



Implementing Avaya one-X Portal

October 2008

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: <http://www.avaya.com/support>

Licenses

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

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 Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Named User License (NU). Customer 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 Product that permits one user to interface with the Product.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and

use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and/or use 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 identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/ThirdPartyLicense/>

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

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya Inc. 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://www.avaya.com/support>

Contents

Chapter 1: Avaya one-X Portal overview.....	7
Avaya one-X Portal overview.....	7
Avaya one-X Portal features.....	7
Avaya one-X Portal system diagram.....	7
Prerequisites for one-X Portal.....	9
Supported languages in one-X Portal.....	10
Security features of one-X Portal.....	11
Capacities and performance of one-X Portal.....	12
Interactions between one-X Portal and other applications.....	14
Limitations on support in one-X Portal and one-X Portal Extensions.....	15
Supporting Windows applications for one-X Portal.....	16
Terminology used in one-X Portal.....	17
Chapter 2: Planning a one-X Portal deployment.....	19
Avaya one-X Portal Implementation Workbook.....	19
Port requirements for one-X Portal.....	19
Required software for one-X Portal components.....	22
Supported versions of third-party software.....	22
Required software for the one-X Portal server.....	23
Required software for integrating servers with one-X Portal.....	23
Supported browsers for the one-X Portal application and the Administration application.....	25
Required software for the Administration application.....	25
Required software for one-X Portal application and one-X Portal Extensions.....	25
Support for one-X Portal applications on Citrix.....	27
Required hardware for one-X Portal components.....	27
Minimum hardware requirements.....	27
Avaya one-X Portal server hardware requirements.....	27
Avaya one-X Portal user and administrator hardware requirements.....	28
Network guidelines for one-X Portal.....	29
Time synchronization requirements.....	29
Telephony network performance between one-X Portal and AE Services.....	30
Network firewall guidelines.....	30
Remote user connection guidelines.....	31
Licensing requirements for one-X Portal.....	32
Licensing requirements.....	32
Location of the Avaya Web License Manager.....	33
Obtaining a host ID.....	33
Requesting a license file.....	34
Customizing one-X Portal.....	35
Rebranding options for one-X Portal.....	35
Rebranding one-X Portal.....	35
Chapter 3: Completing prerequisites for the one-X Portal server.....	37
Environment validation checklist.....	37
Server prerequisites checklist.....	39
Installing required components for integrated servers.....	44
Installing Linux for one-X Portal.....	45
Configuring AE Services for one-X Portal.....	46
Guidelines for installing AE Services.....	46

Creating AE Services users for one-X Portal.....	47
Configuring an H. 323 gateway list for AE Services.....	48
Configuring Enterprise Directory for one-X Portal.....	49
Enterprise Directory integration guidelines.....	49
Determining the Active Directory domain topology.....	51
Configuring Enterprise Directory security groups.....	51
Verifying Enterprise Directory user configuration.....	52
Creating the one-X Portal administrative service account.....	53
Configuring Communication Manager for one-X Portal.....	54
Configuring Send All Calls in Communication Manager for Do Not Disturb in one-X Portal.....	54
Configuring call forwarding.....	55
Configuring emergency call handling.....	55
Disabling AnnexH for Communication Manager 4.0.....	56
Configuring Extension to Cellular for one-X Portal.....	56
Extension to Cellular and one-X Portal.....	56
Enabling user extensions.....	57
Configuring mobility extensions.....	58
Configuring Modular Messaging for one-X Portal.....	59
Configuring Modular Messaging ports and protocols.....	59
Configuring Modular Messaging LDAP access.....	60
Verifying Modular Messaging subscriber values.....	60
Enabling client access for Modular Messaging.....	61
Configuring super-user IMAP4 connections in Modular Messaging 3.1.....	61
Activating NTP in Modular Messaging 3.0 SP2.....	62
Activating super-user IMAP4 connections in Modular Messaging 3.0 SP2.....	63
Creating trusted servers in Modular Messaging 3.0 SP2.....	63
Configuring Meeting Exchange for one-X Portal.....	64
Enabling Meeting Exchange bridge features.....	64
Configuring bridge operators for Meeting Exchange.....	65
Configuring communication between Meeting Exchange and Communication Manager.....	65
Configuring on-demand conferences for PIN prompting (Optional).....	66
Configuring the Presense Server for one-X Portal.....	66
Configuring Presence security certificates.....	66
Configuring non—one-X Portal users in the Presence group.....	69
Configuring the Presence server.....	70
Reducing Axis logging for Presence.....	71
Configuration worksheets for integrated servers.....	72
Configuration worksheet: AE Services.....	72
Configuration worksheet: Communication Manager.....	73
Configuration worksheet: Modular Messaging.....	75
Configuration worksheet: Meeting Exchange.....	79
Configuration worksheet: Presence.....	81
Configuration worksheet: Dial Plan.....	83
Configuration worksheet: Mobility Extension Bank.....	84
Configuration worksheet: Enterprise Directory server.....	85
Chapter 4: Validating the one-X Portal environment.....	89
Environment Validation tool.....	89
Tests performed by the Environment Validation tool.....	89
Log created by the Environment Validation tool.....	90
Sample log file for the Environment Validation tool.....	90
Installing the Environment Validation tool.....	91
Configuring the TSAPI.PRO file for the Environment Validation tool.....	91
Configuring the logs for the Environment Validation tool.....	92

Running the Environment Validation tool.....	93
Environment Validation tool interface.....	94
Chapter 5: Configuring the one-X Portal desktop.....	101
Administrator and user desktop prerequisite checklist.....	101
Creating instructions for users of one-X Portal and the Administration application.....	104
User Worksheet: getting started with one-X Portal.....	105
User worksheet: installing one-X Portal Extensions.....	105
Avaya one-X Portal and Administration application configuration checklist.....	106
Configuring pop-up blockers.....	107
Setting the security zone in Internet Explorer.....	108
Setting advanced browsing options in Internet Explorer.....	108
Configuring Internet Explorer for Citrix access.....	109
Setting JavaScript options in Firefox.....	109
Configuring Safari.....	110
Configuring proxy for Internet Explorer.....	111
Configuring proxy for Mozilla Firefox.....	111
Chapter 6: Installing one-X Portal.....	113
Installation worksheet: network information for servers.....	113
Installation worksheet: information required by Installation Wizard.....	117
Installing one-X Portal.....	126
Avaya one-X Portal Installation Wizard screens.....	127
Chapter 7: Configuring one-X Portal.....	137
Post-installation configuration checklist.....	137
Logging in to the one-X Portal Administration application.....	138
Configuring WebLM for one-X Portal.....	139
Verifying the WebLM settings.....	139
Installing a one-X Portal license.....	139
Creating directories for the Voice Messaging server and the Conferencing server.....	140
Configuring Dial Plans.....	141
Dial Plan services.....	141
Simple Dial Plan transformation.....	142
Pattern Matching transformation.....	144
Regular Expression transformation.....	146
Creating rules for a Dial Plan.....	148
Adding Dial Plans.....	154
Modifying Dial Plans.....	155
Configuring one-X Portal servers.....	157
Telephony servers.....	157
Voice Messaging servers.....	159
Conferencing services.....	161
Presence service.....	161
Mobility Extension Banks.....	162
Enterprise Directory domains.....	163
License server services.....	164
SNMP Traps.....	165
Restarting one-X Portal.....	166
Synchronizing the Enterprise Directory and Modular Messaging.....	167
Configuring users for one-X Portal.....	168
Avaya one-X Portal users.....	168
User Administration options.....	168
User administration checklist.....	170

System Profile.....	171
Group Profiles.....	173
Prototype Users.....	175
Provisioning a portal user.....	177
Configuring one-X Portal for SSL authentication (optional).....	182
Administration Application interface.....	183
Servers field descriptions.....	183
Scheduler field descriptions.....	193
System field descriptions.....	194
Users field descriptions.....	206
Chapter 8: Installing the one-X Portal Extensions.....	209
Installation options for the one-X Portal Extensions.....	209
Installing one-X Portal Extensions through SMS.....	209
Installing the one-X Portal Extensions.....	210
Chapter 9: Setting up one-X Portal on Citrix.....	213
Configuring the Citrix server for one-X Portal.....	213
Configuring the Citrix client for one-X Portal.....	213
Chapter 10: Troubleshooting the one-X Portal installation.....	215
Troubleshooting the one-X Portal installation.....	215
Resolving Administration Web Client Issues.....	216
Logging.....	216
Calling party name incorrect.....	223
AE Services server is not visible to one-X Portal.....	223
Uninstalling one-X Portal.....	224
Avaya one-X Portal uninstallation.....	224
Uninstalling one-X Portal.....	225
Uninstalling the Avaya Voice Player.....	226
Uninstalling the one-X Portal Extensions.....	226
Index.....	227

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 Communication Manager, Avaya Modular Messaging, Avaya Meeting Exchange, and Avaya Intelligent Presence Server.

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
- Avaya Communication Manager telephony features
- Any telephone 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 Meeting Exchange to view and control live conferences
- Integration with Avaya Intelligent Presence Server 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

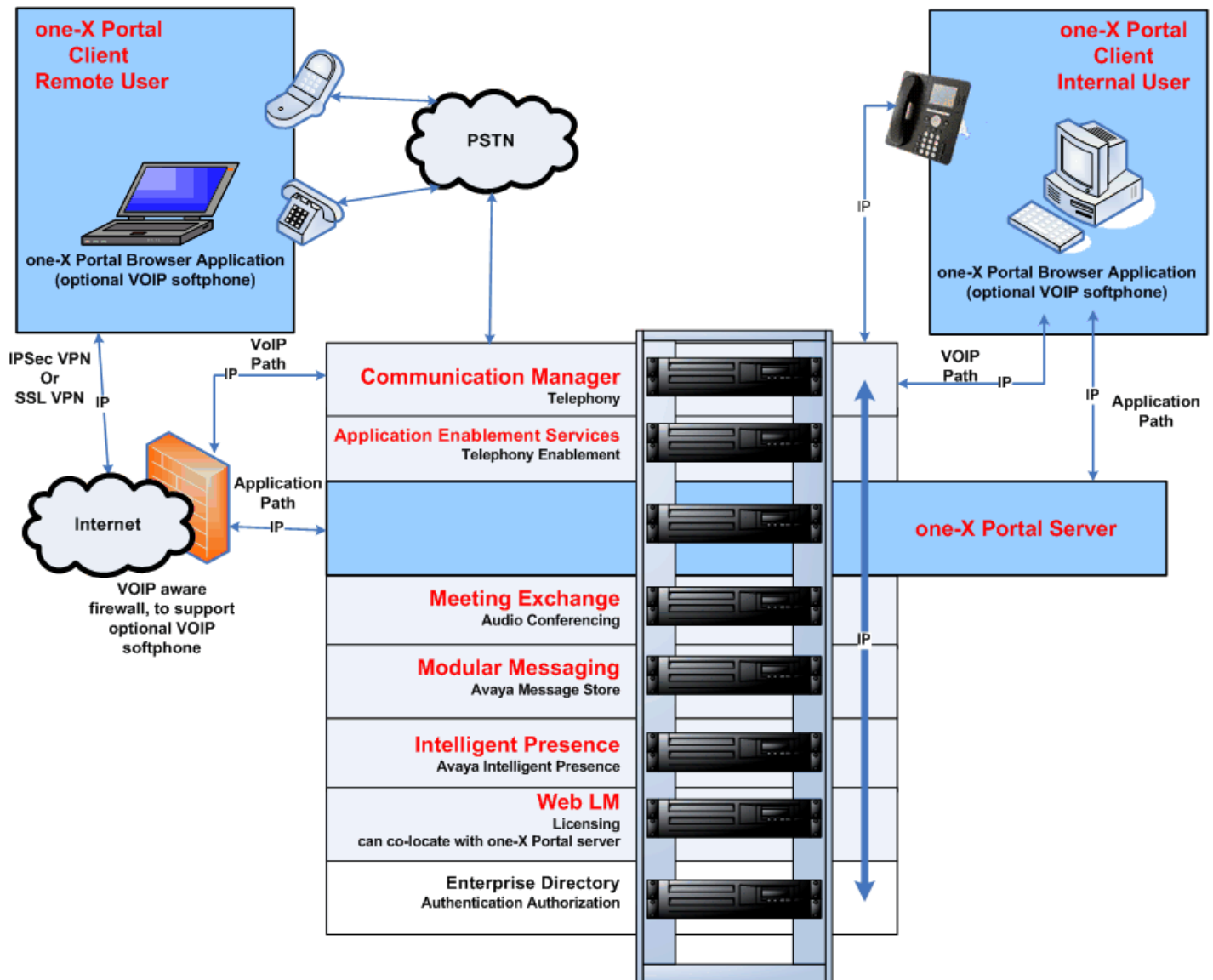
Avaya one-X Portal system diagram

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

External servers deliver telephony, messaging, mobility, conferencing, and presence services from the Avaya Communication Manager switch, Modular Messaging servers, Meeting Exchange servers, and the Avaya Intelligent Presence Server.

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 one-X Portal system:



Prerequisites for one-X Portal

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

- Avaya one-X Portal server
- Avaya WebLM
- Internal 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 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
- French (Parisian)
- German
- Italian
- Japanese
- Portuguese (Brazilian)
- Simplified Chinese
- Spanish (Latin American)

Security features of one-X Portal

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

Secure connections through firewalls

Avaya one-X Portal supports connection through a third-party, external, VOIP-aware firewall. Avaya has successfully tested one-X Portal with several external firewalls and a VPN tunnel.

User authentication through the enterprise directory

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

Access to 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 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 one-X Portal database.
- Encryption for bulk user import.
- Encryption for bulk user export.

Related topics:

[Additional security information](#) on page 11

Additional security information

Additional security information and documentation about all Avaya products, including one-X Portal and the Avaya components that integrate with one-X Portal are available at the [Avaya Security Advisories Website](#). 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 Website](#).

Capacities and performance of one-X Portal

Factors affecting performance

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

- Size of the machine that hosts the 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)	1000 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 login: 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: 20,000.
- Total number of users that can login on to Other Phone mode: 900



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

- CPU: Two dual-core processors, 1.86 Ghz 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 one-X Portal servers	1
Use case assumption for one-X Portal application	1 user session
Use case assumption for 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 one-X Portal with 1500 concurrent sessions. For this scenario, the following minimum hardware is recommended for the one-X Portal server:

- CPU: Two dual-core processors, 1.86 Ghz each
- Memory: 6 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 one-X Portal servers	1
Use case assumption for one-X Portal application	1 user session
Use case assumption for 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 CM 5.0, one-X Portal can run with IP softphone if the user logs on to one-X Portal using shared control mode. Otherwise, only one softphone application can control your business telephone extension. You cannot use one-X Portal at the same time as you use an

IP softphone application to handle calls to your extension. You can install these applications on the same computer as one-X Portal, but you cannot use them simultaneously.

These applications include:

- Avaya IP Softphone
- Avaya one-X Desktop Edition
- Avaya IP Agent

Software interactions with one-X Mobile

Avaya strongly suggests not to use one-X Portal and one-X Mobile with the same telephone extension. If your telephone extension is configured for one-X Mobile and one-X Portal on Avaya Communication Manager, there may be some performance inconsistency in certain situations.

Software interactions with Meeting Exchange

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

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

Software interactions with Modular Messaging

Avaya strongly suggests not to use the Web Client for Modular Messaging if you use one-X Portal to read, reply to, and create messages. 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 computers only. Avaya one-X Portal Extensions are not supported on Mac computers.

VOIP support on Windows only

Avaya one-X Portal supports VOIP for users only with Windows computers with Internet Explorer .

Avaya one-X Portal Message Recorder

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

Supporting Windows applications for one-X Portal

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

Note:

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

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

Avaya Phone Interface

The Avaya Phone Interface is the component that provides the Voice Over IP functionality and allows you to make and receive telephone call using a Windows computer.

You can install the Avaya Phone Interface the first time you log into one-X Portal in Internet Explorer on a Windows computer.

Avaya one-X Portal Message Recorder

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

You can install the Avaya one-X Portal Message Recorder the first time you log into one-X Portal in Internet Explorer on a Windows computer.

Avaya Voice Player

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

You can download and install the Avaya Voice Player from the **Other Settings** dialog box in one-X Portal.

Terminology used in one-X Portal

Term used in 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.

Before you install 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.

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

Port requirements for one-X Portal

- [Server to server ports](#) on page 19
- [AE Services to Communication Manager ports](#) on page 20
- [Avaya one-X Portal and administration applications to server ports](#) on page 21
- [Avaya one-X Portal VOIP client to server ports](#) on page 21
- [SNMP ports](#) on page 22

Server to server ports

Server	Protocol	Default ports		Configurable	Comments
		External Server	One-X Portal		
Modular Messaging	SMTP	25	25	1024-65000	
	IMAP4/SSL	993	993	1024-65000	

Server	Protocol	Default ports		Configurable	Comments
		External Server	One-X Portal		
	LDAP	389	389	No	MM to LDAP
Meeting Exchange	TCP	20002	20002	No	Meeting Exchange 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	
WebLM	HTTP	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	
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
ASAI	Configurable in range 1050-1065	Fixed at 8765

Protocol	AE Services	Communication Manager
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 or HTTPS	80 or 443	Yes
Avaya one-X Portal Extensions	HTTP or HTTPS	80 or 443	Yes
Administration application	HTTP or HTTPS	80 or 443	Yes
Administration application Command Line Interface	SOAP	8880	Yes

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	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 correspondi	one higher than the correspondi	No

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

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

Software	Supported versions	Location
Operating system	Red Hat Enterprise Linux ES 4.0 with the following components: • Update 4, 32 bit • Daylight Savings Time patch 2006m-3.el4.noarch.rpm • X Windows	Avaya one-X Portal server machine
Web browser	Mozilla Firefox 2.0	Avaya one-X Portal server machine Computer used by one-X Portal administrator.



