Configuring Routing Service Gateway

Release 7.6
Issue 01.01
June 2014

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any

license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures to implement the Routing Service Gateway (RSG) model with CS 1000. Do not index this topic.

Intended audience

This document is intended for people who perform the product or solution system administration tasks.

Related resources

Documentation

See the following related documents at http://support.avaya.com.

Document number	Title	Use this document to:	Audience
Implementing			
NN43001–315	*Linux Platform Base and Applications Installation and Commissioning*	Install Linux Platform Base and applications.	Sales engineers, solution architects, implementation engineers, support personnel
NN43001–313	*Avaya IP Peer Networking Installation and Commissioning*	Install Avaya IP peer network.	Sales engineers, solution architects, implementation engineers, support personnel

Document number	Title	Use this document to:	Audience
Using			
NN43001–116	*Unified Communications Management Common Services Fundamentals*	View more information about enabling TLS.	Sales engineers, solution architects, implementation engineers, support personnel
NN43001-125	*Avaya Signaling Server IP Line Applications Fundamentals*	View more information for configuring: • Customer Data Block • IP telephony nodes • D-channel • SIP routes	Sales engineers, solution architects, implementation engineers, support personnel
NN43001–508	*Avaya SIP Line Fundamentals*	View more information for configuring: • Customer Data Block • IP telephony nodes • D-channel	Sales engineers, solution architects, implementation engineers, support personnel
NN43001–283	*Avaya Dialing Plans Reference*	View more information for configuring: • Customer Data Block • IP telephony nodes • D-channel	Sales engineers, solution architects, implementation engineers, support personnel
NN43001–260	*Avaya Converging the Data Network for VoIP Fundamentals*	View additional information about configuring zones.	Sales engineers, solution architects, implementation engineers, support personnel
NN43001–604	*Security Management Fundamentals*	View more information about configuring TLS	Sales engineers, solution architects, implementation engineers, support personnel
NN43001–632	*Element Manager System Reference — Administration*	View additional information about configuring IP telephony nodes..	Sales engineers, solution architects, implementation engineers, support personnel

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.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://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.

Chapter 2: Routing Service Gateway Model

Routing Service Gateway model implementation

The Routing Service Gateway (RSG) model facilitates communication between older CS 1000 systems using Network Routing Service (NRS) and more recent CS 1000 and Aura systems using Session Manager. Earlier, CS 1000 could connect to an Avaya Aura® Session Manager for connectivity to an Aura environment and other CS 1000 systems, release 7.5 and later, and an NRS functioning only as an H.323 gatekeeper. CS 1000 can now be connected to both a Session Manager and an NRS for SIP Redirect Service or SIP Proxy Service. SIP Redirect Service or SIP Proxy Service provides connectivity to CS 1000 systems earlier than Release 7.5. The NRS may still act as an H.323 gatekeeper for CS 1000 systems in the Aura network.

With this capability, you can upgrade existing SIP trunking networks more gradually. For example, you can add a new SIP Signaling Gateway (SSG) to the first switch that is upgraded to Release 7.6 with Service Pack 5 or later. This SSG uses an SM to provide a SIP Routing Service, while retaining the SSG with a connection to the NRS. Other switches can continue to connect to the NRS, using the upgraded CS 1000 to act as a gateway between the NRS and the Session Manager. Electronic Switched Network (ESN) routing can be created to route calls to the appropriate SSG and Routing Service. Calls require a single VTRK on each SSG for every call from the older, NRS based network to the newer, Session Manager based network.

The RSG can be any call server in the network. However, consider the following factors while setting up the RSG:

- the traffic to be handled when adding the SSG for the Session Manager-side of the network
- available traffic capacity on the call server and NRS-side SSG to handle additional tandem calls that will now pass through the RSG node
- change in load when more call servers are migrated from the NRS to the Session Manager

The peak tandem traffic occurs on the RSG when approximately half the systems or applications are migrated to Aura. By that time you might need to add more signalling servers at the RSG. You might also need to configure more call servers to act as RSGs, with routing through the NRS and Session Manager redefined to balance loads.

