.

Refer to the *Call Park and Page Snap-in Reference* for additional information and procedures associated with this snap-in. This document is available on the Avaya Support portal.

Related links

Personal Directory, Callers List, and Redial List

The CS 1000 stations have two variations on a redial list:

- UNIStim stations use a redial list stored in the system, allowing a larger capability.

The Personal Directory, Callers List, and Redial List use a central database, called the IP Phone Application Server, to store directory data and user profile options. The Personal Directory allows a user to enter or copy names to a personal directory, delete entries, or delete the entire list. The Callers List and Redial List are call log features. The content of these lists is generated during call processing. Content cannot be changed. However, a user can delete or, in some cases, copy entries or lists to the Personal Directory.

- Digital 3903 and 3904, phase 3, stores the information on the station.

The system features document for CS 1000 mentions: "The contents of the Redial List, Personal Directory, and Call Log are stored on the Avaya 3900 Series Digital Deskphones itself between login sessions."

In all cases, on CS 1000, the user can access the lists in different ways.

- The Personal Directory is always accessed on an idle station from the dedicated hard button for the directory and log options. The user presses the up and down arrows to access the desired one of the three services and selects it. A password may be required.

  After accessing the directory, the user may scroll through the entries in the directory, delete entries, call the target, or add entries (possibly an entry copied from the callers list or redial list). Up to 100 entries may exist in the directory for most stations supporting the service.

- The Caller List is a log storing the numbers of the last block of callers to the station. Usually 100 entries, but certain stations may limit the number of entries. When the limit is reached, the oldest entry is removed for a new caller.

  The user can access through the Directories and logs hard key on an idle station and select the Callers Log option. Alternatively, the user can select the Callers soft key on the idle station.

  When accessed, the user can scroll up and down through the list and scroll right to see more information or scroll left to return to the list. The information indicates the number of times a caller has called. For example, if a caller at 1-555-555-0100 called four times, this will indicate four calls occurred. There will be one entry indicating four calls, and not four entries.

  The entries include names if a name was presented with the call. If no name was presented, then caller's number is displayed.

  When an entry is selected, the user can copy it for the directory, delete it, or call it.

- The Redial List is the mirror of the callers list, storing the last 20 parties called. Similar to the Callers List, the entries can be copied, called, or deleted. In addition, when the list is full, the oldest entry is removed if a new entry is added.

Device Adapter maintains this operation. The 3903 and 3904 use the existing firmware on the station. UNIStim stations rely on the PPM to store the information.

Device Adapter stores Phase 3 Callers and Redial list information on PPM. The information is stored per user basis. Call history information of the user is shared between different clusters.

For more information, see "Personal Directory," "Callers list," and "Redial list" in "Appendix H: Call processing features and services."

Related links

Enabling Personal Directory support on page 207

Presence notification

Device Adapter publishes the Presence status of the endpoints that are migrated to the Avaya Aura® solution. The Presence status indicates whether a migrated endpoint is active or inactive, that is, on a call or not. These migrated endpoints are not presence capable. The Presence status of the migrated endpoints is published so that other Presence-capable endpoints that are within the Avaya Aura® solution can display it to the interested users.

To enable Presence notification, you must configure the users of the migrated endpoints by using the Avaya Aura® Presence Services snap-in. For more information, see "Checklist for configuring Presence/IM users" in the *Avaya Aura® Presence Services Snap-in Reference* guide.

Privacy (Communication Manager Exclusion)

- CS 1000 endpoint user experience

  Multiple Call Arrangement calls are always private. When a user answers or places a call, there is no indication on any other endpoint sharing the number that the call is in progress. If the lamp flashes while the call rings, the lamp becomes dark and is inaccessible on all stations except that of the person who answered the call.

  By using the Single Call Arrangement functionality, any user sharing the SCA DN can bridge into the call by pressing the corresponding SCA DN key unless the user has invoked privacy.

  A call is private by default. If the user presses the **Privacy Release** soft key, the call toggles into the non-exclusive mode and all DN appearances on all phones blink. Any user sharing the DN can press the DN button. This turns the call into a conference.

  Only one user can bridge in for each **Privacy Release** key press.

- Communication Manager endpoint user experience

  The Exclusion feature is similar. It is activated in the following ways:

  - Manual Exclusion - Users turns the feature on or off by using the **Exclusion** button.

  - Automatic Exclusion - The feature is activated when a user makes a call. Users must manually deactivate it.

  - Buttonless Automatic Exclusion - The feature is activated when a user makes a call and deactivate when the call ends.

- Device Adapter endpoint user experience

  Privacy Release maps to Automatic Exclusion in Device Adapter. Device Adapter adapts this feature in the following ways:

  - The Privacy Release key is mapped to the Exclusion feature button during the database migration.

  - Device Adapter treats the **Exclusion** button as Privacy Release providing existing localization.

  - Phone stations should be configured with Automatic Exclusion. This means Exclusion is activated when a user makes or answers a call and deactivated after the call is ended.

  - Pressing the **Privacy Release** key toggles the Exclusion state.

  - When Exclusion is off, the corresponding DN lamp blinks (U-Hold icon). Other users on bridge appearances do not receive the blink indication when Exclusion is off.

  - When Exclusion is on, the lamp returns to the original state.

- Extra call processing specifics for Exclusion are done by Communication Manager.

- All conference participants must press **Privacy Release** for others to join the conference.

- If the station with call appearance is on hold, turning off Exclusion and bridge could replace call appearance on the call.

However, analog phones do not have the **Privacy Release** (**Exclusion**) button; and hence, cannot change the state of the call to private. Avaya recommends that administrators do not enable **Exclusion** when analog endpoints are used along with digital and UNIStim endpoints. Otherwise, call handling becomes inconsistent and the analog endpoints are unable to make calls unless all other users are not using the call appearance.

The 1210 UNIStim phones cannot bridge a call. Hence, Avaya recommends that you do not configure SCA on 1210 UNIStim phones. If SCA is configured on a 1210 UNIStim phone and if the SCA number is active, the user cannot use any other appearances on the 1210 phone to place a call or join another call. This limitation of the 1210 UNIStim phone is the same in both CS 1000 and Communication Manager.

For more information, see "Privacy" in "Appendix H: Call processing features and services."

Private Line Service

- CS 1000 endpoint user experience

Private Line Service feature reserves PSTN trunks for making and answering calls on specific endpoints.

These endpoints are provisioned with the Private Line key associated with one specific trunk. You cannot access other trunks in the trunk route using the Private Line key.

The PSTN trunk uses the bi-directional line appearance of a specific DN which means that PVR and PVN private line keys uses the reserved PSTN trunk for both incoming and outgoing calls.

In most cases, only a single user will have the DN assigned to the private line key. However, the key may be shared in some cases. As an example, a manager and an executive assistant may share the same private line key.

Using the private line key, a user can directly make outgoing calls to the public network without dialing any route access code, or without using Electronic Switched Networking (ESN) dialing. When the CS 1000 user presses this button, the reserved PSTN trunk is automatically connected to the endpoint and the user receives the dial tone. After hearing the dial tone, the user can dial the required digits of the called party. The caller ID for the outgoing caller ID will be the prime DN that is key 0 in this case.

> ✱ **Note:**
>
> Users should not make internal calls with the private line key. If a user dials an internal number using the private line key, the PVR or PVN key creates a connection with PSTN and a loop with CS 1000, which will use two trunks for an internal call.

CS 1000 routes the incoming calls on the reserved trunks by routing the call to the directory number assigned to the private key. The directory number can be a single appearance or a

multiple appearance number. If MCA is enabled on the private key then all parties sharing the private trunk will have separate private line keys to answer the incoming call but bridging into the call will not be allowed.

- Device Adapter endpoint user experience

  Hotline two-way feature allows an administrator to program a number as an autodial number for a Device Adapter endpoint. The autodial number must be the TAC to reserve the trunk and make an outgoing call. The administrator or the user can change the label to **PVR** or **PVN** for the private line service feature or program the label to show the bridged appearance used for the hotline number for the private line service feature.

  As an example, if a PSTN user calls 1-303-555-1212 to call the private line internal number 1212, the button may be programmed to display 1212 or 5551212, which works similar to CS 1000 user experience functionality.

  A Device Adapter endpoint user answers the incoming calls by pressing the flashing bridged appearances. Bridged appearances in the Private Line Service feature must be in the SCA mode.

Release key

The Release Key is a fixed key on the digital and UNIStim stations used mainly to clear the calls. It performs the same function as the Communication Manager Call Drop button.

The Release Key also has historical uses where it can be used during feature operations as a Cancel or Quit button. The earlier digital stations did not have soft keys; and therefore, the Release key was used in its place.

Related links

[Release key](#) on page 394

Ring Again

- CS 1000 endpoint user experience

  Ring Again is programmable for UNIStim and 39XX endpoints at a fixed position, and digital 200X endpoints at an unfixed position. For UNIStim and 39XX endpoints, it maps to a soft key. This feature works in the following manner:

  - User makes a call to a busy destination. The phone displays the **Ring Again** key.

    ✳ **Note:**

    The phone does not display the **Ring Again** key if the call was made using a PSTN trunk.

  - User presses the **Ring Again** key.

  - The phone screen returns to an idle state with the **Ring Again** key indicating it is active.

- The user can cancel the Ring Again request by pressing the **Ring Again** key before a callback offer is received. A callback offer is received when Avaya Aura® presents the Ringout call invitation.

- When the far-end becomes available, a callback offer is presented to the endpoint. The **Ring Again** key flashes and an audible tone is heard to indicate that a callback offer is received. The user cannot cancel the Ring Again request after the callback offer is received.

- User places a call by selecting a line and pressing the **Ring Again** key.

The Ring Again feature can be activated for calls made from any line DN key. A corresponding variant is available for Ring Again on No Answer (RANA). For RANA, the same button is used, but the behavior is different.

Upon encountering a station that does not answer, a station with the Ring Again capability can activate RANA by pressing the **Ring Again** key. Later, when the desired station goes off-hook to make or receive a call, and then goes on hook, the station that activated Ring Again receives a ring through the telephone's loudspeaker and the lamp flashes if the station is idle. The station user can dial the desired station by lifting the handset and pressing a DN key, and then pressing the **Ring Again** key.

This feature works as follows:

1. User A calls user B. User A receives a ring back tone.

2. The user waits long enough to decide to activate RANA.

3. User A presses the **Ring Again** (RGA) key. The RGA key indicator turns on steadily.

4. User A either goes on-hook or presses the Release (RLS) key. The indicator associated with RGA key remains on and user A is now free to receive or make other calls.

5. User B goes off-hook to make a call, and then goes on-hook. User A is given a short ring through the loudspeaker and the indicator associated with the RGA key flashes.

6. User A either picks up the handset or presses a DN key. User A receives dial tone.

7. User A presses the RGA key. The user against which the Ring Again was placed is rung and the indicator associated with the RGA key is turned off.

If the called party does not accept the call in a duration of six ringing cycles, the request is cancelled. If no appearances are available during that time, the request is cancelled.

If the called party goes off-hook, and if the calling party accepts the Ring Again on No Answer request, the calling party may encounter Ring Again, Busy case.

- Communication Manager endpoint user experience

This feature maps to the Automatic Callback functionality. This feature works in the following manner:

- The phone is assigned the **Automatic Callback** key.

- The **Automatic Callback** button becomes available when a call is made to a busy extension or when a destination does not answer.

- When the destination extension finishes the call or in case of a no answer scenario where the called party becomes active on a call and finishes the call, a Ringout call is initiated.

- The originating phone is notified of the destination's availability.

- The Callback call is presented to the destination phone when the originating phone goes off-hook.

The following limitations exist in the Communication Manager implementation when compared with CS 1000:

- Users cannot activate Automatic Callback from a bridged call appearance.

- If a user activates Automatic Callback from a primary extension number, the return call notification rings at all bridged call appearances.

❗ Important:

There should be a wait time of 32 seconds before attempting second Ring Again to same phone as the previous, over the same network.

• Device Adapter endpoint user experience

This feature is implemented in the following ways:

- For UNIStim endpoints, the **Ring Again** feature key is mapped to the **Auto Callback** key at a fixed position key. This fixed position key maps to a context-sensitive soft key and is active only when the capability is needed and applicable. Device Adapter treats it as a legacy RGA button and provides localization for UNIStim and all 39xx endpoints, except the 3901 endpoints.

For digital M3903, M3904, and M3905 sets, the **Ring Again** feature key is mapped to the **Auto Callback** key at a fixed position in the soft keys, in the same way it is done for the UNIStim endpoints. Other digital sets must have the **Auto Callback** key assigned to one of the available programmable keys. Device Adapter treats the **Auto Callback** button as a legacy RGA button, and provides localization for the M3902 set that has programmable soft keys, and for the M3903, M3904, and M3905 sets.

Analog sets can invoke Ring Again by using the Communication Manager Automatic Call Back Feature Access Code. Device Adapter treats it as a Flexible Feature Code equivalent.

- When the destination is busy and the user presses the **Ring Again** key, Device Adapter subscribes to a Ringout call. The **Ring Again** key with an arrow now appears on the idle screen.

- When the destination does not answer and the user presses the **Ring Again** key, Device Adapter subscribes to a Ringout call. The **Ring Again** key with an arrow now appears on the idle screen. However, in this case, the called party must become active and then become idle to send an indication to the party that activated the Ring Again.

- The user can cancel the Ring Again request by pressing the **Ring Again** key before a callback offer is received. A callback offer is received when Avaya Aura® presents the Ringout call invitation.

- When the endpoint receives a callback offer, the **Ring Again** key flashes and an audible tone is heard to indicate that a callback offer is received. The user cannot cancel the Ring Again request after the callback offer is received.

- When Ringout call is presented by CM, the user receives an incoming call on a free call appearance, and Ring Again soft key flashes indicating this is a Ringout call.

- If the user does not accept the Ringout call before the offer times out, Ring Again is cancelled.

- If the user is on a call, a tone burst is heard and a lamp flashes.

- The user answers this Ringout call like a normal call by off-hook or by selecting the ringing call appearance.

- When the **Ring Again** key flashes to present the callback offer, the user can press the **Ring Again** key to ignore the offer. The **Ring Again** key becomes dark and the audible tone stops. Pressing the **Ring Again** key only ignores the callback offer and does not cancel it. The offer automatically times out after the time-out period is reached.

This behavior is similar to the Ignore option on the Avaya Aura® SIP endpoints. When a callback offer is presented on an Avaya Aura® SIP endpoint, the **Ignore** soft key appears on the endpoint. The user can press the **Ignore** soft key to ignore the callback offer.

✱ **Note:**

There is a difference in configuration between Device Adapter and Communication Manager phones. Device Adapter phones have one call appearance by default and Communication Manager phones have two. Additionally, Communication Manager phones cannot deactivate Ring Again (Automatic Callback) when both call appearance lines are busy. This same behavior is applicable to a Device Adapter phone.

If both lines become busy, users will not be able to use Ring Again unless they restart their phone. The following is an example of this scenario on Device Adapter phones:

 - Assume that User C has only one available call appearance.

 - User A calls User B. User B answers.

 - User C calls User A but User A does not answer. User C presses Ring Again to invoke Ring Again against call User A.

 - User D calls User C and User C answers.

 - User A and User B end their call.

 - The Ring Again is cancelled because there is only one call appearance at user C, and that appearance is in use.

 - User C and User D end their call. Ring Again does not happen.

It is recommended that a second call appearance be configured for Device Adapter phones so that this limitation is not encountered.

For more information, see "Ring Again" in "Appendix H: Call processing features and services."

Send All Calls when the presence status is set as DND

An Avaya Aura® SIP endpoint user can set the presence status from the following available options:

- Automatic
- Available
- Busy
- Away
- Do not Disturb
- Out of Office
- Offline

A user can set the status as DND and can redirect all the incoming calls by implementing the Send All Calls feature.

If the administrator has configured the SAC feature for a user, then the phone screen displays an active icon on the SAC feature key.

If the user changes the status from DND to any other available status options, the SAC feature will be disabled automatically and the active icon will no longer be available for the Send All Calls feature key.

For more information, see the *Avaya Aura® Communication Manager Feature Description and Implementation* document.

CS 1000 and Device Adapter does not support the Send All Calls (SAC) when the presence status is set as DND feature. You cannot set the presence status as DND on the Device Adapter endpoints.

The Presence status options available on the Device Adapter endpoints are active and inactive.

A Device Adapter endpoint can use the SAC feature to redirect the incoming calls only if the user set has set DND on an Aura SIP set (96xx) or on Avaya J-series endpoint and sequentially registers on a Device Adapter phone. The Device Adapter endpoint can activate or deactivate the Send All Calls (SAC) feature but the already set presence status (DND in this case) will not change on the Device Adapter endpoint.

Sequential Registration

As opposed to Multi-Device Access (MDA), which allows 2 or more concurrent endpoint registrations, Sequential Registration allows one endpoint to be registered at one time. You can use the Multi-Device Access (MDA) configuration fields to limit the number of concurrent registered devices to 1 for Sequential Registration.

You must use Sequential Registration, instead of MDA, when a user wants to use multiple UNIStim endpoints so that the number of concurrent registrations is limited to 1. This is because registering two or more UNIStim endpoints with the same TN is non-deterministic in MDA.

Whether a new endpoint can register for MDA or Sequential Registration depends on whether you select or clear the **Block New Registration When Maximum Registrations Active** check box.

- If the **Block New Registration When Maximum Registrations Active** is selected, then the user must manually un-register an existing registered endpoint before registering a new endpoint. Typically, the user logs out from the endpoint to un-register the endpoint.

- If the **Block New Registration When Maximum Registrations Active** is cleared, Session Manager un-registers an existing endpoint that is registered the longest period of time to register the new endpoint.

For example, a user has a 96x1 at the desk, a 96x1 in the lab, and an Avaya Workplace Client on the laptop. All these devices are registered with the same extension number 123456.

- If the user registers with the 96x1, then Session Manager clears any prior registration.