Note:

During RHEL installation, check the option to install Legacy Software Development packages. Verify whether the following RPMs are installed after Red Hat installation is complete:

- compat-libstdc++-33.3.2.3.47.3
- compat-libstdc++-296-2.96132-7.2

Use the command: `rpm -qa | grep compat-libstdc`

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: AE Services requires a dedicated WebLM. Do not install the one-X Portal license on the Web License Manager used by AE Services.

Requirement	Supported versions	Notes
Telephony switch	• Avaya Communication Manager 5.0 • Avaya Communication Manager 4.0 with build greater than 730.2	
Messaging application	• Avaya Modular Messaging 3.0 SP2 with hot fix for deadlock issues. • Avaya Modular Messaging 4.0	
CTI application	Avaya Enablement Services 4.1 and 4.2	Uses DMCC and TSAPI connections through Application Enablement Services.
Conferencing application	• Avaya Meeting Exchange 4.1.2 • Avaya Meeting Exchange 5.0	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 Service for Windows 2003 Server, SP 1 • IBM Domino Server 7.0 • Novell eDirectory 8.8 SP1 • SUN ONE Directory Server 5.1	

Related topics:

[Location of the Avaya Web License Manager](#) on page 33

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 1.5	Yes	Yes	Yes	Yes
Mozilla Firefox 2.0	Yes	Yes	Yes	Yes
Microsoft Internet Explorer 6.0	Yes	No	No	No
Microsoft Internet Explorer 7.0	Yes	Yes	No	No
Apple Safari 2.0	No	No	Yes	No
Apple Safari 3.0	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
- Apple OS X V10.x
- Red Hat Enterprise Linux Desktop 4 Update 4, 32 bit

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 Vista	Apple OS X V10.x	Red Hat Enterprise

Software	Windows XP	Windows Vista	Apple OS X	Red Hat Enterprise Linux Desktop
				Linux Desktop 4 Update 4, 32 bit
Web browser	• Mozilla Firefox 2.0 • Microsoft Internet Explorer 6.0 • Microsoft Internet Explorer 7.0	• Mozilla Firefox 2.0 • Microsoft Internet Explorer 7.0	• Mozilla Firefox 2.0 • Apple Safari 2.0	Mozilla Firefox 2.0
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	Not supported	Not supported
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



Note:

During RHEL installation, check the option to install Legacy Software Development packages. Verify whether the following RPMs are installed after Red Hat installation is complete:

- compat-libstdc++-33.3.2.3.47.3
- compat-libstdc++-296-2.96132-7.2

Use the command: `rpm-qa|grep.compat-libstdc`

Support for one-X Portal applications on Citrix

Avaya one-X Portal supports Citrix Metaframe Presentation Server 4.0 for the one-X Portal and Administration application.



Note:

You cannot host the one-X Portal Extensions or any other supporting applications on Citrix.

Required hardware for one-X Portal components

Minimum hardware requirements

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

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

The hardware requirements provided in this section are minimums only. If you expect one-X Portal to handle a high volume of traffic, or one or more individuals to carry more 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 one-X Portal system.



Important:

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

Related topics:

[Avaya one-X Portal server hardware requirements](#) on page 27

[Avaya one-X Portal user and administrator hardware requirements](#) on page 28

Avaya one-X Portal server hardware requirements

The hardware requirements provided in this section are minimums only. If you expect one-X Portal to handle a high volume of traffic, or one or more individuals to carry more 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 one-X Portal system.

The server that hosts the one-X Portal server must meet the following minimum hardware specifications:

CPU	Two dual-core processors 1.86GHz or higher
Memory	6 GB RAM
Hard drive	Minimum 8 GB free space
Network card	100 Mbps
Optical drive	DVD/CD combination drive

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

The hardware requirements provided in this section are minimums only. If you expect one-X Portal to handle a high volume of traffic, or one or more individuals to carry more 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 one-X Portal system.

- [Windows desktop](#) on page 28
- [Mac desktop](#) on page 29
- [Linux desktop](#) on page 29
- [Peripherals required for all operating systems](#) on page 29



Note:

Avaya one-X Portal Extensions are only supported on Windows desktops.

Windows desktop

Processor	Pentium III 800MHz or better
Memory	512 MB RAM minimum
Hard drive	1.50 GB of free space
Optical drive	CD-ROM drive or DVD-ROM drive
Sound card	As provided with computer

Network card	10 Mbps or better
---------------------	-------------------

Mac desktop

Processor	1.33GHz or higher
------------------	-------------------

Memory	512 MB RAM minimum
---------------	--------------------

Hard drive	1.50 GB of free space
-------------------	-----------------------

Optical drive	CD-ROM drive or DVD-ROM drive
----------------------	-------------------------------

Sound card	As provided with computer
-------------------	---------------------------

Network card	10 Mbps or better
---------------------	-------------------

Linux desktop

Processor	Pentium III 800MHz or better
------------------	------------------------------

Memory	512 MB RAM minimum
---------------	--------------------

Hard drive	1.50 GB of free space
-------------------	-----------------------

Optical drive	CD-ROM drive or DVD-ROM drive
----------------------	-------------------------------

Sound card	As provided with computer
-------------------	---------------------------

Network card	10 Mbps or better
---------------------	-------------------

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 timestamps for all integrated systems are consistent. If time is not synchronized on these machines, end users may see inconsistent entries in one-X Portal.

For example, the Messages portlet may show that a voice message arrived before the related missed call.

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

- The server that hosts one-X Portal.
- All servers that host integrated systems, such as Communication Manager, Modular Messaging, and Avaya Intelligent Presence Server.

For Modular Messaging 3.0, contact Avaya Technical Support for assistance with NTP. Only an Avaya representative has the command line access required to enable NTP.



Important:

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

Telephony network performance between one-X Portal and AE Services

Location of servers

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

- Place the one-X Portal server, AE Services server, and Communication Manager CLAN resources as network-close as possible.
- Follow the AE Services server limits if one-X Portal has to run with other applications running on the same AE Services server.

Guidelines for network performance

Average round trip packet delay	No more than 50 ms
Periodic spiked delays	No more than 1.3 seconds while maintaining the 50 ms average

Network firewall guidelines

If users will access one-X Portal from outside the internal network, Avaya recommends that you implement a third-party, 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 guidelines

Required broadband internet connection

Remote users must connect to 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 kbs per VOIP user
End-to-end average packet delay	120 ms
Average jitter	Less than 20 ms

The VOIP bandwidth requirements for 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 one-X Portal deployment, because network and other conditions can impact bandwidth use.

The VOIP component in one-X Portal uses an 8 kHz one-byte sampling without compression. Assuming only one side of a connection communicates at a time, Avaya estimates that the following guidelines apply to VOIP bandwidth use:

- If 1000 VOIP users talk simultaneously to internal telephones, the bandwidth requirements are 4 Mb/s.
- If 1000 VOIP users talk simultaneously to outside telephones, the bandwidth requirements are 8 Mb/s.

Actual bandwidth used is approximately half of peak use, because the VOIP codec does not transmit data during silence. However, when considering this bandwidth use, you must make allowances for packet collision on local network segments. During one-X Portal activity, Avaya estimates the following network traffic:

- An active one-X Portal user can use up to 16 kb/s 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 five minutes, bandwidth use drops to about 1.6 kb/s. This traffic occurs because one-X Portal polls the server approximately once a second.

Licensing requirements for one-X Portal

Licensing requirements

Before you install one-X Portal, Avaya recommends that you obtain licenses for one-X Portal and all integrated components.

Licenses for one-X Portal

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

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

Licensing requirements for integrated Avaya components

You must obtain license files for all Avaya components that you want to integrate with one-X Portal. For detailed information about the license requirements for these products, see the product documentation or consult your Avaya representative or Avaya BusinessPartner representative.

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

Communication Manager	IP-API-A licenses, Extension to Cellular, Softphone and CT Adjunct Links enabled.
Application Enablement Services	TSAPI and DMCC functions.
Modular Messaging	Message store platform, number of mailboxes, and maximum number of concurrent TTS sessions.
Meeting Exchange	As required by your conference bridge version.

Related topics:

[Requesting a license file](#) on page 34

[Obtaining a host ID](#) on page 33

Location of the Avaya Web License Manager

Avaya Web License Manager location

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

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



Important:

AE Services requires a dedicated WebLM. Do not install the one-X Portal license on the Web License Manager used by AE Services.

Recommendations for WebLM location

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 AE Services, Avaya recommends that you use the existing WebLM for one-X Portal.

Only use the local WebLM server if the network does not include a WebLM, or if the existing WebLM is not a version supported by one-X Portal.

Related topics:

[Environment validation checklist](#) on page 37

[Required software for integrating servers with one-X Portal](#) on page 23

Obtaining a host ID

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

On the machine that will host the one-X Portal server, run the following command:

```
ifconfig -a eth0 | grep -i Hwaddr
```

This command will return the following text. The highlighted text represents the host ID of the machine:

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

Next steps

Request a license from Avaya for the one-X Portal system.

Related topics:

[Licensing requirements](#) on page 32

Requesting a license file

Prerequisites

Obtain the host ID for the machine that hosts the one-X Portal server.

If you have any questions about the process to request a license file, consult your Avaya representative or Avaya BusinessPartner representative.

-
1. To acquire a license file, provide the following information to your Avaya representative or Avaya BusinessPartner:

Required information	Description
Host ID	Host ID for the machine that will host the WebLM for one-X Portal
SAP order number	Avaya assigns one or more numbers to each one-X Portal order in the SAP system.
Customer name and official contact information	Name of the customer who purchased the one-X Portal system with the name, telephone number, and other contact information for the official contact person for that customer.
BusinessPartner, Tier I, and Tier II information	Optional. You only need to provide this information only if applicable.

2. After you receive the one-X Portal license file, place a copy of the license file in a safe location.

Related topics:

[Licensing requirements](#) on page 32

Customizing one-X Portal

Rebranding options for one-X Portal

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

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

Rebranding one-X Portal



Caution:

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

-
1. Copy the ReBranding zip file from the 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 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 one-X Portal has not been damaged.
-

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

Environment validation checklist

This checklist includes the hardware and software required for a complete 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 one-X Portal.

- [Prerequisites for one-X Portal server machine](#) on page 37
- [Prerequisites for integrated components](#) on page 38
- [Prerequisites for system network](#) on page 39

Prerequisites for one-X Portal server machine

For notes and details of tested server hardware, see:

- [Avaya one-X Portal server hardware requirements](#) on page 27
- [Required software for the one-X Portal server](#) on page 23

Requirement	Value		✓
Hardware	CPU	Two dual-core processors 1.86GHz or higher	
	Memory	6 GB RAM	
	Hard drive	Minimum 8 GB free space	
	Network card	100 Mbps	
	Optical drive	DVD/CD combination drive	

Requirement	Value	✓
Operating system	Red Hat Enterprise Linux ES 4.0 with the following components: • Update 4, 32 bit • Daylight Savings Time patch 2006m-3.el4.noarch.rpm • X Windows	
Web browser	Mozilla Firefox 2.0	

Prerequisites for integrated components

For more details about these requirements, see [Required software for integrating servers with one-X Portal](#) on page 23.

Component	Requirement	Supported versions	✓
Telephone	Telephony switch	• Avaya Communication Manager 5.0 • Avaya Communication Manager 4.0 with build greater than 730.2	
	CTI application	Avaya Enablement Services 4.1 and 4.2	
Bridge Conferencing	Conferencing application	• Avaya Meeting Exchange 4.1.2 • Avaya Meeting Exchange 5.0	
Messaging	Messaging application	• Avaya Modular Messaging 3.0 SP2 with hot fix for deadlock issues. • Avaya Modular Messaging 4.0	
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 Service for Windows 2003 Server, SP 1 • IBM Domino Server 7.0	

Component	Requirement	Supported versions	✓
		• Novell eDirectory 8.8 SP1 • SUN ONE Directory Server 5.1	

Prerequisites for system network

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

- [Network firewall guidelines](#) on page 30
- [Telephony network performance between one-X Portal and AE Services](#) on page 30
- [Time synchronization requirements](#) on page 29

Requirement	Value	✓				
Firewall	If users will access one-X Portal from outside the internal network, Avaya recommends that you implement a third-party, external, H.323 VOIP-aware firewall.					
Telephony network performance between one-X Portal server and AE Services	<table><tr><td>Average round trip packet delay</td><td>No more than 50 ms</td></tr><tr><td>Periodic spiked delays</td><td>No more than 1.3 seconds while maintaining the 50 ms average</td></tr></table>	Average round trip packet delay	No more than 50 ms	Periodic spiked delays	No more than 1.3 seconds while maintaining the 50 ms average	
Average round trip packet delay	No more than 50 ms					
Periodic spiked delays	No more than 1.3 seconds while maintaining the 50 ms average					
Time synchronization requirements	The following machines require NTP (Network Time Protocol) software for time synchronization: • The server that hosts one-X Portal. • All servers that host integrated systems, such as Communication Manager, Modular Messaging, and Avaya Intelligent Presence Server.					

Server prerequisites checklist

Verify that the following prerequisites have been configured for one-X Portal before you run the 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 • Meeting Exchange • Application Enablement Services • Avaya Intelligent Presence Server • Directory Service	See the documentation provided with the component. Installing required components for integrated servers on page 44
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 44
3	Install Linux with the required components on the one-X Portal server.	Installing Linux for one-X Portal on page 45
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 51
5	For each one-X Portal user, verify that the Directory user record has the required values.	Verifying Enterprise Directory user configuration on page 52
6	Create a Directory user for the one-X Portal administrative service account to start and stop the one-X Portal server and perform other administrative functions.	Creating the one-X Portal administrative service account on page 53
AE Services configuration		

#	Task	Instructions
7	If the one-X Portal system includes a dedicated AE Services server, install and configure AE Services.	Guidelines for installing AE Services on page 46
8	Create an H.323 Gateway list for the switch.	Configuring an H. 323 gateway list for AE Services on page 48
9	Create DMCC and TSAPI login IDs for one-X Portal.	Creating AE Services users for one-X Portal on page 47
Avaya Communication Manager configuration		
7	Configure Send All Calls in Communication Manager to enable Do Not Disturb for one-X Portal.	Configuring Send All Calls in Communication Manager for Do Not Disturb in one-X Portal on page 54
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 55
9	To enable users to handle calls with their computers, 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 55
Extension to Cellular configuration in Communication Manager		
10	Enable user extensions for one-X Portal.	Enabling user extensions on page 57
11	Add stations for one-X Portal mobility extensions.	Configuring mobility extensions on page 58
Modular Messaging configuration		

#	Task	Instructions
1 2	Configure and enable the following protocols: • IMAP4 • SMTP • LDAP	Configuring Modular Messaging ports and protocols on page 59
1 3	Authorize LDAP access.	Configuring Modular Messaging LDAP access on page 60
1 4	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 60
1 5	Modular Messaging 3.1 only: Create a trusted server for super-user IMAP4 connections.	Configuring super-user IMAP4 connections in Modular Messaging 3.1 on page 61
1 6	Modular Messaging 3.0 SP2 only: • Activate NTP on the MSS that communicates with one-X Portal. • Activate super-user IMAP4 connections.	Contact Avaya Technical Support for assistance with the following tasks: • Activating NTP in Modular Messaging 3.0 SP2 on page 62 • Activating super-user IMAP4 connections in Modular Messaging 3.0 SP2 on page 63
1 7	Modular Messaging 3.0 SP2 only: Create trusted servers for LDAP and super-user IMAP4 connections.	Creating trusted servers in Modular Messaging 3.0 SP2 on page 63
Meeting Exchange configuration		
1 8	Enable and verify the following features: • ANI • Music • PINs (optional) • SIP trunk set	Enabling Meeting Exchange bridge features on page 64

#	Task	Instructions
	• DTMF • Dial	
1 9	Configure the following parameters with the required values: • Operator codes • Flex-DAPI	Configuring bridge operators for Meeting Exchange on page 65
2 0	Make sure that the <code>/usr/ipcb/config/telnumToUri.tab</code> file routes from Meeting Exchange to Communication Manager.	Configuring communication between Meeting Exchange and Communication Manager on page 65
2 1	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 66
Avaya Intelligent Presence Server configuration		
2 2	Configure 1XP security certificates. • 1XP certificate • AcpUMSBus to be "non-secure"	Configuring Presence security certificates on page 66
2 3	Configure AcpUMSBus to be "non-secure"	Configuring AcpUMSBus as non-secure for Presence
2 3	Configure Presence server	Configuring the Presence server on page 70
2 4	Configure SIP Presence server	Configuring the SIP Presence server
2 5	Reduce Axis Logging	Reducing Axis logging for Presence on page 71

Installing required components for integrated servers



Tip:

If a supported version of the software for an integrated server is already up and running in the enterprise, you do not need to install a new system. You can integrate 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 one-X Portal:

Component	Documentation
Communication Manager	• <i>Installing and Configuring the Avaya S8500 Media Server</i> • <i>Administrator Guide for Avaya Communication Manager</i>
Application Enablement Services	• <i>Avaya MultiVantage Application Enablement Services Installation Guide</i> • <i>Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide</i>
Modular Messaging	• <i>Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Installation and Upgrades</i> • <i>Messaging Application Server Administration Guide</i>
Meeting Exchange 4.1 or higher	• <i>Installing the CS700/CS780 Audio Conferencing Server</i> • <i>Installing the S6200 and S6800 Conferencing Servers</i>

Component	Documentation
Avaya Intelligent Presence Server 1.0	• <i>Configuring the CS700/CS780 Audio Conferencing Servers</i>
	• <i>Configuring S6200, S6500, and S6800 Conferencing Servers</i>
	• <i>Installing the OCS Server</i>
	• <i>Installing the OCS Edge Server</i>
	• <i>Installing the CA Server</i>
	• <i>Configuring the OCS and OCS Edge Servers</i>
	• <i>Configuring the CA Server</i>

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

Installing Linux for one-X Portal

Prerequisites

Avaya does not provide a Linux RPM or a Linux installation script. Before you install one-X Portal, you must obtain and install Red Hat Enterprise Linux ES 4.0 with the following components:

- Update 4, 32 bit
- Daylight Savings Time patch 2006m-3.el4.noarch.rpm
- X Windows

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

1. Install Linux on the one-X Portal server with the instructions provided with the Red Hat installation utility.

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

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 one-X Portal.

