



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya one-X® Portal as part of Avaya Unified Communication Mobile Worker Solution– Issue 1.0**

### **Abstract**

These Application Notes describe a sample configuration for Avaya one-X® Portal to support Avaya Mobile Worker Solution. The Avaya one-X® Portal is a browser-based interface to Avaya telephony, mobility, messaging, conferencing and presence services provided by Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, Avaya Modular Messaging, Avaya Meeting Exchange Enterprise and Avaya Aura™ Presence Services. The Avaya one-X® Portal also integrates with Microsoft Active Directory for user authentication and authorization.

This solution was tested in the Solution and Interoperability Test Lab (SIL) in support of the November 2009 product launch activities.

# 1. Introduction

These Application Notes describe a sample configuration for Avaya one-X® Portal to support Avaya Mobile Worker Solution. Avaya Mobile Worker Solution allows users in different locations to have full access to Avaya services. The configuration can be broken down into three types of user or location:

- Enterprise Office User
- Remote User
- Branch Office User

The Enterprise Office User has access to services via normal corporate network connections including wireless LAN. Services include access to centralized Avaya Modular Messaging (voicemail), Avaya one-X® Speech functionality, Avaya Web Conferencing, Avaya Meeting Exchange, Avaya Intelligent Presence Service and wireless network or GSM connection for Avaya one-X® Mobile enabled handsets. Avaya Aura™ Communication Manager resides on both Enterprise and Remote Sites. End users are configured to use a variety of end points including one-X® Communicator, one-X® Portal, Avaya desk phones and a selection of third party mobile phones.

The Remote User has access to the same services on the Enterprise Site by using either an SSL or IPSEC VPN connection. The Remote User can be located either in a home office or perhaps a hotel room. In these cases the one-X Mobile, one-X Communicator and Avaya 9630 VPN desk phone can be used as end points.

The Branch Office User is situated in a separate office location. The Branch Office uses the centralized services located at the Enterprise Office. Connection of one-X® Mobile to either Communication Manager is obtained via GSM or wireless network depending on the location.

The Avaya one-X® Portal is a browser-based interface to Avaya telephony, mobility, messaging, conferencing and presence services. The telephony and mobility services are provided by Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services (AES), the messaging service is provided by Avaya Modular Messaging (MM), the conferencing service is provided by Avaya Meeting Exchange Enterprise (MX) and the presence service is provided by Avaya Aura™ Presence Services (IPS). The Avaya one-X® Portal also integrates with Microsoft Active Directory (AD) for user authentication and authorization.

The telephony and mobility integration with Avaya Aura™ Communication Manager is achieved through Avaya Aura™ Application Enablement Services. Avaya one-X® Portal uses the Avaya Aura™ Application Enablement Services Java Telephony Application Programming Interface (JTAPI) and Device Media and Call Control (DMCC) services to query, monitor, and control the user telephones on Avaya Aura™ Communication Manager. From a configuration standpoint, the Avaya Aura™ Application Enablement Services JTAPI falls under the umbrella of the Avaya Telephony Services Application Programming Interface (TSAPI) service. Therefore all configuration references in Avaya Aura™ Application Enablement Services and Avaya Aura™ Communication Manager will use the label TSAPI instead of JTAPI.

For the mobility service, the Avaya Extension to Cellular (EC500) feature is used on Avaya Aura™ Communication Manager to enable users to extend calls to any PSTN-reachable phone, such as a cell phone.

For the messaging service, Avaya one-X® Portal uses the Internet Messaging Access Protocol 4 (IMAP4) to enable users to access voice messages, and uses the Simple Mail Transfer Protocol (SMTP) for message transmission.

For the conferencing service, Avaya one-X® Portal uses the Scheduler API (SCHAPI) to schedule on-demand conferences, and uses the Avaya Conferencing Program Interface (ACAPI) to manage and control conferences.

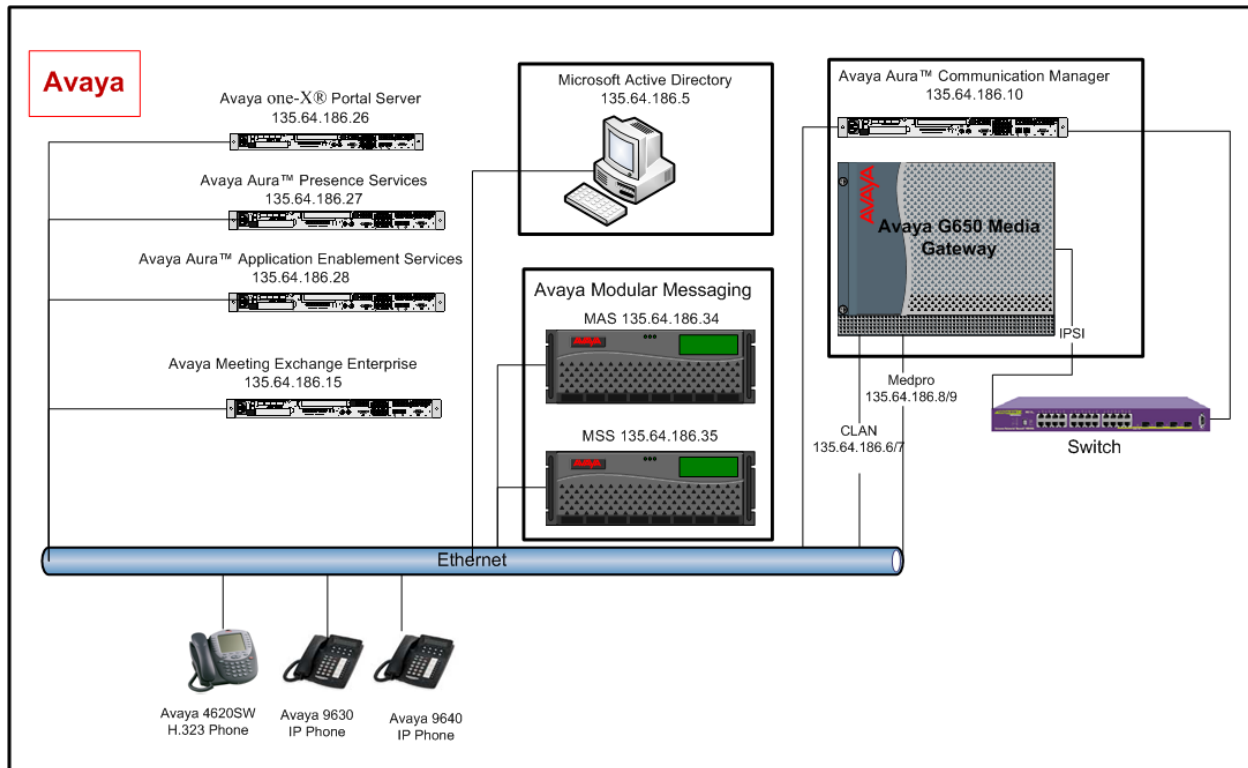
The following is a set of features provided by Avaya one-X® Portal:

- Access the Avaya Aura™ Communication Manager user telephones and features remotely using a VoIP-enabled computer, a cell phone, or any other designated phone.
- View, play, and record Avaya Modular Messaging voice messages.
- View, participate in, and control Avaya Meeting Exchange Enterprise bridge conferences, and view real-time display of conference participants and available conference controls.
- Search, sort, and view personal and enterprise contacts. Call a contact, send a fax or voice message to a contact, or add a contact to a conference.
- Enable delivery of user calls to a second destination such as a cell phone.

These Application Notes assume that the basic installation and configuration of Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, Avaya Modular Messaging, Avaya Meeting Exchange Enterprise, Avaya Aura™ Presence Services and Microsoft AD are already in place, and will focus on the additional configuration required to integrate with Avaya one-X® Portal.

## 2. Reference Configuration

**Figure 1** illustrates the configuration that was used to verify these Application Notes.



**Figure 1: Network Diagram of the Compliance Tested Configuration**

### 3. Equipment and Software Validated

The following hardware and software versions were used for the sample configuration provided in **Table 1** below.

Equipment	Software
Avaya S8720 Server	Avaya Aura™ Communication Manager 5.2 S8720-015-02.1.016.4
Avaya G650 Media Gateway <ul style="list-style-type: none"><li>• TN799DP C-LAN Circuit Pack</li><li>• TN2602AP IP Media Processor</li></ul>	HW01 FW034 HW08 FW049
Avaya S8500 Server	Avaya Aura™ Application Enablement Services R5-2-0-98-0
Avaya Modular Messaging <ul style="list-style-type: none"><li>• Messaging Storage Server</li><li>• Messaging Application Server</li></ul>	V5.2 (9.2.150.7)
Avaya Meeting Exchange Enterprise Server	Avaya Meeting Exchange Enterprise (S6200) 5.2
Avaya S8510 Server	Avaya one-X® Portal 5.2.0.0.18
Avaya S8510 Server	Avaya Aura™ Presence Services IPS-01.00.00-29 IPSSP2-01.00.02-3 IPS_XCP-5.3.6.13-1
Microsoft Active Directory	Microsoft Windows Server 2003 R2 Enterprise x64 Edition Service Pack 2
Avaya 4620SW IP Telephones	2.9 sp1(H.323)
Avaya 9630 IP Telephone	Avaya one-X™ Deskphone Edition H.323 Release S3.0
Avaya 9640 IP Telephone	Avaya one-X™ Deskphone Edition H.323 Release S3.0

**Table 1: Equipment and Software Version Validated**

## 4. Configure Avaya Aura™ Communication Manager

This section assumes the basic configuration is already in place on Communication Manager for the following: dial plan and routing, Extension to Cellular (EC500), connectivity to AES, integration with MM and MX. The section provides a quick overview of the needed feature licenses, and the detail procedures below for integration with one-X Portal:

- Verify Avaya Aura™ Communication Manager License
- Administer System Parameters Features
- Obtain feature access codes
- Administer CTI link
- Administer coverage path
- Administer class of service
- Administer IP network region
- Administer user extensions
- Administer off-PBX station mappings
- Administer mobility extensions

## 4.1. Verify Avaya Aura™ Communication Manager License

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Maximum Off-PBX Telephones – EC500** option is licensed.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V15                                     Software Package: Standard
Location: 1                                           RFA System ID (SID): 1
Platform: 6                                           RFA Module ID (MID): 1

                                USED
Platform Maximum Ports: 44000 153
Maximum Stations: 36000 38
Maximum XMOBILE Stations: 0 0
Maximum Off-PBX Telephones - EC500: 100 10
Maximum Off-PBX Telephones - OPS: 100 4
Maximum Off-PBX Telephones - PBFMC: 100 6
Maximum Off-PBX Telephones - PVFMC: 100 0
Maximum Off-PBX Telephones - SCCAN: 0 0

(NOTE: You must logoff & login to effect the permission changes.)
```

Navigate to **Page 3**, and verify that the **ARS** and **Computer Telephony Adjunct Links** options are licensed.

```
display system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? n                Audible Message Waiting? n
Access Security Gateway (ASG)? n                    Authorization Codes? n
Analog Trunk Incoming Call ID? y                    CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? n              CAS Main? n
Answer Supervision by Call Classifier? n              Change COR by FAC? n
ARS? y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                             Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y                      DCS (Basic)? n
ASAI Link Core Capabilities? n                      DCS Call Coverage? n
ASAI Link Plus Capabilities? n                      DCS with Rerouting? n
Async. Transfer Mode (ATM) PNC? n                   Digital Loss Plan Modification? n
Async. Transfer Mode (ATM) Trunking? n               DS1 MSP? n
ATM WAN Spare Processor? n                          DS1 Echo Cancellation? y
ATMS? n
Attendant Vectoring? n

(NOTE: You must logoff & login to effect the permission changes.)
```

Navigate to **Page 4**, and verify that the highlighted features below are licensed. In the case of **ISDN-BRI Trunks** and **ISDN-PRI**, having one of these two options licensed would be sufficient.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? y
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? n	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? n	
External Device Alarm Admin? y	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? n	Multifrequency Signaling? y	
Global Call Classification? n	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? n	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? n		
(NOTE: You must logoff & login to effect the permission changes.)		

Navigate to **Page 10**, and verify that the highlighted features below are licensed.

display system-parameters customer-options		Page 10 of 11
MAXIMUM IP REGISTRATIONS BY PRODUCT ID		
Product ID	Rel. Limit	Used
<b>IP_API_A</b>	<b>: 100</b>	<b>0</b>
IP_API_B	: 0	0
IP_API_C	: 0	0
IP_Agent	: 1	0
IP_IR_A	: 0	0
<b>IP_Phone</b>	<b>: 18000</b>	<b>11</b>
IP_ROMax	: 18000	0
<b>IP_Soft</b>	<b>: 100</b>	<b>0</b>
IP_eCons	: 0	0
oneX_Comm	: 18000	2
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
(NOTE: You must logoff & login to effect the permission changes.)		



## 4.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming trunk call to a remote destination such as a cell phone or a home phone. For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis. Note that this setting poses significant security risk, and must be used with caution. For alternatives, the Trunk-to-Trunk Transfer feature can be enabled on the trunk class of restriction or station class of service level. Refer to [2] in **Section 13** for more details.

```
change system-parameters features                               Page 1 of 18
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
      Music/Tone on Hold: none
      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

### 4.3. Obtain Feature Access Codes

The Automatic Route Selection (ARS) and EC500 features are assumed to be administered already on Communication Manager. Use the **display feature-access-codes** command, and obtain the access code value assigned to the ARS feature shown below.

```
display feature-access-codes                                     Page 1 of 8
FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code: #00
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: *8
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation:                      Deactivation:
Call Forwarding Activation Busy/DA: *1      All: *2      Deactivation: *3
Call Forwarding Enhanced Status:            Act:          Deactivation:
Call Park Access Code:
Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
CDR Account Code Access Code:
Change COR Access Code:
Change Coverage Access Code:
Conditional Call Extend Activation:           Deactivation:
Contact Closure Open Code:                   Close Code:
```

Navigate to **Page 2**, and obtain the access code values assigned to the EC500 feature highlighted below. These values will be used to configure the one-X Portal server.

```
display feature-access-codes                                     Page 2 of 8
FEATURE ACCESS CODE (FAC)
Contact Closure Pulse Code:
Data Origination Access Code:
Data Privacy Access Code:
Directed Call Pickup Access Code:
Directed Group Call Pickup Access Code:
Emergency Access to Attendant Access Code:
EC500 Self-Administration Access Codes: *6
Enhanced EC500 Activation: *7      Deactivation: *5
Enterprise Mobility User Activation:           Deactivation:
Extended Call Fwd Activate Busy D/A #01 All: #02 Deactivation: #03
Extended Group Call Pickup Access Code:
Facility Test Calls Access Code:
Flash Access Code:
Group Control Restrict Activation:             Deactivation:
Hunt Group Busy Activation:                   Deactivation:
ISDN Access Code:
Last Number Dialed Access Code:
Leave Word Calling Message Retrieval Lock:
Leave Word Calling Message Retrieval Unlock:
```

## 4.4. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. This CTI link will be used for the AES TSAPI and DMCC services. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1										Page 1 of 3	
										CTI LINK	
CTI Link: 1											
Extension: 22222											
Type: ADJ-IP											
										COR: 1	
Name: silstackaesCTI-Link											

## 4.5. Administer Class of Service

To allow one-X Portal users to forward incoming trunk calls to remote destinations, disable the **Restrict Call Fwd-Off Net** field shown below for the relevant class of service. In the interoperability testing, class of service **1** is used for all one-X Portal users.

change cos											Page 1 of 2					
CLASS OF SERVICE																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n
Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y
Data Privacy	n	y	n	n	n	y	y	y	y	n	n	n	n	y	y	y
Priority Calling	n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y
Console Permissions	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Off-hook Alert	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Client Room	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
<b>Restrict Call Fwd-Off Net</b>	y	n	y	y	y	y	y	y	y	y	y	y	y	y	y	y
Call Forwarding Busy/DA	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Personal Station Access (PSA)	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Extended Forwarding All	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Extended Forwarding B/DA	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Trk-to-Trk Transfer Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

## 4.6. Administer IP Network Region

To enable one-X Portal users to access their extensions from remote telephones, retain the default value of **challenge** as one of the permitted **SECURITY PROFILES** on the relevant IP network region. In the interoperability testing, IP network region **1** is used for all one-X Portal users.

change ip-network-region 1	Page 2 of 19
IP NETWORK REGION	
INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY	
Incoming LDN Extension:	
Conversion To Full Public Number - Delete:      Insert:	
Maximum Number of Trunks to Use for IGAR:	
Dial Plan Transparency in Survivable Mode? n	
BACKUP SERVERS(IN PRIORITY ORDER)      H.323 SECURITY PROFILES	
1	1      challenge
2	2
3	3
4	4
5	
6	Allow SIP URI Conversion? y
TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS	
Near End Establishes TCP Signaling Socket? y	
Near End TCP Port Min: 61440	
Near End TCP Port Max: 61444	

## 4.7. Administer User Extensions

Use the **add station n** command, where **n** is the extension of a user that will use the one-X Portal application. Enter a descriptive **Name**, and desired **Security Code**. In the **Coverage Path 1** field, enter the coverage path number from **Section 4.5**. In the **COS** field, enter the class of service number from **Section 4.6**. Enable the **IP SoftPhone** field, to allow the user to control telephone calls via the one-X Portal. Note the field values in the **Extension** and **Security Code** fields, which will be used later to administer one-X Portal.

add station 20015		Page 1 of 5
STATION		
<b>Extension: 20015</b>	Lock Messages? n	BCC: M
Type: 9640	<b>Security Code: 1234</b>	TN: 1
Port: S00054	<b>Coverage Path 1: 1</b>	COR: 1
<b>Name: Test 20015</b>	Coverage Path 2:	<b>COS: 1</b>
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 20015	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? y	
	Customizable Labels? y	

Navigate to **Page 2**. In the **Remote Softphone Emergency Calls** field, verify that the value is not set to **block**. In the **Emergency Location Ext** field, verify that the value is set to the user extension as shown below. Repeat this section for every one-X Portal user extension.

change station 20015		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance?	n
LWC Activation? y	Coverage Msg Retrieval?	y
LWC Log External Calls? n	Auto Answer:	none
CDR Privacy? n	Data Restriction?	n
Redirect Notification? y	Idle Appearance Preference?	n
Per Button Ring Control? n	Bridged Idle Line Preference?	n
Bridged Call Alerting? n	Restrict Last Appearance?	y
Active Station Ringing: single		
	EMU Login Allowed?	n
H.320 Conversion? n	Per Station CPN - Send Calling Number?	y
Service Link Mode: as-needed	EC500 State:	enabled
Multimedia Mode: enhanced		
MWI Served User Type: sip-adjunct	Display Client Redirection?	n
	Select Last Used Appearance?	n
	Coverage After Forwarding?	s
	Multimedia Early Answer?	n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections?	y
Emergency Location Ext: 20015	Always Use? n IP Audio Hairpinning?	n

## 4.8. Administer Off-PBX Station Mappings

For each one-X Portal user, enable calls to the user to also ring a cell phone destination by using the **change off-pbx-telephone station-mapping n** command, where **n** is the user extension. Set **Application** to **EC500**, **Trunk Selection** to **ars**, and **Configuration Set** to an existing configuration set to be used for the off-pbx call treatment.

