Presence Services with Communication Server 1000
Avaya Communication Server 1000

7.5
NN43001-141, 03.03
April 2012

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 generally makes available to users of its products. 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 Web sites 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 its Hardware and Software (“Product(s)”). 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. 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 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release

The following sections detail what is new in the *Presence Services with Communication Server 1000, NN43001-141.* for Avaya Communication Server 1000 Release 7.5.

Features

See the following sections for information about feature changes.

Avaya Aura Presence Server with the CS 1000 and one-X Communicator

The Instant Messaging (IM) and Presence application has changed significantly for Communication Server 1000 Release 7.5. As part of the overall integration of Communication Server 1000 to Avaya Aura®, the supported application for IM and Presence has evolved to Avaya Aura Presence Services (PS) Release 6.1.

The implementation of Communication Server 1000 IM and Presence application for Release 6.0 and 7.0 is not supported for Communication Server 1000 Release 7.5. The clients for Release 6.0 and 7.0, IPSP 3456, and the Web tool are no longer supported for Communication Server 1000 Release 7.5. The Communication Server 1000 Release 7.5 solution for IM and Presence comprises the following four solution elements:

- Avaya Communication Server 1000 Release 7.5 requires the latest DEP list and Service Updates.

  Note:

  Always check the Avaya Support site for the latest versions of the DEP list and Service Updates.

- Avaya Aura Presence Services Release 6.1 is required as the foundational element for Avaya and third-party applications to collect and distribute Presence information and IM capabilities on an enterprise network.
- Avaya System Manager Release 6.1 Service Pack 3 is required. Avaya Aura Presence Services requires System Manager to deploy and manage
- The one-X Communicator 6.1 client specifically for Communication Server 1000 utilizes a Communication Server 1000 SIP Line soft client that is capable of SIP voice and video (point-topoint) services and XMPP-based Instant Messaging and Presence services

The Avaya Aura PS application requires the XMPP protocol to collect and distribute Presence state information and to deliver IM services. Clients supporting the XMPP protocol are able to participate in the IM and Presence services. The one-X Communicator Communication Server 1000 Release 7.5 client uses the XMPP-capable soft client to deliver SIP voice and video as well as XMPP-based IM and Presence services. Communication Server 1000 Release 7.5 continues to support tracking of on-the-phone Presence for Communication Server 1000 lines using non-XMPP capable phones and clients. The core Presence Publisher delivers Presence updates to Avaya Aura PS based on provisioning of PREA Class of Service and implementation of the SIP Converged Desktop ISM for each line to be tracked as in Releases 6.0 and 7.0. Subscriber Manager continues as the management application to define the Presence Services users and is now associated with Avaya System Manager. Subscriber Manager is also used to migrate the Communication Server 1000 users from the previous IM and Presence application to the new Avaya Aura PS.

For more information, see Figure 1: IM and Presence architecture on page 16.

Other changes

See the following section for information about changes that are not feature-related.

Revision History

April 2012	Standard 03.03. This document is up-issued to add details needed for Presence services for Avaya Communication Server 1000 Release 7.5.
December 2011	Standard 03.02. This document is up-issued to support Communication Server 1000 Release 7.5. A note is added in chapter Installation and Commissioning to indicate that a presence account is required for each Presence Publisher user.
December 2011	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 7.5 and reflects changes in technical content for Appendix A, Adding a Subscriber, XMPP message traces and Personal Agent, IM and Presence server commands, and the Overlay commands section.
June 2010	Standard 02.01. This document is up-issued to address content changes to the Avaya Communication Server 1000 IM and Presence Web Tool for Communication Server 1000 Release 7.0.
November 2009	Standard 01.03. This document is up-issued to address content changes to the Communication Server 1000 IM and Presence Web Tool chapter, graphics, and to address adding profile information through Subscriber Manager.

October 2009	Standard 01.02. This document is up-issued to address content changes to the Communication Server 1000 IM and Presence Web Tool chapter, graphics, and provide additional procedural information.
October 2009	Standard 01.01 This document is released to support the Instant Messaging and Presence Services for Communication Server 1000 Release 6.0.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

Navigation

This document contains the following chapters.

Subject

This document supports the Instant Messaging (IM) and Presence Services to the Avaya Communication Server 1000 (CS 1000). The Avaya CS 1000 IM and Presence Services provides IM capability and phone presence information for all CS 1000 users. Only CS 1000 one-X Communicator users can view presence information and exchange instant messages.

Technical documentation

The following technical documents are referenced in this document:

- *Avaya Subscriber Manager Fundamentals, NN43001-120*
- *Avaya Unified Communications Management, NN43001-116*
- *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Avaya Element Manager System Reference - Administration, NN43001-632*
- *Avaya SIP Line Fundamentals, NN43001-508*
- *Avaya Software Input Output Reference — Maintenance, NN43001-711*
- *Overview and Planning for Avaya one-X® Communicator for CS 1000 (for administrator)*
- *Administering Avaya one-X® Communicator for CS 1000 (for administrator)*
- *Implementing Avaya one-X® Communicator for CS 1000 (for user)*
- *Using Avaya one-X® Communicator for CS 1000 (for user)*

Chapter 4: Fundamentals

This chapter explains the concepts that are necessary to understand for implementation of the IM and Presence Services.

Navigation

Deployment model

The following diagram shows the system components and architecture used to support the IM and Presence Services.

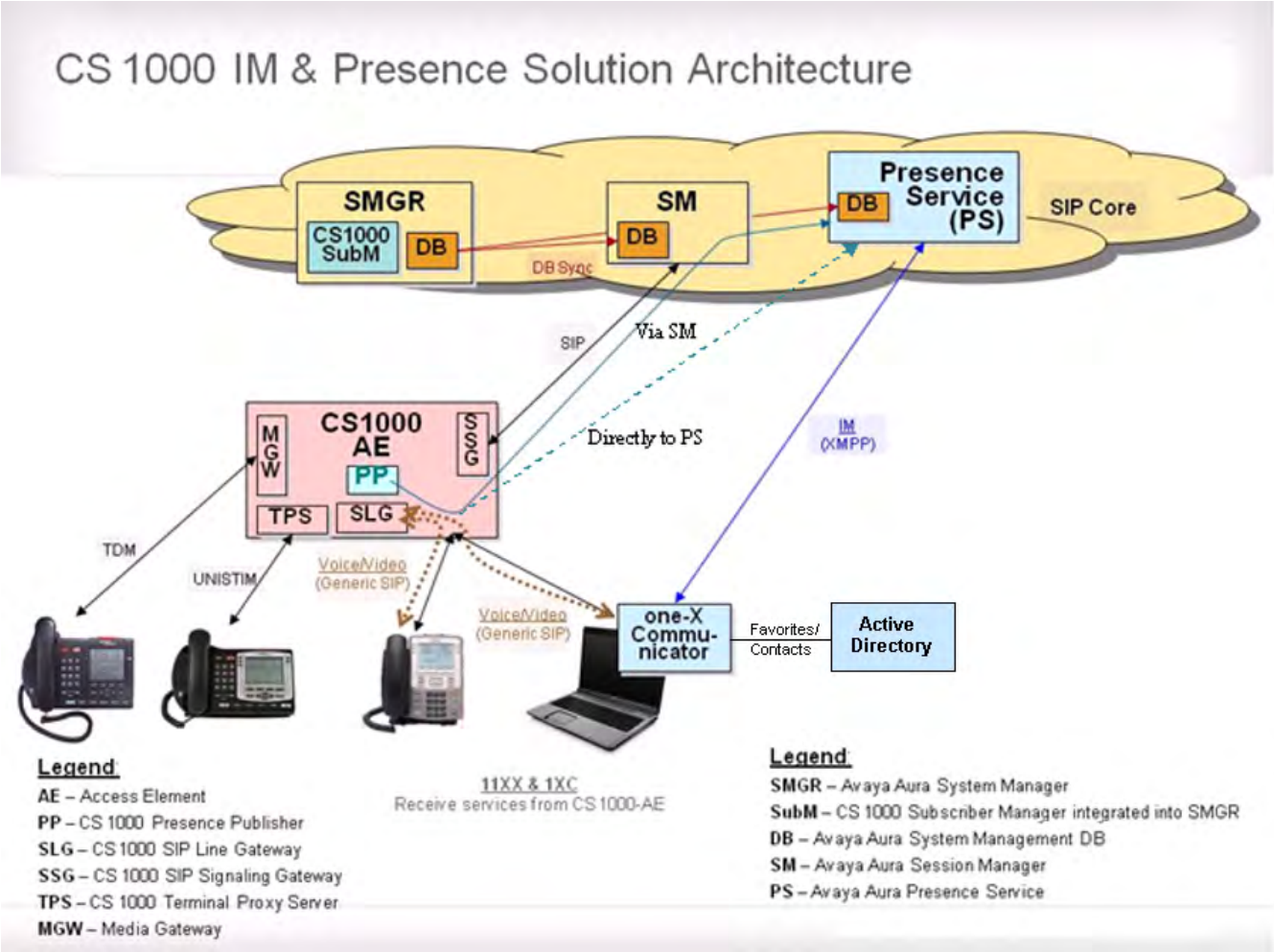


Figure 1: IM and Presence architecture

System component description

The following table provides an overview of the system components used to support the IM and Presence Services.