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

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

- d. Use the Linux default partitioning.

3. Complete the Linux installation.



Note:

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

- compat-libstdc++-33.3.2.3.47.3
- compat-libstdc++-296-2.96132-7.2

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, 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, one-X Portal should 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 allows each "Switch Connection" to be associated with a list of IP Addresses for H.323 gateways.

For some configurations, one-X Portal can function without an H.323 gateway list. However some 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 H.323 gateways configured and one CLAN becomes unavailable, AE Services automatically connects to another CLAN identified in the list.
- Multiple CLANS** An H.323 gateway list enables you to use a different CLAN for H.323 communication between Communication Manager and AE Services than the CLAN used for the VoIP connection between the one-X Portal application and Communication Manager. For this configuration, the H.323 gateway list has to be present in AE Services, and populated with the IP Addresses that AE Services needs to use to communicate with Communication Manager.

Required users for one-X Portal

Create two users for 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 one-X Portal.

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

Switch name

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

Creating AE Services users for one-X Portal

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

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

Telephony adapter should be restarted after AES 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. Select the **User Management** menu from OAM Web and log in to AE Services User Management.
 2. From the **User Management** menu, select **User Management > Add User**.
 3. Add a DMCC (formerly CMAPI) user for one-X Portal.
 4. Add a TSAPI user for one-X Portal with the following permissions:
 - Unrestricted access in AE Services.
 - 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. Select **Administration > Security Database > CTI Users > List All Users** to access the CTI Users page and verify the users that you just created.
-

Configuring an H. 323 gateway list for AE Services

AE Services allows each "Switch Connection" to be associated 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.

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. You can integrate with an existing enterprise directory server, or you can use a dedicated enterprise directory server for one-X Portal.

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

Limitations on support for Active Directory domains

Each 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 one-X Portal users may 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, one-X Portal considers the users in the additional domains to be contacts only, and only obtains address book data from those domains. You cannot provision users from the additional domains, and those users cannot log in to the one-X Portal deployment.

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

Limitations on support for other Enterprise Directory domains

Identity resolution on the other supported enterprise directories is only supported on the LDAP server in the LDAP Domain on one-X Portal.

Supported Active Directory domain topologies

Domain topology	Description
Combined domain	The users and security groups are in the same Active Directory domain. For this topology, you configure one-X Portal with the same domain for the user domain and the resource domain.
Split domain in same forest	The users and security groups are in separate Active Directory domains. These domains are in the same forest.

Domain topology	Description
	For this topology, you configure one-X Portal with different domains for the user domain and resource domain.
Split domain in different forest	Uses two Active Directory domains that are in different forests. For this topology, you configure one-X Portal with different domains for the user domain and resource domain. To ensure the required access, this topology may require a different service account and password for each forest when you install one-X Portal.

Required security groups

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

- Administrative users
- 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 the one-X Portal users.

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

If you plan to deploy more than one one-X Portal server in an environment, Avaya recommends that you create a unique set of security groups for each one-X Portal server in the system, even if both deployments use the same Enterprise Directory domain. You can configure two one-X Portal deployments to use the same security groups. However, you cannot change the security groups assigned to a deployment without reinstalling one-X Portal.

Naming conventions for security groups

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

- Be unique in the Active Directory domain.
- Identify the group as related to one-X Portal
- Identify the 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 one-X Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft KB 275523.

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

- *deployment_name* 1XP Users
- *deployment_name* 1XP Administrators
- *deployment_name* 1XP Auditors
- *deployment_name* 1XP Presence

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

Determining the Active Directory domain topology

Important:

After you install one-X Portal, you cannot change the Active Directory domain topology. You must reinstall one-X Portal to change the domain topology.

-
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 will access one-X Portal.
 3. Identify the resource domain that defines the 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 49

Configuring Enterprise Directory security groups

Note:

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

-
1. In the resource domain, create Enterprise Directory security groups for the following groups of users in each one-X Portal deployment:
 - Administrative users who need access to the Administration application. Include the deployment in the group name, for example, Chicago 1XP Administrators.
 - Users who need access to the one-X Portal. Include the deployment in the group name, for example, Chicago 1XP Users.
 - Auditors who need read-only access to the Administration application. Include the deployment in the group name, for example, Chicago 1XP Auditors.
 - Users who you wish to be able to display presence information about. These users will not be allowed to log into one-X Portal and will not consume a license when configured.
 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 49

Verifying Enterprise Directory user configuration

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

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

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

In the user domain, for each one-X Portal user, verify that the Enterprise Directory user records:

- Are in the domain that hosts one-X Portal.
- Are assigned to at least one one-X Portal security group to provide the user with the required administrative, user, or auditor privileges.
- Have a pre-Windows 2000 logon name that is identical to the one-X Portal logon name.
- Include a user password and the desired password options.

Creating the one-X Portal administrative service account

Avaya one-X Portal requires you to 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 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, one-X Portal also requires a secondary service account in the resource domain.

You can map LDAP attributes to the attributes used in one-X Portal using the **System** tab in the 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.
 - For Active Directory only:
 - Does not require any privileges.
 - Is a member of the one-X Portal users and administrators security groups.
 2. For Active Directory only, for a split domain topology with the user domain and resource domain in different forests only, create a secondary service account in the resource domain 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.
- For Active Directory only:
 - Does not require any privileges.
 - Is a member of the one-X Portal users and administrators security groups.
- Does not have to be a member of either one-X Portal security group.

3. The administrative service account should be able to:

- validate the passwords of other users
- see the members of the security groups
- read any information that one-X Portal wants exported such as user phone numbers.

Configuring Communication Manager for one-X Portal

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

The Do Not Disturb functionality in 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 one-X Portal telephone settings for Do Not Disturb mode.
- Clicks **Ignore** when a call arrives in one-X Portal



Tip:

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

-
1. If necessary, 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.

**Tip:**

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

-
1. If necessary, 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. If necessary, log in to the Avaya Site Administration (ASA) application.
 2. Use the `change station` command to navigate to the Station screen for each extension.
 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.
-

Disabling AnnexH for Communication Manager 4.0

If the one-X Portal system includes users who will access their business extension from a remote telephone, you must disable AnnexH in Communication Manager 4.0. This configuration avoids an issue in Communication Manager 4.0 that can cause the loss of registration requests.



Tip:

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

-
1. In Communication Manager 4.0 administration, execute the following command:
`change ip-network-region x`
where `x` is the region associated with the AES endpoints.
 2. Navigate to page 2 of the administration screen.
 3. On page 2, change the value of **H.323 SECURITY PROFILES** to `CHALLENGE`.
Do not assign any other values to **H.323 SECURITY PROFILES**.
-

Configuring Extension to Cellular for one-X Portal

Extension to Cellular and 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 is dialed out of Communication Manager to the associated cell phone.

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 would dial after reaching the ARS table.

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

Avaya recommends that one-X Portal users configure their phone settings with E.164 format (+19788081234). This format allows one-X Portal to 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 one-X Portal. Avaya recommends values for these fields to ensure that user settings for Extension to Cellular and one-X Portal do not cause issues for users.

For example, Avaya recommends that you set the value of **Mapping Mode** to `termination`. If you set the value to `both`, one-X Portal is not notified of changes in the Extension to Cellular configuration if the user changes the status or number on the switch.



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 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 Stations with Off-PBX Telephone Integration, Page 1, configure the parameters listed in the following table:

Parameter	Recommended value
Station Extension	Extension assigned to the one-X Portal user.
Application	EC500
Dial Prefix	As appropriate for your system configuration.
Phone Number	Telephone number assigned to the extension of the one-X Portal user.
Trunk Selection	ars
Configuration Set	1 or as appropriate for your system configuration.

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

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

Configuring mobility extensions

The mobility extensions are a set of worker stations on the switch. These stations are not user extensions and should be created for use by one-X Portal only. Mobility stations need to be mapped via CM Network Region mapping, or native CLAN Network Region to a region that supports G711. Avaya one-X Portal uses the mobility extensions to dial feature access on the switch.

Each switch can have between 2 and 10 mobility extensions. The number of mobility extensions is related to the number of Extension to Cellular requests that the 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 configurations, see the *Administrator Guide for Avaya Communication Manager*.

-
1. If necessary, 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

```
add station next Page 1 of 4 STATION Extension: 20096 Lock Messages?
n BCC: 0 Type: 4620 Security Code: * TN: 1 Port: Coverage Path 1:
COR: 1 Name: Worker station Coverage Path 2: COS: 1 Hunt-to Station:
STATION OPTIONS Loss Group: 2 Personalized Ringing Pattern: 1 Data
Module? n Message Lamp Ext: 20096 Speakerphone: 2-way Mute Button
Enabled? y Display Language: english Expansion Module? n Survivable
GK Node Name: Media Complex Ext: Survivable COR: internal IP
SoftPhone? y
```

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 one-X Portal Administration application.

-
1. Navigate to the following Modular Messaging administration screen: **Global Administration > System Administration**.
 2. From this 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 one-X Portal.
-

Configuring Modular Messaging LDAP access

-
1. Navigate to the following Modular Messaging administration screen: **Global Administration > Networked Machine Management** .
 2. On the Networked Machine Management screen, set the value of **UpdatesIn** to **Yes** for the MSS in the Modular Messaging domain.
 3. Save the change.
 4. Navigate to the Test LDAP Connection screen and test the LDAP connection.
-

Verifying Modular Messaging subscriber values

For every one-X Portal user, at least one of the Modular Messaging subscriber values must match the corresponding value in the Active Directory record for the user. If none of these values match, 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 Active 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 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 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
 - c. Save your changes.

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

Configuring super-user IMAP4 connections in Modular Messaging 3.1

If your system includes Modular Messaging 3.1, you must activate super-user IMAP4 connections. This activation requires you to define the one-X Portal server as a Trusted Server and establish an SSL connection.

-
1. Navigate to the following Modular Messaging administration screen: **Global Administration > Messaging Administration**.
 2. Click **Trusted Servers**.
 3. On the Add Trusted Server page, add the one-X Portal server. Complete all required fields for the trusted server configuration, including the following:

- **Trusted Server Name:** Unique server name, such as oneXPortal.
 - **Machine Name / IP Address:** IP address of the one-X Portal machine. Do not use the fully qualified domain name.
 - **Access to Cross Domain Delivery:** No.
 - **LDAP Access Allowed:** Yes.
 - **IMAP Super User Access Allowed:** Yes.
 - **Service Name:** One X Portal.
 - **Special Type:** none.
 - **LDAP Connection Security:** No encryption required.
 - **IMAP4 Superuser Connection Security:** Must use SSL or encrypted SASL.
4. Click **Save** to record your changes.
 5. Navigate to the following Modular Messaging administration screen: **Global Administration > Messaging Administration > System Administration**.
 6. On the System Administration page:
 - Set the **IMAP 4 SSL Port** field to **Enabled**.
 - Record the port number in this field in the Modular Messaging configuration worksheet. The default port is 993.
 7. Click **Save** to record your changes.
-

Activating NTP in Modular Messaging 3.0 SP2

If your system includes Modular Messaging 3.0 SP2, you must manually activate NTP on the MSS that communicates with one-X Portal. This procedure ensures that the timestamps are synchronized in Modular Messaging for time synchronization and one-X Portal.



Important:

This procedure requires you to contact Avaya Technical Support for assistance. Only an Avaya representative has the required command line access.

-
1. At a command line on the MSS that communicates with one-X Portal, execute the following command: `\mtce\bin\enable_ntp_administration`.
 2. On the Date and Time page for the MSS, make sure that **Enable NTP** is checked.
-

Activating super-user IMAP4 connections in Modular Messaging 3.0 SP2

If your system includes Modular Messaging 3.0 SP2, you must manually activate super-user IMAP4 connections. This activation requires that a setting in the `config_params` file is updated.



Important:

This procedure requires you to contact Avaya Technical Support for assistance. Only an Avaya representative has the required command line access.

-
1. Edit the `/VM/config/config_params` file for the MSS to update the value of the IMAP4: Trusted Servers May Login As Superusers parameter to 1.
 2. Restart the MSS.
 3. Navigate to the following Modular Messaging administration screen: **Global Administration > System Administration**.
 4. On the System Administration page:
 - Set the **IMAP 4 SSL Port** field to **Enabled**.
 - Record the port number in this field in the Modular Messaging configuration worksheet. The default port is 993.
 5. Click **Save** to record your changes.
-

Creating trusted servers in Modular Messaging 3.0 SP2

If your system includes Modular Messaging 3.0 SP2, you must create two trusted servers for one-X Portal. One trusted server creates a secure connection for the IMAP4 super-user. The second trusted server creates the LDAP connection, which is not a secure connection.

-
1. Navigate to the following Modular Messaging administration screen: **Global Administration > Trusted Server Management > Add Trusted Server**.
 2. On the Trusted Servers page for the MSS, add the IMAP4 trusted server for one-X Portal. Complete all required fields for the trusted server configuration, including the following:
 - **Trusted Server Name:** Unique server name, such as `oneXPIMAP`.
 - **Machine Name / IP Address:** IP address of the one-X Portal machine. Do not use the fully qualified domain name.

- **Access to Cross Domain Delivery:** No.
 - **Service Name:** Unique service name, such as `One X Portal IMAP`.
 - **Special Type:** `none`.
 - **Connection Security:** Must use SSL or SASL.
3. Verify that the Trusted Server configuration for IMAP4 uses a secure socket.
 4. On the Trusted Servers page for the MSS, add the LDAP trusted server for one-X Portal. Complete all required fields for the trusted server configuration, including the following:
 - **Trusted Server Name:** Unique server name, such as `oneXPLDAP`.
 - **Machine Name / IP Address:** IP address of the one-X Portal machine. Do not use the fully qualified domain name.
 - **Access to Cross Domain Delivery:** No.
 - **Service Name:** Unique service name, such as `One X Portal LDAP`.
 - **Special Type:** `none`.
 - **Connection Security:** No encryption required.
 5. Verify that the Trusted Server configuration for LDAP does not use a secure socket.
-

Configuring Meeting Exchange for one-X Portal

Enabling Meeting Exchange bridge features

-
1. Enable the following Meeting Exchange settings:
 - a. ANI: verify that Meeting Exchange is configured to provide ANI (Caller ID) to identify meeting participants.
 - b. Music: verify that the music is available on Meeting Exchange.
 2. Optional: Enable the PINs setting and verify that support for PINs is available on Meeting Exchange.
 3. Enable the following features required for Communication Manager to Meeting Exchange connectivity:

- a. SIP trunk set: verify that calls from Communication Manager to Meeting Exchange provide Caller ID and DNIS correctly.
 - b. DTMF: verify that in-band/out-band DTMF in Communication Manager and Meeting Exchange match and DTMF is being properly received by Meeting Exchange.
4. Enable the Dial feature and verify that Dial from Meeting Exchange to Communication Manager is enabled and properly configured.
-

Configuring bridge operators for Meeting Exchange

-
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 one-X Portal server.
-

Configuring communication between Meeting Exchange and Communication Manager

After you complete the standard Meeting Exchange configuration for Communication Manager, you must ensure that the path from Meeting Exchange 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 Meeting Exchange 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 Meeting Exchange 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 values



Note:

You must configure Meeting Exchange to provide 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 Presense Server for one-X Portal

Configuring Presence security certificates

-
1. Get the IPS certificate:

- a. Copy the `generic.keystore.jks` file from IPS machine to the `/opt/certs` directory on the 1XP machine
- b. Open the command shell from 1XP machine and execute the following commands:
 - `mkdir /opt/certs`
 - `scp root@<IPS_host>: /opt/IPS/jabber/xcp/certs/generic.keystore.jks /opt/certs`
2. Open the WAS Admin console to configure certificates in WebSphere and log in via `http://<host>:9060/ibm/console`.
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** field.
 - c. Move **test alias** 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 > Import** 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 `ips` 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.

 Note:

For a fresh installation (WebSphere 6.1), this step has to be executed for all systems. However, for an upgrade, because the certificate name is “jsrserver” for all WebSphere 6.0, this only has to be done once.

- a. Select **default** certificate or **websphere dummy server** if this system was upgraded from 1XP 1.0.1.
 - 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 **jsrserver**.
 - c. Click **Extract** and complete the following fields:
 - Select **Filename** as `/tmp/default.pem`
 - Set **Data type** as `Base64-encoded`
 - Press **OK**
 11. Copy the `/tmp/default.pem` file from the 1XP machine to the IPS machine.
 12. From 1XP machine, execute this command: `scp /tmp/default.pem root@<IPS_host>:/opt/IPS/jabber/xcp/certs/default.pem`
 13. Save the master configuration.
 14. Stop WebSphere to have security changes activated by stopping the WAS server gracefully by completing the following fields:

 Note:

If this is a multiple 1XP to IPS configuration, perform these steps on the other WAS server.

- a. Set **Server** to `stopServer.sh server1`.
- b. Set **Server** to `stopServer.sh server1`.
- c. Enter Websphere to **User**.
- d. Enter Avaya to **Password**.

 Important:

Do not restart the WAS and 1XP servers until the IPS configuration is completed and XCP is functional.

Configuring non—one-X Portal users in the Presence group

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

1. Add the non-one-X Portal user on the LDAP directory server security group that is designated as the security group to be used by the Presence server.
2. Configure the appropriate Communication Manager and AE Services server from the **Servers** tab in the Administration Web Client application.
3. Create a **User Import** spreadsheet with the appropriate handles and user names of the non-one-X Portal users and set **Enable User** to n.

 Note:

The spreadsheet contains columns for User Monitor, Enable User, Display Name, User Properties, Group Profile Name, Service Providers, Provider parameters. The Enable User column must be the second column from the left on the spreadsheet.