- If the user registers with the J-Series, then Session Manager clears the 96x1 registration.

- Similarly, every new registration clears the old registration.

- <u>CS 1000 endpoint user experience</u>

  The registration handling process upon network failures for UNIStim endpoints and for endpoints on MGC servers in Sequential Registration is similar to that of the CS 1000 TPS.

  The following is the initial registration recovery attempt in CS 1000 for UNIStim endpoints and MGC:

  - UNIStim endpoint: When a CS 1000 UNIStim endpoint restarts or fails over, it attempts to register with the TPS load balancer of the primary server (S1). The UNIStim endpoint may or may not register on the same TPS.

  - MGC: When CS 1000 MGC restarts or fails over, it attempts to register with the primary call server.

  The following the registration recovery attempt in CS 1000 when initial registration attempt fails:

  - UNIStim endpoint: If the primary server TPS is unavailable, then the TPS on the geo-redundant alternate data center is attempted. The endpoint attempts the alternate server (S2). In this case, it does not register on the same CS 1000 that it was originally using. Therefore, it uses a different TPS load balancer.

  - MGC: If the primary call server is unavailable, then a geo-redundant alternative is attempted. MGC attempts to register with the alternate server.

    MGC allows triple redundancy. Which means, there can be a primary MGC and two alternate MGCs that control the devices, unlike the S1/S2 (primary and one alternative) of the UNIStim endpoints.

    If two alternate servers are defined, then MGC attempts the first alternate server. Because triple redundancy is designed to provide a geo-redundant recovery, MGC does not register to the same call server it was originally using. In addition, because there are two alternate servers, if the registration or registration attempt to the first alternate server fails, MGC attempts to register to the second alternate server.

For more information, see the *Communication Server 1000E Planning and Engineering* guide and the CS 1000 documentation.

In both cases, CS 1000 identifies the hardware ID of the registering endpoint or the TN entered by the user when registering a UNIStim endpoint. CS 1000 uses the hardware ID or TN to allow or block fail over and endpoint registration when a UNIStim endpoint or MGC restarts or loses connectivity to the current target. If there is a mismatch in the hardware ID between the original registration and the new one, the registration fails.

Unlike Sequential Registration, CS 1000 rejects a new device attempting to register to an existing registration, but accepts a re-registration on another TPS or call server.

This CS 1000 behavior can be deemed as conditional Sequential Registration. If the same device re-registers at another TPS, the registration is allowed. If a device with a different hardware ID tries to register, the registration is denied.

- Communication Manager endpoint user experience

When a device is already SIP registered, and the user registers from elsewhere as the user identity, Session Manager does the following:

  - Session Manager:

    - Verifies the user identity that is attempting the registration.

    - Detects whether a current registration exists.

    - Detects whether the **Max. Simultaneous Devices** is set to 1. Therefore, the maximum number of devices registered is reached.

  - Session Manager verifies if the user profile is configured to allow or block new registrations:

    - If the **Block New Registration When Maximum Registrations Active** check box is selected, the registration request is rejected. The user must manually un-register an existing device to register the new device.

    - If the **Block New Registration When Maximum Registrations Active** is clear, Session Manager does the following to allow new registrations:

      - Session Manager terminates the registration of an existing device to register the new device.

      - The new registration is completed. If necessary, the device data is mapped to a format suitable for the new endpoint. For example, allowing a J-series to register as a 96x1 identity.

- Device Adapter endpoint user experience

Device Adapter supports Sequential Registration. To configure Sequential Registration, set the MDA configuration fields to the following:

  - Set the **Max. Simultaneous Devices** value to 1.

  - Clear the **Block New Registration When Maximum Registrations Active** check box to allow new registrations. Session Manager terminates the registration of an existing device to register the new device.

This provides a similar CS 1000 user experience in case of a fail over or endpoint restart. However, if a user tries to register a second station to CS 1000, CS 1000 blocks the registration attempt. This is because the fail-over handling in CS 1000 does not find a match in the hardware IDs of both requests.

Whereas, Device Adapter allows the new registration request because the device ID is not available and cannot be sent to Session Manager. If the Session Manager user profile is set to allow new registrations when the maximum number of registered devices is reached, Session Manager allows another endpoint to register by using Sequential Registration.

Sequential Registration allows sequential registration for any endpoint that can use the CS1K-IP station definition to define the endpoint. Although, the Avaya Aura® SIP endpoints will have a different user experience.

The following is an example of Sequential Registration:

1. Device X is SIP registered as the user identity A.

2. Device Y attempts to SIP register as the user identity A.

3. Session Manager verifies whether this is a permissible registration and does one of the following:

   • If the configuration is to block new registrations, the registration request is rejected.

   • If the configuration is to allow new registrations, Session Manager terminates the SIP registration of device X and registers device Y.

For more information, see "Sequential Registration" in "Appendix H: Call processing features and services."

Speed Dial (Speed Call)

Speed dial is frequently used as a phrase to refer to all mechanisms to place a call rapidly. As such, the Autodial feature is frequently included in speed dial.

However, on CS 1000 1speed dial is more accurately the use of one of the Speed Call List variants.

There are two main speed call types:

• Speed Call Lists (SCL): Allows users to place calls by dialing a one-digit, two-digit, or three-digit code. You can use Speed Call for both internal and external calls. To use Speed Call, digital and UNIStim telephones and attendant consoles can have a Speed Call key/lamp pair.

   CS 1000 allowed up to 8191 lists, including speed call lists and system speed call lists.

• System Speed Call (SSC): Extends the capabilities of Speed Call. In addition to abbreviated dialing, System Speed Call allows a user to temporarily override the telephone's Class of Service, Trunk Group Access Restrictions (TGARs), and code restrictions.

Analog endpoints on CS 1000 can also access speed call capabilities by using the applicable feature access code.

Users on CS 1000 can be speed call list users or controllers. A user can use the list but cannot edit it. The controller can change the entries.

A user can make a call with a speed call list (or system speed call list) by either selecting a line and pressing the speed call button, and then entering the index of the desired entry. For devices without a speed call button the user accesses the list by going off hook, dialing the FFC for the speed call access, and dialing the index of the desired entry.

A controller can use the list as it exists or add a new entry. The new entry is added while on hook and without selecting a line. The user presses the speed call key (the lamp flashes), dials the index for this number (0 to 999), and enters the number followed by the octothorpe (#). If accepted, the lamp becomes dark. Otherwise, the lamp continues to flash.

Device Adapter behavior is similar but uses the Communication Manager Abbreviated Dialing Lists. Each user has access to only one of the three sets of system tables.

When the user selects a line and presses the key to make a call, Device Adapter prompts for the index. After the index is received, Device Adapter requests the abbreviated dialing service from Communication Manager and the call proceeds.

When the user selects a line and dials the FAC for the abbreviated dial list, Communication Manager provides audible feedback for the FAC and accepts the list entry.

To program the list, the user either enters the FAC and enters the data, or presses the speed call button while no line is selected and enters the data.

These actions make the user experience almost identical to the CS 1000 experience.

For more information, see "Speed Dial" in "Appendix H: Call processing features and services."

Signaling Security

CS 1000 supports TLS between CS 1000 and outside destinations for SIP signaling, and Datagram Transport Layer Security (DTLS) between the CS 1000 and UNIStim stations. Signaling security is not an issue between the MGC and the call server as the signaling used a proprietary, byte-by-byte signaling protocol.

As with the media security, the DTLS settings allowed Never, Best Effort, and Always.

This is maintained for Device Adapter, including maintaining the terminology for the options. However, using signaling security requires a CA root certificate installed on the IP station.

Related links

Tone and cadence settings

- CS 1000 endpoint user experience

Tone and cadences are administered in Overlay 56 as FTC tables. There are no predefined country tables except NA. Typically, administrators are required to set up special tone tables to match the local public network tones and cadences.

- Communication Manager endpoint user experience

Avaya Aura® SIP phones use the COUNTRY field in the Settings file to provide country-specific tones.

- Device Adapter endpoint user experience

Device Adapter follows the Avaya Aura® SIP phone functionality. Device Adapter introduces a new COUNTRY Service Attribute that points to a predefined set of country-specific tones and cadences for the following tones: dial tone, busy tone, ringback, and overflow. Device Adapter does not support customizable tones and cadences.

Device Adapter does not support media tones through Avaya Aura® Media Server.

For more information, see "Tone and cadence" in "Appendix G: Generic station operations."

Transfer — blind or consult

- CS 1000 endpoint user experience

Call transfer is made using a transfer feature key (TRN) which is predefined for UNIStim and 39XX endpoints at a fixed position and digital 200X endpoints at an unfixed position. The **Transfer** key is available on the phone screen during an active call. The active call is put on hold, and the user receives a new dial tone when it is pressed. After the far-end is reached, the user can either complete the transfer (blind) or wait until the far-end answers the call (consultative) and then complete the transfer. The transfer completion is done by pressing the **Transfer** key again.

The transfer call is made on behalf of an active DN key. For example: Phone A has a primary DN 2000 on key 0, DN 2001 on key 1. When there is an active call with key 1, the user initiates a transfer to another set B. Set B rings displaying DN 2001 as the caller number, not the primary DN of set A.

Analog endpoint transfer operations

To transfer an active call on an analog endpoint, the user would follow these steps:

- Flash the switch-hook. The call is on hold.

- Dial the number where you want to transfer the call.

- Flash the switch-hook and then hang up, or simply hang-up (depending on specific optional Classes of Service) when you hear ringing or after your call is answered.

When your call is answered, you may speak privately with the new party before completing the transfer.

Different Classes of Service will change the basic behavior into more specific behavior. For example:

- The presence or absence of the Conference service can change the ability to transfer on ringing. When the endpoint has a "Conference Allowed" Class of Service, the switch-hook flash will create a conference. At that time, to complete the Conference the transferring party must hang up. Without the Conference Class of Service, the transferring party can hang up while on the consultation call.

- "Three Party Service" allows the transferring party to use a control digit to toggle between the transferee and transfer target before completing the transfer or creating a conference. This also means the transferring party can drop either of the other two parties using a second control digit, when they are not the party on hold.

  • To create a conference, press the "conference" control digit.

  • To transfer the call, you must first create the conference and then release.

Even with Classes of Service permitting transfer on ringing, you may not be allowed to transfer a ringing call involving certain types of trunks. For example, transfer on ringing to an unsupervised trunk is not allowed.

To cancel an incomplete transfer, the typical procedure us to hang up and then lift the handset and flash the switch-hook to return to the call.

• Device Adapter endpoint user experience

 - Digital and UNIStim stations

   The Transfer button is predefined for UNIStim and 39XX endpoints at a fixed position and digital 200X endpoints at an unfixed position. Communication Manager considers it as a restricted call appearance that cannot receive any incoming calls but can only be used for outgoing calls placed in the process of transferring a call. Device Adapter will treat this button as a CS 1000 Transfer key with existing localization.

   Both consultative and blind (transfer a ringing call) transfers are supported.

   The end user behavior is retained with following differences:

   • When a user presses the Transfer or Conference key during an active call, a simple dial tone is given as opposed to a special stuttered dial tone as in CS 1000.

   • A consultative call is made using the Transfer or Conference key which is a call appearance. That means the far end will always see the phone extension as CLID. This differs from the CS 1000 behavior where a consultative call is made on behalf of the DN key of original call. This should be taken into consideration when making an original call from a bridged appearance:

     1. Set A key 0 - brdg-app to Set B

     2. Set A calls Set C from key 0. Set C sees extension of Set B.

     3. Set A presses Transfer, and calls Set D. Set D sees extension of Set A, not Set B.

 - Analog stations

The analog stations also support call transfer on the Device Adapter but with fewer options. CS 1000 permitted a user with an analog station that has transfer capability to:

• Do a transfer or create a three-party conference.

• Do a transfer or create a conference of up to six parties.

When the transfer/conference capability is enabled, Device Adapter always allows six-party conferences in a station that is migrated from the CS 1000. The transfer is always available if conference is allowed.

To do a transfer, the analog station user must be on an active call.

• The user does a switch hook flash and receives a dial tone.

• The user dials the number of the transfer target.

• If the user hangs up while the transfer target is ringing, Device Adapter does a blind transfer.

• If the user hangs up after the call to the transfer target is answered, the transfer is completed as a consultative transfer.

• If the user does a switch hook flash while ringing, the transfer attempt is cancelled.

This approximates the CS 1000 analog station user experience for transfer.

For more information, see "Transfer — blind or consultative" in "Appendix H: Call processing features and services."

Key Expansion Modules

Not all expansion modules are key based, but it is common in CS 1000 terminology to use Key Expansion Module as a phrase to indicate any type of expansion module.

An expansion module is a modular unit with different numbers of keys or touch-sensitive areas on a screen that are based on the specific expansion module. A module that is designed to provide expansion capabilities to a specific station type can be attached to 16-key 2xxx digital phones, specific 39xx digital phones, and most UNIStim IP phones. Note that an expansion module is specific to at most a family and cannot be used with others. For example, to all two column digital stations.

Depending on the history, a specific station may have more than one possible choice of key expansion module. On the other hand, some modules are limited to a subset of the stations in the family having the capability of supporting the added modules. Module A may be usable by a superset, including a subset of the endpoints that support module B.

The modules provide a user with extra programmable keys. These extra keys can be assigned to any combination of lines and features. You can typically add more than one expansion modules to a single telephone. Thereby, increasing the in line/feature keys. However, in all cases there will be a finite limit on the number of permitted extra buttons.

The expansion module usually needs a separate base for the modules. They do not use the same base as the station itself.

The Key Expansion Module connects to the telephone through a ribbon cable running from the base of the telephone. It is physically connected to the telephone by the base, which attaches to the base of the station.

The expansion module requires additional power.

For more information, see "Key Expansion Modules" in "Appendix G: Generic station operations."

Virtual Office

Virtual Office allows an endpoint device to use as a guest phone (logging in as a remote user) to recover its identity and a home phone to retain the identity. A guest phone recovers its identity automatically as soon as the phone is VO logged out. This does not apply at the home phone because a user can do another VO login from a third (or fourth) phone, and that login from the user can log out the guest phone. As opposed to Multi-Device Access (MDA) and Sequential Registration, which does not allow an endpoint device to retain its identity after logging out, the Virtual Office UNIStim phone saves the original TN, which helps it to recover the original identity and register to it. You can use the Multi-Device Access (MDA) configuration fields to limit the number of concurrent registered devices to 1 for Virtual Office to maintain the CS 1000 Virtual Office user experience.

The following is an example of Virtual Office:

1. Device X is the home device and registered with the user identity A.

2. Device Y does the Virtual Office login.

3. Session Manager verifies whether this is a permissible registration and does one of the following:

    - If the configuration is to block new registrations, the registration request is rejected.

    - If the configuration is to allow new registrations, Session Manager terminates the SIP registration of device X and registers device Y.

4. If the configuration is to allow new registrations, device Y takes the user identity A, but the same user identity is still saved in Device X.

5. User presses the "Home" soft key at device X.

6. Device Y reverts to its original identity that is user identity B.

- CS 1000 endpoint user experience

  The registration handling process upon network failures for UNIStim endpoints in Virtual Office is similar to that of the CS 1000 TPS.

  The following is the initial registration recovery attempt in CS 1000 for UNIStim endpoints:

  - UNIStim endpoint: When a CS 1000 UNIStim endpoint restarts or fails over, it attempts to register with the TPS load balancer of the primary server (S1). The UNIStim endpoint may or may not register on the same TPS.

The following is the registration recovery attempt in CS 1000 when initial registration attempt fails:

- UNIStim endpoint: If the primary server TPS is unavailable, then the TPS on the geo-redundant alternate data center is attempted. The endpoint attempts the alternate server (S2). In this case, it does not register on the same CS 1000 that it was originally using. Therefore, it uses a different TPS load balancer.

In both cases, CS 1000 identifies the hardware ID of the registering endpoint or the TN entered by the user when registering a UNIStim endpoint. CS 1000 uses the hardware ID or TN to allow or block fail over and endpoint registration when a UNIStim endpoint restarts or loses connectivity to the current target. If there is a mismatch in the hardware ID between the original registration and the new one, the registration fails.

Unlike Virtual Office, CS 1000 rejects a new device attempting to register to an existing registration, but accepts a re-registration on another TPS or call server.

This CS 1000 behavior can be deemed as conditional Virtual Office. If the same device re-registers at another TPS, the registration is allowed. If a device with a different hardware ID tries to register, the registration is denied.

• Device Adapter endpoint user experience

To configure Virtual Office, set the MDA configuration fields to the following:

- Set the **Max. Simultaneous Devices** value to 1.

- Clear the **Block New Registration When Maximum Registrations Active** check box to allow new registrations. Session Manager terminates the registration of an existing device to register the new device.

This provides a similar CS 1000 user experience in case of a fail over or endpoint restart. However, if a user tries to register a second station to CS 1000, CS 1000 blocks the registration attempt. This is because the fail-over handling in CS 1000 does not find a match in the hardware IDs of both requests.

However, the Device Adapter allows the new registration request, because the device ID of any set which is VO logged in, is not available as the device ID is an attribute of UNIStim phone and not of any other SIP phone. Hence, the device ID cannot be sent to the Session Manager. If the Session Manager user profile is set to allow new registrations when the maximum number of registered devices is reached, Session Manager allows another endpoint to register by using Virtual Office and terminates the registration of the current endpoint.

Virtual Office allows sequential registration for any endpoint that can use the CS1K-IP station definition to define the endpoint. Although, the Avaya Aura® SIP endpoints will have a different user experience.

For more information, see "Virtual Office" in "Appendix H: Call processing features and services."

Voice mail / Inbox button

- CS 1000 endpoint user experience

  CS 1000 calls the configured Call Pilot number when the UNIStim user presses the fixed **Inbox** button. TPS establishes a specific soft key layout when a call made from the **Inbox** key is answered. Pressing these soft keys results in the sending of RFC2833 digit events.

  Digital endpoints have a similar experience, except that many station types do not have soft keys, relying on a programmable key for this role.

