Implementing Avaya one-X® Portal

November 2009

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 AVAYAAFFILIATE 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”).

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License type(s)

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

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

Avaya, the Avaya logo, Avaya one-X® Portal, Communication Manager, Application Enablement Services, Modular Messaging, and Conferencing are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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: Avaya one-X Portal overview

Avaya one-X Portal overview

Avaya one-X® Portal features

Avaya one-X is the first of a new series of next generation Unified Messaging applications that brings Unified Communications to your desktop in a single tool. Avaya one-X® Portal is a browser based interface to Avaya telephony, messaging, mobility, conferencing, and presence services provided by Avaya Aura®Communication Manager, Avaya Modular Messaging, Avaya Conferencing, and Avaya Aura®Presence Services.

Avaya one-X® Portal does not require the installation of any application software on your desktop to deliver its basic functionality.

Avaya one-X® Portal provides the following features:

- Single web client interface
- Communication Manager telephony features
- Only supported telephone types can access Communication Manager features
- Telephony control with supported versions of Communication Manager installed in your enterprise
- Customizable call logs
- Integration with Avaya Modular Messaging to view and play voice messages
- Integration with Conferencing to view and control live conferences
- Integration with Presence Services to receive access requests and publish presence state information.
- Integration with Extension to Cellular for Follow-Me applications
- Integration with Microsoft Active Directory, IBM Domino Server, Novell eDirectory, or Sun One Directory Server for enterprise user information

Note:

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Avaya one-X® Portal Release 5.2 supports, refer to the *Avaya one-*

X Portal® Release 5.2 GA Release Readme available on the Avaya Support Web site, http://www.avaya.com/support.

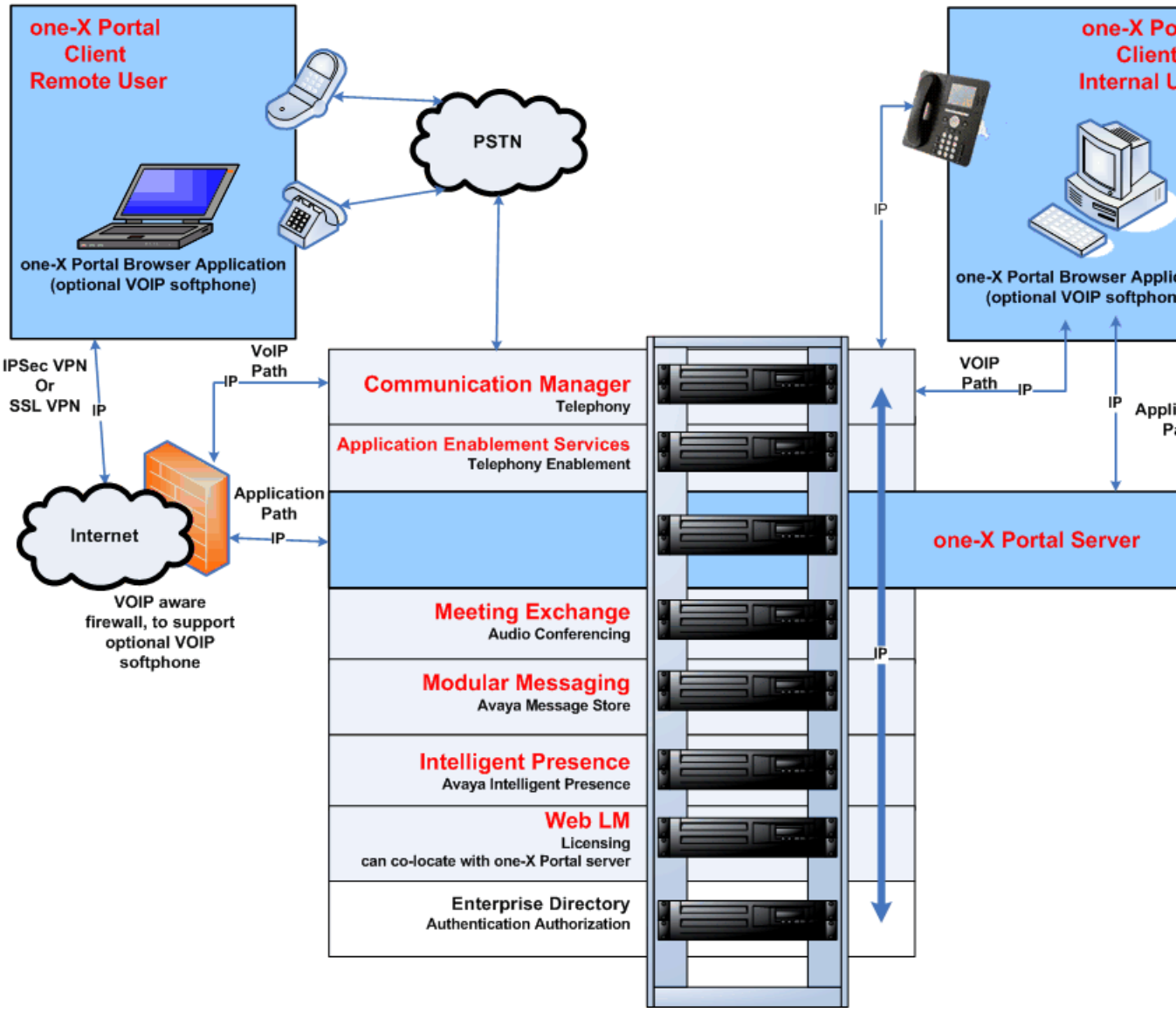
Avaya one-X® Portal system diagram

Avaya one-X® Portal is comprised of external servers and core components.

External servers deliver telephony, messaging, mobility, conferencing, and presence services from the Communication Manager switch, Modular Messaging servers, Conferencing servers, and the Presence Services.

Core components integrate with Directory Services, the WebLM server, and an internal database to support system users. Core components also provide system level functions, such as scheduling database backups or server synchronizations.

The following diagram describes the Avaya one-X® Portal system:



Prerequisites for Avaya one-X® Portal

Avaya one-X® Portal is a software only solution. On the Avaya one-X® Portal DVD, Avaya provides the software for the following components:

- Avaya one-X® Portal server
- Avaya WebLM
- Internal Avaya one-X® Portal database
- Avaya one-X® Portal applications

Avaya one-X® Portal does not include the server or other hardware, or any of the required software for those servers. You must purchase the hardware and required software separately.

Supported languages in Avaya one-X® Portal

Avaya one-X® Portal supports the following languages for this release. These languages are available once the language pack is installed.

- English
- Chinese, Simplified
- Dutch
- French, International
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish, International

Supported telephone types in Avaya one-X® Portal

Avaya one-X® Portal supports the following telephone types.

- 2402, 2410, and 2420
- 4601, 4602, 4602, 4606, 4610, 4612, 4620, 4625, 4624, and 4630
- 6402D, 6408D, 6408D+, 6416D+, and 6424D+
- SPICE 96xx
- 1600 series phone aliased as 4600

Note:
Analog telephones are not supported.

Security features of Avaya one-X® Portal

Avaya one-X® Portal provides you with options for a secure implementation.

Connections through VPN or internal LAN

Avaya one-X® Portal supports connection only through internal LAN or VPN.

User authentication through the enterprise directory

Avaya one-X® Portal integrates with the existing Enterprise Directory. Avaya one-X® Portal uses the Microsoft Active Directory, IBM Domino Server, Novell eDirectory, or Sun ONE Directory Server user records for authentication and authorization.

Access to Avaya one-X® Portal through secure server connections

Avaya one-X® Portal supports access through https:// protocol. Install a secure server certificate obtained from certifying authority such as VeriSign, Thawte, or GTE CyberTrust. Users can then confidently connect to Avaya one-X® Portal.

Connections to integrated components through secure ports

You can configure secure ports for integrated components, including:

- Enterprise directory application
- Web License Manager
- Modular Messaging

Encryption implemented through the Administration Command Line Client

For information on how to implement the following encryption, see the online help provided with the Administration application.

- Encryption for sensitive information in the Avaya one-X® Portal database.
- Encryption for bulk user import.
- Encryption for bulk user export.

Related topics:

Additional security information on page 15

Additional security information

Additional security information and documentation about all Avaya products, including Avaya one-X® Portal and the Avaya components that integrate with Avaya one-X® Portal are available at the Avaya Security Advisories Web site. For example, you can find information about the following:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification

- Security advisories for Avaya products
- Software patches for security issues
- Reporting a security vulnerability
- Automatic e-mail notifications of security advisories

You can also find additional information about security practices at the National Security Agency Security Configuration Guides Web site.

Capacities and performance of Avaya one-X® Portal

Factors affecting performance

Several factors can affect the capacities and performance of Avaya one-X® Portal, including the following factors:

- Size of the machine that hosts the Avaya one-X® Portal software
- Number of concurrently active users
- Amount of data elements that each user maintains.

For example, if a user imports more than 150 personal contacts into one-X Portal, application performance can be significantly slowed.

Capacities

The one-X Portal server supports up to 1500 concurrent user sessions. The services used in AES control the number of Station Control sessions. There are two AES services used by one-X Portal.

AES Service	Current Reported Limit
CMAPI (DMCC)	4000 Station Control sessions
TSAPI	20,000 Station Control sessions

CMAPI

The one-X Portal uses CMAPI service for the following operations:

1. Authentication of user while logon: It sets up a temporary CMAPI Station Control session and releases it once the password is authenticated.
2. When using the Other Phone mode: The CMAPI Station Control session is necessary to keep the remote registration active. While using Other Phone mode to log on, the user does not use the temporary CMAPI Station Control session as described in point 1.
3. To control Mobility Extension banks: One CMAPI Station Control session is used for every station controlled in the Mobility Extension bank. This number is usually small (2 to 10 stations).

TSAPI

The one-X Portal uses TSAPI service for the following operations:

- To control every telephony resource it is associated with, including these modes:
  - This Computer
  - Other Phone
  - Desk Phone
- To continuously monitor station while doing continuous call monitoring.
- To monitor every station in the Mobility Extension bank.

CMAPI and TSAPI phone control sessions

The CMAPI and TSAPI phone control sessions for various one-X Portal login modes are shown in this table.

one-X Portal Login Modes	CMAPI Phone Control Sessions (DMCC)	TSAPI Phone Control Session
Desk Phone	Temporary (less than 5 seconds)	On while the station is monitored by one-X Portal (including continuous call monitor)
This Computer	No session (Authentication is done by the VoIP component inside the user's browser)	On while the station is monitored by one-X Portal (including continuous call monitor)
Other Phone	Session active while the user is logged on using this mode	On while the station is monitored by one-X Portal (including continuous call monitor)

The following figures are concluded from the above table:

- Total number of stations that can be monitored: 10,000.
- Total number of users that can login on to Other Phone mode: 1500
- Total number of users that can be provisioned: 3000

Note:

A few CMAPI (DMCC) sessions are left for the authentication and Mobility Extension bank stations.

Server performance for 1000 concurrent user sessions

Avaya tested the performance of Avaya one-X® Portal with 1000 concurrent sessions. For this scenario, the following minimum hardware is recommended for the Avaya one-X® Portal server:

- CPU: Two quad-core processors, 1.86 Ghz or better each
- Memory: 6 GB RAM

The following table provides the highlights of the performance test for 1000 users.

Test parameter	Value used in performance test
Number of concurrent user sessions.	1000
Number of Avaya one-X® Portal servers	1
Use case assumption for Avaya one-X® Portal application	1 user session
Use case assumption for Avaya one-X® Portal Extensions	1 user session
Transaction types	Concurrent telephony, messaging and conferencing activities for all users.

Server performance for 1500 concurrent user sessions

Avaya tested the performance of Avaya one-X® Portal with 1500 concurrent sessions. For this scenario, the following minimum hardware is recommended for the Avaya one-X® Portal server:

- CPU: Two quad-core processors, 1.86 Ghz or better each
- Memory: 8 GB RAM

The following table provides the highlights of the performance test for 1500 users.

Test parameter	Value used in performance test
Number of concurrent user sessions.	1500
Number of Avaya one-X® Portal servers	1
Use case assumption for Avaya one-X® Portal application	1 user session
Use case assumption for Avaya one-X® Portal Extensions	1 user session
Transaction types	Concurrent telephony, messaging and conferencing activities for all users.

Interactions between one-X Portal and other applications

Software interactions with Avaya IP softphones

When using Communication Manager Release 5.2.1 or later, one-X Portal can run with Avaya IP Softphone if you log in to one-X Portal using shared control mode. Otherwise, only one Avaya one-X® Communicator application can control your business telephone extension. You

cannot use one-X Portal at the same time as you use an Avaya IP Softphone application to handle calls to your extension.

You can install the following applications on the same computer as one-X Portal, but you cannot use them simultaneously.

- Avaya IP Softphone
- Avaya one-X™ Desktop Edition
- Avaya IP Agent
- Avaya one-X® Communicator

Software interactions with Avaya one-X® Mobile

one-X Portal and Avaya one-X® Mobile work in synchronization even when you log in simultaneously with the same extension configured on Communication Manager.

Note:

The EC500 feature does not work when you use Avaya one-X® Mobile. Therefore, the administrator should disable this feature on Communication Manager.

Software interactions with Conferencing

If you start bridge conferences in one-X Portal, Avaya strongly recommends that you do not use other Conferencing client applications to control the conference or the participants. For example, if you mute the conference in a Conferencing application, you cannot unmute the conference in one-X Portal.

You can use a Conferencing application to record the bridge conference, even if you control the conference and participants in Avaya one-X® Portal.

Software interactions with Modular Messaging

If you use one-X Portal to read, reply to, and create messages, Avaya strongly recommends that you do not use the Web Client for Modular Messaging. For example, if you listen to or delete a message in one application, the change may not immediately display in the other application.

Limitations on support in one-X Portal and one-X Portal Extensions

Consider these support limitations when you determine which software to install for one-X Portal users.

Avaya one-X Portal Extensions on Windows only

Avaya one-X Portal Extensions can be installed on Windows operating systems only. Avaya one-X Portal Extensions are not supported on Mac operating systems.

VOIP support on Windows and Mac

Avaya one-X Portal supports VOIP for users with Windows computers with Internet Explorer and for users with Mac with Safari.

Avaya one-X Portal Message Recorder

Avaya one-X Portal Message Recorder is only supported on Windows using Internet Explorer.

Supporting software for one-X Portal on Windows

Avaya one-X® Portal includes some additional applications that you can use on your Windows computer. Unlike Avaya one-X® Portal, you can install these applications on your Windows computer.

If your company does not preinstall the Avaya one-X Portal Extensions and the Avaya Voice Player applications, you can download and install them from the **Other Settings** dialog box in one-X Portal.

Installation of Phone Interface and Message Recorder depends on the security setup of your browser. Depending on the security setup, the browser either installs these applications automatically or does not install them at all, or Avaya one-X® Portal prompts you to allow the browser to install the application.

Note:

If you use Avaya one-X® Portal on Citrix, do not install any supporting Windows applications on your computer, such as the Phone Interface and Message Recorder. If you install these applications, you may not be able to play your messages in Avaya one-X® Portal.

Avaya one-X Portal Extensions

Avaya one-X Portal Extensions complement and extend the features and functionality of one-X Portal. For example, you can use the one-X Portal Extensions to import your personal contacts and include bridge conference information when you schedule conference calls.

The extended features provided by the one-X Portal Extensions include:

- Dial Bar
- Click-2-Dial
- Click-2-Conference
- Click-2-Join

Phone Interface

The Phone Interface is the component that provides the VoIP functionality, which you can use to make and receive telephone calls on a Windows-based computer.

Message Recorder

The Message Recorder is the application that Avaya one-X® Portal uses when you record messages in Avaya one-X® Portal from a Windows computer.

Avaya Voice Player

Use the Voice Player to record audio messages outside Avaya one-X® Portal and upload those messages to Avaya one-X® Portal. For example if you gain access to Avaya one-X® Portal through Firefox, use the Voice Player to record your voice messages.

Supporting software for Avaya one-X® Portal on the Mac

Avaya one-X® Portal works on the Mac, and does not need any extension for direct installation on the Mac. For Voice Mail playback, Avaya one-X® Portal uses the application in the browser associated with the Media files. For most of the OCX systems, this application is the QuickTime plug-in.

Unified Communication VoIP Applet

The Mac supports VoIP using a VoIP applet that is downloaded to the browser when you log in to the system. The Mac caches this applet while the Safari browser is running, but after the browser is closed, the applet does not stay on the desktop.

The Applet is signed by Avaya, using Verisign as the certificate authority. When you load the applet, Safari confirms whether you trust the applet to gain access to the system, and displays the applet name, the Avaya certificate, and the related Verisign certificate. Trusting the applet is necessary for the VoIP functionality to work.

Terminology used in Avaya one-X® Portal

Term used in Avaya one-X® Portal	Term used in some related applications
Desk phone	Share Control
Other phone	Telecommuter
This computer	VoIP Voice over IP Road Warrior
Also Ring	Extension to Cellular
Forward to	Call Forwarding
Do Not Disturb	Send All Calls
Extension	Station

Chapter 2: Planning a one-X Portal deployment

Avaya one-X® Portal Implementation Workbook

The *Avaya one-X® Portal Implementation Workbook* provides the implementation checklists and worksheets from *Implementing Avaya one-X® Portal* in RTF format.

Note:

Avaya one-X® Portal is not customer installable. Only Avaya technicians or Avaya-certified business partners are authorized to perform the installation of Avaya one-X® Portal. For more information, please contact Avaya Support.

Before you install Avaya one-X® Portal

- If necessary, distribute the appropriate checklists and worksheets to the administrators responsible for the components.
- Verify that your network infrastructure fulfills the hardware and software infrastructure prerequisites.
- Complete the infrastructure and installation worksheets.

Port requirements for one-X Portal

Server to server ports

Server	Protocol	Default ports		Configurable	Comments
		External Server	One-X Portal		
Modular Messaging	SMTP	25	25	1024–65000	
	SMTP/SSL	465	465	1024–65000	
	IMAP4/SSL	993	993	1024–65000	
	LDAP	389	389	No	MM to LDAP
Conferencing	TCP	20002	20002	No	Conferencing does not support NAT.
	TCP	5040 with auto-increment	5040	Fixed range	
	UDP	5020 with auto-increment	5020	Fixed range	
Presence	variable	5070	Yes 1024-65000		
	variable	5060			
	variable	7286			
WebLM	HTTPS	8443	8443	Remote WebLM: Yes Local WebLM: No	Whether this port is configurable depends upon the location of the WebLM.
Enterprise Directory	LDAP	389	389	1-65535	
	LDAPS	636	636	1-65535	
AE Services	TCP for TSAPI	450	450	No	
	TCP for TSAPI	1050-1065	1050	Yes	
	DMCC/SSL	4721/4722	4721	Yes	By default, this port is disabled. You must enable this port manually.

AE Services to Communication Manager ports

Protocol	AE Services	Communication Manager
TSAPI	Variable	Fixed at 8765
H.323/RAS	Configurable in range 7000-8100	Fixed at 1719
H.323/CCMS	Configurable in range 3000-4100	Fixed at 1720

Avaya one-X® Portal and administration applications to server ports

Application	Protocol	Default port	Configurable
Avaya one-X Portal	HTTP and HTTPS	80 and 9080 and 9443 (for HTTP) or 443 and 9443 (for HTTPS)	No
Avaya one-X Portal Extensions	HTTP and HTTPS	80 and 9080 and 9443 (for HTTP) or 443 and 9443 (for HTTPS)	No
Administration application	HTTP and HTTPS	80 and 9080 and 9443 (for HTTP) or 443 and 9443 (for HTTPS)	No
Administration application Command Line Interface	SOAP	8880	No

Avaya one-X® Portal VOIP client to server ports

Application	Protocol	VOIP client initiating port	Communication Manager responding port	Configurable
ActiveX VOIP desktop application to Communication Manager	H.323/RAS/TCP	2048	1719	Fixed
	H.323/CCMS/ TCP	2049	1720	Fixed
	RTP/UDP	2048-5000	2048-63535	Negotiable
	RTCP/UDP	one higher than the correspondin	one higher than the corresponding RTP session	No

Application	Protocol	VOIP client initiating port	Communication Manager responding port	Configurable
		g RTP session		

SNMP ports

Application	Protocol	Default port	Configurable
SNMP trap daemon	UDP	162	Yes

Required software for one-X Portal components

Supported versions of third-party software

Avaya supports use of the documented software versions with the current release of this product. These software versions are the minimum versions required by Avaya.

This release does not support operating systems, databases, Web servers, switches, or other software platforms that are not documented here, unless stated otherwise in a Product Support Notice.

Avaya will support subsequent updates and service packs that are released to provide corrections to a bug, defect, or problem for the documented software versions, so long as those updates and service packs:

- Are guaranteed by the manufacturer to be backwards compatible with the supported version.
- Do not include changes to core functionality or new features.

Avaya recommends that you test all updates and service packs subsequent to the supported versions in a development environment before applying them to a production environment.

Required software for the one-X Portal server

Note:

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Avaya one-X® Portal Release 5.2 supports, refer to the *Avaya one-*

X Portal® Release 5.2 GA Release Readme available on the Avaya Support Web site, http://www.avaya.com/support.

Software	Supported versions	Location
Operating system	Red Hat Enterprise Linux 5 (32 bit)	Avaya one-X Portal server machine
Web browser	Mozilla Firefox 2 Mozilla Firefox 3	Avaya one-X Portal server machine Computer used by one-X Portal administrator.

Required software for integrating servers with one-X Portal

Requirement	Supported versions	Notes
Licensing application	Avaya Web License Manager 4.4 and 4.5	Optional. You can use the Web License Manager installed with one-X Portal. **Important:** Application Enablement Services requires a dedicated WebLM. Do not install the Avaya one-X® Portal license on the WebLM used by Application Enablement Services.
Telephony switch	Communication Manager 5.2.1	
Messaging application	Avaya Modular Messaging 4.0 and 5.2	
CTI application	Application Enablement Services 4.2.2 and 5.2	Uses DMCC and TSAPI connections through Avaya Aura®Application Enablement Services.
Conferencing application	Avaya Conferencing 4.1 and 5.2	If the Telephone service is not installed at the same time as the Bridge Conference service, one-X Portal users must initiate all bridge conferences from their telephones.
Presence application	Avaya Intelligent Presence Service 1.0	
Enterprise Authentication	• Microsoft Active Directory 2003, Windows Server 2008	

Requirement	Supported versions	Notes
	Active Directory Domain Services • IBM Domino Server 7.5 • Novell eDirectory 8.8 SP2 • SUN ONE Directory Server 5.2 and 6.3	

Related topics:

Location of the Avaya Web License Manager on page 36

Supported browsers for the one-X Portal application and the Administration application

Web browser	Windows XP	Windows Vista	Apple OS X	Red Hat Enterprise Linux Desktop
Mozilla Firefox 2	Yes	Yes	Yes	Yes
Mozilla Firefox 3	Yes	Yes	Yes	Yes
Microsoft Internet Explorer 6.0	Yes	No	No	No
Microsoft Internet Explorer 7.0	Yes	Yes	No	No
Microsoft Internet Explorer 8.0	Yes	Yes	No	No
Apple Safari 3.1	No	No	Yes	No
Apple Safari 3.2	No	No	Yes	No
Apple Safari 4.0	No	No	Yes	No

Required software for the Administration application

The Administration application resides on the same machine as the one-X Portal server. No additional software is required for the Administration application.

Administrators can access the Administration application through a supported Web browser from any machine with one of the following operating systems:

- Microsoft Windows XP SP2
- Microsoft Windows Vista 32 and 64 bit
- Apple OS X V10.5
- Red Hat Enterprise Linux 5

Required software for one-X Portal application and one-X Portal Extensions

Software	Windows XP	Windows Vista	Apple OS X	Red Hat Enterprise Linux Desktop
Operating system	Microsoft Windows XP SP2 Microsoft Windows 7	Microsoft Windows Vista 32 and 64 bit	Apple OS X V10.5	Red Hat Enterprise Linux Desktop 4 Update 4, 32 bit
Web browser	• Mozilla Firefox 2 • Mozilla Firefox 3 • Microsoft Internet Explorer 6.0 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0	• Mozilla Firefox 2 • Mozilla Firefox 3 • Microsoft Internet Explorer 6.0 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0	• Mozilla Firefox 2 • Mozilla Firefox 3 • Apple Safari 3.1 • Apple Safari 3.2 • Apple Safari 4.0	• Mozilla Firefox 2 • Mozilla Firefox 3
Email application	Microsoft Outlook 2003 and 2007	Microsoft Outlook 2003 and 2007	Not supported	Not supported
SMS application (optional)	SMS Client software	SMS Client software	Not supported	Not supported
VOIP (This Computer)	Software installed with one-X Portal	Software installed with one-X Portal	Supported	Not supported

Software	Windows XP	Windows Vista	Apple OS X	Red Hat Enterprise Linux Desktop
Avaya one-X Portal Extensions	When installed from one-X Portal or via SMS	When installed from one-X Portal or via SMS	Not supported	Not supported

Support for Avaya one-X® Portal applications on Citrix

Avaya one-X® Portal supports Citrix Metaframe Presentation Server 4.5 for the one-X Portal and Administration application.

Note:

- You cannot host the one-X Portal Extensions or any other supporting applications on Citrix.
- Avaya one-X® Portal does not support VOIP mode on Citrix.

.

Required hardware for one-X Portal components

Minimum hardware requirements

When you implement Avaya one-X® Portal, ensure that the following hardware meets the minimum requirements:

- Avaya one-X® Portal server machine, including the Avaya one-X® Portal server and applications, and the internal Avaya one-X® Portal database
- Computers used to access Avaya one-X® Portal applications, such as the Administration application, one-X Portal and the one-X Portal Extensions

This section includes the minimum hardware requirements details. If you expect Avaya one-X® Portal to handle a high volume of traffic, or one or more individuals to carry more than 5,000 contacts, Avaya recommends that you provide hardware with more memory and a faster processor. Contact your Avaya representative or Avaya Business Partner representative for assistance with sizing a Avaya one-X® Portal system.

Important:

Additional hardware is required for Communication Manager, Modular Messaging, Conferencing, AE Services, and other software that the users access through Avaya one-X® Portal. For hardware requirements for those products, see the product documentation.

Related topics:

Hardware requirements on page 31

Avaya one-X Portal user and administrator hardware requirements on page 31

Hardware requirements

This section includes the minimum hardware requirements details. If you expect Avaya one-X® Portal to handle a high volume of traffic, or one or more individuals to carry more than 5,000 contacts, Avaya recommends that you provide hardware with more memory and a faster processor. Contact your Avaya representative or Avaya Business Partner representative for assistance with sizing a Avaya one-X® Portal system.

The server must meet the following minimum hardware specifications:

CPU	Two quad-core processors 2.66 GHz or higher
Memory	6 GB of RAM
Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)
Network card	100 Mbps/1Gbit
Optical drive	DVD/CD combination drive

one-X Portal Release 5.2 also supports Avaya Common Server S8800.

Avaya has successfully tested one-X Portal hosted on IBM xSeries servers and Dell PowerEdge servers that met the minimum specifications.

Avaya one-X Portal user and administrator hardware requirements

This section includes the minimum hardware requirements details. If you expect Avaya one-X® Portal to handle a high volume of traffic, or one or more individuals to carry more than 5,000 contacts, Avaya recommends that you provide hardware with more memory and a faster processor. Contact your Avaya representative or Avaya Business Partner representative for assistance with sizing a Avaya one-X® Portal system.

- Windows desktop on page 32
- Mac desktop on page 32

Windows desktop

Processor	Two quad-core processors 1.86 GHz or higher
Memory	12 GB RAM
Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)
Sound card	As provided with computer
Network card	100 Mbps/1Gbps

Mac desktop

Processor	Two quad-core processors 1.86 GHz or higher
Memory	12 GB RAM
Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)
Sound card	As provided with computer
Network card	100 Mbps/1Gbps

Linux desktop

Processor	Two quad-core processors 1.86 GHz or higher
Memory	12 GB RAM
Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)
Sound card	As provided with computer
Network card	100 Mbps/1Gbps

Peripherals required for all operating systems

Monitor	Video adapter and monitor with Super VGA (800 x 600) or higher resolution
Required accessories	Keyboard and a mouse (or compatible pointing device)
Optional accessories	Microphone and speakers, or headphones with a microphone

Network guidelines for one-X Portal

Time synchronization requirements

Time synchronization ensures that time stamps for all integrated systems are consistent. If time is not synchronized on these computers, end users may see inconsistent entries in Avaya one-X® Portal. For example, the Messages portlet may show that a voice message arrived before the related missed call.

Note:

If the time stamps are not synchronized, the secure SSL connections between the servers fails.

The following servers require Network Time Protocol (NTP) software for time synchronization:

- The server that hosts Avaya one-X® Portal
- All servers that host integrated systems, such as Communication Manager, Modular Messaging, System Manager, and Presence Services

Important:

Do not use batch scripts that periodically set the time. These scripts and tools are not accurate enough for Avaya one-X® Portal.

Telephony network performance between Avaya one-X® Portal and Avaya Aura® Application Enablement Services

Location of servers

For optimal performance of the application call control links, Avaya recommends:

- Place the Session Manager, System Manager, Avaya one-X® Portal server, Application Enablement Services server, and Communication Manager CLAN resources in one network domain, if possible.
- Follow the Application Enablement Services server limits if Avaya one-X® Portal has to run with other applications running on the same Application Enablement Services server.

Guidelines for network performance

Average round trip packet delay	No more than 50 milliseconds (ms)

Periodic spiked delays	No more than 1.3 seconds while maintaining the 50 ms average

Network firewall guidelines

If your users gain access to Avaya one-X® Portal from outside the internal network through VPN, Avaya recommends that you implement an external, H.323 VoIP-aware firewall.

Avaya has successfully tested the following external firewalls with a VPN tunnel to a Juniper Networks SA 1000 device in NCP and ESP mode:

- Juniper Networks SA 1000: 5.4R2.1 (Build 11529)
- Juniper Networks SSG-520: ScreenOS 5.4.0x1.0
- Check Point Firewall: NGX R60_HFA_02 (Hotfix 0.604 - Build 2)
- Cisco 525 PIX: PIX version 7.2(2)
- SonicWALL Pro 3060: SonicOS Enhanced 3.2.0.0-43e; SonicROM 3.1.0.2

Remote user connection requirements

Required Broadband Internet connection

Remote users must connect to Avaya one-X® Portal across a broadband internet connection.

Avaya one-X® Portal does not support a dial-up connection.

VoIP bandwidth requirements

Transport network	100 kilobits per second (kbps) per VoIP user in each direction (100 kbps in and 100 kbps out)
End-to-end average packet delay	120 ms
Average jitter	Less than 20 ms

The VoIP bandwidth requirements for Avaya one-X® Portal are similar to the bandwidth requirements for Avaya IP telephones and other Avaya IP applications. Avaya recommends that you test the VoIP bandwidth requirements for each Avaya one-X® Portal deployment because network and other conditions can impact bandwidth use.

The VoIP component in Avaya one-X® Portal uses 8-KHz, 1-byte sampling without compression. Avaya estimates that the following guidelines apply to VoIP bandwidth use:

- If 1000 VoIP users talk simultaneously to internal telephones, the bandwidth requirements are 100 mbps in each direction.
- If 1000 VoIP users talk simultaneously to outside telephones, the bandwidth requirements are 200 mbps in each direction.

However, when considering this bandwidth use, you must make allowances for packet collision on local network segments. During Avaya one-X® Portal activity, Avaya estimates the following network traffic:

- An active Avaya one-X® Portal user can use up to 16 kbps of bandwidth when performing actions, such as logging in, making calls, listening to messages, and looking up contacts. You can consider this to be peak traffic.
- When a user is idle, and gets a call or message approximately every 5 minutes, bandwidth use drops to about 1.6 kbps. This traffic occurs because Avaya one-X® Portal polls the server approximately once a second.

Licensing requirements for one-X Portal

Licensing requirements

Before you install Avaya one-X® Portal, Avaya recommends that you obtain UC All Inclusive total bundle license, which include licenses for Avaya one-X® Portal and all integrated components.

Licenses for UC All Inclusive total bundle licenses

You must obtain an end-user license from Avaya to provision users for Avaya one-X® Portal. Unprovisioned users cannot access Avaya one-X® Portal.

This license file covers all Avaya one-X® Portal users. An end-user license is consumed when a user is configured and activated for use.

The UC All Inclusive total bundle license has the license files for all Avaya components that you want to integrate with Avaya one-X® Portal. For detailed information about the license requirements for these products, see the product documentation or consult your Avaya representative or Avaya Business Partner representative.

Depending on your system, the license requirements for integrated Avaya components may need to include the following:

Communication Manager	Extension to Cellular, Avaya one-X® Communicator, and CTI Adjunct Links enabled

Note:

Avaya one-X® Portal Release 5.2 consumes an Avaya one-X® Communicator license on Communication Manager for each user logged on to Avaya one-X® Portal in VoIP mode.

Application Enablement Services	Telephony Services Application Programming Interface (TSAPI) functions
Modular Messaging	Message store platform, number of mailboxes, and maximum number of concurrent text to speech (TTS) sessions
Conferencing	As required by your conference bridge version

The type of license consumed from Application Enablement Services (AES) and Communication Manager depend on the system usage. The following licenses are present:

- TSAPI Monitoring license (on Application Enablement Services):

  One TSAPI monitoring license is used for each extension Avaya one-X® Portal monitors. Avaya one-X® Portal and Application Enablement Services multiplex the extension monitor, so Avaya one-X® Portal does not monitor the same extension twice. Avaya one-X® Portal monitors an extension:

  - if the user is set for Continuous Call Monitoring, Avaya one-X® Portal monitors the user's extension continuously.
  - when the user logs in using any of the 3 modes.
  - when each mobility worker station is monitored continuously.

- Avaya one-X® Communicator license:

  One Avaya one-X® Communicator license is used for each user logging in using the VoIP (This Computer) mode.

Related topics:

Host ID on page 37

Location of the Avaya Web License Manager

You can install the Avaya Web License Manager (WebLM) in the following locations:

- Local to Avaya one-X® Portal: Use the Avaya one-X® Portal Installation Wizard to install WebLM on the same server as the Installation Wizard server and applications.
- Remote from Avaya one-X® Portal: Install WebLM on a standalone server or use an existing WebLM. You cannot use the Avaya one-X® Portal Installation Wizard to install WebLM remotely.

Important:

Application Enablement Services requires a dedicated WebLM. Do not install the Avaya one-X® Portal license on the WebLM used by Application Enablement Services.

Recommendations

Avaya recommends that you install licenses for most Avaya products in a single location. If the network already includes a WebLM that is not used by Application Enablement Services, Avaya recommends that you use the existing WebLM for Avaya one-X® Portal.

Use the local WebLM server only if the network does not include a WebLM, or if the existing WebLM is not a version supported by Application Enablement Services.

Related topics:

Required software for integrating servers with one-X Portal on page 27

Environment validation checklist on page 41

Product software and licenses

PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing asset entitlements and electronic delivery of software and related licenses. Using PLDS, you can perform activities such as license activation, license de-activation, license re-host, and software downloads.

Note:

To obtain a license from the PLDS Web site, you must have the Host ID of the computer on which you are installing the WebLM server.

For more information on downloading product software and obtaining licenses, see *Getting Started with Avaya PLDS* on the Avaya Support site.

Host ID

You must provide a host ID for the computer that hosts license components for Avaya one-X® Portal. The host ID is also known as the physical address or MAC address.

Related topics:

Licensing requirements on page 35

Obtaining a host ID from a WebLM server coresident on your Avaya one-X Portal server on page 38

Obtaining a host ID from a standalone WebLM server on page 38

Obtaining a host ID from a WebLM server coresident on your Avaya one-X® Portal server

If the WebLM server is coresident on your Avaya one-X® Portal server, follow this step:

On the computer that hosts the Avaya one-X® Portal server, run the following command: `ifconfig -a eth0| grep -i Hwaddr`
This command returns the following text. The highlighted text represents the host ID of the machine:

`eth0 Link encap:Ethernet HWaddr` *`00:04:23:C3:C2:66`*

Obtaining a host ID from a standalone WebLM server

1. Type the following path on your browser: `http://<WebLM server IP>:8080/WebLM`
2. Log on to the WebLM server using your log-on credentials.
3. On the home page of the WebLM server, in the left pane, click the **Server Properties** link.
4. Note the **Primary Host ID**.
   For more information on installing and configuring an Avaya WebLM server, see *Installing and Configuring Avaya WebLM server* on the Avaya Support site.

   Note:
   You can obtain the LOCAL (C-Dom) WebLM URL from Administration Web site.