**Note:** The **Phone Number** for the cell phone destination can be configured by the user via one-X Portal upon activation of the mobility feature.

change off-pbx-telephone station-mapping 20015						Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION								
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual	
Extension		Prefix			Selection	Set	Mode	
20015	EC500	-			ars	1		

Navigate to **Page 2**, and set **Mapping Mode** to **termination** as shown below, to allow the cell phone to only be used to terminate calls from the associated host phone. Retain the default values in the remaining fields. Repeat this section for every one-X Portal user extension.

change off-pbx-telephone station-mapping 20015						Page	2 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION								
Station	Appl	Call	Mapping	Calls	Bridged	Location		
Extension	Name	Limit	Mode	Allowed	Calls			
20015	EC500	2	termination	all	both			

## 5. Configure Avaya Aura™ Application Enablement Services

Avaya recommends a dedicated Application Enablement Services server be used for integration with one-X Portal. This section assumes that the administration for the basic switch connection on Application Enablement Services with Communication Manager is already in place, and provides procedures for the following areas:

- Verify Avaya Aura™ Application Enablement Services license
- Administer H.323 gatekeeper
- Administer TSAPI link
- Disable security database
- Administer DMCC and TSAPI users
- Configure DMCC ports
- Restart TSAPI service

### 5.1. Verify Avaya Aura™ Application Enablement Services License

Access the Application Enablement Services OAM web-based interface by using the URL **http://ip-address** in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server. The **Login** screen is displayed as shown below. Log in with appropriate credentials.



#### Application Enablement Services

Management Console

Help

Please login here:

Username

Password

© 2009 Avaya, Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next. Select **AE Services** from the left pane.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". In the top right corner, a welcome message is shown: "Welcome: User craft", "Last login: Mon Dec 21 14:50:10 2009 from 135.64.47.64", "HostName/IP: silstackaes/135.64.186.28", "Server Offer Type: TURNKEY", and "SW Version: r5-2-0-98-0". Below this is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. A left-hand menu contains several options: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of domains and their functions: "AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "Licensing - Use Licensing to manage the license server.", "Maintenance - Use Maintenance to manage the routine maintenance tasks.", "Networking - Use Networking to manage the network interfaces and ports.", "Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "Status - Use Status to obtain server status informations.", "User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "Utilities - Use Utilities to carry out basic connectivity tests.", and "Help - Use Help to obtain a few tips for using the OAM Help system". Below the list, a note states: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain." At the bottom center, the copyright notice "© 2009 Avaya, Inc. All Rights Reserved." is displayed.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
Last login: Mon Dec 21 14:50:10 2009 from 135.64.47.64  
HostName/IP: silstackaes/135.64.186.28  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Home Home | Help | Logout

AE Services  
Communication Manager Interface  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

### Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:


- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

© 2009 Avaya, Inc. All Rights Reserved.



The **AE Services** screen is displayed. Verify that Application Enablement Services is licensed by ensuring that **TSAPI Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Mon Dec 21 14:50:10 2009 from 135.64.47.64  
HostName/IP: silstackaes/135.64.186.28  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

AE Services
Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▶ TSAPI

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**AE Services**

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

**License Information**  
You are licensed to run Application Enablement (CTI) version 5.0

## 5.2. Administer H.323 Gatekeeper

Administer a H.323 gatekeeper for one-X Portal to use, for registration of soft phones via the DMCC service to Communication Manager. Select **Communication Manager Interface** → **Switch Connections** from the left pane, to display the **Switch Connections** screen. Select the pre-administered switch connection (not shown), in this case **silstackCM**, and click **Edit H.323 Gatekeeper**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar shows "Communication Manager Interface | Switch Connections" and links for "Home | Help | Logout". A left sidebar lists various services, with "Communication Manager Interface" expanded to show "Switch Connections". The main content area, titled "Switch Connections", features an "Add Connection" button and a table with one entry, "silstackCM". Below the table are buttons for "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", and "Delete Connection".

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
silstackCM	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of the procr (on the S8300 or S8500 Server platforms) or a CLAN card on Communication Manager, for the soft phones to use for registration. In this case, the Processor CLAN with IP address of **135.64.186.6** is used. Click **Add Name or IP**.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Mon Dec 21 14:50:10 2009 from 135.64.47.64  
HostName/IP: silstackaes/135.64.186.28  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

**Edit H.323 Gatekeeper - silstackCM**

135.64.186.6 Add Name or IP  
Name or IP Address  
Delete IP

### 5.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click **Edit Link**.

AE Services | TSAPI | TSAPI Link Home | Help | Logout

AE Services  
CVLAN  
DLG  
DMCC  
SMS  
TSAPI  
TSAPI Links  
TSAPI Properties  
Communication Manager Interface  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

**TSAPI Links**

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	silstackCM	1	4	Unencrypted

Add Link Edit Link Delete Link

The **Edit TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For the **Switch Connection** field, select the **silstackCM** switch connection, as configured in **Section 5.2**, from the drop-down list. For the **Switch CTI Link Number** field, select the CTI link number from **Section 4.4**. Click **Apply Changes**.


The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and user information: 'Welcome: User craft', 'Last login: Mon Dec 21 14:50:10 2009 from 135.64.47.64', 'HostName/IP: silstackaes/135.64.186.28', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-0-98-0'. A red navigation bar contains 'AE Services | TSAPI | TSAPI Link' and links for 'Home | Help | Logout'. The left sidebar lists navigation options: 'AE Services' (expanded), 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (selected), 'TSAPI Properties', 'Communication Manager Interface', 'Licensing', 'Maintenance', 'Networking', 'Security', and 'Status'. The main content area is titled 'Edit TSAPI Links' and contains the following fields: 'Link' (value: 1), 'Switch Connection' (dropdown: silstackCM), 'Switch CTI Link Number' (dropdown: 1), 'ASAI Link Version' (dropdown: 4), and 'Security' (dropdown: Unencrypted). At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.

The **Apply Changes to Link** screen is displayed. Click **Apply**.

The screenshot shows the same Avaya Application Enablement Services Management Console, but the main content area is now titled 'Apply Changes to Link'. It displays a warning message: 'Warning! Are you sure you want to apply the changes? These changes can only take effect when the TSAPI server restarts. Please use the Maintenance -> Service Controller page to restart the TSAPI server.' Below the warning are two buttons: 'Apply' and 'Cancel'.

## 5.4. Administer DMCC and TSAPI Users

Administer a DMCC and a TSAPI user for the one-X Portal server to use. Select **User Management** from the left pane.

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Tue Jan 5 12:34:09 2010 from 198.152.13.67  
HostName/IP: silstackaes/135.64.186.28  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

User ManagementHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ User Management
  - ▶ Service Admin
  - ▶ User Admin
- ▶ Utilities
- ▶ Help


### User Management

User Management provides you with the followings for managing user-related information for AE Services:

- Service Admin -- Use the Service Admin for managing the User Management service itself (for example, synchronizing events between the AE Services user database and the Security database).
- User Admin -- Use the User Admin to manage all AE Services users (add, change or delete users).

### 5.4.1. Administer DMCC User

Select **User Management** → **Add User** from the left pane to administer a DMCC user for one-X Portal. In the **Add User** screen shown below, enter desired values for the **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password** fields. Set **CT User** to be **Yes**, Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Tue Jan 5 15:59:18 2010 from 198.152.13.67  
HostName/IP: silstackaes/135.64.186.28  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

User Management | User Admin | Add UserHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ User Management
  - ▶ Service Admin
  - ▼ User Admin
    - Add User
    - Change User Password
    - List All Users
    - Modify Default Users
    - Search Users
- ▶ Utilities
- ▶ Help

### Add User

Fields marked with \* can not be empty.

\* User Id

\* Common Name

\* Surname

\* User Password

\* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

### 5.4.2. Administer TSAPI User

Select **User Management** → **Add User** from the left pane to administer a TSAPI user for one-X Portal. In the **Add User** screen shown below, enter desired values for the **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password** fields. Set **CT User** to be **Yes**, Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

The screenshot shows the 'Add User' screen in the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'User Management' > 'User Admin' > 'Add User'. The main content area contains the 'Add User' form. At the top right, a welcome message for 'User craft' is displayed, including the last login time and IP address. The form fields are as follows:

Field	Value
* User Id	xportalTSAPI
* Common Name	oneXportalTSAPI
* Surname	oneXportalTSAPI
* User Password	*****
* Confirm Password	*****
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	

### 5.4.3. Enable Unrestricted access for TSAPI User


Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the TSAPI user that was set up in **Section 5.4.2** and click **Edit**.

The screenshot shows the 'CTI Users' screen in the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Security Database' > 'CTI Users' > 'List All Users'. The main content area displays a table of CTI users.

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> avaya	avaya	NONE	NONE
<input type="radio"/> xportalDMCC	xportalDMCC	NONE	NONE
<input checked="" type="radio"/> xportalTSAPI	xportalTSAPI	NONE	NONE

Below the table are two buttons: **Edit** and **List All**.

The **Edit CTI User** screen appears. Check the **Unrestricted Access** checkbox and click **Apply Changes** at the bottom of the screen.



**Application Enablement Services**  
 Management Console

Welcome: User craft  
 Last login: Tue Jan 26 15:41:08 2010 from 135.11.3.4  
 HostName/IP: aes/135.64.186.28  
 Server Offer Type: TURNKEY  
 SW Version: r5-2-0-98-0

Security | Security Database | CTI Users | List All Users
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
- ▶ Account Management
- ▶ Audit
- ▶ Certificate Management
- Enterprise Directory
- ▶ Host AA
- ▶ PAM
- ▼ Security Database
- Control
- **CTI Users**
- **List All Users**
- Search Users
- Devices

### Edit CTI User

User Profile:	User ID Common Name Worktop Name Unrestricted Access	xportalTSAPI xportalTSAPI <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">NONE ▼</div> <input checked="" type="checkbox"/>
---------------	---	---

---

Call Origination and Termination / Device Status


None ▼

---

Call and Device Monitoring:	Device Call / Device Call	<div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">None ▼</div> <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">None ▼</div> <input type="checkbox"/>
-----------------------------	---------------------------------	--

---

Routing Control:
Allow Routing on Listed Devices


None ▼

Apply Changes

Cancel Changes

A screen (not shown) appears to confirm applied changes to CTI User, click **Apply**.

## 5.5. Configure DMCC Ports

To configure DMCC ports, select **Networking** → **Ports**. Enable the **Unencrypted Port 4721** which will be used by oneX-Portal application, as described in **Section 9.2**. Click **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

DMCC Server Ports		Enabled Disabled
Unencrypted Port	4721	<input checked="" type="radio"/> <input type="radio"/>
Encrypted Port	4722	<input checked="" type="radio"/> <input type="radio"/>
TR/87 Port	4723	<input checked="" type="radio"/> <input type="radio"/>

## 5.6. Restart DMCC and TSAPI Service

Restart the DMCC and TSAPI service, which is performed from the Application Enablement Services Management Console web page. Select **Maintenance** → **Service Controller** from the left pane. The **Service Controller** screen is displayed, and shows a listing of the services and associated status. Check the **DMCC Service** and **TSAPI Service**, and click **Restart Service**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message: "Welcome: User craft", "Last login: Tue Jan 26 16:16:23 2010 from 135.11.3.4", "HostName/IP: aes/135.64.186.28", "Server Offer Type: TURNKEY", and "SW Version: r5-2-0-98-0". The main navigation bar has "Maintenance | Service Controller" and "Home | Help | Logout". The left sidebar shows a tree view with "Maintenance" expanded, containing "Date Time/NTP Server", "Security Database", "Service Controller" (highlighted), and "Server Data". The main content area is titled "Service Controller" and contains a table with two columns: "Service" and "Controller Status".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

Below the table, it says "For status on actual services, please use [Status and Control](#)". At the bottom, there are buttons: "Start", "Stop", "Restart Service" (highlighted), "Restart AE Server", "Restart Linux", and "Restart Web Server".

The following **Restart Service** screen is displayed. Click **Restart** to confirm.

The screenshot shows the same Avaya Application Enablement Services Management Console, but now displaying the "Restart Service" dialog. The top header and navigation bar are identical. The left sidebar shows "Maintenance" expanded, with "Service Controller" highlighted. The main content area is titled "Restart Service" and contains a warning message: "Warning! Are you sure you want to restart? Restarting will cause all existing connections to be dropped and associations lost." Below the message are two buttons: "Restart" and "Cancel".



## 6. Configure Avaya Modular Messaging

This section assumes that the administration for integration of Avaya Modular Messaging with Communication Manager is already in place, and focuses on the integration with Avaya one-X Portal. The integration is configured on the Avaya Messaging Storage Server (MSS) and on the Messaging Application Server (MAS) components, and includes the following areas:

- Obtain System Ports
- Administer Directory Updates
- Administer Trusted Server
- Administer Subscribers
- Enabling access to the subscriber's mailbox

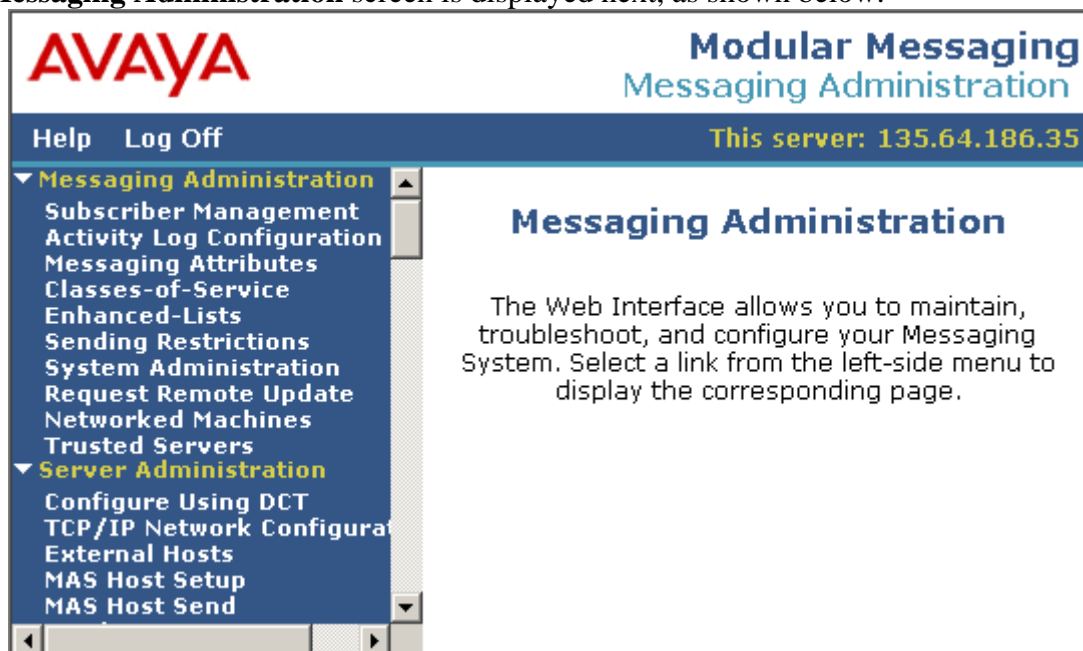
### 6.1. Obtain System Ports

Access the Messaging Administration web-based interface by using the URL **http://ip-address** in an Internet browser window, where **ip-address** is the IP address of the MSS server. The **Logon** screen is displayed. Log on using a valid user name and password. The **Password** field will appear after a value is entered into the **Username** field.

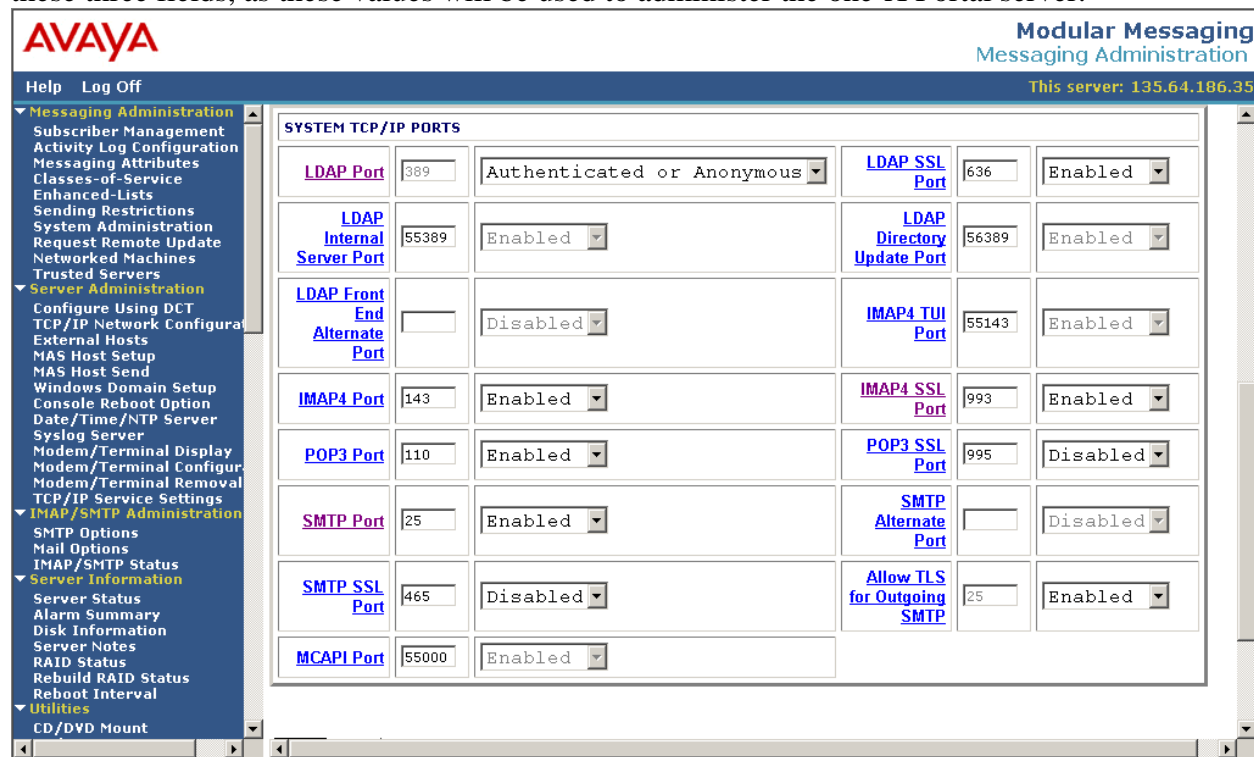


The screenshot displays the Avaya Messaging Administration web interface. At the top left is the Avaya logo in red. To its right, the text "Messaging Administration" is in blue, with "Modular Messaging" in a lighter blue below it. A dark blue horizontal bar contains the word "Help" in white. The main content area has a light blue background. On the left side of this area is a small icon consisting of three squares (blue, yellow, and blue). To the right of the icon is a large blue rectangular box with the word "Logon" in white at the top left. Inside this box, the label "Username" is followed by a white text input field. At the bottom right of the blue box is a blue button with the word "Login" in white. The entire interface is framed by a thin grey border with a vertical scrollbar on the right side.