  Analog endpoints are also provided voice mail, but no visible indication is typically provided. Instead, audio information is used, and the user has to dial directly into the voice mail server to receive the voice mail.

  When a call is placed to the CS 1000 endpoint, the user may be busy or fail to reply. If the endpoint was configured with a redirection destination for these scenarios and the destination was voice mail, the call redirects to voice mail and the caller can leave a message.

  When a message is left, Call Pilot turns on the Message Waiting Indicator lamp or icon. For endpoints without a lamp or icon, CS 1000 provides an audible tone indicating that an unheard voice mail message exists, which is presented as soon as the user goes off hook. The user can carry on with whatever operation the user intends or can go to voice mail and retrieve the message.

- Device Adapter endpoint user experience

  All endpoints supported by Device Adapter have a similar voice mail / inbox experience. All UNIStim and correctly programmed digital endpoints have an indicator light that is lit when a message is waiting. A button is also provided to access waiting messages. Pressing the button places a call to the voice mail number as configured in Communication Manager or Session Manager. This button may be labeled **Voicemail**, **Inbox**, or **MWI** depending on the endpoint.

  Analog endpoints and any digital endpoint without a lamp rely on the audible indication when the user goes off-hook or seizes a line appearance. The indicator tone may differ based on the configuration, voice mail server, and so on.

  The telephony user interface of the voice mail system must be configured to correspond to the Call Pilot pattern if the experience is to remain relatively unchanged. The telephony user interface menu setup is outside the scope of this document, and can be modified on each voice mail system.

  For more information about configuring and administering the applicable voice mail system, see the appropriate documentation.

Related links

[Voice mail and Inbox button](#) on page 592

User experience differences for call center features

Call Center functions

The CS 1000 ACD endpoints and Avaya Aura® endpoints provide very similar user experience. The user experience appears where that call is presented to the endpoint, and the call center server handles directing a call to a specific agent.

All call center-compatible Device Adapter endpoints and legacy SIP devices enable the agent to use the following features:

- The agent can log in and log out as a call center agent.

- The agent can be logged in and change their status so that they can either receive calls or become unavailable for receiving calls.

- With the corresponding status, the agent can receive calls and perform the required operations, such as call transferring or conferencing. The call then can terminate from either end.

- The agent can be provided with a certain time interval between two consecutive calls. This feature is provided by the call center.

- The agent can request the number of unanswered calls in the queue. The report also includes information about how long calls that exceeded the queue "time unanswered in queue" service requirement have been in the queue.

- The agent can request help from a supervisor.

- The supervisor can monitor calls for quality and training purposes whenever the supervisor needs to do so.

- The agent can receive calls that are not call center queue calls, including calls on a secondary number. This feature must be enabled on the agent device.

Although the details might vary depending on the call center server that is used, the core functions remains the same.

> ✷ **Note:**
>
> This document does not contain images of user interface elements of Avaya Aura® SIP devices, such as 96x1 phones, that are used in an Avaya Aura® Call Center Elite environment. For more information about the user interface elements for these devices, see their respective user guides.

CS 1000 states and Avaya Aura® Call Center Elite work modes

Both Avaya Aura® Call Center Elite and CS 1000 support the same hierarchical "state" model. This model consists of the three following levels:

1. Main Login states: The agent can be either logged in or logged out. The respective states are "Logged In" and "Logged Out".

2. Work Mode states: When the agent is logged in, the agent either may or may not take calls. The respective states are "Available" and "Unavailable".

3. Call Processing states: When the agent is available to take calls, this level includes the states for handling a call.

   This level includes states such as the following:

   - Idle: The agent is idle.

   - Ringing: The agent is receiving a notification of a new call.

   - Answered: The agent answers the call.

   - Clearing: The call is released by either party.

While Main Login and Call Processing levels are the same for both Avaya Aura® Call Center Elite and CS 1000, the Work Mode level has some differences:

- When the agent is available to take calls, Avaya Aura® Call Center Elite has two variants of states, while CS 1000 has a single state.

- When the agent is unavailable to take calls, Avaya Aura® Call Center Elite has two variants of states, while CS 1000 has a single state.

The Avaya Aura® Call Center Elite Work Mode level states are called "work modes" in documentation.

In the scope of this section, the following terms are used:

- "Avaya Aura® Call Center Elite work modes" to refer to specific Avaya Aura® Call Center Elite Work Mode level states.

- "CS 1000 states" to refer to CS 1000 Work Mode level states.

Avaya Aura® Call Center Elite work modes and corresponding CS 1000 states are not the only conditions that affect agent endpoints. Agents cannot have a call center work mode unless they log in to the call center. However, Avaya Aura® Call Center Elite work modes and equivalent CS 1000 states are similar.

Main Login state	CS 1000	Avaya Aura® Call Center Elite	Notes
Logged out	Logged out	Logged out	Agents can only perform Unified Communication operations, with few exceptions, such as checking the queue status or communicating with supervisors. Agents cannot handle calls.
Logged in	Logged in	Logged in	Agents can perform call center operations depending on their current work mode.

The following table displays supported CS 1000 states and equivalent Avaya Aura® Call Center Elite work modes when the agent is logged in:

Work Mode state when logged in	CS 1000 states	Avaya Aura® Call Center Elite work modes	Notes
Unavailable for calls	Not Ready	Aux Work After Call Work	Aux Work (Auxiliary Work) is the most common equivalent to the CS 1000 Not Ready state. However, Not Ready also enables the agent to perform and record post call processing tasks related to ACD calls.
Available for calls	Ready (informal name. The state has no formal name).	Auto-In Manual-In	CS 1000 has an equivalent to Auto-In, but has no direct equivalent to Manual-In. CS 1000 documentation refers to these states as "re-entering the queue" when the agent becomes available or able to receive ACD calls.

Avaya Aura® Call Center Elite defines the following two states, or work modes, for the Not Ready state:
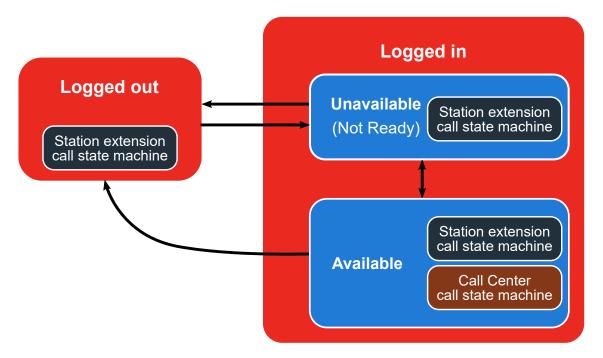
• Not Ready state for completing After Call Work.

• Not Ready state for performing any other operation, such as taking a coffee break.

CS 1000 unifies both these states into a single Not Ready state.

While the agent is logged in, the mode remains constant, but the agent state changes based on whether the agent receives the call, answer the call, modifies the call and so on. For example, if the agent in the Auto-in mode receives and processes a call, this Auto-in mode remains during all phases of the call. The mode does not change when the agent state changes.

CS 1000 availability transitions

The following diagram shows CS 1000 availability transitions:
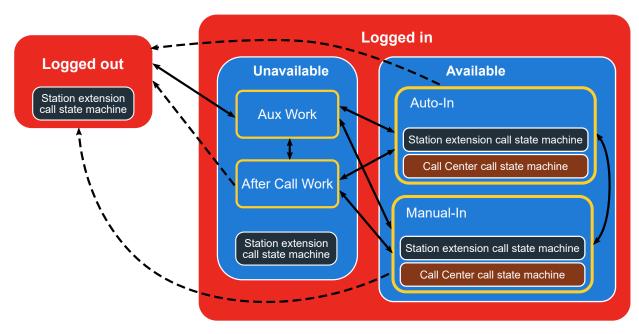
CS 1000 enables the agent to perform the following transitions:

- Logging in and remaining in the Unavailable, or Not Ready, state.
- Logging out from both Unavailable and Available states.
- Switching between Unavailable and Available states.

The call state machines exist within all availability states. However, the call center call state machines are only available when the state is Available.

Avaya Aura® Call Center Elite availability transitions

The following diagram shows Avaya Aura® Call Center Elite availability transitions:

Connector	Description
◄ ▬ ▬ ▬ ▬	One-way transitions.
◄▬▬▬►	Two-way transitions.

Avaya Aura® Call Center Elite enables the agent to perform the following transitions between work modes and states:

- Switching between work modes in the Unavailable state.

- Switching between work modes in the Available state.

- Logging in and remaining in the Unavailable state. In this case, the agent work mode is Aux Work.

- Logging out from any work mode in both Unavailable and Available states.

- Switching between any work mode in the Unavailable state and any work mode in the Available state.

Similarly to CS 1000, call state machines exist within all availability states. However, the call center call state machines are only available when the agent work mode belongs to the Available state.

✱ **Note:**

Avaya Aura® Call Center Elite can change the device state. For example, after the agent logged in, Avaya Aura® Call Center Elite can change the agent work mode to Auto-In.

Text strings and key labels on the Avaya Device Adapter Snap-in endpoints

The text strings and the key labels for the programmable feature keys are localized in the languages supported by the Avaya Device Adapter Snap-in.

The key labels and prompts with default values can be customized. For example, an administrator can rename the **Aux Work** feature key to **Not Ready**.

Logging in and logging out

CS 1000 endpoint user experience

On CS 1000 phones, an agent can log in and log out in the following ways:

• By pressing the **ACD In-calls** key.

• By pressing the **Make Set Busy** key.

An agent can also use the **ACD In-calls** key to receive calls from the call center service.

To log in, the agent must press the **ACD In-calls** key, which corresponds to digit **0**, and enter the agent credentials. To separate the entered data, the agent must press **#**. To indicate the end of entry, the agent must press **##**.

The agent must enter the login data in the following order:

1. The agent ID

2. **#**

3. ACD queue directory number

4. **#**

5. Priority level

6. **#**

CS 1000 supports the Priority Agents feature which enables more experienced and qualified agents to receive high-priority calls. An agent can enter up to five ACD queue directory numbers and set a priority level for each number. For example, if the agent 5001234 sets 5 ACD queue directory numbers with priorities, the entry is the following: `5001234 # 5657421 # 1 # 2823356 # 4 # 7658798 # 1 # 5652272 # 1 # 2829228 # 1 ##`, where

• `5001234 #`: agent ID

• `5657421 # 1 #`: first queue, high priority

• `2823356 # 4 #`: second queue, low priority

• `7658798 # 1 #`: third queue, high priority

- `5652272 # 1 #`: fourth queue, high priority

- `2829228 # 1 ##`: fifth queue, high priority

After logging in successfully, the phone is logged in but in the Not Ready state. The agent can log out by pressing the **Make Set Busy** key. The **Make Set Busy** has different functionality depending on the type of system the agent uses for services.

System	User experience with the Make Set Busy key
CS 1000 in Unified Communications	Agents can use the **Make Set Busy** key to set their state to Busy for all callers. When this feature is activated, the phone does not receive calls.
ACD	An agent can use the **Make Set Busy** key to make the agent appear busy for the ACD queue and non-ACD calls. After pressing this key, the agent logs out. If the agent presses the **Make Set Busy** key again, the phone is available for non-ACD calls but the agent is still logged out.

Avaya Aura® Call Center Elite legacy SIP device user experience

With Avaya Aura®, an agent can log in and log out of the extension using the Features menu on the phone.

An agent must enter the agent ID and passcode in the corresponding fields. The passcode is optional but the agent ID is required.

After logging in successfully, the phone is logged in but in the Aux Work state.

The following table shows the information that the phone displays:

Location on the phone	Displayed information
Top line display	Agent ID
Agent information line	• Shows if the phone displays the Message Waiting Indicator (MWI) of the phone or of the agent. • Skills groups that the agent is logged into. Skills groups can be associated with a certain VDN or ACD directory number. • Skills groups that the agent is not logged into.
The Features List menu	The **Log in** key label changes to **Log out**.

To log out, an agent must go to the Feature List menu and press the **Agent logout** feature key. If the administrator programmed the phone to request a logout reason, such as end of shift or lunch break, the agent must enter a reason code to log out.

The phone logs out from the queue. This does not impact new calls that are not routed to the call center or VDN calls. An agent can still answer calls that were routed to the phone extension.

Avaya Device Adapter Snap-in user experience

The Device Adapter uses a combination of the two approaches along with the functionality unique for the Device Adapter.

Origin of functionality	Description of functionality
CS 1000	• The agent login data consists of the agent ID and delimiters. • The agent login data is displayed on the dialed digits line. • The pound symbol (#) in the login data indicates the end of data entry and triggers registration with the Call Center Elite.
Call Center Elite	• Agent uses **Log in / Log out** key for logging in and logging out. • When a passcode is required, the agent enters it when logging in. • The login data does not include a list of agent skill groups. • After the agent logs in, the endpoint displays the agent ID, the Message Waiting Indicator (MWI) setting specifying whether the phone displays the mailbox status of the phone or of the agent, and the skill groups to which the agent is assigned.

Table continues…

Origin of functionality	Description of functionality

Device Adapter	• The asterisk symbol (*) is used in the login data to separate the agent ID from the passcode in the digit string. If password is required, the agent enters the password after the asterisk and completes the string by entering the pound symbol (#), which indicates the end of data entry.
	
	• Although the formatting of the data that the agent enters is similar to the data formatting of CS 1000, the agent does not enter different ACD queue directory numbers to select queues to service. Instead, the phone for agents who need such a capability is programmed to have a designated feature key to change and manage skills. The agents use the key to add or delete skills when required. For more information on the functionality of this key, see Avaya Device Adapter Snap-in user experience on page 770.
	
	• On the agent info display, the first line, which is used to display the name of a caller in Unified Communications, displays the agent ID. The second line displays the Message Waiting Indicator (MWI), and the third line displays the skills.
	
	• In case of reboot of the phone or restart of the Device Adapter module, for example, due to outage, Call Center Elite is tries to restore the agent status after restart. If Call Center Elite detects outage after it presented a call to the agent, or Return to Queue On No Answer (RONA) is invoked for a call, Call Center Elite transitions the phone into Auxiliary Work mode which corresponds to unavailable for calls state. If Call Center Elite does not detect outage, two scenarios are possible after restart, depending on the environment:
	
	  - In Avaya Aura® environment with single Session Manager, the agent remains in logged-in state, and the phone shows the work mode administered on the System Manager or Communication Manager.
	
	  - In Avaya Aura® environment with both primary and secondary Session Managers, the agent's work mode is set based on the following:
	
	    • When re-registration uses the same Session Manager that was used for the agent before the restart, then after restart the agent remains in logged-in state, and the phone shows the work mode administered on System Manager or Communication Manager.
	
	    • When re-registration uses a different Session Manager than the one used before the restart, then after restart the agent remains in logged-in state but the work mode automatically changes to Auxiliary Work regardless of what value is configured on System Manager or Communication Manager for the work mode on login.

Logging in with agent ID
Procedure

1. To log in, press the programmable **Log in** feature key.

2. When prompted, enter the agent ID.

3. **(Optional)** If required, enter the password.

   By analogy with the Avaya Aura® SIP devices, the key label changes to **Log out** when you successfully log in.

Login credentials format

Type of credentials	Format of credentials
No passcode required	The agent ID in `NNNNN#` format. The `#` indicates the end of data and triggers registration of the agent with the Call Center Elite. The digits entered as `NNNNN` are visible to the agent.
Passcode required	The agent ID and passcode in `NNNNN*nnnnn#` format. The `*` separates the agent ID and the passcode. The `#` indicates the end of data and triggers registration of the agent with Call Center Elite. No double `#` is required, as the `*` provides a non-terminating delimiter and makes the `#` the indicator of the end of data. The digits entered as `NNNNN` are visible to the agent. The digits entered as `nnnnn` are displayed as a string of asterisk symbols (`*****`) for privacy reasons.

Logging out with agent ID
Procedure

1. To log out, press the **Agent-login** feature key labelled as **Logout**.

2. **(Optional)** If the Call Center Elite requires a reason code, enter the reason code.

   If the code is valid, the Call Center Elite logs you out.

   The label changes to **Login** when you successfully log out.

Agent's availability for calls

CS 1000 endpoint user experience

On CS 1000, the agent can become available by using the **Not Ready** toggle key or the **ACD In-Calls** key if the agent is logged in and in the Not Ready state.

When the agent is in the Not Ready state, the lamp or the icon associated with the **Not Ready** key lights or shows the Not Ready active status for the endpoint. The agent can be in this state either immediately after logging in or as a result of specific agent's actions.

If the agent presses the **Not Ready** key in the Not Ready state, the lamp or the icon of the **Not Ready** key goes out. The station becomes ready to receive calls, and the agent becomes available.

Avaya Aura® Call Center Elite legacy SIP device user experience

Avaya Aura® Call Center Elite uses the following modes for the agent's availability:

- Aux Work (Auxiliary Work)
- After Call Work

The station can be in the Aux Work mode either immediately after the agent logs in or as a result of specific agent's actions, for example if the agent presses the **Aux Work** key. The After Call Work mode is mainly a result of specific agent's actions. When the agent is in one of these work modes, the phone displays the icon of a corresponding mode.

After logging in, the agent must select a call answering mode using the Feature list menu. Available answering call modes are the following:

- Automatic-In
- Manual-In

After the agent selected the call answering mode, the phone displays the selected mode, and the icon for Aux Work or After Call Work disappears. The station becomes ready to receive calls, and the agent becomes available.

Avaya Device Adapter Snap-in user experience

Except for selecting the applicable availability mode, the Call Center Elite user experience is similar to the user experience with CS 1000. However, the Device Adapter uses the Avaya Aura® Call Center Elite model because the Call Center Elite model supports two modes, and Device Adapter uses the Call Center Elite server.

In most cases, the Device Adapter endpoint has only one work mode, either Automatic-In or Manual-In. However, because two modes are available, it is not practical to use the key as a toggle by analogy with CS 1000. Therefore, to leave the unavailable for calls state, the agent must press the Automatic-In or Manual-In feature key.