Customizing one-X Portal

Rebranding options for Avaya one-X® Portal

You can customize the look and feel of Avaya one-X® Portal to meet the corporate branding needs. These rebranding options include:

- Changing the name displayed to Avaya one-X® Portal users.
- Changing the logo.
- Changing the color of the application controls.

Note:

You have to repeat the re-branding process whenever you install an upgrade or patch to the Avaya one-X® Portal Server.

Rebranding Avaya one-X® Portal

Caution:

Be very careful when you change the files in the rebranding package. You can damage the integrity of the Avaya one-X® Portal application if you do not take care when you make changes.

1. Copy the ReBranding ZIP file from the Avaya one-X® Portal DVD to a local directory on your computer.
2. Unzip the rebranding file.

   Ensure that your extracted copy retains the folder structure in the zip file.
3. Carefully read the `_readme.txt` file.
4. Following the instructions in the `_readme.txt`, make your changes to rebrand Avaya one-X® Portal.
5. Following the instructions in the `_readme.txt`, install your changes on a test machine.

6. Test your changes and make sure that the integrity of Avaya one-X® Portal has not been damaged.
7. Deploy the changes to the production system using the same method used on the test system.

Note:

Repeat the rebranding steps each time you install an upgrade or patch on the Avaya one-X® Portal server. You must always use the latest version of the `Branding.zip` file from the `/opt/avaya/1xp/` folder. The `Branding.zip` file gets updated during an upgrade or patch install.

Chapter 3: Completing prerequisites for the one-X Portal server

Environment validation checklist

This checklist includes the hardware and software required for a complete Avaya one-X® Portal system. If the system will not integrate with all supported software, omit the requirements for those servers you do not plan to use.

Important:

Implementing Avaya one-X Portal assumes that all required hardware will be in place, and all required software will be up and running before you implement Avaya one-X® Portal.

- Prerequisites for Avaya one-X Portal server machine on page 41
- Prerequisites for integrated components on page 42
- Prerequisites for system network on page 42

Prerequisites for Avaya one-X® Portal server machine

For notes and details of tested server hardware, see:

- Hardware requirements on page 31
- Required software for the one-X Portal server on page 26

Requirement	Value		✔
Hardware	**CPU**	Two quad-core processors 2.66 GHz or higher	
	Memory	6 GB of RAM	
	Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)	
	Network card	100 Mbps/1Gbit	
	Optical drive	DVD/CD combination drive	
Operating system	Red Hat Enterprise Linux 5 (32 bit)		
Web browser	Mozilla Firefox 2		

Requirement	Value	✔
	Mozilla Firefox 3	

Prerequisites for integrated components

For more details about these requirements, see Required software for integrating servers with one-X Portal on page 27.

Component	Requirement	Supported versions	✔
Telephone	Telephony switch	Communication Manager 5.2.1	
	CTI application	Application Enablement Services 4.2.2 and 5.2	
Bridge Conferencing	Conferencing application	Avaya Conferencing 4.1 and 5.2	
Messaging	Messaging application	Avaya Modular Messaging 4.0 and 5.2	
Presence	Presence application	Avaya Intelligent Presence Service 1.0	
Licensing	License server	Optional. You can use the Web License Manager installed with one-X Portal. Avaya Web License Manager 4.4 and 4.5	
Enterprise Authentication and Enterprise Address Book information		• Microsoft Active Directory 2003, Windows Server 2008 Active Directory Domain Services • IBM Domino Server 7.5 • Novell eDirectory 8.8 SP2 • SUN ONE Directory Server 5.2 and 6.3	

Prerequisites for system network

For notes and details of tested third-party firewalls, see:

- Network firewall guidelines on page 34
- Telephony network performance between Avaya one-X Portal and Avaya Aura ® Application Enablement Services on page 33
- Time synchronization requirements on page 33

Requirement	Value	✔
Firewall	If your users gain access to Avaya one-X® Portal from outside the internal network through VPN, Avaya	

Requirement	Value	✔
	recommends that you implement an external, H.323 VoIP-aware firewall.	
Telephony network performance between Avaya one-X® Portal server and AE Services	**Average round trip packet delay** No more than 50 milliseconds (ms) **Periodic spiked delays** No more than 1.3 seconds while maintaining the 50 ms average	
Time synchronization requirements	The following servers require Network Time Protocol (NTP) software for time synchronization: • The server that hosts Avaya one-X® Portal • All servers that host integrated systems, such as Communication Manager, Modular Messaging, System Manager, and Presence Services	

Server prerequisites checklist

Verify that the following prerequisites have been configured for one-X Portal before you run the Avaya one-X® Portal Installation Wizard.

Tip:

For detailed procedures, see the online help and documentation provided with the software.

#	Task	Instructions
1	Make sure that all components required for the system are up and running, such as: • Communication Manager • Modular Messaging • Conferencing • Application Enablement Services • Presence Services • Directory Service	See the documentation provided with the component. Installing required components for integrated servers on page 47
2	For all Avaya components, including Communication Manager and Application Enablement Services, make sure that you have installed all required licenses.	See the documentation provided with the component. Installing required components for integrated servers on page 47

#	Task	Instructions
3	Install Linux with the required components on the Avaya one-X® Portal server.	Installing Linux for Avaya one-X Portal on page 48
Enterprise Directory configuration		
4	Create Directory security groups with the required values for the following types of one-X Portal users: • Administrative users • Avaya one-X Portal users • Auditor users • Presence users group	Configuring Enterprise Directory security groups on page 56
5	For each Avaya one-X® Portal user, verify that the Directory user record has the required values.	Verifying Enterprise Directory user configuration on page 57
6	Create a Directory user for the Avaya one-X® Portal administrative service account to start and stop the Avaya one-X® Portal server and perform other administrative functions.	Creating the Avaya one-X Portal administrative service account on page 57
AE Services configuration		
7	If the Avaya one-X® Portal system includes a dedicated AE Services server, install and configure AE Services.	Guidelines for installing AE Services on page 50
8	Create an H.323 Gateway list for the switch.	H. 323 gateway list configuration for AE Services on page 52
9	Create DMCC and TSAPI login IDs for Avaya one-X® Portal.	Creating AE Services users for Avaya one-X Portal on page 51
Communication Manager configuration		
7	Configure Send All Calls in Communication Manager to enable Do Not Disturb for Avaya one-X® Portal.	Configuring Send All Calls in Communication Manager for Do Not Disturb in Avaya one-X Portal on page 59
8	For call forwarding, in the Class of Service screen: • Set the **Trk-to-Trk Restriction Override** to enable the trunk to trunk transfer permissions for each user. • Set the value of **Restrict Call Fwd-Off Net** to `n`.	Configuring call forwarding on page 59

#	Task	Instructions
9	To activate the telecommuter mode for users, verify that the station settings for Emergency Call Handling are set as follows: • **Remote Softphone Emergency** is not set to Blocking. • **Emergency Location Extension** uses the default value of `STATION`	Configuring emergency call handling on page 60
Extension to Cellular configuration in Communication Manager		
10	Enable user extensions for Avaya one-X® Portal.	Enabling user extensions on page 61
11	Add stations for Avaya one-X® Portal mobility extensions.	Configuring mobility extensions on page 63
Modular Messaging configuration		
12	Configure and enable the following protocols: • IMAP4 • SMTP • LDAP	Configuring Modular Messaging ports and protocols on page 64
13	Authorize LDAP access.	Configuring Modular Messaging LDAP access on page 65
14	For each user, verify that at least one of the following Subscriber Management values matches the same value in the Active Directory user record: • **Telephone Number** • **PBX extension** • **Email Handle** • **Mailbox Number**	Verifying Modular Messaging subscriber values on page 65
Conferencing configuration		
15	Enable and verify the following features: • ANI • Music • PINs (optional) • SIP trunk set • DTMF • Dial	Enabling Conferencing bridge features on page 67

#	Task	Instructions
16	Configure the following parameters with the required values: • Operator codes • Flex-DAPI	Configuring bridge operators for Conferencing on page 68
17	Make sure that the `/usr/ipcb/config/telnumToUri.tab` file routes from Conferencing to Communication Manager.	Configuring communication between Conferencing and Communication Manager on page 68
18	Optional Configure on-demand conferences for PIN prompting, including a new client with the following values: • Participants • Demand • Conference PIN • Moderator PIN • Reservation details • Conference options for Music Source, Moderator Hang-Up, Security, and PIN options	Configuring on-demand conferences for PIN prompting (Optional) on page 69
Presence Services configuration		
19	Configure Avaya one-X® Portal security certificates. • Avaya one-X® Portal certificate • AcpUMSBus to be "non-secure"	Configuring Presence security certificates on page 69
20	Configure AcpUMSBus to be "non-secure"	Configuring AcpUMSBus as non-secure for Presence
21	Configure Presence server	Configuring the Presence server on page 72
22	Configure SIP Presence server	Configuring the SIP Presence server
23	Reduce Axis Logging	Reducing Axis logging for Presence

Installing required components for integrated servers

Tip:

If a supported version of the integrated server software is already functional in the enterprise and the system meets the version and user requirements, you do not need to install a new system. You can integrate Avaya one-X® Portal with the existing system.

The names of the following installation and administration documents were current when *Implementing Avaya one-X® Portal* was released. Review the documentation set provided with your software to ensure that you use the correct document to install and configure the components.

1. Install and configure all required components for servers you want to integrate with Avaya one-X® Portal:

Component	Documentation
Communication Manager	• *Installing and Configuring the Avaya S8500 Media Server* • *Administrator Guide for Avaya Communication Manager*
Application Enablement Services	• *Avaya MultiVantage Application Enablement Services Installation Guide* • *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*
Modular Messaging	• *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Installation and Upgrades* • *Messaging Application Server Administration Guide*
Avaya Aura® Messaging	*Administering Avaya Aura™ Messaging*
Conferencing	• *Installing the CS700/CS780 Audio Conferencing Server* • *Installing the S6200 and S6800 Conferencing Servers* • *Configuring the CS700/CS780 Audio Conferencing Servers*

Component	Documentation
	• *Configuring S6200, S6500, and S6800 Conferencing Servers*
Presence Services	• *Intelligence Presence Server Installation and Configuration guide* • *Installation and Configuration Guide Service Pack 2* • *Intelligence Presence Server 1.0 Release Note* • *Intelligence Presence Server 1.0 Service Pack 1 Release Notes* • *Intelligence Presence Server 1.0 Service Pack 2 Release Notes*

2. Follow the documentation provided with the required Avaya components and install the required licenses, including:
   - Communication Manager
   - Application Enablement Services
   - Modular Messaging
   - Conferencing

Installing Linux for Avaya one-X® Portal

Prerequisites

Avaya does not provide a Linux RPM or a Linux installation script. Before you install Avaya one-X® Portal, you must obtain and install Red Hat Enterprise Linux 5.3.

For more information about the Linux installation and the firewall configuration, see the documentation provided by Red Hat.

1. Install Linux on the Avaya one-X® Portal server with the instructions provided with the Red Hat installation utility.
2. During the Linux installation:
   a. Select the default installation for Linux.

      If you perform a complete install, you may encounter version conflicts with some third-party software required by Avaya one-X® Portal.

b. During RHEL installation, check the option to install Legacy Software Development packages.

c. Disable all Security Enhanced Linux (SELinux) features on the Firewall Configuration screen.

d. Disable the firewall to use the Avaya one-X® Portal Administration Command Line Client and the Administration Command Line Interface.

e. Avaya recommends to install Linux with the default partitioning during the installation script for the Linux OS. If you are installing Linux into separate partitions, use the table below to create separate partitions for each root level directory. Use this table as a guide when you partition your hard drive.

Note:

The numbers in the Size column are minimum critical sizes for those partitions. If your partition is smaller than these values, the software does not load or loads but does not work.

Product	Directory	Size
Avaya one-X® Portal	`/opt`	13 GB
Avaya one-X® Portal	`/home`	4 GB
Avaya one-X® Portal	`/temp`	4 GB
IPS	`/`	4 GB
IPS	`/opt`	2 GB
IPS	`/home`	4 GB
IPS	`/temp`	4 GB
IPS	`/var`	4 GB
IPS	`/usr`	4 GB

Important:

Run level must be set to 5.

3. Complete the Linux installation.

Note:

Verify whether the following RPMs are installed after Red Hat installation is complete:

The latest compat-libstdc++-33 and compat-libstdc++-296 libraries.

4. Restart the server.

Configuring AE Services for one-X Portal

Guidelines for installing AE Services

When you plan your AE Services deployment, Avaya recommends that you follow these guidelines.

Assigning AE Services server

As long as the AE Services limits are respected, Avaya one-X® Portal can work with other applications running on the same AE Services server.

There are Communication Manager performance benefits when TSAPI applications share the same AE Services server, and most applications fall into the same category. Due to the lower limitations of the DMCC server, Avaya one-X® Portal must not share an AE Services server with an application that uses DMCC.

H.323 Gateway list

Create an H.323 Gateway list for the switch. AE Services associates each Switch Connection with a list of IP addresses for H.323 gateways.

Note:

Avaya one-X® Portal Release 5.2 sales offer uses the AES_DMCC_DMC licenses and not the IP_API_A licenses. Therefore, H.323 gateway list administration field is mandatory for all new installations.

In addition to the license requirements, some Avaya one-X® Portal configurations require an H.323 gateway list, including the following:

CLAN failover	An H.323 gateway list facilitates failover on the AE Services server. If AE Services has a list of configured H.323 gateways and one CLAN becomes unavailable, AE Services automatically connects to another CLAN identified in the list.
Multiple CLANs	With an H.323 gateway list, you can use a different CLAN for H.323 communication between Communication Manager and AE Services than the CLAN used for the VoIP connection between the Avaya one-X® Portal application and Communication Manager. For this configuration, the H.323 gateway list must be present in AE Services and populated with the IP Addresses. AE Services needs the IP addresses to communicate with Communication Manager.

Requirements for AE Services to use AES_DMCC_DMC licenses:

To use an AES_DMCC_DMC license, you must meet the following criteria:

- Communication Manager Release 5.2.1 or later
- AE Services Release 4.2.2 or later

- A provisioned switch connection between AE Services and Communication Manager on which the device is registered
- The WebLM server contains available AES_DMCC_DMC licenses on Application Enablement Services

A provisioned switch connection between AE Services and Communication Manager implies that Avaya one-X® Portal and AES/DMCC can identify the switch by the same name and that Application Enablement Services has an H.323 gateway list for the switch connection. This switch name is case sensitive.

The CLAN addresses in the H.323 gateway must accept the H.323 registration and support codec G.711.

Application Enablement Services uses IP_API_A licenses if it cannot use AES_DMCC_DMC licenses. The AES_DMCC_DMC licenses are provisioned in Application Enablement Services and the IP_API_A licenses are provisioned in Communication Manager.

Required users for Avaya one-X® Portal

Create two users for Avaya one-X® Portal, one for DMCC (formerly CMAPI) and one for TSAPI. Make sure that the TSAPI user has unrestricted access in AE Services and does not use SDB. This configuration minimizes the administration overhead of using Avaya one-X® Portal.

Switch name

If your deployment uses more than one AE Services server to connect to Communication Manager, make sure Communication Manager has the same name on every AE Services server.

Creating AE Services users for Avaya one-X® Portal

Avaya one-X® Portal requires two Avaya one-X® Portal users, one for DMCC (formerly CMAPI) and one for TSAPI.

Create two users for Avaya one-X® Portal, one for DMCC (formerly CMAPI) and one for TSAPI. Make sure that the TSAPI user has unrestricted access to AE Services and does not use SDB. This configuration minimizes the administration overheads of using Avaya one-X® Portal.

If Avaya one-X® Portal cannot log into TSAPI with unrestricted access, you must administer the Avaya one-X® Portal TSAPI login ID to control each extension that Avaya one-X® Portal controls.

Restart the Telephony adapter after AE Services upgrade, where the DMCC server version is also upgraded.

Tip:

For more details, see the *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*.

1. From OAM Web, select the **User Management** menu. Log in to AE Services User Management.
2. From the **User Management** menu, select **User Management** > **Add User**.
3. Add a DMCC user for Avaya one-X® Portal.

   Note:
   Set **CTI Users** to **Yes**.
4. Add a TSAPI user for Avaya one-X® Portal with the following permissions:
   - Unrestricted access in AE Services.

     To enable unrestricted access, go to **Administration** > **Security Database** > **CTI Users** > **List All Users**. Select and edit the TSAPI user, and click **Enable** next to Unrestricted Access.
   - Do not allow the DMCC user to use SDB.
5. Note the DMCC and TSAPI user IDs and passwords in the AE Services configuration worksheet.
6. To access the CTI Users page, select **Administration** > **Security Database** > **CTI Users** > **List All Users**. Verify the users that you just created.

H. 323 gateway list configuration for AE Services

AE Services associates each Switch Connection with a list of IP Addresses for H.323 gateways.

Tip:
For more details, see the *Administrator Guide for Avaya Communication Manager* and the *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide.*

When you administer the switch connection, add the switch to the H.323 Gateway list.

Note:

- After administering the AE Services, restart the DMCC and TSAPI services. Sometimes you may need to restart the AE Services Server also.

  The H.323 gateway configuration for AE Services requires that the **CM Name for AES** field on the Avaya one-X® Portal computer matches the configuration

on AE Services exactly. This configuration is case sensitive for the H.323 gateway list but not for TSAPI.

- Avaya one-X® Portal Release 5.2 sales offer uses the AES_DMCC_DMC licenses and not the IP_API_A licenses. Therefore, H.323 gateway list administration field is mandatory for all new installations.

Configuring Enterprise Directory for one-X Portal

Enterprise Directory integration guidelines

Avaya one-X® Portal integrates with the following enterprise directory servers for user records, authentication, and authorization. Avaya one-X® Portal also uses the enterprise directory to search contact information, that is, like an address book. You can integrate with an existing enterprise directory server, or you can use a dedicated enterprise directory server for Avaya one-X® Portal.

- Microsoft Active Directory
- IBM Domino server
- Novell eDirectory server
- Sun One Directory server

Note:

Avaya one-X® Portal does not support enterprise data split between two or more enterprise directories. For example, you cannot create the User Domain on an Active Directory server and the Contact Domain on a Domino server. Also, Avaya one-X® Portal supports only one enterprise directory attribute mapping. Therefore, the list of attributes must be the same for any enterprise directory you administer.

Limitations on support for Active Directory domains

Each Avaya one-X® Portal deployment can authenticate and authorize users from only one Active Directory domain. Depending upon the enterprise Active Directory policy, security groups for Avaya one-X® Portal users can reside in the same domain as the users or in a different domain. The domain that provides the users is known as the user domain. The domain that provides the security groups is known as the resource domain.

You can configure each deployment to access information about users in up to four additional Active Directory domains. However, Avaya one-X® Portal considers the users in the additional domains to be contacts only and does not obtain anything other than the address book data from them. You cannot provision users from the additional domains, and those users cannot log in to the Avaya one-X® Portal deployment.

If you want to provide Avaya one-X® Portal services to users in more than one Active Directory domain, you must implement at least one Avaya one-X® Portal deployment for each domain.

Limitations on support for other Enterprise Directory domains

Only the LDAP server in the LDAP Domain on Avaya one-X® Portal supports identity resolution on other supported enterprise directories.

Supported Active Directory domain topologies

Domain topology	Description
Combined domain	Users and security groups are in the same Active Directory domain. For this topology, configure Avaya one-X® Portal with the same domain for the user and the resource.
Split domain in same forest	Users and security groups are in separate Active Directory domains. These domains are in the same forest. For this topology, configure Avaya one-X® Portal with the same domain for the user and the resource.
Split domain in different forest	Uses two Active Directory domains that are in different forests. For this topology, configure Avaya one-X® Portal with the same domain for the user and the resource. To ensure the required access, this topology requires a different service account and password for each forest when you install Avaya one-X® Portal.

Required security groups

Before you install Avaya one-X® Portal, you must create at least one set of the following Enterprise Directory security groups:

- Administrative users
- Avaya one-X® Portal users
- Auditor users
- Presence users

These security groups belong in the same resource domain where the enterprise maintains other security groups for Avaya one-X® Portal users.

Each Avaya one-X® Portal user must be a member of at least one of the Avaya one-X® Portal security groups. Some users can be members of more than one security group. For example, a user who needs access to the Administration application and to Avaya one-X® Portal must be a member of both the administrator and user security groups.

If you plan to deploy more than one Avaya one-X® Portal server in an environment, Avaya recommends that you create a unique set of security groups for each Avaya one-X® Portal server in the system, even if both deployments use the same Enterprise Directory domain. You can configure two Avaya one-X® Portal deployments to use the same security groups.

However, you cannot change the security groups assigned to a deployment without reinstalling Avaya one-X® Portal.

Naming conventions for security groups

Avaya recommends that you follow existing corporate standards when you create security groups for Avaya one-X® Portal. Each security group name must do the following:

- Be unique in the Active Directory domain.
- Identify the group as related to Avaya one-X® Portal
- Identify the Avaya one-X® Portal deployment
- Identify the purpose of the security group.

Note:

Do not use the default security group names, such as Domain Users, for Avaya one-X® Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

For example, use the following naming conventions for security groups:

- <*deployment_name*> Avaya one-X® Portal Users
- <*deployment_name*> Avaya one-X® Portal Administrators
- <*deployment_name*> Avaya one-X® Portal Auditors
- <*deployment_name*> Avaya one-X® Portal Presence

Using this naming convention, you can identify the Avaya one-X® Portal deployment associated with the security groups. Even if the system only includes one Avaya one-X® Portal deployment, this naming convention ensures that the Active Directory integration can be expanded to include additional Avaya one-X® Portal deployments.

Determining the Active Directory domain topology

After you install Avaya one-X® Portal, you cannot change the Active Directory domain unless you reinstall Avaya one-X® Portal. So it is necessary to ascertain the domain topology that the Enterprise Active Directory uses.

1. Determine which of the following domain topologies the Enterprise Active Directory uses:
   - Combined domain
   - Split domain in same forest
   - Split domain in different forests
2. Identify the user domain that includes the users who access Avaya one-X® Portal.

3. Identify the resource domain that defines the Avaya one-X® Portal security groups.
4. If the user domain and resource domain are different, determine whether they are in the same forest.

Related topics:

Enterprise Directory integration guidelines on page 53

Configuring Enterprise Directory security groups

Note:

Do not use the default security group names, such as Domain Users, for Avaya one-X® Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

1. In the resource domain, create Enterprise Directory security groups for the following groups of users in each Avaya one-X® Portal deployment:
   - Administrative users who need access to the Administration application. Include the deployment in the group name, for example, Chicago Avaya one-X® Portal Administrators.
   - Users who need access to the Avaya one-X® Portal. Include the deployment in the group name, for example, Chicago Avaya one-X® Portal Users.
   - Auditors who need read-only access to the Administration application. Include the deployment in the group name, for example, Chicago Avaya one-X® Portal Auditors.
   - Users who you wish to be able to display presence information about. These users do not have access to log in to Avaya one-X® Portal. When configured, these users do not consume a license.
2. For the **Active Directory** only, make sure that the configuration of each security group includes the following values:
   - The pre-Windows 2000 name has the same value as the group name.
   - The group type is Security.
   - For a split domain topology only, the group scope is Domain Local.

Related topics:

Enterprise Directory integration guidelines on page 53

Verifying Enterprise Directory user configuration

Avaya one-X® Portal accesses the user accounts in the Enterprise Directory for authentication and authorization. If Avaya one-X® Portal can access an existing Enterprise Directory server, you do not need to create new user accounts.

Users can log in with their corporate log-in IDs and passwords. To ensure that enterprise users can access Avaya one-X® Portal, verify that each user account meets the required criteria.

Each Avaya one-X® Portal user must be a member of at least one of the Avaya one-X® Portal security groups. Some users can be members of more than one security group. For example, a user who needs access to the Administration application and to Avaya one-X® Portal must be a member of both the administrator and user security groups.

For each Avaya one-X® Portal user in the user domain, verify the following with regard to the Enterprise Directory user records.

- The domain that hosts Avaya one-X® Portal has the Enterprise Directory user records.
- At least one Avaya one-X® Portal security group is assigned the records to provide the user with the required administrative, user, or auditor privileges.
- The records have a pre-Windows 2000 log-on name that is identical to the Avaya one-X® Portal log-on name.
- The records include a user password and the desired password options.

Creating the Avaya one-X® Portal administrative service account

For Avaya one-X® Portal create at least one administrative service account in the user domain of the Enterprise Directory. This administrative service account must be a member of the administrators security group.

Avaya one-X® Portal uses this service account to start and stop the Avaya one-X® Portal server and perform other administrative functions.

If the Enterprise Directory uses a split domain topology with the user domain and resource domain in different forests, Avaya one-X® Portal also requires a secondary service account in the resource domain.

You can map LDAP attributes to the attributes used in Avaya one-X® Portal using the **System** tab in Administration Web Client.

1. In the user domain, create a primary service account that meets the following criteria:
   - Has a password that meets the requirements of IBM WebSphere. For example, the password cannot contain a space, must start with a number or letter, and must not start with an underscore or other symbol. For more information, see the IBM WebSphere online documentation.
   - Has a password that does not expire.
   - Is a member of the Avaya one-X® Portal users and administrators security groups.
2. The primary service account should be able to:
   - Get the Distinguish Name (DN) of the user based on the user's handle, so the system can validate the password of the user.
   - See the members of the security groups.
   - Read any information that Avaya one-X® Portal wants to export, such as user phone numbers.
3. For Active Directory only, create a secondary service account in the resource domain that meets the same criteria specified in steps 1 and 2. This is only for a split domain topology with the user domain and resource domain in different forests.

Note:

To configure Avaya one-X® Portal LDAP over SSL, refer to the Appendices in this document.

Related topics:

LDAP over SSL configuration on page 231
Avaya one-X Portal and Novell eDirectory setup over SSL on page 237

Configuring Communication Manager for one-X Portal

Configuring Send All Calls in Communication Manager for Do Not Disturb in Avaya one-X® Portal

The Do Not Disturb functionality in Avaya one-X® Portal is similar to the Send All Calls feature in Communication Manager.

Do Not Disturb uses the station coverage path to determine the destination of a call when the user does one of the following:

- Configures the Avaya one-X® Portal telephone settings for Do Not Disturb mode.
- Clicks **Ignore** when a call arrives in Avaya one-X® Portal.

Tip:

For more details about these configurations, see the *Administrator Guide for Avaya Communication Manager.*

1. Log in to the Avaya Site Administration (ASA) application.
2. To change the coverage path for an existing extension, use the `change coverage path` command.
3. Enable Send All Calls with the standard Communication Manager configuration.

Configuring call forwarding

Users may need additional permissions to forward an external call to a telephone that is not controlled by Communication Manager.

Note:

Some problems that these configurations on Communication Manager may cause include the following:

- When you switch off the trunk-to-trunk restriction, a user can use the company trunk to make international calls on behalf of someone else. For example, a user who gets a call from a friend on the business phone number can transfer the call to a common friend overseas on behalf of the first caller.
- In some countries, there is no explicit signaling to indicate to the PBX that the far end has disconnected the call. For example, if a user in the PBX transfers a trunk call to

another trunk, both sides are on trunk calls. In this scenario, the PBX cannot detect when to disconnect the call and free up the trunks.

Tip:

For more details about these configurations, see the *Administrator Guide for Avaya Communication Manager.*

1. Log in to the Avaya Site Administration (ASA) application.
2. In the Class of Service screen:
   a. Set the **Trk-to-Trk Restriction Override** to enable the trunk-to-trunk transfer permissions for each user.
   b. Set the value of **Restrict Call Fwd-Off Net** to `n`.
3. Press `Enter` to save your work.

Configuring emergency call handling

Avaya one-X® Portal uses CMAPI to activate the telecommuter mode for users. CMAPI does not support the Blocked configuration for emergency call handling.

Therefore, to allow users to handle calls from a remote telephone, verify that the station settings for Emergency Call Handling are not set to Blocking.

Tip:

For more details about these configurations, see the *Administrator Guide for Avaya Communication Manager.*

1. Log in to the Avaya Site Administration (ASA) application.
2. To navigate to the Station screen for each extension, use the **`change station`** command.
3. Navigate to page 2 of the Station screen.
4. Verify that **Remote Softphone Emergency** is not set to Blocking.
5. Verify that **Emergency Location Extension** uses the default value of `STATION`.
6. Press `Enter` to save your work.

Configuring Extension to Cellular for one-X Portal

Extension to Cellular and Avaya one-X® Portal

With Extension to Cellular, users can access Communication Manager features and incoming telephone calls on their office telephones and cell phones. To accomplish this, Extension to Cellular maps the network number that you dial out of Communication Manager to the associated cell phone.

Note:

Extension to Cellular feature requires a dial plan entry to convert the dialled string to the EC500 number. This is configured on the Avaya one-X® Portal Admin application.

The Communication Manager Extension to Cellular functionality has two mapping modes:

- Termination. In this mode, when a call arrives at the station that has Extension to Cellular ON, the Communication Manager dials the user cell phone. If the user answers the call on the cell phone, the station stops ringing and it shows a bridged call appearance for the call that is active at the cell phone.
- Origination. When a call made from a cell phone arrives at Communication Manager that is configured with Extension to Cellular in the Origination mode, Communication Manager recognizes the ANI (Caller ID of the call) and maps the cell phone to the station. This happens independently of the Extension to Cellular ON/OFF status on the switch. Origination mapping is also necessary for Feature Named Extensions (FNE) to work.

For Origination mapping, the cell phone ANI within the switch must be unique.

Extension to Cellular does not use the telephone number that a user dials to access the cell phone. Extension to Cellular uses the telephone number that a user a user dials after reaching the ARS table.

In the United States, most users dial `9` to access the ARS table. In other countries, users dial `0` to access the ARS table. For example, in the United States, a user who dials `919788081234` to reach a cell phone sets up the Extension to Cellular number as `+19788081234`.

Avaya recommends that Avaya one-X® Portal users configure their phone settings with E.164 format (+19788081234). Using this format, Avaya one-X® Portal can determine the correct format for the telephone number.

Enabling user extensions

The values that you set for Extension to Cellular have a large impact on the ability of the user to easily control or change the telephone settings in Avaya one-X® Portal. Avaya recommends

values for these fields to ensure that user settings for Extension to Cellular and Avaya one-X® Portal do not cause issues for users.

For example, Avaya recommends that you set the value of **Mapping Mode** to `both`.

Tip:

For more details about these configurations, see the *Administrator Guide for Avaya Communication Manager.*

1. Log in to the Avaya Site Administration (ASA) application.
2. Set the value of **IP Softphone** for the telephone extension of each Avaya one-X® Portal user:
   a. Use the `change station` command to navigate to the Station screen.
   b. Set the value of **IP Softphone** to `y`.
   c. Press `Enter` to save your work.
3. Execute the following command:
   `change off-pbx-telephone station-mapping XXXXX`
   where *XXXXX* is the extension number.
4. On Page 1 of Stations with Off-PBX Telephone Integration, configure the parameters listed in the following table:

Parameter	Recommended value
Station Extension	Extension assigned to the Avaya one-X® Portal user.

Application	`EC500`
	`EC500 / PBFMC for H.323`
	`OPS / PVFMC for SIP`

Dial Prefix	As appropriate for your system configuration.
Phone Number	Telephone number assigned to the extension of the Avaya one-X® Portal user.
Trunk Selection	`ars`
Configuration Set	`1` or as appropriate for your system configuration.

5. On Page 2 of Stations with Off-PBX Telephone Integration, configure the parameters listed in the following table:

Parameter	Recommended value
Call Limit	2 or as appropriate for your system.
Mapping Mode	both
Calls Allowed	all
Bridged Calls	both

Configuring mobility extensions

Mobility extensions are a set of worker stations on the switch. These stations are not user extensions and must be created for use by Avaya one-X® Portal only. To map mobility stations, use Communication Manager Network Region mapping or native CLAN Network Region to a region that supports G711. Avaya one-X® Portal uses mobility extensions to dial feature access on the switch.

Note:

For mobility extensions, set the **Console Permissions** field to **n** on the extension Class Of Service (CoS) in Communication Manager.

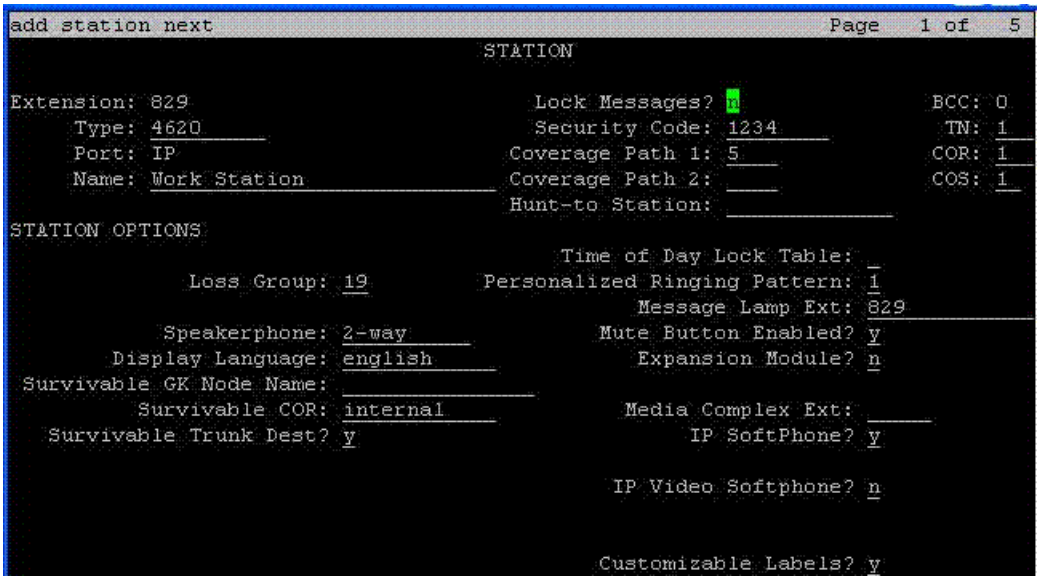
Each switch can have 2 to 10 mobility extensions. The number of mobility extensions is related to the number of Extension to Cellular requests that the Avaya one-X® Portal server has to handle. Typically, each mobility extension can handle 500 Extension to Cellular requests per hour.

Tip:

For more details about these configuration, see the *Administrator Guide for Avaya Communication Manager.*

1. Log in to the Avaya Site Administration (ASA) application.
2. To add a new station for a mobility extension, use the `add station` command to navigate to the Station screen.
3. Configure each mobility extension as shown in the following example of an updated Station screen.

Example



Configuring Modular Messaging for one-X Portal

Configuring Modular Messaging ports and protocols

Important:

If you change the default ports for one or more of these protocols in Modular Messaging, you must change the default settings in the Avaya one-X® Portal Administration application.

1. Navigate to the following Modular Messaging administration screen: **Messaging Administration** > **System Administration**.
2. On the System Administration screen, access the fields required to configure and enable the following protocols:
   - IMAP4/SSL
   - SMTP
   - LDAP
3. Validate the port numbers configured for these protocols against the port requirements for Avaya one-X® Portal.

Configuring Modular Messaging LDAP access

1. Navigate to the following Modular Messaging administration screen: **Messaging Administration** > **Networked Machine Management**.
2. On the Networked Machine Management screen, set the value of **Updates In** to `Yes` for the Message Storage Server in the Modular Messaging domain.
3. Save the change.
4. Navigate to the **Diagnostic** menu and test the LDAP connection.

Verifying Modular Messaging subscriber values

For every Avaya one-X® Portal user, at least one of the Modular Messaging subscriber values must match the corresponding value in the Corporate Directory record for the user. If none of these values match, Avaya one-X® Portal cannot accurately link incoming and outgoing communications with the correct users.

1. Navigate to the following Modular Messaging administration screen: **Global Administration** > **Subscriber Management**.
2. For all local subscribers, verify that at least one of the following values matches the corresponding value in the user record in Corporate Directory:
   - **Telephone Number**

- **PBX extension**
- **Email Handle**
- **Mailbox Number**

Enabling client access for Modular Messaging

Avaya one-X® Portal requires access to the client mailbox. This configuration ensures that subscribers can connect to their mailboxes through Avaya one-X® Portal and access their messages.

1. On the MSS, perform the following steps for every Class of Service that is assigned to a subscriber who needs to access messages through Avaya one-X® Portal:
   a. Navigate to the Manage Classes-of-Service page.
   b. In the **Restrict Client Access** field, set the value to No.
   c. Save your changes.
2. On the MAS, in the Voice Mail System Configuration (VMSC) tool:
   a. Navigate to the Messaging selection and view the **General** tab.
   b. Verify that the value of the **Privacy Enforcement Level** is set to one of the following values:
      - Partial
      - Notification Only

      If the Privacy Enforcement Level is set to Full, validate with the customer that you can change the value.
   c. Save your changes.

