IP Office Platform R12.0

Administering Avaya one-X Portal for IP Office

15-601139 Issue 19a - (Wednesday, April 17, 2024)

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

Documentation disclaimer
"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

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

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.
"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses
The Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components
The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider
WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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

Avaya Toll Fraud intervention
If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities
Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.
Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

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

Contents

6. Document History

Chapter 1.

one-X Portal for IP Office Administration

1. one-X Portal for IP Office Administration

In addition to normal operation by end user, the one-X Portal for IP Office web interface is also used for a number of administration and maintenance functions. This documentation covers the use of those administration menus.

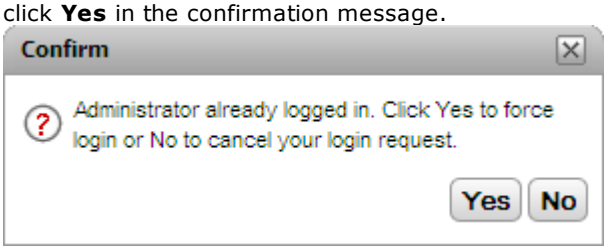
1.1 Log in

Access to the administration menus for one-X Portal for IP Office is via web browser in the same way as user access but with ***?admin=true*** added to the URL. Only one user can login as admin at a time.

- By default, the one-X Portal for IP Office server uses "referred authentication". That means that the portal administration access rights are assigned to IP Office service users configured in the security settings of the IP Office service running on the same server.
- If "referred authentication" is disabled on the IP Office, the portal uses its own local ***Administrator*** account for access to the administration menus, and a local ***Superuser*** account for access to the AFA menus. The passwords for these local accounts are stored by the portal service and are not part of the IP Office security settings.

To log in:

1. In your web browser, enter the URL in the form of ***https://<server name>:<server port>/onexportal-admin.html*** where:
   - ***<server name>*** is the name or the IP address the one-X Portal for IP Office server.
   - ***<server port>*** is the port number used by the one-X Portal for IP Office. This is 9443 for HTTPS access.
   - You can use ***http://*** rather than ***https://*** and ***8080*** as the port if unsecure access has been configured. See Protocol 33.
   - Alternatively, from the normal user login menu, select **Administrator Login**.
2. Enter the one-X Portal for IP Office administrator name and password as configured during installation.
   - If there is already a session connected as an administrator, the following confirmation message box appears. To end the session of the logged in administrator and log in with your administrator credentials, click **Yes** in the confirmation message.

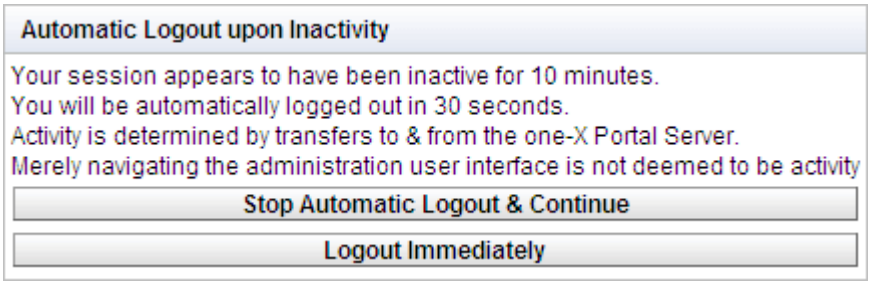


3. Click **Login**.

1.2 Log out

The **Logout** option at the top right of the one-X Portal for IP Office administration menus can be used to log out.

In addition to logging out manually, you will also be prompted after 10 minutes whether you want to remain logged in. Failing to respond will cause you to be automatically logged out.



Chapter 2.
Admin Menus

2. Admin Menus

The one-X Portal for IP Office administration menu provides a range of options for monitoring and configuring the one-X Portal for IP Office application.