When the agent presses the work mode key, the icon for that key lights, and the icon for the unavailable work mode key goes dark. If the phone does not already display the agent ID on the status bar, the agent ID is provided as part of the Idle set display. The agent can receive calls according to the selected mode.

Agent's unavailability for calls

CS 1000 endpoint user experience

The following table describes the methods an agent can use on CS 1000 endpoints to become unavailable for calls:

Method	Description
Logging out	The agent becomes unavailable for calls when the agent logs out.

Table continues…

Method	Description
Pressing the **Not Ready** key	The agent can press the **Not Ready** key to complete the work related to the previous call or for other purposes, such as having a lunch break. If configured, the CS 1000 phone can prompt for an activity code when an agent goes into the inactive state or leaves. If activity codes are required, the Activity Code lamp or icon flashes. The agent presses the **Not Ready** key, enters the code, and presses the key again to confirm the operation. The agent can start the transition into the unavailable for calls state by pressing the **Not Ready** key while on a call. The agent goes into the unavailable state when the call ends. While the agent remains in the unavailable for calls state, the Not Ready lamp or icon is lit.
Automatic transition	The CS 1000 endpoint can automatically answer calls received through the Automatic Call Distribution (ACD) process also known as the Call Forcing. As a part of this capability, the CS 1000 allows the call center to provide a timed pause between releasing a call and taking new calls. When ending a call, the agent can use up to two timers to delay receiving a call. • The first delay timer provides a time interval between the moment the agent ends the call and the moment the agent becomes available. • The second delay timer ensures that during a forced answer procedure a caller receives a programmable number of ringback cadences before the caller is connected to the agent. In this case, no action is required on the agent's side, and no lamp or icon is lit. The agent simply ends the current call and has a short interval before a new call appearance.

Avaya Aura® Call Center Elite legacy SIP device user experience

In the Call Center Elite environment, depending on the settings, the agent can be prompted to enter a reason code for taking a temporary break or completing the work for the current call.

An agent can use one of the following modes to become unavailable for calls:

Unavailability mode	Description	Agent's action

Aux Work	The mode that an agent uses when taking a temporary break.	The agent can go into Aux Work mode in one of the following ways:
		
		• The agent logs in.
		
		  To receive calls, an agent must log in and select a call answering mode: Automatic-In or Manual-In. When the agent logs in, the phone displays the icon for Aux Work next to the original Available work mode. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode.
		
		• The agent presses the Aux Work key after the call ends or when the call is still in progress.
		
		  If the agent presses the key while on a call, and the reason code is required, the agent must enter the reason code to move into Aux Work mode. The phone displays the icon for pending Aux Work mode. When the call ends, the agent switches to Aux Work mode. The phone displays the icon for Aux Work next to the original Available icon. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode again.
		
		  If the agent presses the Aux Work key while not on a call, and the reason code is required, the agent must enter the reason code to move into Aux Work mode. The phone displays the icon for Aux Work next to the original Available icon. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode again.
		
		• The Call Center Elite server puts the agent into Aux Work mode. The phone displays the icon for Aux Work next to the original Available icon. No calls are placed to the agent device until the agent switches to the Automatic-In or Manual-In mode again.

Table continues…

Comments on this document? infodev@avaya.com

Unavailability mode	Description	Agent's action
After Call Work	The mode that an agent uses to complete work for an existing call.	The agent can go into After Call Work mode in one of the following ways: • The agent presses the **After Call Work** key after the call ends or when the call is still in progress. If the agent presses the key while on a call, the phone displays the icon for pending After Call Work mode. When the call ends, the agent switches to After Call Work mode. The phone displays the icon for After Call Work next to the original Available icon. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode again. If the Call Work Code is required, the agent must press the **Call Work Code** key to return to the available state. If the agent presses the **After Call Work** key while not on a call, the phone displays the icon for After Call Work next to the original Available icon. No calls are placed to the agent until the agent switches to Automatic-In or Manual-In mode again. If the Call Work code is required, the agent must press the **Call Work Code** key to return to the available state. • The agent goes into After Call Work mode automatically when in Manual-In mode. When the call ends, the agent switches to After Call Work mode. The phone displays the icon for After Call Work next to the original Available icon. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode again. • The agent goes into After Call Work mode automatically when in Automatic-In mode with the **Timed After Call Work** option activated. When the call ends, the agent switches to After Call Work mode. The phone displays the icon for After Call Work next to the original Available icon. The server runs a timer for the After Call Work. On the timer expiry, the server returns the work mode to Automatic-In. No calls are routed to the agent until the station switches to Automatic-In mode again.

Avaya Device Adapter Snap-in user experience

Most of the user experience with Device Adapter is based on the Call Center Elite model. However, the user experience is more similar to the CS 1000 user experience because the functionality of Aux Work mode is similar to the functionality of the **Not Ready** key in CS 1000.

The user can assign custom labels to the station keys. The **Aux Work** key provides the closest match to the CS 1000 **Not Ready** key, including reason codes (referred to as Activity Codes in CS 1000) for the transitions. If the user assigns the custom label Not Ready to the **Aux Work** key, the user experience of becoming unavailable for calls will be very similar to the user experience with CS 1000. The only differences are that the key is not a toggle in Call Center Elite, and that the reason codes do not require pressing the **Account Activity Code** key to enter the data. The Aux Work transitions with the most basic programming do not require reason codes.

With Device Adapter, an agent can use the **Aux Work** key to go into Aux Work mode or After Call Work mode.

Unavailability mode	Agent's action
Aux Work	The agent can go into Aux Work mode in one of the following ways: • The agent logs in. The phone displays the icon for the **Aux Work** key next to the key. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode. • The agent presses the **Aux Work** key when the call is still in progress or after the call ends. • The Call Center Elite server puts the agent into Aux Work mode. The icon for Aux Work displays `Active` (equivalent of `Answered` on the CS 1000 endpoints) next to the key. No calls are placed to the agent device until the agent switches to Automatic-In or Manual-In mode again.
After Call Work mode	With basic ACD programming on the Call Center Elite, the After Call Work transitions do not require call work codes. The agent can go into After Call Work mode in one of the following ways: • The agent presses the **After Call Work** key when the call is still in progress or after the call ends. • The agent goes into After Call Work mode automatically when in Manual-In mode. When the call ends, the agent switches to After Call Work mode. The icon for the **After Call Work** key displays `Active` (equivalent of `Answered` on the CS 1000 endpoints) next to the key. No calls are routed to the agent device until the agent switches to Automatic-In or Manual-In mode again. • The agent goes into After Call Work mode automatically when in Automatic-In mode with **Timed After Call Work** option activated. When the call ends, the call moves into After Call Work mode. The icon for the After Call Work key displays `Active` (equivalent of `Answered` on the CS 1000 endpoints) next to the key. The server runs a timer for After Call Work mode. On the timer expiry, the server returns the work mode to Automatic-In. No calls are placed to the agent device until the station switches to Automatic-In mode again.

Pressing the Aux Work key while on a call

Procedure

1. While on a call, press the **Aux Work** key.

2. **(Optional)** If required, enter the reason code.

   The icon for pending Aux Work flashes to indicate the pending state.

   You switch to Aux Work mode when the call ends. The icon for the Aux Work key displays `Active` (the icon used for `Answered` on the CS 1000 endpoints) next to the key. No calls are routed to your device until you switch to Automatic-In or Manual-In mode.

Pressing Aux Work key while not on a call

Procedure

1. After the call ends, press the **Aux Work** key.

2. **(Optional)** If required, enter the reason code.

   The icon for the **Aux Work** key displays `Active` (equivalent of `Answered` on the CS 1000 endpoints) next to the key. No calls are routed to your device until you switch to Automatic-In or Manual-In mode.

Pressing the After Call Work key while on a call

Procedure

While on a call, press the **After Call Work** key.

The icon for the **After Call Work** key flashes to indicate the pending state.

When the call ends, you switch to After Call Work mode. The icon for the After Call Work key displays `Active` (equivalent of `Answered` on the CS 1000 endpoints) next to the key. No calls are routed to your device until you switch to Automatic-In or Manual-In mode again.

Next steps

If the call work code is required, you must press the **Call Work Codes** key to return to the available state.

Pressing the After Call Work key while not on a call

Procedure

After the call ends, press the **After Call Work** key.

The icon for the **After Call Work** key displays `Active` (equivalent of `Answered` on the CS 1000 endpoints) next to the key.

No calls are routed to your device until you switch to Automatic-In or Manual-In mode again.

Next steps

If the call work code is required, you must press the **Call Work Codes** key to return to the available state.

Forced agent transition to the logged out state

CS 1000 user experience

Application Module Link (AML) messages from the server initiate the forced logout of the agent station.

When an agent misses an ACD call, the CS 1000 station can log this agent out. Otherwise, the agent moves into the Not Ready state.

A supervisor cannot log agents out.

Avaya Aura® Call Center Elite legacy SIP device user experience

The following are two types of the agent station logout:

- Logout by time
- Logout by a supervisor

To log out the agent station, the supervisor needs an H.323 configuration with the following available options:

- A skill group logout
- Location logout

Logout by time puts a group of agents at the end of the working day into the Logged Out state.

When an agent is on a call, the station remains logged in.

Avaya Device Adapter Snap-in user experience

The Avaya Aura® SIP endpoints do not support the forced supervisor logout by a supervisor.

The forced logout by time and by a supervisor takes place in the following way:

- If an agent is not on an ACD or DAC call, the agent station logs out.
- If an agent is on an ACD or DAC call, with the logout by time, the station provides a sound notification and displays the corresponding icon. The agent is logged out when they end the call.

After logging out, an agent can log in back again.

Overriding forced logout by time

CS 1000 user experience

On CS 1000 phones, overriding forced logout by time is not available. The agent must log in again.

Avaya Aura® Call Center Elite legacy SIP device user experience

If the agent is logged out, they can log in again.

If there is a pending logout before the call ends, and the agent station has a logout override key. The agent can press this key to override a forced logout. However, the agent cannot override a forced logout of a skill group or of a location.

If a forced logout by time and a forced logout by supervisor take place at the same time, either logout takes precedence depending on the configuration.

However, when there is a pending logout, a legacy SIP device shows a pending logout and not the type of a logout. Therefore, if the forced logout by supervisor took precedence, the agent can ignore the override.

Avaya Device Adapter Snap-in user experience

The Device Adapter endpoint uses a similar forced logout to that on Aura with the following differences:

- The icon in front of the **Logout** key flashes. There is no icon bar to display the icons.
- Only the tones generated by the Avaya Aura® Call Center Elite are available.

If the agent receives a pending logout notification during an ACD or DAC call, they can override that logout for a 24-hour period. On the following day, the logout by time will repeat.

If the agent does not or cannot override the logout, and the Avaya Aura® Call Center Elite does not limit the maximum number of registered agents, the agent can log in back again.

Forced agent transition to Aux Work

CS 1000 user experience

The forced agent transition to the Aux Work state is similar to the forced transition into the Not Ready state.

If an agent does not answer an ACD call, the CS 1000 puts the agent into the Not Ready state. In this case, no reason code is required. The Not Ready state is a default programming option.

If a monitoring device is in Not Ready, the phone is also put into Not Ready.

The CS 1000 and associated call center servers can also initiate the Not Ready state for server-related reasons. The CS 1000 endpoint receives a notification and is moved to Not Ready mode with the corresponding reaction.

Avaya Aura® Call Center Elite legacy SIP device user experience

The feature is similar to the forced transition into the Not Ready state on the CS 1000 phones.

If an agent is on an ACD call, the Return On No Answer feature puts the agent into the Aux Work state. In this case, no reason code is required.

If the monitoring device is in the Aux Work state, the phone is also in Not Ready.

The Avaya Aura® Call Center Elite can also initiate the Aux Work state for other reasons. The SIP device receives the Aux Work notification from the server and move to the Aux Work state.

Avaya Device Adapter Snap-in user experience

Except for the key label, the forced agent transition with the CS 1000 is similar to that with the Avaya Aura® Call Center Elite. If feature key customization is enabled and the **Aux Work** feature key is configured, the endpoint displays the transition into Aux Work or Not ready.

You can change the Aux Work state in the following ways:

- By logging out of the extension.
- By selecting the applicable work mode for the endpoint.

Interruptible Aux Work

CS 1000 user experience

The CS 1000 environment does not have an equivalent for the Interruptible Auxiliary (Aux) Work feature.

Call Center Elite legacy SIP device user experience

The Interruptible Aux Work feature allows to make agents who are in Auxiliary Work mode available for receiving incoming calls when the number of available agents is insufficient.

Agents must enter interruptible reason codes when going into Aux Work mode to indicate that they can become available using the Interruptible Aux Work feature.

The following table describes the functionalities available with the Interruptible Aux Work feature:

Functionality	Description
Notification of an agent.	Communication Manager sends a message to the agent who is in Aux Work mode notifying that the agent needs to become available. An agent can receive a notification in the following cases: • The system requests the agent to become available to start handling calls. The agent needs to enter the available state manually. Therefore, a notification of this kind allows to avoid putting an agent into an available state when the agent is not at the agent's desk. • The system notifies the agent of forced transition into the available state. A notification of this kind is not applicable to agents who have the auto-answer feature enabled on their phone. This allows to prevent a call from being automatically answered when the agent is not present at the phone.

Table continues…

Functionality	Description
Forced transition of an agent into the available state.	The administrator can configure the agent's phone to make the agent available for calls automatically by moving the phone from Aux Work mode to Auto-In or Manual-In work modes.
	With this functionality, the agent first receives a notification with a timer, which can be set to a period as short as 1 second. When the timer expires, the agent automatically moves to the available for calls state.
	Because the transition does not require any agent's actions, the phone can become available when the agent is not present at the phone. Therefore, this functionality is not used with the Auto-Answer feature. Without the Auto-Answer feature enabled, if the agent is not present, the unanswered call returns to the queue, and the agent moves to Aux Work mode.
	The administrator can use the forced transition programming to move agents with Manual-In work mode configured who are in After Call Work mode back to Manual-In mode.

Avaya Device Adapter Snap-in user experience

The Device Adapter endpoint uses the Call Center Elite handling.

If the agent ID is not included into the list of agents whose Reserve Level permits the Call Center Elite to notify them that they are needed, the system handles all reason codes for Aux Work mode as non-interruptible.

If the agent ID is included into such a list and the agent switches to Aux Work mode using an interruptible reason code, Call Center Elite leaves the agent in Aux Work mode until the queue threshold is exceeded. When the queue threshold is exceeded:

• The phone displays a notification that the agent needs to become available for calls.

• The phone provides an audible tone.

• The work mode indicator flashes to indicate the request for the agent to service calls.

Further handling depends on the Reserve list setting and is described in the following table:

Reserve list setting	Handling description
Notify only	An agent receives a notification. The phone displays the notification until the queue threshold drops below the interrupt value. ✱ **Note:** Agents who have the Auto-Answer feature enabled on their phone, use the same handling as the agents with the **Notify only** setting. Such agents cannot be moved to Auto-In or Manual-In mode because they might not be present at the phone.

Table continues…

Reserve list setting	Handling description
Auto-In interrupt	An agent who does not have the Auto-Answer feature enabled on the phone, receives a notification which remains for the duration of the Interruptible Aux Notification timer. When the timer expires, Call Center Elite moves the phone into Auto-In mode.
Manual-In interrupt	An agent who is in Aux Work mode with an interruptible reason code or in After Call Work mode receives a notification which remains for the duration of the Interruptible Aux Notification timer. When the timer expires, Call Center Elite moves the phone into Manual-In mode.

Configuration of Interruptible Aux Work mode

Interruptible Aux Work mode does not require any configuration on the phone. The configuration, including the option to make After Call Work mode interruptible, is performed within the Avaya Aura® Call Center Elite programming. However, if the phone has the Auto-Answer feature enabled, it treats the **Auto-In interrupt** and **Manual-In interrupt** settings as the **Notify only** setting.

Related links

[Configuring interruptible auxiliary notification timer](#) on page 219
[Configuring interruptible auxiliary threshold and interruptible auxiliary deactivation threshold](#) on page 217
[Configuring Agent Reserve Level](#) on page 219

Receiving calls

CS 1000 user experience

On 1140e and i2050 phone models, the **ACD In-Calls** key, which corresponds to digit **0**, flashes to indicate an incoming call.

The following table describes the user experience when there is an incoming call and the associated agent's actions:

Agent action	User experience details
The agent gets an incoming call alert.	• The **ACD In-Calls** key displays the Ringing icon. • The phone displays the caller information. • If configured, the phone displays the Dialed Number Identification Service (DNIS) information. The DNIS information contains the digits the caller dialed and the queue number for this call. If a specific DNIS queue is programmed, the phone displays it instead of the caller name.

Table continues…

Agent action	User experience details
The agent answers the call.	• If the call is forced, after the timeout, the phone displays this call as an answered call. • If the call is not forced, the agent must press the line key or on-hook the handset. • The **ACD In-Calls** key displays the Answered icon. • If the SRTP media encryption is used during a call, the phone displays the Encrypted Media icon.
The agent ends the call.	• The caller can always end the call, except in Public Safety Answering Position (PSAP) call centers. • If configured, an agent can end the call. • After the call is ended, the **ACD In-Calls** key displays the Idle icon.

Avaya Aura® Call Center Elite legacy SIP device user experience

The phone displays an incoming call on an idle call appearance line.

The following table describes the user experience when there is an incoming call and the associated agent's actions:

Agent action	User experience details
The agent gets an incoming call alert.	• A line key icon shows a call center call in a queue, a direct call to an agent, or a station call. • The phone displays the **Answer** or **Ignore** soft key. • If configured, the phone displays the information on the selected VDN function. • The phone displays the caller information. • If configured, the phone displays the digits the caller dialed. • If the agent presses the **Ignore** soft key, the incoming call alert is muted.
The agent answers the call.	• If auto-answer is enabled, after the timeout, the phone plays an audio alert and displays the call as answered. • If auto-answer is disabled, the agent must press the **Answer** soft key and lift the handset to answer the call. • The call appearance key LED indicates the call has been answered and the call appearance line shows the Answered icon.
The agent ends the call.	• The caller can always end the call. • If configured, an agent can end the call. • After the call is ended, the call appearance line displays the Idle icon.