Table 1: Presence Component Overview

Component	Description
Avaya Aura® System Manager	This management system coordinates the overall system management. This is the CS 1000 primary security domain and all of the CS 1000 components must join this security domain.
CS 1000 Subscriber Manager	Configures CS 1000 user accounts. This resides within System Manager.

Component	Description
Avaya Aura® Session Manager	Presence Services sends the presence status through Session Manager.
CS 1000 Presence Publisher (PP)	A software application running on the Signaling Server works with the CS 1000 Call Server to provide telephony presence updates to the IM Presence server through the SIP Publish message. The CS 1000 PP sends status of the non-XMPP phones to the Presence Service (directly or through the Session Manager).
Avaya Aura® Presence Service (PS)	PS receives the status from Presence Publisher and sends it to the one-X Communicator client. This is also used to send the presence status directly between two one-X Communicator clients.
Active Directory	Active Directory integrates with one-X Communicator client to add favorites to the client contact list.

The following table provides the version numbers requirements for the IM and P system components:

Component	Version number
System Manager	6.1
Session Manager	6.1
CS 1000	7.5
Presence Services	6.1
Avaya One-X Communicator	CS1000 specific version

System component requirements

This section mentions the patching requirements for IM and P components.

Patch requirements

Following patches are included for the CS 1000 and Presence integration for release 7.5:

- Call Server patch MPLR30782
- Signalling Server SU cs1000-vtrk-7.50.17.16-18.i386.000.ntl (or higher version) on all the signaling servers.
- Avaya Presence Services server must have PS6.1 Service Pack 1 (PS-06.01.01.00-0610) and PS6.1 Service Pack 1-Patch one (PS-06.01.01.01-0608)

Supported IM and Presence clients

One-X Communicator is the only client supported for telephony presence. You will require CS 1000 specific version of the client for CS 1000 integration.

Supported telephony Publishing Presence clients

The one-X Communicator Client views the Idle or Busy status of Analog, Digital, VoIP-Unistim, SIP Line, MobileX, MC 3100 and IP softphone clients.

Chapter 5: Planning and Engineering

This chapter provides information about system planning and engineering.

Navigation

IM and Presence server capacity

The IM and Presence server can support the following:

- A maximum of 10 000 users per server with an average of 25 contacts per user.
- A maximum of 15 Instant Messages (IM) for each user in a one hour period.
- A maximum of 12 presence status changes for each user in a one hour period.
- A maximum of 50 contacts in a user contact list.

Presence Publisher capacity

A Presence Publisher is expected to handle more then 5000 users based on the IM and Presence server capacity described above. In the event that one Presence Publisher instance cannot handle all telephony presence from non IM and Presence clients (Analog, Digital, VoIP-Unistim, SIP Line, MobileX, and MC 3100 and IP Softphone) then additional Presence Publishers can be deployed on existing Signaling Servers available in the system.

Converged Desktop ISM License

Every subscriber Terminal Number (TN) with Class of Service Presence Allowed (PREA) enabled requires one Converged Desktop ISM License. The SIP Presence publishing feature

requires a SIP Converged Desktop ISM. Class of Service PREA is required for phones that do not support the Extensible Messaging and Presence Protocol (XMPP). The one-X Communicator feature does not require PREA as it supports XMPP.

Chapter 6: Installation and Commissioning

This chapter provides information for installing and commissioning CS 1000 7.5 IM and Presence Service. Perform the installation procedures according to the order of appearance in this chapter.

Navigation

Installing Avaya Aura System Manager

Install Avaya Aura® System Manager on a new Commercial off-the-shelf (COTS) server.

For more information about the installation of System Manager, see *Installing and Upgrading Avaya Aura® System Manager*.

Installing Avaya Aura Session Manager

If the Presence Publisher connects to Presence Server through Session Manager, configure the Session Manager to route the presence messages.

For information about Session Manager configuration, see *Installing and Configuring Avaya Aura® Session Manager*.

Installing Avaya Aura Presence Server

Install Avaya Aura® Presence Server on a new COTS server for standalone deployment or a high-end server for system platform deployment.

For more information about Presence Server installation, see *Installing Avaya Aura® Presence Services*.

Installing new CS 1000 Signaling Server package

Presence Publisher service is bundled under the Signaling Server deployment package. Deploy the Presence Publisher service by selecting the Signaling Server deployment package available in UCM Deployment Manager.

For more information about installing the Signaling Server, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

Configuring Presence Publisher

Configure the CS 1000 Presence Publisher (PP) for sending the Presence Server telephony status of all CS 1000 line types that do not use XMPP protocol.

1. Click **UCM Services** in System Manager.

   The system displays the UCM Services page of the CS 1000 Unified Communications Management (UCM).

2. On the Elements page, select the Element Manager element with Element type CS1000.

   The System Overview page displays.

3. Under **System**, click **IP Network** to open a sub-menu.
4. Click **Nodes: Servers, Media Cards**.

   The IP Telephony Nodes displays.

5. Click the node in which the Presence Publisher is to be configured.

   The Node Details page displays.

6. To configure Presence publisher, select the **Presence Publisher** application.

Presence Publisher Configuration Details page appears.

7. Check the box **Enable presence publisher service** to enable the Presence Publisher.
8. From the **IM and Presence server type** drop-down list, select the server type Aura PS.
9. Under Security Policy, select **Best Effort** for TLS connection or **Security Disabled** for TCP connection.

   Note:

   Select **Security Disabled** option when you do not want to connect the Presence Publisher to the Session Manager over TLS. The Session Manager SIP Entity Link must be set up to match this security selection. However, you must use TLS if you want to connect the Presence Publisher directly to the Presence Server.
10. Enter the presence SIP domain name in **IM and presence server FQDN**.

    This entry should match with the value that is configured in "Domain Substituion - To" in /Home/Elements/Presence/Configuration web page of the System Manager
11. Enter the IP address of the Presence Server in the **IM an Presence server IP**.
12. Enter the port number of the Presence Server in **Port** and select TLS in **SIP transport** if Best Effort is selected for Security Policy. Otherwise, select TCP.

    You can use the default ports, however they should not be used by other applications. Also, they should match the actual port numbers of the target servers.
13. Check the box **Client Authentication** if you want the client to share its certificate and the server authenticates it so that a two-way authentication is achieved. Un-check this option to provide server authentication only - the server shares its certificate and the clients authenticates it.

    Check the box **x509 Certificate Authentication enabled** if you want the SIP TLS to provide both encryption and identity verification. Un-check this box to allow the system to accept self-signed certificates from the server side, when operating on the client side of the SIP/TLS connection. In this case, the system provides encryption only and does not verify the identity.
14. In the Outbound Proxy server section, select send the SIP publish message directly to the Presence server or send it to Session Manager, for routing messages to the Presence server.

    Note:

    To be consistent with the Avaya Aura® deployment practice, Avaya recommends sending the messages through the Session Manager.
15. Enter the IP address of the Presence Server in the **Outbound Proxy settings** if you want to send the SIP publish messages directly to the Presence Server.

16. If you are using Session Manager to route the SIP publish messages, configure the following:
    - Enter the IP address of the Session Manager in the **Outbound Proxy settings**.
    - Select TLS if you have selected Bet Effort for security, otherwise select TCP.

      Note:
      Do not use UDP.
    - Configure a Presence server SIP Entity and a Session Manager to Presence server SIP Linkage in the System Manager.
17. Under Server Settings, enter the customer name and the presence service DN (PSDN).

    The values entered here should match the values configured in LD 23. For more information about LD 23 configuration, refer Software Input Output Reference — Administration *NN43001–611*.
18. Click **Save** to save the configuration of the Presence Publisher, and then click **Save** on the Nodes Detail page.