Menu	Sub-Menu	Description
Health	Dashboard 12	Shows a summary of the server status.
	Component Status 13	List the last status change of the server components.
	IM/Presence server status 13	Shows the current status of the instant messaging server component.
	Resiliency 14	Display the status of the servers in a resilient configuration. *(IP Office Server Edition only)*
	Key Recent Events 15	View the last 20 events on the server.
	Active Sessions 16	Show how many sessions are cached by one-X Portal for IP Office.
	Environment 16	Show a summary of the one-X Portal for IP Office server PC.
Configuration	Providers 17	View and edit the providers.
	Users 22	View and edit user one-X Portal for IP Office settings.
	CSV 23	Export the user directory and system directory.
	Branding 23	Specify the text that is displayed on the one-X Portal for IP Office pages after a user has logged in.
	IM/Presence 24	Monitor the status of the IM/Presence server as a Administrator.
	Exchange service 25	Configure the Exchange server to obtain user presence information.
	SMTP Configuration 26	Set the email details used for emailing conference notifications.
	Conference Dial-in 27	Set the fixed text to include in scheduled conference notifications.
	Resiliency 28	Used on an IP Office Application Server to set whether the portal provides resiliency support. *(IP Office Server Edition Select only)*
	Host Domain Name 30	Set the URL used for access to portal services.
	Conference Clean Up 30	Configure how long conference details are retained.
	Central CTI Link 31	Configure whether the server automatically learns about and supports other IP Office systems in a network.
	Block Client Versions 32	Configure specific versions and builds of clients that the server will not support.
Security	HTTP/HTTPS Protocol 33	Set whether the server uses HTTPS or HTTPS and HTTP.
	TLS Settings 33	Configure the TLS support options.
	ESNA Authentication 33	Sets the address of the ESNA server to use for authenticating user login using an ESNA account.
Diagnostics	Logging Configuration 34	Configure the level and method of logging supported.
	Logging Viewer 36	Install and launch Chainsaw for log viewing.
	Network Routes 36	Test the IP connection path to an IP address.
	IP Office Connections 37	Test the IP connection path to an IP Office.
	Database Integrity 37	Test the structure of the database.
	User Data Validation 38	Identify possible cause of user login failure or user data corruption and reset the corrupt data.
	Call/Conference Scheduling 39	Delete a scheduled conference.
	View Conferences 40	Display the historic and future schedule conference details for all users. Allows the deletion and modification of those conferences.
	Generate Memory Dump 40	Create a diagnostic record of the server's current memory usage.

Menu	Sub-Menu	Description
	Generate Thread Dump 40	Create a diagnostic record of the server's current processor threads..
Directory Integration	Directory Synchronization 41	Force a system directory update by the server.
	System Directory 42	View the one-X Portal for IP Office system directory.
	LDAP Directory Search 41	View the external directory for which the one-X Portal for IP Office server has been configured.
Gadgets Configuration	External Gadgets List 43	The external gadgets that are in the system are listed.
	Import External Gadgets 56	Import external gadgets.
	Export External Gadgets 43	Export external gadgets.
IM Archive	Search Archive 44	Search for the IM conversations between the system contacts.
Help & Support	Help 45	Access one-X Portal for IP Office help installed on the server.
	Avaya Support 45	Access the Avaya support web site for Avaya applications.
	About 45	View information about the one-X Portal for IP Office version.

It is important to understand that the one-X Portal for IP Office administrator menus operate as an off-line editor. Within a particular menu, data is fetched (using a **GET** command) from the database, edited and then sent back to the database (using a **PUT** command).

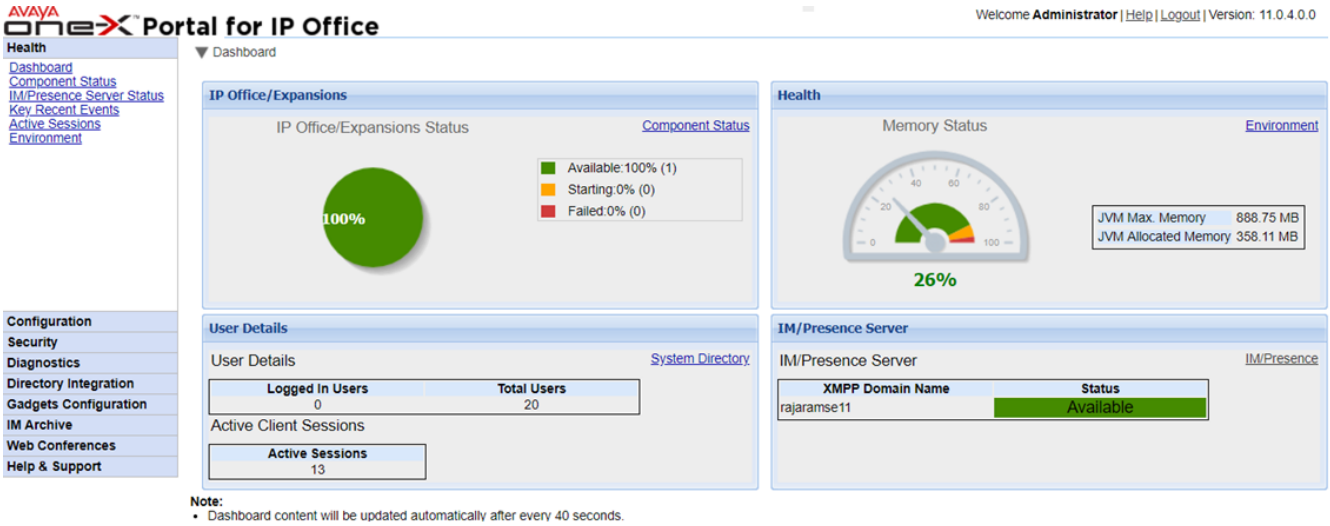
Within each menu, the clicking on the ▶ ▼ icons can be used to show/hide a short description of the menus function and content.