4. Run a full **Enterprise Directory Synchronization** from the **Scheduler** tab in the Administration Web Client.
 5. Run the `User Import` script in the Administration Command Line Client to import the users.
-

Configuring the Presence server

1. Open the XCP configuration page `https://<host>:7300/admin`
2. Select the **Advanced** configuration view.
3. For the **Global Router**, add each of the 1XP 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 1XP 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.
 - d. In the **UMC-to_UMS configuration** section, complete the following field as indicated:
 - **WS Host**:`<IP address of the 1XP machine>`
 - **WS Port**:`9443`
 - **WS Service**:`/ums/services/UserMgmtServicePort`
 - **JMS Host**:`<IP address of the 1XP 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 1XP 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 1XP server.

6. To configure **SIP-PS** (SIP Presence Server), enter the following:
 - a. Set **Server Connection Idle Timeout (seconds)**: -1 (Never) or 0 as last owner disconnects or x time in seconds to -1 (this should be already set)
 - b. Set **interval (in seconds) to wait for SIP dialogs to shutdown cleanly before exiting the application** : 10 (this should be already set)
 - c. Click **Submit** to save SIP Presence Server Configuration
 7. To configure SIP Proxy, go to **SIP Stack Configuration Parameters > TLS Transport details** and complete the following fields as indicated:
 - a. Change **Port** from 5061 to 35061
 - b. Click **Submit** to save the SIP Proxy Configuration.
-

Reducing Axis logging for Presence

To reduce the large amount of Axis logging, separate from the XCP controller page.

-
1. In the shell, change directory to `/opt/IPS/presence/lib/path`.
 2. Add the following lines under `log4j.rootLogger = TRACE, FILE, hostlogsrv`:


```
log4j.logger.org.apache.axis=WARN
log4j.logger.com.avaya.coreservice.dss=WARN
```
 3. Restart the **Presence** server.
-

Configuration worksheets for integrated servers

Configuration worksheet: AE Services

This worksheet lists the information that you need to configure AE Services for one-X Portal. You will 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	AES123334		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		The port number used by the DMCC configuration for the AE Services server.
DMCC Login ID	cmapi		The login ID used by the DMCC configuration for the AE Services server.
DMCC Password			The password associated with the login ID used by the

Property Name	Property values		Notes
	Example value	Your value	
			DMCC configuration for the AE Services server.
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 login ID used by the TSAPI configuration for the AE Services server.
TSAPI Password			The password associated with the login ID used by the TSAPI configuration for the AE Services server.

Configuration worksheet: Communication Manager

This worksheet lists the information that you need to configure Communication Manager for one-X Portal. You will 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.

Property Name	Property values		Notes
	Example value	Your value	
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 Telephony server to enable Extension to Cellular on one-X Portal, for example, *88, *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 Telephony server to enable Extension to Cellular on 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 Telephony server to enable Extension to Cellular on 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

Property Name	Property values		Notes
	Example value	Your value	
			established using the CLAN IP address. Since VOIP connection in 1XP requires CM 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 one-X Portal.
Dial Plan	dialplanhandle		The handle of the Dial Plan used by this server.

Configuration worksheet: Modular Messaging

This worksheet lists the information that you need to configure Modular Messaging for one-X Portal. You will 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 one-X Portal user connections needed to communicate with the Voice Messaging server (the MSS of the Modular Messaging server).

Property Name	Property values		Notes
	Example value	Your value	
			This value is not available in Modular Messaging. You must create this value in the Administration application.
Client Connections Increment	2		The number of the 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 create this value in the Administration application.
Messages Temp Directory			The location of the temporary directory where sections of voice mail message are stored. When creating a new Voice Messaging server, leave this field empty because one-X Portal automatically creates a new directory named msgworkdirectory with the correct permissions for all new Voice Messaging servers. 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

Property Name	Property values		Notes
	Example value	Your value	
			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 login 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 login 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		Check this option. one-X Portal requires a secure IMAP connection for the Voice Messaging server.

Property Name	Property values		Notes
	Example value	Your value	
			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 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 login 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 login 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 checked, 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.

Property Name	Property values		Notes
	Example value	Your value	
LDAP Port	389		The port number used by the LDAP configuration for the Voice Messaging server. Use a non-secure port.
LDAP Login ID	oneXPLDAP		The login 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 login 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: Meeting Exchange

This worksheet lists the information that you need to configure Meeting Exchange for one-X Portal. You will 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 Meeting Exchange 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. This value is not available in Meeting Exchange. 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 used by the BCAPI configuration for the Meeting Exchange server as an IP address or a DNS address.
BCAPI Login ID	username1		The login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Password			The password associated with the login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Secondary Login ID	username2		The Secondary Login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Password			The password associated with the Secondary Login ID used by the BCAPI configuration for the Meeting Exchange server.

Configuration worksheet: Presence

This worksheet lists the information that you need to configure Presence for one-X Portal. You will need these values to configure the Avaya Intelligent Presence Server 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 Avaya Intelligent Presence Server.
Version	1.0		The version of the server configured on the system. For the Avaya Intelligent Presence Server , 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 Avaya Intelligent Presence Server. You must create this value in the Administration application.
Enabled	Yes		When checked by the administrator, enables the server for the system.
IPS Publish To Port	15061		The port number on the Avaya Intelligent Presence Server to which the presence information of the user is published. This is a remote port.
LPS Consumer Port	5070		The port number on the Avaya Intelligent Presence Server where the consumer information is received.

Property Name	Property values		Notes
	Example value	Your value	
			These are local ports where one-X Portal is running.
LPS Supplier Port	5060		The port number on the Avaya Intelligent Presence Server from which the published information is furnished. These are local ports where 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 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 one-X Portal is running.
UMS Login ID	oneXPUMS		The login ID used by this configuration of the User Management Service.
UMS Password			The password associated with the login ID used by this configuration for the User Management Service.

Property Name	Property values		Notes
	Example value	Your value	
UMS Confirm			Verification of the password associated with the login ID used by this configuration for the User Management Service.

Configuration worksheet: Dial Plan

This worksheet lists the information that you need to configure a dial plan for one-X Portal. You will 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. 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 dial before an outbound phone number to get the call out of 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.

Property Name	Property values		Notes
	Example value	Your value	
Prefixes International	011		The digits to dial 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 phone call placed within the country. 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 allowed in a phone call placed within the 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: Mobility Extension Bank

This worksheet lists the information that you need for the Mobility Extension Bank. You will 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.

Property Name	Property values		Notes
	Example value	Your value	
			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: Enterprise Directory server

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

 Tip:

If the 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, one-X Portal considers the users in the additional domains to be contacts only, and only obtains address book data from those domains. You

cannot provision users from the additional domains, and those users cannot log in to the 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.
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 one-X Portal users. There is only one user domain. You cannot change this domain. • Resource: indicates the domain contains the 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.

Property Name	Property values		Notes
	Example value	Your value	
Has Backups	Yes		Indicates if there are secondary Directory servers for this domain by displaying Yes or No.
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)	<i>admin_login</i>		The login 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 one-X Portal Environment Validation tool tests that the systems you have just configured will be able to communicate with one-X Portal. You can find this tool in the Tools directory of the one-X Portal DVD-ROM.

When to run the Environment Validation tool

Run the Environment Validation tool after you configure the prerequisites for one-X Portal and before you install 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 Meeting Exchange 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 one-X Portal server.

-
1. On the 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 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/IBMJava2-142/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 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 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.properties` 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.properties` 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.properties` file.
-

Running the Environment Validation tool

Prerequisites

Before you run the Environment Validation tool:

- Configure the prerequisites for one-X Portal.
- Install the Environment Validation tool and the IBM Java Runtime SDK on the one-X Portal server.
- Configure the `TSAPI.PRO` file.

-
1. In a terminal window on the machine that hosts 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 97
Conferencing	Conferencing Configuration on page 98

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

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

- [Voice Messaging](#) on page 95
- [TSAPI Configuration](#) on page 96
- [DMCC Configuration](#) on page 97
- [Conferencing Configuration](#) on page 98

**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 login 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 login 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		Check this option. 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	<i>CORP#BUIL D ING#CSTA #NNNN3333 3</i>		A drop-down list of available TSAPI services. This test requires the option that includes the hostname of the AE Services server used by one-X Portal.
Login ID	admin_login		The login ID used by the TSAPI configuration for the AE Services server.
Password			The password associated with the login ID used by the TSAPI configuration for the AE Services server.
Source Phone Number			The source telephone number that will make the test call.

Property Name	Property values		Notes
	Example value	Your value	
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 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 login ID used by the DMCC configuration for the AE Services server.
DMCC Password			The password associated with the login 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	9155533312 34		Telecommuter number that will make the test telephone call.

Property Name	Property values		Notes
	Example value	Your value	
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 used by the BCAPI configuration for the Meeting Exchange server as an IP address or a DNS address.
BCAPI Login ID	username1		The login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Password			The password associated with the login ID used by the BCAPI configuration for the Meeting Exchange 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

Property Name	Property values		Notes
	Example value	Your value	
			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 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 one-X Portal.

- [Windows desktop](#) on page 28
- [Mac desktop](#) on page 29
- [Linux desktop](#) on page 29

Windows desktops

Requirement	Value	✓
Desktop hardware	Processor Pentium III 800MHz or better Memory 512 MB RAM minimum Hard drive 1.50 GB of free space Optical drive CD-ROM drive or DVD-ROM drive Sound card As provided with computer Network card 10 Mbps or better	
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	

Requirement	Value	✓
Operating system	• Microsoft Windows XP SP2 • Microsoft Windows Vista	
Web browser	• Mozilla Firefox 1.5 • Mozilla Firefox 2.0 • Microsoft Internet Explorer 6.0 on Windows XP only • Microsoft Internet Explorer 7.0	
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 1.33GHz or higher Memory 512 MB RAM minimum Hard drive 1.50 GB of free space Optical drive CD-ROM drive or DVD-ROM drive Sound card As provided with computer Network card 10 Mbps or better	
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.x	

Requirement	Value	✓
Web browser	• Mozilla Firefox 1.5 • Mozilla Firefox 2.0 • Apple Safari 2.0	
Email application	Not supported	
SMS application (optional)	Not supported	
VOIP (This Computer)	Not supported	
Avaya one-X Portal Extensions	Not supported	

Linux desktops

Requirement	Value	✓
Desktop hardware	Processor Pentium III 800MHz or better Memory 512 MB RAM minimum Hard drive 1.50 GB of free space Optical drive CD-ROM drive or DVD-ROM drive Sound card As provided with computer Network card 10 Mbps or better	
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 1.5 • Mozilla Firefox 2.0	
Email application	Not supported	
SMS application (optional)	Not supported	
VOIP	Not supported	

Requirement	Value	✓
(This Computer)		
Avaya one-X Portal Extensions	Not supported	

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

Users do not need to install 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. If you plan to install or to allow users to install the one-X Portal Extensions and to use remote telephones, make sure users know that they need to sign out of the one-X Portal Extensions after they sign out of one-X Portal to change their telephone settings.

If a user selects **Specify other** when he or she logs in and does not sign out of the one-X Portal Extensions, the user's business extension continues to be associated with the remote telephone even after the user logs out of one-X Portal.
3. Complete and attach the following checklists, as appropriate for the Administration application and one-X Portal users:
 - [User Worksheet: getting started with one-X Portal](#) on page 105
 - [Avaya one-X Portal and Administration application configuration checklist](#) on page 106
 - [User worksheet: installing one-X Portal Extensions](#) on page 105
4. Distribute the appropriate set of instructions to each group of users and administrators.

User Worksheet: getting started with one-X Portal

This worksheet lists information you need to log into 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 one-X Portal	
Your login ID	
Information for your telephone settings	
Display name to be shown in one-X Portal	
Your telephone extension number	
Password for your extension	
Information for your conferencing settings	
Display name to be shown in 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.d omain.com		The server that hosts 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 one-X Portal. The installer automatically completes this field.
Context Root	/1xp/ portalclient		The location of the one-X Portal software on the 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 one-X Portal Installation Wizard.

#	Task	Internet Explorer	Firefox	Safari
1	Configure the browser to include one-X Portal in the Local Intranet security zone.	Setting the security zone in Internet Explorer on page 108	Not applicable.	Not applicable.
2	Configure all pop-up blockers to allow pop-ups for one-X Portal.	Configuring pop-up blockers on page 107	Configuring pop-up blockers on page 107	Configuring pop-up blockers on page 107
3	Turn off the Script Debugging option for JavaScript errors.	Setting advanced browsing options in Internet Explorer on page 108	Not applicable.	Not applicable.
4	Turn off the Reuse windows for launching shortcuts browsing option.	Setting advanced browsing options in Internet Explorer on page 108	Not applicable.	Not applicable.
5	Enable JavaScript.	Not applicable.	Setting JavaScript options in Firefox on page 109	Configuring Safari on page 110
6	Configure proxy	Not applicable.	Not applicable.	Configuring Safari on page 110
7	For users on Citrix only, disable Download signed ActiveX controls in Internet Explorer.	Configuring Internet Explorer for Citrix access on page 109	Not applicable.	Not applicable.

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 one-X Portal server.

Setting the security zone in Internet Explorer

Updates by Microsoft to Internet Explorer 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 Microsoft.

-
1. In Internet Explorer, select **Tools > Internet Options** .
 2. On the **Security** tab, click **Local intranet**, then click the **Sites** button.
 3. In the Local intranet dialog box:
 - a. Make sure that all options are checked.
 - 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 one-X Portal application.
 - b. Do not check the **Require server verification (https:) for all sites in this zone** option.
 - c. Click **Add**.
 - d. Click **OK**.
 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 the following instructions. 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, select **Tools > Internet Options** .
 2. On the **Advanced tab**, scroll down to the **Browsing** section.

3. Uncheck the following options:

- **Disable Script Debugging (Internet Explorer)**
- **Disable Script Debugging (Other)**
- **Reuse windows for launching shortcuts**

If you do not disable **Reuse windows for launching shortcuts**, Internet Explorer will launch a new Website in the one-X Portal window. You will need to log back in to return to the 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 application on your desktop computer when you log in to one-X Portal. To avoid this issue, you need to disable **Download signed ActiveX controls** in Internet Explorer.

Updates by Microsoft to Internet Explorer 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 Microsoft.

-
1. In your Citrix client, connect to the one-X Portal Internet Explorer session.
 2. In Internet Explorer, select **Tools > Internet Options**.
 3. On the **Security** tab, click **Local intranet**, then click the **Custom Level** button.
 4. In the **ActiveX controls and plug-ins** section, click **Disable** under the **Download signed ActiveX controls** option.
 5. Click **OK**.
 6. In the Local intranet dialog box, click **OK**.
 7. 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. Check **Enable JavaScript**.
 4. Click **Advanced**.
 5. In the Advanced JavaScript Settings dialog box:
 - a. Check all 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. From the menu, select **Safari > Preferences** .
 2. In the Preferences dialog box, click **Security**.
 3. Check **Enable JavaScript**.
 4. Uncheck **Block Pop-up Windows**.
 5. In the **Preferences** dialog box, click **Advanced**.
 6. In the **Proxies** area, click **Change Settings....**
 7. In the Network dialog box, exclude the 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 one-X Portal application to the **Bypass proxy settings for these Hosts & Domains** field to explicitly exclude the 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. Open Internet Explorer.
 2. From the menu, click **Tools > Internet Options**.
 3. On Internet Options window click **Connections** tab **Click LAN Settings**.
 4. On Local Area Network (LAN) Settings window, select **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.
 5. Click **Advanced**.
 6. On Proxy Settings window, type Add 135.*.*.* in the text box labeled **Do not use proxy server for addresses beginning with**.
 7. Click **OK** to save settings.
-

Configuring proxy for Mozilla Firefox

-
1. Open Firefox browser.
 2. From the menu, click **Tools > Options**.
 3. On Options window click **Advanced** option.
 4. Click **Network** tab.
 5. Click **Settings**.
 6. On Connection Settings window, type Add 135.*.*.* in **No Proxy for** text box.
 7. Click **OK** to save proxy settings for Firefox.
-

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 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 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	
Subnet Mask	
Gateway	
Host name	

Property Name	Values
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
Avaya Communication Manager server	
IP Address	
Subnet Mask	
Gateway	
Host name	
DNS domain	
NTP server	
ASA login ID	
Password for ASA login ID	
Avaya Modular Messaging server	
IP Address	
Subnet Mask	
Gateway	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
Avaya Meeting Exchange server	
IP Address	
Subnet Mask	
Gateway	
Host name	
DNS domain	

Property Name	Values
NTP server	
Administrative/root login ID	
Password for login ID	
Avaya Intelligent Presence Server server	
IP Address	
Subnet Mask	
Gateway	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
Active Directory server	
IP Address	
Subnet Mask	
Gateway	
Host name	
DNS domain	
NTP server	
Administrative/root login ID	
Password for login ID	
IBM Domino Directory server	
IP Address	
Subnet Mask	
Gateway	
Host name	
NTP server	
Bind DN ID	

Property Name	Values
Password for Bind DN ID	
Novell eDirectory server	
IP Address	
Subnet Mask	
Gateway	
Host name	
NTP server	
Bind DN ID	
Password for Bind DN ID	
SUN ONE Directory Server	
IP Address	
Subnet Mask	
Gateway	
Host name	
NTP server	
Bind DN ID	
Password for Bind DN ID	
If not hosted on one-X Portal server, Avaya WebLM server	
IP Address	
Subnet Mask	
Gateway	
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 one-X Portal. The information and properties follow the same organization as the Installation Wizard.

Required administrator privileges

To run the one-X Portal Installation Wizard, you must use a Linux account with root user privileges for the machine that will host 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 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 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 one-X Portal database. Avaya one-X Portal requires the Admin username to configure and access the database.

Property Name	Property values		Notes
	Example value	Your value	
			To meet database requirements, this username cannot have more than 8 characters. 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 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 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.