Routing Service Gateway model description

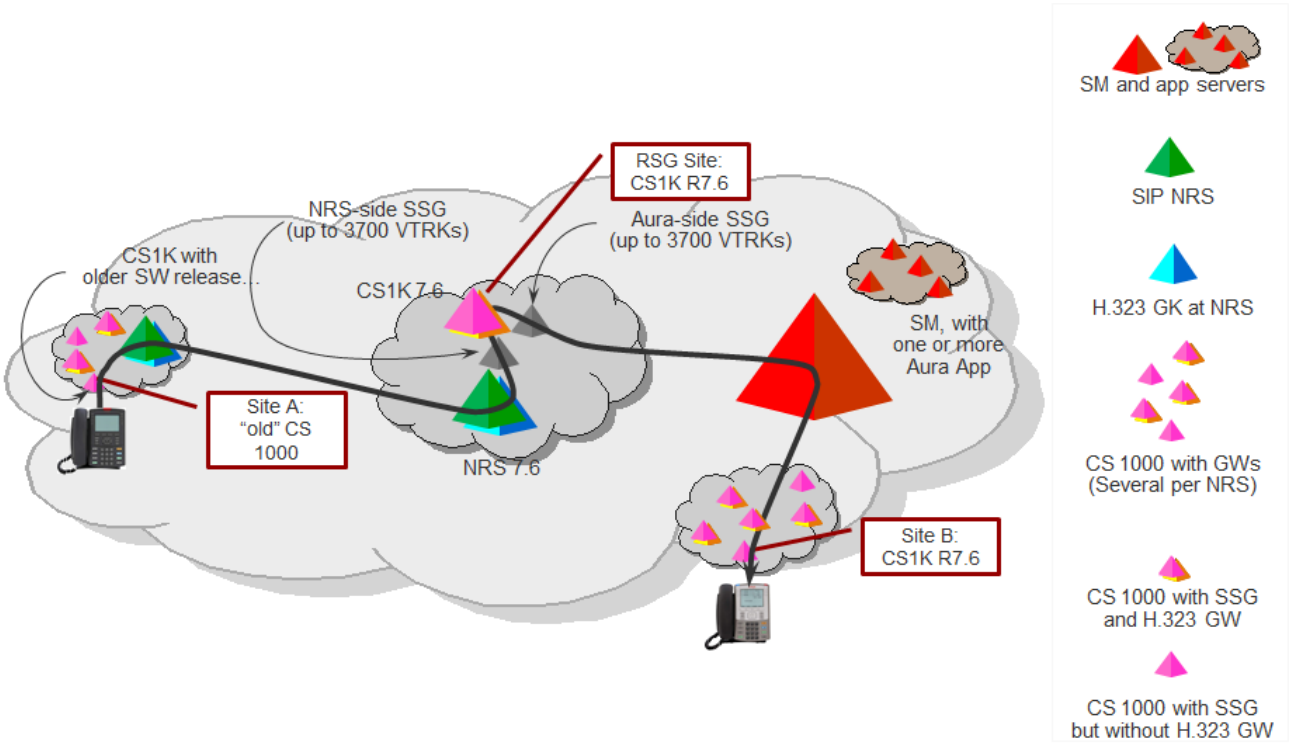

Figure 1: Routing Service Gateway model

Site A	CS 1000 releases prior to Release 7.6 connected to Release 7.6 NRS Users are CS 1000 users with TDM and IP sets.
Site B	CS 1000 7.6 or Communication Manager connected to Session Manager. Note that these systems may also connect to an H.323 Gatekeeper by using an H.323 GW. However, this is outside the scope of the Routing Service Gateway. Users can be CS 1000 users or Communication Manager users.
RSG Site	2 SIP Signaling Gateways (CS 1000 7.6) with one SSG dedicated to the NRS and another to the Session Manager. Both SSGs are connected to one Call Server. This CS 1000 functions as a gateway between all older release CS 1000, prior to Release 7.5, and all newer release CS 1000 systems, Release 7.6 and later, on Session Manager. Calls require a single VTRK on each SSG for every call from the older NRS based environment to the newer Session Manager based environment.