2.1 Health

This section allows you to view the status of the various components of the server.

2.1.1 Dashboard

The Dashboard menu provides a summary of the server status.

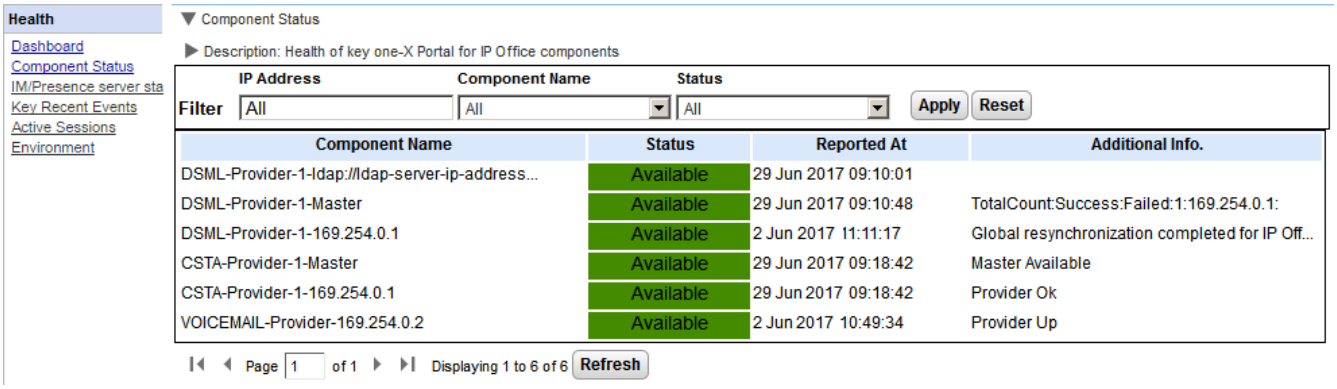


- **IP Office/Expansion Status**
  This section summaries the status of the connections from the portal server to the IP Office systems that it is supporting.
- **Health**
  This section summaries the servers memory usage.
- **User Details**
  This section summaries the number of configured and logged in users. It also shows the number of active sessions which includes users of Avaya Communicator for Web, Outlook plug-in, one-X Portal for IP Office.
- **IM/Presence Server**
  This section summaries the status of XMPP component of the server.

2.1.2 Component Status

The **Component Status** menu shows the last recorded status changes of each of the major components of the one-X Portal for IP Office application.

- For a service in a IP Office Server Edition Network and using centralized CTI link mode, there should be only one DSML provider to the primary IP Office system. There should also be one CSTA provider to the primary IP Office system unless using portal resilience in which case there should also be a CSTA provider to the secondary IP Office system.
- There should be one DSML LDAP provider if LDAP is being used.

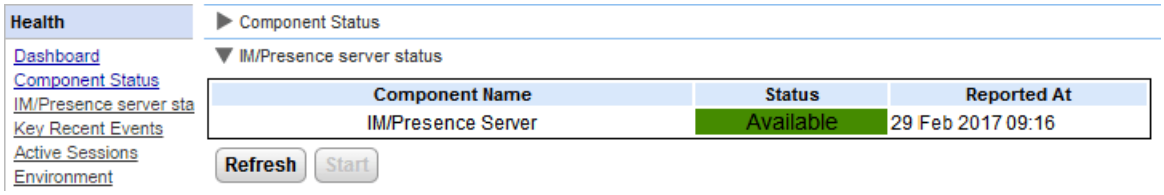


To view the component status:

1. Select **Health** and then **Component Status**.
2. Click **Get All** to retrieve the status records from the one-X Portal for IP Office database.
3. Use the page controls to browse through the records.
4. The **Delete** option deletes the status record, it does not affect the component. The check boxes and **Delete Selected** can be used to delete multiple records.