The **Messaging Administration** screen is displayed next, as shown below.



Select **Messaging Administration** → **System Administration** from the left pane, to display the **Administer System Attributes and Ports** screen. Scroll down the right pane to display the **SYSTEM TCP/IP PORTS** section. Verify that the **LDAP Port** is **Authenticated or Anonymous**, **SMTP Port** and **IMAP4 SSL Port** fields are **Enabled**. Note the port numbers for these three fields, as these values will be used to administer the one-X Portal server.



## 6.2. Administer Directory Updates

Select **Messaging Administration** → **Networked Machines** from the left pane, to display the **Manage Networked Machines** screen. Select the MSS server from the table listing, and click **Edit the Selected Networked Machine** toward the bottom right of the screen.

The screenshot shows the Avaya Modular Messaging Messaging Administration interface. The left pane contains a tree view with 'Messaging Administration' expanded, showing 'Networked Machines' selected. The main pane displays the 'Manage Networked Machines' screen. It features a table with the following data:

Machine	IP Address	Machine Type	Total Subs
mss	135.64.186.35	local	26

Below the table are four buttons: 'Display Report of Networked Machines', 'Delete the Selected Networked Machine', 'Add a New Networked Machine', and 'Edit the Selected Networked Machine'.

The **Edit Networked Machine** screen is displayed. In the **Updates In** field, select **yes** from the drop-down list to enable directory updates from networked machines.

The screenshot shows the 'Edit Networked Machine' screen. It contains a form with the following fields and values:

<b>Machine Name</b>	mss	<b>Password</b>	
		<b>Confirm Password</b>	
<b>IP Address</b>	135.64.186.35	<b>Machine Type</b>	tcpip
<b>Mailbox Number Length</b>	5	<b>Default Community</b>	1
<b>Updates In</b>	yes	<b>Updates Out</b>	yes
<b>LDAP Port</b>	56389	<b>Log Updates In</b>	no

### 6.3. Administer Trusted Server

Select **Messaging Administration** → **Trusted Servers** from the left pane, to display the **Manage Trusted Servers** screen. Click **Add a New Trusted Server** toward the bottom left of the screen (not shown below).

The screenshot shows the Avaya Modular Messaging Messaging Administration web interface. The left navigation pane is expanded to 'Trusted Servers' under 'Server Administration'. The main content area is titled 'Manage Trusted Servers' and contains a table with the following data:

Trusted Server	IP Addr/Name	Service Name
One-XSpeech	135.64.189.41	Speech Access
OneXMobile	135.64.186.30	edge
VVSTS	192.168.1.250	MWI Server
mas	192.168.1.250	Messaging Application Server

Below the table are four buttons: 'Display Report of Trusted Servers', 'Delete the Selected Trusted Server', 'Add a New Trusted Server', and 'Edit the Selected Trusted Server'. The top right of the interface shows 'This server: 135.64.186.35'.

The **Add Trusted Server** screen is displayed. Enter desired values for the **Trusted Server Name**, **Password**, **Confirm Password**, and **Service Name** fields. For the **Machine Name / IP Address** field, enter the IP address of the one-X Portal server. Select **yes** from the **IMAP4 Super User Access Allowed** field drop-down list, and select **Must use SSL or encrypted SASL** from the **IMAP4 Super User Connection Security** field drop-down list. Retain the default values in the remaining fields.

**AVAYA** Modular Messaging Messaging Administration  
This server: 135.64.186.35

Help Log Off

**Add Trusted Server**

<b>Trusted Server Name</b>	oneXPortal	<b>Password</b>	
		<b>Confirm Password</b>	
<b>Machine Name / IP Address</b>	135.64.186.26	<b>Service Name</b>	One-X Portal
<b>Minutes of Inactivity Before Alarm</b>	0	<b>Default Community</b>	1
<b>Access to Cross Domain Delivery</b>	no	<b>Special Type</b>	(none)
<b>LDAP Access Allowed</b>	yes	<b>LDAP Connection Security</b>	No encryption required
<b>IMAP4 Super User Access Allowed</b>	yes	<b>IMAP4 Super User Connection Security</b>	Must use SSL or encrypted SASL

Save Delete  
Back Help

## 6.4. Administer Subscribers

Select **Messaging Administration → Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. In the **Local Subscribers** row, click **Manage**.

**AVAYA** Modular Messaging Messaging Administration  
This server: 135.64.186.35

Help Log Off

**Manage Subscribers**

• Local Subscriber Mailbox Number  Add or Edit

	<b>Machine Name</b>	<b>Local Subscriber Mailboxes</b>	<b>Total Subscribers</b>	<b>Filtered Subscribers</b>
• Local Subscribers	mss	22	26	26

Filter Manage

The **Manage Local Subscribers** screen is displayed next. For each one-X Portal user, select the corresponding subscriber entry and click **Edit the Selected Subscriber**.

Modular Messaging  
Messaging Administration

Help Log Off

This server: 135.64.186.35

▼ Messaging Administration

Subscriber Management  
Activity Log Configuration  
Messaging Attributes  
Classes-of-Service  
Enhanced-Lists  
Sending Restrictions  
System Administration  
Request Remote Update  
Networked Machines  
Trusted Servers

▼ Server Administration

Configure Using DCT  
TCP/IP Network Configuration  
External Hosts  
MAS Host Setup  
MAS Host Send  
Windows Domain Setup  
Console Reboot Option  
Date/Time/NTP Server  
Syslog Server  
Modem/Terminal Display  
Modem/Terminal Configuration  
Modem/Terminal Removal  
TCP/IP Service Settings

▼ IMAP/SMTP Administration

SMTP Options  
Mail Options  
IMAP/SMTP Status

▼ Server Information

Server Status  
Alarm Summary  
Disk Information  
Server Notes  
RAID Status  
Rebuild RAID Status  
Reboot Interval

▼ Utilities

CD/DVD Mount  
CD/DVD Unmount

Manage Local Subscribers

Local Subscriber Mailboxes: 23

Total Subscribers: 27

System Mailboxes: 4

Filtered Subscribers: 27

ASCII Name	Mailbox Number	Numeric Address	COS	CID	Subscriber Name
20015	20015	20015	3	1	20015, EntUser
20020	20020	20020	3	1	20020, Ent
20031	20031	20031	3	1	740021, User
20032	20032	20032	3	1	20032, User
20033	20033	20033	3	1	20033, User
20036	20036	20036	3	1	20036, User
20050	20050	20050	3	1	20050, VPN_User
20051	20051	20051	3	1	20051, VPN
20052	20052	20052	3	1	20052, Ent
20070	20070	20070	3	1	20070, 20070
34001	34001	34001	3	1	ASM, 34001
40001	40001	40001	3	1	40001, 40001
40010	40010	40010	3	1	40010, Branch
740021	40021	740021	3	1	40021, Branch
Home 2	20090	20090	3	1	20090, Home

Sort and Filter Subscribers

Launch Subscriber Options

Display Report of Subscribers

Delete the Selected Subscriber

Add a New Subscriber

Edit the Selected Subscriber

Make certain that at least one of the values in the following fields match to the already administered values in the corresponding Microsoft Active Directory user record: **Mailbox Number**, **PBX Extension**, **Email Handle**, and **Telephone Number**. If none of these values match, then the one-X Portal server cannot accurately link incoming and outgoing communication with the correct users. Verify the administered values for every one-X Portal user and make adjustments as necessary.

The screenshot displays the Avaya Modular Messaging Administration web interface. The top header includes the Avaya logo, 'Modular Messaging Messaging Administration', and the server IP '135.64.186.35'. A left-hand navigation menu lists various administrative tasks. The main content area is titled 'Add Local Subscriber' and contains two sections: 'BASIC INFORMATION' and 'SUBSCRIBER DIRECTORY'.

**BASIC INFORMATION \* (Required Fields)**

*Last Name	20015	First Name	EntUser
*Password	....	*Mailbox Number	20015
*Numeric Address	20015	PBX Extension	20015
*Class Of Service	3 - class03-MM	*Community ID	1

**SUBSCRIBER DIRECTORY**

Email Handle	20015@mss.silstack.com	Telephone Number	20015
Common Name	20015	ASCII Version of Name	20015

## 6.5. Enabling access to the subscriber's mailbox

Avaya one-X Portal requires access to the client mailbox on Modular Messaging. This configuration ensures that subscribers can connect to their mailboxes through one-X Portal and access their messages. In order to enable access to the subscriber's mailbox following actions need to be performed:

- Configure Class-of-Service on MSS
- Configure Messaging on MAS

### 6.5.1. Configure Class-of-service on MSS

On the MSS server, Select **Messaging Administration** → **Classes-of-service** from the left pane, to display the **Manage Classes-of-Service** screen. Select the Class of Service that was assigned to configured subscribers, **class03-MM** and click **Edit the Selected COS**.

The screenshot shows the Avaya Modular Messaging Administration web interface. The left navigation pane is expanded, showing the 'Messaging Administration' section with 'Classes-of-Service' selected. The main content area is titled 'Manage Classes-of-Service' and displays a table of COS names and numbers. The table has two columns: 'COS Name' and 'COS Number'. The rows are listed from 'class00' to 'class14', with 'class03-MM' highlighted. Below the table, there is a 'Sort By Name' button and two buttons at the bottom: 'Display Report of COSs' and 'Edit the Selected COS'.

COS Name	COS Number
class00	0
class01	1
class02	2
class03-MM	3
class04	4
class05	5
class06	6
class07	7
ELA	8
class09	9
class10	10
class11	11
class12	12
class13	13
class14	14



On the **Edit a Class-of-Service** screen that appears, scroll down to the **SUBSCRIBER FEATURES and SERVICES** section(not shown). In the **Restrict Client Access** field, set the value to **No** and click **Save**.

**AVAYA** Modular Messaging  
Messaging Administration  
This server: 135.64.186.35

Help Log Off

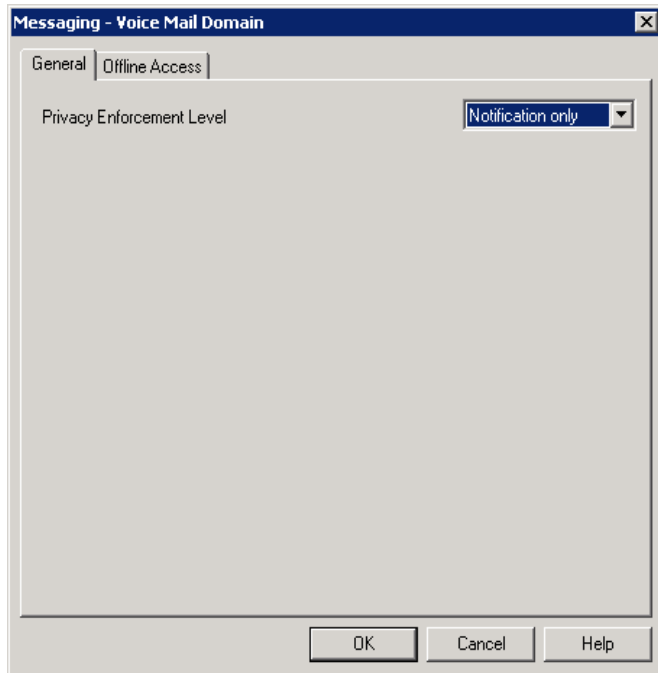
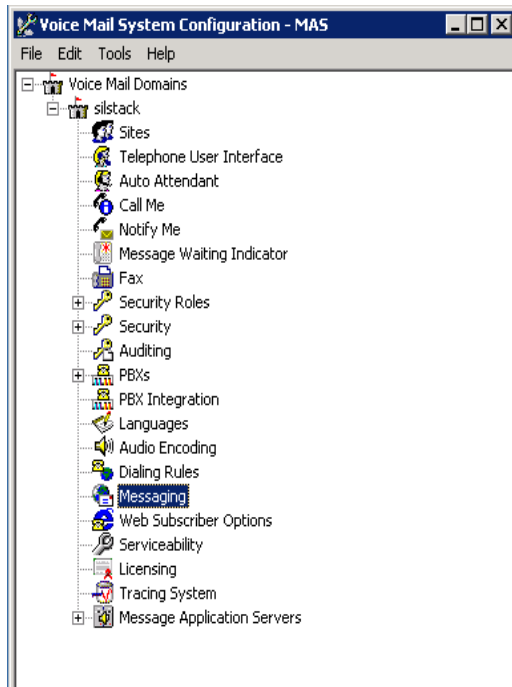
▼ Messaging Administration  
Subscriber Management  
Activity Log Configuration  
Messaging Attributes  
Classes-of-Service  
Enhanced-Lists  
Sending Restrictions  
System Administration  
Request Remote Update  
Networked Machines  
Trusted Servers  
▼ Server Administration  
Configure Using DCT  
TCP/IP Network Configura  
External Hosts  
MAS Host Setup  
MAS Host Send  
Windows Domain Setup  
Console Reboot Option  
Date/Time/NTP Server  
Syslog Server  
Modem/Terminal Display  
Modem/Terminal Configur  
Modem/Terminal Removal  
TCP/IP Service Settings  
▼ IMAP/SMTP Administration  
SMTP Options  
Mail Options  
IMAP/SMTP Status  
▼ Server Information  
Server Status  
Alarm Summary  
Disk Information  
Server Notes  
RAID Status  
Rebuild RAID Status  
Reboot Interval  
Utilities

<a href="#">Find Me Allowed</a>	yes ▼	<a href="#">Notify Me Allowed</a>	no ▼
<a href="#">Call Handling</a>	yes ▼	<a href="#">Call Screening</a>	yes ▼
<a href="#">Outbound Fax Calls</a>	no ▼	<a href="#">Extended Absence Greeting Allowed</a>	yes ▼
<a href="#">Inbound Fax</a>	yes ▼	<a href="#">Aria TUI Date &amp; Time Playback</a>	Never
<a href="#">Page via PBX</a>	no ▼	<a href="#">Record Mailbox Greetings</a>	yes ▼
<a href="#">Caller Application Announcement Recording</a>	no ▼	<a href="#">Caller Application</a>	(none) ▼
<a href="#">Telephone User Interface</a>	MM Aria ▼	<a href="#">Restrict Client Access</a>	no ▼
<a href="#">Personal Operator Configuration</a>	no ▼	<a href="#">Unsent Message Allowed</a>	no ▼
<a href="#">Allow message after EAG</a>	Always ▼		

Back Save Help

### 6.5.2. Configure Messaging on MAS

Log in to the Avaya MAS server using the appropriate credentials. Select **Start→ Programs → Avaya Modular Messaging →Voice Mail System Configuration** to start the Voice Mail System Configuration tool. From the Voice Mail System Configuration window, go to **Voice Mail Domains → silstack → Messaging**. From the subsequent Voice Mail Domain window, confirm that the **Privacy Enforcement Level** is set to **Notification only**. Click **OK**.

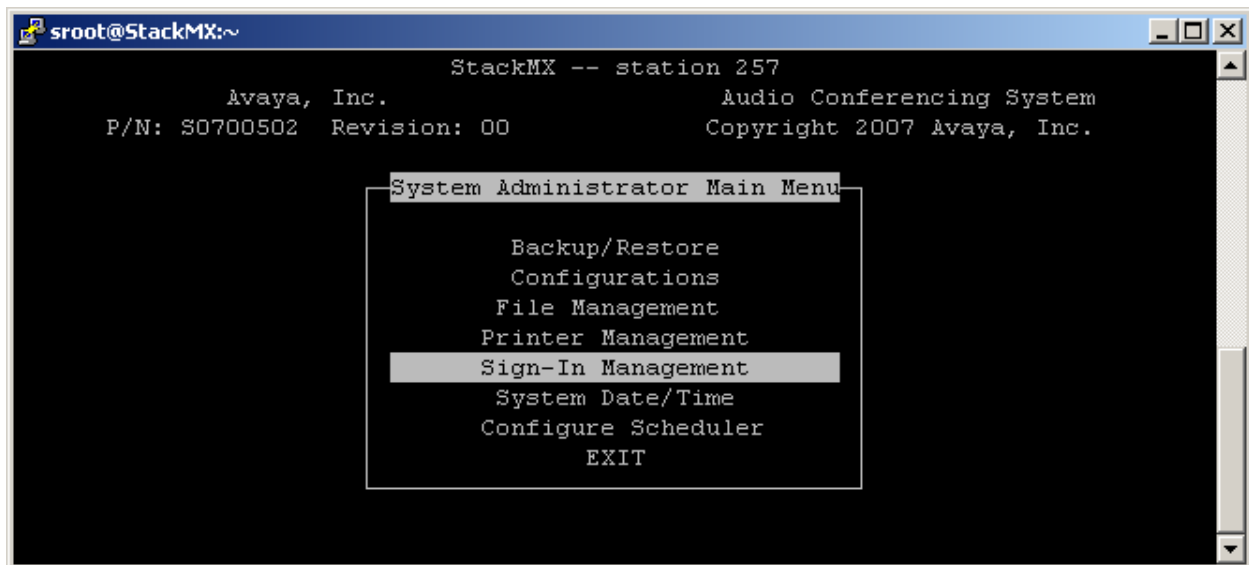


## 7. Configure Avaya Meeting Exchange Enterprise

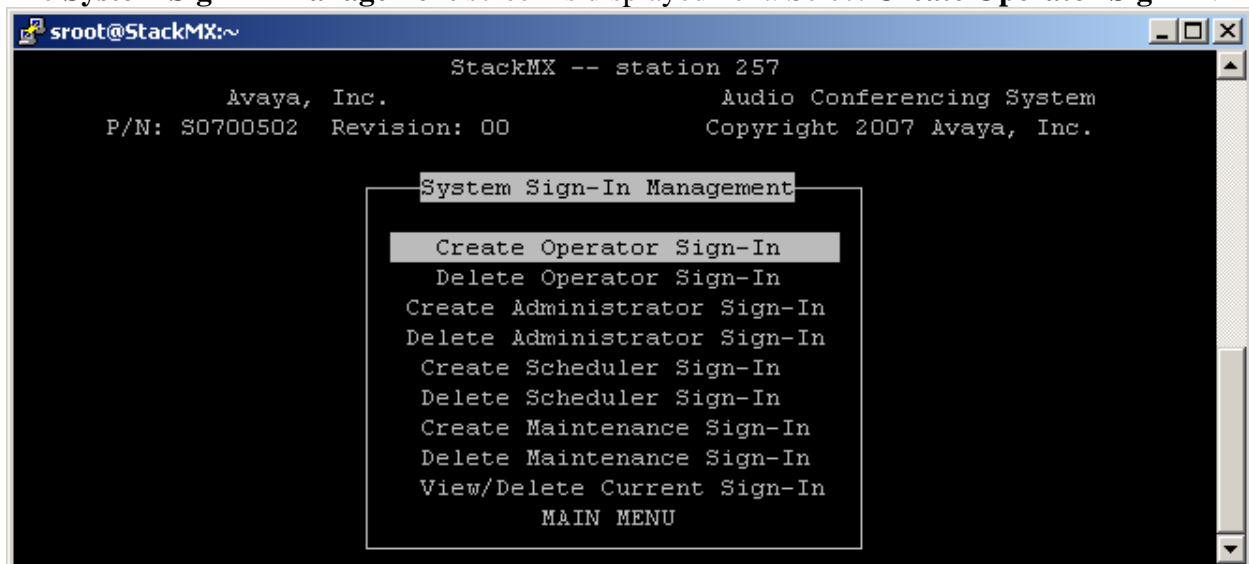
This section assumes that the administration for Meeting Exchange integration with Communication Manager is already in place, and that the following settings are enabled: ANI and DNIS, music source, Dial feature, bridge number, moderator code, and participant code. For information on configuring features listed above, refer to [6] in **Section 13**. This section provides the procedure to integrate with one-X Portal, which includes administration of two operators.