    The configuration is saved to the Call Server. A Node Saved page displays.
19. Click **Transfer Now** to transfer the configuration to the signaling server.
20. Click **Restart Application** to start the Presence Publisher service on the designated server.

Note:
AML, VAS, and PSDN must be configured for Presence Publisher to work. For more information about these configurations, see Overlay commands—LD 17 on page 67.

Note:
A presence account is required for each Presence Publisher user. For presence account configuration, refer XMPP IM and Presence configuration on page 27.

Note:
To configure ACL in the System Manager set the Default Policy for Presence ACL to **Allow** by navigating to Users > User Management > System Presence ACLs in the System Manager.

Related topics:

TLS configuration between CS 1000 and Session Manager on page 24

TLS configuration between CS 1000 and Session Manager

The following sections provide the procedures for configuring TLS between the CS 1000 and Session Manager.

Related topics:

Adding a CS 1000 UCM Primary Certificate Authority on Session Manager on page 25
Updating installed certificates on page 26
Replacing the Session Manager default certificate on page 26
Changing the Session Manager operating certificate on page 27
TLS configuration if Presence Publisher is to Connect To PS Directly on page 27

Adding a CS 1000 UCM Primary Certificate Authority on Session Manager

Add a CS 1000 UCM Primary Certificate Authority on Session Manager.

1. Log on to UCM and download the UCM Private Certificate Authority to your PC.
    a. In the UCM navigation tree, click **Security > Certificates**.

        The Certificate Management Web page appears.

    b. On the UCM Certificates page, download the “UCM Private Certificate Authority” ca.cer file to your PC.

    c. Click the **Private Certificate Authority** tab.

        The Private Certificate Authority page displays.

    d. Click **Download**.

    e. Click **Save** to save the ca.cer to your PC.

2. Add the UCM ca.cer file as a trusted certificate for Session Manager.
    a. In System Manager, navigate to **Elements > Inventory**.

    b. In the navigation tree, click **Manage Elements**.

    c. In the Entities section, select a Session Manager Application from the table for the required Session Manager instance.

        If you do not find Session Manager Application in the table, create a new Session Manager Application entity. For information on these steps, refer *Unified Communications Management Common Services Fundamentals* NN43001–116.

    d. From the **More Actions** menu, choose **Configure Trusted Certificates**.

    e. Click **Add** to add a UCM Primary certificate.

    f. Choose **Import from file**.

    g. Click **Browse** to select the ca.cer file on your PC.

    h. Click **Retrieve Certificate** and review the certificate details before you continue.

i. Click **Commit** to add the trusted certificate.

Updating installed certificates

Update installed certificates for Session Manager.

1. In System Manager, navigate to **Elements > Session Manager > System Status**.

   The System Status page appears.
2. In the navigation tree, click **Security Module Status**.
3. In the Entities section, select a Session Manager Application from the table for the Session Manager instance you require.
4. Click **Update Installed Certificates** to update the imported UCM certificates.
5. Click **Confirm** to confirm the selected Session Manager.

Replacing the Session Manager default certificate

Replace the Session Manager default certificate as it uses a hard coded Common Name.

1. In System Manager, navigate to **Elements > Inventory**.
2. In the navigation tree, click **Manage Elements**.
3. In the Entities section, select a Session Manager instance.
4. From the **More Actions** menu, click **Configure Identity Certificates**.
5. Click **security module**, and click the **Replace**.
6. Click **Replace this Certificate with Internal CA Signed Certificate**.
7. Configure the following values and click **Key Algorithm** and **Key Size**.
   - **Common Name:** FQDN of the Session Manager server
   - **Organization:** Your company name.
   - **Country:** Select a country from the list.
   - **Organization Unit:** A division within your company.
8. Verify your data, and click **Commit**.

Changing the Session Manager operating certificate

Change the Session Manager operating certificate.

1. In System Manager, navigate to **Elements > Session Manager > System Status**.

   The System Status page appears.
2. In the navigation tree, click **Security Module Status**.
3. In the Entities section, select the Session Manager instance.
4. Click **Certificate Management > Use Customer Certificate**.
5. Click **Confirm**.

TLS configuration if Presence Publisher is to Connect To PS Directly

If the Presence Publisher (PP) is to connect to the PS directly (instead of routing through the SM), the administrator needs to add the CS1000 CA certificate into the PS.

1. In UCM CA, download CS1000's CA certificate (for example, "ca.cer").
2. FTP or SFTP the downloaded file to your PS Server and run:

   ```
   /opt/Avaya/Presence/presence/bin/prescert import pem <ca.cer>
   ```

   ```
    /opt/Avaya/Presence/presence/bin/prescert exportTS
   ```

   (The certificate is in /opt/Avaya/Presence/jabber/xcp/certs)
3. Login to the XCP Controller – presence.
4. Click **Core Router** ->**Edit**.
5. Set Configuration View to "Advanced".
6. Add your PP host to "Mutually Trusted TLS Hostnames".
7. Restart PS.

XMPP IM and Presence configuration

Configure the XMPP IM and Presence feature for a user with one-X Communicator CS 1000 client. Use the procedures in this section to add presence elements, create a subscriber, and create an account for a subscriber.

Adding a presence element

A presence element is required for configuring a presence account for each user so that the user's data is populated to the Presence Server.

1. In System Manager, click **Administrators**.

   The system displays the Administrative Users page of the CS 1000 Unified Communications Management.

2. Under **Network**, click **Elements**.

   The Elements page displays the elements in Unified Communications Management.

3. To add a new element, click **Add**.
4. From the **Type** list, select **Avaya Presence**, and click **Next**.
5. Enter the name and the description of the element.
6. In the **SMGR IP address** field, enter the System Manager FQDN or IP address.
7. In the **SMGR URL** field, enter the System Manager IP address.
8. In the Presence Account Password field, enter the default presence password.

   Note:

   This password is pushed to the System Manager as the Communication Profile Password for the Presence Server for the user. It is overwritten by the subscriber password after you perform password synchronization.

9. Click **Save**.
10. Return to the Elements page to verify the new element you just added.

Creating a subscriber

Create a subscriber.

1. In System Manager, click **Administrators**.

   The system displays the Administrative Users page of the CS 1000 Unified Communications Management.

2. Under **Network**, click **Subscriber Manager**.
3. Under **Subscribers**, click **Add** to add a new subscriber.
4. Type the details of the new subscriber, such as Last name, First name, Employee ID, and so on.

   Username, domain, and password are mandatory fields. The Username and domain are stored in the Presence Server for identifying a user for routing the IM and Presence status to the intended user. The Username and domain are also stored in the CS 1000 so that they match what are in the Presence Server when a SIP Publish message is sent. The username is stored in the CS1000 Call Server as PUID in the TN data block. The password is same for both registering the oneX Communicator to the CS1000 as SIP Line and for registering to the Presence Server as an IM and Presence user. one-X client registers to CS 10000 as SIPL and to

Presence Server as XMPP client (Other details could be used by the one-X client if it supports OpenLDAP).

You must synchronize the password of all the presence and telephony accounts so that you use the same password for Presence and Instant Messaging and for logging on to the one-X Communicator as SIP Line phones. Password synchronization sends the password configured in the subscriber manager to both the CS1000 Call Server and the Presence Server. In the CS1000 Call Server, it is stored in the UPWD prompt in the TN data block

For more information on steps for password synchronization see, Synchronizing your password on page 45.

5. In the **E-mail** field, type <*username*>@<*domain*>, for example, jsmith@avaya.com.

   The username/domain combination is required for searching contacts using the one-X Communicator with IM Handle Mapping using E-mail address.

6. Click **Save**.

Creating a Presence account for a subscriber

Create a Presence account for a subscriber.

1. Select the subscriber.
2. Click **Add Accounts**.
3. From the **Service type** list, click **Presence** as the service type for the subscriber.
4. Specify the values for **Location** and **Element**.

   The Target and Template fields can be left as the default selection.

5. Click **Save**.

Note:

The user data, such as the Jabber ID and the login name of the subscriber, is replicated in the System Manager database and the PS local and XCP databases.

Chapter 7: Migration of CS 1000 7.5 IM and Presence to System Manager

This chapter provides information about migrating CS 1000 7.5 IM and Presence to System Manager.

All CS 1000 servers need to join the System Manager security domain as member servers. For more information about migration to System Manager, see *Unified Communications Management Common Services Fundamentals, NN43001-116*.