Avaya Device Adapter Snap-in user experience

On 1140e and i2050 phones, an incoming call displays on an idle call appearance.

The following table describes the user experience when there is an incoming call and the associated agent's actions:

Agent action	User experience details

The agent gets an incoming call alert.	The phone displays the following:
	
	• The Ringing icon.
	
	• The caller information.
	
	• A prefix, which specifies the call type. The options are the following:
	
	  - `ACD`: For a call to a center call.
	
	  - `DAC`: For a direct call to the agent.
	
	  - No prefix: For a call to the station extension.
	
	• A name for the Vector Directory Number (VDN), if configured.
	
	• The digits that the caller dialed, if this feature is configured on the phone.
	
	In the Avaya Device Adapter Snap-in environment, the phone does not display the **Answer** or **Ignore** soft keys.

The agent answers the call.	• If auto-answer is enabled, after the timeout, the phone plays an audio alert and displays the call as answered. • If auto-answer is disabled, the agent must press the programmable feature key and lift the handset to answer the call. • The call appearance line displays the Answered icon. • If the SRTP media encryption is used during a call, the phone displays the Encrypted Media icon.
The agent ends the call.	• The caller can always end the call. • If configured, an agent can end the call. • After the call is ended, the call appearance line displays the Idle icon.

Receiving a MADN secondary number call

CS 1000 user experience

The MADN secondary numbers include both numbers that are using Multiple Call Arrangement (MCA) or Single Call Arrangement (SCA). With Multiple Call Arrangement, every agent has one key and can accept a call. With Single Call Arrangement, one call appearance is displayed for several agents. Agents can use SCA extension specifically for call center specific functions. For example, instead of overflowing to another ACD queue, calls exceeding the maximum waiting time can be directed to a MADN extension and to the agents that have the MADN key configured.

The phone displays the call to a MADN extension as the call to multiple appearance Directory Numbers (DNs). However, the agent is aware of the purpose of the MADN extension and can process the call accordingly.

Avaya Aura® Call Center Elite SIP device user experience

MADN is a CS 1000 feature and there is no Avaya Aura® Call Center Elite equivalent for this functionality. However, an overflowing call can be sent to a bridging extension rather than to another skill group.

The phone displays a MADN call as the call to a call or bridged appearance. However, the agent is aware of the purpose of the MADN extension and can process the call accordingly.

Avaya Device Adapter Snap-in user experience

The CS 1000 and Avaya Aura® Call Center Elite SIP device functionality is very similar. The major difference is that an agent can receive calls to all line appearances on the X-Port with one MADN key, but they can answer only one call. If another agent answers the current call, the key becomes idle, and the phone can display a new call. On a legacy SIP device, the bridged appearance key is used for a single line appearance. If an agent answers the call, the line appearance is engaged with that call, and the phone cannot display the second call for this key.

The Avaya Device Adapter Snap-in functionality is similar to that with CS 1000, if the MADN key was configured on the Avaya Aura®.

Making outgoing calls

CS 1000 user experience

Agents can only make outgoing calls to transfer a call or to create a conference using the **ACD In-Calls** key, which corresponds to digit **0**. For more information, see

In all other cases, agents makes outgoing calls using a secondary Directory Number (DN) key. The secondary DN key is any key on the phone other than digit 0. This key cannot be an ACD key, which functionality is restricted to digit 0. However, this can be a Single Call Arrangement key configured only on this phone and corresponding to the extension for this phone. CS 1000 refers to this extension as the Individual Directory Number, or IDN.

Agents can use the secondary DN key as a multiple appearance DN shared among multiple phones. You can configure the secondary DN key in one of the following ways:

- Single Call Arrangement: Only one agent can make a call and other callers can bridge in if the call is not private.
- Multiple Call Arrangement: Every agent with this key can use it for incoming and outgoing calls.

With the standard configuration on CS 1000, the identity is used for the call of the secondary DN. For example, if you configure digit **4** as Multiple Call Arrangement (MCR), the DN and the matching name of the digit is used for all calls from digit **4**.

The following is the call flow when an agent presses the Single Call Arrangement (SCA) key:

Action	User experience details
The agent presses the idle SCA key.	• The icon lights. • The agent hears the dial tone. • Other agents with this key see indications of an outgoing call.
The agent dials the number.	• The agent hears call the waiting tone. • Depending on the CS 1000 configuration, the called party can see the caller's name and extension for an incoming call. However, agents can usually see only the extension.
The called party answers.	• Call waiting tone ends, and a two-way media path is created. • Full identity information is displayed, unless identity privacy is enabled on one of the endpoints. • Other agents can bridge in, if the call is not private, or privacy was released. • The call ends when the second last participant releases.

The following is the call flow when an agent presses the Multiple Call Arrangement (MCR) key:

Action	User experience details
The agent presses the idle MCR key	• The icon lights. • The agent hears the dial tone. • No other agent is aware of the call.
The agent dials the number.	• The agent hears call the waiting tone. • Depending on the CS 1000 configuration, the called party can see the caller's name and extension for an incoming call. However, agents can usually see only the extension.
The called party answers.	• Call waiting tone ends, and a two-way media path is created. • Full identity information is displayed, unless identity privacy is enabled on one of the phones. • No other agents can bridge in. • The call ends when either participant releases.

Avaya Aura® Call Center Elite legacy SIP device user experience

Agent can use a call appearance or a bridged call appearance to make a call.

Action	User experience details
The agent presses an idle call appearance or bridged call appearance key.	• The key LED lights, and the agent hears the dial tone. • Unless this is a bridged call appearance or another user has it as a bridged call appearance, no other agent is aware of the call. • If a bridged call appearance is configured for this line appearance, any agent with the same line appearance is aware of the call.

Table continues…

Action	User experience details
The agent dials the number.	• The agent hears the waiting tone. • Depending on the CS 1000 configuration, the called party can see the caller's name and extension for an incoming call.

The called party answers.	• The call waiting tone ends, and a two-way media path is created. Full identity information is displayed, unless identity privacy is enabled on one of the endpoints.
	
	• Unless this is a bridged call appearance or another user has it as a bridged call appearance, no other agent is aware of the call.
	
	• If a bridged call appearance is configured for this line appearance, any agent with the same line appearance is aware of the call.
	
	  - If Call Exclusion is enabled, the other agent or agents cannot bridge in.
	
	  - If Call Exclusion is not enabled, the other agent or agents can bridge in.

Avaya Device Adapter Snap-in user experience

If you configure the secondary extension keys as MADN keys, or SCA keys as bridged appearances of a call appearance key, the flow is the same as on CS 1000 phones.

Checking status of calls in the queue

CS 1000 endpoint user experience

On CS 1000 endpoints, the **Display Queue** key is available to supervisors and not to agents.

The key referred to as **Display Queue** in the User Guides is the **Display Waiting (ACD) Calls**, or

DWC. This key provides the following information to the screen when pressed:

- The number of calls in the queue
- The number of logged in agents
- The time the oldest call in the queue has waited for an agent
- The number of calls that have done an overflow by waiting time into the queue

In addition, the lamp or icon state indicates the queue status as follows:

- Off: few or no calls waiting
- On: an acceptable number of calls waiting
- Slow flash: calls are backing up; the queue is getting close to overflowing
- Fast flash: any new call is overflowing to another queue

Avaya Aura® Call Center Elite legacy SIP device user experience

The equivalent functionality in the Call Center Elite is the Queue Status which a user can check using the **q-calls** key on the SIP endpoints. Both supervisors and agents can use it.

The SIP endpoints have two lamps for each key. This allows them to show the status of the Oldest Queue Time and Number of Queued Calls separately.

Oldest Queue Time:

- Off: no calls in the queue

- On: the oldest call has been waiting for an acceptable amount of time

- Flash: threshold for the time to answer has been reached

Number of Queued Calls:

- Off: no more than one call waiting

- On: an acceptable number of calls waiting

- Flash: the threshold for the number of calls queued has been reached

The Queue Stats (q-calls) feature key is assigned on a per-skill group basis and is available to a logged-out agent. The label is displayed as Queue Stats followed by the skill group number tracked in brackets, for example `Queue Stats (4)`. The feature key provides the following information:

- The configured name of the skill group associated with the Queue Stats feature key

- The time the oldest call in the queue has waited

- Number of calls in queue

Avaya Device Adapter Snap-in user experience

The stations supported by the Device Adapter have only one indicator icon. The Queue Stats capability of the **q-calls** key provides additional information not displayed on the screen but displayed by the two lamps.

The Device Adapter provides a modified version of the Call Center Elite user experience. The request sent when pressing the **q-calls** key causes a response from the Call Center Elite. This includes the following:

- The name of the Vector Directory of the skill group

- The age of the oldest call in the skill group queue

- The number of calls in the skill group queue

- An indication of whether the number of calls threshold has been exceeded

- An indication of whether the oldest call threshold has been exceeded

The Device Adapter endpoints use this information to provide lamp states and a text display:

- If no calls are present, the icon is dark

- If calls are present but no threshold has been exceeded, the icon is lit

- If calls are present and at least one threshold has been exceeded, the icon flashes

  - If the time in queue threshold is exceeded, the icon does a slow flash

  - If the number of calls threshold is exceeded, the icon does a fast flash

  - If both the time in queue and the number of calls thresholds are exceeded, the icon does a slow flash followed by a fast flash

- The initial press of the **q-calls** key displays the information available to the Avaya Aura® SIP device user including the following:

  - The name of the skill group

  - The number of calls in the queue

  - The time in seconds the oldest call has waited in the queue

- Multiple presses of the **q-calls** key switch screens, including re-displaying the current status. The second screen of queue display includes the following:

  - The skill group number

  - The values of the threshold flags (with a label for the flags)

- If the agent is on a call, and SRTP (encrypted media) is used, a lock icon and potentially the word `Encrypted` is displayed. If there are over 12 additional characters to be displayed, the word `Encrypted` is omitted, as the lock icon indicates encryption is in progress.

Entering Call Work Code

CS 1000 user experience

On CS 1000 phones, the equivalent to Call Work Codes (CWC) is Activity Code (AC) used together with the **Not Ready** key and recording call related activities. However, these codes do not apply to a supervisor monitoring an agent, making and answering a call from an agent, and making an emergency call. These actions automatically put a supervisor into the Not Ready state.

Phones without displays cannot process activity codes. The codes also cannot be used when the phone is logged out.

Agents can use the **Activity Code** key to enter the appropriate activity code for their current work. For example, an agent can record an account number of the caller, a social security number, or a customer defined value.

Post processors use the **Activity Code** key to handle billing or record the agent time that he spent on a task.

The agent can enter Call Work Codes (CWC) in the following cases:

- During a call
- In the Not Ready state

The following flow describes how the agent can use a CWC during a call:

1. The agent presses the **Activity Code** key. The icon or key LED lights.

2. The agent enters the Call Work Code. To delete a character, the agent must press * or #.

3. The agent presses the **Activity Code** key again. The information is sent to the server and the icon is off.

The agent can enter a CWC during a call several times if the activity changes.

The following flow describes how the agent enters a CWC in the Not Ready state:

1. The agent presses the **Not Ready** key. The Not Ready icon lights and the Activity Code key icon flashes.
2. The agent presses the **Activity Code** key. The icon or key LED lights.
3. The agent enters Call Work Code. To delete a character, the agent must press ∗ or #.
4. The agent presses the **Activity Code** key again. The information is sent to the server and the icon is off.

The agent can enter a CWC in the Not Ready state several times if the activity changes.

A default activity code is provided and used whenever an agent does not enter the code.

Avaya Aura® Call Center Elite legacy SIP device user experience

An agent can use Call Work Codes (CWC) to record call related activities. If configured, the agent can use a CWC to move into the After Call Work state. However, these codes do not apply to a supervisor's transitions related to supervisor functions.

An agent cannot use the codes in the Logged Out state or in Aux Work mode.

The agent uses the **Call Work Code** feature key to enter an appropriate activity code for their current work. For example, the account number of the caller, a social security number, or a customer defined value.

Post processors use the **Call Work Code** key to handle billing or record the agent time that he spent on a task.

The agent can enter Call Work Codes (CWC) in the following ways:

- During a call
- In the After Call Work state

The following flow describes how the agent can use CWC during a call:

1. The agent presses the **Call Work Code** feature key on the Feature List menu. The icon or key LED lights.
2. The agent enters a CWC.
3. The agent presses the **Enter**, **OK**, or **#** key. The phone sends the activity record to the server.

The agent can enter a CWC during a call several times if the activity changes.

The following flow describes how the agent can use CWC in the After Call Work state:

1. The agent presses the **After Call Work** feature key on the Feature List menu. The icon or key LED lights.
2. The agent presses the **Call Work Code** key.
3. The agent enters a CWC.
4. The agent presses the **Enter**, **OK**, or **#** key. The phone sends the activity record to the server.

The agent can enter a CWC in the After Call Work state several times if the activity changes.

Avaya Device Adapter Snap-in user experience

The procedures of entering work codes on Avaya Device Adapter Snap-in are similar to those on Avaya Aura® Call Center Elite endpoints. However, on an Avaya Device Adapter Snap-in phone, an agent must press the configured soft keys to enter work codes instead of using the Features List menu.

Entering Call Work Codes feature

About this task

You can enter Call Work Codes during an ACD or DAC call to record call related activities. You can enter a CWC several times if the activity changes.

Procedure

1. On the phone, go to the Feature List menu

2. Press the **Call Work Code** feature key.

   The icon or key LED lights.

3. Enter the required Call Work Code.

4. Press one of the following:

   • **Enter**

   • **OK**

   • **#**

   The phone sends the activity record to the server.

Entering a Call Work Code in the After Call Work mode

About this task

You can enter a Call Work Code to record call related activities in the After Call Work mode. You can enter a CWC in the After Call Work mode several times if you need to record more than one activity.

Procedure

1. On the phone, go to the Feature List menu.

2. Press the **After Call Work** feature key.

   The icon or key LED lights.

3. Press the **Call Work Code** key.

4. Enter the required Call Work Code.

5. Press one of the following:

   • **Enter**

   • **OK**

• **#**

The phone sends the activity record to the server.

Request supervisor assistance

CS 1000 user experience

On CS 1000 phones, you can request assistance by pressing one of the following keys:

- the **Supervisor** key
- the **Emergency** key

Using the Supervisor key

The **Supervisor** key allows an agent to perform the following:

- Make a call to a supervisor
- Make a conference call with a supervisor using Automatic Call Distribution calls (ACD)
- Transfer an ACD call to a supervisor

Each time an agent presses the **Supervisor** key, any active call is put on hold and the agent makes a call to the supervisor.

The following is the call flow when an agent presses the **Supervisor** key during a call:

1. The agent presses the idle **Supervisor** key.
2. The current call is placed on hold.
3. The supervisor gets an alert.
4. If the supervisor answers a call before getting an alert, the agent and supervisor have a consultative call.

The following is the call flow when an agent presses the **Supervisor** key when not on a call:

1. The agent presses the **Supervisor** key.
2. The supervisor gets an alert.
3. The supervisor answers the call.

An agent can resume the previous call in the following ways:

- If an agent was on an ACD call and wants to resume it after talking to the supervisor, they must press the **In-Calls** key.
- If an agent was on a call and wants to resume it after talking to the supervisor, they must press the Directory Number (DN) line key.

With this feature, an agent can add a supervisor to a conference call in the following way:

1. On a consultation call, the agent presses the **Supervisor** key.
2. A conference call with two-way media is established.

An agent can transfer a call to a supervisor after setting up a conference call with them, or transfer by conference, in the following way:

1. On a consultation call, the agent presses the **Supervisor** key.

2. A conference call with two-way media is established.

3. The agent presses the **End Call** key to leave the conference.

4. The call between the caller and supervisor continues.

Avaya Aura® Call Center Elite legacy SIP device user experience

With Avaya Aura® Call Center Elite, you cannot use the **Supervisor Assist** key for requesting assistance. Alternatively, on an H.323 phone, you can use the Malicious Call Trace Controller key for contacting a supervisor.

Using the Supervisor Assist key

The **Supervisor** assist key allows an agent to perform the following:

• Make a call to a supervisor

• Make a conference call with a supervisor using Automatic Call Distribution calls (ACD)

• Transfer an ACD call to a supervisor

To make a conference call or transfer an ACD call to a supervisor, the agent must have the second call appearance key available on the phone.

An agent can have several **Supervisor Assist** keys. The keys can be labelled with the corresponding supervisor skills or left blank.

A supervisor that an agent contacts is determined in the following ways:

1. If the agent is on a call and the skill group is not specified, by the skill group of this call. In this case, if the agent has several skill groups, they can contact a supervisor of the skill group related to the call.

2. If the agent is idle, by the first listed skill group for this agent.

Each time an agent presses the **Supervisor** key, any active call is put on hold and the agent makes a call to the supervisor.

The following is the call flow when an agent presses the **Supervisor** key during a call:

1. The agent presses the **Supervisor** key.

2. The current call is placed on hold.

3. The supervisor gets an alert.

4. If the supervisor answers a call before getting an alert, the agent and supervisor have a consultative call.

The following is the call flow when an agent presses the **Supervisor** key when not on a call:

1. The agent presses the **Supervisor** key.

2. The supervisor gets an alert.

3. The supervisor answers the call.

An agent can resume the previous call in either of the following ways:

- If an agent was on an VDN call and wants to resume it after talking to the supervisor, they must press the line key for the VDN call.

- If an agent was on a call and wants to resume it after talking to the supervisor, they must press the line key for the previous call.