Configuring Meeting Exchange for one-X Portal

Enabling Conferencing bridge features

1. Enable the following Conferencing settings:
   a. ANI. Verify that Conferencing is configured to provide ANI (Caller ID) to identify meeting participants.

      This is configured by the `UriToTelnum.tab` file located at `/usr/ipcb/config/UriToTelnum.tab`. This is generally configured and working by default.

   b. Music. Verify that the music is available on Conferencing.

      The music setting is also enabled and configured by default. The music files are located in `/usr2/annun`. They are labelled as music_source1, music_source2, music_source3, music_source4
2. (Optional) Enable the PINs setting and verify that support for PINs is available on Conferencing.

   Note:

   This is an optional feature and is enabled only if the customer likes to use unique PINs. By default, the system is set to accept moderator and participant codes.
3. Enable the following features required for Communication Manager to Conferencing connectivity:
   a. SIP trunk set. Verify that calls from Communication Manager to Conferencing provide Caller ID and DNIS correctly.

      The SIP trunk set is enabled by default unless you manually turn it off. The SIP trunk set is in the trunk setting on page 3. The Numbering Format should be set to **`public`**.

   b. DTMF. Verify that in-band/out-band DTMF in Communication Manager and Conferencing match and Conferencing receives DTMF properly.

      The DTMF setting is in the signaling group settings on page 1. DTMF over IP should be set to **`rtp-payload`**.
4. Enable the Dial feature and verify that Dial from Conferencing to Communication Manager is enabled and properly configured. To enable dialout perform one of the following:

For Meeting Exchange Release 5.2, insert a record in `/usr/ipcb/config/telnumToUri.tab` file where column values are:

- TelnumPattern = *
- TelnumConversion = *sip:$0@135.122.32.134:5060;transport=tcp*
- Comment = *A comment*

Replace the IP address in the TelnumConversion column with the CLAN or Processor Ethernet IP to allow dialout.

Configuring bridge operators for Conferencing

1. Navigate to the **Flex-DAPI (FDAPI) Configuration** menu and configure the following settings:
   a. Operators. Set for `2` plus the number of operators required for Bridge Talk.
   b. Music. Define a music source.
2. Navigate to the **Administrator** menu and select **Sign-In Management**.
3. In the Create Operator Sign-In screen, create the two operators required by the Avaya one-X® Portal server.

Configuring communication between Conferencing and Communication Manager

After you complete the standard Conferencing configuration for Communication Manager, you must ensure that the path from Conferencing to Communication Manager is properly set. Avaya one-X® Portal requires this communication path to add a new participant into an ongoing conference.

Verify that the `/usr/ipcb/config/telnumToUri.tab` file routes from Conferencing to Communication Manager.

Configuring on-demand conferences for PIN prompting (Optional)

If you want to enforce PIN identity for conferences, you must configure the individual PINs in PIN Code Administration 2.0. For more information, see the Conferencing documentation.

You can configure on-demand conferences for PIN prompting in one of the following ways:

- With a specific PIN list that you generate with PIN Administrator software
- With a value of ANYPIN that allows a user to enter any PIN value

Note:
You must configure Conferencing to provide Avaya one-X® Portal with the values for moderator code, participant code, and PIN relative to the configuration of user resources.

1. In the CRS system, navigate to the Customer Bookings window.
2. Create a new client.
3. Complete or enable the following values for the new client:
   - Participants
   - Demand
   - Conference PIN
   - Moderator PIN
   - Reservation details
   - Conference options for Music Source, Moderator Hang-Up, Security, and PIN options.

Configuring the Presence Server for one-X Portal

Configuring Presence security certificates

1. Get the IPS certificate:

To get the IPS certificate, copy the `generic.keystore.jks` file from the IPS machine to the `/opt/certs` directory on the one-X Portal computer.

To open the command shell from one-X Portal computer, execute the following commands:

- `mkdir /opt/certs`
- `scp root@<IPS_host>:/opt/IPS/jabber/xcp/certs/generic.keystore.jks /opt/certs`

Note:

Provide the Presence Services server root password during this step.

2. Open the WAS Admin console to configure certificates in WebSphere and log in via `http://<host>:9060/ibm/console`.

Note:

You can use the log-in credentials of Avaya one-X® Portal service account created for the installation of Avaya one-X® Portal to log in to the WebSphere.

3. Go to **Security** > **SSL Certificate and Key Management** > **Key Stores and Certificates** > **New**.
4. Complete the following fields:
   a. Enter `IPS Keystore` in **Name** .
   b. Enter `/opt/certs/generic.keystore.jks` in **Path** .
   c. Enter `avaya01` in **Password**.
   d. Enter `JKS` in **Type**.
   e. Press **OK**.
5. Go to **Security** > **SSL Certificate and Key Management** > **Key Stores and Certificates**.
6. Complete the following fields:
   a. Check the check box for the **IPS Keystore** and **NodeDefaultTrustStore** fields.
   b. Click the **Exchange signers** button.
   c. Move **testalias** to the **NodeDefaultTrustStore signers** field.

Note:

You may get `An error occurred creating the key store: null`. You can ignore this.

   d. Click **Save**.

7. Go to **Security** > **SSL Certificate and Key Management** > **Key Stores and Certificates** > **NodeDefaultTrustStore** > **Personal Certificates**. Click the **Import** button and complete the following fields:
   a. Enter `/opt/certs/generic.keystore.jks` in **Key filename**.
   b. Enter `JKS` in **Type**.
   c. Enter `avaya01` in **Key file password**.
   d. Click **Get key file aliases**.
   e. Enter `testalias` in **Certificate alias to import**.
   f. Enter `lps` in **Imported certificate alias**.
   g. Click **OK**.
8. Save these changes to the master configuration.
9. Go to **Security** > **SSL Certificate and Key Management** > **SSL configurations** > **NodeDefaultSSLSettings** and complete the following fields:
   a. Click **Get certificate aliases**.
   b. For both the **Default server certificate alias** and **Default client certificate alias** fields, select either **default** for a fresh installation or **websphere dummy server** for an upgrade from the previous version.
10. Go to **Security** > **SSL Certificate and Key Management** > **Key Stores and Certificates** > **NodeDefaultKeyStore** > **Personal Certificates** to export WebSphere certificate to IPS computer.

    Note:

    For a fresh installation (WebSphere 6.1), execute this step for all systems. However, for an upgrade from one-X Portal 1.0 or oone-X Portal 1.1 to one-X Portal 5.2, you must execute the step only once. This is because the certificate name is `jserver` for all WebSphere 6.0.

    a. If you upgraded this system from one-X Portal 1.0.1, select **default certificate** or **websphere dummy server**.
    b. Take note of the value for CN in this certificate.
       - If the certificate alias is **default**, the CN should be the FQDN of this machine.
       - If the certificate alias is **websphere dummy server**, the CN should be **jserver**.
    c. Click **Extract** and complete the following fields:
       - Select **Filename** as `/tmp/default.pem`
       - Set **Data type** as `Base64-encoded`

- Press **OK**.

11. Save the master configuration.
12. Copy the `/tmp/default.pem` file from the one-X Portal machine to the IPS machine.
13. From the one-X Portal machine, execute this command: **`scp /tmp/default.pem root@<IPS_host>:/opt/IPS/jabber/xcp/certs/default.pem`**

    Note:

    The above command copies the default.pem file to the IPS machine. But, if a .pem file already exists, this command overwrites it. To avoid this, you can include the IP address of the source machine to the destination filename. For example, if the IP address of the one-X Portal machine is "135.27.153.38", the command should be `scp /tmp/default.pem root@<IPS_host>:/opt/IPS/jabber/xcp/certs/default_135.27.153.38.pem`
14. To activate the security changes, restart the WAS server gracefully by executing the following commands:

    Note:

    If this is a multiple one-X Portal to IPS configuration, perform these steps on the other WAS server.

    a. To change the current directory, type `cd/opt/IBM/WebSphere/Appserver/profiles/default/bin`

    b. To stop the server, type `./stopServer.sh server1 -username <WebSphereadmin> -password <WebSpherepassword>`

    c. To start the server, type `./startServer.sh server1`

    Important:

    Do not restart the WAS and one-X Portal servers until the IPS configuration is complete and XCP is functional.

Configuring the Presence server

1. Open the XCP configuration page of IPS by `https://<host_IPS>:7300/admin`.
2. Select the **Advanced** configuration view.

3. For the **Global Router**, add each of the Avaya one-X® Portal host names to the Trusted TLS Host Names. This must match the CN value obtained from **default** or **WebSphere dummy server** certificate in WAS.
   - If **default**, enter the FQDN of the Avaya one-X® Portal machine
   - If **WebSphere** dummy server, enter `jserver`

   Submit the name changes.
4. Complete the following fields for the **Presence Server** as indicated.
   a. **AES Username**:`<AES username>`. For example, admin_login
   b. **AES password**:`<AES password>`. For example, Admin1_password
   c. In the **MS RTC Collection Configuration** section, change **Port** from 35061 to 5061 (this should be already set).
   d. In the **UMC to UMS configuration** section, complete the following fields as indicated:
      - **WS Host**.`<IP address of the one-X Portal machine>`
      - **WS Port**.`9443`
      - **WS Service**.`/ums/services/UserMgmtServicePort`
      - **JMS Host**.`<IP address of the one—X Portal machine>`
      - **JMS Port**.`7286`
      - **Login**.`<WebSphere system username>`
      - **Password**.`<WebSphere system password>`
      - **Secure connection**.`Yes`
      - **Retry interval (seconds)**.`180`
   e. Click **Submit** to save these changes.
5. For each Avaya one-X® Portal server, you must add a new Presence server component. Follow these steps to add a new Presence server:
   a. Select `Presence` from the **Component** list.
   b. Click **Go**.

   Important:
   Perform steps 3, 4, and 5 for the second Avaya one-X® Portal server.
6. To import the certificates from various one-X Portal servers to IPS keystore, perform the following steps:
   a. Run the **`tls_generic.sh`** command from`/opt/IPS/jabber/xcp/certs`.

b. Execute the command **./tls_generic.sh <certificate file name>**

Note:

For example, if the certificate is from a Avaya one-X® Portal server whose IP address is 135.27.153.38, the command should be **./tls_generic.sh default_135.27.153.38.pem**

c. To check if the certificate is imported, execute the command **/usr/java/jdk1.5.0_07/bin/keytool -list -keystore generic.keystore.jks**. The password is `avaya01`.

7. After you complete these changes, use the XCP controller page to restart the IPS. It is generally unnecessary to use `service wdinit restart` for these types of changes.

Configuring non- Avaya one-X® Portal users in the Presence group

To see presence for non-Avaya one-X® Portal users in Avaya one-X® Portal, perform the following steps to configure these users using thePresence group that was selected during the Avaya one-X® Portal installation:

Note:

If you select All Enterprise Users during the Avaya one-X® Portal installation and want to control who is added for Presence through Avaya one-X® Portal Administration Web client, these steps are not necessary.

1. Add the non-Avaya one-X® Portal user on the LDAP server used by the Presence server.
2. Create a **User Import** spreadsheet with the appropriate handles and user names of the non-Avaya one-X® Portal users and set **Enable User** to **no**.

   Use the template file provided with the Administration Command Line client to ensure that the file format is compatible and make sure these users are disabled. Be sure to include a telephony configuration for those non Avaya one-X® Portal users to whom you want to provide access to telephony Presence.
3. Run a full **Enterprise Directory Synchronization** from the **Scheduler** tab in the Administration Web Client.
4. Run the **User Import** script in the Administration Command Line Client to import the users.

Configuration worksheets for integrated servers

Configuration worksheet for AE Services

This worksheet lists the information that you need to configure AE Services for Avaya one-X® Portal. You need these values to configure the Auxiliary server in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	aeshandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago AES		A short description of the server that uniquely identifies the AE Services server. You must create this value in the Administration application.
AES Machine Name	AES1234		The hostname of the AE Services server. Use the hostname command on the AES machine to get this host name.
DMCC Host	###.###.###.###		The network address used by the **DMCC** configuration for the AE Services server as an IP address or a DNS address.
DMCC Port	4721 or 4722		The port number used by the **DMCC** configuration for the AE Services server.
DMCC Login ID	cmapi		The log-in ID used by the **DMCC** configuration for the AE Services server.
DMCC Password			The password associated with the log-in ID used by the **DMCC** configuration for the AE Services server.

Property name	Property values		Notes
	Example value	Your value	
TSAPI Host	###.###.###.###		The network address used by the **TSAPI** configuration for the AE Services server.
TSAPI Port	450		The port number used by the **TSAPI** configuration for the AE Services server.
TSAPI Login ID	admin_login		The log-in ID used by the **TSAPI** configuration for the AE Services server.
TSAPI Password			The password associated with the log-in ID used by the **TSAPI** configuration for the AE Services server.

Configuration worksheet for Communication Manager

This worksheet lists the information that you need to configure Communication Manager for Avaya one-X® Portal. You need these values to configure the Communication Manager services in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	cmhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago CM PBX		A short description of the server that uniquely identifies the Telephony server. You must create this value in the Administration application.
PBX Name for AES	CMSWITCH		The SwitchConnection name of the AE Services server associated with the Telephony server.
EC500 Enable Code	*88		The feature access code used by the Telephony server to enable Extension to Cellular on Avaya one-X® Portal, for example, *88,

Property name	Property values		Notes
	Example value	Your value	
			*89, *87. Contact the local Communication Manager administrator to get the code configured on the system.
EC500 Disable Code	*89		The feature access code used by the Telephony server to enable Extension to Cellular on Avaya one-X® Portal, for example, *88, *89, *87. Contact the local Communication Manager administrator to get the code configured on the system.
EC500 Modify Code	*87		The feature access code used by the Telephony server to enable Extension to Cellular on Avaya one-X® Portal, for example, *88, *89, *87. Contact the local Communication Manager administrator to get the code configured on the system. This code is also known as the Extension to Cellular self-administer code.
Host	###.###.###.###		The network address of the server as an IP address (of the CLAN card) or a DNS host name. This IP address is the Communication Manager IP address that is accessible by the clients, where the VOIP client establishes the VOIP (H.323) connection. Thus, the VOIP connection is established using the CLAN IP address. Since VOIP connection in Avaya one-X® Portal requires Communication Manager to support G.711 codec, CLAN should be configured to support G.711.
AES Servers - Available	aeserver1		The handles of the AE Services servers configured on Avaya one-X® Portal.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.

Configuration worksheet for Modular Messaging

This worksheet lists the information that you need to configure Modular Messaging for Avaya one-X® Portal. You need these values to configure the Voice Messaging server in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	mmhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago MM Server		A short description of the server that uniquely identifies the Voice Messaging server. You must create this value in the Administration application.
Initial Number of Server Connections	50		The minimum number of Avaya one-X® Portal user connections needed to communicate with the Voice Messaging server of the MSS of the Modular Messaging server. This value is not available in Modular Messaging. You must create this value in the Administration application.
Client Connections Increment	2		The number of times to increment the connections based on the number of users in the connections. For example, if this value is 2 and there are 100 users per connection, the connections are incremented every 200 users. This value is not available in Modular Messaging. You must create this value in the Administration application.
Users Per Client Connection	10		The number of users assigned per connection to the Voice Messaging server. This value is not available in Modular Messaging. You must

Property name	Property values		Notes
	Example value	Your value	
			create this value in the Administration application.
Messages Temp Directory	/tmp or / msgWorkDir		The location of the temporary directory where sections of voice mail message are stored. When creating a new Voice Messaging server, enter either the name of the default directory /msgWorkDir or the name of the directory you created for the Voice Messaging server. See Creating a directory for the Voice Messaging server. This value is not available in Modular Messaging. You must create this value in the Administration application.
Temp Purge Interval	60		The number of minutes that the sections of voice mail messages can remain in storage before the temporary directory is purged and the sections are deleted. This value is not available in Modular Messaging. You must create this value in the Administration application.
Mail Domain	server.xyzcorp .com		The fully qualified domain name of the MSS of the Modular Messaging server.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.
IMAP Host	###.###.###.###		The network address of the MSS of the Modular Messaging Server. This field must include an IP address, not a fully qualified domain name.
IMAP Port	993		The secure port number used by the **IMAP** configuration for the Voice Messaging server.
IMAP Login ID	oneXPIMAP		The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server**

Property name	Property values		Notes
	Example value	Your value	
			Name in your Voice Messaging server.
IMAP Password			The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Secure Port	Yes		If you select this option, Avaya one-X® Portal requires a secure **IMAP** connection for the Voice Messaging server. Verify that this port is the correct port for a secure connection.
SMTP Host	###.###.###.###		The network address of the MSS of the Modular Messaging Server.
SMTP Port	25		The port number used by the **SMTP** configuration for the Voice Messaging server.
SMTP Login ID	oneXPIMAP		The secure log-in ID used by the **SMTP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Password			The secure password associated with the log-in ID used by the **SMTP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Secure Port	Yes		If selected, indicates **SMTP** is configured to use a secure connection for the Voice Messaging server. A secure **SMTP** connection to the Voice Messaging server is optional.

Property name	Property values		Notes
	Example value	Your value	
LDAP Host	###.###.###.###		The network address of the MSS of the Modular Messaging Server. This field must include an IP address, not a fully qualified domain name.
LDAP Port	389		The port number used by the **LDAP** configuration for the Voice Messaging server. Use a nonsecure port.
LDAP Login ID	oneXPLDAP		The log-in ID used by the **LDAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
LDAP Password			The password associated with the log-in ID used by the **LDAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.

Configuration worksheet for Conferencing

This worksheet lists the information that you need to configure Conferencing for Avaya one-X® Portal . You need these values to configure the Conference services in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	mxhandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago Conf Server		A short description of the server that uniquely identifies the Conferencing server.

Property name	Property values		Notes
	Example value	Your value	
			You must create this value in the Administration application.
BCAPI Logger Directory	/tmp		The path name of the directory where information about **BCAPI** issues is stored. See Creating a directory for the Conferencing server. This value is not available in Conferencing. You must create this value in the Administration application.
Dial Plan	Dialplan		The handle of the Dial Plan used by this server.
BCAPI Host	###.###.###.###		The network address that the **BCAPI** configuration uses for the Conferencing server as an IP address or a DNS address.
BCAPI Login ID	username1		The log-in ID that the **BCAPI** configuration uses for the Conferencing server.
BCAPI Password			The password associated with the log-in ID that the **BCAPI** configuration uses for the Conferencing server.
BCAPI Secondary Login ID	username2		The **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.
BCAPI Password			The password associated with the **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.

Configuration worksheet for Presence

This worksheet lists the information that you need to configure Presence for Avaya one-X® Portal. You need these values to configure the Presence Services in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Type	apas		The type of server configured on the system. For the Presence Services displays apas.
Version	1.0		The version of the server configured on the system. For the Presence Services , displays 1.0.
Handle	ipshandle		The unique name assigned to the server by the administrator. You must create this value in the Administration application.
Description	Chicago IPS Server		A short description of the server that uniquely identifies the Presence Services. You must create this value in the Administration application.
Enabled	Yes		When selected by the administrator, enables the server for the system.
IPS Publish To Port	5061		The port number on the Presence Services where the presence information of the user is published. This is a remote port.
LPS Consumer Port	9072		The port number on the Presence Services that receives the consumer information. These are local ports where Avaya one-X® Portal is running.
LPS Supplier Port	9070		The port number on the Presence Services that furnishes the published the information. These are local ports where Avaya one-X® Portal is running.
UMS URL	http://localhost:9080/ums/services/UserMgmtServicePort		The URL that is used to access the Web based User Management Service.
LPS Host	###.###.###.###		The network address used by this configuration of the Local

Property name	Property values		Notes
	Example value	Your value	
			Presence Service as an IP address or a DNS address.
LPS Port	25061		The port number used by this configuration of the Local Presence Service. This is a remote port.
UMS Host	localhost		The network address used by this configuration of the User Management Service as an IP address or a DNS address.
UMS Port	7276		The port number used by this configuration of the User Management Service. These are local ports where Avaya one-X® Portal is running.
UMS Login ID	oneXPUMS		The log-in ID used by this configuration of the User Management Service.
UMS Password			The password associated with the log-in ID used by this configuration for the User Management Service.
UMS Confirm			Verification of the password associated with the log-in ID used by this configuration for the User Management Service.

Configuration worksheet for Dial Plan

This worksheet lists the information that you need to configure a dial plan for Avaya one-X® Portal . You need these values to configure the dial plan in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Handle	Dialplan		The unique name assigned to the server by the administrator.

Property name	Property values		Notes
	Example value	Your value	
			You must create this value in the Administration application.
Phone Numbers PBX Main	15555551234		A sample of a valid telephone number on the switch. The Dial Plan compares this number with other telephone numbers to determine whether a telephone number is internal or external.
Phone Numbers Automatic Routing Service	9		The digit to prefix before an outbound phone number is dialed on the PBX. For example, in the phone number 9-1-800-8888, 9 is the **Automatic Routing Service** number.
Prefixes Regional	1555		The area code of the region.
Prefixes Inter-Regional	1		The digit to dial between area codes in an **Inter-Regional** phone call.
Prefixes International	011		The digits to prefix to place an **International** phone call. For example, in the phone number 011-1-800-8888, 011 is the **International** prefix code.
Number of Digits National Call Maximum	10		The maximum number of digits allowed in a domestic telephone call. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Local Call	7		The maximum number of digits in a telephone call within an area code. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Extension to Extension Call	5		The maximum number of digits allowed in a phone extension at the enterprise. Typically, this value is 7 or less.

Configuration worksheet for Mobility Extension Bank

This worksheet lists the information that you need for the Mobility Extension Bank. You need these values to configure the Mobility Extension Bank in the Administration application.

Property name	Property values		Notes
	Example value	Your value	
Telephony Server	Telephony Provider1		The unique name assigned to the Telephony server associated with the Mobility Extension Bank .
Description	Chicago MEB		The unique name assigned to the Mobility Extension Bank . You must create this value in the Administration application.
Extension to Extension Call			The maximum number of digits allowed in a phone extension at the enterprise. Typically, this value is 7 or less.
1st Extension	4990001		The first extension phone number to which you want to map the Mobility Extension Bank .
# To Add	5		The number of extensions to add. For example, if this extension in the **1st Extension** field is 5500, and the number to add is 5, the system adds extensions 5500, 5501, 5502, 5503, and 5504.
Password			Enter a password for each of the extensions on the list for security purposes.

Configuration worksheet for Enterprise Directory server

This worksheet lists the information that you need about the Enterprise Directory server. You need these values to configure the Enterprise Directory domains in the Administration application.

Tip:

If the Avaya one-X® Portal deployment needs to support more than one Enterprise Directory domain, complete one of these worksheets for each domain.

You can configure each deployment to access information about users in up to four additional Active Directory domains. However, Avaya one-X® Portal considers the users in the

additional domains to be contacts only and does not obtain anything other than the address book data from them. You cannot provision users from the additional domains, and those users cannot log in to the Avaya one-X® Portal deployment.

Property name	Property values		Notes
	Example value	Your value	
Domain	<NNNNN>.xyz-corp.com		The name assigned to the domain in the Active Directory. For example, enter the **User** domain as <*NNNNN*>.xyz-corp.com, and the **Resource** domain as <*nnnn*>pptdomain.xyz-corp.com. The **Contact** domain is the same as the **User** domain. You can add Contact domain with another name. You cannot add a User or a Resource domain.
Type	User		Indicates how the domain is used. The same domain can be used in more than one way. • **User**. Indicates the domain contains the Avaya one-X® Portal users. There is only one user domain. You cannot change this domain. • **Resource**. Indicates the domain contains the Avaya one-X® Portal security groups. There is only one resource domain. You cannot change this domain. • **Contact**. Indicates the domain contains enterprise address book information. The user domain is always the first contact domain. You can add up to four more contact domains.
Primary Server	###.###.###.###		The IP address of the primary Directory server for the domain.
Has Backups	Yes		Indicates if there are secondary Directory servers for this domain by displaying Yes or No.

Property name	Property values		Notes
	Example value	Your value	
Host	###.###.###.###		The network address of the server as an IP address.
Port	389		The port number used by the server.
Login ID (Active Directory) **Bind DN** (other directories)	*admin_login*		The log-in ID used by the server.
Password (Active Directory) **Bind Password** (other directories)			The password associated with the Login ID used by the server.
Base DN	DC=entpm, DC=xyz, DC=corp, DC=com		The Distinguished Name (DN) of a node in the domain that identifies which part of the domain is used. If blank, the entire domain is used.
Page Size	50		The number of names returned by the Enterprise Directory server per query.
Range Size	500		The number of values for an attribute that are returned by the Enterprise Directory server per query. The attributes include names and phone numbers. For example, if a security group contains 1,000 members, you can retrieve the members 200 at a time.

Chapter 4: Validating the one-X Portal environment

Environment Validation tool

The Avaya one-X® Portal Environment Validation tool tests that the systems you have just configured will be able to communicate with Avaya one-X® Portal. You can find this tool in the Tools directory of the Avaya one-X® Portal DVD-ROM.

When to run the Environment Validation tool

Run the Environment Validation tool after you configure the prerequisites for Avaya one-X® Portal and before you install Avaya one-X® Portal.

Related topics:

[Tests performed by the Environment Validation tool](#) on page 89
[Log created by the Environment Validation tool](#) on page 90
[Sample log file for the Environment Validation tool](#) on page 90

Tests performed by the Environment Validation tool

Voice Messaging

Performs the following tests to validate the Modular Messaging configuration:

- Checks the connectivity to the host and validates the credentials.
- If configured, validates the SSL configuration.
- Checks for messages in a voice mail box.

TSAPI

Performs the following tests to validate the connection between AE Services and Communication Manager:

- Checks that the Service Name is valid.
- Checks the connectivity to the host and validates the credentials.
- Dials a call from a source to a destination.
- Place the call on hold and then drops the call.

DMCC

Performs the following tests to validate the Communication Manager configuration:

- Checks the connectivity to the host and validates the credentials.
- Makes a call.
- Presses keypad buttons and places the call on-hook.

Conferencing

Performs the following tests to validate the Conferencing configuration:

- Connects to the conference bridge and validates the credentials.
- Starts a conference.
- Calls the moderator.
- Closes the conference and drops all the calls.

Log created by the Environment Validation tool

The Environment Validation tool checks each prerequisite system sequentially. The log file layout does not mix results from different components.

The log includes information about the tests that were performed and the results of those tests. If a test failed, the log provides as much detail as possible about the reason for the failure. After all validation tests are completed, the final section of the log summarizes all of the test results.

You can view a summary of the test results in the final screen of the Environment Validation tool. The Environment Validation tool also outputs a more detailed log file.

Sample log file for the Environment Validation tool

The following is an example of the test results that display in the final screen of the Environment Validation tool after all tests have been run.

```
Starting Configuration Utility.
                                        Voice Messaging
Voice Messaging - running tests......
Voice Messaging: Check Connectivity - Success.
Voice Messaging: Check Messages in Mail Box - Success.
                                        TSAPI
TSAPI - running tests......
TSAPI: Check Initialization - Success.
TSAPI: Login - Success.
TSAPI: Call and Hangup - Failed. failure to monitor device.
                                        DMCC
DMCC - running tests......
DMCC: Initialization - Success.
DMCC: Check Making,OnHook and Dropping a call - Success.
                                        Conferencing
```

```
Conferencing - running tests......
Conferencing: testBridgeConnection
Conferencing: Check Connection - Success.
Conferencing: Dial Moderator - Success.
For more details see the output file (env-validation-tool.log)
```

Installing the Environment Validation tool

Prerequisites

Before you run the Environment Validation tool, you must install the tool and the IBM Java Runtime SDK on the Avaya one-X® Portal server.

1. On the Avaya one-X® Portal DVD-ROM, navigate to the Tools directory and open the `conftool.zip` file.
2. Unzip the Environment Validation tool in a destination directory on the Avaya one-X® Portal server.
3. Open a terminal window and navigate to the directory where you unzipped the Environment Validation tool.
4. Execute the following command to install the IBM Java Runtime SDK: **`rpm -i ibm-java2-i386-sdk-5.0-6.0.i386.rpm`**
5. Execute the following command to add the IBM Java Runtime SDK to your PATH: **`PATH=/opt/ibm/java2-i386-50/bin:$PATH`**

Configuring the TSAPI.PRO file for the Environment Validation tool

The Environment Validation tool uses the contents of a `TSAPI.PRO` file to determine how to access the TSAPI servers used for AE Services. The `TSAPI.PRO` file is in the zip file with the Environment Validation tool.

If this file does not list an AE Services machine or other machine that includes a TSAPI server, the Environment Validation tool cannot test communications with that machine.

Note:

Ignore the line in the `TSAPI.PRO` which states that the file must be located in a CLASSPATH directory. You do not need to move the `TSAPI.PRO` file for the Environment Validation tool.

1. In a terminal window on the machine that will host Avaya one-X® Portal, navigate to the directory where you unzipped the Environment Validation tool.
2. Open the `TSAPI.PRO` file.
3. Use the format of the example server in the file and add an entry at the end for each AE Services and TSAPI server that will be integrated into the Avaya one-X® Portal deployment.

Example

The following is an example of the `TSAPI.PRO` file.

```
#tsapi.pro
#
# This file must be located in one of the directories found in CLASSPATH
#
# This is a list of the servers offering Telephony Services via TCP/IP.
# Either domain name or IP address may be used; default port number is 450
# The form is: host_name=port_number   For example:
#
# tserver.mydomain.com=450
# 127.0.0.1=450
#
# (Remove the '#' when creating actual server entries. Replace xxx with the
# appropriate section of the IP address of the machine.)
xxx.xxx.xxx.xxx=450
xxx.xxx.xxx.xxx=450
```

Configuring the logs for the Environment Validation tool

You can configure the `log4j.txt` file for the Environment Validation tool to change the following:

- Directory where the Environment Validation tool creates the log file.
- Log level.
- Format of the log output.

1. In a terminal window, navigate to the directory where you unzipped the Environment Validation tool.
2. Open the `log4j.txt` file.
3. To change the location or the name of the log file, change the path or name in the following line: **`log4j.appender.R.File=`***path*/*name*`.log`**
4. To send the log output to the console, make sure that the following line includes **`stdout`**: **`log4j.rootLogger=debug, stdout, R`**
5. To stop sending the output to the console, remove **`stdout`** from the line.
6. To change the log level, replace **`debug`** in the following line with another log level: **`log4j.rootLogger=debug, stdout, R`**

   The available log levels are:

   - debug
   - info
   - warn
   - error
   - fatal
7. To change the format of the log, replace the variables in the following line: **`log4j.appender.R.layout.ConversionPattern=`***%d - %m%n*

   Where *%d* includes the date and time, - *%m* includes the log output, and *%n* is a line separator.
8. Save the `log4j.txt` file.

Running the Environment Validation tool

Prerequisites

Before you run the Environment Validation tool:

- Configure the prerequisites for Avaya one-X® Portal.
- Install the Environment Validation tool and the IBM Java Runtime SDK on the Avaya one-X® Portal server.
- Configure the `TSAPI.PRO` file.
- Run the Environment Validation tool either at the server itself or within X-Windows or use the VNC client, if you want to execute it from a remote machine.

1. In a terminal window on the machine that hosts Avaya one-X® Portal, navigate to the directory where you unzipped the Environment Validation tool.
2. Execute the following command to give permissions to run the tool: **chmod 755 run.sh**
3. Execute the following command to start the Environment Validation tool: **./run.sh**
4. On the first screen, select one or more of the following options to configure the components you want to validate:
   - **Voice Messaging**
   - **TSAPI**
   - **DMCC**
   - **Conferencing**
5. As you move through the Environment Validation tool, complete the fields for the configurations that you selected, click **Save**, then click **Next** to move to the next screen.

Configuration	Field descriptions
Voice Messaging	Voice Messaging on page 95
TSAPI	TSAPI Configuration on page 96
DMCC	DMCC Configuration on page 96
Conferencing	Conferencing Configuration on page 97

6. After you complete all of the configuration fields for the components you selected, click **Save&Run** on the last screen.

Result

By default, the Environment Validation tool displays a summary of the test results in the final screen of the Environment Validation tool. The Environment Validation tool also outputs more detailed results in an `env-validation-tool.log` file. By default, the `env-validation-tool.log` file is created in the same directory as the Environment Validation tool.

Environment Validation tool interface

- DMCC Configuration on page 96
- Conferencing Configuration on page 97

Tip:

Some of the values required by the Environment Validation tool are the same values that you entered in the configuration worksheets.

Voice Messaging

Property Name	Property values		Notes
	Example value	Your value	
IMAP Host	###.###.###.###		The network address of the MSS of the Modular Messaging Server. This field must include an IP address, not a fully qualified domain name.
IMAP Port	993		The secure port number used by the **IMAP** configuration for the Voice Messaging server.
IMAP Login ID	oneXPIMAP		The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Password			The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Secure Port	True		If you select this option, Avaya one-X® Portal requires a secure **IMAP** connection for the Voice Messaging server. If you use a secure port, verify that the **IMAP Port** is the correct port for a secure connection.

Property Name	Property values		Notes
	Example value	Your value	
Mailbox Number	40000409		Number of a Modular Messaging mailbox that the Environment Validation tool can use to send a test message.
Mailbox User ID	40000409		User ID associated with the mailbox.
Mailbox Password			Password associated with the mailbox.

TSAPI Configuration

Property Name	Property values		Notes
	Example value	Your value	
Service	*CORP#BUILDING#CSTA#NNNN33333*		A drop-down list of available TSAPI services. This test requires the option that includes the hostname of the AE Services server used by Avaya one-X® Portal.
Login ID	admin_login		The log-in ID used by the **TSAPI** configuration for the AE Services server.
Password			The password associated with the log-in ID used by the **TSAPI** configuration for the AE Services server.
Source Phone Number			The source telephone number that will make the test call.
Destination phone number			The destination telephone number that will receive the test call.

DMCC Configuration

Property Name	Property values		Notes
	Example value	Your value	
DMCC Host	###.###.###.###		The network address used by the **DMCC** configuration for the AE Services server as an

Property Name	Property values		Notes
	Example value	Your value	
			IP address or a DNS address.
DMCC Port	4721		The port number used by the **DMCC** configuration for the AE Services server.
DMCC Login ID	cmapi		The log-in ID used by the **DMCC** configuration for the AE Services server.
DMCC Password			The password associated with the log-in ID used by the **DMCC** configuration for the AE Services server.
Telecommuter Address	###.###.###.###		IP address of the Call Server.
Telecommuter Extension	4000439		The extension number to use for the telephone call test.
Extension Password			Password for the extension.
Telecommuter Number	915553331234		Telecommuter number that will make the test telephone call.
Call Appearance Number	265		Call appearance number to use in the test telephone call.
Destination Number	4000481		The destination telephone number that will receive the test call.

Conferencing Configuration

Property Name	Property values		Notes
	Example value	Your value	
BCAPI Host	###.###.###.###		The network address that the **BCAPI** configuration uses for the Conferencing server as an IP address or a DNS address.
BCAPI Login ID	username1		The log-in ID that the **BCAPI** configuration uses for the Conferencing server.

Property Name	Property values		Notes
	Example value	Your value	
BCAPI Password			The password associated with the log-in ID that the **BCAPI** configuration uses for the Conferencing server.
CRS Host	###.###.###.###		The network address used by the CRS configuration for the Meeting Exchange server as an IP address or a DNS address.
Is Open Conference			The method used to start the conference. The possible values are: • **True**: Dial automatically after the conference is open. • **False**: Do not dial automatically.
Moderator Code	11111		Host code to use to start the conference.
Moderator Phone Number	915553335678		If an open conference, telephone number the bridge should use to dial the conference host.

Chapter 5: Configuring the one-X Portal desktop

Administrator and user desktop prerequisite checklist

This checklist includes the hardware and software required for an administrator or user to run a Avaya one-X® Portal application on a supported operating system.

Important:

Implementing Avaya one-X Portal assumes that all required hardware will be in place, and all required software will be up and running before you implement Avaya one-X® Portal.