Navigation

Subscriber Manager data migration task flow

The following figure is a high-level task flow to migrate Subscriber Manager data to System Manager.

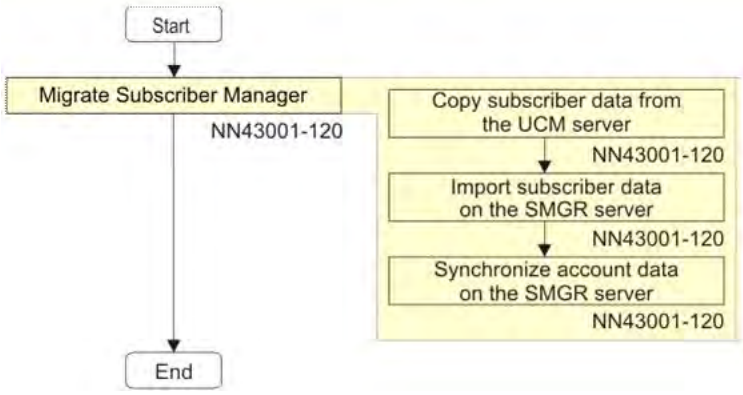


Figure 2: Task flow

Migrating Subscriber data from UCM to System Manager

Use the following procedures to migrate Subscriber data from a UCM server to System Manager by migrating the subscribers on the source to the destination system. Use the following procedures to obtain the subscribers.

On the source system:

1. Log on to the primary UCM server by using `admin2` for Release 7.5 systems or `nortel` for Release 7.0 and earlier systems.
2. Switch to super user (su).
3. Type the command `cd /opt/nortel/cnd`.
4. Type the command `./cnd.sh stop_service`.
5. Type the command `./slapcat -f slapd.conf-s ou=subscribers,dc=nortel,dc=com-a objectclass=nortelsubscriber -l subscriberData.ldif`.
6. Type the command `./cnd.sh start_service`.

   Use a secure FTP client to copy subscriberData.ldif to the `/opt/nortel/cnd` folder of the destination system.

On destination system:

1. Log on to the primary System Manager server command line.
2. Switch to super user (su).
3. Type the command `cd /opt/nortel/cnd`.
4. Type the command `./cnd.sh stop_service`.
5. Enter the following command:

   ```
   ./slapadd -f slapd.conf -l subscriberData.ldif -c .
   ```

6. Type the command `./cnd.sh start_service`.

Replace Openfire Server by Avaya Aura Presence Server

In CS 1000 Release 7.5, the Openfire Server is not supported. It is replaced by the Avaya Aura® Presence Server. Configure the following to support Avaya Aura® Presence Server.

- CS 1000 Presence Publisher:
  - Reconfigure the CS 1000 Presence Publisher to point to the Avaya Aura® Presence Server. For more information, see Configuring Presence Publisher on page 22.
- For XMPP IM and Presence:
  - Add Presence Element in Element Manager. For more information, see Adding a presence element on page 28.
  - Add Presence Account to all subscribers that are XMPP IM and Presence users in the Subscriber Manager. For more information, see Creating a Presence account for a subscriber on page 29.

Migrating XMPP client

In Release 7.5, Communication Server 1000 supports only the one-X Communicator client. Therefore, all existing XMPP clients must switch to one-X Communicator clients.

Configure the PREA status on your existing XMPP clients from Allowed to Denied. This configuration change prevents sending duplicate call status changes to the Presence Server. For example, a call status change being sent using SIP Publish through the Presence Publisher and the other using XMPP.

For more information about this configuration, see LD 11 Configure client on page 68.

Chapter 8: Maintenance

This chapter provides information about CLI commands and logs for maintenance on the IM and Presence Services.

Navigation

Call Server CLI commands

Turn on the AML trace using LD 48.

The following is an example of an AML trace to help verify that the Call Server sends the USM message to the Presence Publisher application.

AML trace

--- Turn on AML trace

```
>48

LNK000

.enl msgo 32

ELAN32 O MTYP=1A USM  TN=096 0 00 26  TIME=07:12:36
ELAN32  IN 7D311A47 OUT 00000000 QSIZE 00000000
ELAN32  03 36 00 00 61 82 16 1A 00 00  00 00 37 02 61 82 36 02 85 29
ELAN32  3B 01 08 38 01 02 39 02 85 12  96 04 00 00 7E 58 F2 08 63 6F
ELAN32  72 65 73 69 70 6C 5F 07 01 06  14 0B 07 0C 24
```

--- Turn off AML trace

```
>48

LNK000
```

```
.dis msgo 32
```

Note:

In the preceding output, look for USM messages that are output to the Presence Publisher application.

For example:

38—Code for the status of the party:

01—The number of bytes that follow

02—Off-hook (04 is Active and 05 is USMDisc)

F2—code for PUID:

08—The number of characters.

63 6F 72 65 73 69 70 6C – coresipl

Presence Publisher Service CLI commands

The following are some useful Presence Integration Service CLI commands.

Presence Publisher Service application status commands

puaAmlShow

Use puaAmlShow to display the status of the AML link.

```
vxShell vtrk puaAmlShow
```

hAppBlk	TaskName	Tid	LinkState	NumRetry	LinkNum	Trace
0x9c5ef8	PUA	0xf300	UP	0	32	0
AML Link Timer:						
Not Active.						

puaShow

The puaShow commands displays the summary of the Presence Integration Service application. It shows the state of the Presence Integration Service application and the status of the AML link.

puaShow						

===== VTRK =====						
======== General ========						
PUA State = AppReady						

===== AML Info =====						
hAppBlk	TaskName	Tid	LinkState	NumRetry	LinkNum	Trace
0x9c5ef8	PUA	0xf300	UP	0	32	0
AML Link Timer:						
Not Active.						

puaConfigShow

Use the command puaonfigShow to display the configuration of the Presence Integration Service application.

puaConfigShow

===== VTRK =====

Service Domain : testbed1.com

Primary Presence Server : 47.11.113.209:5080:UDP

Secondary Presence Server : 0.0.0.0:0:UDP

Local SIP Port : 5075

Local TLS Port : 5076

Customer Number : 0

CDN Number : 2060

Presence Publisher Service application trace commands

puaAmlTrace

Use puaAMLTrace to run a Presence Integration Service application trace. The most practical level to set the trace is 5. This enables message printing and full decoding. To turn off AML trace, use level 0.

The logs are captured in /var/log/nortel/ss_common.log file.

```
vxShell vtrk puaAmlTrace 5
```

```
Set PUA AML message trace level: 5
value = 0x23 (35)
```

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: Message Type: USM (0x1a)

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: Application : TPS (0x16)

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0x37) = ThisPartyTN, Len 0x2, Data = [60 48]

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0x36) = ThisPartyDN, Len 0x2, Data = 3124 [31 24]

[05]Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0x3b) = ThisPartyDNType, Len 0x1, Data = Internal [08]

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0x38) = ThisPartyStatus, Len 0x1, Data = Disconnect [05]

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0x96) = CallID, Len 0x4, Data = [07 65 4e 02]

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0xf2) = UserId, Len 0xf, Data = 3124@NORTEL.COM [33 31 32 34 40 4e 4f 52 54 45 4c 2e 43 4f 4d]

Aug 28 14:20:38 mhou-cppm vtrk: (INFO) tPUA: IE (0x5f) = EnhancedTimeStamp, Len 0x7, Data = [1c 08 14 09 0e 14 2b]

sipNpmAppDebugSet

Set a global debug field for Presence Integration Service application. The “debugField” is a string name of the debug flag. This trace command is common to all SIPNPM based applications (SSG, SLG, PUA). For the Presence Integration Service application , the most useful one is sipMsgPrint.