An agent can add a supervisor to a conference call with the caller in the following ways:

1. During a consultative call, the agent resumes the previous call.

2. The call between the agent and supervisor is placed on hold.

3. The agent presses the conference soft key, both calls are placed on hold.

4. The agent presses the call appearance of the supervisor, the multi-party conference call is performed.

An agent can transfer by conference in the following way:

1. During a consultative call, the agent resumes the previous call.

2. The call between the agent and supervisor is placed on hold.

3. The agent presses the **Conference** soft key, both calls are placed on hold.

4. The agent presses the supervisor call appearance key, the conference call starts.

5. The agent presses the **Release** key to leave the conference. The call between the caller and supervisor continues.

An agent can transfer by conference using the **Transfer** soft key in the following way:

1. During a consultative call, the agent resumes the previous call.

2. The call between the agent and supervisor is placed on hold.

3. The agent presses the **Conference** soft key, both calls are placed on hold.

4. The agent presses the supervisor call appearance key, the conference call is initiated.

5. The agent presses the **Transfer** soft key to complete the transfer. The call between the caller and supervisor continues.

Avaya Device Adapter Snap-in user experience

The user experience when requesting assistance on the CS 1000 phones is similar to and that with the Avaya Aura®.

However, the Device Adapter user experience is closer to the Avaya Aura® user experience because the Device Adapter uses the Avaya Aura® Call Center Elite server.

Using the Supervisor Assist key

With CS 1000 and Avaya Aura® Call Center Elite, an agent can use the **Supervisor Assist** key to perform the following:

- Make a call to a supervisor

- Make a conference call with a supervisor using Automatic Call Distribution (ACD)

- Transfer an ACD call to a supervisor

An agent can have several **Supervisor Assist** keys. The keys can be labelled with the corresponding supervisor skills or left blank.

To make a conference call or transfer an ACD call to a supervisor, the agent must have the second call appearance key available on the phone.

The agent can transfer a call to a supervisor by making a conference call with them in one of the following ways:

- By pressing the **Conference** soft key
- By pressing the **Transfer** soft key

Making a call to a supervisor during a call

About this task

You can make a call to a supervisor during your call to request assistance.

Procedure

During a call, press the **Supervisor Assist** key.

The current call is put on hold.

The supervisor gets an alert. If the supervisor answers a call before getting an alert, you have a consultation call with the supervisor.

Making a call to a supervisor in an idle state

About this task

You can make a call to a supervisor to request assistance between your calls.

Procedure

1. In an idle state, press the **Supervisor Assist** key.

   The supervisor gets an alert and answers the call.

2. **(Optional)** You can resume the previous call in one of the following ways:

   - For a VDN call, press the VDN line key.
   - For other calls, press the corresponding line key.

Adding a supervisor to a conference call

About this task

You can add a supervisor to a conference call to consult them on a caller's question.

Procedure

1. During a consultation call, make a call to your supervisor.

   The first call is put on hold.

2. Resume the previous call.

   The call with the supervisor is put on hold.

3. Press the **Conference** soft key.

   The previous call and the call with the supervisor are put on hold.

4. Press the supervisor call appearance key.

   The conference call with the caller and supervisor starts.

Transferring a call by conference to a supervisor with the Conference key

About this task

You can transfer a call to a supervisor by making a conference call with them using the **Conference** key.

Procedure

1. During a consultation call, make a call to your supervisor.

   The first call is put on hold.

2. During a consultation call with a supervisor, resume the previous call.

   The call with the supervisor is put on hold.

3. Press the **Conference** soft key.

   The previous call and the call with the supervisor are put on hold.

4. Press the supervisor call appearance key.

   The conference call starts.

5. **(Optional)** To leave the conference, press the **Release** key.

   The call between the caller and supervisor continues.

Transferring a call by conference to a supervisor using the Transfer key

About this task

You can transfer a call to a supervisor by making a conference call with them using with the **Transfer** key.

Procedure

1. During a consultation call, make a call to your supervisor.

   The first call is put on hold.

2. Resume the previous call.

   The call with the supervisor is put on hold.

3. Press the **Transfer** soft key.

   You leave the conference call. The call between the caller and supervisor continues.

MCT as Emergency

CS 1000 user experience

The functionality available with the **Emergency** key is similar to the Malicious Call Trace (MCT) feature and transfer by conference. The difference between the functionality available with the CS 1000 **Emergency** and MCT key is that CS 1000 not only records the call and logs the call information, but also notifies an agent's supervisor. On CS 1000, an agent normally notifies their supervisor using the **Supervisor** key. The difference between the functionality available with the CS 1000 **Emergency** and **Supervisor** key is that **Emergency** not only notifies an agent's supervisor, but also records the call and logs the call information. This information allows to find the specific call in any recordings.

In case of threatening or abusive calls, the agent can see the trunk access code and trunk member number or the caller information on the phone display, unless the caller has presentation restriction enabled. When the agent presses the **Emergency** key, CS 1000 initiates a no-hold conference with the agent's supervisor. The supervisor receives a notification about the emergency call and information about the calling agent and answers the call using the **Answer Emergency** key. To record the emergency call, a customer can configure a tape recorder or maintenance TTY, or both.

If the supervisor accepts the emergency call, then both the agent and the supervisor must stay on the call until the call ends and the recording stops.

When the agent presses the **Emergency** key, the associated LED or icon indicates the supervisor or recording trunk status as follows:

Emergency key status	Description
Dark	Both the supervisor and the recording trunk are unavailable. For example, the supervisor can be unassigned to the agent, can be busy on another emergency call, or might not have the **Answer Emergency** key on their telephone. The recording trunks can all be busy or unassigned.
Flashing	The supervisor is available but has not answered the emergency call.
Constantly lit	Either the supervisor or the recording trunk, or both, are joined the call.

The following is the call flow when an agent presses the **Emergency** key during a call:

1. During a call, the agent presses the **Emergency** key.
2. CS 1000 generates a report log.
3. If the queue is configured to record emergency calls, CS 1000 starts recording the call.
4. If the call is from an Integrated Services Digital Network (ISDN) trunk and the system is configured to send the MCT signals over that trunk, the system alerts the PSTN that the call is malicious.
5. A no-hold conference call is initiated.

6. The supervisor receives the emergency call on the supervisor's **Answer Emergency** key. The supervisor also receives audio and visual alerts about the incoming emergency call. The supervisor's phone displays the agent's position ID.

7. After the supervisor receives the call, the **Emergency** key LED or icon on the agent's phone flashes.

8. The supervisor presses the **Answer Emergency** key to answer the call.

9. After the supervisor answers the call, the **Emergency** key LED or icon on the agent's phone lights.

10. The supervisor listens to the call through the speaker.

    The phone headset remains on the cradle. ACD stations in CS 1000 enable the party to log out by removing a headset from the cradle. In this case, the headset must not be plugged in to answer the call.

11. The supervisor can put the call on hold to make other calls, such as placing a 911 call. To retrieve the emergency call that is put on hold, the supervisor must press the **Answer Emergency** key.

Communication Manager user experience

MCT as Emergency on Communication Manager

On Avaya Aura®, the Malicious Call Trace (MCT) feature has three following distinct phases:

1. Activation
2. Control
3. Deactivation

An agent can handle only one MCT at a time. An agent *cannot* make another MCT until the MCT controller deactivates current MCT.

The Avaya Aura® user experience of using the MCT feature differs from the CS 1000 user experience. Some of the differences are the following:

- Number of controllers or supervisors. Avaya Aura® enables the administrator to configure several controllers for an agent, whereas CS 1000 only supports a single supervisor.

- Whether a controller joins the call. Avaya Aura® does not joins the controller into the call. Usually, the call is recorded, so bringing in the controller consumes network resources but adds minimal value.

When an agent presses the **Emergency** key, the associated lamp indicates the action performed by a controller as follows:

Lamp status	Description
Dark	All available controllers are notified, but no controller accepted the emergency call notification yet.
Constantly lit	A controller accepted the call. If a recording device is programmed and available, it is also joined the call.

For more information about the MCT feature on Avaya Aura®, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

Malicious Call Trace activation

A user or an agent can use the following options to activate a MCT:

- **mct-act** feature key
- Feature Access Code (FAC) for MCT

MCT can be activated by either the call recipient or another user or attendant, for example in case of a conferencing call.

Call flow of an Emergency (MCT) call

The following is a call flow for MCT activation. The MCT activation call flow is similar to the MCT activation call flow on CS 1000.

- The agent identifies the call as an emergency call.
- The agent presses the **mct-act** key that is labelled as **Emergency**.

  The associated lamp is currently dark.

Malicious Call Trace control

On Avaya Aura®, the MCT control phase has significant differences from the control phase on CS 1000:

- CS 1000 relies on contacting a single supervisor that is configured in the station programming. If the supervisor is unavailable, no supervisor can be assigned to a malicious call.
- Avaya Aura® enables you to assign several controllers to an agent to handle malicious calls. This feature improves chances that a suitable monitoring party answers a malicious call. After one of controllers answers the call, it becomes the MCT controller, and Avaya Aura® stops notifying other potential controllers.

A potential MCT controller is a station or an attendant that has the **mct-contr** key.

1. When an agent presses the **mct-act** key, the system initiates call recording if programmed to record calls.
2. When the agent presses the **mct-act** key, the system notifies potential MCT controllers associated with this agent.

   To notify potential MCT controllers, the system does the following:

   - Generates an alert tone on the controller's phone.
   - Flashes the lamp associated with the **mct-contr** key.

3. A user that presses the **mct-contr** key first becomes the MCT controller of the call.

   The system stops alerting other potential MCT controllers.

4. After the controller presses the **mct-contr** key, the system displays the following emergency call details on the controller's phone:

   - The called number.
   - The activating number. This is the agent ID, the station extension, or the bridged appearance number that is used when the MCT feature is activated.

- The call status.

- Information about other participant of the call.

Depending on the call origin, the system can display the following information about the call participants:

- The calling number if the call originates inside the system or on the same node within a Distributed Communications System (DCS) network.

- The calling number if the call originates outside the system and an Integrated Services Digital Network (ISDN) or SIP calling number identification is available on the incoming trunk.

- The location of the incoming trunk for all other calls. In this case, the user must call the connecting server to get more information about the malicious call.

5. If configured, the system sends an MCT notification to the PSTN.

   This feature relies on having a signaling mechanism on the trunk. You can also configure ISDN and specific DS1 trunks to provide MCT notifications. For more information, see "Screens for administering Malicious Call Trace" in *Avaya Aura® Communication Manager Feature Description and Implementation*.

   The system notifies the PSTN when the original PSTN trunk is reached over the SIP network or is a PSTN SIP trunk. Communication Manager always sends an MCT notification over SIP to the trunk gateway or Session Border Controller and notify the PSTN if the capability exists and is programmed.

6. The system generates MCT reports.

   For more information, see "Reports for Malicious Call Trace" in *Avaya Aura® Communication Manager Feature Description and Implementation*.

Malicious Call Trace deactivation

The MCT deactivation call flow on Avaya Aura® is similar to the call flow on CS 1000. The difference is that CS 1000 does not use Flexible Feature Codes (CS 1000 FAC).

1. The MCT controller dials the FAC configured for MCT deactivation.

   Deactivation frees any blocked resources that were used for MCT.

2. When all parties left the call, the system disconnects the MCT call recorder.

   When using a SIP endpoint, an agent does not need to remain on the call for the monitoring and recording to continue.

If the MCT controller does not deactivate MCT the call recorder keeps recording the call.

An agent cannot make a second MCT or, if using Device Adapter, an emergency call until the controller releases the resources that are used for MCT.

A Communication Manager MCT controller cannot be a SIP device. Therefore, SIP devices does not have keys to activate or deactivate MCT. An MCT controller must use a H.323 endpoint. The activation and deactivation functionality can be configured on that endpoint using the H.323 attendant console.

Avaya Device Adapter Snap-in user experience

The functionality available with the Malicious Call Trace (MCT) feature is similar to the **Emergency** key and transfer by conference.

During an emergency call, the monitoring device can display an emergency notification. The system sends a malicious call trace request to the public network.

After the emergency call is established, a supervisor can deactivate the MCT feature.

Adding a supervisor to an emergency call

About this task

You can add a supervisor to an emergency call to request their assistance. If required, the supervisor can record the conference call.

Procedure

During a call, press the **Emergency** key.

The supervisor gets an alert. The MCT controller icon flashes.

Emergency call use cases

Sunny Day scenario: Agent activates emergency call handling

The emergency activation requires an MCT controller, which can be an H.323 or DCP station on Communication Manager.

1. An agent identifies a call as malicious.

2. During a call, the agent presses the **Emergency** key.

   • The Device Adapter sends a message that the agent pressed the **Emergency** key to Communication Manager.

   • The MCT lamp remains dark because no MCT controller has pressed the MCT controller key.

3. Communication Manager performs programmed operations.

   • The system generates a report log.

   • The system starts recording the call, if programmed.

   • If the call is from a PSTN trunk that can be notified of malicious calls and the system can send MCT signals over that trunk, then the system signals to the PSTN that the call is malicious.

   • Communication Manager notifies all available MCT controllers.

4. MCT controllers receive the emergency call notification on the MCT controllers **mct-contr** key.

   • The agent does *not* receive a notification that controllers are alerted.

   • H.323 and DCP MCT controllers receive audio and visual alerts about the incoming emergency call. These alerts comply with H.323 and DCP MCT controller notifications.

   • The MCT controller displays the Communication Manager specific data on controllers' stations.

5. One MCT controller answers the call using the MCT controller key.

   • The MCT lamp on the agent's phone lights.

   • Other MCT controllers' stations stop receiving notifications about the emergency call.

   • The MCT controller can monitor the call in the manner applicable to an H.323 station MCT controller. However, this feature requires adding a capability to create conferences or expand existing conferences. This capability is not part of a normal MCT controller feature set.

6. When the call ends, the controller deactivates MCT.

Rainy Day scenario: No recording trunk available

The emergency activation requires an MCT controller, which can be an H.323 or DCP station on Communication Manager.

The following is a call flow for a scenario where a malicious call cannot be recorded.

1. An agent identifies a call as malicious.

2. During a call, the agent presses the **Emergency** key.

   • The Device Adapter sends a message that the agent pressed the **Emergency** key to Communication Manager.

   • The MCT lamp remains dark because no MCT controller has pressed the MCT controller key.

3. Communication Manager performs programmed operations.

   • The system generates a report log.

   • The system attempts to start recording the call, but this attempt fails. For example, all recording resources might be in use.

   • If the call is from a PSTN trunk that can be notified of malicious calls and the system can send MCT signals over that trunk, then the system signals to the PSTN that the call is malicious.

   • If the call is from a PSTN trunk that can be notified of malicious calls and the system can send MCT signals over that trunk, then the system signals to the PSTN that the call is malicious.

   • Communication Manager notifies all available MCT controllers.

4. MCT controllers receive the emergency call notification on the MCT controllers **mct-contr** key.

   • The agent does *not* receive a notification that controllers are alerted.

   • H.323 and DCP MCT controllers receive audio and visual alerts about the incoming emergency call. These alerts comply with H.323 and DCP MCT controller notifications.

   • The MCT controller displays the Communication Manager specific data on controllers' stations.

5. One MCT controller answers the call using the MCT controller key.

   • The MCT lamp on the agent's phone lights.

   • Other MCT controllers' stations stop receiving notifications about the emergency call.

- If the system is programmed to notify the controller that the call is being recorded, the controller can detect the recording failure.

- The MCT controller can monitor the call in the manner applicable to an H.323 station MCT controller. However, this feature requires adding a capability to create conferences or expand existing conferences. This capability is not part of a normal MCT controller feature set.

6. When the call ends, the controller deactivates MCT.

Rainy Day scenario: No controller available

The emergency activation requires an MCT controller, which can be an H.323 or DCP station on Communication Manager.

The following is a call flow for a scenario where no controllers are available to handle the call.

1. An agent identifies a call as malicious.

2. During a call, the agent presses the **Emergency** key.

   - The Device Adapter sends a message that the agent pressed the **Emergency** key to Communication Manager.

   - The MCT lamp remains dark because no MCT controller has pressed the MCT controller key.

3. Communication Manager performs programmed operations.

   - The system generates a report log.

   - The system starts recording the call, if programmed.

   - If the call is from a PSTN trunk that can be notified of malicious calls and the system can send MCT signals over that trunk, then the system signals to the PSTN that the call is malicious.

   - Communication Manager notifies all available MCT controllers.

4. MCT controllers receive the emergency call notification on the MCT controllers **mct-contr** key.

   - No controllers are available. For example, the controllers might be offline or might already control MCT calls.

     The MCT lamp on the agent's station remains dark.

   - Because no controllers are available, the system does not provide audio or visual alerts to the controllers.

5. No controller answer the emergency call.

   The MCT lamp on the agent's station remains dark.

6. When the call ends, no controller can deactivate MCT.

Advanced call operations

Advanced call operations include putting a call on hold, resuming a call, transferring a call, making a conference call, using the Automatic Hold feature when selecting another line. Each feature provides at least one method to resume the initial call.

CS 1000 user experience

CS 1000 agents can perform the following:

- Put a call on hold or resume a call, including an ACD call.
- Transfer a call, including transfer to a supervisor or to another ACD queue.
- Make a conference call with one or more parties, including a supervisor.
- Forward calls to an individual directory number, or IDN, or any multiple appearance directory number for which this phone is primary. Individual Directory Number is an extension assigned to the phone but not on the prime DN key.

CS 1000 agents cannot do the following:

- Forward ACD calls using the Call Forward Unconditional feature.
- Forward calls or use the Hunt feature for calls when the called party is busy or does not answer.

Advanced call operations on CS 1000 phones are basically identical to non-call center equivalent functionalities.

Avaya Aura® Call Center Elite legacy SIP device user experience

Avaya Aura® Call Center Elite legacy SIP phone agents can do the following:

- Put a call on hold or resume a call, including an ACD or DAC call.
- Transfer a call, including transfer to a supervisor or to another VDN.
- Make a conference call with one or more parties, including a supervisor.
- Forward a call or provide coverage for calls to the phone extension

Avaya Aura® Call Center Elite legacy SIP phone agents cannot do the following:

- Forward or provide coverage for ACD or DAC calls unconditionally.
- Forward or provide coverage for ACD or DAC calls when the called party is busy or does not answer.