Chapter 3: Configuring Routing Service Gateway Site

Overview

This section provides procedures for configuring the Service Gateway site. Since this configuration is used mostly in upgrade scenarios, the SSG for the NRS and the NRS itself, will already exist. You must configure Routing Service Gateway using Element Manager. Routing Service Gateway systems must already be upgraded to release 7.6, service pack 5 or later, and deployed.

For more information about installation and configuration, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315* and *Signaling Server IP Line Applications Fundamentals, NN43001–125*.

Configuring the SSG dedicated to the Session Manager

Checklist for configuring the SSG dedicated to the Session Manager

Use this checklist to configure the SSG dedicated to the Session Manager.

No.	Task	Description	✔
1	Configure a new IP Telephony Node and configure the SIP gateway.	See Configuring a new IP telephony node and SIP gateway on page 11.	
2	Configure a D-channel over IP.	See Configuring a D-channel over IP on page 11.	
3	Configure zones.	See Configuring zones on page 12.	
4	Configure SIP routes.	See Configuring a SIP route on page 12.	
5	Configure Virtual trunks.	See Configuring virtual trunks on page 13.	
6	Configure Virtual loops.	See Configuring virtual loops on page 12.	

No.	Task	Description	✔
7	Configure call routing (Route List Block and Digit Manipulation Index).	See Configuring call routing on page 13.	
8	Configure Routing Prefixes to reach the Aura network (such as Distant Steering Code)	See Routing prefixes configuration on page 14.	
9	Configure TLS.	See TLS on the SSG on page 15	

Configuring a new IP telephony node and SIP gateway

Procedure

1. Log in to UCM and access EM to configure a new node on CS 1000.
2. Go to **EM** > **System** > **IP Network** > **Nodes : Servers, Media Cards**.
3. Select a node and click **Add**.
4. Choose a unique Node Number and new Node IP for the TLAN, Gateways for the ELAN and TLAN, and subnet mask.

   Ensure that you use the same Call Server IP address as the existing nodes.
5. Select the **Virtual Trunk Gateway (SIPGw, H323Gw)** check box and click **Next**.
6. In the **Vtrk gateway application** field, click **SIP Gateway (SIP Gw)**.
7. Enter the required SIP domain name, local SIP port, gateway endpoint name, and application node ID.
8. In the **Primary TLAN IP address** field, enter type the Session Manager SIP Entity IP address, and clear the **Support registration** check box.
9. Save the node, and synchronize and restart applications.

Configuring a D-channel over IP

Procedure

1. From the EM navigation pane, click **Routes and Trunks** > **D-Channel**.
2. In the Configuration section, type the D-channel number and type.
3. Click **to Add**.
4. In the **D channel Card Type** field, type `DCIP`.
5. In the **User** field, click **Integrated Services Signaling Link Dedicated (ISLD)**.
6. In the **Interface type for D-channel** field, click **Meridian Meridian1 (SL1)**.

7. Click **Submit** to save the changes.

Configuring zones

Procedure

1. From the EM navigation pane, go to **System** > **IP Network** > **Zones** > **Bandwidth Zones**.
2. In the **Intrazone Bandwidth (INTRA_BW)** field, click **Best Quality (BQ)**.
3. In the **Interzone Bandwidth (INTER_STGY)** field, click **Best Quality (BQ)**.
4. In the **Zone Intent (ZBRN)** field, click **VTRK (VTRK)**.