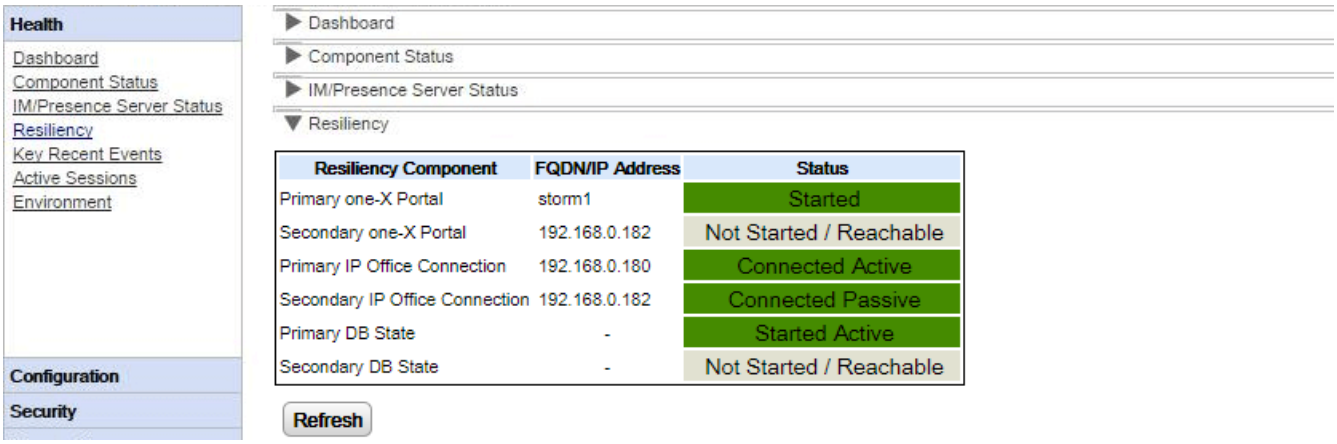
2.1.3 IM/Presence Server Status

This menu shows the current status of the instant messaging server used as a component service by the one-X Portal for IP Office. For various maintenance processes relating to IM and presence, see Instant Messaging 67.



2.1.4 Resiliency

This menu is shown on IP Office Server Edition Select network portal servers. It shows the current status of the portal and IP Office services on the primary and secondary servers when using IP Office Server Edition resilience 14.



For example, the screenshot above shows a system where the primary and secondary IP Office servers are running and the primary portal server is running but the secondary portal service has not been started. When the portal service is started, the status of the secondary portal will change to ***Started*** and the **Secondary DB** to ***Started Passive***.

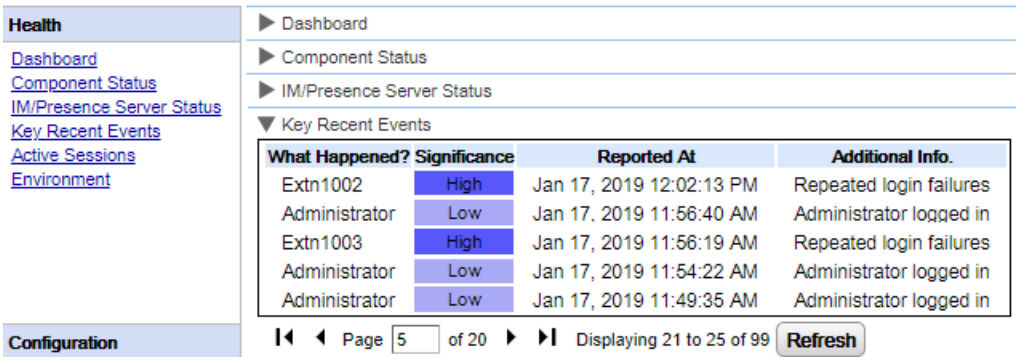
The terms used in the status display have the following meanings. The terms may be combined:

- **Started**
  The service is running.
- **Stopped** or **Not Started**
  The service is not running.
- **Connected**
  This portal server has a connection to the service.
- **Reachable**
  The server hosting the service was detected but there is no connection as the service on that server has not started.
- **Active**
  The service is currently being used to support portal users.
- **Passive**
  The service is running but is not currently being used to support portal users.

2.1.5 Key Recent Events

The **Key Recent Events** menu displays the last 20 events recorded by the one-X Portal for IP Office application. These can be actions performed by the one-X Portal for IP Office service and also administration actions such as administrator log in/log out, administrator password changes, provider changes, and configuration restorations.

The list also includes failed user login attempts if more than 10 failures occur in a 5 minute period. Failed login attempts are based on the user name.