- Windows desktop on page 32
- Mac desktop on page 32
- Linux desktop on page 32

Windows desktops

Requirement	Value		✔
Desktop hardware	**Processor**	Two quad-core processors 1.86 GHz or higher	
	Memory	12 GB RAM	
	Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)	
	Sound card	As provided with computer	
	Network card	100 Mbps/1Gbps	
Peripherals	**Monitor**	Video adapter and monitor with Super VGA (800 x 600) or higher resolution	
	Required accessories	Keyboard and a mouse (or compatible pointing device)	

Requirement	Value	✔
	Optional accessories Microphone and speakers, or headphones with a microphone	
Operating system	• Microsoft Windows XP SP2 • Microsoft Windows 2003 • Microsoft Windows Vista 32 and 64 bit	
Web browser	• Mozilla Firefox 2 • Mozilla Firefox 3 • Microsoft Internet Explorer 6.0 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0 • Apple Safari 3.1 • Apple Safari 3.2 • Apple Safari 4.0	
Email application	Microsoft Outlook 2003 and 2007 Not required for Administration application.	
SMS application (optional)	SMS Client software Not required for Administration application.	
VOIP (This Computer)	Software installed with one-X Portal Not required for Administration application.	
Avaya one-X Portal Extensions	When installed from one-X Portal or via SMS Not required for Administration application.	

Mac desktops

Requirement	Value	✔
Desktop hardware	**Processor** Two quad-core processors 1.86 GHz or higher **Memory** 12 GB RAM **Hard drive** 40 GB (10 GB free space in /tmp and 21 GB free space in /) **Sound card** As provided with computer **Network card** 100 Mbps/1Gbps	

Requirement	Value		✔
Peripherals	**Monitor**	Video adapter and monitor with Super VGA (800 x 600) or higher resolution	
	Required accessories	Keyboard and a mouse (or compatible pointing device)	
	Optional accessories	Microphone and speakers, or headphones with a microphone	
Operating system	Apple OS X V10.5		
Web browser	• Mozilla Firefox 2 • Mozilla Firefox 3 • Apple Safari 3.1 • Apple Safari 3.2 • Apple Safari 4.0		
Email application	Not supported		
SMS application (optional)	Not supported		
VOIP (This Computer)	Supported		
Avaya one-X Portal Extensions	Not supported		

Linux desktops

Requirement	Value		✔
Desktop hardware	**Processor**	Two quad-core processors 1.86 GHz or higher	
	Memory	12 GB RAM	
	Hard drive	40 GB (10 GB free space in /tmp and 21 GB free space in /)	
	Sound card	As provided with computer	
	Network card	100 Mbps/1Gbps	

Requirement	Value		✔
Peripherals	**Monitor**	Video adapter and monitor with Super VGA (800 x 600) or higher resolution	
	Required accessories	Keyboard and a mouse (or compatible pointing device)	
	Optional accessories	Microphone and speakers, or headphones with a microphone	
Operating system	Red Hat Enterprise Linux Desktop 4 Update 4, 32 bit		
Web browser	• Mozilla Firefox 2 • Mozilla Firefox 3		
Email application	Not supported		
SMS application (optional)	Not supported		
VOIP (This Computer)	Not supported		
Avaya one-X Portal Extensions	Not supported		

Creating instructions for users of Avaya one-X® Portal and the Administration application

Users do not need to install Avaya one-X® Portal or the Administration application. However, to simplify and improve the first experiences of users with these applications, Avaya recommends that you provide each user and administrator with a set of instructions.

If you want to note additional information in the checklists, modify the RTF versions of those checklists, available in the *Avaya one-X® Portal Implementation Workbook.*

1. Create instructions for users and for administrators that include the following:
   - Web page address for the application that the user needs to access.
   - The name of a person that users or administrators can contact if they encounter problems.

- Any other instructions that are specific to your corporate policies.

2. Complete and attach the following checklists, as appropriate for the Administration application and Avaya one-X® Portal users:
   - User Worksheet: getting started with Avaya one-X Portal on page 103
   - Avaya one-X Portal and Administration application configuration checklist on page 105
   - User worksheet: installing one-X Portal Extensions on page 104
3. Distribute the appropriate set of instructions to each group of users and administrators.

User Worksheet: getting started with Avaya one-X® Portal

This worksheet lists information you need to log into Avaya one-X® Portal for the first time.

If you have any questions about the information in this worksheet, consult your supervisor or the contact person provided with this worksheet.

Information	Values
Web page address for Avaya one-X® Portal	
Your login ID	
Information for your telephone settings	
Display name to be shown in Avaya one-X® Portal	
Your telephone extension number	
Password for your extension	
Information for your conferencing settings	
Display name to be shown in Avaya one-X® Portal	
Primary telephone number for your bridge	
Alternate telephone number for your bridge, such as a toll-free number	
Host or moderator code for your bridge	
Participant code for your bridge	
Personal Identification Number (PIN) for your bridge, if used.	

User worksheet: installing one-X Portal Extensions

The connection to one-X Portal is configured when the one-X Portal Extensions are installed. If you encounter problems with this connection, review and correct the connection settings. If you do not know the information required to complete these fields, consult your supervisor.

Property Name	Property values		Notes
	Example value	Your value	
Scheme	HTTP		The internet protocol scheme at the beginning of the Web address that you use to access one-X Portal. The installer automatically completes this field.
Server	onexportal.domain.com		The server that hosts Avaya one-X® Portal. You must enter the IP address or the fully-qualified domain name of the server. The installer does not automatically complete this field. This information is part of the Web page address for one-X Portal.
Port	80		The port that the one-X Portal Extensions uses to communicate with Avaya one-X® Portal. The installer automatically completes this field.
Context Root			The location of the one-X Portal software on the Avaya one-X® Portal server. The installer automatically completes this field.
Window Title	one-X Portal		The title displayed in one-X Portal. The installer automatically completes this field.

Avaya one-X Portal and Administration application configuration checklist

This checklist summarizes the configuration steps required for one-X Portal and Administration application prerequisites.

Tip:

Avaya recommends that you complete this configuration before you run the Avaya one-X® Portal Installation Wizard.

#	Task	Internet Explorer	Firefox	Safari
1	Configure the browser to include Avaya one-X® Portal in the Local Intranet security zone.	Setting the security zone in Internet Explorer on page 106	Not applicable.	Not applicable.
2	Configure all pop-up blockers to allow pop-ups for Avaya one-X® Portal.	Configuring pop-up blockers on page 106	Configuring pop-up blockers on page 106	Configuring pop-up blockers on page 106
3	Turn off the **Script Debugging** option for JavaScript errors.	Setting advanced browsing options in Internet Explorer on page 107	Not applicable.	Not applicable.
4	Turn off the **Reuse windows for launching shortcuts** browsing option.	Setting advanced browsing options in Internet Explorer on page 107	Not applicable.	Not applicable.
5	Enable JavaScript.	Not applicable.	Setting JavaScript options in Firefox on page 108	Configuring Safari on page 108
6	Configure proxy	Not applicable.	Not applicable.	Configuring Safari on page 108
7	For users on Citrix only, disable **Download signed**	Configuring Internet Explorer for Citrix access on page 107	Not applicable.	Not applicable.

#	Task	Internet Explorer	Firefox	Safari
	ActiveX controls in Internet Explorer.			

Configuring pop-up blockers

You must configure all pop-up blockers, including pop-up blockers in the Web browser, in browser toolbars, and in Internet security applications.

Configure all pop-up blockers to allow pop-ups for the Avaya one-X® Portal server.

Setting the security zone in Internet Explorer

Updates by Microsoft to Internet Explorer may result in changes to this procedure. If these steps or options do not match what you see in your Web browser, see the online help provided by Microsoft.

1. In Internet Explorer, click **Tools** > **Internet Options**.
2. On the **Security** tab, click **Local intranet**, then click **Sites**.
3. In the Local intranet dialog box:
   a. Make sure that all check boxes are selected.
   b. Click **Advanced**.
4. In the advanced Local intranet dialog box:
   a. In the **Add this Web site to the zone** field, type the address of the Web site that you use to access the Avaya one-X® Portal application.
   b. Do not select the **Require server verification (https:) for all sites in this zone** check box.
   c. Click **Add**.
   d. Click **Close**.

5. In the Local intranet dialog box, click **OK**.
6. In the Internet Options dialog box, click **OK**.

Setting advanced browsing options in Internet Explorer

Updates by Microsoft to Internet Explorer may result in changes to this procedure. If these steps or options do not match what you see in your Web browser, see the online help provided by Microsoft.

1. In Internet Explorer, click **Tools** > **Internet Options**.
2. On the **Advanced** tab, scroll down to the **Browsing** section.
3. Clear the following options:
   - **Disable script debugging (Internet Explorer)**
   - **Disable script debugging (Other)**
   - **Reuse windows for launching shortcuts (when tabbed browsing is off)**

   If you do not disable **Reuse windows for launching shortcuts (when tabbed browsing is off)**, Internet Explorer launches a new Web site in the Avaya one-X® Portal window. You need to log back in to return to Avaya one-X® Portal.
4. In the Internet Options dialog box, click **OK**.

Configuring Internet Explorer for Citrix access

Problems can occur if you install any of the supporting applications on your desktop computer when you log in to Avaya one-X® Portal. To avoid these problems, use the following procedure to disable the **Download signed ActiveX controls** option in Internet Explorer.

Updates by Microsoft to Internet Explorer may result in changes to this procedure. If these steps or options do not match what you see in your Web browser, see the online help provided by Microsoft.

1. In your Citrix client, connect to the Avaya one-X® Portal Internet Explorer session.
2. In Internet Explorer, click **Tools** > **Internet Options**.

3. On the **Security** tab, click **Local intranet**, then click **Custom level**.
4. In the **ActiveX controls and plug-ins** section, click **Disable** under the **Download signed ActiveX controls** option.
5. Click **OK**.
6. In the Internet Options dialog box, click **OK**.

Setting JavaScript options in Firefox

Updates by Mozilla to Firefox may result in changes to the following instructions. If these steps or options do not match what you see in your Web browser, see the online help provided by Mozilla.

1. In Firefox, click **Tools** > **Options**.
2. In the Options dialog box, click **Content**.
3. Select the **Enable JavaScript** check box.
4. Click **Advanced**.
5. In the Advanced JavaScript Settings dialog box:
   a. Select all check boxes.
   b. Click **OK**.
6. In the Options dialog box, click **OK**.

Configuring Safari

Updates by Apple to Safari may result in changes to the following instructions. If these steps or options do not match what you see in your Web browser, see the online help provided with Safari.

1. On the **Safari** menu, click **Preferences**.
2. In the Preferences dialog box, click **Security**.
3. Select the **Enable JavaScript** check box.

4. Clear the **Block Pop-up Windows** check box.
5. In the **Preferences** dialog box, click **Advanced**.
6. In the **Proxies** area, click **Change Settings...**.
7. In the Network dialog box, exclude the Avaya one-X® Portal server either explicitly or implicitly.
8. In the Network dialog box, add the address of the Web site that you use to access the Avaya one-X® Portal application to the **Bypass proxy settings for these Hosts & Domains** field to explicitly exclude the Avaya one-X® Portal server.
9. In the Network dialog box, click **Apply Now**.
10. In the Preferences dialog box, click **OK**.

Configuring proxy for Internet Explorer

1. In Internet Explorer, click **Tools** > **Internet Options**.
2. On the **Connections** tab, click **LAN settings**.
3. In the Local Area Network (LAN) Settings dialog box, select the **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)** and **Bypass proxy server for local addresses** check boxes.
4. Click **Advanced**.
5. In the Proxy Settings window, type `Add` *`IP address of the proxy server`* in the text box labeled **Do not use proxy server for addresses beginning with**. For example, for Avaya network, type `Add 135.*.*.*`
6. Click **OK** to save the settings.
7. In the Local Area Network (LAN) Settings dialog box, click **OK**.
8. In the Internet Options dialog box, click **OK**.

Configuring proxy for Mozilla Firefox

1. In Firefox, click **Tools** > **Options**.
2. In the Options dialog box, click **Advanced**.
3. Click **Network** .
4. Click **Settings**.
5. In Connection Settings dialog box, click **Manual proxy configuration**.
6. Type `Add 135.*.*.*` in **No Proxy for** text box.
7. Click **OK** to save proxy settings for Firefox.
8. In the Options dialog box, click **OK**.

Chapter 6: Installing one-X Portal

Installation worksheet: network information for servers

This worksheet lists information about the network settings on the servers that host Avaya one-X® Portal and the integrated component. If you do not know or cannot access the information on the server, contact your network administrator.

If you want to note additional information for a server, modify the table in the RTF version of this worksheet in the *Avaya one-X® Portal Implementation Workbook*.

Note:

Depending upon how and when the Avaya one-X® Portal server is added to the network, you may need to configure some or all of these values on the server. If you have any questions, consult your network administrator.

Property Name	Values
Avaya one-X® Portal server	
IP Address	
Subnet Mask	
Gateway	
Host name	
DNS domain	
NTP server	
Root username	
Password for root username	
Avaya AE Services server	
IP Address	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	

Property Name	Values
Password for login ID	
Avaya Communication Manager server	
IP Address	
Host name	
DNS domain	
NTP server	
ASA login ID	
Password for ASA login ID	
Avaya Modular Messaging server	
IP Address	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
Avaya Conferencing server	
IP Address	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
Presence Services server	
IP Address	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
Active Directory server	
IP Address	

Property Name	Values
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
IBM Domino Directory server	
IP Address	
Host name	
NTP server	
Bind DN ID	
Password for Bind DN ID	
Novell eDirectory server	
IP Address	
Host name	
NTP server	
Bind DN ID	
Password for Bind DN ID	
SUN ONE Directory Server	
IP Address	
Host name	
NTP server	
Bind DN ID	
Password for Bind DN ID	
If not hosted on Avaya one-X® Portal server, Avaya WebLM server	
IP Address	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	

Installation worksheet: information required by Installation Wizard

This worksheet lists the information that you need to install Avaya one-X® Portal. The information and properties follow the same organization as the Installation Wizard.

Required administrator privileges

To run the Avaya one-X® Portal Installation Wizard, you must use a Linux account with root user privileges for the machine that will host Avaya one-X® Portal.

Installation configuration information

Avaya does not recommend that you use the values in the Example value column. For security purposes, use unique values when you configure Avaya one-X® Portal.

Property Name	Property values		Notes
	Example value	Your value	
Avaya one-X® Portal database configuration			
Instance Username	dbinst		This account has full privileges for the Avaya one-X® Portal database, including SYSADM. Avaya one-X® Portal requires the Instance username to connect to and create the database. This user ID must be unique. To meet database requirements, this username cannot have more than 8 characters. You must create this value in the Installation Wizard.
Instance Password			Password for the instance username account. You must create this value in the Installation Wizard.
Admin Username	dbadmin		This account has full privileges for the Avaya one-X® Portal database. Avaya one-X® Portal requires the Admin username to configure and access the database. To meet database requirements, this username cannot have more than 8 characters.

Property Name	Property values		Notes
	Example value	Your value	
			You must create this value in the Installation Wizard.
Admin Password			Password for the Admin username account. You must create this value in the Installation Wizard.
Fence Username	dbadmin		This account has privileges to administer the Avaya one-X® Portal database. Avaya one-X® Portal requires the Fence username to run stored procedures on the database. To meet database requirements, this username cannot have more than 8 characters. You must create this value in the Installation Wizard.
Fence Password			Password for the Fence username. You must create this value in the Installation Wizard.
Read-only Instance Username	roinst		This account has read-only privileges for the Avaya one-X® Portal database. Avaya one-X® Portal requires this read-only instance username to connect to and read the database. To meet database requirements, this username cannot have more than 8 characters. You must create this value in the Installation Wizard.
Read-only Instance Password			Password for the read-only instance username. You must create this value in the Installation Wizard.
Avaya one-X® Portal application server configuration			
App Server Username	appsvr		Avaya one-X® Portal uses this account to log into and run the Avaya one-X® Portal application server. This account has full privileges for the application server, including rights to start and stop the server.

Property Name	Property values		Notes
	Example value	Your value	
			To meet application server requirements, this username cannot have more than 8 characters. You must create this value in the Installation Wizard.
App Server Password			Password for the App Server username account. You must create this value in the Installation Wizard.
Avaya WebLM configuration: required only if system uses remote WebLM			
WebLM URL	See Notes for example.		Optional. Not required if you install the WebLM with Avaya one-X® Portal. URL of the server page for the WebLM. The WebLM URL is case-sensitive. Example: `http://<machine_name>.<domain>:<WebLM_port>/WebLM/` **Important:** Application Enablement Services requires a dedicated WebLM. Do not install the Avaya one-X® Portal license on the WebLM used by Application Enablement Services.
Microsoft Active Directory configuration			
Active Directory user domain and resource domain			Are users and groups in the same Active Directory domain or in separate Active Directory domains? If the Enterprise Directory has users defined in one domain and security groups defined in another domain, the Installation Wizard presents you with two Enterprise Directory configuration screens. Configure the user domain in the first screen. Configure the resource

Property Name	Property values		Notes
	Example value	Your value	
			domain for security group in the second screen.
Enterprise Directory IP Address	*###.###.###.###*		IP address of the computer that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	*users.domain.xyzcorp.com* *groups.domain.xyzcorp.com*		Fully qualified domain name configured on the Enterprise Directory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.
Enterprise Directory Username	*admin_service_user*		Enterprise Directory user that you created for the Avaya one-X® Portal administrative service account.
Enterprise Directory Password			Password for the Avaya one-X® Portal administrative service account.
For a split domain topology, resource domain: **Enterprise Directory IP Address**	*###.###.###.###*		IP address of the computer that hosts the Enterprise Directory server.
For a split domain topology, resource domain: **Enterprise Directory Port**	389		Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
For a split domain topology, resource domain: **Enterprise Directory Domain**	*users.domain.xyzcorp.com*		Fully qualified domain name configured on the Enterprise Directory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.

Property Name	Property values		Notes
	Example value	Your value	
For a split domain topology, resource domain: **Enterprise Directory Username**	*sec_admin_service_user*		Enterprise Directory user that you created for the Avaya one-X® Portal administrative service account. This is the secondary administration service account.
For a split domain topology, resource domain: **Enterprise Directory Password**			Password for the Avaya one-X® Portal administrative service account.
Admin Group	cn=onexpAdmin,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the administrator security group to assign permissions to users who will administer Avaya one-X® Portal in the Administration application.
Audit Group	cn=onexpAudit,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the Avaya one-X® Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the Avaya one-X® Portal configuration in the Administration application.
User Group	cn=onexpUser,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the user security group to assign permissions to users who will access the Avaya one-X® Portal application.
Presence Group	cn=onexpPresenceUser,ou=Groups,dc=Company,dc=com or Select **Everybody** if you want to select All Enterprise Users.		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the Avaya one-X® Portal application. See Configuring non- Avaya one-X Portal users in the Presence group on page 74

Property Name	Property values		Notes
	Example value	Your value	
	Note: Selecting **Everybody** bypasses the Base DN selected for presence user group. This also eliminates the need to have all users populated in the presence users group in LDAP and can be administered and controlled by Avaya one-X® Portal Administration.		
IBM Domino Directory configuration			
Enterprise Directory IP Address	###.###.###.###		IP address of the computer that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
Bind DN	CN=username, O=organization		Enterprise Directory user that you created for the Avaya one-X® Portal administrative service account.
Enterprise Directory Password			Password for the Avaya one-X® Portal administrative service account.
For a split domain topology, resource domain: **Enterprise Directory IP Address**	###.###.###.###		IP address of the computer that hosts the Enterprise Directory server.

Property Name	Property values		Notes
	Example value	Your value	
For a split domain topology, resource domain: **Enterprise Directory Port**	389		Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
Admin Group	cn=onexpAdmin,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the administrator security group to assign permissions to users who will administer Avaya one-X® Portal in the Administration application.
Audit Group	cn=onexpAudit,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the Avaya one-X® Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the Avaya one-X® Portal configuration in the Administration application.
User Group	cn=onexpUser,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the user security group to assign permissions to users who will access the Avaya one-X® Portal application.
Presence Group	cn=onexpPresenceUser,ou=Groups,dc=Company,dc=com or Select **Everybody** if you want to select All Enterprise Users. **Note:** Selecting **Everybody** bypasses the Base DN selected for		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the Avaya one-X® Portal application. See Configuring non- Avaya one-X Portal users in the Presence group on page 74

Property Name	Property values		Notes
	Example value	Your value	
	presence user group. This also eliminates the need to have all users populated in the presence users group in LDAP and can be administered and controlled by Avaya one-X® Portal Administration.		
Novell eDirectory configuration			
Enterprise Directory IP Address	###.###.###.###		IP address of the computer that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	*users.domain.xyzcorp.com* *groups.domain.xyzcorp.com*		Fully qualified domain name configured on the Enterprise Directory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.
Bind DN	CN=username, O=organization		Enterprise Directory user that you created for the Avaya one-X® Portal administrative service account.
Enterprise Directory Password			Password for the Avaya one-X® Portal administrative service account.
Admin Group	cn=onexpAdmin,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the administrator security group to assign permissions to users who will administer Avaya one-X® Portal in the Administration application.

Property Name	Property values		Notes
	Example value	Your value	
Audit Group	cn=onexpAudit,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the Avaya one-X® Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the Avaya one-X® Portal configuration in the Administration application.
User Group	cn=onexpUser,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the user security group to assign permissions to users who will access the Avaya one-X® Portal application.
Presence Group	cn=onexpPresenceUser,ou=Groups,dc=Company,dc=com or Select **Everybody** if you want to select All Enterprise Users. **Note:** Selecting **Everybody** bypasses the Base DN selected for presence user group. This also eliminates the need to have all users populated in the presence users group in LDAP and can be administered and controlled by		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the Avaya one-X® Portal application. See Configuring non- Avaya one-X Portal users in the Presence group on page 74

Property Name	Property values		Notes
	Example value	Your value	
	Avaya one-X® Portal Administration.		
Sun One Directory Server configuration			
Enterprise Directory IP Address	###.###.###.###		IP address of the computer that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	*users.domain.xyzcorp.com* *groups.domain.xyzcorp.com*		Fully qualified domain name configured on the Enterprise Directory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.
Bind DN	At installation, enter uid=username, ou=People, dc=company, dc=com		Enterprise Directory user that you created for the Avaya one-X® Portal administrative service account.
Enterprise Directory Password			Password for the Avaya one-X® Portal administrative service account.
Admin Group	cn=onexpAdmin,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the administrator security group to assign permissions to users who will administer Avaya one-X® Portal in the Administration application.
Audit Group	cn=onexpAudit,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the Avaya one-X® Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the Avaya one-X® Portal

Property Name	Property values		Notes
	Example value	Your value	
			configuration in the Administration application.
User Group	cn=onexpUser,ou=Groups,dc=Company,dc=com		The Installation Wizard uses the user security group to assign permissions to users who will access the Avaya one-X® Portal application.
Presence Group	cn=onexpPresenceUser,ou=Groups,dc=Company,dc=com or Select **Everybody** if you want to select All Enterprise Users. **Note:** Selecting **Everybody** bypasses the Base DN selected for presence user group. This also eliminates the need to have all users populated in the presence users group in LDAP and can be administered and controlled by Avaya one-X® Portal Administration.		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the Avaya one-X® Portal application. See Configuring non- Avaya one-X Portal users in the Presence group on page 74

Installing Avaya one-X® Portal

Prerequisites

Complete all pre-installation and configuration worksheets and checklists, including the following:

- Environment validation checklist on page 41
- Server prerequisites checklist on page 43
- Installation worksheet: information required by Installation Wizard on page 114

If you install from a directory on a network machine, execute `chmod +x setup.bin` to add execution rights to `setup.bin`.

1. Login as root on the server that will host Avaya one-X® Portal.
2. Type `runlevel` to verify your run level is *5*
3. Type `df -h` to see the partitioning of the drive and directories.
4. Verify that the directory sizes are large enough.
5. Type `uname -a` to verify Linux is 32-bit and not 64-bit.

   Note:
   If Linux is 64–bit (which is not supported), the system output shows `X86_64` in the result.
6. Execute the following command to validate the version of Linux on the server: `cat /etc/redhat-release`
   The following is an example of the response returned by this command when executed on a linux machine running RHEL 5.3 Update 5.3: `Red Hat Enterprise Linux Server release 5.3 (Tikanga).`

   a. Verify that your response includes the following key items: `Red Hat Enterprise Linux Server release 5.3 (Tikanga).`

   b. If one or more of the key items are not correct, do not install Avaya one-X® Portal. Update the version of Linux to the correct version first.

   Note:
   You get a similar kind of response, even if the machine is running a different RHEL version.
7. If the one-X Portal DVD does not mount automatically, execute the following command: `mount /dev/cdrom /media/cdrom`

8. Execute the following commands to change the directory to the `cdrom` folder and launch the Installation Wizard. Run these commands on a terminal that has access to an X-Windows environment.
   - `cd /media/cdrom`

     Note:
     In the command `cd /media/cdrom`, depending on the hardware, the media could also be a *cdrecorder* or a *dvd*.
   - `./setup.bin`
9. Follow the installer prompts and enter the required information from the installation worksheet.

   Note:
   During an installation or upgrade, the installer may appear to be stuck at 95% or 100% completion for a prolonged period of time. This screen delay does not indicate that the installer has stopped responding . It may take 20 minutes before the status changes and the installation or upgrade completes.

Avaya one-X Portal Installation Wizard screens

Avaya one-X® Portal Installation Wizard

The Avaya one-X® Portal installation includes:

- Avaya one-X® Portal server
- Avaya Administration application
- Avaya one-X® Portal client applications
- Avaya one-X® Portal application server
- Avaya one-X® Portal database
- Avaya Web License Manager (Optional - you can use a remote WebLM)

Important:
To run the Avaya one-X® Portal Installation Wizard, you must use a Linux account with root user privileges.

The following buttons are available on all Installation Wizard screens:

Name	Description
Cancel	Cancels the installation of Avaya one-X® Portal and discards all information entered in the Installation Wizard.
Previous	Discards the information entered in the current screen and returns to the previous installer screen.
Next	Saves the information entered in the current screen and moves to the next installer screen.

End-user license agreement

Name	Description
I accept the terms of the license agreement	Records that you have agreed to the terms of the agreement and continues the Avaya one-X® Portal installation.
I do not accept the terms of this license agreement	The Avaya one-X® Portal Installation Wizardexits if you do not agree to the terms of the agreement.

Installation types

Name	Description
Typical	Avaya recommends that you select this installation type. Although this option provides a complete installation, only those components and services that you have configured for integration will function. Installs all Avaya one-X® Portal components, including: • Avaya one-X® Portal server • Avaya Administration application • Avaya one-X® Portal client applications • Avaya one-X® Portal application server • Avaya one-X® Portal database • Avaya Web License Manager (Optional - you can use a remote WebLM)
Custom	Allows you to select the Avaya one-X® Portal services that you want to install and run on the machine. Installs the selected services and all other Avaya one-X® Portal components.

Avaya one-X® Portal installation directory

Name	Description
Directory name	The directory where Avaya one-X® Portal will be installed. You can type in a new directory if you do not want to accept the default.
Browse	Allows you to navigate to the desired installation directory if you do not know the directory path.

Avaya Service user accounts for Avaya one-X® Portal

Avaya Support uses the Service user accounts to log in to your Avaya one-X® Portal server remotely and troubleshoot issues. The Service user accounts are the same secure accounts that are created to facilitate support of other Avaya products.

Name	Description
Yes. Create Avaya Service user accounts.	Creates the Avaya Service user accounts.
No. Do not create Avaya Service User accounts.	Does not create the Avaya Service user accounts.

Provision Avaya one-X® Portal users

You can allow users to configure their own telephone, messaging, and conferencing accounts in Avaya one-X® Portal, or you can have the administrators provision the all user accounts in the Administration application.

Name	Description
Yes. Allow users to provision their own resources.	Configures Avaya one-X® Portal to allow end users to configure their own telephone, messaging, and bridge conference resources. If you answer Yes, Avaya recommends that you create installation instructions for the users with the information they need to complete the configuration.
No. Only allow administrators to provision user resources.	Configures Avaya one-X® Portal to require that administrators configure all user resources in the Administration application. If you answer No, users cannot change these settings in their one-X Portal settings.

Database Instance username

This account has full privileges for the Avaya one-X® Portal database, including SYSADM. Avaya one-X® Portal requires the Instance username to connect to and create the database.

To meet database requirements, this username cannot have more than 8 characters.

Name	Example value	Description
Instance Username	dbinst	This user ID must be unique.
Instance Password		Password for the instance username account.

Database Admin username

This account has full privileges for the Avaya one-X® Portal database. Avaya one-X® Portal requires the Admin username to configure and access the database.

To meet database requirements, this username cannot have more than 8 characters.

Name	Example value	Description
Admin Username	dbadmin	
Admin Password		Password for the Admin username account.

Database Fence username

This account has privileges to administer the Avaya one-X® Portal database. Avaya one-X® Portal requires the Fence username to run stored procedures on the database.

To meet database requirements, this username cannot have more than 8 characters.

Name	Example value	Description
Fence Username	dbadmin	
Fence Password		Password for the Fence username.

Database read-only instance username

This account has read-only privileges for the Avaya one-X® Portal database. Avaya one-X® Portal requires this read-only instance username to connect to and read the database.

To meet database requirements, this username cannot have more than 8 characters.

Name	Example value	Description
Instance Username	roinst	
Instance Password		Password for the read-only instance username.

Application server username

Avaya one-X® Portal uses this account to log into and run the Avaya one-X® Portal application server. This account has full privileges for the application server, including rights to start and stop the server.

To meet application server requirements, this username cannot have more than 8 characters.

Name	Example value	Description
App Server Username	appsvr	This user ID must be unique.
App Server Password		Password for the App Server username account.

Web License Manager location

You can install Avaya Web License Manager (WebLM) on the same machine as the Avaya one-X® Portal server, or you can use an existing WebLM used by your other Avaya applications. The existing WebLM must be a version supported by Avaya one-X® Portal.

Important:

Application Enablement Services requires a dedicated WebLM. Do not install the Avaya one-X® Portal license on the WebLM used by Application Enablement Services.

Name	Description
Install WebLM locally	Installs WebLM on the same machine as the Avaya one-X® Portal server.

Name	Description
Use existing remote WebLM Server	Configures Avaya one-X® Portal to use an existing WebLM on a remote machine. The Avaya one-X® Portal machine must have network access to this machine.

WebLM remote configuration

If you chose to use a remote WebLM, the Installation Wizard uses this information to configure Avaya one-X® Portal to access the license in the WebLM.

Name	Example value	Description
WebLM URL	`http://<machine_name>.<domain>:<WebLM_port>/WebLM/`	URL of the server page for the WebLM. The WebLM URL is case-sensitive.

Enterprise Directory domain for users and security groups

If Avaya one-X® Portal will integrate with the existing Enterprise Directory, select the option that best defines how users and security groups are set up in the enterprise Active Directory.

If Avaya one-X® Portal will use a dedicated Enterprise Directory, select the option that best defines how you set up users and security groups in that Enterprise Directory.

Name	Description
Users and groups are defined in the same domain.	Select this option if the users and security groups for this Avaya one-X® Portal deployment are in the same domain.
Users are defined in one domain, and security groups are defined in another domain.	Select this option if the users for this Avaya one-X® Portal deployment are in a different domain than the security groups.

Enterprise Directory configuration

The Installation Wizard uses this information to configure the connection between Avaya one-X® Portal and the Enterprise Directory server.

If the Enterprise Directory has users defined in one domain and security groups defined in another domain, the Installation Wizard presents you with two Enterprise Directory

configuration screens. Configure the user domain in the first screen. Configure the resource domain for security group in the second screen.

Name	Example value	Description
Enterprise Directory IP Address	*###.###.###.###*	IP address of the computer that hosts the Enterprise Directory server.
Enterprise Directory Port	389	Port that the Avaya one-X® Portal computer will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	*users.domain.xyzcorp.com* *groups.domain.xyzcorp.com*	Fully qualified domain name configured on the Enterprise Directory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.
Enterprise Directory Username	*admin_service_user*	Enterprise Directory user that you created for the Avaya one-X® Portal administrative service account.
Enterprise Directory Password		Password for the Avaya one-X® Portal administrative service account.

Enterprise Directory administrator security group

The Installation Wizard uses the administrator security group to assign permissions to users who will administer Avaya one-X® Portal in the Administration application.

Note:

Do not use the default security group names, such as Domain Users, for Avaya one-X® Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

Name	Example value	Description
Admin Group	`cn=onexpAdmin,ou=Groups,dc=Company,dc=com`	Security group for Avaya one-X® Portal administrators.

Enterprise Directory auditor security group

The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the Avaya one-X® Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the Avaya one-X® Portal configuration in the Administration application.

Note:

Do not use the default security group names, such as Domain Users, for Avaya one-X® Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

Name	Example value	Description
Audit Group	`cn=onexpAudit,ou=Groups,dc=Company,dc=com`	Security group for Avaya one-X® Portal administrative auditors.

Enterprise Directory user security group

The Installation Wizard uses the user security group to assign permissions to users who will access the Avaya one-X® Portal application.

Note:

Do not use the default security group names, such as Domain Users, for Avaya one-X® Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

Name	Example value	Description
User Group	`cn=onexpUser,ou=Groups,dc=Company,dc=com`	Security group for Avaya one-X® Portal users.

Enterprise Directory presence security group

The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the Avaya one-X® Portal application.

Note:

Do not use the default security group names, such as Domain Users, for Avaya one-X® Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

Name	Example value	Description
Presence Group	`cn=onexpPresenceUser,ou=Groups,dc=Company,dc=com` or Select **Everybody** if you want to select All Enterprise Users. **Note:** Selecting **Everybody** bypasses the Base DN selected for presence user group. This also eliminates the need to have all users populated in the presence users group in LDAP and can be administered and controlled by Avaya one-X® Portal Administration.	Security group for Avaya one-X® Portal users from whom you want to be able to retrieve presence information. These users are listed as unprovisioned users. They cannot login to Avaya one-X® Portal and do not consume a license for Avaya one-X® Portal.

Summary of one-X Portal installation

This screen summarizes the selections and configuration information that you entered in the Installation Wizard.

Review this summary carefully. If you need to change any of the configuration information, click **Previous**.

Completing the Avaya one-X® Portal installation

Click **Finish** to complete the Avaya one-X® Portal installation.

Chapter 7: Configuring one-X Portal

Post-installation configuration checklist

You must configure these prerequisites in sequence after you run the Avaya one-X® Portal Installation Wizard.

Task	Instructions
Log in to the Administration application	Logging in to the Avaya one-X Portal Administration application on page 136
Verify the WebLM configuration	Verifying the WebLM settings on page 137
Install Avaya one-X® Portal license in WebLM	Installing a Avaya one-X Portal license on page 137
Analyze the Dial Plan on the switch and add a Dial Plan to Avaya one-X® Portal	Dial Plan services on page 139
Add the Telephony servers	Adding the Telephony servers on page 156
Add a Communication Manager server	Adding the Telephony servers on page 156
Add an AE Services server	Adding AE Services Auxiliary servers on page 157
Optional: Add a Modular Messaging server	Adding the Voice Messaging servers on page 158
Optional: Install a security certificate for the Modular Messaging connection	Installing the Modular Messaging security certificates on page 158
Optional: Add a Conferencing server	Adding the Conferencing servers on page 160
Optional: Configuring the Presence Services to point to Presence server	Configuring the Presence server on page 161
Optional: Add a contact domain	Adding the contact domains on page 164
Configure the license server	Configuring the license servers on page 164
Configure the SNMP traps	Configuring SNMP traps on page 165

Task	Instructions
Add an SNMP destination	Adding SNMP destinations on page 166
Restart the Avaya one-X® Portal	Restarting Avaya one-X Portal on page 166
Synchronize the enterprise directory and Modular Messaging	Synchronizing the Enterprise Directory and Modular Messaging on page 167
Provision the usersAvaya one-X® Portal	Provisioning a portal user on page 178

Logging in to the Avaya one-X® Portal Administration application

1. In your Web browser, type or select the Web page address for Avaya one-X® Portal administration.

   The default Web page address is `http://oneXportal_machine/admin`, where *oneXportal_machine* is the IP address or the fully qualified name and domain of the computer that hosts one-X Portal.

   For example, if the computer is named oneXportal and the domain is xyzcorp.com, the Web page address for your Administration application is `http://oneXportal.xyzcorp.com/admin/`.

2. In the Logon window, type your administrator **Login ID** and **Password**.

   Note:

   Administrator login ID must be a member of the Avaya one-X® Portal admin security group.

3. Click **Logon**.

Configuring WebLM for one-X Portal

Verifying the WebLM settings

Verify that the settings for the WebLM are correct for your environment. These settings were provided when you installed Avaya one-X® Portal.

1. In the Administration application, select the **System** tab.
2. On the left navigation pane, select **License Server**.
3. Verify that all of the settings are correct for your environment.

Installing a Avaya one-X® Portal license

Prerequisites

If the Avaya one-X® Portal system uses a proxy server or enhanced security for Internet Explorer, include the WebLM address in the browser exception list.