Configuring a SIP route

Procedure

1. In the EM navigation pane, click **Routes and Trunks** > **Routes and Trunks**.
2. In the row associated with the customer, click **Add route**.
3. In **Basic Configuration**, select a route number from the **Route Number (ROUT)** field.
4. In the **Trunk Type (TKTP)** field, click **TIE trunk data block (TIE)**.
5. Enter the Access Code for the trunk route (ACOD).
6. Select the **The route is for a virtual trunk route (VTRK)** check box.
7. Enter the zone number , node ID, and protocol ID.

   The VTRK zone is used here.
8. Select the **Integrated services digital network option (ISDN)** check box.
9. In the **Mode of operations (MODE)** field, click **Route uses ISDN Signaling Link (ISLD)**.
10. In the **Interface type for route (IFC)** field, click **Meridian M1 (SL1)**.
11. Select the **Network Calling Name Allowed (NCNA)** check box.

Configuring virtual loops

Procedure

1. Click **System** > **Core Equipment** > **Superloops**.
2. Choose the superloop number that you want to add.
3. Click **Add**.
4. In the **Superloop Type** field, click **Virtual**.
5. Click **Save**.

A Virtual TN number is assigned. For example, if you add virtual super loop 84, then the Virtual TN is 84-0-0-0 to 84-1-15-31 (1024 TNs).

Configuring virtual trunks

Procedure

1. In the EM navigation pane, click **Routes and Trunks** > **Routes and Trunks**
2. Select the customer for whom you are configuring virtual trunks.
3. To add new trunk members, in the row containing the route listing, click **Add trunk**.
4. When using more than one trunk, select **multiple trunk input number (MTINPT)**.
5. In the **Trunk data block** field, click **IP Trunk (IPTI)**.
6. Type a **Terminal number** (TN).
7. Type a **Member number** (RTMB).
8. Click **IMM (immediate)** in the **Start arrangement Incoming** field.
9. In the **Class of Service** field, click **Edit**.
10. Select appropriate options such as restriction level UNR or dial pulse DTP or DIP.
11. Click **Return Class of Service**.
12. Type a **Channel id for this trunk** (CHID).

    Depending on the hardware type of the Signaling Server, the CHID can be a number in the range 1 to 382 or 683 to 4000.
13. Click **Save**.

Configuring call routing

Before you begin

Configure ESN database, including ESN Access Codes, Basic Parameters, and Network Control before configuring call routing. Also configure the First Digit Manipulation index .

Procedure

1. In the EM navigation pane, click **Dialing and Numbering Plans** > **Electronic Switched Network**.
2. On the Electronic Switched Network (ESN) webpage, click **Customer xx** > **Network Control & Services** > **Digit Manipulation Block (DGT)**.

   The system displays the Digit Manipulation Block List page.
3. In the **Please choose the** field, select a Digit Manipulation Block Index number and click **to Add**.

4. Enter appropriate data in the Digit Manipulation Block page, and click **Submit**.

   The system completes the Digit Manipulation index configuration.

5. To configure Route List block, go to the EM navigation pane and click **Dialing and Numbering Plans** > **Electronic Switched Network**.
6. On the Electronic Switched Network (ESN) page, click **Customer xx** > **Network Control & Services** > **Route List Block (RLB)**.
7. In the **Please enter a route list index** field, enter the route list index number and click **to Add**.
8. On the Route List Block page, enter appropriate information and click **Submit**.

   The system generates the new Route List Block and loads the Route List Blocks page.

Next steps

Configure ESN entities to direct calls to the Session Manager that should be associated with switches or applications configured on the SM side of the RSG. This includes entities such as Location Codes, Numbering Plan Area Codes, or Steering Codes. When subsequent CS 1000 switches are moved from the NRS side to the SM side, additional data will direct calls through the SM-side SSG. In some cases, this could be done easily by changing an existing entity to use an RLB that contains the SSG trunk routes associated with the SM-side SSG.