Advanced call operations on Avaya Aura® Call Center Elite legacy SIP phones are basically identical to non-call center equivalent functionalities. However, transferring a call for a legacy SIP device differs from the CS 1000 feature.

Avaya Device Adapter Snap-in user experience

Holding and resuming a call

The behavior of Avaya Device Adapter Snap-in phones for advanced call operations is the same both for call center calls and non-call center calls.

The basic functionality for holding and resuming a call is the same as the on non-call center phones, but the use of Supervisor Assist and other services place the phone on hold automatically. To resume an automatically held call, an agent must end all call center operations, such as releasing a call to the supervisor, and press the held call appearance key.

Call Transfer

The behavior of Avaya Device Adapter Snap-in phones for the Call Transfer functionality is the same both for call center calls and non-call center calls.

Avaya Device Adapter Snap-in uses the same behavior for call center services as an Avaya Aura® Call Center Elite legacy SIP device for call center calls.

Avaya Device Adapter Snap-in uses a normal transfer operation for a simple transfer.

Conference calls

The behavior of Avaya Device Adapter Snap-in phones for conference calls is the same both for call center calls and non-call center calls.

Avaya Device Adapter Snap-in uses the same behavior for call center services as an Avaya Aura® Call Center Elite legacy SIP device for call center calls.

Avaya Device Adapter Snap-in uses a normal operation for a simple conference.

Transferring a call

About this task

As an agent, you can transfer a call to a supervisor if the caller needs additional consultation.

Procedure

1. When on an ACD call, press the **Assist** key.

   The call is put on hold and the call with a supervisor starts.

2. To transfer the first call to the supervisor, switch back to the ACD call.

   The call with the supervisor is put on hold.

3. Press the call appearance key for the held call with the supervisor.

   Avaya Device Adapter Snap-in transfers the first call to the supervisor.

Making a conference call

About this task

As an agent, you can add a supervisor to your current call to make a conference call.

Procedure

1. When on an ACD call, press the **Assist** key.

The call is put on hold and the call with a supervisor starts.

2. To transfer the first call to the supervisor, switch back to the ACD call.

   The call with the supervisor is put on hold.

3. Press the **Conf** key.

   The ACD call is put on hold. A new call is created on the **Conf** key, and you can hear the dial tone.

Supervisor calling an agent

CS 1000 user experience

Supervisors can call agents using the position ID of the agent phone as the destination number. Supervisors do not use the agent identity to call the agent.

The supervisor can enter the position ID using the **Agent** key or by dialing the position ID manually. The following table describes both methods:

Method	Description
Using the **Agent** key	The system administrator can program the **Agent** key on the supervisor station to specify an agent position ID. When the supervisor presses the programmed **Agent** key, the station automatically dials the extension of respective agent. The number of agents the supervisor can call using this method is limited to the number of keys available for this function. For example, if a 1140 phone is equipped with an 18-key expansion module, a user can assign up to 18 agents to the **Agent** key. The LED or icon for an **Agent** key indicate the status of the agent. The meaning of the LED or icon mode depends on the type of features implemented on the supervisor station. If the supervisor station operates with the basic features, the LED or icon for an **Agent** key have the following indication: • Dark: the agent is logged out. • Flashing slowly: the agent is waiting for a call. • Lit: the agent is on an Automatic Call Distribution (ACD) call or in the Not Ready state. • Flashing fast: the agent is on a non-ACD call. If the supervisor station operates with the advanced features, the LED or icon for an **Agent** key support Separate Post-Call Processing option and have the following indication: • Dark: the agent is logged out. • Flashing slowly: the agent is waiting for a call. • Lit: the agent is on an ACD call. • Flashing fast: the agent is on a non-ACD call, or the agent is in the Not Ready state. The functionality of the **Agent** key is limited to calling or monitoring agents.

Table continues…

Method	Description
Dialing the position ID manually	Dialing the position ID manually is the only way the supervisor can call an agent for whom **Agent** key is not programmed.
	Also, the supervisor must manually dial the position ID when calling an agent using the **Call Agent** key.
	The supervisor can initiate the call to an agent using the **Call Agent** key, which acts as a line appearance and places the agent station in the Not Ready state. When the supervisor presses the **Call Agent** key, the icon or LED for the key lights. Then the supervisor manually enters the agent position ID or presses the pre-programmed **Agent** key. The respective agent receives the call.
	The supervisor can route the call to another agent by pressing the **Agent** key with the pre-programmed position ID or by pressing the **Agent** key without the position ID and manually entering the position ID.
	To end the call, the supervisor presses the **Release** key, and the **Call Agents** LED or icon goes dark.
	The supervisor can call several agents sequentially without pressing the **Call Agent** key for every call. This functionality requires an **Agent** key without an assigned agent identity. The supervisor presses the **Agent** key without an assigned agent identity and then manually dials the position ID. When the supervisor presses the **Agent** key, the station ends the prior call and initiates a new call.

Avaya Aura® Call Center Elite legacy SIP device user experience

The Call Center Elite user experience of a supervisor calling an agent is different from the CS 1000 user experience.

In the Call Center Elite environment, the supervisor can call a specific agent by using the call appearance and dialing the agent ID. This type of connection is called a Direct Agent Call from the supervisor.

The **Busy Indicator** key does not support an agent ID as a target. The Busy indication is only available for extensions, trunk groups, hunt groups, or loudspeaker paging zones. However, the user can use the **Autodial** key and enter the agent ID as an extension for the user experience corresponding to using the **Agent** key on the CS 1000 to call an agent.

To end the call, the supervisor uses the standard call processing operations, such as going on hook or using the call drop softkey.

Avaya Device Adapter Snap-in user experience

The Device Adapter user experience of a supervisor calling an agent is based on the Call Center Elite model.

Supervisor calling an agent using Avaya Device Adapter Snap-in

Before you begin

Ensure the following:

- You have an available call appearance.

- If you need the capability of receiving calls while calling an agent, you have at least two available call appearances.

Procedure

1. Do one of the following:

   - Log out

   - Put the phone in Aux Work or After Call Work mode

2. Select an idle call appearance by pressing any idle line appearance key for the station call appearances.

3. Dial the agent ID by using one of the following:

   - The speed call list

   - The **Autodial** key

   - The dial pad

Processing of the supervisor's call to an agent

Call phase	Processing description

The supervisor dials the agent ID.	• If the agent phone has an idle appearance:
	  - The agent sees alerting indication on the phone.
	    The agent phone displays DAC if the phone supports Direct Agent Calling for such a call type.
	    The phone displays the station extension call if the phone does not support Direct Agent Calling for such a call type.
	  - The agent phone displays the extension of the supervisor as the calling party name.
	  - The supervisor phone provides the ring-back tone, and the call appearance icon flashes to indicate the ringing.
	• If the agent does not have an idle appearance or is not logged in:
	  - The call fails.
	  - The supervisor hears the busy tone and sees the corresponding icon state.

The agent answers the call.	• The supervisor sees the destination number or name. • Icon states show the answered call on all the phones involved in the call. • Media paths are available for communication. • Any dial operations allowed for a non-call center call are available. For example, the users can use the user interface digit sequences used for the voice mail system.

Table continues…

Call phase	Processing description
The agent does not answer the call, and the call goes to voice mail.	• The supervisor sees the destination on the phone and hears the notification. • Media paths are available to leave the voice mail message.
One of the parties ends the call.	All the phones involved in the call go to the Idle state.

Related links

[Configuring DAC calling on the supervisor's phone](#) on page 234

Changing the queue serviced by an agent

CS 1000 user experience

With Automatic Call Distribution (ACD) and the Multiple Queue Assignment (MQA) feature enabled, the agent can change the queues serviced by them when logging in.

The MQA feature enables agents to perform the following:

- Log in at any station using their agent ID
- Specify up to five ACD queues at login and assign a priority value to them based on the agent's skills

MQA for an agent requires displaying assigned queues. Deskphones without display capability do not support the MQA functionality.

The MQA feature ensures forwarding calls to an agent's Individual Directory Number (IDN) mailbox. The IDN is a Single Call Arrangement or Multiple Call Arrangement number assigned to an agent. However, the Message Waiting Indicator (MWI) shows only the message waiting state of the station extension, not of the agent or ACD DN (VDN).

This functionality requires configured ACD Auxiliary Data System. The ACD data block determines if the agent can do the following:

- Use the agent ID or position ID to log in
- Enter the supervisor extension to be used
- Enter the queue priorities

The agent is assigned calls from the queue with the highest priority. If there are no calls from the highest priority queue and there is a call from one of the lower priority queues, this call is routed to the agent. If two queues have an equal priority, a circular approach is used to select from one of the queues.

When the agent logs out, there is no change in the assigned queues. If the agent logs in then without changing the assigned queues, they remain the same at logout. However, if the agent moves to a new queue, all prior data is deleted. This enables the agent to change queues by logging out and logging back in. However, a supervisor can change the assigned queues without the agent logging out or in.

The agent enters the queue extensions separated by a pound sign (#). To indicate the final entry, the agent enters the pound sign twice. The following table provides examples of queue extension entry:

Queue extension entered by the agent	Description
5551212#5554455##	Agent 5551212 is assisting the queue associated with the ACD DN (VDN) 5554455.
5551212#5554455#5558888##	Agent 5551212 is assisting the queues associated with the ACD DN (VDN) 5554455 and 5558888.
5551212#5554455#5558888#5556789#5557171#5550987##	Agent 5551212 is assisting the queues associated with the ACD DN (VDN) 5554455, 5558888, 5556789, 5557171, and 5550987.

> ✳ **Note:**
>
> Adding a supervisor and priorities for agent skills can increase the entered data string significantly.

Avaya Aura® Call Center Elite legacy SIP device user experience

In earlier releases, the agents could assist multiple skill groups with the required base station configuration and using FACs. In Release 8.1.2 and later, the Call Center Elite and Avaya Aura® Communication Manager provide a feature key for this functionality.

The configured agent data contains a table of agent skills, including the skill group number, the skill level, and other parameters. The highest skill level is 1. As the table allows multiple rows, the agent can have more than one skill. This is conceptually the same as the MQA feature on the CS 1000 endpoints.

When logging in, the agent can see on the phone display the skill groups assigned to them. The SIP agent or supervisor whose station is configured with the **add-rem-sk** feature keys can change their skill group by pressing the **add-rem-sk** key and specifying one of the following options using the assigned dial keys:

- **Add**: To include the skill group number and the skill level.
- **Remove**: To specify the skill group number.

The agent station shows the skill group change as soon as the Call Center Elite accepts and approves the request.

Both the supervisor and the agent have the capability to change skills. To change the agent skills, the supervisor must enter the ID of the agent. The agent can only change the agent's own skills.

Avaya Device Adapter Snap-in user experience

Avaya Device Adapter Snap-in uses the function of adding and removing skills implemented in the Call Center Elite, but the user interface is different.

Adding and removing skills on Avaya Device Adapter Snap-in endpoints

About this task

When the station registers with Avaya Aura®, the key map loads. It includes the feature key for adding and removing skills. By default, the feature key is labeled as **add-rem-skill**.

Before you begin

Ensure that the station and the user configuration support this functionality.

Procedure

1. Log in to the endpoint.

2. Press the **add-rem-skill** key.

   The lamp lights up. The endpoint displays the following message: `Remove: 0# Add: 1#`.

3. Specify the desired action by entering one of the following using the dial pad keys:

   • Press `0#` to remove a skill. The endpoint displays `agent*skill#`.

   • Press `1#` to add a skill. The endpoint displays `agent*skill*level#`.

   > ✱ **Note:**
   >
   > Enter data in accordance with the

   If you enter only the pound sign (#) or any other digit or digit string, the endpoint displays the following message for 5 seconds: `Bad skill change input`. Then the display shows the current idle or active call state, and the lamp goes dark.

4. Enter the parameters for the desired action using the dial pad keys.

   When adding a skill, enter data in the following format: `<agent_ID>*<skill_ID>*<skill_level>#`.

   When removing a skill, enter data in the following format: `<agent_ID>*<skill_ID>#`.

   > ✱ **Note:**

   The limits for the number of digits are as follows:

   • Agent ID: maximum 15 digits

   • Skill ID: maximum 4 digits

   • Skill Level: maximum 2 digits

   • If you entered valid data, and Call Center Elite accepts it, Call Center Elite adds or removes the skill from the agent depending on the parameters the agent entered in step 3. The endpoint displays the following message for 5 seconds: `Skill changed success`. Then the display shows the current idle or active call state, and the lamp goes dark.

   • If you entered invalid data for agent, skill, priority level or for any combination of these parameters, Call Center Elite rejects the request and performs no actions. The endpoint

displays the following message for 5 seconds: `Skill change failed`. Then the display shows the current idle or active call state, and the lamp goes dark.

- If you exceed the maximum number of digits, the endpoint displays the following message for 5 seconds: `Size exceeded`. Then the display shows the current idle or active call state, and the lamp goes dark.

- If you entered data slowly, and the input timer expired, the endpoint displays the following message for 5 seconds: `Skill change aborted`. Then the display shows the current idle or active call state, and the lamp goes dark.

- If you press another feature key or receive and incoming call while entering the data, the endpoint does not send the request to the server and does not display any notification. The display changes to the screen appropriate for the event.

- If you press another feature key or receive and incoming call while waiting for a response from the server, the endpoint sends the request to the server, and the display changes to the screen appropriate for the event. The result of the change skill status request is not displayed.

Monitoring an agent

CS 1000 user experience

To analyze the quality of an agent's service, the supervisor can monitor ACD calls of any agent.

To monitor an agent, the supervisor presses the **Observe Agent** key and enters the agent ID or the key for that agent. When the supervisor presses the **Observe** key, the phone moves into the Not Ready state.

Initially, an administrator can monitor agents in Listen Only mode. After activating the Agent Observe feature, the supervisor can hear both the caller and agent. However, in Listen Only mode the supervisor cannot participate in the conversation.

An administrator can use Listen and Talk mode for monitoring an agent in the following way:

- The supervisor can select Listen and Talk mode. If the supervisor joins the conversation by pressing the **Call Agent**, or **Ring Agent**, key in Listen In mode, a conference call between the supervisor, the agent and caller is initiated.

- If the supervisor presses a key for a different agent during the conference, the supervisor leaves the call and starts monitoring a new agent in Listen In mode.

- If the supervisor presses any key other than the RAG key, agent monitoring ends. The supervisor can only press the **Release** key to end the session.

With Allow Observation of Supervisor Class of Service enabled, the supervisor can monitor another supervisor by pressing the **Observe Agent** key and dialing a position ID of the supervisor.

If Agent Observe is enabled, the supervisor does not have to activate this feature for each incoming call. If the feature is enabled, the supervisor observes each call displayed for an agent. If an agent does not answer the call, the supervisor can press the **Observe Agent** key, and the call is presented to another available agent. Otherwise, the call is put at the top of the ACD queue. If

an agent receives an Enhanced ACD Routing (EAR) call and the supervisor presses the **Observe Agent** key, the supervisor cannot monitor this call.

Observe Warning Tone

With the Observe Warning Tone feature, the monitored ACD agent might not hear an intermittent tone.

When the supervisor presses the **Observe Agent** key and the key corresponding to the required agent, the monitored agent can hear a periodic warning tone. The warning tone lasts 256 ms and repeats every 16 seconds.

The administrator can set the following **OBTN** values in the ACD settings for the ACD directory number:

- **AGT**: an agent can hear the tone.
- **ALL**: both a caller and agent can hear the tone.
- **NO**: neither a caller nor an agent can hear the tone.

This functionality is similar to VDN agents receiving a warning tone.

Without the tone, there is no indication that the supervisor monitors the agent except for the indication on the supervisor's phone. This configuration is default for all queues in the system.

If there is a pure IP for an IP call, an agent might hear a conference warning tone. This happens if the ACD agent phone is an IP Phone and the connection to an external caller is made via an H.323 or SIP trunk tandem in an 1000E/1000T or MO/BO environment. For such a call a conference unit is used, and the agent can hear a conference warning tone if it is enabled.

Avaya Aura® Call Center Elite legacy SIP device user experience

To analyze the quality of an agent's service, a supervisor can monitor the calls routed in the following way:

- To any agent
- To any extension
- To any attendant
- To any VDN

The supervisor phone must be either logged out or in Aux Work mode.

To monitor an agent, the supervisor presses the **Service Observe** feature key, enters the required option and the agent ID, station or VDN extension. If Agent Observe is enabled, the supervisor can monitor this call.

Listen Only is the default mode for monitoring an agent. When the supervisor presses the **Service Observe** key, they can hear both the agent and caller. With Listen Only mode, the supervisor cannot join the conversation.

Service Observe modifications

The following scenarios describe different modes for monitoring an agent:

- The supervisor can select the **Listen and talk** option. If the supervisor joins the conversation by pressing the **Listen Only** key in Listen In mode, a conference call between the supervisor, the agent and caller is initiated.

- The supervisor can press the **Coach** key. If the supervisor joins the conversation by pressing the **Coach** key in Listen In mode, the supervisor monitors the call between the agent and caller. Only the agent can hear the supervisor.

- If the supervisor presses the **Release** or **Service Observe** feature key, answers or initiates a call, resumes a held call, logs out, Listen In mode is off.

If Service Observe is enabled, the LED state indicates the current status of the call. The supervisor cannot monitor a held call or the call with the maximum number of participants.

The supervisor does not have to activate Service Observe for each incoming call. If the feature is enabled, the supervisor can view each call displayed for an agent.

Observe Warning Tone

With the Observe Warning Tone feature, the monitored ACD agent can hear an intermittent tone.

When the supervisor presses the **Service Observe** key and the key corresponding to the required agent, the monitored agent can hear a periodic warning tone every 16 seconds.