Important:
Application Enablement Services requires a dedicated WebLM. Do not install the Avaya one-X® Portal license on the WebLM used by Application Enablement Services.

1. In your Web browser, navigate to the address of the WebLM.
   The WebLM address format is usually the following: `http://<machine_name>.<domain>:<WebLM_port>/WebLM/`
   For example, a valid WebLM address is `http://testbox.xyzcorp.com:8080/WebLM/`
2. Log into License Administration.

   Note:
   If this is your first log in, WebLM may force you to change your username and password from the following default values:

   - Default username: admin

- Default password: weblmadmin

3. Install a ONEXPORTAL license with the appropriate number of users.

Creating directories for the Voice Messaging server and the Conferencing server

Prerequisites

Perform this task after you install Avaya one-X® Portal and before you create the Voice Messaging server and Conferencing server.

The Avaya one-X® Portal server runs with the Application server user, which is a non-root user. Therefore, if you do not use the default temp directories for the Voice Messaging server and the Conferencing server, you must create these directories and provide the Application Server user with read/write permissions. The default temp directory for the Voice Messaging server is /msgWorkDir and of the Conferencing server is /tmp.

Perform this task only if the Avaya one-X® Portal deployment meets the following criteria:

- Includes one or both of Modular Messaging and Conferencing.
- When you create the servers for these products in the Administration application, you do not plan to use the default temp directories.

Do not perform this task if you plan to use the default directories provided in the Administration application when you create these servers.

1. Determine the names that you plan to use for the following directories:
   - Voice Messaging server: Messages Temp Directory
   - Conferencing server: BCAPI Logger Directory
2. Create these directories.

   Avaya recommends that you create these directories in the home directory for the Application Server user.

   For example, create the following directories: `/home/appsvr/chicagomsgworkdirectory` and `/home/appsvr/chicagobcapitmpdirectory`
3. Execute the following command for each directory to give the Application Server user read/write privileges: `chown -R` *`appsvr.appsvr /path/to/new/msgworkdirectory`*

Where *appsvr.appsvr* is the Application server user name that you provided in the Installation Wizard and */path/to/new/msgworkdirectory* is the relative path from the home directory of the Application Server user to the directories that you created.

Configuring Dial Plans

Dial Plan services

Most enterprise directory systems, including Active Directory, store telephone numbers in the standard E.164 format (+19788081234). The E.164 format provides a unique description for each telephone number. Avaya one-X® Portal uses a Dial Plan to:

- Convert telephone numbers from the E.164 standard format to a sequence of numbers that the switch can dial or use for EC500 configuration.
- Convert a sequence of numbers received from the switch to the standard E.164 format .

Note:

For Avaya one-X® Portal dial plan transformations, all numbers must be stored in the standard E.164 format.

Avaya one-X® Portal supports enhanced EC500 functionality of Communication Manager. The rules for conversion of the dialed string to EC500 number are defined in a separate number transformation table on the Dial Plan page. The EC500 transformation, therefore, happens independently according to the type of transformation selected (Simple, Pattern Matching, or Regular Expression) and can be configured to fit the enhanced EC500 number format.

Important:

The Console Privileges for mobility stations should be set to **n** to use the enhanced EC500 functionality.

The Console Privileges for Worker Station should be set to **n** to use the enhanced EC500 functionality.

Avaya one-X® Portal includes the following Dial Plan transformations:

- Simple Dial Plan transformation
- Pattern Matching transformation
- Regular Expression transformation

Related topics:

Prerequisites on page 140

Prerequisites

Expertise

You must work with a subject matter expert who understands how the Dial Plan is configured in the switch to configure a Dial Plan in Avaya one-X® Portal . If the Dial Plan configuration in both the switch and Avaya one-X® Portal do not match, telephone calls do not reach the correct recipients.

Avaya one-X® Portal configuration

Each Dial Plan must have a Simple Dial Plan transformation.

If the Dial Plan in the switch includes more complex transformation rules, you can add either a Pattern Matching transformation or a Regular Expression transformation or both. A Dial Plan has three conversion rules tables: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Portal Client**, and **Conversion from dialed string to EC500 number**. You can use either the Pattern Matching transformation or the Regular Expression transformation for each conversion table in the Dial Plan.

Simple Dial Plan transformation

All Dial Plans configured in Avaya one-X® Portal must use the Simple Dial Plan transformation. This transformation uses the same number transformation that people use when they automatically convert a telephone number before they begin dialing the number in the switch. For example, in the United States, many users dial 9 before a phone number to make the connection. To call +1(978) 555-1111, they dial 919785551111. A Simple Dial Plan transformation performs the same type of conversion.

The Simple Dial Plan transformation can transform any input into a valid, final output. Therefore, this transformation is always the last transformation applied to any number. If you configure another transformation, Avaya one-X® Portal only uses the Simple Dial Plan transformation if the other transformation rules are unable to convert the input to a valid output.

Note:

The Simple Dial Plan transforms any input into a valid final output. However, sometimes the transformed output may be a valid telephone number, but this number connects to an incorrect destination. Simple Dial Plan cannot control the output after transformation, but other dial plan entries can do so. Simple Dial Plan provides a good starting point for the configuration, but over time most of the Dial Plan configurations tend to migrate to other Dial Plans. When this happens, you can configure the system to stop using Simple Dial Plan by providing a rule that matches any input as the final rule of the other dial plans.

The Simple Dial Plan transformation procedure

The Simple Dial Plan transformation uses a set of values to deduce if the user wants to make one of the following types of calls. It automatically adjusts the number format to match the sequence of numbers expected by the switch:

- Extension to extension call
- Local call
- National call
- International call

Related topics:

[Recommended uses for the Simple Dial Plan transformation](#) on page 141
[Example: Simple Dial Plan transformation](#) on page 141

Recommended uses for the Simple Dial Plan transformation

Always configure a Simple Dial Plan transformation for each Dial Plan in the switch.

Avaya recommends that you use Simple Dial Plan transformation for the following types of Avaya one-X® Portal implementation:

- The Dial Plan in the switch does not have any complex rules.
- The deployment is at a small to mid-size corporation inside the United States or any other country.
- The deployment is not required to support inter-switch dialing.

Avaya recommends that you configure Simple Dial Plan transformation with one of the other transformations for corporations where there is an overlap between the call length of extensions and local phone numbers. In addition, due to variations between dial plans, some countries may not be able to use this transformation alone.

Example: Simple Dial Plan transformation

This example describes how a Simple Dial Plan transformation uses the Dial Plan configuration to ensure that telephone numbers dialed in Avaya one-X® Portal reach the correct destination.

Dial Plan configuration

Parameter	Value
Main switch number	15553335000
Outside line access code	9
Local Region Prepend	555

Parameter	Value
Inter-region prepend	1
International prepend	011
National call length	10
Local call length	7
Extension length	5

This Simple Dial Plan transformation transformation does the following:

1. Uses the main switch number as a template for all other telephone numbers.
2. Modifies the telephone number that is dialed by a user to match the template.

Dial Plan results

The Simple Dial Plan transformation uses this Dial Plan configuration to create the following transformations on telephone numbers dialed by users:

Telephone number dialed by user	Transformed telephone number
+15553335111	35111
+15554440000	94440000
+15087641234	915087641234
+551151856200	9011551151856200

Pattern Matching transformation

The Pattern Matching transformation is very similar to the algorithm used by Communication Manager. The system evaluates the Pattern Matching rules in the order that they are specified in the user interface. The first rule to match the input is used as the transformation rule.

The Pattern Matching transformation matches a pattern based on the following three values:

- String at the beginning of the number
- Minimum length of the string
- Maximum length of the string

After the Dial Plan matches the number, the Pattern Matching transformation deletes the specified number of characters and inserts the configured set of characters.

Note:

A Dial Plan has three conversion rules tables: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Portal Client**, and **Conversion from dialed string to EC500 number**. You can use either the Pattern Matching

transformation or the Regular Expression transformation for each conversion table in the dial plan. However, a dial plan can be a combination of either of them.

Related topics:

Recommended uses for the Pattern Matching transformation on page 143
Example: Pattern Matching transformation on page 143

Recommended uses for the Pattern Matching transformation

When to configure the Pattern Matching transformation

Avaya recommends that you use the Pattern Matching transformation for the following type of Avaya one-X® Portal implementations:

- When the Simple Dial Plan transformation cannot convert all required number formats.
- When the telephone number used to dial out depends upon the length of the number and the first digit in the number.
- If the user needs to dial a specific numerical prefix to make international or cell phone calls.
- When a deployment includes switch networks.

For example, in a deployment that includes switch networks, a user in one location can call an employee at another location without dialing a long distance number. Each location has a dedicated switch, which is networked to the switch at the other location. To call a local extension, the user dials 7 plus a five-digit number. To call an extension at the other location, the user dials 8 plus a five-digit number.

When not to configure the Pattern Matching transformation

In the following situations, Avaya recommends that you use Regular Expression transformation in place of Pattern Matching transformation:

- When the telephone number depends upon specific ranges in the number, such as a country code and a city code.
- If the telephone number used to dial out does not require a specific number for the first digit, but instead the first digit can be one of a range of numbers.
- When the Dial Plan requires a large number of rules to match the possible patterns in the telephone numbers.

Example: Pattern Matching transformation

This example describes how Pattern Matching transformation matches patterns to ensure that telephone numbers dialed in Avaya one-X® Portal reach the correct destination.

Patterns to be matched

If the cell entry is <blank>, the pattern can match any possible value for that entry.

Starts with	Minimum length	Maximum length	Delete	Prepend	Description
+1555333	12	12	8	6	Internal extension calls. Dial the extension number.
+1555	12	12	5	9	Local calls
+1	12	12	2	91	Domestic long distance calls
+	12	<blank>	1	9011	International calls
<blank>	1	<blank>	0		Not a E.164 number. Dial as is.

Dial plan results

The Pattern Matching transformation uses these patterns to create the following transformations on telephone numbers dialed by users:

Telephone number dialed by user	Transformed telephone number
+15553335111	65111
+15553310000	93310000
+15087641234	915087641234
+551155551234	9011551155551234
915552225555	915552225555

Regular Expression transformation

The Regular Expression transformation is the most flexible transformation but also most difficult to configure.

The Regular Expression transformation uses the syntax defined by Java Regular Expressions. This transformation takes the list of regular expressions and replacement patterns that you define and applies them to the telephone number.

Note:

A Dial Plan has three conversion rules tables: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Portal Client**, and **Conversion from dialed string to EC500 number**. You can use either the Pattern Matching transformation or the Regular Expression transformation for each conversion table in the dial plan. However, a dial plan can be a combination of either of them.

Related topics:

Recommended uses for the Regular Expression transformation on page 145

Example: Regular Expression transformation on page 145

Recommended uses for the Regular Expression transformation

When to use the Regular Expression transformation

Avaya recommends that you use the Regular Expression transformation when the other transformations are not flexible enough to transform the telephone numbers. For example, use the Regular Expression transformation for the following type of Avaya one-X® Portal implementations:

- When the telephone number depends upon specific ranges in the number, such as a country code and a city code.
- If the telephone number used to dial out does not require a specific number for the first digit, but instead the first digit can be one of a range of numbers.
- When the Dial Plan requires a large number of rules to match the possible patterns in the telephone numbers.

When not to use the Regular Expression transformation

Avaya does not recommend the use of this transformation in the following scenarios:

- Dial Plan in the switch does not have any complex rules.
- Deployment is not required to support inter-switch dialing.
- When the telephone number used to dial out depends upon the length of the number and the first digit in the number.
- If the user needs to dial a specific numerical prefix to make international or cell phone calls.
- When the Dial Plan does not require a large number of rules to match the possible patterns in the telephone numbers.

Example: Regular Expression transformation

This example describes how a Regular Expression transformation matches patterns and regular expressions to ensure that telephone numbers dialed in Avaya one-X® Portal reach the correct destination.

Patterns to be matched

Pattern	Replacement	Explanation
\+1555333(\d{4,4})	6$1	Internal extension calls. Dial the extension number.
\+1555(\d{7,7})	9$1	Local calls
\+1(\d{10,10})	91$1	Domestic long distance calls

Pattern	Replacement	Explanation
\+55(\d{2,2}[89]\d{7,7})	9101045855$1	For making calls to Brazil, for any cell phone number that locally starts with an 8 or 9. These numbers must be prefixed by a special number to go through a cheaper carrier.
\+(\d{10,})	9011$1	Any other international number can go through the normal long distance carrier.
(\d{10,10})	91$1	A 10 digit number in a user contact that does not use the E.164 format.
(\d{4,})	$1	Other numbers can be dialed as entered.

Dial plan results

The Regular Expression transformation uses these patterns to create the following transformations on telephone numbers dialed by users:

Telephone number dialed by user	Transformed telephone number
+15553335111	65111
+15553211234	93211234
+15087641234	915087641234
+551191851234	91010458551191851234
+551155551234	9011551155551234
7204441000	917204441000
919785551234	919785551234

Creating rules for a Dial Plan

Before you create or configure a Dial Plan in Avaya one-X® Portal, you must gather information and determine what you need to support the Dial Plan in the switch.

1. Obtain the following information from the switch administrator:
   - For all information required in the Dial Plan worksheet in the Avaya one-X® Portal, see Configuration worksheet for Dial Plan on page 84.
   - A list of the E. 164 formats used for telephone numbers in the enterprise directory system. These formats form the E. 164 rules for the expected number inputs for the Dial Plan.

- A list of the expected number formats that the switch shows or dials. These formats form the network rules for the expected numbers received from the network.

2. Analyze the information that you receive and create the rules for the Dial Plan:
   a. Create a table of the E. 164 formats for the expected inputs.
   b. Create a table of the formats for the numbers that you expect Avaya one-X® Portal to receive from the network.
   c. Write the E. 164 rules required to transform the expected inputs into each type of expected output number.
   d. Write the network rules required to transform the expected numbers received from the network into each type of expected output.
   e. List the E. 164 rules in order from the most specific to the most general, and eliminate any duplicate rules.
   f. List the network rules in order from the most specific to the most general, and eliminate any duplicate rules.
3. Create a Simple Dial Plan transformation in the Administration application.
4. Run a set of basic sanity tests that covers each of the rules created in step 2 for calls dialed out with the Dial Plan.
5. If the Dial Plan does not ensure that all calls are delivered to the correct recipients, determine whether you need to create a Pattern Matching transformation or a Regular Expression transformation.
6. If you create a new transformation, run a set of basic sanity tests that covers each of your rules for calls dialed out with the Dial Plan.

Related topics:

Example: Creating rules for a Dial Plan on page 147

Example: Creating rules for a Dial Plan

This example creates the rules for a Pattern Matching transformation.

This example lists the tasks involved in step 2 of Creating rules for a Dial Plan on page 146. This step requires that you analyze the information that you received about the Dial Plan in the switch and create the rules for the Dial Plan.

E. 164 formats for the expected inputs

The enterprise directory uses these formats to store telephone numbers.

Expected number input	Description
+15553375247	Local extension

Expected number input	Description
+12228523657	Number in second location of switch network
+15553341234	Local number
5553341234	Personal active directory number that is not formatted using the E.164 format
+14447641234	Domestic long distance telephone number
+551151856280	International telephone number

Expected numbers that Avaya one-X® Portal receives from the network

The switch displays these numbers on the user extension and in Avaya one-X® Portal. They do not have to be numbers that a user can dial.

Number received from network	Description
75247	Local extension call
23657	Call from number in second location of switch network
5553341234	Call from local number
4447641234	Call from domestic long distance telephone number
551151856280	Call from international telephone number. This number can vary significantly.

E. 164 rules to transform the formats into expected output

After you have the expected E. 164 formats, write the E. 164 rules needed to transform each format into the expected output.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Expected number input	Description	Expected Output	Rule
+15553375247	Local extension	75247	Starts with: +1555337 Minimum length: 12 Maximum length: 12 Delete length: 7
+12228523657	Number in second location of switch network	23657	Starts with: +1222852 Minimum length: 12 Maximum length: 12 Delete length: 7
+15553341234	Local number	915553341234	Starts with: +1555 Minimum length: 12 Maximum length: 12 Delete length: 1 Prepend: 9

Expected number input	Description	Expected Output	Rule
5553341234	Personal active directory number that is not formatted using the E.164 format	915553341234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete length: 0 Prepend: 91
+14447641234	Domestic long distance telephone number	914447641234	Starts with: +1 Minimum length: 12 Maximum length: 12 Delete length: 1 Prepend: 9
+551151856280	International telephone number	9011551151856280	Starts with: + Minimum length: 10 Maximum length: 15 Delete length: 1 Prepend: 9011

Network rules to transform the numbers received from the network into expected output

After you have the list of numbers expected from the network, write the network rules needed to transform each sequence numbers into the expected output.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Number from network	Description	Expected Output	Rule
75247	Local extension call	+15553375247	Starts with: 7 Minimum length: 5 Maximum length: 5 Delete: 0 Prepend: +155533
23657	Call from number in second location of switch network	+12228523657	Starts with: 2 Minimum length: 5 Maximum length: 5 Delete: 7 Prepend: +122285
5553341234	Call from local number	+15553341234	Starts with: 555 Minimum length: 10 Maximum length: 10 Delete: 0 Prepend: +1
4447641234	Call from domestic long distance	+14447641234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10

Number from network	Description	Expected Output	Rule
	telephone number		Delete: 0 Prepend: +1
551151856280	Call from international telephone number. This number can vary significantly.	+551151856280	Starts with: <*blank*> Minimum length: 11 Maximum length: 15 Delete: 0 Prepend: +

Organize the E. 164 rules and eliminate duplicates

After you have the sequence of E. 164 rules, organize the rules in order from the most specific to the most generic. The most specific rules match the most digits in the number. The most generic rules match the least digits. For example, the Pattern Matching transformation must first attempt to match the number to a more specific rule for numbers that start with +1555. If that match fails, then the transformation must next attempt to match the number to a more generic rule for numbers that start with +1.

Delete all duplicate rules from the table.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Expected number input	Description	Expected Output	Rule	#
+15553375247	Local extension	75247	Starts with: +1555337 Minimum length: 12 Maximum length: 12 Delete length: 7	1
+12228523657	Number in second location of switch network	23657	Starts with: +1222852 Minimum length: 12 Maximum length: 12 Delete length: 7	2
	Local number			Duplicate rule. Deleted.

Expected number input	Description	Expected Output	Rule	#
5553341234	Personal active directory number that is not formatted using the E.164 format	915553341234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete length: 0 Prepend: 91	3
+14447641234	Domestic long distance telephone number	914447641234	Starts with: +1 Minimum length: 12 Maximum length: 12 Delete length: 1 Prepend: 9	4
+551151856280	International telephone number	0911551151856280	Starts with: + Minimum length: 10 Maximum length: 15 Delete length: 1 Prepend: 9011	5

Organize the network rules and eliminate duplicates

After you have the sequence of network rules, organize the rules in order from the most specific to the most generic. Then, delete any duplicate rules.

In this table, if the cell entry is <*blank*>, the pattern can match any possible value for that entry.

Number from network	Description	Expected Output	Rule	#
75247	Local extension call	+15553375247	Starts with: 7 Minimum length: 5 Maximum length: 5 Delete: 0 Prepend: +155533	1

Number from network	Description	Expected Output	Rule	#
23657	Call from number in second location of switch network	12228523657	Starts with: 2 Minimum length: 5 Maximum length: 5 Delete: 7 Prepend: +122285	2
	Call from local number			Duplicate rule. Deleted.
4447641234	Call from domestic long distance telephone number	+14447641234	Starts with: <*blank*> Minimum length: 10 Maximum length: 10 Delete: 0 Prepend: +1	3
551151856280	Call from international telephone number. This number can vary significantly.	+551151856280	Starts with: <*blank*> Minimum length: 11 Maximum length: 15 Delete: 0 Prepend: +	4

Adding Dial Plans

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.
3. On the Dial Plans page, click **Add New Dial Plan**.

   If you want to add Pattern Match and Regular Expression rules to the Dial Plan, modify the Dial Plan using the steps in Modifying Dial Plans on page 153 after you complete these steps.
4. On the Add New Dial Plan page, enter the appropriate information and click **OK** to add the **Dial Plan**.

For more information on the fields, see Dial Plan field descriptions on page 196.

5. In the **Dial Plan Transformation** section of the page, you can transform a phone number to display the **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to Displayed string in Portal Client**, and **Conversion from mobility string to PBX string for mobility (EC500)** numbers from this dial plan to determine if the Dial Plan is correctly configured.
   - **Conversion from dialed string to PBX dialable string**. Displays how the dial plan converts the number entered by the user, either by typing the number or selecting the number from the contact information, to a string that Communication Manager can use to dial the destination.
   - **Conversion from ANI to Displayed string in Portal Client**. Displays how the dial plan converts an ANI to display on the Avaya one-X® Portal client.
   - **Conversion from mobility string to PBX string for mobility (EC500)**. Displays how the dial plan converts a number to a string for Mobility.

   a. In the **Number to Transform** field, enter the phone number.
   b. Click **Transformation** to display the **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to Displayed string in Portal Client**, and **Conversion from mobility string to PBX string for mobility (EC500)** numbers for that number in the dial plan number.
6. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.
7. Click **Reset** to restore the settings to the last saved page or the default values if this is a new object.
8. Click **Cancel** to exit the page without making any changes.

Modifying Dial Plans

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.
3. From the list of the Dial Plans configured on the system, click the name of a Dial Plan in the **Handle** field to display the Modify Dial Plan page.
4. Modify the **Dial Plan**. See Dial Plan field descriptions on page 196.
5. Add Conversion Rules.

   The **Conversion Rules** table is divided into 3 sections: **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Portal Client**, and **Conversion from dialed string to EC500 number**. Select the

desired algorithm **Pattern Match** or **Regular Expression** for each conversion rule.

6. For the **Pattern Match** algorithm, complete the following fields:
   a. Select **Add**, to add the new conversion rule to the **Dial Plan**.
   b. In **Sort Position**, enter the order in which this rule is executed from the list of rules in this section. Enter 1 for first, 2 for second, and so on. When you save the dial plan, the order is displayed in increments of 5, 1 becomes 5, 2 becomes 10, and so on.
   c. In **Minimum Length**, enter the minimum number of digits allowed in the phone number.
   d. In **Maximum Length**, enter the maximum number of digits allowed for the phone number.
   e. In **Starts With**, enter the pattern of the algorithm to match to the **Regional Prefix**. For example, if the value of **Regional Prefix** is 978, enter +1978.
   f. In **Delete Length**, enter the number of digits to delete from the beginning of the phone number.
   g. In **Prepend**, enter any numbers you want to append to the beginning of the phone number.
7. For the **Regular Expression** algorithm, complete the following fields:
   a. Select **Add**, to add the new conversion rule to the **Dial Plan**.
   b. In **Sort Position**, enter the order in which this rule is executed from the list of rules in this section. Enter 1 for first, 2 for second, and so on. When you save the dial plan, the order is displayed in increments of 5, 1 becomes 5, 2 becomes 10, and so on.
   c. In **Regular Expression**, enter the Regular Expression pattern that applies to the phone number.
   d. In **Prepend**, enter the replacement pattern that applies to the phone number. A Regular Expression pattern of \+14259(\d{7.}) and a Replacement pattern of 9$1 could transform the phone number +14252417293 to 92417293.
8. To delete one or more conversion rule from the Existing Rules, select the **Del** check box adjacent to a rule, and click **Save**.
9. In the **Dial Plan Transformation** section of the page, you can transform a phone number to display its **Conversion from dialed string to PBX dialable string**, **Conversion from ANI to displayed string in Portal Client**, and **Conversion from mobility string to PBX string for mobility (EC500)** numbers from this dial plan to determine if these changes are correctly configured.
   - **Conversion from dialed string to PBX dialable string**. Displays how the dial plan converts the number entered by the user, either by typing the number or

selecting the number from the contact information, to a string that Communication Manager can use to dial the destination.

- **Conversion from mobility string to PBX string for mobility**. Displays how the dial plan converts a number to a string for Mobility.
- **Conversion from mobility string to PBX string for mobility (EC500)**. Displays how the dial plan converts an ANI to display on the Avaya one-X® Portal client.

a. In the **Number to Transform** field, enter the phone number.

b. Click **Transformation** to display the **Conversion from dialed string to PBX dialable string**, **Conversion from mobility string to PBX string for mobility**, and **Conversion from mobility string to PBX string for mobility (EC500)** numbers for that number in the dial plan number.

10. Click **Test** to run a short test of your changes. The results of the test are displayed immediately so you can make any necessary changes.
11. Click **Save** to update the **Dial Plan**.
12. Click **Reset** to restore the settings to the last saved page or the default values if this is a new object.
13. Click **Delete** to delete the dial plan.
14. Click **Cancel** to exit the page without making any changes.

Configuring one-X Portal servers

Telephony servers

The Telephony server adapter on Avaya one-X® Portal provide computer telephony integration (CTI) with Communication Manager switches to provide a single Avaya interface to the portfolio of Avaya products.

Avaya one-X® Portal supports call management features like make a call, answer a call, hang up a call, put a call on hold, transfer a call, and handle multiple call appearances.

In addition to the above, the telephony server adapter (SIP Service) on enables SIP Communication with Communication Manager directly or through Session Manager.

uses the SIP domain information as provided in the SIP Local configuration to communicate with Communication Manager. SIP Service uses SIP address such as example user@domain

to communicate with Communication Manager. This service supports mobility features such as Also Ring, Call back, and Block All Calls.

This section describes how to configure Telephony servers and AE Services servers to make them communicate with each other.

Related topics:

Adding the Telephony servers on page 156
Adding AE Services Auxiliary servers on page 157

Adding the Telephony servers

1. Select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, in the **Server Type** field, select the version of the Communication Manager server installed on your system.
4. Click **Add** to display the Add Telephony Server Configuration page.
5. Enter the appropriate information.

   For more information on the fields, see Telephony server field descriptions on page 188.
6. Add the AE Services server to be used by the Telephony server.
   a. In the **AES Servers Available** field, select the name of the AE Services server to add to the Telephony server configuration.
   b. Click **Add** to move the selected server(s) to the **AES Servers Selected** field. You can also click **Add ALL** to move all of the servers.
   c. Repeat these steps to add additional AE Services servers to set up a failover strategy. If the first AE Services server on the list fails, the Telephony server uses the next server on the list.
   d. Select the server name and click **Move Up** or **Move Down** to reorder the list.
   e. Select the server name and click **Remove** to remove the server and move it back to the **AES Servers Available**. You can also select multiple servers and click **Remove All**.
7. Select a dial plan from the **Dial Plan** drop-down list.
8. Click **OK** to add the server.
9. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.

   If the TSAPI.PRO file has the AE Services server IP address when the Telephony adapter starts, the test is considered successful. The IP address and Port number

of the TSAPI of AES gets stored in the *192.168.1.176=450* format, where *192.168.1.176* is the IP address of TSAPI and *450* is the port number of TSAPI.

If this is a new AE Services server and the system displays error messages, such as AE Services server is not found, check the TSAPI.PRO file. To check the file:

a. Save the Auxiliary Server configuration as this causes the AE Services server IP Address to be saved in the `/opt/IBM/WebSphere/AppServer/lib/TSAPI.PRO` file.

b. Restart the Telephony adapter so it can read the new TSAPI.PRO file.

c. Run the test again after the Telephony adapter restarts.

Adding AE Services Auxiliary servers

1. Select the **Servers** tab.
2. From the left pane, select **Auxiliary Servers**.
3. On the Auxiliary Servers page, in the **Server Type** field, select the version of the AE Services server installed on your system.
4. Click **Add**.
5. On the Add Auxiliary Server Configuration page, enter the server configuration information and click **Save** to add the server.

   For more information, see Auxiliary server (AE Services) field descriptions on page 190.
6. After you add the new AE Services server, restart the Telephony service to save the changes to the `TSAPI.pro` file.

   For instructions, see Monitoring Telephony services.
7. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.
8. Click **OK** to add the auxiliary server.
9. Click **Reset** to restore the settings to the last saved page.
10. Click **Cancel** to exit the page without making any changes.

Voice Messaging servers

Modular Messaging servers on Avaya one-X® Portal provide messaging capabilities such as viewing, hearing, and deleting voice mail messages.

The Modular Messaging servers communicate with Communication Manager and the Telephony servers to provide these capabilities.

Related topics:

Adding the Voice Messaging servers on page 158
Installing the Modular Messaging security certificates on page 158

Adding the Voice Messaging servers

1. Select the **Servers** tab.
2. From the left pane, select **Voice Messaging**.
3. From the Voice Messaging page, in the **Server Type** field, select the version number of the Modular Messaging server installed on the system.
4. Click **Add** to display the Add Voice Messaging Server Configuration page.
5. Enter the appropriate information and click **OK** to add the server.
   For more information on the fields, see Voice Messaging server field descriptions on page 191.
6. Click **Test** to run a short test of your entries.
   The results of the test are displayed immediately so you can make any necessary changes.

Installing the Modular Messaging security certificates

To secure a communication channel between Avaya one-X® Portal and Modular Messaging, configure the server certificates to secure the Java mail API. The Java mail API is used to connect the IMAP connection to Modular Messaging. These certificates establish a trust relationship between Avaya one-X® Portal and Modular Messaging.

Install Modular Messaging security certificates as part of the **Voice Messaging** server configuration on the Administration Web Client.

1. Select the **Servers** tab.
2. From the left pane, select **Voice Messaging**.
   The Voice Messaging page displays a list of the Modular Messaging servers installed on the system.
3. Click the name of a Modular Messaging server in the **Handle** field to display the Modify Voice Messaging Server Configuration page for the server.
4. Retrieve the security certificate in the **SSL Certificate** field if necessary and click **Save** to update the server.
   For more information on the fields, see Voice Messaging server field descriptions on page 191.

   Note:
   You must restart the MSS server to save your changes. For more information, see Monitoring Voice Messaging services.

   Note:
   You must restart the MSS server to save your changes.
5. Click **Test** to run a short test of your changes. The results of the test are displayed immediately so you can make any necessary changes.
6. Click **Reset** to restore the settings to the last saved page or, if this is a new object the default values.
7. Click **Cancel** to exit the page without making any changes.

Conferencing services

Conferencing servers on Avaya one-X® Portal provide bridge conferencing capabilities such as creating on-demand conferences, controlling the conference (for conferences in session), and scheduling one-time or recurring conferences.

Bridged conferences are not like conference calls through phone services which is generally limited to 6 parties. Large number of participants can join a bridge conference and one or more moderators control the bridge. Using the client application, some of the tasks the bridge conference moderators can do are:

- add participants
- drop participants
- mute participants

- put the participants line on hold
- secure the conference room by blocking participants from joining the conference

Related topics:

Adding the Conferencing servers on page 160

Adding the Conferencing servers

1. Select the **Servers** tab.
2. To display a list of the servers on the system, from the left pane, select **Conferencing**.
3. In the **Server Type** field, select the version number of the Conferencing server installed on the system.
4. Click **Add** to display the Add Conferencing Server Configuration page.
5. Enter the appropriate information and click **OK** to add the server.

   For more information on the fields, see Conferencing server field descriptions on page 194.
6. Click **Test** to run a short test of your entries. The results of the test are displayed immediately so you can make any necessary changes.

   Note:

   If you have entered correct credentials, but the test fails and the system displays an error message that the Meeting Exchange server is not visible and prompts you to verify the ports and the IP address. You can ignore this message, save the Meeting Exchange profile, and restart the Meeting Exchange adaptor. When you restart the adaptor, the status of the connection changes to "Connected". You can now run the Meeting Exchange profile test again.
7. Click **Reset** to restore the settings to the last saved page or, if this is a new page, the default values.
8. Click **Cancel** to exit the page without making any changes.

Presence service

You can integrate a Presence Services server with Avaya one-X® Portal. Presence Services provides presence capabilities to the client applications such as Avaya one-X® Portal and Avaya one-X® Mobile.

- Aggregated presence - Aggregated presence is the combination of presence status such as Available, Busy, Unavailable, out of Office and system message such as *On a call* or personal message such as *Working for Beta release*.
- Channel presence - Channel presence shows the presence status of the use on various channels such as telephone, e-mail, and Microsoft Office Communicator (MOC). The phone state on the client application may show free or busy status. The Instant Messaging (IM) icon on the client application appear either free, busy, or user can set the status to appear as offline.

Note:

Presence feature also provides instant messaging and presence capabilities if Presence Services is integrated with Microsoft Office Communicator (MOC).

The Presence Services server stores the personal availability record of users (also known as presentity) on Avaya one-X® Portal. This record is available to other users (watchers) to convey a user's availability for communication.

Related topics:

Configuring the Presence server on page 161

Configuring the Presence server

1. Select the **Servers** tab.
2. From the left pane, select **Presence**.
3. On the Presence Servers page, in the **Server Type** field, select **apas 6.0** or **apas 6.1**, which is the version number of the Presence server installed on the system.
4. Click **Add** to display the Add Presence Server Configuration page.
5. Enter the appropriate information and click **OK**.

   For more information on the fields, see Presence server field descriptions on page 195.

Mobility Extension Banks

A Mobility Extension Bank on Avaya one-X® Portal associates extension numbers with the Telephony servers configured on Avaya one-X® Portal. The Telephony server uses these extensions to perform Extension to Cellular functions on the other extensions on the Telephony server using the EC500 code that is administered on the Telephony server.

The Mobility Extension Bank feature enables you to administer the extension numbers in the Mobility Extension Bank and associate them with the desired Telephony server.

Mobility extensions are a set of worker stations on the switch. These stations are not user extensions and must be created for use by Avaya one-X® Portal only. To map mobility stations, use Communication Manager Network Region mapping or native CLAN Network Region to a region that supports G711. Avaya one-X® Portal uses mobility extensions to dial feature access on the switch.

For mobility extensions, the connection to Communication Manager is made through AES. If the H.323 gateway list is administered in AES, then the CLAN will be used from this gateway list.

Each switch can have 2 to 10 mobility extensions. The number of mobility extensions is related to the number of Extension to Cellular requests that the Avaya one-X® Portal server has to handle. Typically, each mobility extension can handle 500 Extension to Cellular requests per hour.

Avaya recommends assigning at least 2 extension banks to each user, providing a backup extension bank in the event of a failure.

Related topics:

Adding Mobility Extension Banks on page 162

Adding Mobility Extension Banks

1. Select the **Servers** tab.
2. From the left pane, select **Mobility**.

   The Mobility Extension Banks page displays a list of the Mobility Extension Banks on the system.
3. Click **Add New Extension Bank** to display the Add Extension Bank Configuration page.
4. Enter the appropriate information and click **OK** to add the **Extension Bank**.

   For more information on the fields, see Mobility Extension Bank field descriptions on page 197.

5. Click **Reset** to restore the settings to the last saved page or, if this is a new object, the default values.
6. Click **Cancel** to exit the page without making any changes.

Enterprise Directory domains

The Enterprise Directory server connects Avaya one-X® Portal with the Active Directory. Users must exist in the Enterprise Directory before they can be provisioned as users on Avaya one-X® Portal.

The Enterprise Directory server is added to domains in the Active Directory to access the records in the domains. Except the Active Directory, all other Enterprise Directories require the User domain and Resource domain to be on the same server. There are three types of domains in Active Directory and you can add multiple Enterprise Directory servers to any domain type:

- The User domain can contain users, security groups, and contacts. There is only one User domain and it is created in Active Directory. You cannot add a User domain or modify the name or type of a User domain.
- The Resource domain contains security groups. Security groups are privilege-based groups set in the Active Directory. These groups are defined by their permissions on Avaya one-X® Portal, such as Administrator, Auditor, or User. There is only one Resource domain and it is created in Active Directory. You cannot add a Resource domain or modify the name or type of a Resource domain.
- Contact domains contain information about the contacts with which Avaya one-X® Portal users communicate. Contact information includes details such as name, phone number, and address. You can add Contact domains to Avaya one-X® Portal and modify the names of existing Contact domains. You cannot change the type of a Contact domain. For example, if your enterprise acquires another company, you may want to access the contact information for the other company in a new Contact domain. But even if you add contact domains, Avaya one-X® Portal supports only same the type of Enterprise Directory. For example, if you are using Active Directory for your user domain, then all the contact directories must be in Active Directory.

Related topics:

Adding the contact domains on page 164

Adding the contact domains

1. Click the **System** tab.
2. In the left pane, select **Enterprise Directory**.

   The Enterprise Directory Domains page displays a list of the domains on the system.
3. Click **Add Contact Domain** to display the Add Enterprise Contact Domain page.
4. Enter the appropriate information and click **OK** to add the domain.

   For more information on the fields, see Enterprise Directory field descriptions on page 201.
5. Click **Reset** to restore the settings to the last saved page or, if this is a new object, the default values.
6. Click **Cancel** to exit the page without making any changes.