Routing prefixes configuration

In the customer network, many options might be available to provide routing. These options are described in detail in the following documents:

- *NN43001–632 Element Manager System Reference — Administration*
- *NN43001-313 IP Peer Networking Installation and Commissioning*, in the *Using Element Manager for configuration* and *Configuring call types* sections

The Distant Steering Code steps are included in this document only for reference. Customers might need to provision any combination of these steering codes including Location Codes, International, National, Subscriber, or Special Number prefixes, on a customer-by-customer basis. For more information about provisioning these areas, see *NN43001–632 Element Manager System Reference — Administration* and *NN43001-313 IP Peer Networking Installation and Commissioning*.

Related Links

Configuring distant steering codes on page 14

Configuring distant steering codes

Procedure

1. In the EM navigation pane, click **Dialing and Numbering Plans** > **Electronic Switched Network**.
2. On the Electronic Switched Network (ESN) page, click **Customer xx** > **Coordinated Dialing Plan (CDP)** > **Distant Steering Code (DSC)**.

3. Select **Add** from the drop-down list.
4. Enter the steering code in the **Please enter a distant steering code** field, and click **to Add**.
5. On the Distant Steering Code page, enter the appropriate details and click **Submit**.

Related Links

Routing prefixes configuration on page 14

CS 1000 UCM SHA256 support

With SHA256 update applied, all the newly generated x509 certificates are signed with the latest SHA256 algorithm. SHA256 is included from Release 7.6, Service Pack 5 onwards. You can force switch back to SHA1 for the whole system using the **`defaultSAconfig`** linux command.

For customers with mixed release systems (7.5, 7.0, or lower)

In mixed release systems (releases 7.5. 7.0 or lower), SHA1 cannot register through SIP TLS to NRS SHA256. Hence, for mixed release systems, use only SHA1.

Before installing Service Pack 5 on Primary UCM server, note that:

- After installing SP5 on Primary UCM server, all the newly created Default, WebSSL, DTLS and SIP TLS certificates are signed with SHA256 algorithm.
- To avoid CS 1000 systems negotiation breakage, SHA1 certificate must be generated. You can use the Linux command **`defaultSAconfig`** on the Primary UCM server under user admin2 to change back to SHA1. After this, all newly created Default, WebSSL, DTLS and SIP TLS certificates are signed with SHA1 algorithm.
- When the older systems migrate to 7.6 or are decommissioned, you can change the Signature algorithm to SHA256 again by using the **`defaultSAconfig`** command.
- During backup on Primary UCM or Member Linux server, all the certificates are dumped. Therefore, restoring backup with SHA1 on the SHA256 server will roll the server back to SHA1

Related Links

Changing signing algorithm to SHA2 from System Manager UCM on page 15

Changing signing algorithm to SHA2 from System Manager UCM

Procedure

1. On the System Manager UCM home page, click **Configuration** > **Settings** > **SMGR** > **Trust Management**.
2. In the **Preference setting for the signing algorithm to be used by the CA** field, click **2**.

Related Links

CS 1000 UCM SHA256 support on page 15

TLS on the SSG

Before enabling TLS on SSG, you must have certificates ready on all servers.

The NRS serves SSGs from Release 7.6 Service Pack 5, and Release 7.5, 7.0, and older releases. Therefore, to enable TLS for NRS, you must use SHA1 for the following components:

- NRS server upgraded to Release 7.6, Service Pack 5
- SIP gateway that connects to NRS

Important:

Do not use Best Effort for calls on this SSG. Incompatibilities between Aura Best Effort and CS 1000 Best Effort result in calls being rejected.

To enable and use TLS, you must use port 5061. For more information about enabling TLS , see:

- *Security Management Fundamentals, NN43001–604*
- *Unified Communications Management Common Services Fundamentals, NN43001–116*, Appendix

Index