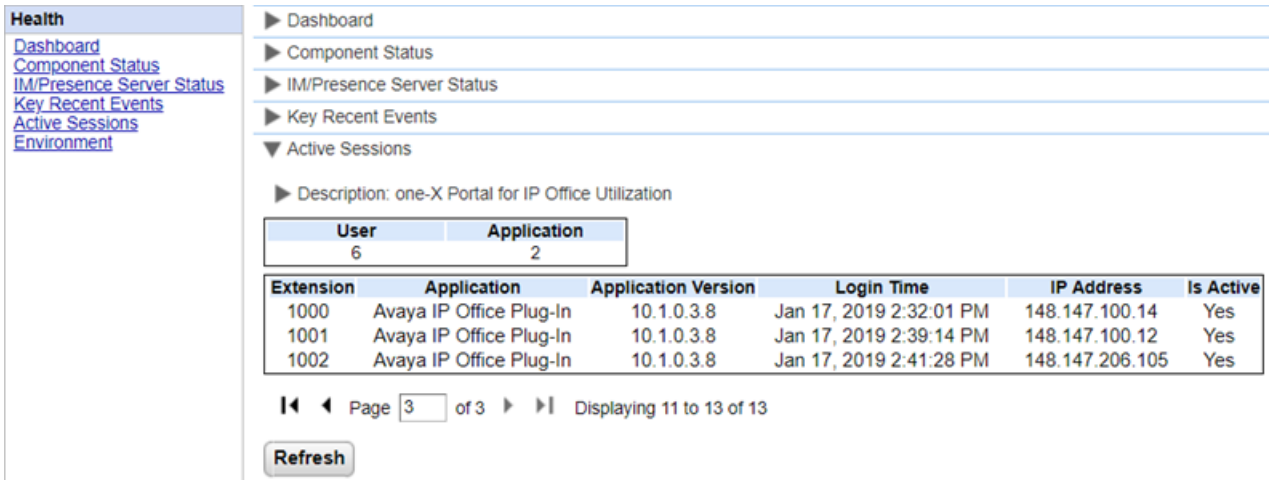
To view key recent events:

1. Select **Health** and then **Key Recent Events**. Click **Refresh**.
2. Click **Get All** to retrieve the event records from the one-X Portal for IP Office database.
3. Use the page controls to browse through the records.
4. The **Delete** option deletes the status record, it does not affect the component. The check boxes and **Delete Selected** can be used to delete multiple records.

2.1.6 Active Sessions

The **Active Session** menu displays the number of Avaya internal client, 3rd party client application sessions connected to the one-X Portal for IP Office server.

3rd Party CTI displays number of internal/external 3rd Party CTI users logged into one-X Portal for IP Office.