License server services

The WebLM server is a Web-based license manager that enables you to track and manage licenses of multiple Avaya software products installed on Avaya one-X® Portal from a single location. To track and manage these licenses, WebLM requires a license file of the product that contains product information, such as major release, the licensed features of the product, and the licensed capacities of each feature purchased by the organization.

Related topics:

Configuring the license servers on page 164

Configuring the license servers

1. Click the **System** tab.
2. In the left pane, select **License Server**.
3. On the License Server Configuration page, enter the appropriate information and click **Save** to configure the server.

For more information on the fields, see License server field descriptions on page 203.

4. Click **Reset** to display the settings from the start of this session.

SNMP Traps

Avaya one-X® Portal can notify Network Management Stations (NMS) about alarm events by sending SNMP Traps.

Use the SNMP Traps option to define both the alarm events for which you want to send SNMP traps and the destinations where you want to send the SNMP traps.

Related topics:

Configuring SNMP traps on page 165
SNMP Destinations on page 165
Adding SNMP destinations on page 166

Configuring SNMP traps

1. Select the **System** tab.
2. From the left pane, select **SNMP Traps**.
3. On the SNMP Traps page, enable or disable the SNMP Traps as desired.
   - Select the check box for each SNMP Trap you want to enable.
   - Click **Check All** to enable all the SNMP Traps on the list.
   - Click **Uncheck All** to disable all the SNMP Traps on the list.
4. Click **Save** to save your changes.
5. Click **Refresh** to display the settings from the start of this session.

SNMP Destinations

SNMP Destinations are devices to which you can send specified traps, also called event notifications. On Avaya one-X® Portal, these devices can either be the Avaya Services Security Gateway (SSG) or industry standard Network Monitoring Software (NMS) such as HP

Openview or IBM Tivoli. Use this option to define specified destinations when certain events take place on Avaya one-X® Portal.

Adding SNMP destinations

1. Select the System tab.
2. From the left pane, select **SNMP Destinations**.
3. On the SNMP Destinations page, click **Add New SNMP Trap Destination** to display the Add SNMP Destination Configuration page.
4. Enter the appropriate information and click **OK** to add the server.
   For more information on the fields, see SNMP destinations field descriptions on page 204.
5. Click **Reset** to display the settings from the start of this session.
6. Click **Cancel** to exit the page without making any changes.

Restarting Avaya one-X® Portal

To restart Avaya one-X® Portal, you must restart the Web Application server (WAS).

1. Log in with the Application server user name created during the one-X Portal installation. For example, the default user name is appsvr.
2. Run the following command to stop the one-X Portal server: `/opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1 -username admin_service_user -password admin_service_password`
   In this command *admin_service_user* is the one-X Portal administrative service account that you created in Active Directory, and *admin_service_password* is the password for that account.
3. Run the following command to restart the one-X Portal server: `/opt/IBM/WebSphere/AppServer/bin/startServer.sh server1`

Synchronizing the Enterprise Directory and Modular Messaging

For information on how to schedule a synchronization, see the online help for the Administration application.

Note:
Synchronization can affect the operation and performance of the system.

1. Select the **Scheduler** tab.

   Note:
   If you are an **Auditor**, the **Scheduler** tab is not available.
2. From the left pane, select **Enterprise Directory Synchronization**.
3. Click **Run Now**.

   Wait approximately 3 to 5 minutes until the Enterprise Directory synchronization has completed.
4. From the left pane, select **Modular Messaging Synchronization**.
5. Click **Run Now**.

   Wait approximately 2 to 3 minutes until the Modular Messaging synchronization has completed.

Configuring users for one-X Portal

Avaya one-X® Portal users configuration

The users of Avaya one-X® Portal must be listed in the Enterprise Directory. The Enterprise Directory administrator should list these users in the Avaya one-X® Portal user group in the Enterprise Directory.

After you provision the users, they are able to access the Avaya one-X® Portal application.

Unprovisioned users

Users who are in the Avaya one-X® Portal user group of the Enterprise Directory but have not been provisioned on Avaya one-X® Portal.

Provisioned users

Users assigned to the Avaya one-X® Portal user group or the Presence user group. Each user group is associated with an application inside Avaya one-X® Portal. Therefore, users in the one-X Portal user group are associated with the Avaya one-X® Portal Application, and the users in the Presence user group are associated with the Presence application. The same users can exist in two or more applications. Users associated with the Presence application do not need explicit enabling forAvaya one-X® Portal. They do not require Avaya one-X® Portal licenses and use the Command Line Interface (CLI) for provisioning. Users of Avaya one-X® Portal need to be explicitly enabled for Avaya one-X® Portal application. They use a single Avaya one-X® Portal license for each user enabled for Avaya one-X® Portal. Only users enabled for the Avaya one-X® Portal application can log in to the Avaya one-X® Portal Client. Users in the Presence application can have telephony resources provisioned. Presence Services use these resources for reporting telephony Presence.

User Administration options

Depending upon the needs of a Avaya one-X® Portal system and the types of users that the system needs to support, you can simplify the provisioning and administration of users through a combination of prototype users, group profiles, and the system profile. You do not need to administer each Avaya one-X® Portal user individually.

User analysis

Each user administration option performs a different purpose. Before you provision and administer the Avaya one-X® Portal users, review the needs of the users and the resources they will require. After you have that information, you can determine the optimum way to administer the users.

System profile

After you have analyzed the needs of your users, review the default values in the system profile and modify those values as needed for your Avaya one-X® Portal system.

The System Profile is a collection of the following properties applicable to groups that are members of the system.

- **Continuous extension monitoring**
- **Telecommuter**
- **VOIP**
- **Send DTMF for calls**
- **SIP Station**
- **Mobility**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum number of history records**
- **Maximum days to keep history**

- **Maximum number of favorites**
- **Usage Disclaimer**
- **Usage Disclaimer URL**
- **Feedback Email Address**
- **Maximum number of entries per portal view**
- **Default access type**
- **Default access level**
- **Minimum access level**

Group profiles

After you update the system profile, you can add a group profile for each group of users who require a different set of values for the group profile properties than the values in the system profile.

Use a group profile to apply values to a group of users who use the same values for the following properties:

- **Continuous extension monitoring**
- **Telecommuter**
- **VOIP**
- **Send DTMF for calls**
- **SIP Station**
- **Mobility**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum number of favorites**

If the values for these properties are not forced from the System level, you can override the System value with a different value for the users assigned to the group profile.

Prototype users

You can implement prototype users instead of group profiles or, depending upon the needs of your users, you can implement prototype users in addition to group profiles.

A Prototype user is a collection of configuration settings and service provisioning values that you can apply to other users while provisioning a user. You can use Prototype users as templates to speed up the configuring and provisioning of users, who have similar settings.

Individual user administration

You can also administer an individual user. However, Avaya recommends that you administer individual users only if that user has a unique set of values that are not shared by other users.

User administration checklist

This checklist summarizes the configuration steps required to provision and administer Avaya one-X® Portal users.

#	Task	Instructions	✔
1	Analyze the needs of Avaya one-X® Portal users and determine which resources they require.		
2	Review the system profile and, if necessary, modify the values of the profile properties.	Modifying the System profile on page 171	
3	Optional: add one or more group profiles. Avaya recommends that you add a group profile for each group of users who require a different set of values for the group profile properties than the values in the system profile.	Adding group profiles on page 174	
4	Optional: add one or more prototype users. Avaya recommends that you add a prototype user for each group of users who require the same configuration settings. If necessary, you can use prototype users in combination with group profiles.	Adding Prototype users on page 175	
5	Provision the Avaya one-X® Portal users. You apply profiles and prototype users during this step.	Provisioning a portal user on page 178	

System Profile

The System Profile is a collection of the following properties applicable to groups that are members of the system.

- **Continuous extension monitoring**
- **Telecommuter**

- **VOIP**
- **Send DTMF for calls**
- **SIP Station**
- **Mobility**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum number of history records**
- **Maximum days to keep history**
- **Maximum number of favorites**
- **Usage Disclaimer**
- **Usage Disclaimer URL**
- **Feedback Email Address**
- **Maximum number of entries per portal view**
- **Default access type**
- **Default access level**
- **Minimum access level**

Avaya one-X® Portal provides one System Profile which you can modify to apply its property values to all users and groups on the system. For System Profile properties, you can accept the default value, set a new system value, or force the value at the Group Profiles level.

Important:
At the system and group levels, **force** does not affect the Presence and ACL settings. User settings override the forced system level settings.

Related topics:

Modifying the System profile on page 171

Modifying the System profile

1. Click the **Users** tab.
2. In the left pane, click **System Profile**.
3. On the System Profile page, change the values of the following profile properties as needed.

   You can accept the default values for these properties or set new values. You can also force the value of the property to any Group profile that uses this property.

If you set the **System Value** as **Accept default** and if you do not specify a **Group Value**, it is set as the **Default** value of the **System Profile**. If you set the **System Value** as **Set System Value**, and if you do not specify a **Group Value**, it is set as the value as specified in the **System Profile**. If you set the **System Value** as **Force Value in Groups**, the **Group Value** is set as the **System Value** as specified in the **System Profile** even if you specify a different value in the **Group Profile**.

Options	Description
Property	**Description**
Continuous extension monitoring	Click **Enabled**, to monitor the extension of the user whether the user is logged in to Avaya one-X® Portal or not. Provides call information like missed calls to the user.
Telecommuter	Click **Enabled** to turn on the **Telecommuter** functionality on Avaya one-X® Portal .
VoIP	Click **Enabled** to turn on **Voice over IP** on Avaya one-X® Portal.
Send DTMF for calls	Click **Disabled** to turn off the **Send DTMF for calls** option when in a call.
SIP Station	Click **Enabled** to stop the telephony server from checking if the station is connected to the Communication Manager before allowing a user to log in in the shared control mode. **Note:** If you set the **SIP Station** to **Enabled**, you must set the **Telecommuter**, **VOIP**, and **Send DTMF for calls** options to **Disabled** because in Avaya one-X® Portal you cannot use the **Telecommuter**, **VOIP**, and **Send DTMF for calls** options when you are using a SIP station.
Mobility	Click **Enabled** to turn on the **Mobility** functionality Avaya one-X® Portal.
Forward voice messages to inbox	Click **Enabled** to forward the voice messages received by a user on Avaya one-X® Portal to the e-mail inbox of the user.
Save to voice messages file	Click **Enabled** to save the voice messages received by a user on Avaya one-X® Portal to the voice messages file.
Maximum number of entries per portal view	Specify the maximum number of entries to allow per portal view on Avaya one-X® Portal. Enter a value between **1** and **200**.

Options	Description
Maximum number of history records	Specify the maximum number of records to archive on Avaya one-X® Portal. Enter a value between **1** and **400**.
Maximum days to keep history	Specify the maximum number of days to keep these records in archive on Avaya one-X® Portal. Enter a value between **1** and **14** days.
Maximum number of favorites	Specify the maximum number of favorites a Avaya one-X® Portal user can keep on their Portal Client application. Enter a value between **1** and **5000**.
Usage Disclaimer	Click **Enabled** to turn on the **Usage Disclaimer** on Avaya one-X® Portal.
Usage Disclaimer URL	Specify the URL for the **Usage Disclaimer** on Avaya one-X® Portal. The default value is **usage.jsp**.
Feedback e-mail address	Specify the e-mail address for the user to provide feedback to the Avaya one-X® Portal administrator.
Default Access Type	Specify one of the following access types. This value is used when the presence resource for the user does not have the access type specified in an ACL. • **ALLOW**: Accept the watcher request. • **BLOCK**: Deny the watcher request. • **PENDING**: Ask the user to accept or deny the watcher request.
Default Access Level	Specify one of the following access levels to indicate which devices support Presence functionality: • **FULL**: Telephone and IM • **TEL_ONLY**: Telephone only
Minimum Access Level	Specify **TEL_ONLY** to provide Presence support on the telephone at all times.

4. Click **Save** to save these settings to the profile.
5. Click **Reset** to display the settings from the start of this session.

Group Profiles page

A Group profile is a collection of the following properties applicable to users who are members of the group.

- **Continuous extension monitoring**
- **Telecommuter**
- **VOIP**
- **Send DTMF for calls**
- **SIP Station**
- **Mobility**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum number of favorites**

Use a Group profile to apply values to the users in the group who use the same properties. When you set values that are forced from the system level, Group profiles inherit values from System profiles. Forced values are system-level values that cannot be changed at the lower Group profile or user profile levels. If the values are not forced from the system level, you can either accept the system level value for a Group profile or override it with a group value.

Related topics:

Adding group profiles on page 174

Adding group profiles

1. Select the **Users** tab.
2. From the left pane, select **Group Profiles**.
3. On the Group Profiles page, click **Add New Group Profile** to display the Create a New Group Profile page.
4. Enter the name of the profile in the **Handle** field.
5. Enter a brief description of the profile in the **Description** field.
6. Set the following properties in the profile as needed.

   You can accept the system default value or set a new Group profile value. If the value of the property is forced from the System profile, you cannot change that value.

- **Continuous extension monitoring**
- **Telecommuter**
- **VOIP**
- **Mobility**
- **Forward voice messages to inbox**
- **Save to voice messages file**
- **Maximum number of favorites**

7. Click **OK** to create the profile.
8. Click **Reset** to display the settings from the start of this session.
9. Click **Cancel** to exit the page without making any changes.

Prototype Users

A Prototype user is a collection of configuration settings and service provisioning values that you can apply to other users while provisioning a user. You can use Prototype users as templates to speed up the configuring and provisioning of users, who have similar settings.

Note:

Use Prototype users for provisioning users only. The resources you have assigned to a prototype user are copied to the users you are provisioning. Once you provision a user using a prototype user, any change made to the Prototype user does not impact the users that are provisioned using this Prototype user.

Related topics:

Adding Prototype users on page 175
Assigning a Telephony resource to a Prototype user on page 176
Assigning a Voice Messaging resource to a Prototype User on page 177
Assigning a Conferencing resource to a Prototype User on page 177

Adding Prototype users

1. Select the **Users** tab.
2. From the left pane, select **Prototype Users**.

3. On the Prototype Users page, click **Create Prototype User** to display the Create Prototype User page.
4. In the **Handle** field, enter the name of the Prototype user.
5. In the **Description** field, enter a short description of the name of the Prototype user.
6. Click **Continue** to save these fields.
7. Add the following resources to the Prototype user:
   - Telephony resource. Perform the steps in Assigning a Telephony resource to a Prototype user on page 176.
   - Messaging resource. Perform the steps in Assigning a Voice Messaging resource to a Prototype User on page 177.
   - Conferencing resource. Perform the steps in Assigning a Conferencing resource to a Prototype User on page 177
   - Presence resource. Perform the steps in Assigning a Presence resource to a user on page 182.
8. Click **Finished** to save the Prototype User.
9. Click **Delete** to remove the Prototype User.

Assigning a Telephony resource to a Prototype user

1. Select the **Users** tab.
2. From the left pane, select **Prototype User**.

   For a new Prototype User, you have assigned the **Handle** and the **Description** and are now adding resources.
3. For an existing Prototype User, search for and select the Prototype User you want to assign the resource.
4. In the **Telephony** group box, click **Add**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the Communication Manager server.
   b. In the **Display Name** field, type a descriptive name for this resource which users see in the Avaya one-X® Portal.
6. Click **Save**.

The browser returns to the Prototype User page.

Assigning a Voice Messaging resource to a Prototype User

1. Select the **Users** tab.
2. In the left navigation pane, select **Prototype Users**.
   For a new Prototype User, you have assigned the **Handle** and the **Description** and are now adding resources.
3. For an existing Prototype User, search for and select the Prototype User you want to assign the resource.
4. In the **Voice Messaging** group box, click **Add**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the Modular Messaging server.
   b. In the **Display Name** field, type a descriptive name for this resource which users see in the Avaya one-X® Portal.
6. Click **Save**.
   The browser returns to the Prototype User page.

Assigning a Conferencing resource to a Prototype User

1. Select the **Users** tab.
2. In the left navigation pane, select **Prototype Users**.
   For a new Prototype User, you have assigned the **Handle** and the **Description** and are now adding resources.
3. For an existing Prototype User, search for and select the Prototype User you want to assign the resource.
4. In the **Conferencing** group box, click **Add**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the Conferencing server.

b. In the **Display Name** field, type a descriptive name for this resource which users will see in the Avaya one-X® Portal.

c. In the **Bridge Number** field, type the telephone number that the user dials to log in to the bridge.

d. In the **Bridge Number Backup** field, type the secondary telephone number that the user can dial to log in to the bridge.

e. Select the **Allow Call Me** check box.

6. Click **Save**.
   The browser returns to the Prototype User page.

Provisioning a portal user

You can also use the Administration Command Line Interface to provision users on Avaya one-X® Portal.

Note:
To add a user to , they must first be a member of the Portal users group in the enterprise directory.

To perform a bulk import of users, see the Administration Command Line Client online help.

1. Select the **Users** tab.
2. In the left navigation pane, select **Unprovisioned Users**.
   The Unprovisioned Users page lets you search for unprovisioned users on the system.
3. If you know the user ID of the unprovisioned user, you can enter the user ID in the **Direct To Enterprise Directory** section and click **Provision** to provision that user.
4. If you do not know the user ID of the unprovisioned user, select from the following criteria and press **Search** to display a list of users that match the criteria.
   - In the **Search By** field, the options are
     - **Any**
     - **User ID**
     - **Display Name**
     - **First Name**
     - **Last Name**

- In the **Pattern** field, you can enter a pattern search for the option selected in the **Search By** field. The **Pattern** field is activated after a selection is made in the **Search By** field. An example of a pattern is using "sm*" to sort for a list of all users whose last name starts with "sm" when **Last Name** is selected in the **Search By** field. One or more wildcards can be used anywhere in the search pattern.

5. Click **Provision** in the row of the user you wish to provision.
6. At the Provision User page, assign the Group profile and Prototype user (if any) to the user.
7. Select **Enable**.
8. Click **Save**.

Note:

You should do a Modular Messaging synchronization, if you are assigning a new voice mailbox number to a provisioned user. If you assign a new voice mailbox number to a user in the administration application but do not synchronize Modular Messaging, the Message icon does not appear for the user in the Avaya one-X® Portal client application. See Scheduling Modular Messaging Synchronization.

Related topics:

Assigning a Telephony resource to a user on page 179
Assigning a Voice Messaging resource to a user on page 180
Assigning a Conferencing resource to a user on page 181
Assigning a Presence resource to a user on page 182

Assigning a Telephony resource to a user

You can also use the Administration Command Line Interface to assign resources to users on Avaya one-X® Portal.

To perform bulk import of users, see the Administration Command Line Client online help.

1. In the Administration application, click the **Users** tab.
2. From the left pane, select **Portal Users**.
3. Search for and select the user to whom you want to assign the resource.
4. In the **Telephony** group box, click **Add**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the Communication Manager server.

b. In the **Display Name** field, type a descriptive name for this resource which users will see in the Avaya one-X® Portal.

c. In the **Display Address** field, type the text to display in the Avaya one-X® Portal for this extension.

d. In the **Extension** field, type the extension assigned to the user.

e. In the **Password** field, type the password for the extension.

6. Select the service you want to modify for the user by clicking **Add** or **Update**.
7. Make the desired changes to the service.
8. Click **Save** to save your changes.
9. Click **Delete** to delete this resource.

Note:
You must disable the user before deleting a resource assigned to the user.

10. After making changes to all of the user resources, click **Finished**.

Assigning a Voice Messaging resource to a user

You can also use the Administration Command Line Interface to assign resources to users on Avaya one-X® Portal .

To perform a bulk import of users, see the Administration Command Line Client online help.

1. In the Administration application, Select the **Users** tab.
2. In the left navigation pane, select **Portal User**.
3. If necessary, search for and select the user to whom you want to assign the resource.
4. In the **Voice Messaging** group box, click **Add**.
5. Complete the following fields:

a. From the **Server** drop-down list, select the handle of the Modular Messaging server.

b. In the **Display Name** field, enter a descriptive name for this resource which users see in the Avaya one-X® Portal .

c. In the **Display Address** field, enter text to display in Avaya one-X® Portal for this mailbox.

d. In the **Mailbox** field, enter the mailbox assigned to the user.

e. In the **Password** field, enter the password for the mailbox and confirm it in the **Password** field.

6. Select the service you want to modify for the user by clicking **Add** or **Update**.
7. Make the desired changes to the service.
8. Click **Save** to save your changes.
9. Click **Delete** to delete this resource.

Note:
You must disable the user before deleting a resource assigned to the user.

10. After making changes to all of the user resources, click **Finished**.

Assigning a Conferencing resource to a user

You must assign a conferencing resource for all users who need to access conferencing in Avaya one-X® Portal. Users do not have permissions to add or delete conferencing resources in their Avaya one-X® Portal settings. Users can only update an existing conferencing resource.

Note:
To enable users to have access to conferencing feature, you must enable the user in Meeting Exchange as well.

You can also use the Administration Command Line Interface to assign resources to users on Avaya one-X® Portal.

To perform a bulk import of users, see the Administration Command Line Client online help.

1. In the Administration application, select the **Users** tab.
2. In the left navigation pane, select **Portal User**.
3. If necessary, search for and select the user to whom you want to assign the resource.
4. In the **Conferencing** group box, click **Update**.
5. Complete the following fields:
   a. From the **Server** drop-down list, select the handle of the Conferencing server.
   b. In the **Display Name** field, enter a descriptive name for the resource that users see in Avaya one-X® Portal.
   c. In the **Display Address** field, enter text to display in Avaya one-X® Portal for this conferencing account.

d. In the **Moderator Code** field, enter the host code assigned to the account.

e. In the **Participant Code** field, enter the participant code assigned to the account.

f. In the **PIN Code** field, enter the unique PIN code assigned to the account.

Each user must have a unique PIN Code. If duplicate PIN Codes are assigned, the users with the duplicate PIN codes are not able to participate in bridge conferences if another user with the same PIN code is already participating in a conference.

g. In the **Bridge Number** field, enter the telephone number that the user dials to log in to the bridge.

h. In the **Bridge Number Backup** field, enter the secondary telephone number that the user can dial to log in to the bridge.

6. Click **Save** to save your changes.
7. Click **Reset** to reset the page settings.
8. After making changes to all resources of the user, click **Finished**.

Assigning a Presence resource to a user

You must assign a presence resource to all users who want to publish their presence state to watchers on Avaya one-X® Portal.

You can also use the Administration Command Line Interface to assign resources to users on Avaya one-X® Portal.

To perform a bulk import of users, see the Administration Command Line Client online help.

1. In the Administration application, select the **Users** tab.
2. In the left navigation pane, select **Portal User**.
3. If necessary, search for and select the user to whom you want to assign the resource.
4. In the **Presence Information** group box, click **Update**.
5. Complete the following fields:

a. From the **Server** drop-down list, select the handle of the AIPS server.

b. In the **Display Name** field, enter a descriptive name for the resource that users see in Avaya one-X® Portal.

c. In the **Display Address** field, enter text to display in Avaya one-X® Portal for this presence account.

d. In **SES ID** field, enter `presence`.

e. In **Password** and **Confirm** fields, enter `presence`.

6. Click **Save** to assign the server to the user.
7. After making changes to all of the user resources, click **Finished**.
8. Click **Delete** to delete this resource.
   You must disable the user before deleting a resource assigned to the user.

Configuring the URLs of Avaya one-X Portal Administration and Client Applications (Optional)

Administrators can configure the URLs of one-X Portal administration and client applications to simplify them. This change is made by modifying a script file. This script restarts the server, therefore users must do this process in the maintenance window hours.

To configure the URLs, perform the following steps:

1. Log in to the one-X Portal console.

   Note:
   You can also do a ssh session with the one-X Portal server.
2. Open the directory where one-X Portal is installed and press Enter.
   For example, `cd /opt/avaya/1xp`
3. Type `vi configappurls.py` and press Enter.
4. Scroll down to the bottom of the screen.
5. In the `setAppContextRoot ("1XP_Client_Portal","");`, enter any value that you want the user to enter after the server IP address to access the one-X Portal client application.
   For example, if you want the URL of the one-X Portal client application to be <one-X Portal server IP address>/client, then enter `client` in between the inverted commas.
6. Similarly, in `setAppContextRoot ("1XP_Client_Admin","admin");` ,enter a string for the one-X Portal administration application in place of **admin**.
7. Press Esc+:+ x+ ! to save the changes.
8. In the console, type **ls -l runcon*.sh** to check whether the **`runconfigappurls.sh`** script file has executable permission or not.

- if the **runconfigappurls.sh** script file is executable, the system returns the value as `-r-xr-xr-x`
- if the **runconfigappurls.sh** script file is not executable, the system returns the value as `-r--r--r--`

9. If the **runconfigappurls.sh** script file is not executable, type `chmod +x runconfigappurls.sh` and press Enter.
   This makes the **runconfigappurls.sh** script file executable.
10. Type `./runconfigappurls.sh <was_home> <1xp_install_dir> <was_user>< was_password>` to save the changes made to the one-X Portal admin and client URLs.
    Type `./runconfigappurls.sh /opt/IBM/WebSphere/AppServer/opt/avaya/1xp/ admin Avaya123`, where `<was_home>` = `/opt/IBM/WebSphere/AppServer/`, `<1xp_install_dir>` = `/opt/avaya/1xp/`, `was_user` = `admin`, and `was_password` = `Avaya123`.
11. Restart the one-X Portal server.
12. You can now verify the changes by using the new URLs to access the one-X Portal administration and client applications.

Configuring Avaya one-X® Portal for HTTPS access

You need to always use SSL authentication when you access Avaya one-X® Portal.

Note:

You do not have to use HTTPS for overall Portal use, but when you try to login to Avaya one-X® Portal, you always get a secure login page using HTTPS. If you use an HTTP URL to access the login page, you are logged in through HTTPS but then further access to other pages after logging in is through HTTP.

Avaya one-X® Portal supports access through `https://` protocol. After you install a secure server certificate obtained from a certifying authority such as VeriSign, Thawte, or GTE CyberTrust, users can confidently connect to Avaya one-X® Portal from outside your firewall.

1. Obtain a secure site certificate for SSL:
   a. Generate SSL authentication keys and a certificate request, as described in the procedure provided by the certifying authority.

b. Submit the certificate request to a certifying authority such as VeriSign, Thawte, or GTE CyberTrust.

2. Import the signed certificate and configure the Avaya one-X® Portal server for SSL as described in the documentation provided by IBM.
For example, see *IBM WebSphere v6.1 Security* from the IBM WebSphere handbook series.

WebSphere security adjustments for Avaya one-X® Portal

This section describes the procedures for creating and activating a self-signed and self-addressed certificate during one-X Portal deployment. If you are upgrading from Avaya one-X® Portal 1.1 and have already created and activated a certificate, you can skip this section. content for the first section.

1. Creating a new WebSphere certificate after upgrade from Avaya one-X® Portal 1.0 or 1.1 to Avaya one-X® Portal 5.2.

   - In this scenario, WebSphere is upgraded from 5.0 to 6.0, which means original WebSphere certificates are preserved.
   - When the upgrade from 5.0 to 6.0 is completed, the CN=jserver certificate is preserved, which does not match the machine's Fully Qualified Domain Name (FQDN) and the browser warns the user of an invalid certificate. Even if jserver certificate is loaded to the browser's certificate store, depending on the browser, the warning continues to display the next time a connection is attempted to Avaya one-X® Portal.

     The solution is to replace the jserver certificate with a self-signed certificate.

     Note:

     On fresh installs, WebSphere 6.1 creates a certificate with appropriate CN.

2. Replacing WebSphere 6.1 certificate.

   Some customers do want to create their own certificate, or periodically replace the self-signed certificate which comes with WebSphere. One might create a new certificate in WebSphere, but it needs to be made active in the WebSphere.

Related topics:

Creating a new certificate on page 186
Extracting a certificate on page 186
Adding a certificate on page 187
Activating a certificate on page 187

Creating a new certificate

You can skip this procedure if you are doing a fresh installation because this is already done during WebSphere installation. This procedure is recommended when you upgrade from Avaya one-X® Portal 1.0 or 1.1 to 5.2.

1. Login as Administrator to WebSphere console.
2. Go to **Security** > **SSL Certificate and Key Management**.
3. Go to **Key Stores and Certificate**.
   a. Click **NodeDefaultKeyStore**.
   b. Click **Personal Certificates**.
   c. Select **Create a Self-signed Certificate**.
   d. Enter certificate alias (Avaya suggests to keep this value to default).
   e. Enter FQDN for this machine.
   f. Enter Organization name.
   g. Enter other optional values.
   h. Click **OK**.
   i. Save the configuration.

Extracting a certificate

You can extract a certificate from key or trust stores. This procedure is constructed using NodeDefaultKeyStore as the starting point.

1. Login as Administrator to the WebSphere console.
2. Go to **Security** > **SSL Certificate and Key Management**.
3. Click **Key Stores and Certificates**.
4. Click **NodeDefaultKeyStore**.
5. Click **Personal Certificates**.
6. Select the certificate you want to extract.
7. Click **Extract**.

8. Enter the file name (Avaya suggests you to *\tmp\default.pem*).
9. Click **OK**.

Adding a certificate

If you want to use a certificate as the default WebSphere certificate, it should exist in the key (Personal) and trust (Signer) stores. The procedure is created using NodeDefaultTrustStore, as starting point.

1. Login as Administrator to WebSphere console.
2. Go to **Security** > **SSL Certificate and Key Management**
3. Click **Key Stores and Certificates**
4. Click **NodeDefaultTrustStore**
5. Click **Signer Certificates**.
6. Click **Add**.
7. Enter alias for this certificate.
8. Enter file name where certificate is located.
9. Click **OK**.
10. Save configuration.

Activating a certificate

1. Log on as Administrator to WebSphere console.
2. Go to **Security** > **SSL Certificate and Key Management**.
3. Go to **SSL Configurations**.
4. Click **NodeDefaultSSLSettings**.
5. Select **Get Certificate Aliases**.
6. Select default server and client aliases.
7. Click **OK**.

8. Save configuration.
9. Restart the WebSphere.

Administration Application interface

Servers field descriptions

Telephony server field descriptions

Name	Description
Type	The type of switch configured on the system. For Communication Manager, displays CM.
Version	The version of the switch configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Telephony server.
Enabled	When selected by the administrator, enables the server for the system.
PBX Name for AES	The SwitchConnection name of the AE Services server associated with the Telephony server. This field is case sensitive. Enter the exact name of the PBX as defined in the AE Services. In AE Services, go to **Communication Manager Interface** > **Switch Connections** > **Switch Connection Name**.
EC500 Enable Code	The feature access code used by the Telephony server to enable Extension to Cellular on Avaya one-X® Portal, for example, *88, *89, *87.

Name	Description
	Contact the local Communication Manager administrator to get the code configured on the system.
EC500 Disable Code	The feature access code used by the Telephony server to enable Extension to Cellular on Avaya one-X® Portal, for example, *88, *89, *87. Contact the local Communication Manager administrator to get the code configured on the system.
EC500 Modify Code	The feature access code used by the Telephony server to enable Extension to Cellular on Avaya one-X® Portal, for example, *88, *89, *87. Contact the local Communication Manager administrator to get the code configured on the system. This code is also known as the Extension to Cellular self-administer code.
Host	The network address of the server as an IP address (of the CLAN card) or a DNS host name. This IP address is the Communication Manager IP address that is accessible by the clients, where the VOIP client establishes the VOIP (H.323) connection. Thus, the VOIP connection is established using the CLAN IP address. Since VOIP connection in Avaya one-X® Portal requires Communication Manager to support G.711 codec, CLAN should be configured to support G.711. Communication Manager can be configured with two sets of IP addresses: one set open for the public, and another set for a private network used to communicate with AE Services. If the H.323 connection between AE Services and Communication Manager uses a private network, you must configure AE Services with an H.323 Gatekeeper list. This configuration alerts the Telephony server to request that AE Services use that list for communication with Communication Manager.
AES Servers - Available	The handles of the AE Services servers configured on Avaya one-X® Portal. Select a server and click **Add** to move it to the **Selected** field.
AES Servers - Selected	The handles of the AE Services servers selected for this Telephony server. Select a server and click **Remove** to move it to the **Available** field.
Dial Plan	The handle of the Dial Plan used by this server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Avaya one-X® Portal.

Name	Description
Test	Tests the new or updated server settings and gives the results immediately. In case of errors, you can make the necessary corrections at once.

Auxiliary server (AE Services) field descriptions

Name	Description
Type	The type of server configured on the system. For AE Services, displays AES.
Version	The version of the server configured on the system. For AE Services, displays 4.2.2 or 5.2. If using AES 4.2.2 or 5.2, the behavior of the server will be the same, and should be configured as AES 4.2.2 or 5.2 respectively.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the AE Services server.
Enabled	When selected by the administrator, enables the server for the system.
AES Machine Name	The hostname of the AE Services server. Use the hostname command on the AES machine to get this host name.
CM Servers Associated with this AES	A list of the CM servers that are associated with the selected AE Services server.
DMCC Host	The network address used by the **DMCC** configuration for the AE Services server as an IP address or a DNS address. **Note:** Device, Media, and Call Control (DMCC) is one of the services provided by AE Services. The DMCC service enables access to device, media, and basic third-party call control capabilities of Communication Manager.
DMCC Port	The port number used by the **DMCC** configuration for the AE Services server.
DMCC Login ID	The log-in ID used by the **DMCC** configuration for the AE Services server. The number of characters in this entry must not exceed the character length limitation in **DMCC**.
DMCC Password	The password associated with the log-in ID used by the **DMCC** configuration for the AE Services server. The number of characters in this entry must not exceed the character length limitation in **DMCC**.

Name	Description
DMCC Confirm	Verification of the password associated with the log-in ID used by the **DMCC** configuration for the AE Services server.
TSAPI Host	The network address used by the **TSAPI** configuration for the AE Services server. **Note:** Telephony Server API (TSAPI) is an API which provides a full complement of third-party call control capabilities such as controlling specific calls or stations, routing of incoming calls, receiving notifications of events, invoking Communication Manager features, and querying Communication Manager for information.
TSAPI Port	The port number used by the **TSAPI** configuration for the AE Services server.
TSAPI Login ID	The log-in ID used by the **TSAPI** configuration for the AE Services server. The number of characters in this entry must not exceed the character length limitation in **TSAPI**.
TSAPI Password	The password associated with the log-in ID used by the **TSAPI** configuration for the AE Services server. The number of characters in this entry must not exceed the character length limitation in **TSAPI**.
TSAPI Confirm	Verification of the password associated with the log-in ID used by the **TSAPI** configuration for the AE Services server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Avaya one-X® Portal.
Test	Tests the new or updated server settings and gives the results immediately. In case of errors, you can make the necessary corrections at once.

Voice Messaging server field descriptions

Name	Description
Type	The type of server configured on the system. For the Modular Messaging server, displays MM.
Version	The version of the server configured on the system. For Modular Messaging, displays *4.0* or *5.2* or *6.x*.

Name	Description
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Voice Messaging server.
Enabled	When selected by the administrator, enables the server for the system.
Initial Number of Server Connections	The minimum number of Avaya one-X® Portal user connections needed to communicate with the Voice Messaging server of the MSS of the Modular Messaging server.
Max Number of Server Connections	The maximum number of Avaya one-X® Portal server connections that can be assigned to the Voice Messaging server. The default value is 200, the maximum number of connections allowed is 2200.
Client Connections Increment	The number of times to increment the connections based on the number of users in the connections. For example, if this value is 2 and there are 100 users per connection, the connections are incremented every 200 users.
Users Per Client Connection	The number of users assigned per connection to the Voice Messaging server.
Messages Temp Directory	The location of the temporary directory where sections of voice mail message are stored. When creating a new Voice Messaging server, enter either the name of the default directory /msgWorkDir or the name of the directory you created for the Voice Messaging server. See Creating a directory for the Voice Messaging server.
Temp Purge Interval	The number of minutes that the sections of voice mail messages can remain in storage before the temporary directory is purged and the sections are deleted.
Mail Domain	The fully qualified domain name of the MSS of the Modular Messaging server.
SSL Certificate	Indicator for an SSL Certificate for this server. • Displays **SSL Certificate Exists** if the security certificate exists for this server. • Press **Retrieve SSL Certificate** button if the security certificate for this server is not found. The security certificate is retrieved for the server.
Dial Plan	The handle of the Dial Plan used by this server.
IMAP Host	The network address of the MSS of the Modular Messaging Server. This field must include an IP address, not a fully qualified domain name.
IMAP Port	The secure port number used by the **IMAP** configuration for the Voice Messaging server.