For a list of all sipNpmAppDebugSet commands refer to, *Avaya SIP Line Fundamentals , NN43001-508*.

```
vxshell> vtrk sipNpmAppDebugSet tPUA sipMsgPrint 1
```

```
sipMsgPrint changed from 0 to 1
value = 0x0 (0)
```

sipNpmAppDataShow

Use sipNpmAppDataShow to print details of an SIPNPM-based application data.

```
vxshell> vtrk sipNpmAppDataShow tPUA 5
```

```
Application = tPUA,   tid = 0x8aa6a40,   Category = 0xf300
MsgQId      = 0xf3, MsgType = 0xf300, MsgQSize = 30000, MsgQFD=0x10
GlobalData Address=0xa0ba30, CallBackData Address=0xa116cc
tPUA -- StatusData Address = 0xa0639c
appInitialized   = yes
appStop          = no
stackInitialized = yes
proxyRegistered  = no
tPUA -- DebugData Address =  0xa063ac
rvLogFile    = 0
rvLogConsole = 0
sipMsgMonOut = 0
sipMsgMonIn  = 0
sipMsgPrint  = 1
sipCallTraceMsgDetailOn = 0
keepAliveMsgPrint       = 0
keepAliveSupport        = 1
prackSupport            = 0
enable415               = 0
test415                 = 0
gen415Allowed           = 0
infoSupport             = 0
mcdnUpdate              = 0
mcdnDebug               = 0
esn5Debug               = 0
loopbackSupport         = 0
maskLoopCode            = 0
optionSupport           = 0
renegotiationFlag       = 0
sdptDebug               = 0
sslConnectionDebug      = 0
regTrace                = 0
sniffPrint              = 0
snifferFilter           = ::0
tcpPersistency          = 1
SDescLevel              = 7
mediaTestLogLevel       = 7
eventLogLevel           = 7
forkingLogLevel         = 7
keepAliveLogLevel       = 7
tlsLogLevel             = 7
tlsRenegotiateLogLevel  = 7
traceID                 = -1
acpDebug                = 0
maltDebug               = 7
mediaTestMode           = 0
mediaTestNoCodecRetry   = 0
tPUA -- ConfigData Address = 0xa06658
Domain              = testbed1.com
Local Port          = 5075
RvSipStackCfg              = 0xa0b668
RvSdpStackCfg              = 0xa0b9ac
RvSipMidCfg                = 0xa0b9bc
tPUA -- StackData Address = 0xa0b9ec
RvSipStackHandle           = 0x8acd674
RvSipMsgMgrHandle          = 0x8acf4c4
RvSipCallLegMgrHandle      = 0x8ccae5c
RvSipTransportMgrHandle    = 0x8acf52c
```

```
RvSipTransmitterMgrHandle  = 0x8cc0aa4
RvSipSubsMgrHandle         = 0x8cf8974
RvSipMidMgrHandle          = 0x8cfdccc
RvSipTranscMgrHandle       = 0x8cc0d3c
HRPOOL                     = 0x8234044
RV_LOG_Handle              = 0x8acd888
RV Log file                = /var/log/nortel/RvSipPua.log
tPUA -- GlobalData Address = 0xa0ba30
tPUA -- CallBack Functions = 0xa116cc
appMsgHandler             = 0x6fe39b
cardEventHandler          = 0x6fe47f
configParaGet             = 0x701281
tlsConfigGet              = (nil)
appInit                   = 0x6fe34d
appShutdown               = 0x6fe37a
stackCallbackSet          = (nil)
sipUriCreate              = (nil)
sipSessionDel             = (nil)
callLegStateChgEv         = (nil)
callLegMsgToSendEv        = (nil)
transactionStateChangedEv = 0x6ffb88
NameToNumConvert          = (nil)
IsReInviteSendAllowed     = (nil)
callLegReferStateChgEv    = (nil)
callLegModifyStateChgEv   = (nil)
reInviteAnswerSent        = (nil)
audioCapHandler           = (nil)
sendAcsUiFwdSdp           = (nil)
earlyMediaUpdateSend      = (nil)
delayRetrieveHandler      = (nil)
value = 0x0 (0)
```

IM and Presence server commands

Start/Stop/Restart or check status of Presence server process

Start or restart the Presence server process:

```
/opt/Avaya/Presence/presence/bin/start.sh
```

Stop the Presence server process:

```
/opt/Avaya/Presence/presence/bin/stop.sh
```

Check the status of the Presence server process:

```
/opt/Avaya/Presence/presence/bin/presstatus
```

Unified Communication (Presence) server file location

The `/var/log/presence` is the file location for IM and Presence Services server files.

Presence server traces

SIP message traces

There are two ways to see SIP message traces on the presence server:

- Use Wireshark
- Get the SIP log file on Unified Communication (Presence) server (file location, check the server configuration page)

XMPP message traces

Use Wireshark to get XMPP message traces on the Unified Communication (Presence) server. Log files for one-X Communicator can be found at `C:\Documents and Settings\ \Application Data\Avaya\Avaya one-X Communicator\Log Files`.

For more information about enabling diagnostics for one-X Communicator, see One-X Communicator diagnostics on page 42.

SM traces

Use traceSM-x command if presence service does not receive the SIP publish message.

1. Log into the SM shell as root.
2. Enter the command **`traceSM -x`**.
3. Press **`s`** to start tracing.
4. Perform the testing.
5. Press **`s`** to stop tracing.

   You can find the traceSM.log in the directory `/var/log/Avaya/sm/ServiceHost`.

Diagnostic logs

This section provides the diagnostic logs for IM and Presence Service.

Signaling Server logs

You can view log messages in the `/var/log/nortel/ss_common.log` file.

Debug log:

To enable debug log, enter `syslogLevelSet vtrk tPUA 7`

To disable debug log, enter `syslogLevelSet vtrk tPUA 6`

AML Log:

To enable AML log, enter `vxShell vtrk puaAmlTrace 5`

To disable AML log, enter `vxShell vtrk puaAmlTrace 0`

SIP Message Log:

To enable SIP message log, enter `vxShell vtrk sipNpmAppDebugSet tPUA sipMsgPrint 1`

To disable SIP message log, enter `vxShell vtrk sipNpmAppDebugSet tPUA sipMsgPrint 0`

One-X Communicator diagnostics

1. Navigate to **Settings > General Settings > Advanced**.
2. Click **Diagnostic Logging**.
3. Select the **Enable Diagnostic Logging** check box.
4. Click the type of logging, and click **OK**.

Chapter 9: IM and Presence user information

Avaya Communication Server 1000 (Avaya CS 1000) IM and Presence Services provides presence information and IM capability for all Avaya CS 1000 users. A CS 1000 user can view presence information and exchange Instant Messages using the one-X Communicator CS 1000 Client.

For more information about the configuration of one-X Communicator client, see Avaya one-X Communicator CS 1000 client configuration on page 47.

Navigation

Presence Aggregation

Presence Aggregation is to ensure uniform presence regardless of the client being used.

Personal Agent

Use the Personal Agent (PA) application to change your password and to synchronize your passwords so that you use the same password for Presence and Instant Messaging, logging on to the one-X Communicator, and SIP Line phones.

Note:

Whether or not the password has been changed, you must synchronize the password at least once to ensure logon access to one-X Communicator and for IM and Presence to work properly.

The PA is a standalone application that is installed on the same server as Subscriber Manager (SubM) during the SubM deployment; however, UCM security does not apply. The Personal Agent application is accessed from your Web browser as a single page and no logon is required, as shown in the following figure.

Figure 3: Personal Agent

Changing your password for Presence and Instant Messaging

Change your Presence and Instant Messaging password.

Note:

The new password is subject to the restrictions as configured in Unified Communications Management (UCM) by the security administrator and these rules are displayed on the Personal Agent screen. The rules displayed and the details of the rules depend on the password configuration in UCM.

1. On your Web browser, enter the URL of the Personal Agent provided by your system administrator. For example, `http://<FQDN of UCM primary server>/pa`.

   The Presence and Instant Messaging page opens.
2. In the **Username** field, enter your user name.
3. In the **Current Password** field, enter your current password.
4. In the **New Password** field, enter the new password.

   Note:

   The new password must follow the rules displayed on the screen.
5. In the **Confirm Password** field, enter the new password again.
6. Click **Save**.

   Any messages relating to the success or failure of the password change appears below the page title. If the password is not accepted, check the password restrictions and try again.

Synchronizing your password

After the Presence and Instant Messaging password has been changed, synchronize the password with all the presence and telephony accounts belonging to the subscriber.

1. On the Personal Agent Web page, click **Synchronize Account Passwords**.
2. In the **Username** field, enter the user name.
3. In the **Password** field, enter the password.
4. Click **Show Accounts**.

   The accounts for the user appear at the bottom of the page.
5. Click **Synchronize Password**.

   Upon successful completion, the message Succeeded appears in the Status column.

Note:

Password synchronization fails for non-SIP Line phone accounts as the Unified Communications (UC) password is only used by SIP Lines.

Chapter 10: Avaya one-X Communicator CS 1000 client configuration

This chapter provides the procedures for configuring the Avaya one-X® Communicator Communication Server 1000 client for viewing presence information and exchange Instant Messaging (IM) with the Extensible Messaging and Presence Protocol (XMPP).