Without the tone, there is no indication that the supervisor monitors the agent except for the indication on the supervisor's phone. This configuration is default for all queues in the system.

Avaya Device Adapter Snap-in user experience

The Avaya Device Adapter Snap-in Service Observe feature is more similar to that of the Avaya Aura® Call Center Elite than to the CS 1000 functionality. With this feature enabled, both the environments allow the following:

- Listen Only supervisor monitoring

- Interaction of a supervisor with the caller and agent

- Setting a monitoring alert tone

- Repeated monitoring until the supervisor ends it

The Avaya Device Adapter Snap-in endpoints do not have the Features menu or the corresponding windows and soft keys for data entry. Therefore, the options are the same as those on the Avaya Aura® Call Center Elite SIP devices, but the operation differs.

As with the CS 1000 and legacy SIP devices, the supervisor presses the key for the Service Observe feature. This feature key is programmable on the Avaya Device Adapter Snap-in endpoint and has the default **Svc Obsrv** label.

When the supervisor presses the **Svc Obsrv** key, the phone prompts the user for the agent ID. The icon for the Service Observe key flashes 60 times per minute, and the phone screen shows the `Observe agent, enter ID` notification.

The CS 1000 endpoint supervisor can observe an agent or supervisor, but he cannot observe call attendants and queues. However, for consistency with the Avaya Aura® Call Center Elite endpoints, the ID that the supervisor must enter can be any valid target for Service Observe and not just an agent ID. Avaya Device Adapter Snap-in supervisors use agent IDs. They are entered as an agent ID digit string, followed by `#`. For example, for the agent 123444 the entry is `123444#`.

The following table describes different Service Observe modes and the corresponding icon states:

Mode	Icon state	Description
Avaya Aura® Call Center Elite accepts the agent ID. The icon of the Service Observe key shows the status of the agent.	The icon flashes 60 times per minute.	The agent is not on a call or the call is not answered.
	The icon is lit steadily, and the supervisor is in Listen Only mode.	• The agent is on a call. • There was no prior call displayed for the agent that was in Listen and Talk or Coaching mode.
	The icon flashes 120 times per minute, and the supervisor is in Listen and Talk mode.	There was a prior call displayed for the agent that was in Listen and Talk mode.
	The icon flashes 120 times per minute.	The supervisor is monitoring the agent and interacting with both the caller and agent.
	The icon flashes 30 times per minute, and the supervisor is in Coaching mode.	• The agent is on a call. • There was a prior call displayed for the agent that was in Coaching mode.
	The icon flashes 30 times per minute.	The supervisor is coaching the agent and listening to both the caller and agent.
Avaya Aura® Call Center Elite rejects the agent ID. The phone displays one of the following error messages:`Service Observe Failed` or `Agent is not logged in.`	The icon for the Service Observe key goes dark.	During agent monitoring the supervisor wants to end monitoring by pressing the **Release** key. Displaying the queue status also ends Service Observe.

Auto-Answer

Auto-Answer is not only a call-center functionality. Its variations exist on CS 1000 phones for Unified Communications and Contact Center. Except for some customizable programming options, such as different ways to set the call interval for an agent, the user experience is similar on different phones.

CS 1000 user experience

The Auto-Answer functionality used on CS 1000 Unified Communications phones corresponds to the Call Forcing feature for CS 1000 call centers.

Call Forcing is an alternative to standard manual call handling. With this feature enabled, the phone automatically displays a call for an agent in an answered state following a short buzzing signal. In this case, the agent does not need to press the **In-Calls** key to answer the call.

Different scenarios are possible when an agent ends the call. By default, unless the agent presses the **Not Ready** key to finish processing (similarly to the After Call Work functionality on Avaya Aura® Call Center Elite phones), the call just ends. The agent is available after a programmable Flexible Call Force timer elapses. The timer value is 2 seconds by default and has a range from 0 to 30 seconds. This timer is used for ending all call-related activities, including call recording.

Advanced functionality allows an administrator to set two timers instead of the Flexible Call Force timer. The first is Forced Answer Delay Time, similar to the Flexible Call Force timer. The difference is that the system administrator can determine if the phone displays calls immediately after this timer expires. The second timer is Forced Answer Delay for Ring Back with which a caller has a certain time to hear the ring-back tone before the phone displays the call.

Call forcing usually implies the use of a speakerphone or headset, but it can also be used when a handset is off hook. If the handset is on hook, the agent must go off hook to answer the first call. Subsequent calls can be forced until the agent goes on hook.

Avaya Aura® Call Center Elite legacy SIP device user experience

Avaya Aura® Call Center Elite has a similar model to Auto-Answer on CS 1000 phones.

An agent with Automatic Answer enabled hears a zip tone and immediately switches to incoming calls.

An agent has two available work modes to answer calls. When an agent is using Auto-In mode, they can enable Timed After Call Work (TACW) to set the interval between a call end and the next call. The agents in Manual-In mode can automatically move to After Call Work and must manually enable the available state.

Avaya Device Adapter Snap-in user experience

Avaya Device Adapter Snap-in uses the Avaya Aura® Call Center Elite programming, which is the same as the CS 1000 Flexible Call Force timer functionality.

For more information on the Auto-Answer feature configuration, see Prerequisites for Auto-Answer on page 237.

When the phone displays a call for an agent, a short tone is heard. Feature handling is different when the call ends.

Auto-In mode

An agent can receive a call immediately. The zip tone is shorter than a second, and the call is presented to the agent immediately afterwards. The agent usually has TACW administered on the phone to have a brief interval for handling the previous call.

After the TACW timer interval, the agent can be assigned to another call. With an automatic answer enabled, the phones displays the next call in less than a second after the agent is assigned to that call.

Manual-In mode

In Manual-In mode, agents move to After Call Work immediately after the call. This allows an agent to process any call-related details.

The agent then presses the **Manual-In** key again and becomes available for calls. With the automatic answer enabled, the phone displays the next call in less than a second after the agent is assigned to that call.

Alternate display options

The agent can view various types of information, including the following:

- The name of the VDN processing the call
- The original dialed number (Dialed Number Identification Service, or DNIS)

The server controls the agent display data which is visible on the endpoint.

CS 1000 user experience

The agent can see the dialed number received from the public network as the DNIS.

If DNIS is not available, agents with multiple queues do not receive an indication of the specific queue for which the call applies. The phone can display additional information entered by the caller, for example, the caller's Social Insurance Number.

If the Multiple Queue Assignment (MQA) feature is disabled, an agent services a single queue and therefore has all the information necessary to provide the services. With MQA enabled, a Computer Telephony Interface (CTI) controller is used to provide additional information to the agent.

Normally, calls to the station extension are calls to a directory number assigned to a secondary Dialed Number (DN) key which is any key other than key 0. Calls to this key receive the Unified Communications (UC) treatment.

If a call uses secure media, a padlock icon and the `Encrypted` string is displayed next to the caller identification number. If the number is longer than 11 digits, the phone skips the `Encrypted` string.

Avaya Aura® Call Center Elite legacy SIP device user experience

The Avaya Aura® Call Center Elite legacy SIP device users receive the following information when logged into the call center from the station:

- A DNIS string (alternatively, a vector DN or a label with a name assigned to the vector DN)
- Icons indicating the type of call: an Automatic Call Distribution (ACD) queue call, a call directly to the agent ID or to the extension station
- Additional information provided by the caller, for example, a Social Insurance Number

Avaya Device Adapter Snap-in user experience

The Avaya Device Adapter Snap-in phone receives a user experience based on the Avaya Aura® Call Center Elite. Prefixes ACD and DAC are used instead of icons to differentiate between the call types as described in the following table:

Call type	Description
ACD queue calls	The phone displays an ACD prefix for such calls. The first display line shows a DNIS string, a vector Dialed Number or a pre-programmed caller ID label. The second display line shows the caller phone number. The third display line shows data entered by the caller.
Direct calls to the agent	The phone displays a DAC prefix. The first display line shows the caller name. The second display line shows the caller phone number.
Calls to the station extension	These calls have no prefix. The first display line shows the caller name. The second display line shows the caller phone number.

If a call uses secure media, a padlock icon and the `Encrypted` string is displayed next to the caller identification number. If the number is longer than 11 digits, the phone skips the `Encrypted` string.

No programming occurs for the station beyond the UC capability to display the caller information. All other programming is specific to Avaya Aura® Call Center Elite.

User-to-user information

The user-to-user information (UUI) on SIP devices consists of the Adjunct Switch Application Interface (ASAI) information. This must not be confused with the Integrated Services Digital Network (ISDN) user-to-user information.

The ASAI UUI data includes one or more of the following details:

- UCID: a unique 20-digit call identifier
- The number of seconds the call waited in the queue, which consists of 4 digits
- Information provided by the caller similar to the ISDN UUI
- VDN name, which is also provided in the core SIP messaging
- Collected digits, which are also provided in the core SIP messaging

For more information on UUI feature configuration, see Enable the display of UUI information on a CC phone on page 224.

> 📌 **Note:**
>
> The administrator can program the feature system parameters to create a UCID including the UCID network node ID, or any other part of UUI details for the agent.

CS 1000 user experience

CS 1000 phones do not support the full UUI functionality. However, phones can display some UUI data for other features. An agent can view some information using the desktop application and the auxiliary processor which is used to drive the application, and not using the phone.

ASAI UUI data component	CS 1000 equivalent functionality
UCID	CS 1000 phones support a Call ID package, similar to providing a UCID. This provides a network-unique identifier for the call.
	However, other services, such as enhanced Malicious Call Trace, networked 9-1-1 centers, and enhanced name display, use the Call ID as an additional function. The phone does not display the ID to the agent, although it is logged as a part of the MCT handling and can change other UUI data.
The number of seconds the call waited in the queue	The phone uses the time during which a call was in the queue for displaying the time of the earliest ACD call. This value is also used by auxiliary processors. CS 1000 phones do not display the time a call has been in the queue. An agent can view it in the agent desktop application using the auxiliary processor module link.
Information provided by the caller	User information, such as the ISDN UUI, is received by CS 1000 making it potentially available for display.
	CS 1000 phones do not display UUI details provided from the caller but an agent can view some parts in the agent desktop application.
VDN name	The ACD queue name is not displayed for an CS 1000 agent unless the caller does not provide a name.
Collected digits	The phone displays the collected digits, but not in the UUI.

Avaya Aura® Call Center Elite legacy SIP device user experience

If the call an agent receives has UUI associated with it, the **UUI Info** feature key in the Feature menu is lit.

When an agent presses the **UUI Info** key, the phone displays the UUI details on the Agent Information line, with the UUI icon before the call information. An agent can view multiple lines of data by pressing the **Next** soft key.

When the phone screen displays the collected digits, the UUI information replaces them for a short period of time.

Avaya Device Adapter Snap-in user experience

Avaya Device Adapter Snap-in phones display the user-to-user information provided by Call Center Elite.

- The VDN name is already provided if a name was programmed for the VDN.
- The collected digits are already provided if the agent entered the digits.

An agent can view the UUI details while on active call. If an agent presses the **UUI Info** key in an idle state, the phone briefly displays `UUI Unavailable`.

When an agent presses the **UUI Info** key during a call, the phone displays the following:

- If no UUI details are available, the phone displays the `UUI Unavailable` message for 5 seconds.
- If only the VDN name and collected digits are available, the phone displays the `UUI Unavailable` message for 5 seconds.

- Otherwise, the three display lines show the UUI data.

Some components might not be present. The UUI can contain any or all of the following five components:

- UCID

- The number of seconds the call waited in the queue

- Information provided by the caller

- VDN name

- Collected digits

Avaya Device Adapter Snap-in phones display the data on three lines, each 24 characters wide, with text headers to differentiate between sections.

The phone displays the UUI details on three lines containing 22 characters. The display provides 24 characters, but whenever the media is encrypted, the screen displays a two-character Media Access Locked icon, leaving only 22 characters for the UUI.

The phone displays the information provided to the agent in one or more of the following sections:

UUI details	Header	Data format	Examples

Time in VDN before displaying the call to the agent	`InVDNTime`	1 to 4 digits indicating the time in VDN. The value is 1 through 9999 seconds.	`InVDNTime:7___`
			
			`InVDNTime:255_`

UCID	`UCID`	20 UCID digits, typically displayed on 2 lines	`UCID:1234567890123`
			`4567`
			
			`890`
			
			`InVDNTime255_`
			`UCID:12`
			
			`345678901234567890`

ASAI UUI	`ASAI`	Up to 96 ASCII characters, typically displayed on 2 or more screens.	`123456789012345678` `9012`

Table continues…

UUI details	Header	Data format	Examples

			The first screen displays:
			
			`ASAI:First=Fred;Se`
			`cond`
			
			`=Doe;Simulated=yes`
			`;Lon`
			
			`g=yes;NeedToInterp`
			`ret=`
			
			The second screen displays:
			
			`probably;DigitData`
			`=121`
			
			`7654883285525`

			The first screen displays:
			
			`InVDNTime255_`
			`UCID:12`
			
			`345678901234567890`
			
			`ASAI:First=Fred;Se`
			`cond`
			
			The second screen displays:
			
			`=Doe;Simulated=yes`
			`;Lon`
			
			`g=yes;NeedToInterp`
			`ret=`
			
			`probably;DigitData`
			`=121`
			
			The third screen displays:
			
			`7654883285525`

Viewing UUI details

About this task

You can view available UUI details during a call. If you have multiple screens displaying UUI details, you can switch between them by pressing the **UUI Info** key.

Before you begin

- The **UUI Info** key must be configured as a phone feature key or as a key on the expansion module.
- Make a call.

Procedure

1. While on an active call, press the **UUI Info** key.

   After 5 seconds the phone displays the previous screen.

2. **(Optional)** To switch between several screen, press the **UUI Info** key again before 5 seconds elapse.

Avaya Aura® Call Center Elite features not requiring user actions

Several Avaya Aura® Call Center Elite features do not require the agent interaction. They are not visible to the agent, and Avaya Aura® Call Center Elite operates them independently, using Device Adapter and phones as an ecosystem.

VDN return destination

The VDN Return Destination features place calls back in a processing queue after all call participants, except the caller, drop the call. The use of VDN Return Destination depends on the call center configuration.

This service is programmed in Avaya Aura® Call Center Elite and Communication Manager. You can use the data collected by this service in user experience surveys.

For more information about the VDN Return Destination features, see *Avaya Aura® Call Center Elite Feature Reference*.

Avaya Aura® Call Center Elite report management

Avaya Basic Call Management (Avaya BCM) or Avaya Call Management systems provide information about agent activity to Avaya Aura® Call Center Elite.

The Skill Status report shows the skills of agents that log in and the level for each skill. The administrator can change the skill allocation to modify staffing and achieve a better skill balance with the help of the **Change Skills** key.

Call recording on Device Adapter phones

Avaya Aura® Call Center Elite and SIP devices provide an on-demand call recording feature, which Device Adapter does not support. Administrator can configure Avaya Aura® Call Center Elite to record all calls or specific calls before they are assigned to a Device Adapter phone. In this case, the phone provides media for the call, but does not manage call recording.

On Device Adapter phones, call recording can be triggered by the following:

- Avaya Aura® Call Center Elite directly
- Another phone, when a SIP call is directed to Avaya Aura® Call Center Elite
- An agent, before transferring the call to Avaya Aura® Call Center Elite
- A CTI controller application on an agent desktop

For more details about configuration, see the documentation for your call recording device.

Interflow, Night Service, Intraflow, and Overflow

Interflow, Night Service, Intraflow, and Overflow are terms describing mechanisms of sending calls in a queue to another skill group or VDN.

These mechanisms have the following common functions:

- Occur when caller threshold is exceeded: minimum number of agents is available, maximum number of calls to be queued, and the call time in queue is too high.

- Redirect new calls to a specified handling.

- Redirect calls already queued either immediately, or when another threshold is exceeded.

Call Center Elite handles programming and processing of Interflow and Night Service. For more details about these features, see *Avaya Aura® Call Center Elite Feature Reference*.

Interflow

Interflow refers to leaving the local server for an ACD skill group on another server. It can also refer to redirecting a call to some other target on another system, such as a different group. Exceeding call number or call answering time can trigger interflow. When the call waiting time in a queue reaches a specific threshold, new calls can overflow without the threshold being exceeded. If calls stay in a queue for too long, they can interflow without exceeding the call number. Calls in a queue where the last agent becomes unavailable can also interflow.

Night Service

Night Service refers to call redirection outside of site working hours. Since no agents are available at this time, the calls are redirected to a secondary location, such as another ACD number, attendant group, or an answering post extension. Rarely, the call is disconnected after an announcement.

Night Service has different variations. It can be combined with a hunt group, trunk group, or a Night Service system. However, feature handling remains the same. Both new calls and calls in a queue can be redirected to Night Service.

Intraflow

Intraflow redirects calls from the current ACD skill group to another on the same server. This can occur within a specific event, such as the last agent logging out. Intraflow can also occur when a call event or agent status triggers call redirection, for example, calls that have been in the queue for too long can intraflow to another skill group.

When the call waiting time in a queue reaches a specific threshold, new calls can intraflow without the threshold being exceeded. Calls that have been in a queue for too long can intraflow without exceeding the call number. Calls in a queue where the last agent becomes unavailable can also intraflow.

Overflow

Overflow is a generic term indicating that a call is redirected from the current skill group. This term is used in the interflow definition for Call Center Elite, but applies when calls leave a skill group to land in a night service location or when they are handled internally. However, overflow often refers to redirecting a new call.

Glossary

Term	Description
CS 1000	Avaya Communication Server 1000
Communication Manager	Avaya Aura® Communication Manager
DSA	Digital Set Adaptor
MADN	Multiple Appearance Directory Number
MCA	Multiple Call Arrangement
PD	Personal Directory
Session Manager	Avaya Aura® Session Manager
System Manager	Avaya Aura® System Manager

Index

Special Characters

Numerics

A

B

T

Index

V

W

X