Name	Description
IMAP Login ID	The secure log-in ID used by the **IMAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Password	The secure password associated with the log-in ID used by the **IMAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
IMAP Confirm	Verification of the password associated with the log-in ID used by the **IMAP** configuration for the Modular Messaging server.
IMAP Secure Port	If you select this option, Avaya one-X® Portal requires a secure **IMAP** connection for the Voice Messaging server. Verify that this port is the correct port for a secure connection.
SMTP Host	The network address of the MSS of the Modular Messaging Server. This field must include an IP address, not a fully qualified domain name.
SMTP Port	The port number used by the **SMTP** configuration for the Voice Messaging server.
SMTP Login ID	The secure log-in ID used by the **SMTP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Password	The secure password associated with the log-in ID used by the **SMTP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
SMTP Confirm	Verification of the password associated with the log-in ID used by the **SMTP** configuration for the Modular Messaging server.
SMTP Secure Port	If selected, indicates **SMTP** is configured to use a secure connection for the Voice Messaging server. A secure **SMTP** connection to the Voice Messaging server is optional.
LDAP Host	The network address of the MSS of the Modular Messaging Server. This field must include an IP address, not a fully qualified domain name.
LDAP Port	The port number used by the **LDAP** configuration for the Voice Messaging server. Use a nonsecure port.
LDAP Login ID	The log-in ID used by the **LDAP** configuration for the Voice Messaging server. This ID must match the name used for the **Trusted Server Name** in your Voice Messaging server.

Name	Description
LDAP Password	The password associated with the log-in ID used by the **LDAP** configuration for the Voice Messaging server. This password must match the password used for the **Trusted Server Name** in your Voice Messaging server.
LDAP Confirm	Verification of the password associated with the log-in ID used by the **LDAP** configuration for the Modular Messaging server.
LDAP Secure Port	Do not select this field. Avaya one-X® Portal does not support a secure **LDAP** connection for the Voice Messaging server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Avaya one-X® Portal.
Test	Tests the new or updated server settings and gives the results immediately. In case of errors, you can make the necessary corrections at once.

Conferencing server field descriptions

Name	Description
Type	The type of server configured on the system. For Conferencing, displays MX.
Version	The version of the server configured on the system. For Conferencing , displays 5.1.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Conferencing server.
Enabled	When selected by the administrator, enables the server for the system.
BCAPI Logger Directory	The path name of the directory where information about **BCAPI** issues is stored. See Creating a directory for the Conferencing server.
Dial Plan	The handle of the Dial Plan used by this server.
BCAPI Host	The network address that the **BCAPI** configuration uses for the Conferencing server as an IP address or a DNS address.
BCAPI Login ID	The log-in ID that the **BCAPI** configuration uses for the Conferencing server.

Name	Description
	The number of characters in this entry must not exceed the character length limitation in **BCAPI**.
BCAPI Password	The password associated with the log-in ID that the **BCAPI** configuration uses for the Conferencing server. The number of characters in this entry must not exceed the character length limitation in **BCAPI**.
BCAPI Confirm	Verification of the password associated with the log-in ID used by the **BCAPI** configuration for the Conferencing server.
BCAPI Secondary Login ID	The **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.
BCAPI Password	The password associated with the **Secondary Login ID** used by the **BCAPI** configuration for the Conferencing server.
BCAPI Confirm	Verification of the password associated with the secondary log-in ID used by the **BCAPI** configuration for the Conferencing server.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Avaya one-X® Portal.
Test	Tests the new or updated server settings and gives the results immediately. In case of errors, you can make the necessary corrections at once.

Presence server field descriptions

Name	Description
Type	The type of server configured on the system. For the Presence Services, displays apas.
Version	The version of the server configured on the system. For the Presence Services , displays 1.0.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Presence Services.
Enabled	When selected by the administrator, enables the server for the system.

Name	Description
IPS Publish To Port	The port number on the Presence Services where the presence information of the user is published.
LPS Consumer Port	The port number on the Presence Services that receives the consumer information.
LPS Supplier Port	The port number on the Presence Services that furnishes the published the information.
UMS URL	The URL that is used to access the Web based User Management Service.
LPS Host	The network address used by this configuration of the Local Presence Service as an IP address or a DNS address.
LPS Port	The port number used by this configuration of the Local Presence Service.
UMS Host	The network address used by this configuration of the User Management Service as an IP address or a DNS address.
UMS Port	The port number used by this configuration of the User Management Service.
UMS Login ID	The log-in ID used by this configuration of the User Management Service.
UMS Password	The password associated with the log-in ID used by this configuration for the User Management Service.
UMS Confirm	Verification of the password associated with the log-in ID used by this configuration for the User Management Service.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Avaya one-X® Portal.

Dial Plan field descriptions

Name	Description
Handle	The unique name assigned to the server by the administrator.
Phone Numbers PBX Main	A sample of a valid telephone number on the switch. The Dial Plan compares this number with other telephone numbers to determine whether a telephone number is internal or external.

Name	Description
Phone Numbers Automatic Routing Service	The digit to prefix before an outbound phone number is dialed on the PBX. For example, in the phone number 9-1-800-8888, 9 is the **Automatic Routing Service** number.
Prefixes Regional	The area code of the region.
Prefixes Inter-Regional	The digit to dial between area codes in an **Inter-Regional** phone call.
Prefixes International	The digits to prefix to place an **International** phone call. For example, in the phone number 011-1-800-8888, 011 is the **International** prefix code.
Number of Digits National Call Maximum	The maximum number of digits allowed in a domestic telephone call. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Local Call	The maximum number of digits in a telephone call within an area code. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Extension to Extension Call	The maximum number of digits allowed in a phone extension at the enterprise. Typically, this value is 7 or less.
OK or **Save**	**OK** used on Add/Create pages saves the new resource. **Save** used on Modify pages saves updates to the resource. See Dial Plan services on page 139 for more details.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Avaya one-X® Portal.
Test	Tests the new or updated server settings and gives the results immediately. In case of errors, you can make the necessary corrections at once.

Mobility Extension Bank field descriptions

Name	Description
Description	The unique name assigned to the Mobility Extension Bank . When modifying a Mobility Extension Bank , you can change this value.
Telephony Server	The unique name assigned to the Telephony server associated with the Mobility Extension Bank .

Name	Description
	When adding a new Mobility Extension Bank , select the Telephony server before you configure the Mobility Extension Bank When modifying a Mobility Extension Bank , you can change this value.
1st Extension	The first extension phone number to which you want to map the Mobility Extension Bank .
# To Add	The number of extensions to add. For example, if this extension in the **1st Extension** field is 5500, and the number to add is 5, the system adds extensions 5500, 5501, 5502, 5503, and 5504.
Extension	The extensions entered above are listed here. Select **Delete** next to the extension, and then click **Save** to remove the extension from the list.
Password	Enter a password for each of the extensions on the list for security purposes.
Confirm	Re-enter the same password verify authentication with the extension.
Description	If you want to change the description of the Mobility Extension Bank , you can do it here.
Telephony Server	If you want to change the Telephony server to which the Mobility Extension Bank is assigned, you can do it here.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the extension from Avaya one-X® Portal.

Scheduler field descriptions

Name	Description
Enabled	Enables scheduling of cleanup or synchronization settings when selected.
Schedule Mode	Lists the various scheduling options for the specified task. For Enterprise Directory Servers, pertains to Full and Incremental synchronizations. For Statistics Cleanup, pertains to Usage and Performance statistics.
Daily	Schedules the task to run every day at the specified time.
Weekly	Schedules the task to run every week on the specified day of the week.

Name	Description
Monthly	Schedules the task to run every month at a specified day of the month.
Week of the Month	Specifies the week of the month to run the task.
Day of the Week	Specifies the day of the week to run the task.
Day	For a **Daily** schedule, this field is disabled. For a **Weekly** schedule, specifies the day of the week on which to run the task. For a **Monthly** schedule, specifies the day of the month (1-31) on which to run the task.
Hour	For all schedule types, specifies the hour of the day (0-23) on which to run the task.
Minute	For all schedule types, specifies the minute of the specified hour (0-59) on which to run the task.

Backup File to Location	For database backup, specifies the path name of the directory where the backup file is to be stored.
	Note:
	To specify a location for the database backup file in the Administration application, go to the **Scheduler** > **Database Backup** tab and specify the location in the **Backup File Location** field.
	To create a directory with full permission to the owner and the group for the dbinst user on the Avaya one-X® Portal server, log in to the Avaya one-X® Portal server as root.
	`su - dbinst`
	`mkdir /home/dbinst/backups`
	`cd ..`
	`chown dbinst backups`
	`chgrp dbinst backups`
	Avaya recommends that you create a directory called `/home/dbinst/backups`.

Run Now	Runs the task immediately to incorporate recent changes. This button allows the task to be run one time per change. **Note:** Some tasks, such as database backup and Directory Server Synchronization, affect the operation of the system.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Task Status	The **Task Status** fields include the **Time**, **Task ID**, **Task Type**, and **Task Status** of the scheduling task.

Name	Description
	The **Task Status** fields display a list of previous schedule runs, which shows the history of this task. When you start a new task run, leave the Scheduler page, and return to display the status of the current run. The system no longer displays the previous runs. You must leave the Scheduler page to update the status of the run. At the end of the run, the system displays a success or failure message.

System field descriptions

Related topics:

[General Settings field descriptions](#) on page 200
[Enterprise Directory field descriptions](#) on page 201
[License server field descriptions](#) on page 203
[SNMP Traps field descriptions](#) on page 204
[SNMP destinations field descriptions](#) on page 204
[Statistics field descriptions](#) on page 206
[Logging field descriptions](#) on page 206
[JDBC field descriptions](#) on page 210

General Settings field descriptions

The General Settings page displays the following fields:

Name	Description
URL	The Web address or the e-mail address used to contact the system administrator or technical support in the event of an issue with Avaya one-X® Portal.
Product ID	The product ID code that is used for alarming and identifying which unique product is generating the alarm. This number is issued when Avaya one-X® Portal is registered for technical support.
Save	Exits the page with the current settings saved.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Enterprise Directory field descriptions

The Enterprise Directory Domains page displays the following fields:

Name	Description
Domain	The name assigned to the domain in the Active Directory. For example, enter the **User** domain as <*NNNNN*>.xyz-corp.com, and the **Resource** domain as <*nnnn*>pptdomain.xyz-corp.com. The **Contact** domain is the same as the **User** domain. You can add Contact domain with another name. You cannot add a User or a Resource domain.
Type	Indicates how the domain is used. The same domain can be used in more than one way. • **User**. Indicates the domain contains the Avaya one-X® Portal users. There is only one user domain. You cannot change this domain. • **Resource**. Indicates the domain contains the Avaya one-X® Portal security groups. There is only one resource domain. You cannot change this domain. • **Contact**. Indicates the domain contains enterprise address book information. The user domain is always the first contact domain. You can add up to four more contact domains.
Primary Server	The IP address of the primary Directory server for the domain.
Has Backups	Indicates if there are secondary Directory servers for this domain by displaying Yes or No.

The Add Enterprise Contact Domains page displays the following fields:

Name	Description
Host	The network address of the server as an IP address.
Port	The port number used by the server.
Login ID	The log-in ID used by the server.
Password	The password associated with the Login ID used by the server.
Confirm	Reenter the password associated with the Login ID used by this server.
Base DN	The Distinguished Name (DN) of a node in the domain that identifies which part of the domain is used. If blank, the entire domain is used. You can change this value to improve search performance. However, changes may exclude information from other parts of the domain.
Page Size	The number of names returned by the Enterprise Directory server per query.

Name	Description
Range Size	The number of values for an attribute that are returned by the Enterprise Directory server per query. The attributes include names and phone numbers. For example, if a security group contains 1,000 members, you can retrieve the members 200 at a time.
OK	Exits the page with the current settings saved.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

The View Enterprise Directory Domain page displays the following fields:

Name	Description
Domain	The name assigned to the domain in the Active Directory.
Type	Indicates how the domain is used. The same domain can be used in more than one way. • **User** domains are fixed. There can only be one domain, and the domain attributes, such as name and type, cannot be changed. **User** domains can contain user records, security group information, and contact information. • **Resource** domains are fixed as well and they contain security group information. • **Contact** domains can be added and modified. They contain the contact information used by users.
Description	A description entered by the user to help identify the Contact domain. This can be anything the user creates.
Enable	Select this check box to enable the Enterprise Directory domain.
Base DN	The Distinguished Name (DN) used by the LDAP server.
Login ID	The log-in ID used by the server.
Password	The password associated with the Login ID used by the server.
Confirm	Reenter the password associated with the Login ID used by this server.
Server	The number assigned to each Enterprise Directory server connected to the domain to determine the failover order. Number 1 is the primary server. Numbers 2 to n are secondary servers. In the event of a failure, server failover starts at number 2.
Host	The network address of the server as an IP address.
Port	The port number used by the server.
Secure Port	When checked, the port number used by the server is secure.
Page Size	The number of names returned by the Enterprise Directory server per query.

Name	Description
Range Size	The number of values for an attribute that are returned by the Enterprise Directory server per query. The attributes include names and phone numbers. For example, if a security group contains 1,000 members, you can retrieve the members 200 at a time.
Add Server	Adds another server to the domain. Complete the fields for the new server and use the **Move Up** and **Move Down** buttons for each of the servers in the domain to create the server failover order. Use the **Mark For Delete** button to delete a server from the domain.
Save	Exits the page with the current settings saved.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.

License server field descriptions

License Server configuration page displays the following fields:

Name	Description
Host	The network address of the server as an IP address.
Port	The port number used by the server.
Secure Port	If selected, indicates the system is configured to use a secure connection for the License server.
URL	The Web address where the WebLM server is installed.
Mode	The status of the current mode of the WebLM server as Error, Restricted, or Normal.
Mode Last Changed	The date and time that the license mode of the WebLM server last changed.
Server Up	The running status of the WebLM server as **Yes** or **No**. If set to no, the WebLM server is unreachable.
Server Last Changed	The date and time that the running status of the WebLM server changed.
Product Name	The name of the product, Avaya one-X® Portal.
Feature Name	The name of the feature which provides the number of licensed users.
Desired Units	The requested number of license units.

Name	Description
Acquired Units	The acquired number of license units. Used to determine if the number of licenses were over provisioned.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

SNMP Traps field descriptions

The SNMP Traps page displays the following fields:

Name	Description
Trap Name	The unique name assigned to the SNMP Trap (event notification).
Description	Brief description of the SNMP Trap.
Check All	Selects all of the SNMP Traps and enables them. Select the check box next to the SNMP Trap to enable that trap only.
Uncheck All	Selects all of the SNMP Traps and disables them. Select the check box next to the SNMP Trap to disable that trap only.

SNMP destinations field descriptions

Name	Description
Handle	The unique name assigned to the server by the administrator.
Enable	Enables the configuration of the SNMP trap.
Device	The device to which traps are generated. The selections are: • **SSG**. The Avaya Services Security Gateway. Only INADS traps are sent here. • **NMS**. Industry standard Network Monitoring Software, such as HP Openview or IBM Tivoli. INADS traps are not sent here.
Host	The **IP Address** of the **Device** that receives the traps.
Port	The TCP/UCP port number used when sending the traps.
Notification Type	Indicates the method of notification for this destination.

Name	Description
	The selections are: • **Trap**. Notification is sent using the SNMP Trap command. There is no handshake with the receiver of the trap to verify it was received. Trap can be used with all versions of SNMP. • **Inform**. Notification is sent using the SNMP Inform command. The receiver sends a response packet to indicate the notification was received. Inform can only be used with SNMP versions 2c and 3.
SNMP Version	Indicates the version of SNMP to use for this destination. You can select from three versions: 1, 2c, and 3.
User Name	Indicates the user name associated with this destination. For security reasons, you cannot enter the words "public" or "private" in this field.
Security Level	Indicates the security level assigned to this destination. The selections are: • **None**. Do not use the authentication and privacy fields. • **Authentication**. Use the authentication fields only. • **Privacy**. Use the privacy fields only. • **Authentication and Privacy**. Use both the authentication and privacy fields.
Authentication Protocol	Indicates the Authentication protocol to use to authenticate SNMP version 3 messages. The selections are **None**, **MD5**, or **SHA**.
Authentication Password	Indicates the Authentication password for authenticated SNMP version 3 messages.
Confirm	Reenter the Authentication password for verification.
Privacy Protocol	Indicates the Privacy Protocol used to encrypt SNMP version 3 messages. Select from **DES**, **AES128**, **AES198**, or **AES256**.
Privacy Password	Indicates the Privacy password for encrypted SNMP version 3 messages.
Confirm	Reenter the Privacy password for verification.
OK	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Exits the destination.

Statistics field descriptions

The Statistics configuration page displays the following fields for Performance Statistics and Usage Statistics:

Name	Description
Enable Collection	Indicates that the system collects the specified statistics, Performance or Usage or both.
Collection Interval	The duration in which the system collects the specified statistics. Select from 1 to 240 minutes.
Retention Period	The number of days that the system keeps the collected statistics. Select from 1 to 90 days.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Logging field descriptions

The **Logging** configuration page displays the following fields.

Name	Description
General Logging	Avaya one-X® Portal logging that provides high-level system information. Generally, the system writes the logs to SystemOut.log and also to trace.log if any of the Protocol, Aspect, and/or Other Loggers are activated.
Level	The level of **General Logging** to run from the following options: **All**, **Fatal**, **Error**, or **Warning**.
Protocol Logging	Low-level logging that debugs issues with the protocols used by Avaya one-X® Portal. The system generates messages for debugging protocol exchanges. For example, SMTP or SIP. The system writes the logs only to trace.log.
Protocol	The protocol for which you want to run logging. Select the desired protocol from the drop-down list.
Level	The level of logging to run for protocol logging levels. You can select from **Summary** or **Traffic** (detailed).

Name	Description
List of Current Protocol Loggers	The Protocol Level logger. • **api**. Debugs general client issues. The client API uses this protocol in Avaya one-X® Portal. • **bcapi**. Debugs conferencing issues. Conferencing services use this protocol to connect to Conferencing. • **cmapi**. Debugs Telephony issues. For example, Other Phone log in problems and EC500 issues. • **cmcontact**. Reports the communication between the Telephony Adapter and the Contact Services. • **cmstore**. Reports database information. Telephony services use this protocol to report information that is stored in the database. • **contlogtrim**. Used by the service that trims Contact Logs. • **crypt**. Used by Encryption/Decryption methods. • **fwclient**. Used to view traffic between client and service layers. The protocol used by framework client. • **fwintercept**. Used by Service Framework during method intercept. • **fwservice**: Used by Service Framework. • **imap**. Used to connect to Modular Messaging. Use this protocol to debug messaging problems. • **jtapi**. Used to connect to Communication Manager. Telephony services use this as one of the protocols to connect to Communication Manager. Use this to resolve Telephony issues. • **lps**. Debugs Presence issues. Presence service uses this protocol to connect to the Avaya Aura®Presence Services. • **snmp**. Used by Alarm service to issue SNMP notifications. • **spectel**. Debugs Conferencing issues. Conferencing services use this as one of the protocols to connect to Conferencing. • **weblm**. Debugs licensing issues. The Avaya one-X® Portal uses this protocol to connect to the licensing services.
Aspect Logging	Low-level logging used to debug issues with the Avaya one-X® Portal components. The system generates messages for debugging subsystem activity. For example, Telephony or Conferencing. This can be enabled for specific Users in the system. The system writes the logs only to trace.log.
Aspect	The Aspect for which you want to run logging. Select the desired protocol from the drop-down list.
Level	The level of logging to run for aspect logging levels. Selections are **Summary**, **Detail**, **Off**.

Name	Description
User ID	The identifier of the user for whom you want to debug a component issue. For example, you can debug a Telephony issue for a selected user. To turn logging on, the user must be specified.
List of Current Aspect Loggers	The available aspect loggers that help you to debug issues with protocols. • **admincli**. Logs the admin CLI client activities. The command line client logs to a file (by default acp_admin_cli.log) in the logs directory of the WebSphere profile. • **api**. Logs all the activity in the layer of code that the clients interact with. This is the Client API aspect that can be used to debug client issues. • **bulk**. Logs bulk operations information such as bulk import/export of users • **client**. Supports Portal Clients and all clients integrated with Avaya one-X® Portal. It is an end-client aspect that can be used to debug client issues. • **cmtelephony**. Logs Communication Manager Telephony activity for a specified user. If you do not specify a user, this logs information about the service. If you specify a user, this logs information about the user interaction with the telephony adapter. • **contactlog**. Used by the Service that writes Contact Logs. • **dirstores**. Logs the Directory Service activities. It reports information about the interactions with the LDAP providers, such as Directory Synchronization tasks and user group membership lookup. • **framework**. Logs Service Framework activities around ServiceMBean and ServiceRegistry. • **fwadmin**. Logs Service Framework application for Server Management Operations (administration). • **fwasync**. Logs Service Framework asynchronous method invocation. • **fwproxy**. Logs Service Framework proxy interface operations. • **ldapclient**. Specific for the LDAP client used to connect to the LDAP server. It logs low-level LDAP information, such as queries to LDAP server and responses. • **licensing**. Logs License Server activity. • **mmclient**. Logs activities, such as request and response, to and from Modular Messaging (voice messaging) service over client channel. • **mmldap**. Logs activities related to Modular Messaging directory synchronization. • **mmservice**. Logs activities on Modular Messaging (voice messaging) service.

Name	Description
	• **mmsystem**. Logs activities, such as request and response, to and from Modular Messaging (voice messaging) service over system channel. • **mxclient:**. Logs activities, such as request and response, to and from Conferencing (bridge conferencing) service over client channel. • **mxservice**. Logs activities on Conferencing Exchange (bridge conferencing) service. • **mxsystem**. Logs activities, such as request and response, to and from Conferencing (bridge conferencing) service over system channel. • **prsncclient**. Logs activities, such as request and response, to and from Presence service over client channel. • **prsncservice**. Logs activities related to Presence service. • **prsncsystem**. Logs activities, such as request and response, to and fromPresence service over system channel. • **statistics**. Logs runtime statistics collected by statistics service. At summary level, logs statistics at every collection interval. By default, this interval is 15 minutes. At detail level, logs statistics as they are collected. • **user**. Logs User Service activities.
Other Loggers	Low-level logging used to debug issues with non-Avaya and internal components. The system internal log messages that may be useful during development. The logs are written only to trace.log. This information is normally provided by the Services that support the product.
Logger	The name or identifier of the logger for which to run logging. For example, org.springframework.
Level	The level of logging to run for non-Avaya or internal loggers. Selections are **Fatal**, **Severe**, **Warning**, **Audit**, **Info**, **Config**, **Detail**, **Fine**, **Finer**, **Finest**, **All**.
List of Current Other Loggers	The other loggers, non-Avaya or internal, that are available for use to debug issues with components such as WebSphere or the Spring framework.
Trace Log File Settings	Trace-level logging.
File Name	The name of the trace log file. For example, ${SERVER_LOG_ROOT}/trace.log.
Maximum number of historical files	The maximum number of trace log files to retain before deleting the oldest file.
Rollover File Size (MB)	The maximum size of the trace log file, in megabytes, before the file is rolled over to another historical file.

Name	Description
Error Log File Settings	Error-level logging.
File Name	The name of the error log file. For example, ${SERVER_LOG_ROOT}/SystemErr.log
Maximum number of historical files	The maximum number of error log files to retain before deleting the oldest file.
Rollover File Size (MB)	The maximum size of the error log file, in megabytes, before the file is rolled over to another historical file.
System Log File Settings	System-level logging.
File Name	The name of the system log file. For example, ${SERVER_LOG_ROOT}/SystemOut.log
Maximum number of historical files	The maximum number of system log files to keep before deleting the oldest file.
Rollover File Size (MB)	The maximum size of the system log file, in megabytes, before the file is rolled over to another historical file.
Service Log File Settings	Service-level logging.
File Name	The name of the service log file. For example, ${SERVER_LOG_ROOT}/activity.log
Rollover File Size (MB)	The maximum size of the service log file, in megabytes, before the file is rolled over to another historical file.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

JDBC field descriptions

Name	Description
Database Name	The name or identifier assigned to the Avaya one-X® Portal database.
Max Connections	The maximum number of connections to the database that you can create in this connection pool. Once you reach this number, you cannot

Name	Description
	create new connections and you must wait until a connection currently in use is returned to the connection pool.
Min Connections	The minimum number of connections to the database that you can create in this connection pool. If the size of the connection pool is at or below this number, existing connections are not discarded.
Connection Timeout	The number of seconds a request for a connection to the database waits when no connections are available in the connection pool and no new connections can be created, because the maximum number of connections has been reached.
Aged Timeout	The time interval, in seconds, after which an idle or unused connection to the database is discarded. When set to 0, active connections to the database remain in the pool indefinitely. Set the **Aged Timeout** parameter higher than the **Reap Time** for optimal performance.
Unused Timeout	The time interval, in seconds, after which an idle or unused connection to the database is discarded. Set the **Unused Timeout** parameter higher than the **Reap Time** for optimal performance.
Reap Time	The time interval, in seconds, between connection pool maintenance runs to remove unused connections. The more often this parameter is run, the greater the efficiencies in connection pool management. Set the **Reap Time** parameter less than the values of **Aged Timeout** and **Unused Timeout**.
Save	Saves the current settings on the page.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.

Users field descriptions

Name	Description
User ID	The unique identifier assigned to the portal user by the administrator.
First Name	The first name of the portal user.
Last Name	The last name of the portal user.
Nick Name	The familiar or "nickname" used to identify the portal user.
State	The current state of the user.

Name	Description
	Select **Enabled** or **Disabled**.
Group	The name of the group profile, if any, to which the user is assigned. Select **Update** to edit this field.
Sessions **Login Time**	The log-in date and time (for example, Tues Mar 13 17:05:01 EDT 2007) of the session to which the user is logged in.
Sessions **Session Type**	The type of session (for example, Portal) to which the user is logged in.
Sessions **Logoff Session**	Select this option to log the user off the current session.
Sessions **Kill All Sessions**	Select this option to terminate all active sessions for the user.
Telephony	The **Telephony** fields pertain to the Communication Manager server used for Telephony services. Avaya one-X® Portal supports one Telephony resource per user.
Server	The name of the Communication Manager server to which the user is connected for Telecommuter, VoIP, Mobility, and other Telephony services.
Display Name	The name assigned to the phone extension used for Telephony services.
Display Address	The display address of the phone extension used for Telephony services.
Extension	The phone extension used for Telephony services.
Password	The password assigned to the user to gain access to Telephony services.
Property	The Value and Source assigned to the Continuous extension monitoring, Telecommuter, VOIP, and Mobility properties. These are read-only fields because **Value** and **Source** are inherited from either the System or Group profile to which the user is assigned.
Voice Messaging	The **Voice Messaging** fields pertaining to the Modular Messaging server used for Voice Messaging services. Avaya one-X® Portal supports multiple Modular Messaging servers per user.

Name	Description
Server	The name of the Modular Messaging server to which the user is connected for Voice Messaging services.
Display Name	The name assigned to the mailbox used for Voice Messaging services.
Display Address	The display address of the mailbox used for Voice Messaging services.
Mailbox	The identifier assigned to the mailbox used for Voice Messaging services.
Password	The password assigned to the user to gain access to Voice Messaging services.
Property	The Value and Source assigned to the Forward Voice Messages and Save Voice Messages properties. These are read-only fields because Value and Source are inherited from either the System or Group profile to which the user is assigned.
Conferencing	The **Conferencing** fields pertaining to the Conferencing server used for conferencing services. Avaya one-X® Portal installs one Conferencing resource per user. This resource can be modified but not deleted.
Server	The name of the Conferencing server to which the user is connected for Conferencing services.
Display Name	The name assigned to the phone extension used for Conferencing services.
Display Address	The display address of the phone extension used for Conferencing services.
Pin Code	The user password for the Conferencing server. This is an optional field in most Conferencing servers. Enter this value if your Conferencing server requires a password.
Moderator Code	The code used by the user who moderates the conference. The user must enter this code to make the conference available to the other attendees.
Participant Code	The code used by the users who attend the conference. The moderator must enter the moderator code to make the conference available to these users.
Bridge Number	The phone number used for the conference call. All attendees dial this number to access the conference.
Bridge Number Backup	The backup phone number used for the conference call in the event the original bridge number is unavailable.

Name	Description

Chapter 8: Installing the one-X Portal Extensions

Installation options for the one-X Portal Extensions

Avaya one-X Portal Extensions are not fully-featured, independent applications. They complement and extend the features and functionality of the one-X Portal. Avaya one-X® Portal installs all of the one-X Portal Extensions on the user desktop.

Avaya one-X Portal Extensions can be installed on Windows operating systems only. Avaya one-X Portal Extensions are not supported on Mac operating systems.

You can select either of the following installation options for one-X Portal Extensions:

- Push the silent one-X Portal Extensions installation to the user desktop with SMS.
- Allow users to download and install the one-X Portal Extensions from their one-X Portal.

Installing one-X Portal Extensions through SMS

You can use SMS to push the silent one-X Portal Extensions installation to users who have Windows computers.

1. Copy the `One-X.msi` file from the Avaya one-X® Portal DVD to the location required by your SMS system.
2. Follow the instructions for your SMS system to push the installation.
3. Use one of the following commands to start the silent installation:

Option	Command
Without parameters	**`msiexec /i One-X.msi /qn`**
With all parameters	**`msiexec /i One-X.msi /qn`** `SCHEME=`*`HTTP(S)`*

Option	Command
	SERVER=###.###.###.### PORT=*80* ROOT=
With a log file	**msiexec /i One-X.msi /qn /log log.txt**

4. If you choose to install the one-X Portal Extensions with all parameters, the parameters in the command are:

Parameter	Description
SCHEME	The internet protocol scheme at the beginning of the Web address that you use to access one-X Portal. Example: HTTP
SERVER	The server that hosts Avaya one-X® Portal. You must enter the IP address or the fully-qualified domain name of the server. Example: ###.###.###.### or machine.domain.com
PORT	The port that the one-X Portal Extensions uses to communicate with Avaya one-X® Portal. Example: 80
ROOT	The location of the one-X Portal software on the Avaya one-X® Portal server. Example: /1xp/portalclient

Installing the one-X Portal Extensions

Prerequisites

You must close Microsoft Outlook before you install the one-X Portal Extensions.

Avaya one-X Portal Extensions can be installed on Windows operating systems only. Avaya one-X Portal Extensions are not supported on Mac operating systems.

1. On the Application controls, select **Settings** > **Other Settings**.
2. Select the **Other** tab.
3. Click **Download** on the entry for the one-X Portal Extensions.
4. In the File Download - Security window, click one of the following:
   - **Run** to install the one-X Portal Extensions immediately.

- **Save** to save the installer to your computer and install the one-X Portal Extensions at a later time.

5. If you saved the one-X Portal Extensions installer, navigate to the location and double-click the `1XP_Extensions.msi` file.
6. In the Welcome screen, click **Next**.
7. In the License Agreement screen, read the entire license agreement carefully, then do one of the following and click **Next**:
   - Click **I accept the terms in the license agreement** to continue with the installation.
   - Click **I do not accept the terms in the license agreement** to exit the installation.
8. In the Destination Folder screen, do one of the following then click **Next**:
   - Accept the default installation folder.
   - Click **Change** and navigate to your preferred installation folder.
9. In the Setup Type screen, select **Complete** to install all one-X Portal Extensions on your computer then click **Next**.
10. In the one-X Portal Server Settings screen:
    a. Complete the **Server** field.

       The server that hosts Avaya one-X® Portal. You must enter the IP address or the fully-qualified domain name of the server.

       For example, onexportal.xyzcorp.com. If you do not know the value to enter in this field, contact your supervisor.

    b. Click **Next**

    The installer completes all other fields on the one-X Portal Server Settings screen.
11. Click **Install** to install the one-X Portal Extensions on your computer.
12. After the installer has finished the installation of the one-X Portal Extensions, do the following:
    a. Check the **Launch Avaya one-X Portal Extensions** option.
    b. Click **Finish**.

Result

If you checked the **Launch Avaya one-X Portal Extensions** option, the one-X Portal Extensions starts and logs you in automatically.

Portal Desktop Extension dependency on MSXML

PDE requires MSXML 4.0 patch to be installed on the system for users to log on to PDE. MSXML 4.0 comes installed in most Windows systems but it is not a standard in Windows XP. Therefore, most users may not face any problems when they log on to PDE but for systems that do not have the patch installed, users cannot go ahead of the log on window. In such a case, the PDE log on window neither accepts the user credentials nor displays an error message. Users can download and install MSXML 4.0 from http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=3144B72B-B4F2–46DA–4B6–C5D7385F2B5 and resolve the issue.

Chapter 9: Setting up one-X Portal on Citrix

Configuring the Citrix server for Avaya one-X® Portal

Prerequisites

Make sure that the Citrix server is running Citrix Metaframe Presentation Server 4.5.

This document provides a high-level list of the tasks required to configure Citrix for Avaya one-X® Portal. Consult the documentation provided by Citrix for detailed instructions.

1. Log in to the Citrix management console.
2. Add an application under the Citrix farm for each of the following applications that the Citrix server will host:
   - The Avaya one-X® Portal application
   - The Administration application
3. For each application, add a command line for the login.
   `iexplore.exe http://1xpServerName.company.com/`
4. Configure each application for either content or desktop mode.
5. For each application, enable legacy audio.
6. Add your servers and users to each application.
7. Configure the remaining options for each application as required or recommended by Citrix.

Configuring the Citrix client for Avaya one-X® Portal

This document provides a high-level list of the tasks required to configure Citrix for Avaya one-X® Portal. Consult the documentation provided by Citrix for detailed instructions.

1. In the ICA Client for each user, configure the following settings for the ICA Connection:
   - Uncheck **sound custom default**.
   - Check **enable sound**.
2. To avoid the issue where users are prompted to install applications when they log in to Avaya one-X® Portal, do one of the following:
   - Make sure that all users disable downloads, as described in Configuring Internet Explorer for Citrix access on page 107.
   - Use the Windows Group Policy to disable the **Download signed ActiveX controls** option in Internet Explorer.
   - Train your users to understand that they should not download or install any of the supporting applications for Avaya one-X® Portal.
3. If a user downloads one or more supporting applications, remove the files from the Temporary Internet Files folder assigned to that user.

Chapter 10: Troubleshooting the one-X Portal installation

Troubleshooting the Avaya one-X® Portal installation

If you encounter an issue with the Avaya one-X® Portal installation, Avaya recommends that you do the following:

1. Review the topics in this Troubleshooting section for possible resolutions to your problem.
2. Retry the action. Carefully follow the instructions in the online documentation.
3. Retrieve the log files and review all applicable error messages.
4. If the problem occurs in a Avaya one-X® Portal application:
   a. Check the Portal status in Avaya one-X® Portal for any messages that indicate a problem with the Avaya one-X® Portal system.
   b. In Avaya one-X® Portal, click the **System Status** icon to open the System Status window and check the detailed status of your system.

      Review the system status. If a service status is Impaired or Failed, review and follow the recommended action.
5. Note the sequence of steps and events that led to the problem and the exact messages displayed.
6. If possible, capture screen shots that show what happens when the issue occurs.

Next steps

Tip:

If the proposed solutions do not resolve your problem, or if you encounter an issue that is not included in this section, follow your corporate process to obtain support.

Resolving Administration Web Client Issues

Logging

Avaya one-X® Portal provides the following types of Logging for system analysis and debugging purposes.

- General high-level system logging
- Protocol-level logging
- Aspect-level, also called component-level, logging by user
- Non-Avaya or Internal logging

Logging provides the following types of log files:

- Trace logs
- Error logs
- System logs
- Service logs

Note:

If you are an Auditor, you do not have access to the Logging page. The system displays a WebSphere Administration rights message. Click **Back** to return to the previous page.

Related topics:

Retrieving log files from Linux environment on page 222
Downloading log files on page 224
Configuring logging on page 224

Retrieving log files from Linux environment

Avaya one-X® Portal provides a shell script (1xp_grab_logs.sh) that enables the administrator or technical support representative to retrieve log files to troubleshoot issues on Avaya one-X® Portal. This topic describes how to run this shell script from a Linux machine.

Important:

To run this script, you must be logged in as a user with permissions to create files and folders in the directory from which the script is run. You must also have permissions to read and list files in the temporary directory source files created by the script.