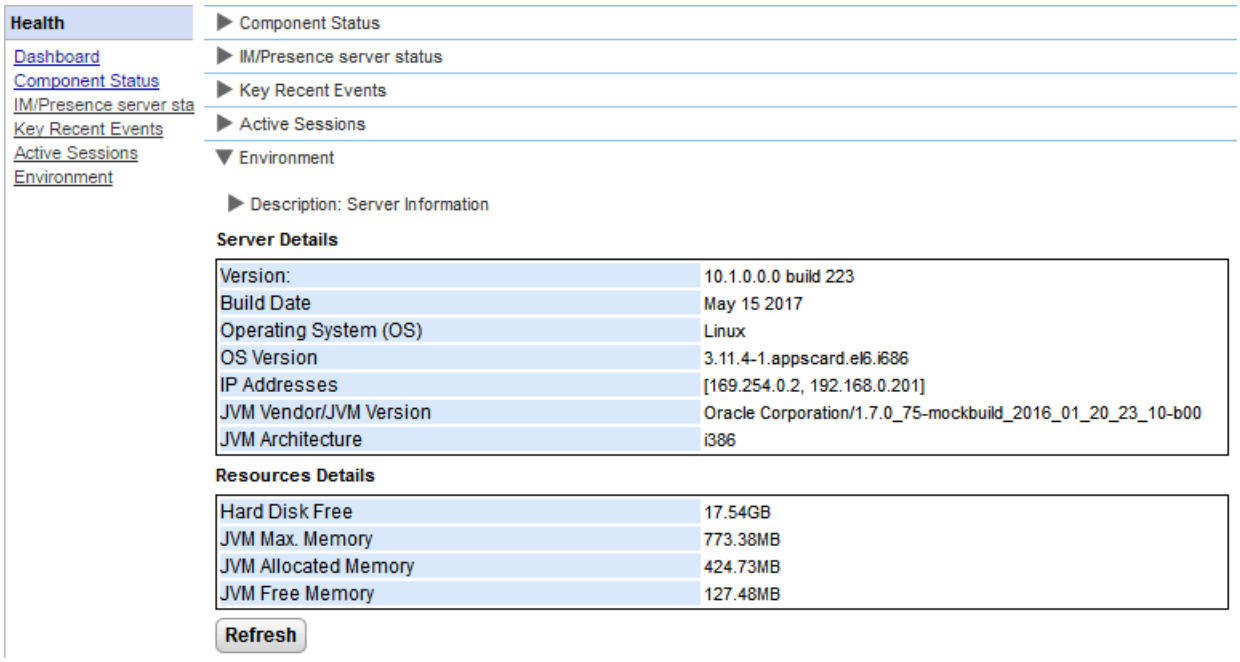


To view the active sessions:

1. Select **Health** and then **Active Sessions**.
2. To update the details, click **Refresh**.

2.1.7 Environment

The **Environment** menu display information about the one-X Portal for IP Office server PC. The information available varies depending on the type of portal server.



To view the environment details:

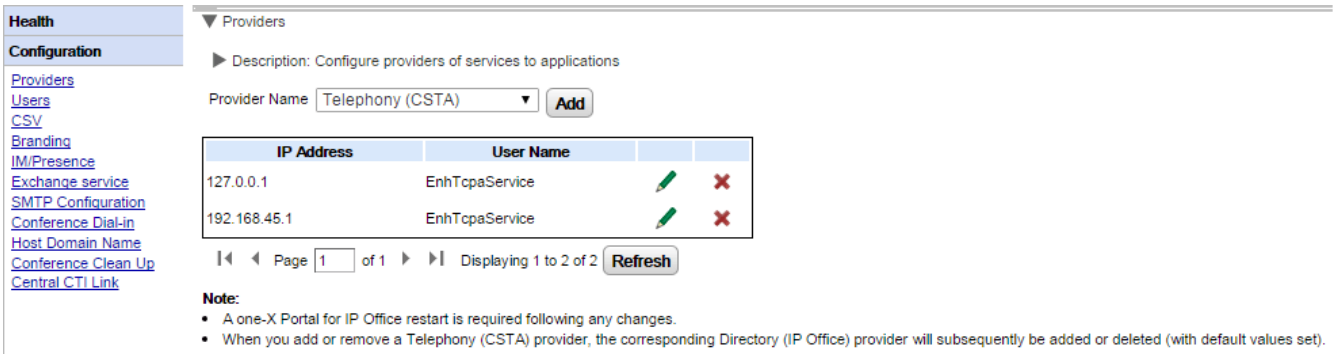
1. Select **Health** and then **Environment**.
2. Click on **Refresh**.

2.2 Configuration

This section allows you to view and check various configuration options.

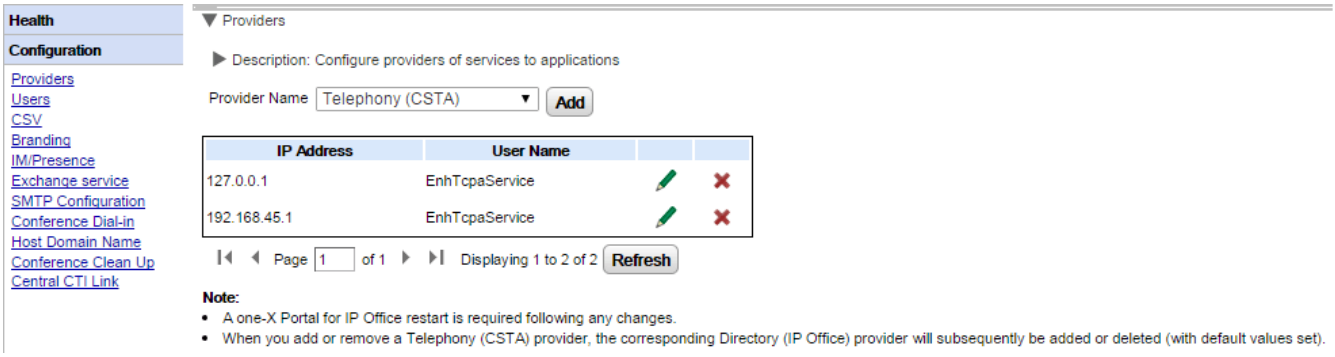
2.2.1 Providers

This menu shows the service providers configured on the one-X Portal for IP Office server. The **Providers** menu allows editing of which IP Offices and LDAP servers are assigned to the providers.