### 7.1. Administer Operators

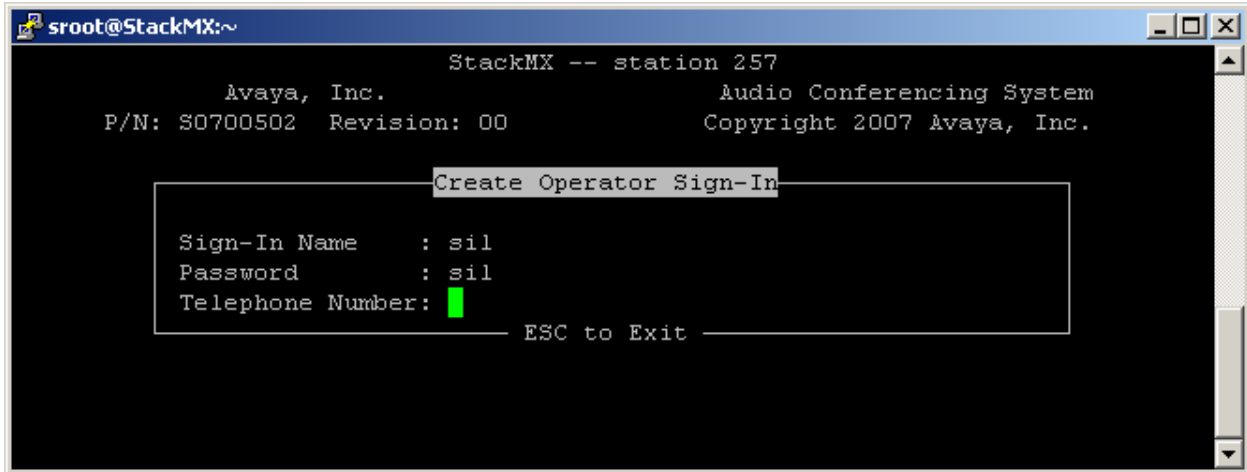
Open a putty session to MX, and log in with system administrator credentials. The **System Administrator Main Menu** is displayed, as shown below. Select **Sign-In Management**.



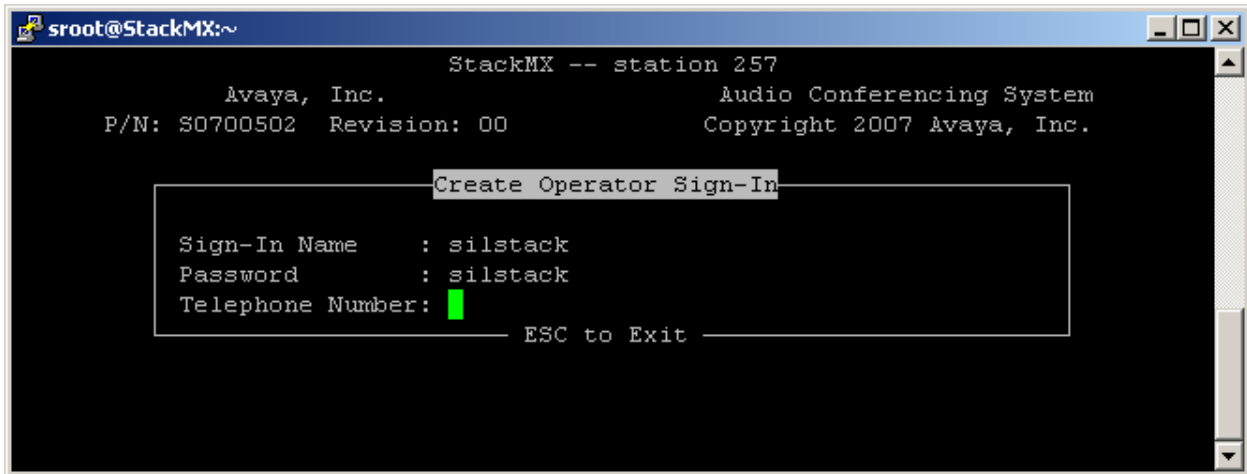
The **System Sign-In Management** screen is displayed next. Select **Create Operator Sign-In**.



The **Create Operator Sign-In** screen is displayed. Enter desired values for **Sign-In Name** and **Password**. Repeat this procedure to add a second operator for the one-X Portal server to use. In the interoperability testing, two operators **sil** and **silstack** were added.



A terminal window titled 'sroot@StackMX:~' displays the 'StackMX -- station 257' header. Below the header, it shows 'Avaya, Inc. Audio Conferencing System' and 'P/N: S0700502 Revision: 00 Copyright 2007 Avaya, Inc.'. The main screen is titled 'Create Operator Sign-In' and contains a form with the following fields: 'Sign-In Name : sil', 'Password : sil', and 'Telephone Number: ' followed by a green cursor. At the bottom of the form, it says 'ESC to Exit'.



A terminal window titled 'sroot@StackMX:~' displays the 'StackMX -- station 257' header. Below the header, it shows 'Avaya, Inc. Audio Conferencing System' and 'P/N: S0700502 Revision: 00 Copyright 2007 Avaya, Inc.'. The main screen is titled 'Create Operator Sign-In' and contains a form with the following fields: 'Sign-In Name : silstack', 'Password : silstack', and 'Telephone Number: ' followed by a green cursor. At the bottom of the form, it says 'ESC to Exit'.

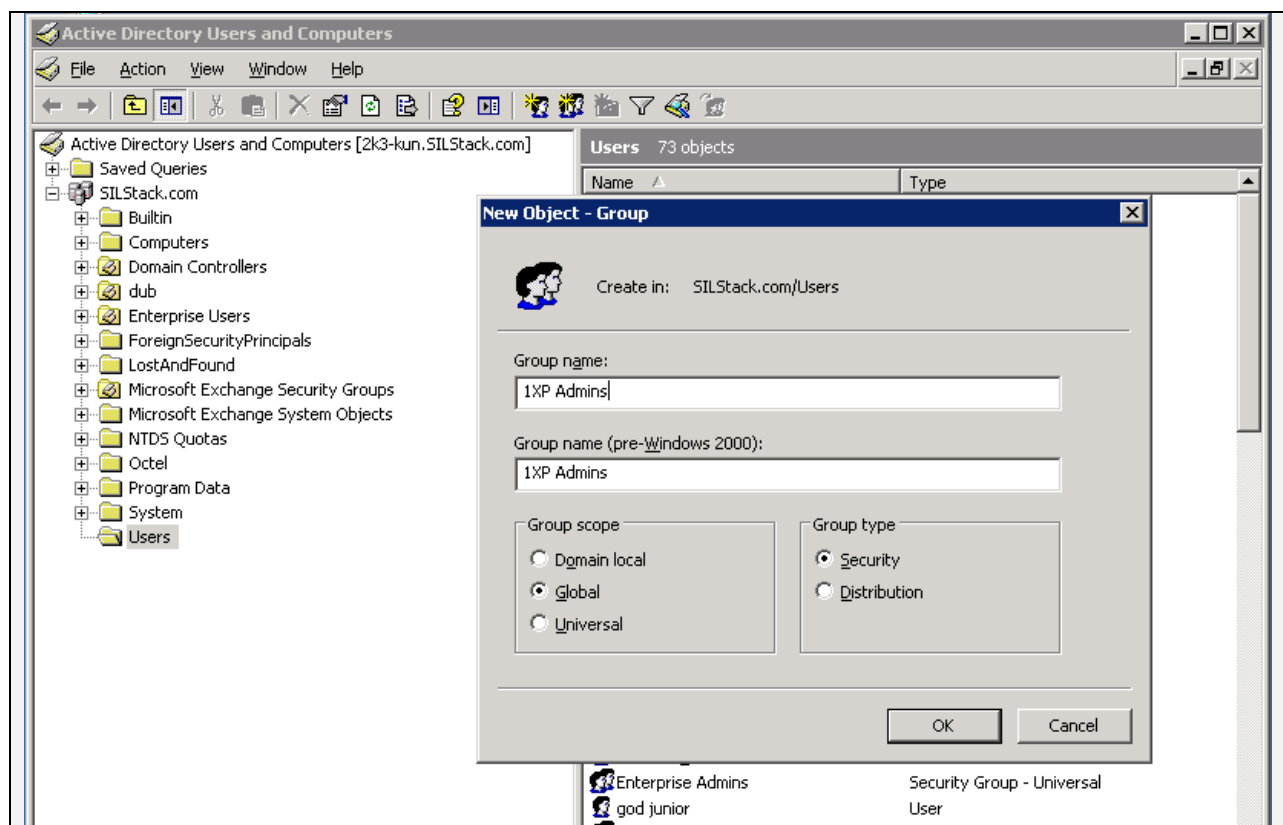
## 8. Configure Microsoft Active Directory

This section assumes that the network domain and user records are already in place in Microsoft Active Directory, and provides the additional procedures to integrate with one-X Portal. The procedures include the following:

- Administer security groups
- Administer service account
- Administer user accounts

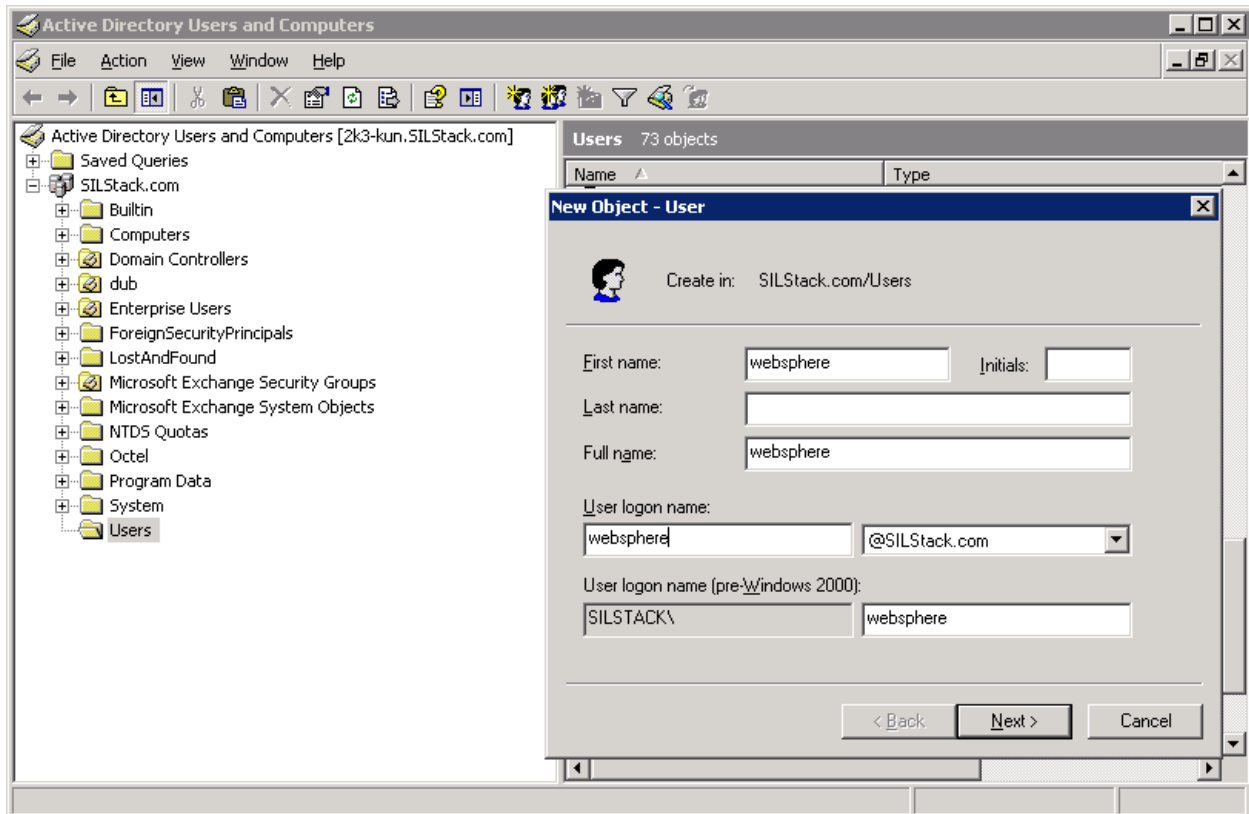
### 8.1. Administer Security Groups

Before installing one-X Portal, create a set of Active Directory security groups. On the Microsoft Active Directory server, launch **Programs → Administrator Tools → Active Directory Users and Computers**. The **Active Directory Users and Computers** screen is displayed. In the left pane, locate the proper domain name for the network configuration, in this case **SILStack.com**, and right-click on **Users** below it. From the right-click drop-down menu (not shown below), select **New → Group**. In the **New Object – Group** dialog box that is displayed, enter a descriptive **Group name** to denote the administrator security group. Retain the default values in the remaining fields. Repeat this procedure to create a security group for the users and a security group for the auditors. In the interoperability testing, the three created security groups are **1XP Admins**, **1XP Users**, and **1XP Auditors**.

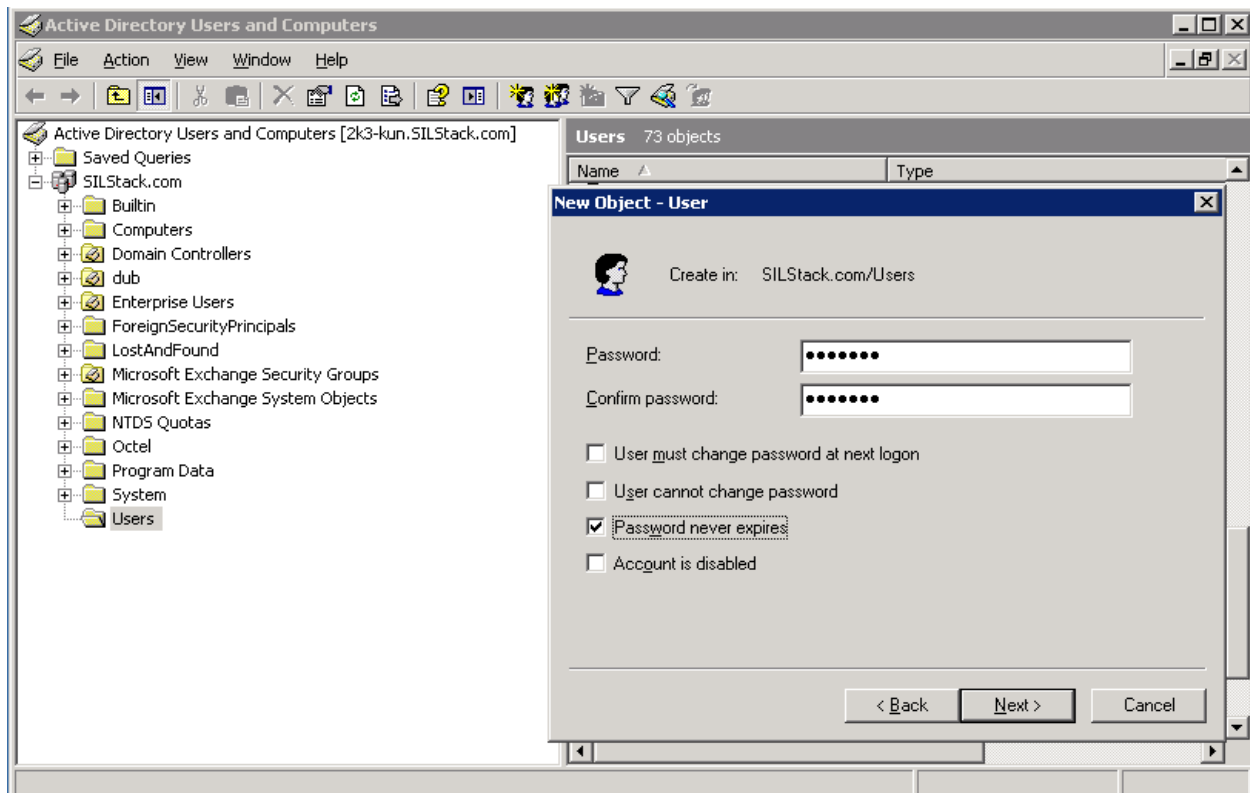


## 8.2. Administer Service Account

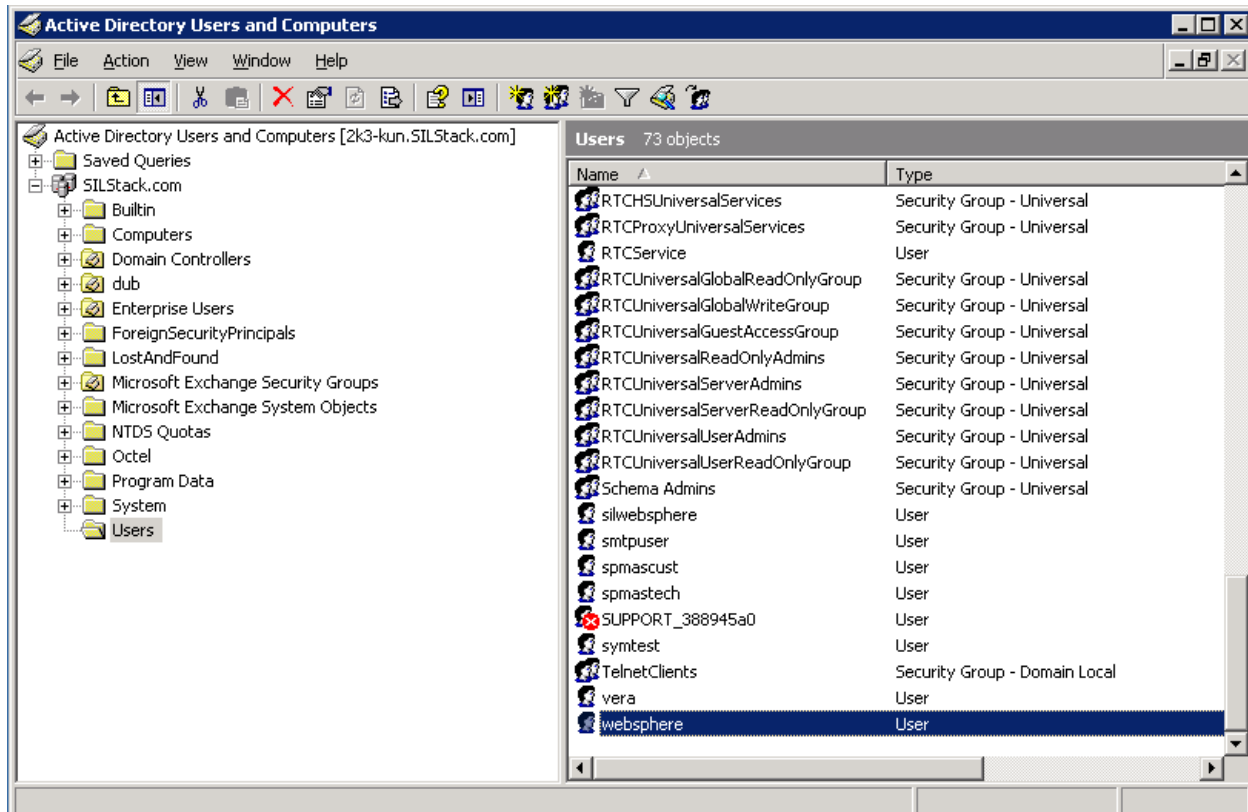
Create an administrative service account in the user domain. The administrative service account must be members of both the user and administrator security groups. In the left pane, locate the proper domain name for the network configuration, and right-click on **Users** below it. From the right-click drop-down menu (not shown below), select **New → User**. In the **New Object – User** dialog box that is displayed, enter a descriptive **Full name** and **User logon name**. Retain the default values in the remaining fields, and click **Next**.