Property Name	Property values		Notes
	Example value	Your value	
Avaya one-X Portal application server configuration			
App Server Username	appsvr		Avaya one-X Portal uses this account to log into and run the 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. 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 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/LicenseServer  Important: AE Services requires a dedicated WebLM. Do not install the one-X Portal license on the Web License Manager used by AE Services.
Microsoft Active Directory configuration			
Active Directory user domain and resource domain			Are users and groups in the same Active Directory

Property Name	Property values		Notes
	Example value	Your value	
			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 domain for security group in the second screen.
Enterprise Directory IP Address	###.###.##.###		IP address of the machine that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the one-X Portal machine 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 EnterpriseDirectory 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 one-X Portal administrative service account.
Enterprise Directory Password			Password for the one-X Portal administrative service account.
For a split domain topology, resource domain: Enterprise Directory IP Address	###.###.##.###		IP address of the machine 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 one-X Portal machine will use to communicate with the Enterprise Directory server.
For a split domain topology, resource domain: Enterprise Directory Domain	<i>users.domain.xyzcorp.com</i>		Fully qualified domain name configured on the EnterpriseDirectory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.
For a split domain topology, resource domain: Enterprise Directory Username	<i>sec_admin_service_user</i>		Enterprise Directory user that you created for the 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 one-X Portal administrative service account.
Admin Group	1XP Administrator s		The Installation Wizard uses the administrator security group to assign permissions to users who will administer one-X Portal in the Administration application.
Audit Group	1XP Auditors		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the one-X Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the one-X Portal

Property Name	Property values		Notes
	Example value	Your value	
			configuration in the Administration application.
User Group	1XP Users		The Installation Wizard uses the user security group to assign permissions to users who will access the one-X Portal application.
Presence Group	1XP Presence		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the one-X Portal application.
IBM Domino Directory configuration			
Enterprise Directory IP Address	###.###.##.###		IP address of the machine that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the one-X Portal machine will use to communicate with the Enterprise Directory server.
Bind DN	CN=username, O=organization		Enterprise Directory user that you created for the one-X Portal administrative service account.
Enterprise Directory Password			Password for the one-X Portal administrative service account.
For a split domain topology, resource domain: Enterprise Directory IP Address	###.###.##.###		IP address of the machine that hosts the Enterprise Directory server.
For a split domain topology, resource domain: Enterprise Directory Port	389		Port that the one-X Portal machine will use to communicate with the Enterprise Directory server.

Property Name	Property values		Notes
	Example value	Your value	
Admin Group	1XP Administrators		The Installation Wizard uses the administrator security group to assign permissions to users who will administer one-X Portal in the Administration application.
Audit Group	1XP Auditors		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the one-X Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the one-X Portal configuration in the Administration application.
User Group	1XP Users		The Installation Wizard uses the user security group to assign permissions to users who will access the one-X Portal application.
Presence Group	1XP Presence		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the one-X Portal application.
Novell eDirectory configuration			
Enterprise Directory IP Address	###.###.##.###		IP address of the machine that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the one-X Portal machine will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	<i>users.domain.xyzcorp.com</i>		Fully qualified domain name configured on the EnterpriseDirectory server.

Property Name	Property values		Notes
	Example value	Your value	
	<i>groups.domain.xyzcorp.com</i>		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 one-X Portal administrative service account.
Enterprise Directory Password			Password for the one-X Portal administrative service account.
Admin Group	1XP Administrators		The Installation Wizard uses the administrator security group to assign permissions to users who will administer one-X Portal in the Administration application.
Audit Group	1XP Auditors		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the one-X Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the one-X Portal configuration in the Administration application.
User Group	1XP Users		The Installation Wizard uses the user security group to assign permissions to users who will access the one-X Portal application.
Presence Group	1XP Presence		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the one-X Portal application.

Property Name	Property values		Notes
	Example value	Your value	
Sun One Directory Server configuration			
Enterprise Directory IP Address	###.###.##.###		IP address of the machine that hosts the Enterprise Directory server.
Enterprise Directory Port	389		Port that the one-X Portal machine 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 EnterpriseDirectory 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 one-X Portal administrative service account.
Enterprise Directory Password			Password for the one-X Portal administrative service account.
Admin Group	1XP Administrators		The Installation Wizard uses the administrator security group to assign permissions to users who will administer one-X Portal in the Administration application.
Audit Group	1XP Auditors		The Installation Wizard uses the auditor security group to assign permissions to users who will have read-only access to the one-X Portal configuration in the Administration application. Members of the auditor security group cannot make

Property Name	Property values		Notes
	Example value	Your value	
			changes to the one-X Portal configuration in the Administration application.
User Group	1XP Users		The Installation Wizard uses the user security group to assign permissions to users who will access the one-X Portal application.
Presence Group	1XP Presence		The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the one-X Portal application.

Installing one-X Portal

Prerequisites

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

- [Environment validation checklist](#) on page 37
- [Server prerequisites checklist](#) on page 39
- [Installation worksheet: information required by Installation Wizard](#) on page 117

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 one-X Portal.
 2. 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: Red Hat Enterprise Linux ES release 4 (Nahant Update 4).

- a. Verify that your response includes the following key items: Red Hat Enterprise ES release 4 Update 4.
- b. If one or more of the key items are not correct, do not install one-X Portal. Update the version of Linux to the correct version first.
3. If the one-X Portal DVD does not mount automatically, execute the following command: `mount /dev/cdrom /media/cdrom`
4. Execute the following commands to change the directory to the `cdrom` folder and launch the Installation Wizard:
 - `cd /media/cdrom`
 - `./setup.bin`
5. Follow the installer prompts and enter the required information from the installation worksheet.

**Note:**

At the end of the installation, the installer may continue to display 100% completed for up to twenty minutes. This screen delay indicates that the installer is completing the final task in the installation. This screen delay does not indicate that the installer has frozen.

Avaya one-X Portal Installation Wizard screens

one-X Portal Installation Wizard

The 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 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 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 one-X Portal installation.
I do not accept the terms of this license agreement	The one-X Portal Installation Wizard exits 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 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 one-X Portal services that you want to install and run on the machine. Installs the selected services and all other one-X Portal components.

one-X Portal installation directory

Name	Description
Directory name	The directory where 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 one-X Portal

Avaya Support uses the Service user accounts to log in to your 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 one-X Portal users

You can allow users to configure their own telephone, messaging, and conferencing accounts in 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 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 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 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 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 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 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 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 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 one-X Portal.



Important:

AE Services requires a dedicated WebLM. Do not install the one-X Portal license on the Web License Manager used by AE Services.

Name	Description
Install WebLM locally	Installs WebLM on the same machine as the one-X Portal server.
Use existing remote WebLM Server	Configures one-X Portal to use an existing WebLM on a remote machine. The 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 one-X Portal to access the license in the WebLM.

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

Enterprise Directory domain for users and security groups

If 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 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 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 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 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	<code>###.###.###.###</code>	IP address of the machine that hosts the Enterprise Directory server.
Enterprise Directory Port	389	Port that the one-X Portal machine will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	<code>users.domain.xyzcorp.com</code>	Fully qualified domain name configured on the EnterpriseDirectory server.

Name	Example value	Description
	<i>groups.domain.xyzcorp.com</i>	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	<i>admin_service_user</i>	Enterprise Directory user that you created for the one-X Portal administrative service account.
Enterprise Directory Password		Password for the 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 one-X Portal in the Administration application.



Note:

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

Name	Example value	Description
Admin Group	1XP Administrators	Security group for 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 one-X Portal configuration in the Administration application. Members of the auditor security group cannot make changes to the one-X Portal configuration in the Administration application.



Note:

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

Name	Example value	Description
Audit Group	1XP Auditors	Security group for 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 one-X Portal application.

 Note:

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

Name	Example value	Description
User Group	1XP Users	Security group for 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 one-X Portal application.

 Note:

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

Name	Example value	Description
Presence Group	1XP Presence	Security group for 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 one-X Portal and do not consume a license for 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 one-X Portal installation

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

Chapter 7: Configuring one-X Portal

Post-installation configuration checklist

You must complete the configuration of these prerequisites after you run the one-X Portal Installation Wizard.

#	Task	Instructions
1	Log into the Administration application.	Logging in to the one-X Portal Administration application on page 138
2	Verify the WebLM configuration.	Verifying the WebLM settings on page 139
3	Install the one-X Portal license in the WebLM.	Installing a one-X Portal license on page 139
4	Analyze the Dial Plan on the switch and add a Dial Plan to one-X Portal.	Dial Plan services on page 141
5	Add a Communication Manager server.	Adding Telephony servers on page 157
6	Add an AE Services server.	Adding Auxiliary servers on page 158
7	Add a Modular Messaging server.	Adding Voice Messaging servers on page 159
8	Optional: install a security certificate for the Modular Messaging connection.	Installing Modular Messaging security certificates on page 160
9	Add a Meeting Exchange conference server.	Adding Conferencing servers on page 161
10	Add a Presence conference server.	Adding Presence servers on page 162
11	Add a Mobility Extension Bank.	Adding Mobility Extension Banks on page 163
12	Optional: add a Contact domain.	Adding Contact Domains on page 164
13	Add a License server.	Configuring License Servers on page 165

#	Task	Instructions
1 4	Configure SNMP Traps.	Configuring SNMP Traps on page 165
1 4	Add an SNMP Destination to define the events for which you want notifications sent and the destinations where you want the notifications to be sent.	Adding SNMP Destinations on page 166
1 6	Restart the one-X Portal.	Restarting one-X Portal on page 166
1 7	Synchronize the Enterprise Directory and Modular Messaging.	Synchronizing the Enterprise Directory and Modular Messaging on page 167
1 8	Analyze the needs of the one-X Portal users, then provision the users.	User administration checklist on page 170

Logging in to the one-X Portal Administration application

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

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

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

2. In the Logon window, type your administrator **Login ID** and **Password**.
 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 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 one-X Portal license

Prerequisites

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



Important:

AE Services requires a dedicated WebLM. Do not install the one-X Portal license on the Web License Manager used by AE 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/LicenseServer`
For example, a valid WebLM address is `http://testbox.xyzcorp.com:
8443/webLM/LicenseServer`
 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: webImadmin

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 one-X Portal and before you create the Voice Messaging server and Conferencing server.

The 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.

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

- Includes one or both of Modular Messaging and Meeting Exchange.
- 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 will 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 username 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 .

Avaya one-X Portal supports the Avaya Communication Manager enhanced EC500 functionality. 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 (Simple, Pattern Matching, or Regular Expression) selected and can be configured to fit the enhanced EC500 number format.



Important:

The Console Privileges for mobility stations should be set to None 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



Tip:

For more information about Dial Plans in Communication Manager, see the *Administrator Guide for Avaya Communication Manager*.

Related topics:

[Dial Plan requirements](#) on page 142

Dial Plan requirements

Required experience

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 one-X Portal. If the Dial Plan configuration in both the switch and one-X Portal do not match, telephone calls will not be delivered to the correct recipients.

Required configuration in one-X Portal

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 to one-X Portal. The Pattern Matching transformation and the Regular Expression transformation are mutually exclusive. You cannot use both of them for the same Dial Plan.

Simple Dial Plan transformation

All dial plans configured in 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 dial dialing the number in the switch. For example, in the United States many users know to 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 this 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, one-X Portal only uses the Simple Dial Plan transformation if the other transformation could not transform the input into valid output.

How the Simple Dial Plan transformation works

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 and 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 143

[Example: Simple Dial Plan transformation](#) on page 143

Recommended uses for the Simple Dial Plan transformation

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

When to configure the Simple Dial Plan transformation only

Avaya recommends that you use only the Simple Dial Plan transformation for the following types of 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.
- The deployment is not required to support inter-switch dialing.

When to configure the Simple Dial Plan transformation with another transformation

Avaya recommends that you also configure 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 the way that a Simple Dial Plan transformation uses the Dial Plan configuration to ensure that telephone numbers dialed in one-X Portal go the correct destination.

Dial Plan configuration

Parameter	Value
Main switch number	15553335000
Outside line access code	9
Local Region Prepend	555
Inter-region prepend	1
International prepend	011
National call length	10
Local call length	7

Parameter	Value
Extension length	5

Transformations performed by the Simple Dial Plan transformation

This 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
+15553330000	95553330000
+15087641234	915087641234
+551151856200	9011551151856200

Pattern Matching transformation

The Pattern Matching transformation is very similar to the algorithm used by Communication Manager. The pattern matching rules are evaluated in the order they specified in the user interface, and the transformation rule that will be used is the first rule to match the input.

How the Pattern Matching transformation works

This transformation attempts to match 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 transformation deletes the specified number of characters, and inserts the configured set of characters.

Related topics:

[Recommended uses for the Pattern Matching transformation](#) on page 145

[Example: Pattern Matching transformation](#) on page 145

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 one-X Portal implementation:

- 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

Avaya does not recommend that you use this 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 be able to match the possible patterns in the telephone numbers.

In the above situations, Avaya recommends that you use the Regular Expression transformation.

Example: Pattern Matching transformation

This example describes the way that a Pattern Matching transformation matches patterns to ensure that telephone numbers dialed in one-X Portal go 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

Starts with	Minimum length	Maximum length	Delete	Prepend	Description
+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	35111
+15553310000	93310000
+15087641234	915087641234
+551155551234	9011551155551234
915552225555	915552225555

Regular Expression transformation

The Regular Expression transformation is the most flexible transformation. However, this transformation is also the most difficult to configure.

How the Regular Expression transformation works

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.

Related topics:

[Recommended uses for the Regular Expression transformation](#) on page 147

[Example: Regular Expression transformation](#) on page 147

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 one-X Portal implementation:

- 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 be able to match the possible patterns in the telephone numbers.

When not to use the Regular Expression transformation

Avaya does not recommend that you use this transformation:

- 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 be able to match the possible patterns in the telephone numbers.

Example: Regular Expression transformation

This example describes the way that a Regular Expression transformation matches patterns and regular expressions to ensure that telephone numbers dialed in one-X Portal go 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
\+55(\d{2,2}[89]\d{7,7})	9101045855\$1	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

Pattern	Replacement	Explanation
\+(\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	35111
+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 one-X Portal, you must gather information and determine what you need to support the Dial Plan in the switch.

1. Consult the switch administrator and obtain the following information:
 - All information required by the Dial Plan worksheet in the *Avaya one-X Portal Implementation Workbook*.
 - 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 received 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 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. Put the E. 164 rules in order from the most specific to the most general, and eliminate any duplicate rules.
 - f. Put 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 your rules 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. 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 149

Example: creating rules for a Dial Plan

This example goes through the tasks involved in step 2 of [Creating rules for a Dial Plan](#) on page 148. This step requires you to analyze the information that you received about the Dial Plan in the switch and create the rules for the Dial Plan.

This example creates the rules for a Pattern Matching transformation.

E. 164 formats for the expected inputs

The enterprise directory uses these formats to store telephone numbers.

Expected number input	Description
+15553375247	Local extension
+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

Expected number input	Description
+551151856280	International telephone number

Expected numbers received by one-X Portal from the network

The switch sends these numbers to display on the user extension and in 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
+1555337524 7	Local extension	75247	Starts with: +1555337 Minimum length: 12 Maximum length: 12 Delete length: 7
+1222852365 7	Number in second location of switch network	23657	Starts with: +1222852 Minimum length: 12 Maximum length: 12 Delete length: 7
+1555334123 4	Local number	915553341234	Starts with: +1555 Minimum length: 12 Maximum length: 12 Delete length: 1 Insert length: 9
5553341234	Personal active directory number that is not formatted using the E.164 format	915553341234	Starts with: <i><blank></i> Minimum length: 10 Maximum length: 10 Delete length: 0 Insert length: 91

Expected number input	Description	Expected Output	Rule
+14447641234	Domestic long distance telephone number	914447641234	Starts with: +1 Minimum length: 12 Maximum length: 12 Delete length: 1 Insert length: 9
+551151856280	International telephone number	0911551151856280	Starts with: + Minimum length: 10 Maximum length: 15 Delete length: 1 Insert length: 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 Insert length: +155533
23657	Call from number in second location of switch network	+12228523657	Starts with: 2 Minimum length: 5 Maximum length: 5 Delete: 7 Insert length: +122285
5553341234	Call from local number	+15553341234	Starts with: 555 Minimum length: 10 Maximum length: 10 Delete: 0 Insert length: +1
4447641234	Call from domestic long distance telephone number	+14447641234	Starts with: <i><blank></i> Minimum length: 10 Maximum length: 10 Delete: 0 Insert length: +1
551151856280	Call from international telephone number. This number can	+551151856280	Starts with: <i><blank></i> Minimum length: 11 Maximum length: 15 Delete: 0 Insert length: +

Number from network	Description	Expected Output	Rule
	vary significantly.		

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.
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	3

Expected number input	Description	Expected Output	Rule	#
			Insert length: 91	
+14447641234	Domestic long distance telephone number	914447641234	Starts with: +1 Minimum length: 12 Maximum length: 12 Delete length: 1 Insert length: 9	4
+551151856280	International telephone number	0911551151856280	Starts with: + Minimum length: 10 Maximum length: 15 Delete length: 1 Insert length: 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 Insert length: +155533	1
23657	Call from number in second location of switch network	12228523657	Starts with: 2 Minimum length: 5 Maximum length: 5 Delete: 7	2

Number from network	Description	Expected Output	Rule	#
			Insert length: +122285	
	Call from local number			Duplicate rule. Deleted.
4447641234	Call from domestic long distance telephone number	+14447641234	Starts with: <i><blank></i> Minimum length: 10 Maximum length: 10 Delete: 0 Insert length: +1	3
551151856280	Call from international telephone number. This number can vary significantly.	+551151856280	Starts with: <i><blank></i> Minimum length: 11 Maximum length: 15 Delete: 0 Insert length: +	4

Adding Dial Plans

1. Select the **Servers** tab.
2. From the left pane, select **Dial Plan**.
3. On the Dial Plans page, click on **Add New Dial Plan** to display the Add New Dial Plan page where you add the Simple Dial Plan Transformation.
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 155 after you complete these steps.
4. 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 191.
5. In the **Dial Plan Transformation** section of the page, you can transform a phone number to display the **Dialable**, **Network**, and **Normalized** numbers from this dial plan to determine if the dial plan is correctly configured.