2.2.1.1 Telephony (CSTA) Provider

The settings below are shown for a Telephony (CSTA) provider. These should only be changed if you are experienced with the installation and operation of one-X Portal for IP Office.

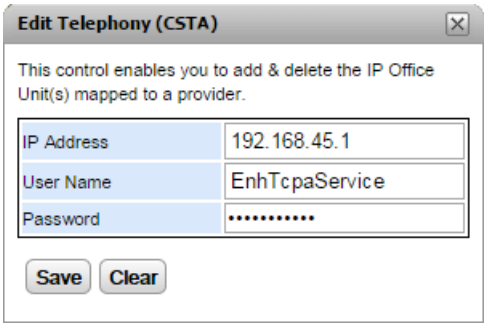


To add a new CSTA provider, click on **Add**. The provider settings are displayed. Note that adding a new CSTA provider also automatically adds a new DMSL provider to the same address. Adding a new provider would only be necessary in a network not using centralized configuration 31.

To edit an existing CSTA provider, click on the edit icon next to the existing entry. The provider settings are displayed.

CSTA Provider Settings

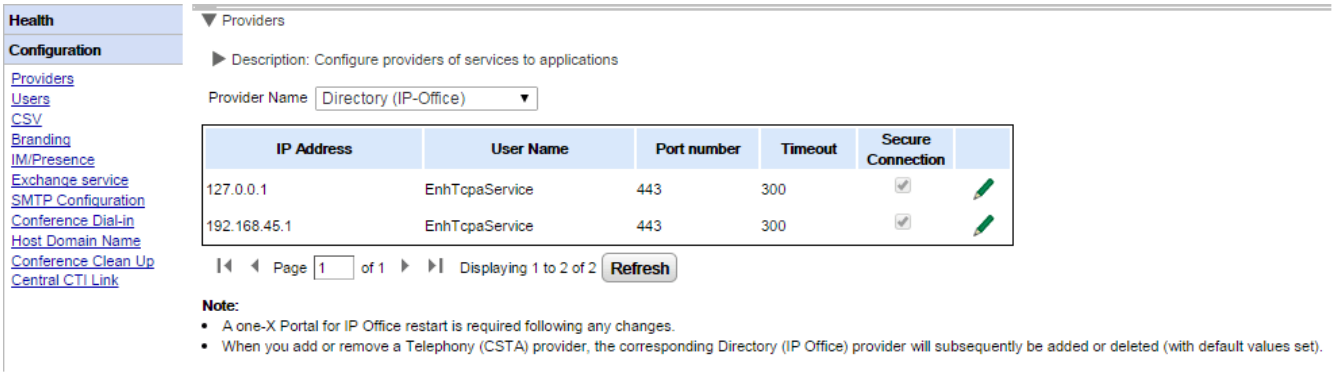
Any changes to provider settings requires you to restart the portal service 48.



- **IP Address**
  The IP address of the IP Office system.
- **User Name**
  The name of the TCPA service user configured in the security settings of the IP Office system. The default user is ***EnhTcpaService***.
- **Password**
  The password set for the TCPA service user.
  - **Warning:** Placing the cursor focus on the password field removes the existing password.

2.2.1.2 Directory (IP Office) Provider

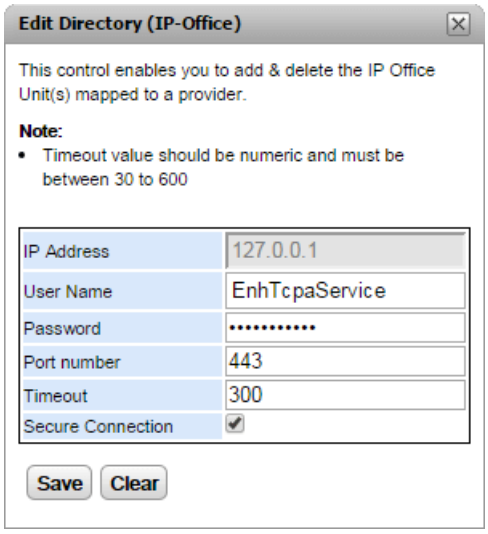
The settings below are shown for a Directory (IP-Office) provider. These should only be changed if you are experienced with the installation and operation of one-X Portal for IP Office.



To add a new Directory provider, user the options for adding a CSTA provider 18. To edit an existing provider, click on the edit icon next to the existing entry.