Enter a desired password into the **Password** and **Confirm password** fields, and check the checkbox for the **Password never expires** field.

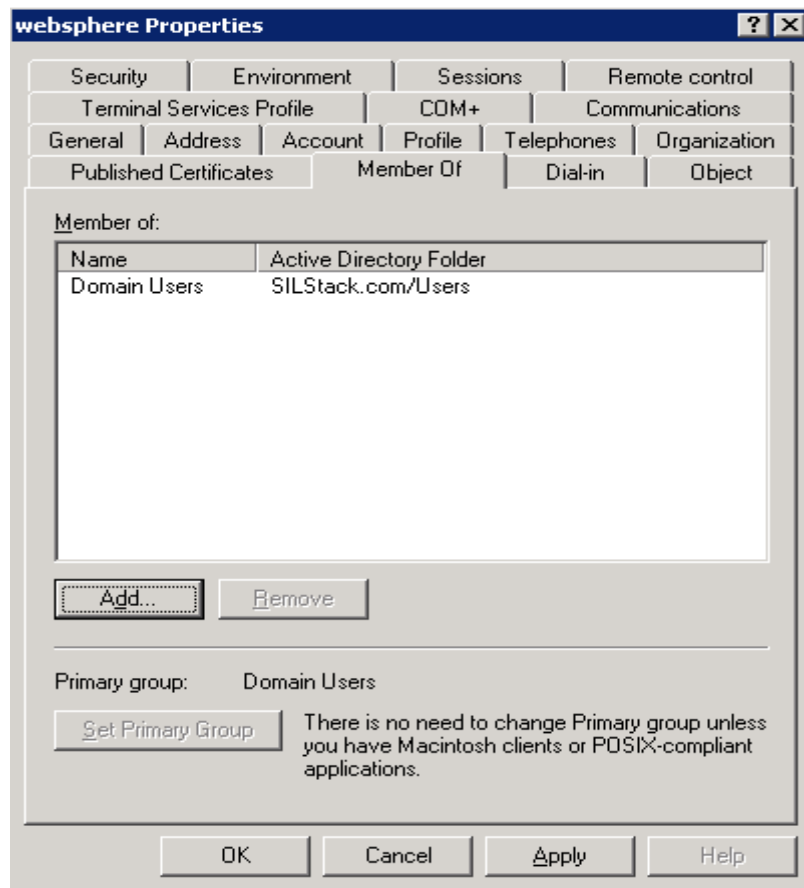


After the service account is created, the account will be listed in the right pane, as shown below. Double-click on the newly created service account, in this case **websphere**.

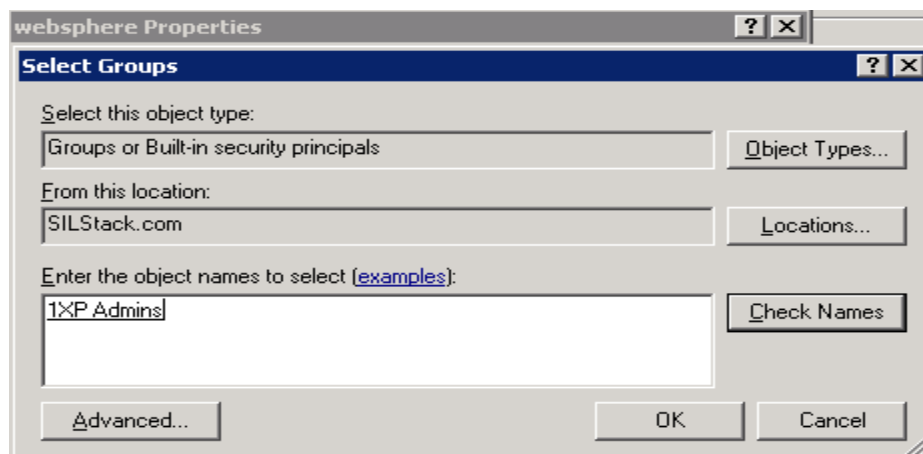




The **websphere Properties** screen is displayed. Select the **Member Of** tab, and click **Add**.

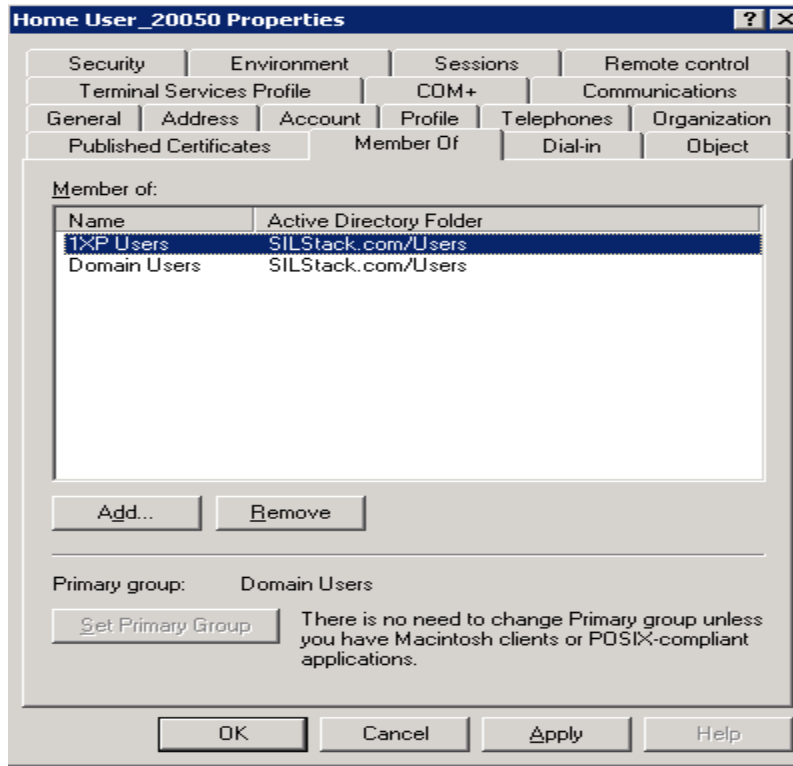


In the **Select Groups** dialog box, enter the administrator security group from **Section 8.1** in the **Enter the object names to select** section, as shown below. Click **OK**, and repeat the procedure to set the service account to also be a member of the user security group from **Section 8.1**.



### 8.3. Administer User Accounts

The user accounts in Microsoft Active Directory are used by one-X Portal for authentication and authorization, so that users can log into one-X Portal using their corporate credentials. Each Avaya one-X Portal user must be a member of at least one of the security groups created in **Section 8.1**, and are assumed to be in the same domain as the one-X Portal server. For each one-X Portal user, use the **Member Of** tab to join the user to the one-X Portal user security group created in **Section 8.1**, as shown below.



## 9. Configure Avaya one-X® Portal

This section provides the procedures for configuring one-X Portal. The procedures include the following areas:

- Verify one-X Portal license
- Administer auxiliary server
- Administer telephony server
- Administer voice messaging server
- Administer conferencing server
- Administer presence server
- Administer enterprise directory
- Restart Portal server
- Synchronize enterprise directory
- Synchronize modular messaging
- Administer system profile
- Administer users

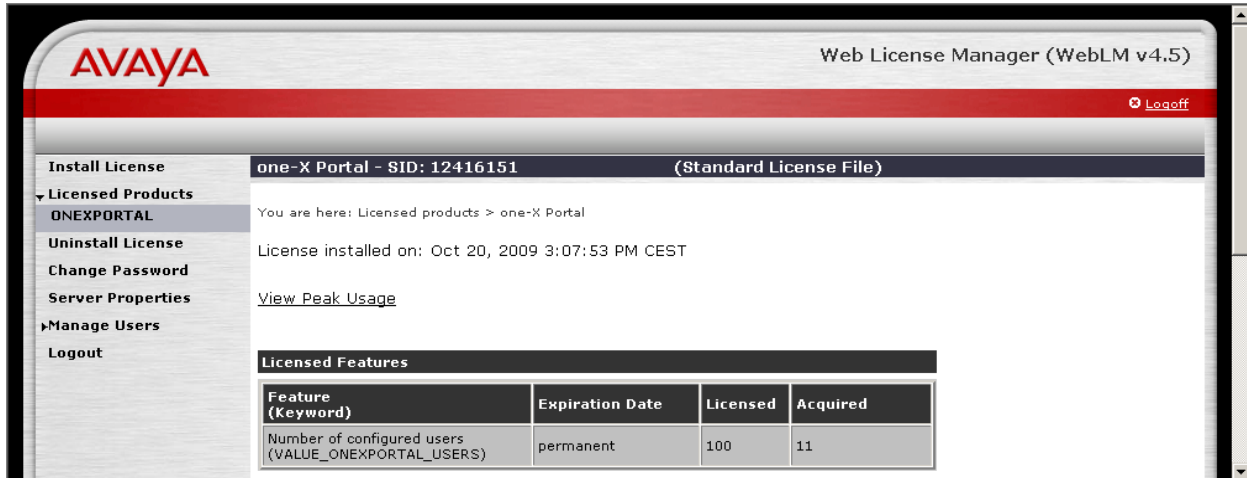
### 9.1. Verify one-X Portal License

Access the one-X Portal WebLM web-based interface by using the URL

**http://ipaddress:8080/WebLM/LicenseServer** in an Internet browser window, where **ip-address** is the IP address of the One-X Portal server. The **Logon** screen is displayed as shown below. Log on with appropriate credentials.

The image shows a web-based login interface for the Avaya Web License Manager (WebLM v4.5). At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Web License Manager (WebLM v4.5)". The main heading is "Logon". There are two input fields: "User Name:" and "Password:". To the right of the password field is a button with a right-pointing arrow. The entire interface is set against a light gray background with a subtle gradient.

In the subsequent screen that is displayed, select **ONEXPORTAL** from the left pane. In the right pane, verify that there are sufficient user licenses in the **Licensed** column, as shown below.



The screenshot shows the Avaya Web License Manager (WebLM v4.5) interface. The left pane contains a navigation menu with options: Install License, Licensed Products (selected), ONEXPORTAL (selected), Uninstall License, Change Password, Server Properties, Manage Users, and Logout. The right pane displays the license details for 'one-X Portal - SID: 12416151 (Standard License File)'. It shows the license installed on 'Oct 20, 2009 3:07:53 PM CEST' and a link to 'View Peak Usage'. Below this is a table titled 'Licensed Features' with the following data:

Feature (Keyword)	Expiration Date	Licensed	Acquired
Number of configured users (VALUE_ONEXPORTAL_USERS)	permanent	100	11

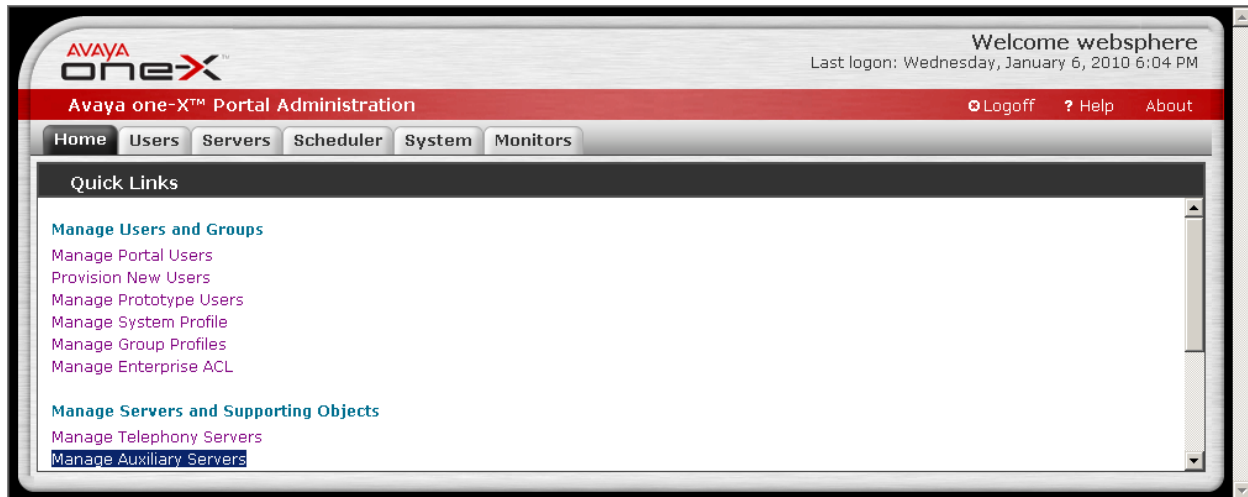
## 9.2. Administer Auxiliary Server

Access the one-X Portal web-based administration interface by using the URL **http://ipaddress/admin** in an Internet browser window, where **ip-address** is the IP address of the one-X Portal server. The **Logon** screen is displayed as shown below. Log on with appropriate credentials.

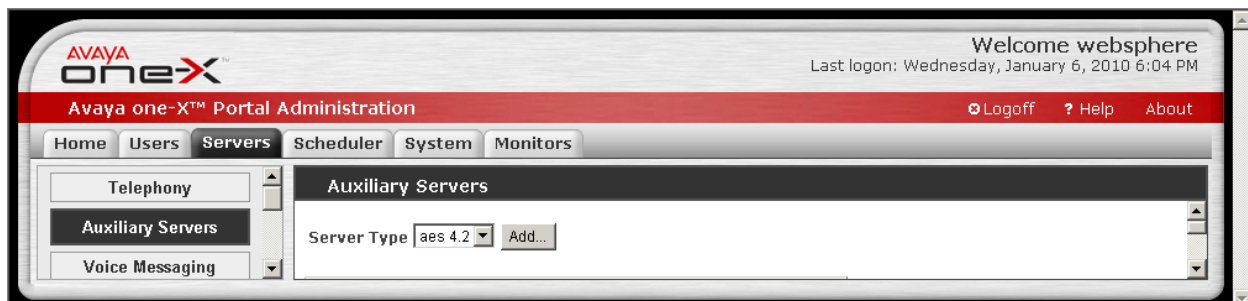


The screenshot shows the Avaya one-X Portal Administration Logon screen. It features the Avaya one-X logo at the top, followed by the text 'Avaya one-X™ Portal Administration'. Below this is a 'Please log on.' prompt. There are two input fields: 'Logon:' and 'Password:'. A 'Logon' button is located at the bottom of the form.

The **Quick Links** screen is displayed next. Select **Manage Servers and Supporting Objects** → **Manage Auxiliary Servers**.



**Auxiliary Servers** screen is displayed as shown below. For the **Server Type** field, select the corresponding version of Application Enablement Services in the network configuration from the drop-down list, and click **Add**.



The **Add Auxiliary Server Configuration** screen is displayed in the right pane. In the **Handle** field, enter a unique name for this auxiliary server. Check the **Enabled** checkbox to enable the server for the system. In the **AES Machine Name** field, enter the host name of the AES server, which can be obtained from the AES server by typing **uname -n** at the Linux command prompt. In the **DMCC** and **TSAPI** sections, enter the IP address or host name of the AES server into the **Host** field. Retain the default value in the **Port** field. For the **Login ID**, **Password**, and **Confirm** fields, enter the DMCC and TSAPI user credentials from **Section 5.4.1** and **Section 5.4.2** respectively. Click **OK** at the bottom of the screen.

The screenshot displays the 'Add Auxiliary Server Configuration' window within the Avaya one-X Portal Administration interface. The window is titled 'Add Auxiliary Server Configuration' and features a sidebar on the left with navigation links: Home, Users, Servers, Scheduler, System, and Monitors. Under the 'Servers' tab, the 'Telephony' section is expanded, showing options for Auxiliary Servers, Voice Messaging, Conferencing, Presence, Dial Plan, and Mobility. The main configuration area includes the following fields and sections:

- Type:** aes
- Version:** 4.2
- \* Handle:** SILStackAES
- Description:** (empty text area)
- Enabled:** ☒
- \* AES Machine Name:** silstackaes
- Device, Media and Call Control (DMCC):**
  - \* Host:** 135.64.186.28
  - \* Port:** 4721
  - \* Login ID:** xportalDMCC
  - \* Password:** (masked with dots)
  - \* Confirm:** (masked with dots)
- Telephony Server Application Programming Interface (TSAPI):**
  - \* Host:** 135.64.186.28
  - \* Port:** 450
  - \* Login ID:** xportalTSAPI
  - \* Password:** (masked with dots)
  - \* Confirm:** (masked with dots)

At the bottom of the window, there are four buttons: OK, Reset, Cancel, and Test.

### 9.3. Administer Telephony Server

Select **Telephony** from the left pane, to display the **Telephony Servers** screen. For the **Server Type** field, select the corresponding version of Communication Manager in the network configuration from the drop-down list, and click **Add**.