- Dialable - displays how the dial plan will convert a dialed number to a dialed string to a PBX.
 - Network - displays how the dial plan will convert a number to a string for Mobility.
 - Normalized - displays how the dial plan will convert an ANI to display on the one-X Portal client.
- a. In the **Number to Transform** field, enter the phone number.
 - b. Click **Transformation** to display the **Dialable**, **Network**, and **Normalized** numbers for that number in the dial plan number.
The results of the transformation (successful, unsuccessful) are displayed for each of these numbers. If unsuccessful, the message indicates the problem. Make the appropriate changes and try again.
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, if this is a new object the default values.
 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. The Dial Plans page displays a list of the Dial Plans installed on the system.
4. Click on the name of a Dial Plan in the **Handle** field to display the Modify Dial Plan page for the Dial Plan.
5. Modify the **Dial Plan** described on [Dial Plan field descriptions](#) on page 191 if desired.
6. Add Conversion Rules.
The Conversion Rules table is divided into 2 sections: E.164 (outbound calls) and Network (inbound calls). Select the desired algorithm **Pattern Match** or **Regular Expression**.
7. For the **Pattern Match** algorithm, complete the following fields:
 - a. Check **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, etc. When you save the dial plan, the order is displayed in increments of 5, 1 becomes 5, 2 becomes 10, etc.

- 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 **Pattern Match**, enter the pattern of the algorithm to match to the **Regional Prefix**. For example, if the value of **Regional Prefix** is 978, you may want to enter +1978.
 - f. In **Delete Length**, enter the number of digits to delete from the beginning of the phone number.
 - g. In **Replacement**, enter any numbers you want to append to the beginning of the phone number.
8. For the **Regular Expression** algorithm, complete the following fields:
- a. Check **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, etc. When you save the dial plan, the order is displayed in increments of 5, 1 becomes 5, 2 becomes 10, etc.
 - c. In **Regular Expression**, enter the Regular Expression pattern that applies to the phone number.
 - d. In **Replacement**, 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.
9. To delete Conversion Rules from Existing Rules in the appropriate section, check **Delete**, for the existing conversion rule.
10. In the **Dial Plan Transformation** section of the page, you can transform a phone number to display its **Dialable**, **Network**, and **Normalized** numbers from this dial plan to determine if these changes are correctly configured.
- Dialable - displays how the dial plan will convert a dialed number to a dialed string to a PBX.
 - Network - displays how the dial plan will convert a number to a string for Mobility.
 - Normalized - displays how the dial plan will convert an ANI to display on the one-X Portal client.
- a. In the **Number to Transform** field, enter the phone number.
 - b. Click **Transformation** to display the **Dialable**, **Network**, and **Normalized** numbers for that number in the dial plan number.
The results of the transformation (successful, unsuccessful) are displayed for each of these numbers. If unsuccessful, the message indicates the problem. Make the appropriate changes and try again.
11. 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.

12. Click **Save** to update the **Dial Plan**.
 13. Click **Reset** to restore the settings to the last saved page or, if this is a new object the default values.
 14. Click **Cancel** to exit the page without making any changes.
-

Configuring one-X Portal servers

Telephony servers

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

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

Related topics:

[Adding Telephony servers](#) on page 157

[Adding Auxiliary servers](#) on page 158

Adding 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 on **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 183.
 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 will use 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. Click **OK** to add the server.
 8. 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:

The test will only be successful if the TSAPI.PRO file had the AE Services server IP address when the Telephony adapter started. If this is a new AE Services server, there may be some errors saying that the AE Services server was not found, and check the TSAPI.PRO file. If you get this error, save that the Auxiliary Server configuration (as this will cause the AE Services server IP Address to be saved in the TSAPI.PRO file), restart the Telephony adapter (so it can read the new TSAPI.PRO file), and run the test after the Telephony adapter is back up.

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

Adding 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 on **Add** to display the Add Auxiliary Server Configuration page.
 5. Enter the appropriate information and click to add the server.
- For more information on the fields, see [Auxiliary server \(AE Services\) field descriptions](#) on page 184.

6. After you add the new AE Services server, you must restart 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 **Restore** to restore the settings to the last saved page or, if this is a new object, the default values.
 9. Click **Exit** to exit the page without making any changes.
-

Voice Messaging servers

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

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

This section describes how to configure Modular Messaging servers for one-X Portal and its users.

Related topics:

[Adding Voice Messaging servers](#) on page 159

[Installing Modular Messaging security certificates](#) on page 160

Adding 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 186.
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, if this is a new object, the default values.
 8. Click **Cancel** to exit the page without making any changes.
-

Installing Modular Messaging security certificates

To secure communication between one-X Portal and Modular Messaging, server certificates must be configured to secure the Java mail API which is used for the IMAP connection to Modular Messaging. These certificates are used to establish a trust relationship between one-X Portal and Modular Messaging.

Modular Messaging security certificates are installed 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**.
 3. The Voice Messaging page displays a list of the Modular Messaging servers installed on the system.
 4. Click on the name of a Modular Messaging server in the field to display the Modify Voice Messaging Server Configuration page for the server.
 5. Retrieve the security certificate in the **SSL Certificate** field if necessary and click to update the server. For more information on the fields, see [Voice Messaging server field descriptions](#) on page 186



Note:

You must restart the server to save your changes. For more information, see [Monitoring Voice Messaging services](#)

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

Conferencing services

Meeting Exchange servers on one-X Portal provide bridge conferencing capabilities such as creation of on-demand conferences, conference control for conferences in session, and setting up one time conferences or recurring schedules of conferences.

The Meeting Exchange servers communicate with the other one-X Portal servers to provide these capabilities.

This section describes how to configure Meeting Exchange servers for one-X Portal and its users.

Related topics:

[Adding Conferencing servers](#) on page 161

Adding Conferencing servers

-
1. Select the **Servers** tab.
 2. From the left pane, select **Conferencing**.
 3. The **Conferencing** page displays a list of the servers on the system.
 4. In the **Server Type** field, select the version number of the Meeting Exchange server installed on the system.
 5. Click **Add** to display the Add Conferencing Server Configuration page.
 6. Enter the appropriate information and click **OK** to add the server.
For more information on the fields, see [Conferencing server field descriptions](#) on page 189.
 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 **Reset** to restore the settings to the last saved page or, if this is a new page, the default values.
 9. Click **Cancel** to exit the page without making any changes.
-

Presence service

The Avaya Intelligent Presence Server provides presence information that indicates the availability of a one-X Portal user.

The Avaya Intelligent Presence Server server stores the user's personal availability record (also known as presentity) on one-X Portal and makes it available to other users (watchers) to convey the user's availability for communication.

This section describes how to configure the Avaya Intelligent Presence Server server for one-X Portal and its users.

Related topics:

[Adding Presence servers](#) on page 162

Adding Presence servers

-
1. Select the **Servers** tab.
 2. From the left pane, select **Presence**.
 3. On the Presence Configuration page, in the **Server Type** field, select **apas 1.0**, which is the version number of the Avaya Intelligent Presence Server server installed on the system.
 4. Click **Add** to display the Add Presence Server Configuration page.
 5. Enter the appropriate information and click **OK** to add the server.
For more information on the fields, see [Presence server field descriptions](#) on page 190.
 6. Click **Reset** to restore the settings to the last saved page or, if this is a new page, the default values.
 7. Click **Cancel** to exit the page without making any changes.
-

Mobility Extension Banks

A Mobility Extension Bank on one-X Portal associates extension numbers with the Telephony servers configured on 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.

The mobility extensions are a set of worker stations on the switch. These stations are not user extensions and should be created for use by one-X Portal only. Mobility stations need to be mapped via CM Network Region mapping, or native CLAN Network Region to a region that supports G711. Avaya one-X Portal uses the mobility extensions to dial feature access on the switch.

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

Avaya one-X Portal supports up to 600 requests per hour per user. 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 163

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 192.
 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 one-X Portal with the Active Directory. Users must exist in the Enterprise Directory before they can be provisioned as users on one-X Portal.

An 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 3 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 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 one-X Portal users communicate. This information includes contact names, phone numbers, etc. The User domain is delivered with contacts. You can add Contact domains to 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 has acquired another company, you may want to access the contact information for the other company in a new Contact domain.

Related topics:

[Adding Contact Domains](#) on page 164

Adding Contact Domains

-
1. Select the **System** tab.
 2. From the left pane, select **Enterprise Directory**.
 3. The Enterprise Directory Domains page displays a list of the domains on the system.
 4. Click on **Add Contact Domain** to display the Add Enterprise Contact Domain page.
 5. Enter the appropriate information and click **OK** to add the domain.
For more information on the fields, see [Enterprise Directory field descriptions](#) on page 195.
 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.
-

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 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 License Servers](#) on page 165

Configuring License Servers

-
1. Select the **System** tab.
 2. From 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 197.
 4. Click **Reset** to display the settings from the start of this session.
-

SNMP Traps

SNMP Traps are notifications that are sent to specified destinations on one-X Portal when certain events take place. The SNMP Traps option enables you to define both the events for which you want notifications sent and the destinations where you want the notifications to be sent.

Related topics:

[Configuring SNMP Traps](#) on page 165

[SNMP Destinations](#) on page 166

[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.

- Click 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 (event notifications). On 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. This option enables you to define specified destinations when certain events take place on 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 on **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 198.
 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 one-X Portal

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

To restart the one-X Portal server:

-
1. Login with the Application server username created during the one-X Portal installation. For example, the default username is `appsrvr`.
 2. Execute 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` where `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. Execute 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**, you do not have access to this page.

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 Synchronozation**.
 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

The users of one-X Portal must reside in the Enterprise Directory. The administrator of the Enterprise Directory enables these users for one-X Portal by placing them in the one-X Portal user group in the Enterprise Directory.

Unprovisioned users

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

Provisioned users

Provisioned users are users that are assigned to the one-X Portal user group or the Presence user group. Each user group is associated with an application inside one-X Portal. Therefore, users in the one-X Portal user group are associated with the one-X Portal Application, and the users in the Presence user group are associated with the Presence application. Same users can exist in two or more applications. Users associated with the Presence application are always enabled for Presence (no explicit enabling is required). Presence only users do not consume any one-X Portal licenses and are provisioned using the CLI. Users associated with the one-X Portal application need to be explicitly enabled for one-X Portal, and a single one-X Portal license is consumed for each user enabled for one-X Portal. Only users enabled for the one-X Portal application can login to the one-X Portal Client. Users in the Presence application can have telephony resources provisioned, and these resources will be used by the IPS for reporting telephony Presence.

User Administration options

Depending upon the needs of a 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 one-X Portal user individually.

User analysis

Each user administration option performs a different purpose. Before you provision and administer the 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 one-X Portal system.

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

- **Continuous extension monitoring**
- **Telecommuter**
- **VOIP**
- **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**
- **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 can be applied to other users. Use Prototype Users as templates to speed up configuration and provisioning of users who have the same 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 one-X Portal users.

#	Task	Instructions	✓
1	Analyze the needs of 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 172	
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	

#	Task	Instructions	✓
5	Provision the one-X Portal users. You apply profiles and prototype users during this step.	Provisioning a portal user on page 177	

System Profile

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

- **Continuous extension monitoring**
- **Telecommuter**
- **VOIP**
- **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 to 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 172

Modifying the System Profile

1. Select the **Users** tab.
2. From the left pane, select **System Profile**.
3. On the System Profile page, change the values of the following profile properties as needed.

You can accept the system default value or set a new system value. You can also force the value of the property to any Group Profiles that use this property.

Options	Description
Property	Settings
Continuous extension monitoring	Select Enabled , to monitor the extension of the user whether the user is logged in to one-X Portal or not. Provides call information like missed calls to the user.
Telecommuter	Select Enabled to turn on the Telecommuter functionality on one-X Portal.
VoIP	Select Enabled to turn on Voice over IP on one-X Portal.
Mobility	Select Enabled to turn on the Mobility functionality on one-X Portal.
Forward voice messages to inbox	Select Enabled to forward the voice messages received by a user on one-X Portal to the email inbox of the user.
Save to voice messages file	Select Enabled to save the voice messages received by a user on 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 one-X Portal. Enter a value between 1 and 200 entries.
Maximum number of history records	Specify the maximum number of records to archive on one-X Portal. Enter a value between 1 and 400 entries.
Maximum days to keep history	Specify the maximum number of days to keep these records in archive on one-X Portal. Enter a value between 1 and 14 days.

Options	Description
Maximum number of favorites	Specify the maximum number of favorites a one-X Portal user can keep on their Portal Client application. Enter a value between 1 and 5000 entries.
Usage Disclaimer	Select Enabled to turn on the Usage Disclaimer on one-X Portal.
Usage Disclaimer URL	Specify the URL for the Usage Disclaimer on one-X Portal. The default value is usage.jsp .
Feedback email address	Specify the email address for the user to provide feedback to the one-X Portal administrator.
Default Access Type	Specify one of the following access types. This value is used when the user (presencee) 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 will 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.

- Click **Save** to save these settings to the profile.
- Click **Reset** to display the settings from the start of this session.

Group Profiles

A Group Profile is a collection of the following properties that are applied to users who are members of the group.

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

- **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. Group Profiles inherit values from the System Profiles level when the values are set as "forced" from the System level. Forced values are system level values that cannot be changed at the lower Group Profile or the User Profile levels. If the values are not forced from the System level, Group Profiles can elect to accept the System level value 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 on **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 system 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 field**
 - **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 can be applied to other users. Use Prototype Users as templates to speed up configuration and provisioning of users who have the same settings.

Prototype Users are used for provisioning users only. Their resources that are copied to the user. Once the user is provisioned, the user has no reference to the Prototype User. Changes to the Prototype User have no impact on the users provisioned from 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 176

[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 and add resources to the Prototype User.
 - a. To add a **Telephony** resource, perform the steps in [Assigning a Telephony resource to a Prototype User](#) on page 176
 - b. To add a **Messaging** resource, perform the steps in [Assigning a Voice Messaging resource to a Prototype User](#) on page 176
 - c. To add a **Conferencing** resource, perform the steps in [Assigning a Conferencing resource to a Prototype User](#) on page 177
 - d. To add a **Presence** resource, perform the steps in [Assigning a Presence resource to a user](#) on page 181
 7. Click **Finished** to save the Prototype User.
 8. Click **Delete** to remove the Prototype User.
-

Assigning a Telephony resource to a Prototype User

-
1. Select the **Users** tab.
 2. In the left navigation 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 will see in the 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 will see in the 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 Meeting Exchange server.
 - b. In the **Display Name** field, type a descriptive name for this resource which users will see in the 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. Check **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 one-X Portal.

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**.

3. The Unprovisioned Users page lets you search for unprovisioned users on the system.
4. If you know the user ID of the unprovisioned user, in the **Direct To Enterprise Directory** section, you can enter the user ID and click **Provision** to provision that user.
5. 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 who's 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.
6. Click **Provision** in the row of the user you wish to provision.
7. At the Provision User page, assign the Group Profile and Prototype User (if any) to the user.
8. Check **Enable**.
9. Click **Save**.

Related topics:

[Assigning a Telephony resource to a user](#) on page 178

[Assigning a Voice Messaging resource to a user](#) on page 179

[Assigning a Conferencing resource to a user](#) on page 180

[Assigning a Presence resource to a user](#) on page 181

Assigning a Telephony resource to a user

You can also use the Administration Command Line Interface to assign resources to users on 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. 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 one-X Portal.
 - c. In the **Display Address** field, type the text to display in the 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.
 10. After making changes to all of the user's 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 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, type a descriptive name for this resource which users will see in the one-X Portal.
 - c. In the **Display Address** field, type the text to display in the one-X Portal for this mailbox.
 - d. In the **Mailbox** field, type the mailbox assigned to the user.
 - e. In the **Password** field, type the password for the mailbox.
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.
 10. After making changes to all of the user's 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 one-X Portal. Users do not have permissions to add or delete conferencing resources in their one-X Portal settings. Users can only update an existing conferencing resource.

You can also use the Administration Command Line Interface to assign resources to users on 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 Meeting Exchange server.
 - b. In the **Display Name** field, type a descriptive name for the resource that users will see in the one-X Portal.
 - c. In the **Display Address** field, type the text to display in the one-X Portal for this conferencing account.
 - d. In the **Moderator Code** field, type the host code assigned to the account.

- e. In the **Participant Code** field, type the participant code assigned to the account.
 - f. In the **PIN Code** field, type 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 will not be 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, type the telephone number that the user dials to log in to the bridge.
 - h. In the **Bridge Number Backup** field, type the secondary telephone number that the user can dial to log in to the bridge.
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.
 10. After making changes to all of the user's resources, 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 one-X Portal.

You can also use the Administration Command Line Interface to assign resources to users on 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, type a descriptive name for the resource that users will see in the one-X Portal.

- c. In the **Display Address** field, type the text to display in the one-X Portal for this presence account.
 - d. Leave the **SES ID**, **Password**, and **Confirm** fields unchanged as they are not significant for this task and version of one-X Portal.
6. Click **OK** to assign the server to the user.
 7. Click **Reset** to refresh the screen and start over.
 8. Click **Cancel** to revert to View User window without saving the edits.
 9. After making changes to all of the user's resources, click **Finished**.
-

Configuring one-X Portal for SSL authentication (optional)

You do not need to use SSL authentication if users will only access one-X Portal inside the corporate firewall.

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 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 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.
-

Administration Application interface

Servers field descriptions

- [Telephony server field descriptions](#) on page 183
- [Auxiliary server \(AE Services\) field descriptions](#) on page 184
- [Voice Messaging server field descriptions](#) on page 186
- [Conferencing server field descriptions](#) on page 189
- [Dial Plan field descriptions](#) on page 191
- [Mobility Extension Bank field descriptions](#) on page 192

Telephony server field descriptions

The Telephony server configuration page displays the following fields:

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. For Communication Manager, displays 3.1, 4.0, and 5.0.
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 checked 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 using the proper case in the name.
EC500 Enable Code	The feature access code used by Telephony server to enable Extension to Cellular on one-X Portal, for example, *88, *89, *87. Contact the local Communication Manager administrator to get the code configured on the system.
EC500 Disable Code	The feature access code used by Telephony server to enable Extension to Cellular on 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 Telephony server to enable Extension to Cellular on one-X Portal, for example, *88, *89, *87.