For more information about Avaya one-X® Communicator for Communication Server 1000, download the following documents from the Avaya Web site at www.avaya.com.

- *Overview and Planning for Avaya one-X® Communicator for CS 1000* (for administrator)
- *Administering Avaya one-X® Communicator for CS 1000* (for administrator)
- *Implementing Avaya one-X® Communicator for CS 1000* (for user)
- *Using Avaya one-X® Communicator for CS 1000* (for user)

Navigation

Configuring IM and Presence

Configure IM and Presence.

1. In the General Settings, in the left pane, click **IM and Presence**.

The Instant Message and Presence Service settings window appears in the right pane.

2. Select **Enable Instant Messaging and Presence** to enable the Instant Message and Presence Service settings.
3. In the **Server** field, type the IP address of the Presence Server.
4. Enter the presence SIP domain name.

   This entry should match with the value that is configured in "Domain Substituion - To" in /Home/Elements/Presence/Configuration web page of the System Manager.
5. In the **IM username** field, type the username as configured in Subscriber Manager.
6. In the **IM password** field, type the synchronized password for the subscriber.

Configuring Phones

Configure phones.

1. In the General Settings, in the left pane, click **Phone**.

   The Phone settings screen appears in the right pane.
2. In the **Login** field, type the phone extension number or the user name. This is the SIP User Name field in the SIP Line phone account configuration in Element Manager.
3. In the **Phone password** field, type the synchronized password for the subscriber.
4. In the **Domain** field, type the SIP domain name.
5. In the **SIP Line Gateway (SLG) node** field, type the IP address and port.

Active Directory configuration

This section provides the procedures to configure Active Directory (AD).

For example purposes, the procedures in this section use the following common configuration data.

Table 2: Common configuration example data

Active Directory IP address	100.20.52.3
AD domain	interop.com
Organization Unit	ps

Presence User ID (PUID) configured in Subscriber Manager. **Note:** There is a maximum of 16 PUIDs for each user.	1347
Presence domain	presence.interop.com

Creating an organization unit in Active Directory

Create an organization unit in AD.

1. From the Start menu, select Run, and type `dsa.msc`.

   The Active Directory Users and Computers window appears, as shown in the following figure.

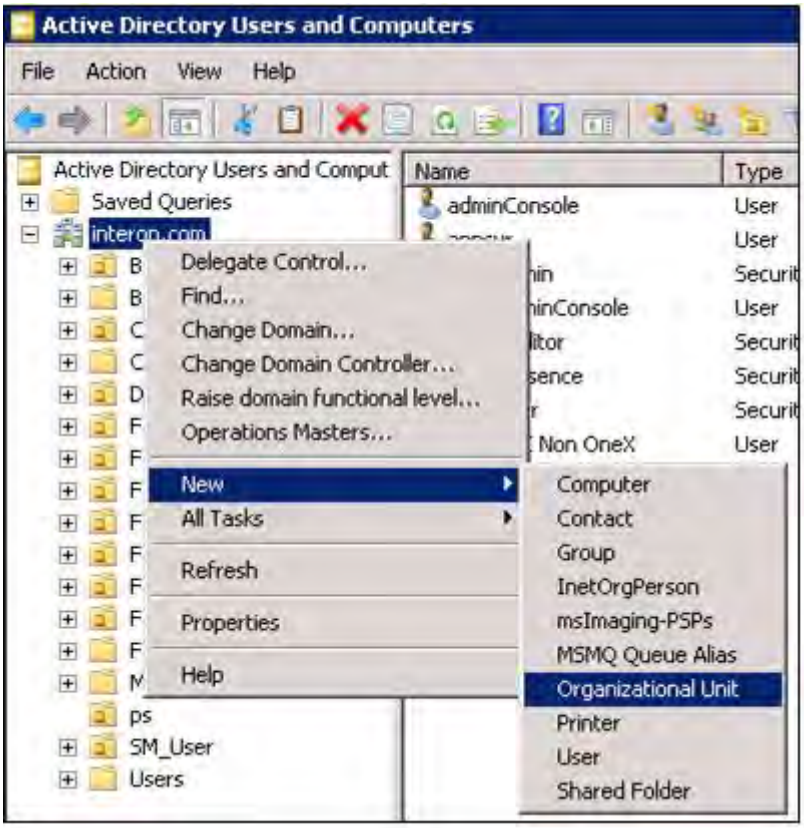


Figure 4: Active Directory Users and Computers

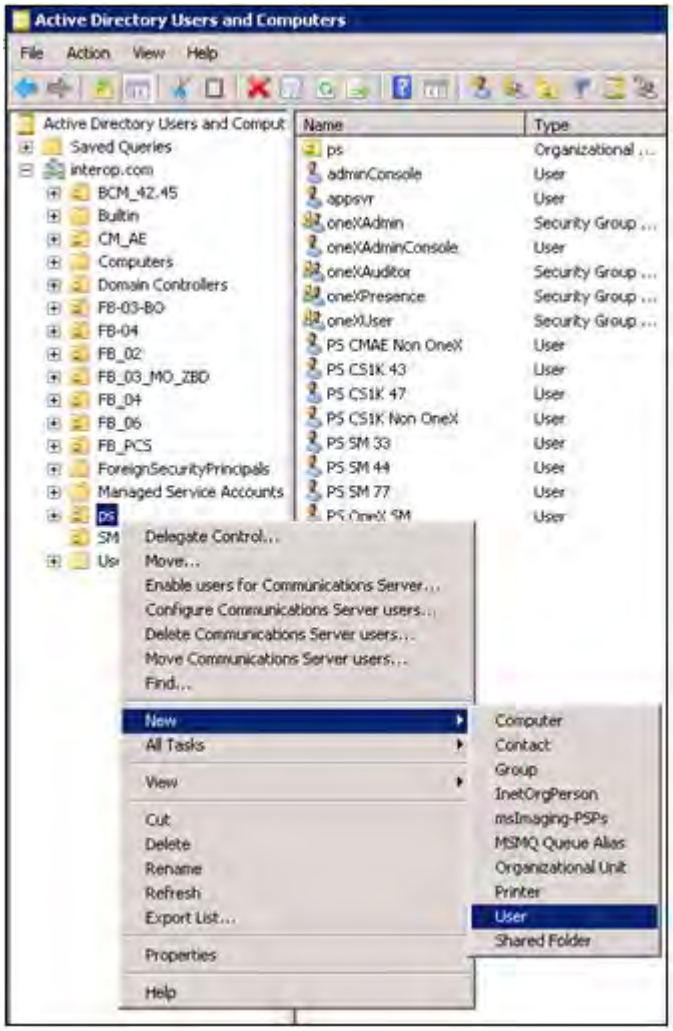
2. Right-click the folder where you want the organization unit to be created.
3. Click **New > Organizational Unit**.

The new organization unit appears in the left pane. In this example, the organization unit is ps.

Creating a user in Active Directory

Create a user in AD.

1. Right-click the organization unit you just created. For example, ps



2. Click **New > User**.

   The New Object — User window appears, as shown in the following figure.

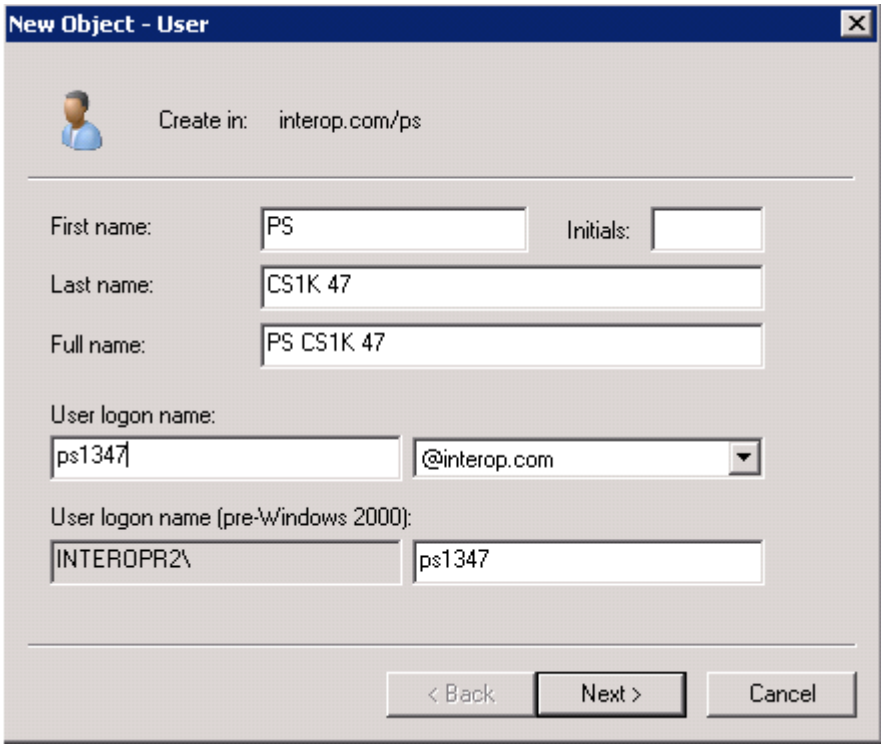


Figure 5: New Object — User

3. In the **First name** field, type the first name of the organization unit.
4. In the **Last name** field, type the last name of the organization unit.
5. In the **Full name** field, type the full name of the organization unit.
6. In the **User logon name** field, type the user logon name.
7. Click **Next**.
8. In the **Password** field, type a password.
9. In the **Confirm password** field, type the password again to confirm.
10. Select the options **User cannot change password** and **Password never expires**.
11. Click **Next**.
12. Click **Finish**.