The **Add Telephony Server Configuration** screen is displayed in the right pane. Enter the following:

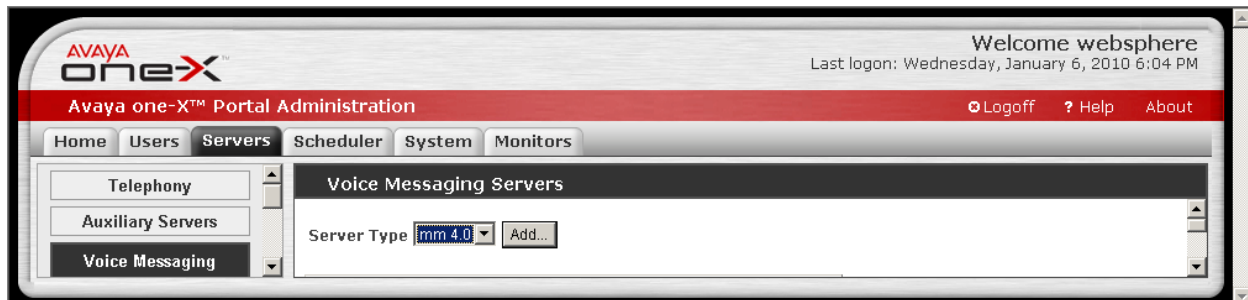
- **Handle:** A unique name for this telephony server.
- **Enabled:** Check the checkbox to enable the server for the system.
- **PBX Name for AES:** Existing AES switch connection name as shown in **Section 5.2**.
- **EC500 Enable Code:** Enhanced EC500 Activation access code from **Section 4.3**.
- **EC500 Disable Code:** Enhanced EC500 Deactivation access code from **Section 4.3**.
- **EC500 Modify Code:** EC500 Self-Administration Access Code from **Section 4.3**.
- **Host:** IP address or host name of Communication Manager that is accessible by the VoIP clients to establish H.323 connections.

Add Telephony Server Configuration	
Type	cm
Version	5.0
* Handle	SILStackCM
Description	
Enabled	<input checked="" type="checkbox"/>
* PBX Name for AES	silstackCM
* EC500 Enable Code	*7
* EC500 Disable Code	*5
* EC500 Modify Code	*6
* CLAN Host	135.64.186.6

For the **AES Servers** section, select the AES auxiliary server name from **Section 8.3** in the **Available** box, and click **Add** to move the selection to the **Selected** box as shown below. Click **OK** at the bottom of the screen.

## 9.4. Administer Voice Messaging Server

Select **Voice Messaging** from the left pane, to display the **Voice Messaging Servers** screen. For the **Server Type** field, select the corresponding version of Modular Messaging in the network configuration from the drop-down list, and click **Add**.





The **Add Voice Messaging Server Configuration** screen is displayed in the right pane.

- In the **Handle** field, enter a unique name for this voice messaging server.
- Check the **Enabled** checkbox to enable the server for the system.
- In the **Mail Domain** field, enter the domain name of the network configuration, in this case **SILStack.com**. Retain the default values in the remaining fields.
- In the **IMAP** section, enter the IP address or host name of the Avaya MSS server into the **Host** field.
- For the **Port** field, enter the IMAP4 SSL port number from **Section 6.1**.
- For the **Login ID**, **Password**, and **Confirm** fields, enter the one-X Portal trusted server credentials from **Section 6.3**.
- Retain the check in the **Secure Port** checkbox.

#### Add Voice Messaging Server Configuration

Type	mm
Version	4.0
* Handle	SILstackMM
Description	
Enabled	<input checked="" type="checkbox"/>
Initial Number of Server Connections	50
Max Number of Server Connections	200
Client Connections Increment	2
Users Per Client Connection	10
Messages Temp Directory	/home/appsvr/silstackmsgworkdir
Temp Purge Interval (minutes)	60
* Mail Domain	SILStack.com

Dial Plan No Dial Plans are configured

#### Internet Message Access Protocol (IMAP)

* Host	135.64.186.35
* Port	993
* Login ID	oneXPortal
* Password	*****
* Confirm	*****
Secure Port	<input checked="" type="checkbox"/>

#### Simple Mail Transport Protocol (SMTP)

Scroll down the right pane to display the **SMTP** and **LDAP** sections.

- In the **SMTP** section, enter the IP address or host name of the Avaya MSS server into the **Host** field.
- For the **Port** field, enter the SMTP port number from **Section 6.1**.
- For the **Login ID**, **Password**, and **Confirm** fields, enter the one-X Portal trusted server credentials from **Section 6.3**.
- In the **LDAP** section, enter the IP address or host name of the Avaya MSS server into the **Host** field.
- For the **Port** field, enter the LDAP port number from **Section 6.1**.
- For the **Login ID**, **Password**, and **Confirm** fields, enter the One-X Portal trusted server credentials from **Section 6.3**.
- Click **OK**.

#### Simple Mail Transport Protocol (SMTP)

* Host	<input type="text" value="135.64.186.35"/>
* Port	<input type="text" value="25"/>
* Login ID	<input type="text" value="oneXPortal"/>
* Password	<input type="password" value="••••••"/>
* Confirm	<input type="password" value="••••••"/>
Secure Port	<input type="checkbox"/>

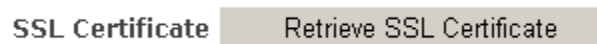
#### Lightweight Directory Access Protocol (LDAP)

* Host	<input type="text" value="135.64.186.35"/>
* Port	<input type="text" value="389"/>
* Login ID	<input type="text" value="oneXPortal"/>
* Password	<input type="password" value="••••••"/>
* Confirm	<input type="password" value="••~•••"/>
Secure Port	<input type="checkbox"/>

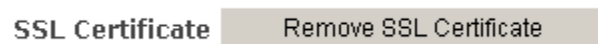
After the Voice Messaging Server was added, go back to the **Voice Messaging Servers** window. Click on **SILStackMM** entry.



A new button **Retrieve SSL Certificate** is shown in the **Voice Messaging Servers** window.



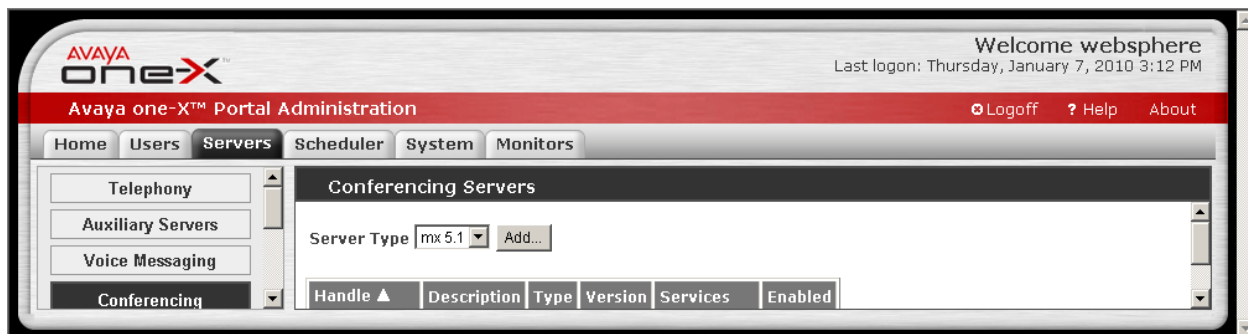
Click on the button and it will change to **Remove SSL Certificate** button.



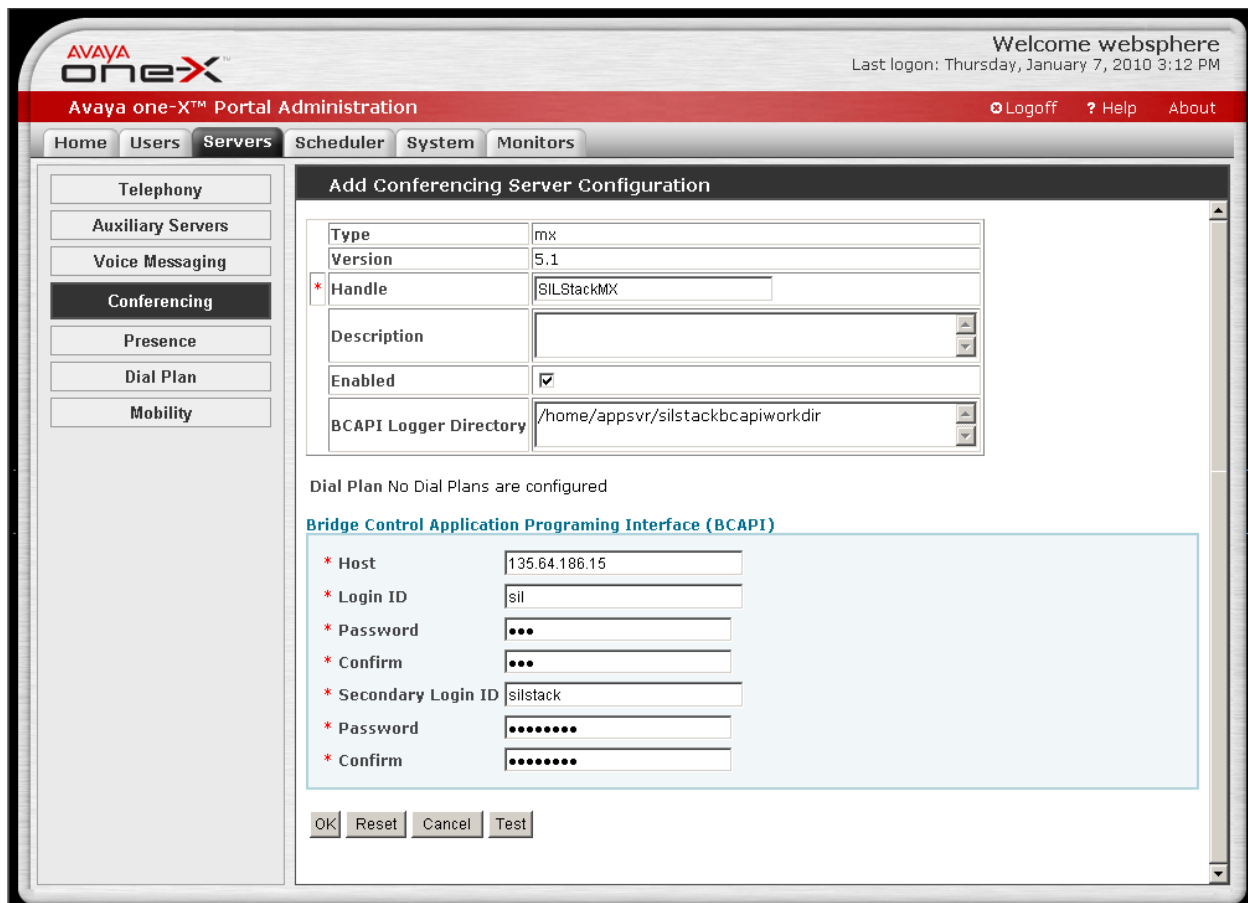
Click **Save** button (not shown) to save the changes. For more details regarding the SSL Certificate, refer to [7] in **Section 13**.

## 9.5. Administer Conferencing Server

Select **Conferencing** from the left pane, to display the **Conferencing Servers** screen. For the **Server Type** field, select the corresponding version of MX in the network configuration from the drop-down list, and click **Add**.

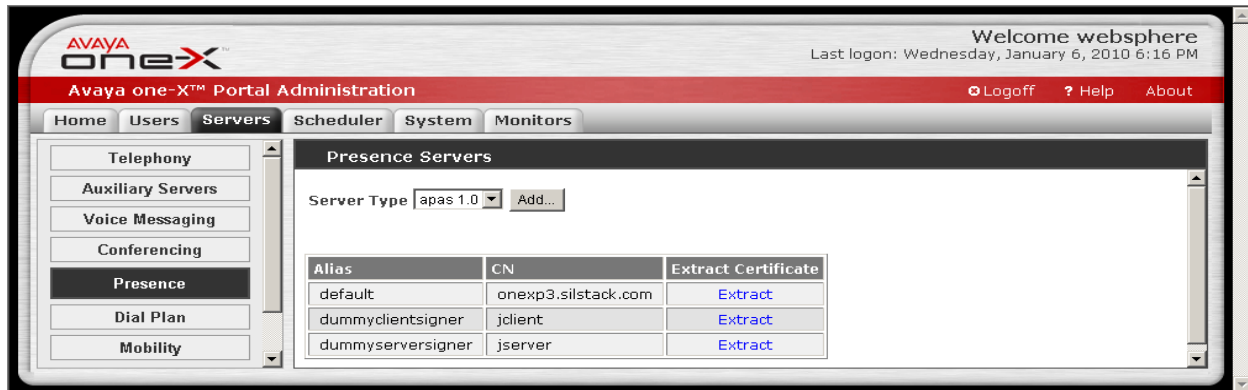


The **Add Conferencing Server Configuration** screen is displayed in the right pane. In the **Handle** field, enter a unique name for this conferencing server. Check the **Enabled** checkbox to enable the server for the system. Retain the default values in the remaining fields. In the **BCAPI** section, enter the IP address or host name of the Avaya MX server in the **Host** field. Enter the credentials of the two operators from **Section 7.1** in the remaining fields. Scroll down to the bottom of the screen and click **OK**.

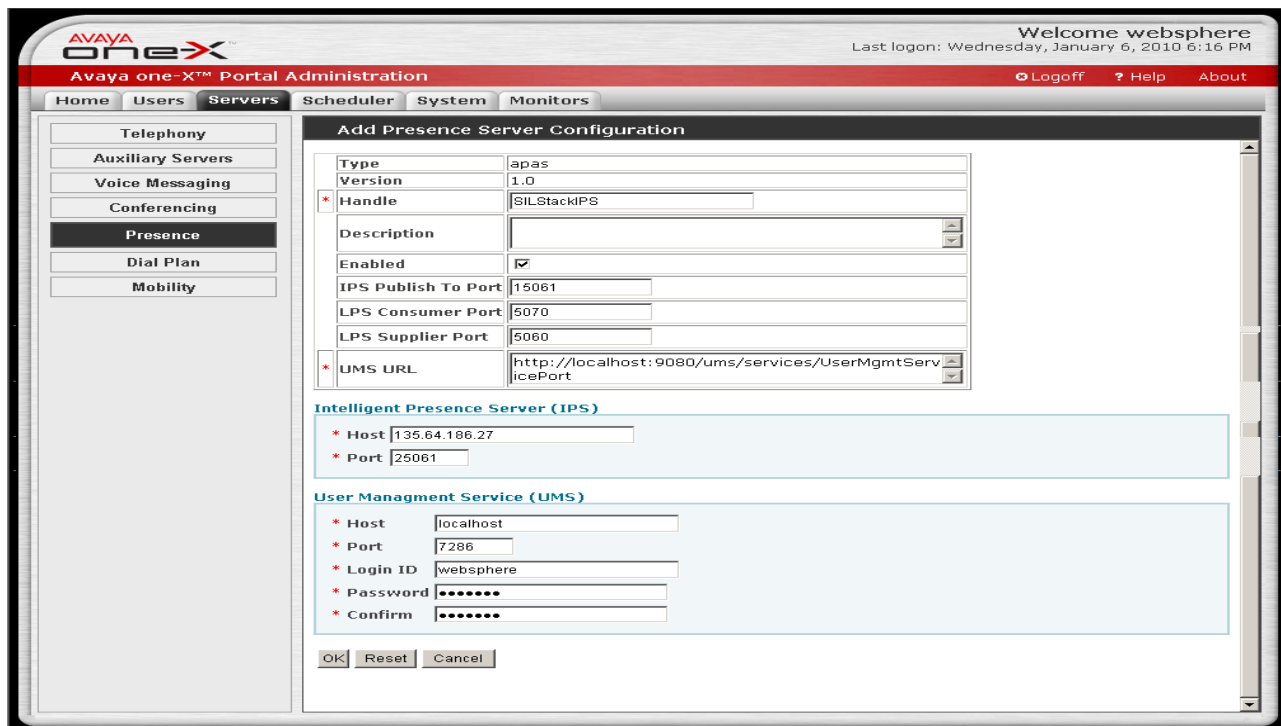


## 9.6. Administer Presence

Select **Presence** from the left pane, to display the **Presence Servers** screen. For the **Server Type** field, select the corresponding version of Presence in the network configuration from the drop-down list, and click **Add**.

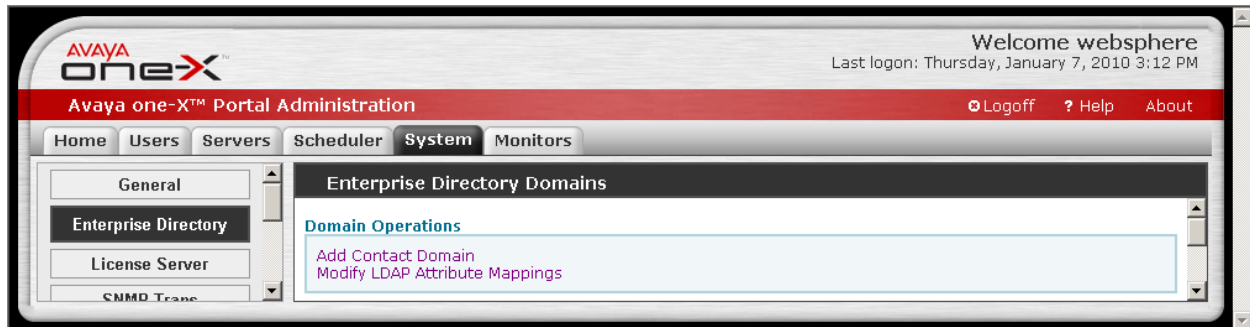


The **Add Presence Server Configuration** screen is displayed in the right pane. In the **Handle** field, enter a unique name for this conferencing server. Check the **Enabled** checkbox to enable the server for the system. Retain the default values in the remaining fields. In the **Intelligent Presence Server (IPS)** section, enter the IP address or host name of the Avaya Presence server in the **Host** field. In the **User Management Service (UMS)** section, enter **localhost** in the **Host** field. Enter the administrative service account credentials from **Section 8.2** into the **Login ID**, **Password**, and **Confirm** fields. Scroll down to the bottom of the screen and click **OK**.