Name	Description
	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 1XP requires CM 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 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 is used on Add/Create pages to save the new resource. Save is used on Modify pages to save 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 one-X Portal.
Test	Runs a test of the new or updated server settings and returns the results immediately. If errors are returned, you can make the necessary corrections.

Auxiliary server (AE Services) field descriptions

The Auxiliary Server configuration page displays the following fields for AE Services configuration:

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 4.1. If using AES 4.1 or 4.2, the behavior of the server will be the same, and should be configured as AES 4.1.
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 checked 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.
DMCC Port	The port number used by the DMCC configuration for the AE Services server.
DMCC Login ID	The login 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 DMCC .
DMCC Password	The password associated with the login 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 Confirm	Verification of the password associated with the login 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.
TSAPI Port	The port number used by the TSAPI configuration for the AE Services server.
TSAPI Login ID	The login 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 login ID used by the TSAPI configuration for the AE Services server.

Name	Description
	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 login ID used by the TSAPI configuration for the AE Services server.
OK or Save	OK is used on Add/Create pages to save the new resource. Save is used on Modify pages to save 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 one-X Portal.
Test	Runs a test of the new or updated server settings and returns the results immediately. If errors are returned, you can make the necessary corrections.

Voice Messaging server field descriptions

The Voice Messaging configuration page displays the following fields:

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 3.1.
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 checked by the administrator, enables the server for the system.
Initial Number of Server Connections	The minimum number of one-X Portal user connections needed to communicate with the Voice Messaging server (the MSS of the Modular Messaging server).
Max Number of Server Connections	The maximum number of 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 the 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.

Name	Description
Messages Temp Directory	The location of the temporary directory where sections of voice mail message are stored. When creating a new Voice Messaging server, leave this field empty because one-X Portal automatically creates a new directory named msgworkdirectory with the correct permissions for all new Voice Messaging servers.
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.
IMAP Login ID	The secure login 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 login 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 login ID used by the IMAP configuration for the Modular Messaging server.
IMAP Secure Port	Check this option. 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.

Name	Description
SMTP Login ID	The secure login 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 login 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 login ID used by the SMTP configuration for the Modular Messaging server.
SMTP Secure Port	If checked, 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 non-secure port.
LDAP Login ID	The login 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 login 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 login ID used by the LDAP configuration for the Modular Messaging server.
LDAP Secure Port	Do not check this field. one-X Portal does not support a secure LDAP connection for the Voice Messaging server.
OK or Save	OK is used on Add/Create pages to save the new resource. Save is used on Modify pages to save 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 one-X Portal.

Name	Description
Test	Runs a test of the new or updated server settings and returns the results immediately. If errors are returned, you can make the necessary corrections.

Conferencing server field descriptions

The Conferencing Server configuration page displays the following fields:

Name	Description
Type	The type of server configured on the system. For Meeting Exchange, displays MX.
Version	The version of the server configured on the system. For Meeting Exchange, displays 4.0.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the Meeting Exchange server.
Enabled	When checked 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.
Dial Plan	The handle of the Dial Plan used by this server.
BCAPI Host	The network address used by the BCAPI configuration for the Meeting Exchange server as an IP address or a DNS address.
BCAPI Login ID	The login ID used by the BCAPI configuration for the Meeting Exchange server. The number of characters in this entry must not exceed the character length limitation in BCAPI .
BCAPI Password	The password associated with the login ID used by the BCAPI configuration for the Meeting Exchange 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 login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Secondary Login ID	The Secondary Login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Password	The password associated with the Secondary Login ID used by the BCAPI configuration for the Meeting Exchange server.
BCAPI Confirm	Verification of the password associated with the secondary login ID used by the BCAPI configuration for the Meeting Exchange server.
OK or Save	OK is used on Add/Create pages to save the new resource. Save is used on Modify pages to save updates to the resource.

Name	Description
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 one-X Portal.
Test	Runs a test of the new or updated server settings and returns the results immediately. If errors are returned, you can make the necessary corrections.

Presence server field descriptions

The Presence Configuration page displays the following fields:

Name	Description
Type	The type of server configured on the system. For the Avaya Intelligent Presence Server, displays apas.
Version	The version of the server configured on the system. For the Avaya Intelligent Presence Server , 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 Avaya Intelligent Presence Server.
Enabled	When checked by the administrator, enables the server for the system.
IPS Publish To Port	The port number on the Avaya Intelligent Presence Server to which the presence information of the user is published.
LPS Consumer Port	The port number on the Avaya Intelligent Presence Server where the consumer information is received.
LPS Supplier Port	The port number on the Avaya Intelligent Presence Server from which the published information is furnished.
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 login ID used by this configuration of the User Management Service.

Name	Description
UMS Password	The password associated with the login ID used by this configuration for the User Management Service.
UMS Confirm	Verification of the password associated with the login ID used by this configuration for the User Management Service.
OK or Save	OK is used on Add/Create pages to save the new resource. Save is used on Modify pages to save 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 one-X Portal.

Dial Plan field descriptions

The Dial Plan configuration page displays the following fields:

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.
Phone Numbers Automatic Routing Service	The digit to dial before an outbound phone number to get the call out of 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 dial 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 phone call placed within the country. For example, if the phone number is 508-852-0010, the value is 10.
Number of Digits Local Call	The maximum number of digits allowed in a phone call placed within the area code. For example, if the phone number is 508-852-0010, the value is 10.

Name	Description
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 is used on Add/Create pages to save the new resource. Save is used on Modify pages to save 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 one-X Portal.
Test	Runs a test of the new or updated server settings and returns the results immediately. If errors are returned, you can make the necessary corrections.

Mobility Extension Bank field descriptions

The Extension Bank Configuration page displays the following fields:

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. 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. Check Delete next to the extension 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.

Name	Description
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 one-X Portal.

Scheduler field descriptions

The one-X Portal Scheduler displays the following fields for each of the tasks.

Name	Description
Enabled	Enables scheduling of this when checked.
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.
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 (Saturday, Sunday, etc.) 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.

Name	Description
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.
Run Now	Runs the task immediately to incorporate recent changes. This button allows the task to be run one time per change. <i>Note: some tasks, such as Database Backup and Directory Server Synchronization, affect the operation of the system.</i>
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. The Task Status fields display a list of previous schedule runs to provide a 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 previous runs are no longer displayed. You must leave the Scheduler page to update the status of the run. At the conclusion of the run, a success or failure message is displayed.

System field descriptions

Related topics:

- [General Settings field descriptions](#) on page 194
- [Enterprise Directory field descriptions](#) on page 195
- [License server field descriptions](#) on page 197
- [SNMP Traps field descriptions](#) on page 198
- [SNMP Destinations field descriptions](#) on page 198
- [Statistics field descriptions](#) on page 200
- [Logging field descriptions](#) on page 200
- [JDBC field descriptions](#) on page 205

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 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 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 <code><NNNNN>.xyz-corp.com</code> , and the Resource domain as <code><nnnn>pptdomain.xyz-corp.com</code> . The Contact domain is the same as the User domain. You can add Contact domains 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 one-X Portal users. There is only one user domain. You cannot change this domain. • Resource: indicates the domain contains the 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 login ID used by the server.
Password	The password associated with the Login ID used by the server.
Confirm	Re-enter 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.
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 1 and the domain name, type, etc., 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.
Base DN	The Distinguished Name (DN) used by the LDAP server.
Login ID	The login ID used by the server.
Password	The password associated with the Login ID used by the server.

Name	Description
Confirm	Re-enter 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.
Range Size	The number of names returned by the Enterprise Directory server per query.
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 checked, 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.

Name	Description
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, 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.
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. Check the check box next to the SNMP Trap to enable that trap only.
Uncheck All	Selects all of the SNMP Traps and disables them. Check the check box next to the SNMP Trap to disable that trap only.

SNMP Destinations field descriptions

The SNMP Destinations configuration page displays the following fields:

Name	Description
Handle	The unique name assigned to the server by the administrator.
Enable	When checked, enables the configuration of the SNMP trap.

Name	Description
Device	The device to which traps are generated. Selections are: • SSG - Avaya Services Security Gateway. Only INADS traps are sent here. • NMS - industry standard Network Monitoring Software such as HP Openview or IBM Triboli. INADS traps are not sent here.
Host	The IP Address of the Device that will receive the traps.
Port	The TCP/UCP port number used when sending the traps.
Notification Type	Indicates the method of notification for this destination. 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. Selections are version 1, 2c, or 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. Selections are: • None - the authentication and privacy fields are not used. • 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. Select from None, MD5, or SHA.
Authentication Password	Indicates the Authentication password for authenticated SNMP version 3 messages.
Confirm	Re-enter 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..

Name	Description
Privacy Password	Indicates the Privacy password for encrypted SNMP version 3 messages.
Confirm	Re-enter 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	When checked, enables the system to collect the specified statistics, Performance and/or Usage.
Collection Interval	Specifies how often, in minutes, the system will collect the specified statistics. Select from 1 to 240 minutes.
Retention Period	Specifies how long, in days, the system will keep 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	one-X Portal logging that provides high level system information. Generally, the logs are written to SystemOut.log, and also to trace.log if any of the Protocol, Aspect, and/or Other Loggers is enabled.
Level	The level of General Logging logging to run.

Name	Description
	Selections are All , Fatal , Error , or Warning .
Protocol Logging	Low level logging used to debug issues with the protocols used by one-X Portal. It generates messages for debugging protocol exchanges. For example, SMTP or SIP. The logs are written 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. Selections are Summary or Traffic (detailed).
List of Current Protocol Loggers	The Protocol Level logger. • api: Debugs general client issues. The client API uses this protocol in one-X Portal. • bcapi: Debugs conferencing issues. Conferencing services use this protocol to connect to Meeting Exchange. • cmapi: Debugs Telephony issues. For example, Other Phone log in problems and EC500 issues. • cmcontact: Reports posting of contact log. Telephony services use this protocol to report posting of contact log information to Contact Logger service. • 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 • vfwclient: 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 Avaya Communication Manager. Telephony services use this as one of the protocols to connect to Avaya Communication Manager. Use this to resolve Telephony issues. • ips: Debugs Presence issues. Presence service uses this protocol to connect to the Avaya Intelligent Presence Server. • snmp: Used by Alarm service to issue SNMP notifications.

Name	Description
	• spectel: Debugs Conferencing issues. Conferencing services use this as one of the protocols to connect to Meeting Exchange. • webim: Debugs licensing issues. The one-X Portal uses this protocol to connect to the licensing services
Aspect Logging	Low level logging used to debug issues with the one-X Portal components. It generates messages for debugging subsystem activity. For example Telephony or Conferencing. This can be enabled for specific Users in the system. The logs are written 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 .
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 aspect loggers that are available for use 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 WebSphere profile's logs directory. • 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 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 no user is specified, this will log information about the service. If a user is specified, this will log information about the user's 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.

Name	Description
	• fwadmin: Logs Service Framework application 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 (request/response) to/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. • mmsystem: Logs activities (request/response) to/from Modular Messaging (voice messaging) service over system channel. • mxclient: Logs activities (request/response) to/from Meeting Exchange (bridge conferencing) service over client channel. • mxservice: Logs activities on Meeting Exchange (bridge conferencing) service. • mxsystem: Logs activities (request/response) to/from Meeting Exchange (bridge conferencing) service over system channel. • prsnclient: Logs activities (request/responses) to/from Presence service over client channel. • prsnservice: Logs activities related to Presence service. • prsnssystem: Logs activities (request/response) to/from Presence service over system channel. • statistics: Logs runtime statistics collected by statistics service. At summary level, statistics are logged when every collection interval is up (every 15 minutes by default). At detail level, statistics are logged as they are collected. • user: Logs User Service activities.
Other Loggers	Low level logging used to debug issues with non-Avaya and internal components. it generates internal log messages that may be useful during development. The logs are written only to

Name	Description
	trace.log. This information is normally provided by Services that support the product.
Logger	The name or identifier of the logger for which to run logging. Example, org.springframework
	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 like WebSphere or the Spring framework.
Trace Log File Settings	Trace level logging.
File Name	The name of the trace log file. Example, \${SERVER_LOG_ROOT}/trace.log
Maximum number of historical files	The maximum number of trace log files to keep 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.
Error Log File Settings	Error level logging.
File Name	The name of the error log file. Example, \${SERVER_LOG_ROOT}/SystemErr.log
Maximum number of historical files	The maximum number of error log files to keep 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. 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. Example, \${SERVER_LOG_ROOT}/activity.log

Name	Description
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 one-X Portal database.
Max Connections	The maximum number of connections to the database that you can create in this connection pool. Once this number is reached, no new connections are created 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, usually 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.

Name	Description
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

Portal User field descriptions

The Portal User configuration pages display the following fields:

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. 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 login 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 the 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. one-X Portal supports 1 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.

Name	Description
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 pertain to the Modular Messaging server used for Voice Messaging services. one-X Portal supports multiple Modular Messaging servers per user.
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 pertain to the Meeting Exchange server used for Voice Messaging services. one-X Portal installs one Meeting Exchange resource per user. This resource can be modified but not be deleted
Server	The name of the Meeting Exchange 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's password for the Conferencing server. This is an optional field that is not required by most Conferencing servers. Enter this value if your Conferencing server requires a password.

Name	Description
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.

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 computers only. Avaya one-X Portal Extensions are not supported on Mac computers.

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 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	<code>msiexec /i One-X.msi /qn</code>
With all parameters	<code>msiexec /i One-X.msi /qn SCHEME=HTTP(S) SERVER=###.###.###.### PORT=80 ROOT=/1xp/ portalclient</code>

Option	Command
With a log file	<code>msiexec /i One-X.msi /qn /log log.txt</code>

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 one-X Portal. You must enter the IP address or the fully-qualified domain name of the server. Example: <code>###.###.###.###</code> or <code>machine.domain.com</code>
PORT	The port that the one-X Portal Extensions uses to communicate with one-X Portal. Example: 80
ROOT	The location of the one-X Portal software on the one-X Portal server. Example: <code>/1xp/portalclient</code>

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 computers only. Avaya one-X Portal Extensions are not supported on Mac computers.

-
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 one-X Portal. You must enter the IP address or the fully-qualified domain name of the server.

For example, `onexpportal.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**.

If you checked the **Launch Avaya one-X Portal Extensions** option, the one-X Portal Extensions starts and logs you in automatically.

Chapter 9: Setting up one-X Portal on Citrix

Configuring the Citrix server for one-X Portal

Prerequisites

Make sure that the Citrix server is running Citrix Metaframe Presentation Server 4.0.

This document provides a high-level list of the tasks required to configure Citrix for 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 one-X Portal application
 - The Administration application
 3. For each application, add a command line for the login.
`iexplore.exe http://lxpServerName.company.com/lxp/portalclient/logon.jsp`
 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 one-X Portal

This document provides a high-level list of the tasks required to configure Citrix for 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 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 109.
 - 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 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 one-X Portal installation

If you encounter an issue with the one-X Portal installation, Avaya recommends that you do the following:

-
1. Review the topics in this Troubleshooting section and in the Troubleshooting documentation 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 one-X Portal application:
 - a. Check the Portal status in one-X Portal for any messages that indicate a problem with the one-X Portal system.
 - b. In 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 screenshots that show what happens when the issue occurs.

Next steps



Tip:

If the resolutions provided 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

one-X Portal provides the following types of Logging for system analysis and debugging purposes.

- General high level system logging
- Protocol level logging
- Aspect (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 are denied access to this 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 216

[Download log files](#) on page 218

[Configuring Logging](#) on page 218

[Logging field descriptions](#) on page 200

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 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 the 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 will be zipped and saved in the file system on the computer where one-X Portal is running.

Download log files

Prerequisites

To download log files on one-X Portal you must also be logged in to the WebSphere Administration page.

-
1. Select the System tab.
 2. From the left pane, select **Logging**.
 3. On the Logging Configuration page, in the **Download Log Files** field, click the **All Log Files** link.
 4. At the **File Download** dialog, the message **Do you want to open or save this file?**.
 - a. Name: (log file name)
 - b. Type: WinZip File
 - c. From (IP address of the Administration application).
 5. Click **Open** to open the log files on your machine.
 6. Click **Save** to save the log filesto your machine.
 7. Click **Cancel** to close the dialog.
-

Configuring Logging

To configure Logging on one-X Portal you must also be logged in to the WebSphere Administration page.

-
1. Select the System tab.
 2. From 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 200.
 4. Click **Reset** to display the settings from the start of this session.
-

Logging field descriptions

The **Logging** configuration page displays the following fields.

Name	Description
General Logging	one-X Portal logging that provides high level system information. Generally, the logs are written to SystemOut.log, and also to trace.log if any of the Protocol, Aspect, and/or Other Loggers is enabled.
Level	The level of General Logging logging to run. Selections are All , Fatal , Error , or Warning .
Protocol Logging	Low level logging used to debug issues with the protocols used by one-X Portal. It generates messages for debugging protocol exchanges. For example, SMTP or SIP. The logs are written 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. Selections are Summary or Traffic (detailed).
List of Current Protocol Loggers	The Protocol Level logger. • api: Debugs general client issues. The client API uses this protocol in one-X Portal. • bcapi: Debugs conferencing issues. Conferencing services use this protocol to connect to Meeting Exchange. • cmapi: Debugs Telephony issues. For example, Other Phone log in problems and EC500 issues. • cmcontact: Reports posting of contact log. Telephony services use this protocol to report posting of contact log information to Contact Logger service. • 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 • vfwclient: 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.