Configuring a user in Active Directory

Configure the data for the user.

1. In the Active Directory Users and Computers page, right-click the name in the right pane, and select **Properties**. For example, PS CS1K 47.
2. Click the **General** tab.
3. Complete the following fields:
   - First name
   - Last name
   - Display name
   - Telephone number
   - E-mail
4. Click **OK**.

Client configuration for Avaya one-X Communicator

This section provides the procedures for configuring the Avaya one-X® Communicator client.

Enabling the public directory

Enable the public directory.

1. Log on to the Avaya one-x Communicator.

2. In the General Settings window, click **Desktop Integration** in the left pane.

   The desktop integration options appear in the right pane.

3. In **Name Look-Up**, select **Public Directory**.
4. Click **OK**.

Configuring public directory

Configure the public directory information.

1. In the General Settings window, click **Public Directory** in the left pane.

   Public Directory options appear in the right pane.

2. Complete the fields, and click **OK**.

Note:

You may be required to restart the one-X application.

Note:

The user portion of the email address or the phone number selected for the IM handle mapping is used for searching and creating IM handles for users in the Presence server. Therefore, the selection must match the IM username entered in the IM and Presence window. If the email address, “id@mycompany.com” is selected, then “id” must also be entered for the IM username. If the work number is selected, then the work number must be entered for the IM username.

Adding a contact

Add a contact to the one-X Communicator.

1. In the **Search** field, type the contact, and click the search icon.

   The name appears in the bottom pane.

2. Right-click the name you want to add the contact, and click **Add to Favorites**, as shown in the following figure.

The name is added to the favorite list, as shown in the following figure.

Note:

You may be required to log off and log on to one-X Communicator for the updated view.

TLS certificates for Avaya one-X Communicator

This section provides the procedures in the order of installation for installing certificates for the Avaya one-X® Communicator and registering to the SIP Line Gateway (SLG) using TLS.

Adding a UCM primary certificate authority

Add the UCM primary certificate authority on the same system where the Avaya one-X® Communicator is installed.

1. In System Manager, navigate to **Services > UCM Services**.
2. From the UCM navigation tree, click **Security > Certificates**.

3. Click the **Private Certificate Authority** tab.

   The private Certificate Authority window appears.

4. In the Private Certificate Authority Details section, click **Download** to download the certificate contents as a security certificate file to the PC.

   The File Download – Security Warning window appears.

5. Click **Save**.

   The Certificate Details window appears showing the details of the certificate.

6. Click **Ok**.

7. After the UCM certificate is saved to the Avaya one-X® client PC, open the certificate file and follow the instructions for installation to your Windows PC.

Adding an Avaya one-X Communicator root certificate authority to UCM

Add the Avaya one-X® Communicator root Certificate Authority (CA) to UCM. The one-X® Communicator Root Certificate Authority can be downloaded from the Avaya one-X® Communicator page at https://support.avaya.com.

1. In System Manager, navigate to **Services > UCM Services**.
2. From the UCM navigation tree, click **Security > Certificates**.
3. Click the **Certificate Endpoints** tab.

   The private Certificate Endpoints screen appears.

4. In the Certificate Endpoints section, click the option next to the SIP Line Gateway (SLG) node.
5. In the Certificate Authorities section, click **Add**.
6. Copy the one-X Communicator root CA contents and paste into the text area.
7. Click **Submit**.

Creating a certificate for SIP TLS

Create a certificate for SIP TLS.

1. In System Manager, navigate to **Services > UCM Services**.
2. From UCM navigation tree, click **Security > Certificates**.
3. Click **Certificate Endpoints** tab.

   The private Certificate Endpoints window appears.

4. In the Certificate Endpoints section, click the option next to the SIP Line Gateway (SLG) node.
5. Click **SIP TLS**.
6. Click **Create a new certificate, signed by local private Certificate Authority**, and click **Next**.
7. Type values for **Friendly name** and **Bit Length**, and click **Next**.

   For example:

   - Friendly name: Type a string that would be used to identify the certificate, for example, SIP TLS.
   - Bit Length: Type a value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.
8. Type the **Organization** and **Organization unit**, and click **Next**.

   For example:

   - Organization: Your company name.
   - Organization unit: A division within your company.
9. Type a value for **Common Name**. For example, type the FQDN of the server you are configuring. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.
10. In the **Subject Alt Name** field, click **Other**, and type `critical,DNS:` *domain name*, where the domain name is the domain name on the SIP Line Gateway.
11. Click **Next**.
12. Complete the Geographical information, and click **Next**.

    The Certificate Summary page appears.
13. Verify the information, and click **Commit** to generate a certificate in X.509 format.

    The Certificate Summary page shows the certificate information.
14. Click **Finished**.

    The status is changed to signed.
15. Restart the server.

Configuring Avaya one-X Communicator for Best Effort Cap negotiation

Configure the Avaya one-X® Communicator for Best Effort negotiation.

1. In the General Settings, click **Advanced > SRTP Settings**.
2. Select **Enable SRTP** to enable SRTP on one-X Communicator.
3. Configure Cipher1 or Cipher2 to AES_CM_128_HMAC_SHA1_80.
4. Configure the mapping table for one-X Communicator capability and Class of Service for UEXT.

   For example,

   - SRTP enabled <-> MSBT
   - SRTP not enabled <-> MSNV

Feature Interactions

Sigma telephone:

Sigma telephones cannot make outgoing calls if the phone is configured with Best Effort Cap negotiation and TN is configured with MSBT Class of Service. Attempts to make an outgoing call result in the destination phone ringing and the originator receiving an overflow tone.

Best Effort negotiation implementation:

If Avaya one-X® Communicator for Best Effort negotiation is implemented through an m-line (using tcap and pcfg attributes) and MSBT Class of Service is configured, the Avaya one-X® Communicator cannot make outgoing calls, the destination phone does not ring, and the originator does not receive the overflow tone.

Chapter 11: Troubleshooting

This section provides information to assist in troubleshooting problems related to Presence Services or the one-X Communicator client for Communication Server 1000.

Navigation

Presence Server—local database

Verify that the user data is successfully replicated to the Presence Server. For local database, enter the following command in the Presence Server shell:

```
psql -U postgres -d presence -c "select* from csuser"
```

For example, if the user name is John Smith, the display is:

```
374 | 2011-01-06 16:27:42.339 |0 | FMVqzkyG5PNIjssq3wjcWw== |
728ab064-82fc-4873-ac3c-db4c645446fc | f| t| johnsmith@avaya.com |||
86|
```

Presence Server—XCP database

Verify that the user data is successfully replicated to the Presence Server. For the XCP database, enter the following command in the Presence Server shell:

```
psql -U postgres -d xcp -c "select * from users"
```

For example, if the user name is John Smith, the display is:

```
10343 | johnsmith@pspit.avaya.com | -| F| 2011-01-06 16:23:35 |
2011-01-06 16:23:35 | 0 | 2011-01-06 |
```

AML link is not up

Check if an ELAN link is configured for LD 22.