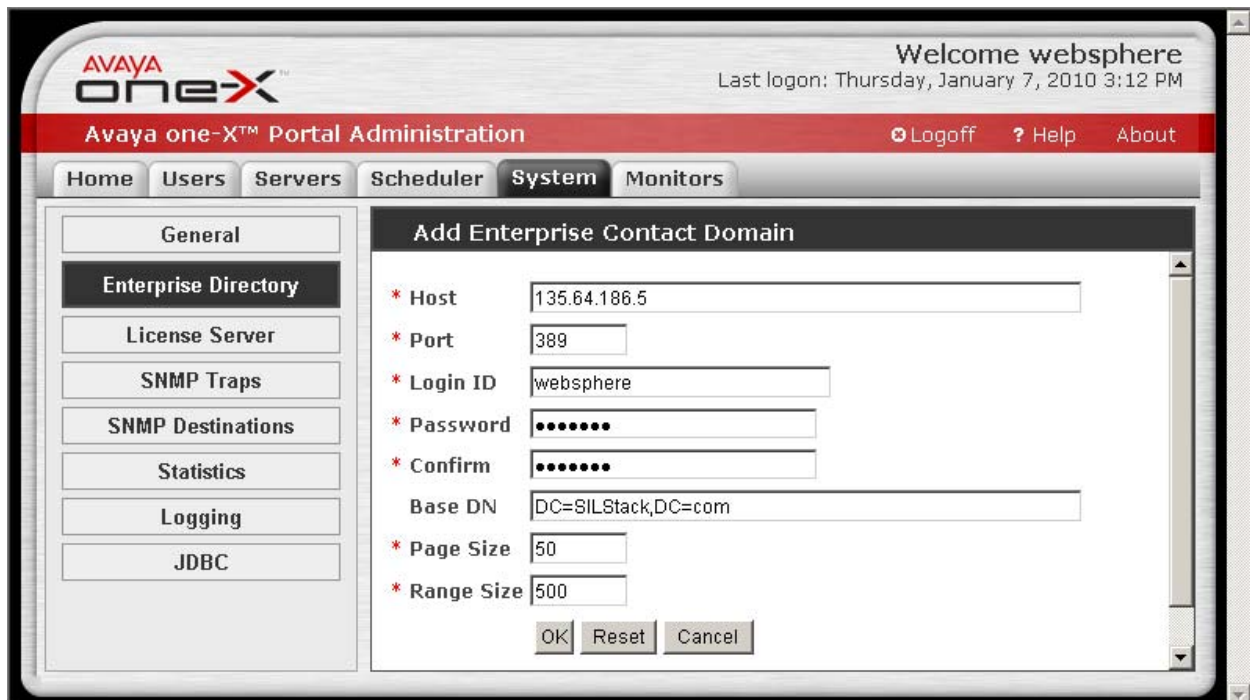


## 9.7. Administer Enterprise Directory

Select the **System** tab from the top, followed by **Enterprise Directory** in the left pane. The **Enterprise Directory Domains** screen is displayed. Click **Add Contact Domain**.

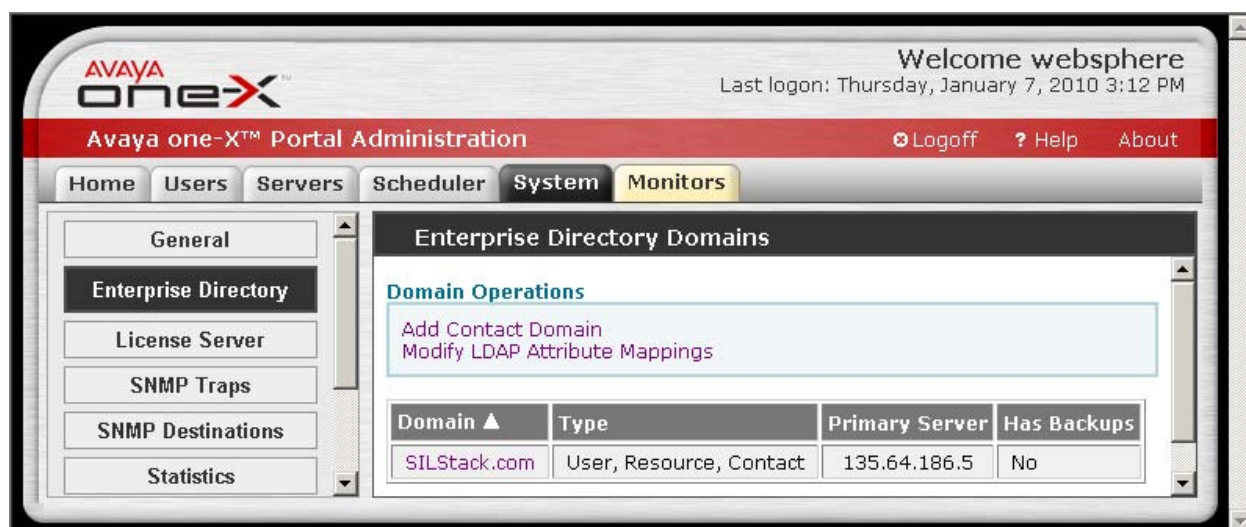


The **Add Enterprise Contact Domain** screen is displayed next. Enter the domain name for the network configuration into the **Host** field. Enter the administrative service account credentials from **Section 8.2** into the **Login ID**, **Password**, and **Confirm** fields. Retain the default values in the remaining fields, and click **OK**.

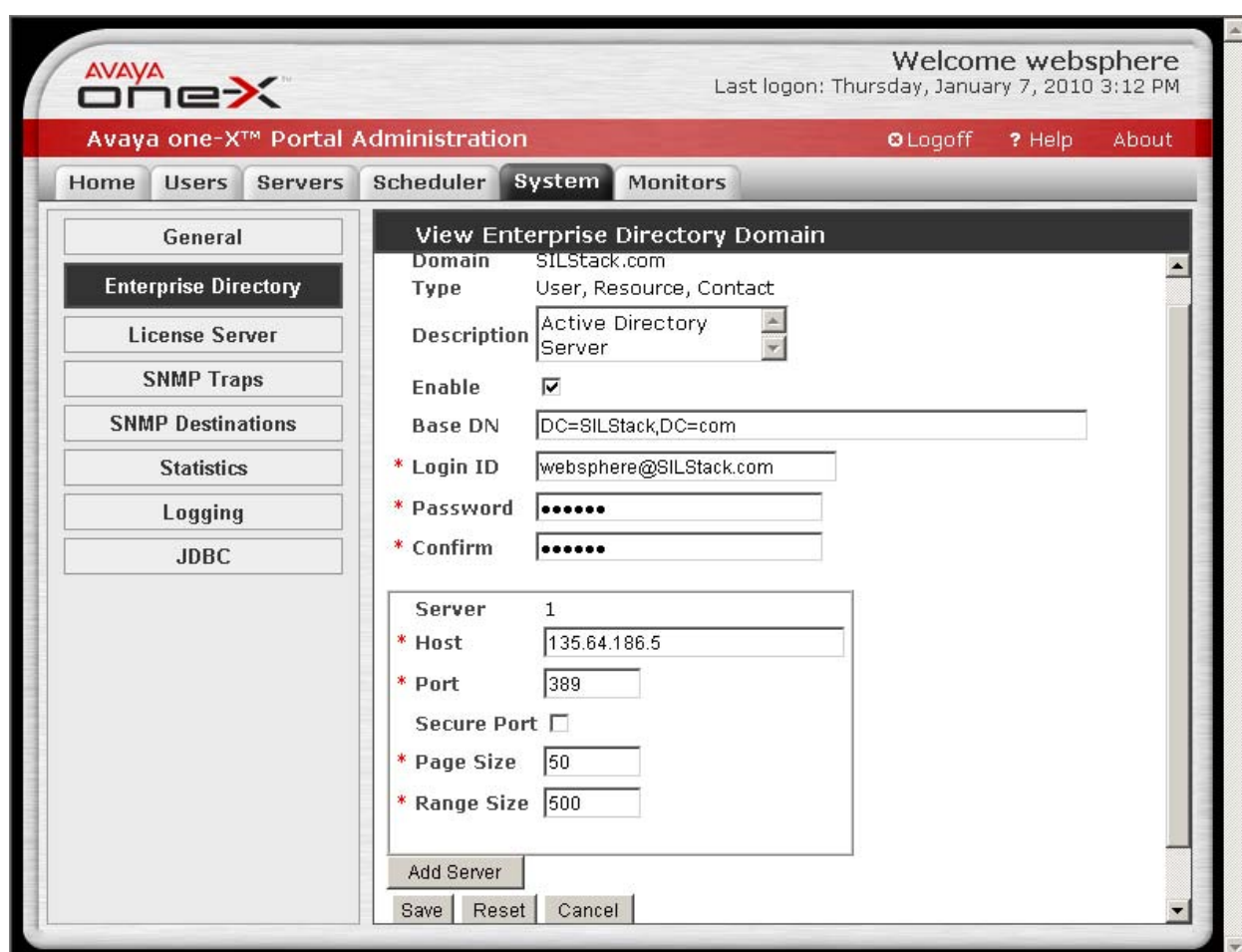




The **Enterprise Directory Domains** screen is displayed again. Click on the **Domain** field value for the newly created enterprise domain, in this case **SILStack.com**.



The **View Enterprise Directory Domain** screen is displayed. Click **Save** button.

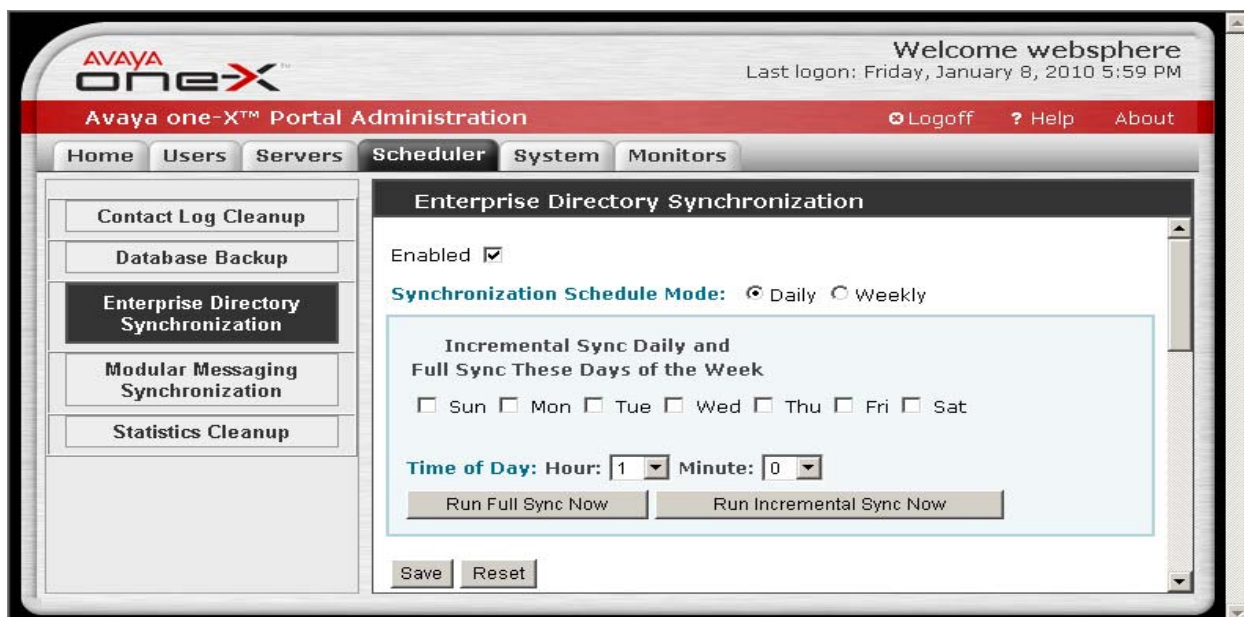


## 10. Restart Avaya one-X® Portal Server

From the one-X Portal server's Linux shell, restart the application using the stopServer.sh and startServer.sh commands. Refer to document [7] in **Section 13** for more details.

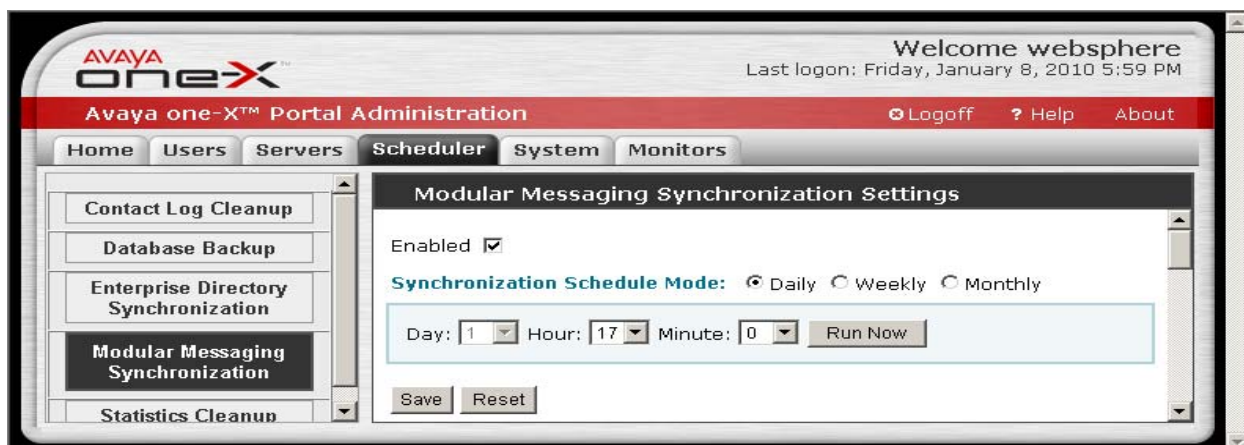
### 10.1. Synchronize Enterprise Directory

Select the **Scheduler** tab from the top, followed by **Enterprise Directory Synchronization** in the left pane. Click **Run Full Sync Now** to synchronize immediately with Microsoft Active Directory.



### 10.2. Synchronize Modular Messaging

Select **Modular Messaging Synchronization** from the left pane. Click **Run Now** to synchronize immediately with Modular Messaging.





### 10.3. Administer System Profile

Select the **Users** tab from the top, followed by **System Profile** in the left pane. The system profile contains a collection of properties that can be applied to users and groups. Set the values as desired for each property. In the interoperability testing, the **VOIP** property was changed to **Enabled** on the system profile, and this system profile was applied to all users. Note that group profiles may be used to create additional combinations of property settings. Click **Save** at the bottom of the screen (not shown below).

The screenshot shows the Avaya one-X Portal Administration interface. The top navigation bar includes 'Home', 'Users', 'Servers', 'Scheduler', 'System', and 'Monitors'. The left sidebar lists 'Portal Users', 'Unprovisioned Users', 'Prototype Users', 'System Profile' (selected), 'Group Profiles', and 'Enterprise ACL'. The main content area is titled 'System Profile' and contains a table with the following data:

Property	Service	Default	Value Range	System Value
Continuous extension monitoring	CM Service	Disabled	Boolean	Accept Default   Enabled
Telecommuter	CM Service	Enabled	Boolean	Accept Default   Enabled
<b>VOIP</b>	CM Service	Disabled	Boolean	Set System Value   Enabled
Mobility	CM Service	Enabled	Boolean	Accept Default   Enabled
Send DTMF for calls	CM Service	Enabled	Boolean	Accept Default   Enabled
SIP Station	CM Service	Disabled	Boolean	Accept Default   Enabled
Forward voice messages to inbox	MM Service	Enabled	Boolean	Accept Default   Enabled

### 10.4. Administer Unprovisioned Users

Select **Unprovisioned Users** from the left pane, and click **Search** in the right pane.

The screenshot shows the Avaya one-X Portal Administration interface with the 'Unprovisioned Users' section selected. The left sidebar lists 'Portal Users', 'Unprovisioned Users' (selected), 'Prototype Users', 'System Profile', 'Group Profiles', and 'Enterprise ACL'. The main content area is titled 'Unprovisioned Users' and contains the following sections:

**Direct To Enterprise Directory**

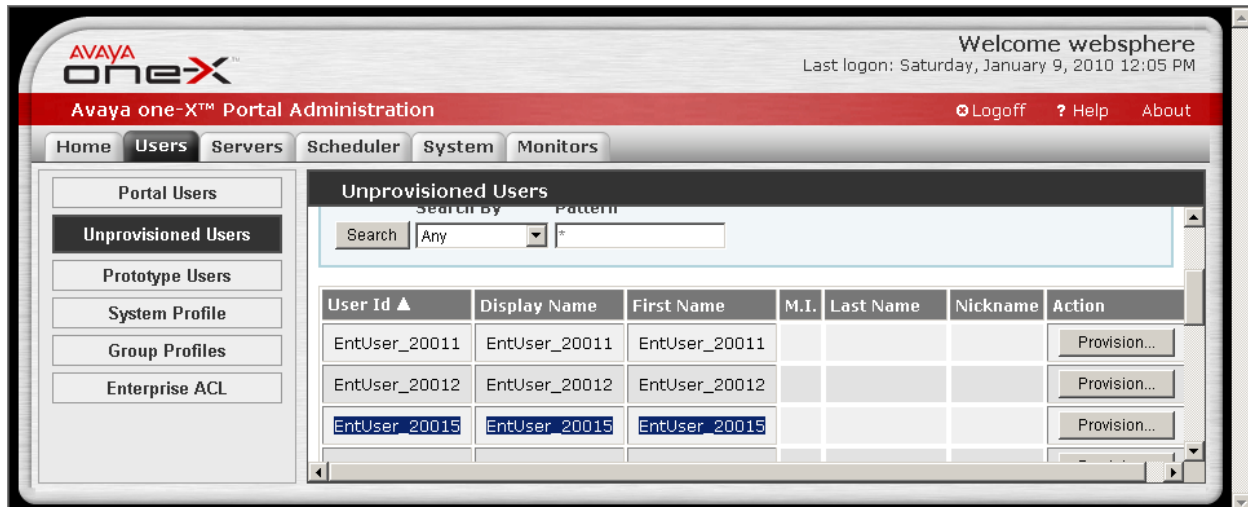
User Id  Provision...