Name	Description
	• jtapi: Used to connect to Avaya Communication Manager. Telephony services use this as one of the protocols to connect to Avaya Communication Manager. Use this to resolve Telephony issues. • lps: Debugs Presence issues. Presence service uses this protocol to connect to the Avaya Intelligent Presence Server. • 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 Meeting Exchange. • weblm: Debugs licensing issues. The one-X Portal uses this protocol to connect to the licensing services
Aspect Logging	Low level logging used to debug issues with the one-X Portal components. It generates messages for debugging subsystem activity. For example Telephony or Conferencing. This can be enabled for specific Users in the system. The logs are written 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 .
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 aspect loggers that are available for use 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 WebSphere profile's logs directory. • 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 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 no user is specified, this will log information about the service. If a user is specified, this

Name	Description
	will log information about the user's 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 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 (request/response) to/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. • mmsystem: Logs activities (request/response) to/from Modular Messaging (voice messaging) service over system channel. • mxclient: Logs activities (request/response) to/from Meeting Exchange (bridge conferencing) service over client channel. • mxservice: Logs activities on Meeting Exchange (bridge conferencing) service. • mxsystem: Logs activities (request/response) to/from Meeting Exchange (bridge conferencing) service over system channel. • prsnclient: Logs activities (request/responses) to/from Presence service over client channel. • prsnservice: Logs activities related to Presence service. • prsnsystem: Logs activities (request/response) to/from Presence service over system channel.

Name	Description
	• statistics: Logs runtime statistics collected by statistics service. At summary level, statistics are logged when every collection interval is up (every 15 minutes by default). At detail level, statistics are logged as they are collected. • user: Logs User Service activities.
Other Loggers	Low level logging used to debug issues with non-Avaya and internal components. it generates internal log messages that may be useful during development. The logs are written only to trace.log. This information is normally provided by Services that support the product.
Logger	The name or identifier of the logger for which to run logging. Example, org.springframework
	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 like WebSphere or the Spring framework.
Trace Log File Settings	Trace level logging.
File Name	The name of the trace log file. Example, \${SERVER_LOG_ROOT}/trace.log
Maximum number of historical files	The maximum number of trace log files to keep 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.
Error Log File Settings	Error level logging.
File Name	The name of the error log file. Example, \${SERVER_LOG_ROOT}/SystemErr.log
Maximum number of historical files	The maximum number of error log files to keep 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. Example, \${SERVER_LOG_ROOT}/SystemOut.log

Name	Description
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. 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.

Calling party name incorrect

Some of the name instances on 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 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 one-X Portal

When opening a connection to an AE Services server or testing a connection to an AE Services server, 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, 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 one-X Portal uninstaller performs all steps needed to remove the one-X Portal software from the machine, including:

- Stops and uninstalls the one-X Portal server.
- Stops and uninstalls the one-X Portal database.
- If you installed the WebLM with one-X Portal, stops and uninstalls the WebLM.

Files not deleted by the one-X Portal uninstaller

The 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 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`
- If you chose to create Avaya service accounts, `/home/sroot`
- If you chose to create Avaya service accounts, `/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/lxp`.

Avaya one-X Portal logs: These logs are located at `/opt/avaya/lxp/waslogs`.

Uninstalling one-X Portal

1. Back up the one-X Portal database:
 - a. In the Administration application, use the **Database Backup** option of the **Scheduler** tab to perform a full database backup.
 - 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 one-X Portal server.
3. Execute the following command to start the one-X Portal uninstaller: `/opt/avaya/lxp/_uninst/uninstaller.bin`
4. Follow the prompts and answer questions asked by the uninstaller to remove one-X Portal from the machine.

The questions asked by the uninstaller depend upon the selections that you made when you installed 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 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: <pre>\$ cd db-inst-home \$ mv lxp-db-dir new-dir</pre> For example: <pre>\$ cd /home/dbinst \$ mv ACPDB SAVED_1XPDB</pre>
Delete the database user home directories and database files.	From the Linux command line, execute the following command: <pre>\$ cd db-user-home-dir</pre>

Procedure	Commands
For a list of the files and folders that the uninstaller does not delete, see Avaya one-X Portal uninstallation on page 224.	<pre>\$ rm -rf lxp-db-dir</pre> For example, to delete the user directory for a database instance user named dbinst:: <pre>\$ cd /home/dbinst</pre> <pre>\$ rm -rf ACPDB</pre>

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.

Index

A		Axis logging 71
access, LDAP 60		
Active Directory		B
domains 51		bandwidth, VOIP 31
ports 19		BCAPI Logger Directory 140
properties 117		Bridge Conference server 37
server information 113		bridge conferencing 79
synchronizing 167		broadband connection 31
version 38		browser toolbars 107
Administration application		browsers, supported 25
software requirements 25		
Administration Application		C
configuring prerequisites 106		call forwarding 55
hardware 28 , 101		Caller ID 64
ports 21		calling party name problems
software 101		calling party name different 223
user instructions 104		capacities 12
administration, users 168		checklists
AE Services		client configuration 106
configuration 72		environment validation 37
H. 323 gateway list 48		post-installation configuration 137
installing 46		user administration 170
ports 20		Cisco 525 PIX 30
Servers		Citrix
network worksheet 113		configuring client 213
users 47		configuring Internet Explorer 109
version 37		configuring server 213
AE Services server		operating system 101
not visible 223		support 27
analyzing dial plan 148 , 149		client
ANI 64		configuring prerequisites 106
AnnexH 56		hardware 28 , 101
ANYPIN 66		software 101
AOL toolbar 107		client access 61
applications, support 15		Communication Manager
applications, supporting 16		call forwarding 55
assigning 177 – 181		communication, Meeting Exchange 65
conferencing resource 177 , 180		configuration 73
messaging resource 179		configuring Extension to Cellular 57 , 58
presence resource 181		dial plans 141
Auxiliary servers		disabling AnnexH 56
adding 158		Do No Disturb 54
Avaya Phone Interface 16		emergency call handling 55
Avaya Voice Player		Extension to Cellular 56
about 16		H. 323 gateway list 48
uninstalling 226		ports 19
Avaya1XPMsgRecorder.cab 16		version 37
AvayaPhoneInterface.cab 16		

conferences		downloading one-X Portal Extensions	105
bridge features	64	downloads, Citrix	109
bridge operators	65	DTMF	64
on-demand	66		
Conferencing services		E	
adding	161	e-mail application	101
description	161	E.164 format	141
configuration tool	89	e911	55
configure, Presence group	69	EC500, see Extension to Cellular	56, 57
configure, Presence server	70	emergency call handling	55
configure, security certificates	66	encryption	11
configuring		Enterprise Directory	
AE Services	72	guidelines	49
Citrix	213	security groups	51
client prerequisites	106	service account	53
Communication Manager	73	users	52
dial plan	83	Enterprise Directory domains	
Enterprise Directory domains	85	adding	164
environment validation logs	92	configuration	85
Environment Validation tool	94	description	163
Extension to Cellular	56–58	enterprise directory fields	195
Meeting Exchange	64–66, 79	environment validation tool	
Mobility Extension Bank	84	timing, environment validation	89
Modular Messaging	75	when to run	89
Presence	81	Environment Validation tool	
SSL authentication	182	about	89
configuring Safari	110	configuring logs	92
connection, broadband	31	configuring TSAPI.PRO	91
creating user instructions	104	installing	91
customization	35	interface	94
		log file	90
D		running	93
database properties	117	sample logs	90
definitions	17	tests performed	89
deinstallation	224, 225	example	
Dial feature, Meeting Exchange	64	dial plan rules	149
Dial plan services		pattern matching transformation	145
adding	154	regular expression transformation	147
creating rules	148, 149	simple dial plan transformation	143
description	141	explorer proxy settings	111
modifying	155	Extension to Cellular	
pattern matching transformation	145	about	56
requirements	142	user extensions	57
simple dial plan transformation	143	worker stations	58
worksheet	83	extensions, mobility	58
dial plans		extensions, user	57
pattern matching transformation	144		
regular expression transformation	146, 147	F	
simple dial plan transformation	142	FDAPI	65
disabling AnnexH	56	features	7
Do Not Disturb	54	features, Meeting Exchange	64
domains, Active Directory	51	FF proxy	111
downloading			
one-X Portal Extensions	210		

-
- Firefox[25](#), [101](#), [109](#)
 - JavaScript[109](#)
 - version[101](#)
 - Firefox proxy[111](#)
 - Firefox proxy settings[111](#)
 - firewall, requirements[30](#), [39](#)
 - Flex-DAPI[65](#)
-
- ## G
- general settings
 - product ID[194](#)
 - reset[194](#)
 - save[194](#)
 - URL[194](#)
 - getting started, user worksheet[105](#)
 - Google toolbar[107](#)
 - group profiles
 - adding[174](#)
 - description[173](#)
 - guidelines
 - AE Services[46](#)
 - Enterprise Directory[49](#)
 - firewall[30](#)
-
- ## H
- H. 323 gateway list[48](#)
 - hardware
 - client[28](#), [101](#)
 - ports[19](#)
 - prerequisites[9](#)
 - server[37](#)
 - hardware information[113](#)
 - hardware requirements
 - application desktop[28](#), [101](#)
 - minimum[27](#)
 - server[27](#)
 - host ID[33](#)
-
- ## I
- IBM WebSphere
 - Enterprise Directory[53](#)
 - properties[117](#)
 - IE proxy[111](#)
 - IMAP4[59](#), [61](#), [63](#)
 - installation privileges[117](#)
 - installing[44–46](#), [91](#), [126](#), [139](#), [160](#), [209](#), [210](#)
 - AE Services[46](#)
 - Environment Validation tool[91](#)
 - license[139](#)
 - Linux[45](#)
 - one-X Portal Extensions[209](#), [210](#)
 - prerequisites[44](#)
 - security certificate[160](#)
 - installing one-X Portal Extensions[105](#)
 - instructions, users[104](#)
 - integrations, software requirements[23](#)
 - interactions, software[14](#)
 - Internet Explorer
 - Citrix configuration[109](#)
 - JavaScript[108](#)
 - security zone[108](#)
 - shortcuts[108](#)
 - version[101](#)
 - Internet Explorer proxy[111](#)
 - interoperability[14](#), [15](#)
 - IP softphones[14](#)
 - Modular Messaging[15](#)
 - one-X Mobile[15](#)
 - IP Agent[14](#)
 - IP Softphone[14](#)
-
- ## J
- JavaScript, configuring for[108](#), [109](#)
 - JDBC fields[205](#)
 - jitter[30](#), [39](#)
 - Juniper Networks SSG-520[30](#)
-
- ## L
- languages, supported[10](#)
 - LDAP[59](#), [60](#)
 - legal notices[2](#)
 - License server
 - configuring[165](#)
 - description[164](#)
 - license server fields[197](#)
 - licensing
 - host ID[33](#)
 - installing license[139](#)
 - requesting license[34](#)
 - requirements[32](#)
 - WebLM location[33](#)
 - limitations
 - VOIP[15](#)
 - limits, performance[12](#)
 - Linux
 - installing[45](#)
 - required privileges[117](#)
 - version[23](#), [37](#)
 - local intranet, Internet Explorer[108](#)
 - local WebLM.[139](#)
 - location
 - Environment Validation tool[89](#)

location, WebLM	33
log files	
Environment Validation tool	90 , 92
retrieving	216
Log files	
downloading	218
Logging	
configuring	218
description	216
logging fields	200 , 219
logging in	138

M

MAC address	33
Mac, client prerequisites	101
Meeting Exchange	
BCAPI Logger Directory	140
bridge operators	65
Communication Manager	65
configuration	79
dial plans	141
enabling features	64
on-demand conferences	66
ports	19
software interactions	15
version	37
Message Recorder	16
messages	
Avaya Voice Player	16
one-X Portal Message Recorder	16
Messages Temp Directory	140
Messaging server	37
Mobility Extension Banks	
adding	163
description	162
worksheet	84
mobility extensions	58
Modular Messaging	
client access	61
configuration	75
IMAP4	61 , 63
LDAP	60
Messages Temp Directory	140
NTP	62
ports	19 , 59
protocols	59
software interactions	15
subscriber values	60
super-user	61 , 63
time synchronization	62
version	37
Modular Messaging Web Client	15
Music	64

N

naming conventions	17
network	19 , 29–31 , 39 , 113
broadband internet	31
firewall	30
performance	30 , 39
ports	19
remote users	31
requirements	30
time synchronization	29
VOIP bandwidth	31
notices, legal	2
NTP	62

O

obtaining host ID	33
on-demand conferences	66
one-X Desktop Edition	14
one-X Mobile	15
one-X Portal	
Citrix	27 , 213
configuring prerequisites	106
hardware	28 , 101
limitations	15
ports	21
restarting	166
server information	113
software	101
software requirements	25
user instructions	104
VOIP	15
one-X Portal Extensions	
about	16
hardware	28 , 101
installation options	209
installing	105 , 209 , 210
limitations	15
ports	21
software	28 , 101
software requirements	25
uninstalling	226
one-X Portal Message Recorder	16
operators, Meeting Exchange	65

P

packet delay	30 , 39
pattern matching transformation	144 , 145
performance limitations	12
performance, network	39

periodic spiked delays	30
Phone Interface	16
physical address	33
PINs	64, 66
pop-up blockers	107
ports	19–22
Administration Application	21
AE Services	20
one-X Portal	21
one-X Portal Extensions	21
SNMP	22
VOIP	21
post-installation checklist	137
prerequisites	
about	9
Active Directory	51
AE Services	46
Communication Manager	54–58
Enterprise Directory	49, 51–53
Extension to Cellular	56–58
installing	44
Linux	45
Meeting Exchange	64–66
Modular Messaging	59–63
server	23, 39, 44
WebLM	33, 139
presence	81
Presence	
configuration	81
Presence group	
configuring	69
Presence group configuring	69
Presence server	66, 70, 71
Axis logging	71
configuring	70
security certificates	66
Presence service	
description	161
Presence services	
adding	162
privileges, installation	117
prompting, PINs	66
properties	
AE Services	72
Communication Manager	73
dial plan	83
Enterprise Directory domains	85
Meeting Exchange	79
Mobility Extension Bank	84
Modular Messaging	75
Presence	81
prototype users	
adding	175
conferencing resource	177

description	175
messaging resource	176
telephony resource	176

R

rebranding	35
reduce, Axis logging	71
regular expression transformation	146, 147
requesting license	34
requirements	
Administration application	25
Administration Application	25
broadband internet	31
Citrix	27
dial plan	142
firewall	30
hardware	27
integrations	23
licensing	32
network	30
one-X Portal	25
one-X Portal Extensions	25
remote users	31
server hardware	27
server software	23
time synchronization	29
VOIP bandwidth	31
resource domain	51
resources	
conferencing	177, 180
messaging	176, 179
presence	181
telephony	176, 178
responsibility for prerequisites	9
running, Environment Validation tool	93

S

Safari	
configuring	110
Scheduler	
fields	193
synchronization	167
secure site certificate	182
Security	11, 19, 30, 61, 63, 160, 182
firewall	30
installing certificates	160
secure ports	19
SSL authentication	182
trusted server	61, 63
security certificates	66
security groups, Enterprise Directory	51
security zone, Internet Explorer	108

server		
configuring	137	
configuring prerequisites	39	
hardware	37	
hardware information	113	
hardware requirements	27	
installation	117	
installing prerequisites	44	
ports	19	
software	37	
software requirements	23	
server information	113	
Servers		
fields	183	
time synchronization	29	
service account		
administrative	53	
shortcuts, Internet Explorer	108	
simple dial plan transformation	142 , 143	
SIP trunk set	64	
SMS, one-X Portal Extensions	209	
SMTP	59	
SNMP Destinations		
adding	166	
description	166	
SNMP destinations fields	198	
SNMP ports	22	
SNMP Traps		
configuring	165	
description	165	
SNMP traps fields	198	
software		
client	101	
prerequisites	9	
server	37	
software interactions	14	
software requirements		
Administration application	25	
Administration Application	25	
Citrix	27	
integrations	23	
one-X Portal	25	
one-X Portal Extensions	25	
server	23	
SonicWALL Pro 3060	30	
SSL authentication	182	
stations, worker	58	
Statistics fields	200	
subscriber management	60	
super-user, Modular Messaging	61 , 63	
support	215	
supported browsers	25	
supported languages	10	
supported versions	22	
supporting applications	16	
synchronizing		
enterprise directory	167	
synchronizing time	29	
System diagram	7	
System features	7	
system profile		
description	171	
modifying	172	
T		
Telephony server	37	
Telephony servers		
about	157	
adding	157	
terminology	17	
testing environment	89	
time synchronization		
Modular Messaging 3.0	62	
requirements	29	
tool, environment validation	89–94	
topology, Active Directory	51	
transformations		
pattern-matching	144 , 145	
regular expression	146 , 147	
simple dial plan	142 , 143	
transport network	39	
troubleshooting	215	
trunk to trunk transfer	55	
TSAPI.PRO	91	
U		
uninstalling		
Avaya Voice Player	226	
one-X Portal	224 , 225	
one-X Portal Extensions	226	
user domain	51	
users		
administration	168 , 170	
AE Services	47	
conferencing resource	180	
description	168	
Enterprise Directory	52	
extensions	57	
fields	206	
instructions	104	
messaging resource	179	
presence resource	181	
provisioning	177	
remote connection	31	
service account	53	
telephony resource	178	

worksheet	105	properties	117
		verifying	139
V		WebLM server	
validating environment	89 , 92–94	configuring	165
verifying WebLM	139	description	164
voice messaging	75	Windows, client prerequisites	101
Voice Messaging servers		workbook	19
adding	159	worker stations	58
description	159	worksheet, one-X Portal Extensions	105
Voice Player		worksheets	
uninstalling	226	AE Services	72
VOIP	15 , 16 , 21 , 30 , 31 , 39	Communication Manager	73
bandwidth requirements	31	Dial Plan	83
firewall	30 , 39	Enterprise Directory	85
Phone Interface	16	installation information	117
ports	21	Meeting Exchange	79
W		Mobility Extension Bank	84
Web browser	101	Modular Messaging	75
web browsers, supported	25	network information	113
Web Client, Modular Messaging	15	Presence	81
WebLM		server prerequisites	39
configuring	33 , 139	users	105
local	139	Y	
ports	19	Yahoo toolbar	107
		Z	
		zone, security	108