Proposed Solution 1

1. From the command prompt on a Linux machine, go to `/opt/avaya/1xp`.
2. Enter `./1xp_grab_logs.sh`.
3. Press **Enter**.
4. The shell script performs the following steps:
   a. Creates a temporary directory structure.
      logs

      /logs/1xp

      /logs/1xp_config

      /logs/weblm

      /logs/weblm/tomcat5

      /logs/server1

      /logs/logs
   b. Retrieves the system information.
   c. Copies the logs into the temporary directory structure.
   d. Generates a log file using the date and time in the log file name.
   e. Tars and compresses the log files.
   f. Performs cleanup procedures.
   g. Displays a closing message.
5. The log file with all the logs is in the `/opt/avaya/1xp` directory with the specified file name.
6. Transfer the log file to Avaya Technical Support for analysis.

Proposed Solution 2

Go to **System** > **Logging** >**All log files**.

The log files are zipped and saved in the file system on the computer using the one-X Portal Administration application.

Downloading log files

Prerequisites

To download log files on Avaya one-X® Portal, you must also be logged in to the WebSphere Administration page.

1. Click the **System** tab.
2. In the left pane, select **Logging**.
3. On the Logging Configuration page, in the **Download Log Files** field, click **All Log Files**.
   The system opens the **File Download** dialog box. It displays the message **Do you want to open or save this file?**. It also displays the Name: *log file name*, Type: *WinZip File*, and From: *IP address of the Administration application*.
4. Click **Open** to open the log files on your computer.
5. Click **Save** to save the log files to your computer.
6. Click **Cancel** to close the dialog box.

Configuring logging

To configure logging on Avaya one-X® Portal, you must also be logged in to the WebSphere Administration page.

1. Click the System tab.
2. In the left pane, select **Logging**.
3. On the Logging Configuration page, enter the appropriate information and click **Save** to configure the server.
   For more information on the fields, see Logging field descriptions on page 206.
4. Click **Reset** to display the settings from the start of this session.

Calling party name incorrect

Some of the name instances on Avaya one-X® Portal display different names for the same user. You can initiate a call from the Communications portlet, but name resolution is defined in Modular Messaging.

Proposed Solution

To maintain the continuity of user names across Avaya one-X® Portal, the user name defined in Modular Messaging, Communication Manager, and Active Directory on one-X Portal must be the same on all three services. The name must contain the same order of the first and last name with spaces or punctuation, if any.

AE Services server is not visible to Avaya one-X® Portal

When opening a connection to an AE Services server or testing a connection to an AE Services server, Avaya one-X® Portal generates an error that the AE Services server is not visible error.

Proposed Solution

Make sure the IP address of the AE Services server is in the TSAPI.PRO file in the opt/IBM/WebSphere/AppServer/lib directory. If the IP address is not in this file, Avaya one-X® Portal cannot "see" the AE Services server. The JTAPI library uses the TSAPI.PRO file to find the AE Services servers it can communicate with. Sometimes when a new AE Services server AES is administered on the system, the update to the TSAPI.PRO should enable the JTAPI client to see the server. If that fails, the JTAPI client is unable to connect to the AE Services server. The TSAPI.PRO file is read by the JTAPI library when the Telephony adapter starts up. If the

telephony adapter is already running, you will need to restart it to allow the JTAPI library to load the new TSAPI.PRO file, and view the new AE Services server.

Uninstalling one-X Portal

Avaya one-X® Portal uninstallation

The Avaya one-X® Portal uninstaller performs all steps needed to remove the Avaya one-X® Portal software from the machine, including:

- Stops and uninstalls the Avaya one-X® Portal server.
- Stops and uninstalls the Avaya one-X® Portal database.
- If you installed the WebLM with Avaya one-X® Portal, stops and uninstalls the WebLM.

Files not deleted by the Avaya one-X® Portal uninstaller

The Avaya one-X® Portal uninstaller removes the database accounts, but does not delete files or folders that include user and database data. You must manually delete these files and folders.

The files that the Avaya one-X® Portal uninstaller does not delete include:

User home directories: These directories include the following:

- Database instance user, for example `/home/dbinst`
- Database administrative user, for example `/home/dbadmin`
- Database fence user, for example `/home/dbfenc`
- Database read-only instance user, for example `/home/roinst`
- Database `/home/appsvr`
- InstallShield directory `/root/InstallShield`
- If you chose to create Avaya service accounts, `/home/sroot` and `/home/craft`

Avaya one-X® Portal database directory: This directory is `/home/dbinst/ACPDB` and is located in the home directory for the database instance users.

Avaya one-X® Portal installation and configuration logs: These logs are located at `/opt/avaya/1xp`.

Avaya one-X® Portal logs: These logs are located at `/opt/avaya/1xp/waslogs`.

Uninstalling Avaya one-X® Portal

1. Back up the Avaya one-X® Portal database:
   a. In the Administration application, use the **Database Backup** option of the **Scheduler** tab to perform a full database backup.

      Note:

      To specify a location for the database backup file in the Administration application, go to the **Scheduler** > **Database Backup** tab and specify the location in the **Backup File Location** field.

      To create a directory with full permission to the owner and the group for the dbinst user on the one-X Portal server, log into the one-X Portal server as root, su to dbinst, and enter `mkdir /home/dbinst/backups`.

      Avaya recommends you create a directory called /home/dbinst/backups.

   b. Store the database backup file in a safe location on another network server or computer.
2. Login as root on the machine that hosts the Avaya one-X® Portal server.
3. Execute the following command to start the Avaya one-X® Portal uninstaller: `/opt/avaya/1xp/_uninst/uninstaller.bin`
4. Follow the prompts and answer questions asked by the uninstaller to remove Avaya one-X® Portal from the machine.

   The questions asked by the uninstaller depend upon the selections that you made when you installed Avaya one-X® Portal. These questions may include:

   - Do you want to uninstall the database server?
   - Do you want to uninstall WebLM?
5. If you plan to reinstall Avaya one-X® Portal, delete all files and directories that the uninstaller did not remove.

   Caution:

   This step removes all files or folders that include user and database data. If you have not backed up your database, you will permanently erase this information from the machine.

Procedure	Commands

Rename and move the database files in the database user home directory.	From the Linux command line, execute the following command:
	`$ cd db-inst-home`
	`$ mv 1xp-db-dir new-dir`

Procedure	Commands

	For example:
	`$ cd /home/dbinst`
	`$ mv ACPDB SAVED_1XPDB`

Delete the database user home directories and database files.
For a list of the files and folders that the uninstaller does not delete, see Avaya one-X Portal uninstallation on page 226.
	From the Linux command line, execute the following command:
	`$ cd db-user-home-dir`
	`$ rm -rf 1xp-db-dir`
	For example, to delete the user directory for a database instance user named dbinst::
	`$ cd /home/dbinst`
	`$ rm -rf ACPDB`

Uninstalling the Avaya Voice Player

1. If necessary, log out of one-X Portal.
2. From the Windows **Start** menu, select **Start** > **Settings** > **Control Panel**.
3. In the Windows Control Panel, select **Add/Remove Programs**.
4. In the Add/Remove Programs window, select the entry for the Avaya Voice Player in the list of currently installed programs.
5. Click **Remove** on the Avaya Voice Player entry.
6. Click **Yes** to answer **Are you sure you want to remove Avaya Voice Player from your computer?**

   The uninstaller removes the Avaya Voice Player from your computer.

Uninstalling the one-X Portal Extensions

Prerequisites

You must close Microsoft Outlook before you uninstall the one-X Portal Extensions.

1. If necessary, exit from the one-X Portal Extensions.
2. From the Windows **Start** menu, select **Start** > **Programs** > **Avaya one-X Portal Extensions** > **Avaya one-X Portal Extension Deinstallation**.
3. Click **Yes** to answer **Are you sure you want to uninstall this product?**
   The uninstaller removes the one-X Portal Extensions from your computer.

Appendix A: LDAP over SSL configuration

You can configure Avaya one-X® Portal communication with Active Directory using Lightweight Directory Access Protocol (LDAP) over Secure Socket Layer (SSL), also known as LDAPS, using the procedures described in this section. The configuration involves the following steps:

1. Configuring Active Directory SSL
2. Configuring WebSphere
3. Configuring Avaya one-X® Portal for LDAPS

Prerequisite

Install Avaya one-X® Portal using LDAP and then configure WebSphere with the Active Directory certificate authority (CA) to communicate using SSL.

Configuring Active Directory SSL

This procedure is only necessary if you have not configured Active Directory to use SSL.

Prerequisites

- Certificate Authority (CA) must be installed on a Windows 2003 server
- Active Directory must be present on a Windows 2003 server

Use the following steps to configure Active Directory to enable communication using SSL.

1. Obtain a root certificate using the following steps:
   a. Open certificate authority Web page in your browser using the *http://<CA-server>/certsrv* link.
   b. When prompted for a user service and a password, use an account with Administrator privileges on the CA server.
   c. Click **Download a CA certificate, certificate chain, or CRL** link.
   d. Select **Base-64** and then click **Download CA certificate**.
   e. Use download function of your browser to save the certificate as a file with a .cer extension.

Note:

All root certificates from the same certificate authority are functionally the same. You can download a certificate once and use it repeatedly until it expires.

2. Open the certificate manager using the following steps:
   a. Click **Start** > **Run** on your desktop and type `mmc` in the Run window.
   b. On Microsoft Management Console, click **File** > **Add/Remove Snap-in**. This shows the Add/Remove Snap-in window.
   c. On Add/Remove Snap-in window, select the **Standalone** tab and click **Add**. This shows the Add Standalone Snap-in window.
   d. Select certificates from Add Standalone Snap-in window and click **Add**.
   e. Select a computer account and click **Next**.
   f. Select a local computer and click **Finish**.
   g. Click **Close** on the Add Standalone Snap-in window.
   h. Click **OK** on the Add/Remove Snap-in window
3. Install the root certificate for the Certificate Authority with the following steps on the Microsoft Management Console:
   a. On the left pane, open the `Certificates (Local Computer)\Trusted Root Certificate Authorities\Certificates` folder.
   b. Click **Action** > **Tasks** > **Import**.
   c. On the Certificate Import wizard, click **Next**.
   d. Click **Browse**, select the root certificate file, and click **Open** > **Next**.
   e. Click **Next**.
   f. Select **Place all certificates in the following store**.
   g. Click **Browse**, select **Trusted Root Certificate Authorities**, and click **OK**.
   h. Click **Next**.
   i. Click **Finish**.
   j. On the right pane, select the new certificate you just imported.
   k. Click **Action** > **Properties**.
   l. Enter a name that identifies the CA.
   m. Click **OK**.
4. Generate a policy file for the Domain Controller on the DC machine using the following steps:

a. Obtain a copy of the reqdccert.vbs script. This can be found on the Web at several locations.

b. From the command prompt, run the **reqdccert.vbs** script.

c. Verify that the following files have been created:

- <dc-name>.inf
- <dc-name>-req.bat
- <dc-name>-vfy.bat

5. Edit <dc-name>.inf with a text editor using the following steps:

a. Under the line that says “[NewRequest]”, add a line:

```
Subject="CN=<dc-fqdn>"
```

where <dc-fqdn> is the fully qualified domain name (FQDN) of the DC. You can view the FQDN of the DC from **Start** > **Control Panel** > **System** > **Computer Name**, where it is displayed as **Full Computer name**. Do not forget to add the prefix `CN=` and put the whole subject in quotes.

b. Delete the line that says **Critical=2.5.29.17**. (WebSphere does not recognize this extension.)

c. Save the file.

6. Create the certificate request on the Domain Controller using the following steps:

a. Open the directory where the <dc-name>.inf is located and run the command:

```
certreq –new <dc-name>.inf <dc-name>.req
```

b. Copy the <dc-name>.req and <dc-name>-req.bat file to the CA machine.

7. Create the domain controller certificate using the following steps:

a. Open the command prompt, and go to the directory where the files were copied.

b. Run the BAT file: <dc-name>-req

c. When prompted, select the CA and click **OK**. The script prompts you to save the <dc-name>.cer file.

d. Log on to the CA, and open the Certification Authority application from **Start** > **Administrative Tools** > **Certification Authority**.

e. Open the **Pending Requests** folder.

f. Accept the request for <dc-name>.

g. Open the **Issued Certificates** folder.

h. Open the new certificate.

i. Click the **Detail** tab and click **Copy to file**.

j. Select a Base-64.cer file and export it.

8. Install the Domain Controller Certificate on the Domain Controller as explained in the following steps:
   a. Copy the .cer file from CA to the DC machine.
   b. In the directory where the <dc-name>.cer file is located, run the command:
      `certreq –accept <dc-name>.cer`
   c. Open the certificate manager for the local system as described in step 2.
   d. In the left pane, open the **Certificates** folder from the`<local drive>\Personal\Certificates` folder and make sure the certificate is installed.
   e. (Optional) Rename the certificate. For example, Enable LDAPS.
   f. Reboot the Domain Controller.

Configuring WebSphere

After configuring the Active Directory for LDPS, use the IBM WebSphere console to configure WebSphere. To configure WebSphere:

1. Log on to the IBM WebSphere console using the Avaya one-X® Portal administrative credentials. The address for the IBM administrative console is `https://<oneXPortalMachine>:9043/ibm/console`.
2. Under the **Security** section, click the **SSL certificate and key management** link.
3. On the SSL certificate and key management page, go to **Key stores and certificates** > **NodeDefault** > **Signer certificates** and click **Retrieve from port**.
4. Enter the **Host**, **Port** and **Alias** information. The **Host** is the IP Address of your DC machine, and the **port** is the port for the LDAPS service (port 636 by default).
5. Click the **Retrieve signer information** button.
6. Click **OK** and save the configuration.
7. Use the IBM console to verify the connection with the LDAP server. This test does not use Avaya one-X® Portal code, so it is a good validation for the environment setup. To perform validation on the IBM console:
   a. Click **Security** > **Secure administration, applications, and infrastructure**.
   b. If your system is already set up to talk to a single AD environment, the **Available realm definitions** field must be set to Standalone LDAP registry.

c. Click **Configure**.

d. Configure the parameters for your Active Directory. If the system is already configured to communicate with Active Directory, change the **Port** to `636` and the **SSL Settings** to enable SSL.

e. Click **Test connection**. If the test is successful, the following message displays: `<LDAP IP Address> on port 636 was successful`

Note:

If the test is not successful, you must take a corrective action based on the error message.

f. Log out of the IBM Console.

Important:

Do not change the configuration here, since changing the configuration on Avaya one-X® Portal also changes this configuration. Do not save the connection at WAS.

Configuring Avaya one-X® Portal for LDAPS

1. Log on to Avaya one-X® Portal administration client: `https://<oneXPortalServer>:9443/admin` .
2. Open the **System** tab and click **Enterprise Directory**.
3. Select the domain for which you need to set the LDAPS configuration.
4. Change **Port** value to `636` and the select **Secure Port**.
5. Save the configuration.
6. Restart Avaya one-X® Portal.

Appendix B: Avaya one-X® Portal and Novell eDirectory setup over SSL

This section describes the steps to configure Avaya one-X® Portal communication with Novell eDirectory using LDAP over SSL. You must have simultaneous access to WebSphere and Novell iManager utility to create, exchange, and configure server certificates.

Prerequisites

Install the following utilities on the system that you want to use to administer Novell eDirectory:

- Novell iManage. To administer Novell eDirectory.
- Certificate Manager add–in. To obtain the Novell Certificate Server configurable from Novell iManager.
- LDAP plug-in. To administer LDAP Server from Novell iManager.

Perform the following steps to configure Avaya one-X® Portal and Novell eDirectory setup over SSL.

Creating a trusted root container on iManager

Open the iManager utility in your browser and perform the following steps.

1. Click **Novell Certificate Server** > **Create Trusted Root Container**.
2. Specify a container name of your choice in the **Container** field.
3. Click **Object selector** and set **Context** as Security .
4. Click **OK**.

Exporting Novell CA self-signed certificate as a DER file

Important:

Do not export the private key when you export.

1. On iManager, click **Novell Certificate Server** > **Configure Certificate Authority**.
2. On the **Certificates** tab, select **Self Signed Certificate** and click **Export**.
3. Clear the **Export private key** check box.
4. Select the **DER** format and click **Next**.
5. Save the file.

Adding the self-signed certificate as a trusted root

Prerequisites

First export the self-signed certificate as a DER file. For more information, see Exporting Novell CA self-signed certificate as a DER file on page 238

1. On iManager, click **Novell Certificate Server** > **Create Trusted Root**.
2. Enter a name for the trusted root.
3. Select `<trusted root container>.Security` file that you exported in the previous step.

Exporting WebSphere certificate from Avaya one-X® Portal server and importing into Novell

1. In WebSphere Web console, click **Security** > **SSL certificate and key management** > **Key stores and certificate**.
2. On the Key stores and Certificates page, click **NodeDefaultKeyStore** > **Personal Certificates** links.
3. Select the default certificate, and click **Extract**.
4. Save the certificate as a DER file on the Avaya one-X® Portal file system, and transfer that file to the machine where iManager is installed.

Adding WebSphere certificate as a trusted root on Novell eDirectory

1. On iManager, click **Novell Certificate Server** > **Create Trusted Root** links.
2. Enter a name for the trusted root.
3. Select **Security** container as created in previous steps.
4. Browse and select the DER file that was received from WebSphere.
5. Configure the LDAP Server Connection using the following steps:
   a. Set the **Client Certificate** = Requested, and the **Trusted Root Containers** = <trusted root container>.Security.
   b. Click **Save** and then **Refresh**.

Importing Novell CA certificate into WebSphere

1. In WebSphere Web console, click **Security** > **SSL Certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates**.
2. Select the certificate and click **Retrieve from port**.
3. Enter the Novell eDirectory IP Address in **Host** and SSL LDAP port (usually 636) in **Port** fields. Do not save the configuration yet. Use the Avaya one-X® Portal administration user interface to save this configuration as described in step 8.
4. In the WebSphere Web console, select **Security** > **Secure administration, applications, and infrastructure**.
5. Make sure the **Standalone LDAP** registry is selected, and click **Configure**.
6. Change the **Port** to be the SSL LDAP port (usually `636`).
7. Select the **SSL Enabled** check box to enable SSL and click **Test connection**.

   Caution:
   Do not click **Apply** or **Save** at this step.
8. Log on to the Avaya one-X® Portal administration client.
9. On the **System** tab, select **Enterprise Directory**.
10. Select the Novell eDirectory domain, and change the configuration to use the SSL LDAP port.
11. Select the **Secure Port** check box.
12. Save the configuration and restart WebSphere.

Appendix C: Avaya one-X® Portal and SunONE directory setup over SSL

You need to use your own certificate authority to enable SSL on a SunONE directory, since SunONE does not have an integrated Certificate Authority (CA). You may have a custom Certificate Authority environment, and it is out of the scope of this document to describe the details for any particular environment.

This section describes how to configure Avaya one-X® Portal communication with SunONE directory using LDAP over SSL.

Requesting the certificate using the console

You must create the request for server certificate from the SunONE directory, process the request for server certificate on CA, and then get the certificate back from CA.

1. To begin the request:
   - On the top-level **Tasks** tab of the Directory Server console, click **Manage Certificates**.
   - On the top-level **Tasks** tab, select the **Manage Certificates** item from the **Console** > **Security** menu.

   This displays the Manage Certificates window.
2. Select the **Server Certs** tab and click **Request**. This opens the Certificate Request Wizard.

   If you have installed a plug-in that allows the server to communicate directly with CA, you must select it now. Otherwise, you must request a certificate manually by transmitting the generated request through e-mail or a Website.
3. Click **Next** on the Certificate Request Wizard.
4. Enter the following information on the wizard screen.

Field	Description
Server Name	Fully qualified host name of the Directory Server as it is used in DNS lookups.
Organization	The legal name of your company or institution. Most CAs require you to verify this information with legal documents such as a copy of a business license.
Organizational Unit (optional)	Descriptive name for your division or business unit within the company.
Locality (optional)	Name of your city.
State or Province	Name of your state or province.
Country	Two-character abbreviation for your country name in ISO format. The country code for the United States is US. For a list of ISO country codes, see *Appendix C: Directory Internationalization* in the *Sun ONE Directory Server Reference Manual*.

Click **Next** to proceed to the next screen.

5. Enter the password of your security device, then click **Next**. This is the password set in Creating a Certificate Database.
6. Select **Copy to Clipboard** or click **Save to File** to save the certificate request information in a text file that you need to send to the Certificate Authority.
7. Click **Done** to close the Certificate Request Wizard.

Installing the server certificate

1. Send the server certificate request information to your Certificate Authority, according to prescribed procedures.

   For example, you may be asked to send the certificate request in an e-mail, or you may be able to enter the request through the CA Website.
2. Wait for the CA to respond with your certificate.

Response time for your request varies. For example, if your CA is internal to your company, it may only take a day or two to respond to your request. If your selected CA is external to your company, the response time can be longer.

3. When CA sends a response, save the information in a text file.

   The PKCS #11 certificate in PEM format appears similar to the example.

Example

```
BEGIN CERTIFICATE

MIICjCCAZugAwIBAgICCEEwDQYJKoZIhKqvcNAQFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoGlBhbG9a2FWaWxsZGwSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTW3FrZXJzICdSJyBVczEpMCcGAx1UEAxgVGVzdCBUXN0IFRlc3QgVGVz
dCBUZXN0IFlc3QgQ0EswHhcNOTgwMzEyMDIzMzUWhcNOTgwMzI2MDIzMpzU3WjBP
MQswCYDDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZN0b3J5VIFB1Ymxp
Y2F0aW9uczEWMB4QGA1UEAxMNZHVgh49dq2tLNvbjTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYkCQCksMR/aLGdfp4m0OiGgijG5KgOsyRNvwGYW7kfW+8mmijDtZaRjYNj
jcgpF3VnlbxbclX9LVjjNLC5737XZdAgEDozYwpNDARBglghkgBhvhCEAQEEBAMC
APAwHkwYDVR0jBBgwFAU67URjwCaGqZHUpSpdLxlzwJKiMwDQYJKoZIhQvcNAQEF
BQADgYEAJ+BfVem3vBOPBveNdLGfjlb9hucgmaMcQa9FA/db8qimKT/ue9UGOJqL
bwbMKBBopsDn56p2yV3PLIsBgrcuSoBCuFFnxBnqSiTS7YiYgCWqWaUA0ExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=

END CERTIFICATE
```

Next steps

You must back up the certificate data in a safe location. If your system ever loses the certificate data, you can reinstall the certificate using your backup file. Once you have your server certificate, you are ready to install it in the certificate database of your server.

Installing server certificate using the console

1. To begin installation of server certificate using the console:
   - On the top-level **Tasks** tab of the Directory Server console, click **Manage Certificates**.
   - On the top-level **Tasks** tab of the Directory Server console, select the **Manage Certificates** from the **Console** > **Security** menu.
2. Select the **Server Certs** tab, and click **Install**. This opens the Certificate Install Wizard.

3. Choose one of the following options for the certificate location:
   - **In this file**. Enter the absolute file path to save the certificate.
   - **In the following encoded text block**. Copy the clipboard text from Certificate Authority or from the text file you created and paste it in this field.
4. Click **Next**.
5. Verify that the certificate information displayed is correct, and then click **Next**.
6. Enter the certificate name and then click **Next**. This name is displayed in the table of certificates.
7. Verify the certificate by providing the password that protects the private key. This is the same password that you provided for Creating a Certificate Database.
8. Click **Done** to close the wizard.

   Your new certificate must appear in the list on the **Server Certs** tab. Your server is now ready for SSL activation.

Trusting the Certificate Authority using the console

After securing the CA certificate, you can use the Certificate Install Wizard to configure the Directory Server to trust the Certificate Authority.

1. Perform one of the following steps to begin:
   - On the **Tasks** tab of the Directory Server console, click **Manage Certificates**.
   - On the top-level **Tasks** tab of the Directory Server console, select the **Manage Certificates** from the **Console** > **Security** menu.

   This displays the Manage Certificates window.
2. On Manage Certificates window, select the **CA Certs** tab and click **Install**. This opens the Certificate Install Wizard window.
3. Perform one of the following steps to submit the certificate:
   - If you saved the certificate to a file, enter the path in the field provided and click **Next**.
   - If you received the certificate through e-mail, copy and paste the certificate including the headers into the text field provided and click **Next**.
4. Verify that the certificate information displayed is correct for your CA and then click **Next**.

5. Specify the certificate name, and then click **Next**.
6. Select the purpose of trusting this CA from the following choices. You can select one or both depending on your corporate requirement and policy:
   - **Accepting connections from clients (Client Authentication)**. Select this check box if your LDAP clients perform certificate-based client authentication by presenting certificates issued by this CA.
   - **Accepting connections to other servers (Server Authentication)**. Select this check box if your server functions in a replication supplier role over SSL with another server that has a certificate issued by this CA.
7. Click **Done** to close the wizard.

Activating SSL on SunONE

Activate SSL on SunONE and configure SSL to use the new server certificate. The following procedure activates SSL communications and enables encryption mechanisms in the directory server:

1. On the top-level **Configuration** tab of the Directory Server console, select the root node with the server name, and then select the **Encryption** tab in the right panel. The **Encryption** tab displays the current server encryption settings.
2. Select the **Enable SSL for this Server** check box to enable encryption.
3. Select **Use this Cipher Family** check box.
4. Select the certificate that you want to use from the drop-down menu.
5. Click **Cipher Settings** and select the ciphers you want to use in the Cipher Preference dialog.
6. Set your preferences for client authentication. Select one of the following preferences:
   - **Allow client authentication**. This is the default setting. With this option, authentication is performed on the clients request.
   - **Use SSL in Sun ONE Server Console**. Select this option if you want the console to use SSL when communicating with Directory Server.
7. Click **Save** or set the secure port you want the server to use for SSL communications in both LDAP and DSML-over-HTTP protocols.

Note:

All connections to the secure port must use SSL regardless of whether you configure the secure port. After SSL is activated, clients may use the Start TLS operation to perform SSL encryption over the nonsecure port.

8. Restart the directory server.

Adding server certificate in WebSphere

To import the SunONE certificate into WebSphere:

1. Go to the WebSphere (WAS) console by using the *https://<onexp server ip>:9043/ibm/console* link.
2. In WebSphere Web console, select **Security** > **SSL Certificate and key management** > **Key stores and certificates** > **Node Default Trust Store** > **Signer certificate**.
3. Select **Retrieve from port**.
4. Specify the SunONE IP address and SSL LDAP port (usually 636).
5. Enter an **Alias** for the certificate. For example, `sunonecert`.
6. Click **Retrieve Signer information**.
7. Click **OK**.

Important:

Do not save the connection here. Use Avaya one-X® Portal administration application to save the configuration.

Testing connection from WebSphere to SunONE

Test the LDAP connection to see if it works but do not save it. Use Avaya one-X® Portal administration UI to save this configuration.

1. In the WebSphere Web console, select **Security** > **Secure administration, applications, and infrastructure** and make sure the **Standalone LDAP registry** is selected.
2. Click **Configure**.
3. Change the port to make it an SSL LDAP port (usually 636).
4. Select **SSL enabled** check box to enable SSL .
5. Click **Test Connection**. The system must return a success message.

Changing Avaya one-X® Portal configuration for secure connection

1. Log in to the Avaya one-X® Portal administration client.
2. Select **System** tab and click **Enterprise Directory**.
3. Choose the SunONE domain, and change the configuration to use the SSL LDAP port.
4. Select the **Secure Port** check box.
5. Save the configuration and restart WebSphere.

Appendix D: Avaya one-X® Portal and Domino directory setup over SSL

You must use your CA to enable SSL on a Domino directory since Domino does not have an integrated CA. You may have a custom CA environment, but it is out of the scope of this document to describe the details for a particular environment. This section describes how to configureAvaya one-X® Portal to enable communication with the Domino directory using LDAP over SSL.

Registering an Internet certifier

1. Launch the Domino Administrator client by using the Administrator ID file.
2. Select the correct domain and server.
3. Click **Configuration** to go to the **Configuration** tab.
4. From the menu, click **Configuration** > **Registration** > **Internet Certifier**.
5. Select **I want to register a new Internet certifier that uses the CA process**, and click **OK**.
6. In the **Register a New Internet Certifier** dialog box, click **Create Certifier Name** and fill in a common name such as `MyCompany CA`, and click **OK**.
7. Select the server on which you want to put the certifier for the CA.
8. You can use the default Issued Certificate List (ICL) database name or modify it. For example, icl\icl_MyCompany.nsf.
9. Select one of the following options for the **Encrypt Certifier ID with** settings:
   - Encrypt ID with Server ID: lowest security, no password required
   - Encrypt ID with Server ID and Require password to activate certifier
   - Encrypt ID with Locking ID and choose the person whose ID will be used to secure the new CA
10. Click **OK**.

The system displays a success message.

Next steps

Run the certificate authority task.

Running the CA task

1. On the **Configuration** tab of the Domino Administrator client, perform one of the following actions:
   - Type **load** *ca* if the task is not running.
   - Type **tell** *ca refresh* if the CA task is running.
2. To ensure that the new CA is ready for use, type **tell** *adminp process all*.
3. Type **tell** *ca stat*.
   If your new CA does not show up in the list, type **tell** *adminp process all*.
4. Type **tell** *ca refresh*.
   The system displays the new CA, if included in the list.
5. To verify that the new CA has been properly initialized, type **tell** *ca stat*.
6. To activate your password when your CA is not active, type **tell** *ca activate certifier number password*
7. To obtain the actual value for certifier number, type **tell** *ca stat*.
   Each CA is listed with a number preceding it. Use this number to identify a **tell** command.

Next steps

Creating and setting up the certification request database

Creating and setting up the certification request database

1. On the Domino Administrator client, select **File** > **Database** > **New**, then select your server.
2. In the **Specify New Database Name and Location** section of the **New database** page, enter a title for the database. For example, enter `Western CA database`.
3. Enter a name for the database file, for example, `certreq.nsf`.

   Each Internet Certifier requires a unique Certificate Requests database. If you are going to create additional Internet CAs in future, provide a unique title for the associated CAs in the Certificate Requests database. For example, you can provide the title `Cert Req MyCompany`, and a file name such as `CR_myco.nsf`. Keep the file name short so that it is easier to enter as part of a URL in a Web browser.
4. In the **Specify Template for New Database** section of the **New database** page, ensure that the template server is set to **server**, and not to **local**.
5. Select **Show Advanced Templates** and select the template name **Certificate Requests (6)** with the file name `certreq.ntf`.
6. To create the Certificate Requests database, click **OK**.
   The system creates the database.
7. Close the **About...** document.

   The system displays the **Database Configuration** form.

   - Select the administration server.

     This server runs the CA process for the supported CA.
   - Select the CA you created in the Configuring Domino SSL topic.
   - Select the intended purpose of this CA:
     - **Server Certificates Only**
     - **Both Client and Server Certificates**

   Do not select **Client Certificates Only** if you want to create a server key ring for SSL.
8. From the **Processing Method** drop-down list, select one of the following processing methods:

   - **Automatic**
   - **Automatic Transfer Server (optional)**

If you select the **Automatic** method, the person designated as an RA must be listed amongst those who can select **Run unrestricted methods and operations** in the Administration Server's server document.

RA is often the same person who creates the Certificate Requests database, that is, `certreq.nsf`. To verify this or to make necessary changes, open the Domino Directory, navigate to the **Server/Servers** view, open the appropriate server document, and navigate to the **Security** section to see the **Processing Method** field.

If you do not set the **Processing Method** field properly, you will not be able to run the agents in the Certificate Requests database.

9. Select whether you want the applicant to receive the confirmations.
10. Click **Save & Close**.

Next steps

Creating a key ring

Creating a key ring

1. Open the Domino administration client.
2. On **Files** tab, open the Certification Requests database.
3. Select **Domino Key Ring Management** >**Create Key Ring**.
   The system displays the **Create Key Ring** form.
4. In the **Key Ring File Name** field, enter a file name for the key ring file without the .kyr extension.
5. In the **Password** and **Confirm Password** fields, enter identical passwords.
6. From the **Key Size** drop-down list, select a key size.
7. In the **Common Name** field, enter the common name of the server.
   The common name of the server should be a fully qualified host name, for example, server.company.com.
8. In the **Organization** field, enter the organization name.
   All other fields are optional.
9. Click **Create Key Ring**.

10. To automatically add your CA as a trusted root and to generate a certificate request for your server, in the **Key Ring Created** dialog box, verify the information and click **OK**.
11. In **Merge Trusted Root Certificate Confirmation** dialog box, verify the information and click **OK**.
    The system displays the **Certificate received into key ring and designated as trusted root** confirmation screen.
12. Click **OK**.
    The system displays the **Certificate Request Successfully Submitted for Key Ring** dialog box.
13. To dismiss the message, click **OK**.

Next steps

Approving a key ring request

Approving a key ring request

1. Open the Certificate Requests database.
2. To refresh the view, on the **Pending/Submitted Requests** view, press `F9` if you do not find your request.
3. If the status of the request is **Submitted to Administration Process**, go to step 5. If the status of the request is **Pending Submission**, select the request and click **Submit Selected Requests**. The system displays the **Successfully submitted 1 request(s) to the Administration Process** message.
4. Click **OK**.
   Keep the Certificate Requests database open.
5. Open the Administration Requests database `Admin4.nsf`, go to the **Certification Authority Requests/Certificate Requests** view, and find your new request.
6. Double-click the request to open it, click **Edit Request**, and verify the information of the request.
7. Once you have verified the information and finished making any optional changes, click **Approve Request**.
8. Press `F9` till the state of the request changes from the **New** state to the **Issued** state.

The request state might change to **Approved** state before changing to the **Issued** state.

Next steps

Checking the status of a key ring request

Configuring a port

1. In the **Server/Servers** view of the Domino directory, find the server document.
2. Open the server document and click **Edit Server**.
3. In the **Ports - Internet Ports** section, enter the name of the new key ring file.
   Do not enter the full path of the key ring file.
4. Scroll down the page and locate the **SSL Port Status** field, and change it from **Disabled** to **Enabled**.
5. To enable SSL on the server, on the server console, type **`tell`** *`http restart`* if HTTP is running.
6. To verify that the HTTP server is now listening on ports 80 and 443, on the server console, type **`show`** *`task`*.

Next steps

Establishing a secure session over SSL by using Internet Explorer.

Establishing a secure session over SSL using IE

1. To confirm that SSL works on the server, open a browser and type https://<server>.<company>.com/<CR_myco.nsf>.
   The system displays the **Security Alert** screen.
2. Click **View Certificate**.
3. Click **Install Certificate**.

4. On the **Certificate Import Wizard** screen, click **Next**.
5. On the **Certificate Store** screen, retain the default selection **Automatically select the certificate store based on the type of certificate**, and click **Next**.
6. On the **Completing the Certificate Import Wizard** screen, click **Finish**.
   The system displays **The import was successful** message.
7. Click **OK**.
8. On the **Security Alert** screen, click **Yes**.
   If the system displays a secured padlock near the top of the Internet Explorer window, it means you have successfully established a secure session over SSL.

Next steps

Configuring the WebSphere server.

Configuring the WebSphere server

1. Log in to the IBM WebSphere Administrative Console by using the administrative credentials.

   The address for IBM WebSphere Administrative Console is `https://<oneXPortalMachine>:9043/ibm/console`.
2. In the **Security** section, select **SSL certificate and key management**.
3. Navigate to **Key stores and certificates** >**NodeDefaultTrustStore** > **Signer certificates** and click **Retrieve from port**.
4. In the **Host**, **Port**, and **Alias** fields, enter the host, port, and alias.

   The host is the IP address of the Domain Controller (DC) machine, and the port is the port for the LDAPS service. The default port is 636.
5. Click **Retrieve signer information**.
6. To save the configuration, click **OK**.
7. To verify the connection, check whether you can connect to the LDAP server by using the IBM Console.

   This test does not use any Avaya one-X® Portal code, so it is a good validation for the environment setup.
8. On the administrative console, navigate to **Security > Secure administration, applications, and infrastructure**.

If your system is already set up to communicate with a single LDAP environment, the **Available realm definitions** option should already be set to **Standalone LDAP registry**.

9. Click **Configure** and configure the LDAP parameters.
   Do not save any information now.
10. If the system is already configured to communicate with LDAP, change the port to 636, and select the **SSL Enabled** check box in the **SSL Settings** section.
11. Click **Test connection**.

Next steps

Configuring Avaya one-X® Portal for LDAPS

Configuring Avaya one-X® Portal for LDAPS

1. Log on to the Avaya one-X® Portal administration client by using `https://<oneXPortalMachine>:9043/ibm/console`.
2. Click the **System** tab.
   The system displays the **System** tab.
3. Click **Enterprise Directory**.
4. Select the domain for which you need to set the LDAPS configuration.
5. Change the port value to `636`.
6. Select **Secure Port**.
7. To save the configuration, click **Save**.
8. Restart Avaya one-X® Portal.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

R

S

T

U

V

W

Z