**Users Found During Enterprise Directory Synchronization**

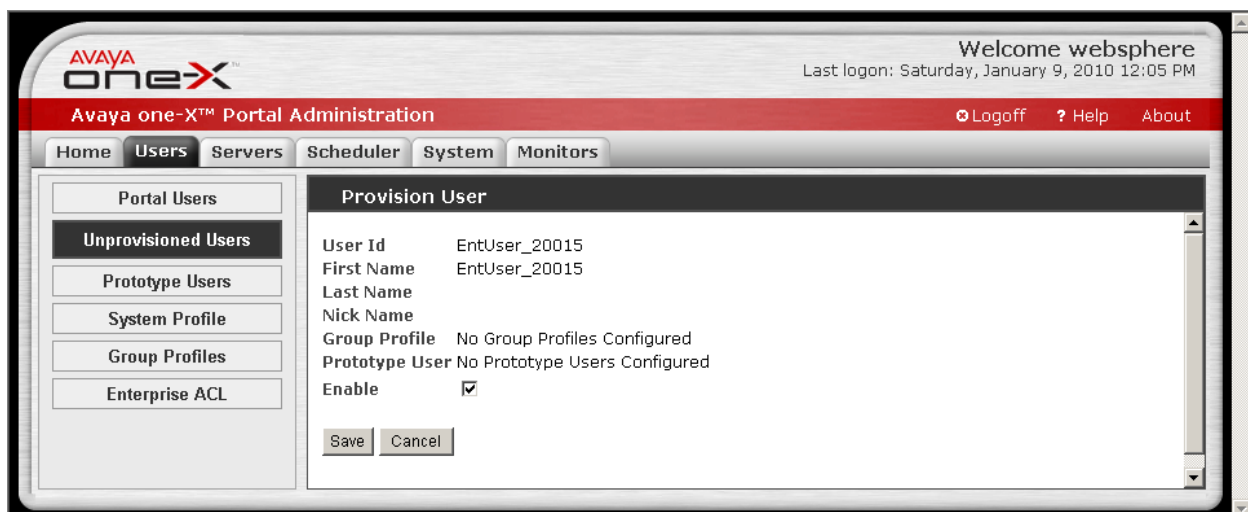
Search By  Pattern

Search

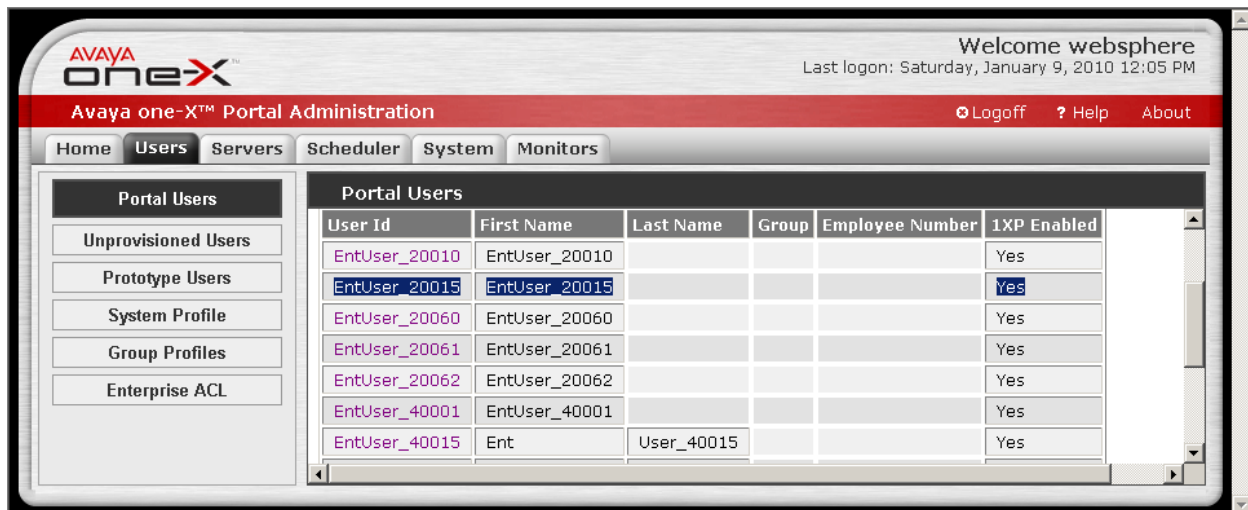
The **Unprovisioned Users** screen is updated with a list of un-provisioned users picked up from Microsoft Active Directory. Click the **Provision** button corresponding to an unprovisioned user, in this case **EntUser\_20015**.



The **Provision User** screen is displayed in the right pane, as shown below. If the network configuration uses a group profile and prototype users, then select the proper values from the field drop-down lists (not used in the interoperability testing). Retain the check in the **Enable** checkbox, and click **Save**. This will move the user out of the un-provisioned state. Repeat this procedure for the remaining un-provisioned users.

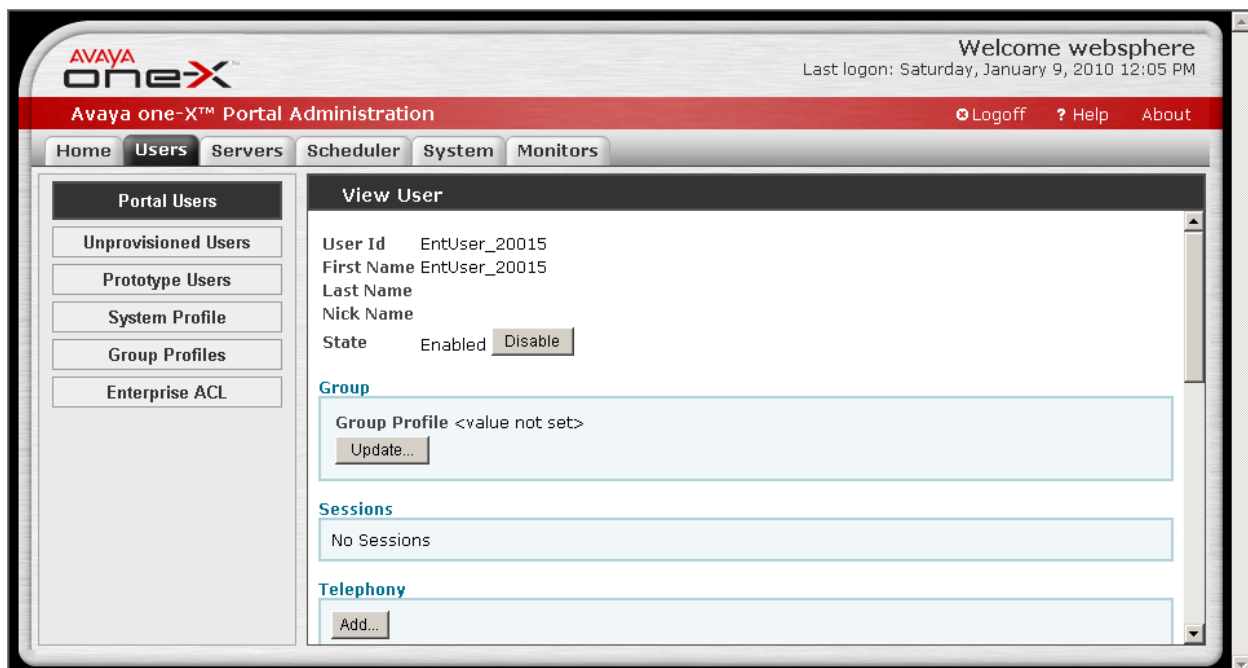


Select **Portal Users** from the left pane. In the right pane, click **Search** to obtain a listing of all Portal users. Click on the **User Id** of the previously provisioned user, in this case **EntUser\_20015**.



## 10.5. Administer Portal Users

The **View User** screen is displayed in the right pane. Click the **Add** button in the **Telephony** section.



The **Add Resource** screen is displayed in the right pane. For the **Server** field, select the telephony server handle from **Section 9.3**. Enter the user name into the **Display Name** field. For the **Extension**, **Password**, and **Confirm** fields, enter the user telephone extension and security code from **Section 4.7**. Click **OK**.

The **View User** screen is displayed again with the administered values in the **Telephony** section. Scroll down the right pane to click the **Add** button in the **Voice Messaging** section.

#### Telephony

Server	SILStackCM
Display Name	EntUser_20015
Display Address	<value not set>
Extension	20015
Password	<value is set>

Property	Value	Source
Send DTMF for calls	Enabled	System Default
SIP Station	Disabled	System Default
Continuous extension monitoring	Disabled	System Default
Telecommuter	Enabled	System Default
VOIP	Enabled	System Profile
Mobility	Enabled	System Default

Update...

#### Voice Messaging

Add...

The **Add Resource** screen is displayed in the right pane. For the **Server** field, select the voice messaging server handle from **Section 9.4**. Enter the user name into the **Display Name** field. For the **Mailbox**, **Password**, and **Confirm** fields, enter the user mailbox number and password from **Section 6.4**. Click **OK**.

The **View User** screen is displayed again with the administered values in the **Voice Messaging** section. Scroll down the right pane and click the **Update** button in the **Conferencing** section.

The **Update Resource** screen is displayed in the right pane. For the **Server** field, select the conferencing server handle from **Section 9.5**. Enter the user name into the **Display Name** field. For the **Moderator Code**, **Confirm**, and **Bridge Number** fields, enter the pre-existing Meeting Exchange bridge number and moderator code. Click **Save**.

The screenshot shows the Avaya one-X Portal Administration interface. The top navigation bar includes 'Home', 'Users', 'Servers', 'Scheduler', 'System', and 'Monitors'. The 'Users' tab is active. On the left, a sidebar menu lists 'Portal Users', 'Unprovisioned Users', 'Prototype Users', 'System Profile', 'Group Profiles', and 'Enterprise ACL'. The main content area is titled 'Update Resource' and contains the following fields:

Server	SILStackMX		
Display Name	EntUser_20015		
Display Address			
Pin Code		Confirm	
Moderator Code	.....	Confirm	.....
Participant Code			
Bridge Number	235421		
Bridge Number Backup			
Allow Call Me	<input checked="" type="checkbox"/>		

At the bottom of the form are three buttons: 'Save', 'Reset', and 'Cancel'.

The **View User** screen is displayed again with the administered values in the **Conferencing** section. Scroll down the right pane and click the **Add** button in the **Presence Information** section.

The **Update Resource** screen is displayed in the right pane. For the **Server** field, select the presence server handle from **Section 9.6**. Enter the user name into the **Display Name** field. For the **SES ID**, **Password** and **Confirm** fields, enter **presence**. Click **Save**.



## 11. Verification Steps

This section provides the steps that can be performed to verify proper configuration for Avaya one-X Portal.

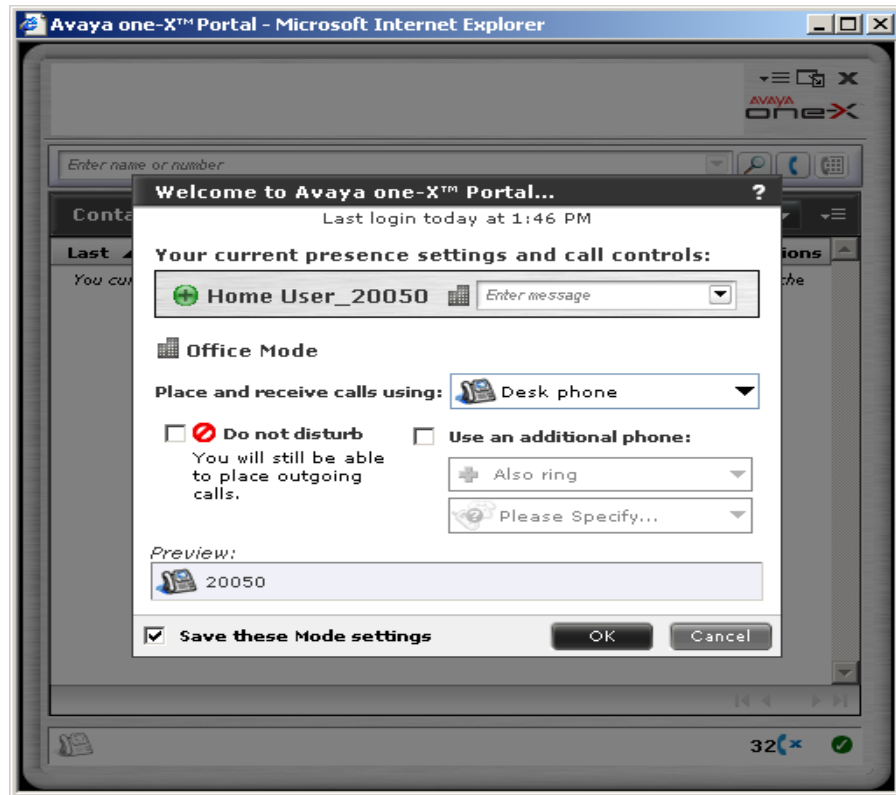
### 11.1. Verify Telephony

From the user desktop, launch an Internet browser window and access the one-X Portal web-based application by using the URL **http://ip-address**, where **ip-address** is the IP address of the one-X Portal server. Log in with the user's corporate credentials discussed in **Section 8.3**. In this case, **User\_20050** is used.





In the **one-X Portal** pop-up screen below, retain the default selection to use the desk phone and click **OK**.



Make a call to the user. Verify that the call is ringing on the user desk phone, and that the Communications portlet shows the calling party information, along with the green **Answer** and red **Hangup** icons. Click the green **Answer** button to answer the call.



Verify that the user is connected to the caller with two-way talk path, and that the icons for the user are updated to Green **Hold** and Red **Hang Up** in the Communications portlet.




Assume the user would like to conference in **User\_20090**, and needs to look up the telephone number. Click on **Contacts** toward the bottom of the screen to expand the portlet. In the **Search** box, enter **User\_200** as a partial string match for users starts with **User\_200**. The portlet is updated with all matching entries from Microsoft Active Directory. Click on the down-arrow for the desired entry to view additional actions.

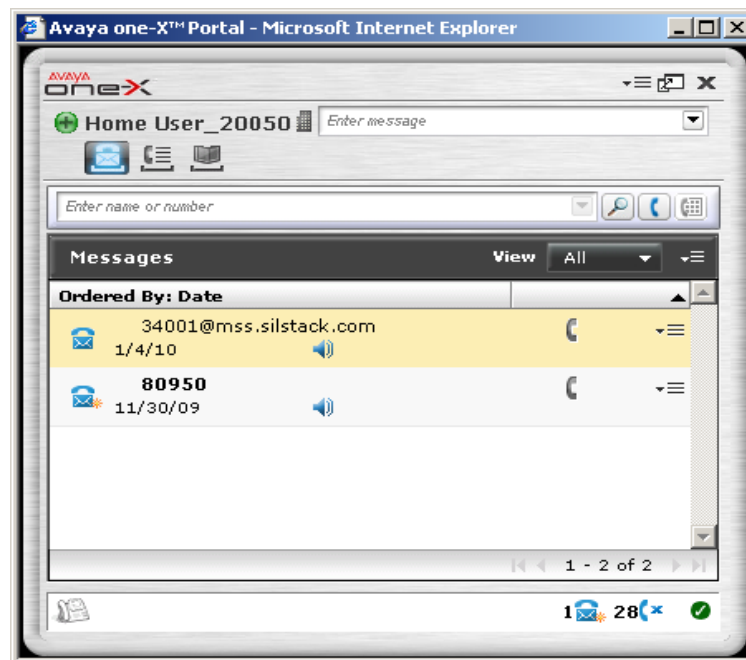



The pop-up box for additional actions is displayed, and shows **Conference** and **Transfer** at the top of the list, as the application knows that there is an active call.

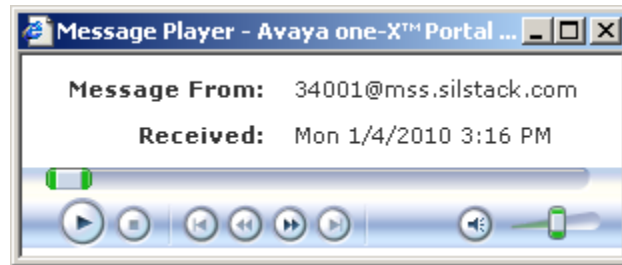


## 11.2. Verify Messaging





Make a call to the user. Do not answer the call and let it cover to Avaya Modular Messaging. Leave a voice message for the user. Click on the  message icon. Verify that the **Message** portlet for the user shows voice messages.




Click on the  button next to the voice message entry. Verify that the **Message Player – Avaya one-X** pop-up screen is displayed, and that the voice message is played automatically.

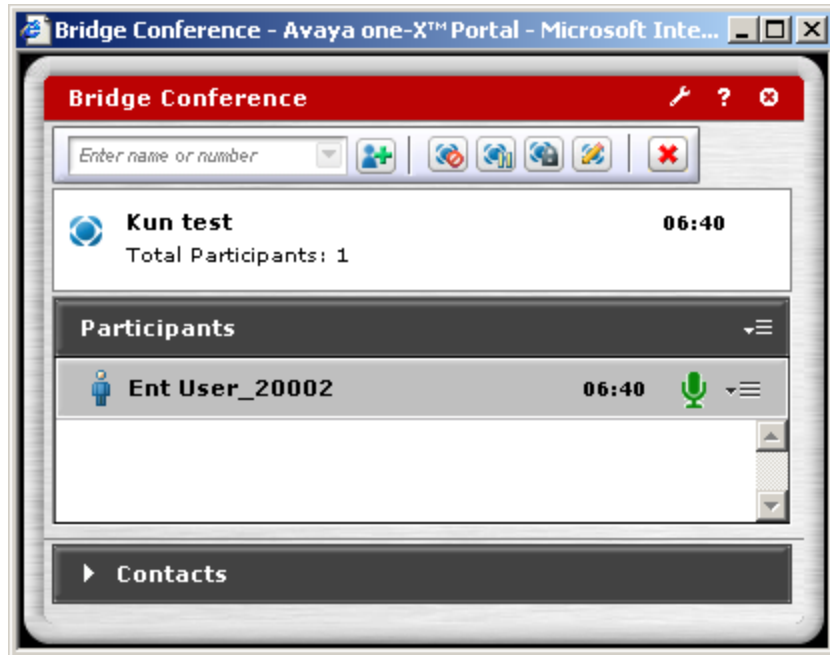


### 11.3. Verify Conferencing

Click the  icon toward the top of the screen, to launch an unattended bridge conference as the moderator. Verify that the Communications portlet for the user shows three icons. The three icons **Mute Me** , **Show**  and **Exit Conference**  are for conference management and control.



After joining the bridge conference, verify that the **Bridge Conference** portlet pops up. Also verify that toward the top of the portlet is a series of icons for conference control, and that the **Participants** section shows the name of the user along with the  image indicating moderator permissions.



## 12. Conclusion

These Application Notes provides a sample configuration for one-X Portal to support Avaya Mobile Worker Solution. The one-X Portal is a browser-based interface to Avaya telephony, mobility, messaging, conferencing and presence services provided by Communication Manager, Application Enablement Services, Avaya Modular Messaging, Avaya Meeting Exchange Enterprise and Presence Services.

## 13. Additional References

This section references the product documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 5.0, May 2009, available at <http://support.avaya.com>.
- [2] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 7, May 2009, available at <http://support.avaya.com>.
- [3] *Avaya Extension to Cellular and Off-OBX Station (OPS) Installation and Administration Guide*, Document 210-100-500, Issue 9, June 2005, available at <http://support.avaya.com>.
- [4] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Document ID 02-300357, Issue 11, Nov 2009, available at <http://support.avaya.com>.
- [5] *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.2 Installation and Upgrades*, Release 5.2, Nov 2009, available at <http://support.avaya.com>.
- [6] *Administering Meeting Exchange Servers*, Document 04-603419, Issue 1, Nov 2009, available at <http://support.avaya.com>.
- [7] *Implementing Avaya one-X Portal*, Release 5.2, Nov 2009, available at <http://support.avaya.com>.
- [8] *Intelligent Presence Server Installation and Configuration Guide SP2*, Release 1.0, Document 02-602753, Release 1.0, May 2009, available at <http://support.avaya.com>

---

**©2010 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabinotes@list.avaya.com](mailto:interoplabinotes@list.avaya.com)