Example output of LD 22.

```
>LD 22
```

```
PT2000
MARP NOT ACTIVATED
```

Table 3: LD 22

Prompt	Response
REQ	PRT
TYPE	ADAN ELAN

```
ADAN     ELAN 32
CTYP ELAN
DES  elan_slg
N1   512
ADAN     ELAN 33
CTYP ELAN
DES  SIPL
N1   512
ADAN     ELAN 34
CTYP ELAN
DES  AMLCD
N1   512
```

Example output

```
>LD 23
```

```
ACD000
MEM AVAIL: (U/P): 48592002    USED U P: 2864309 173766    TOT: 51630077
DISK SPACE NEEDED: 254 KBYTES
ACD DNS               AVAIL: 23991    USED:     9    TOT: 24000
```

Table 4: LD 23

Prompt	Response
REQ	PRT

Prompt	Response
TYPE	CDN
CUST	0
CDN	<CR> Carriage Return

```
TYPE CDN
CUST 0
CDN  2070
FRRT
SRRT
FROA NO
UUI  NO
MURT
CDSQ NO
NAME NO
CMB  NO
CEIL 2047
OVFL NO
TDNS NO
RPRT YES
AACQ YES
ASID 17
SFNB 16  17  18  19  21  22  23
USFB
CALB 0  1  2  3  4  5  6  7  8  9  10  11  12
CNTL YES
VSID
HSID
CWTH 1
BYTH 0
OVTH 2047
STIO
TSFT 20
```

Does the CDN/PSDN configured on CS match the one in the Presence Publisher configuration? : Check Presence Publisher Configuration page in Element Manager.

Presence is not updated when a telephone makes a call

- Is CLS PREA configured for the set? : Print set configuration in LD 10 / LD 11, or in Element Manager.
- Is PSDN properly configured for the set? : Print set configuration in LD 10 / LD 11, or in Element Manager.
- Is PUID configured properly for the set? : Print set configuration in LD 10 / LD 11, or in Element Manager.
- Are USM messages sent from CS? : Enable AML traces in LD 48. See Call Server CLI commands on page 35.
- Are USM messages received on the Presence Publisher Server? : Run puaAmlTrace 5. See Presence Publisher Service application trace commands on page 38.

- Are PUBLISH messages sent from the Presence Publisher Server? : Run sipNpmAppDebugSet tPUA sipMsgPrint 1, or pcap start/stop, or wireshark on the Presence Publisher Server.
- Are PUBLISH messages received on the IM and Presence server? Run wireshark on the IM & Presence Services server.

Presence Publisher not operational

Invoke the following command in the Signaling Server in which the Presence Publisher (PP) resides:

puaShow

Example display for an operational PP:

```
=== VTRK ===
===== General    ======
PUA State             = AppReady
Server Type           = Avaya Aura PS
===== AML Info   ======
hAppBlk     TaskName         Tid     LinkState      NumRetry  LinkNum  Trace
0xb921c0    PUA              0xf300  Up             0         32       0
```

Presence publisher configuration not displayed

Invoke the following command in the to display the presence publisher configuration:

puaConfigShow

For example:

```
=== VTRK ===
Service Domain  : pspit.ca.nortel.com
Primary Outbound Server : 47.11.112.242:5061:TLS
Secondary Outbound Server : 47.11.253.179:15061:TLS
Local SIP Port  : 5080
Local TLS Port  : 15061
Presence Server : 47.11.253.179:15061:TLS
Customer Number : 0
CDN Number      : 5280
```

TLS status

Check the `/var/log/nortel/ss_common.log` file to see if there is a **TLS up** message. If not, check TLS configuration and the network status.

For example:

```
May 26 17:43:34 fb-04-ldr vtrk: (INFO) tPUA: sipNpmTlsCheckSANandCN:
Remote IP=100.20.25.130 from Session Manager, grant
```

CDN or PSDN ASID VALUE is incorrect

On the Call Server, load overlay 23 and print the CDN data.

```
Ld 23
REQ  Prt
TYPE  Cdn
CUST  <customer #>
CDN <cdn #>
```

For example:

```
TYPE CDN
CUST 0
CDN  5280
FRRT
SRRT
FROA NO
UUI  NO
MURT
CDSQ YES
DFDN 8990
NAME NO
CMB  NO
CEIL 2047
CLRO NO
OVFL NO
TDNS NO
AACQ YES
ASID 32     □----------------------This number must be the same as the ELAN number
for thePP
SFNB
USFB
CALB 0  1  2  3  4  5  6  7  8  9  10  11
CNTL YES
VSID
HSID
CWTH 1
BYTH 0
OVTH 2047
```

If the ASID number is not the same as the ELAN number for the PP, configure the same CDN again. Then, type **`appstart vtrk restart`** on the Signaling Server where the PP resides. To find the ELAN number for the PP, enter the following:

```
>ld 48
LNK000
stat elan
```

Example display:

```
SERVER TASK:  DISABLED
ELAN #: 032
 APPL_IP_ID: 47 .11 .71 .72 : 0000F300 LYR7: ACTIVE  EMPTY   APPL ACTIVE
ELAN #: 033
```

```
 APPL_IP_ID: 47 .11 .71 .72 : 0000FB00 LYR7: ACTIVE  EMPTY   APPL ACTIVE
ELAN #: 034
 APPL_IP_ID: 47 .11 .71 .72 : 0000F800 LYR7: ACTIVE  EMPTY   APPL ACTIVE
ELAN #: 035
 APPL_IP_ID: 47 .11 .71 .72 : 0000F700 LYR7: ACTIVE  EMPTY   APPL ACTIVE
```

Get the ELAN number that has type 0000F300 (In this example, it is 32).

one-X Communicator Fails to Register to CS1000

- Make sure that the root certificate authority for the one-X Communicator has been installed in the UCM.
- Make sure that the SIP TLS certificate is re-created if the domain name for the SIP Line gateway is changed.
- Make sure that password synchronization has been done and the UC password is used instead of the SCPW.

IM and Presence does not work for the one-X Communicator

- Make sure that the domain name entered on the IM and Presence page of the one-X Communicator is the domain name for the PS.

Appendix A: Overlay commands

Navigation

Overlay commands—LD 17

The following Overlay commands can be used to enable Presence service on the Call Server.

Table 5: LD 17 Configure ELAN AML link

Prompt	Response	Description
REQ	CHG	Change ADAN
TYPE	ADAN	
ADAN	New ELAN <ELAN number>	New AML ELAN link. The link number should be greater than or equal to 32
CTYP	ELAN	

Every AML over ELAN link configured on the Avaya Communication Server 1000 (Avaya CS 1000) system requires a Value Added Server (VAS) ID for the AML messages to be sent. Use the following overlay commands to associate a Value Added Server (VAS) with AML over ELAN.

Table 6: LD 17 Configure VAS ID for AML link

Prompt	Response	Description
REQ	CHG	Change ADAN
TYPE	VAS	
VAS	New	New VAS
VSID	vasID	The VAS ID number

Prompt	Response	Description
ELAN	<ELAN number>	ELAN number, should match the one configured in previous step.

Overlay commands—LD 11 and LD 23

Table 7: LD 23 Configure ACD DN

Prompt	Response	Description
REQ	New	New ACD
TYPE	ACD	
CUST	custNum	Customer number
ACDN	Xxxx	An ACD DN to be used when configuring CDN
MAXP	1 or greater	Maximum position for ACD DN queue

Table 8: LD 23 Configure CDN

Prompt	Response	Description
REQ	New	New CDN
TYPE	CDN	
CUST	custNum	Customer number
CDN	Xxxx	A CDN number to be used by Presence Publisher **Note:** This CDN is used as the PSDN for each subscriber.
CDSQ	Yes	Configure to yes so the presence activity sends to the Presence Publisher.
DFDN	Xxxx	ACD DN configured in the table Table 7: LD 23 Configure ACD DN on page 68.

LD 11 Configure client

The telephony account can be provisioned in the call server overlay.

Table 9: LD 11 Configure client

Prompt	Response	Description
REQ	New/Chg	New TN or change an existing TN
TYPE	<TN Type>	
CUST	custNum	Customer number
CLS	PREA (PRED)	New CLS PREA is used to enable presence service for phones that do not support Extensible Messaging and Presence Protocol (XMPP). The one-X Communicator feature does not require PREA as it supports XMPP. The default value is PRED
PSDN	CDN number	Enter the CDN number.
PUID	<>	The Presence User ID (PUID) is the user name for the subscriber to which the telephony account belongs. **Note:** Configure the Unified Communications (UC) password using Subscriber Manager and perform password synchronization. You cannot use the CLI. There is a maximum of 16 PUIDs for each user.
UPWD	<>	UC password is used for SIP Line login. **Note:** Configure the PUID using Subscriber Manager and from the Phones section in Element Manager. You cannot use the CLI.