Directory Provider Settings

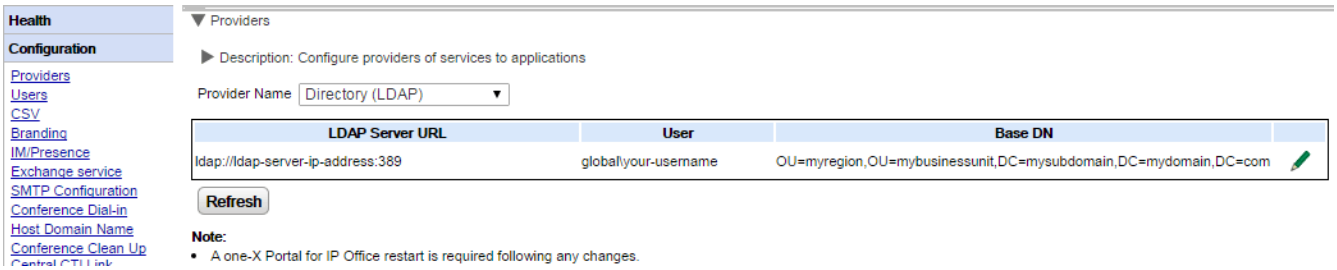
Any changes to provider settings requires you to restart the portal service 48.



- **IP Address**
  The IP address of the IP Office system.
- **User Name**
  The name of the TCPA service user configured in the security settings of the IP Office system. The default user is ***EnhTcpaService***.
- **Password**
  The password set for the TCPA service user.
  - **Warning:** Placing the cursor focus on the password field removes the existing password.
- **Port number**
  The port number on which the IP Office system accepts connections.
- **Timeout**
  The timeout value between 30 to 600 seconds.
- **Secure Connection**
  Set to connect with the telephone system directory service.

2.2.1.3 DSML (LDAP) Provider

The settings below are shown for a **Directory (DSML LDAP)** provider.

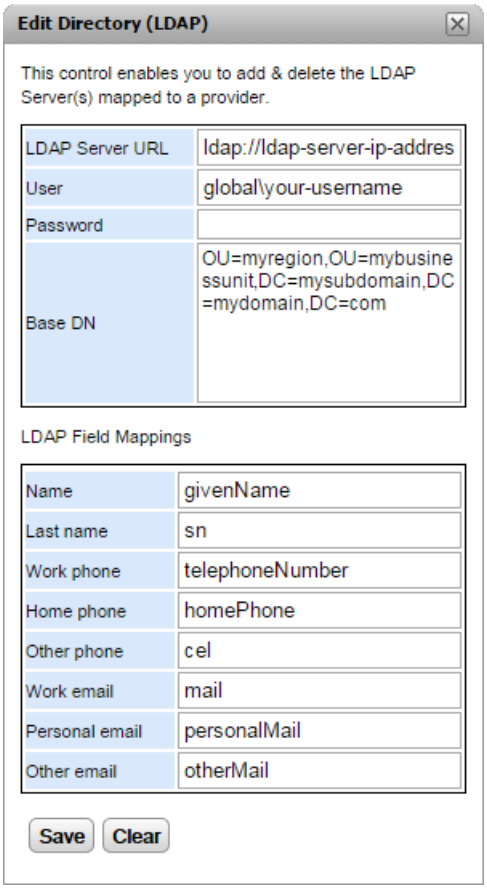


To edit the provider, click on the edit icon.

- **Warning:** Placing the cursor focus on the password field removes the existing password.

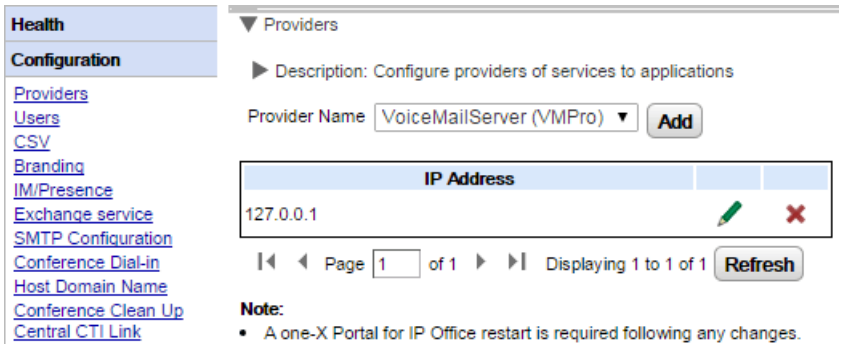
LDAP Provider Settings

Any changes to provider settings requires you to restart the portal service 48.



2.2.1.4 Voicemail Provider

The settings below are shown for a **VoiceMailServer** provider.



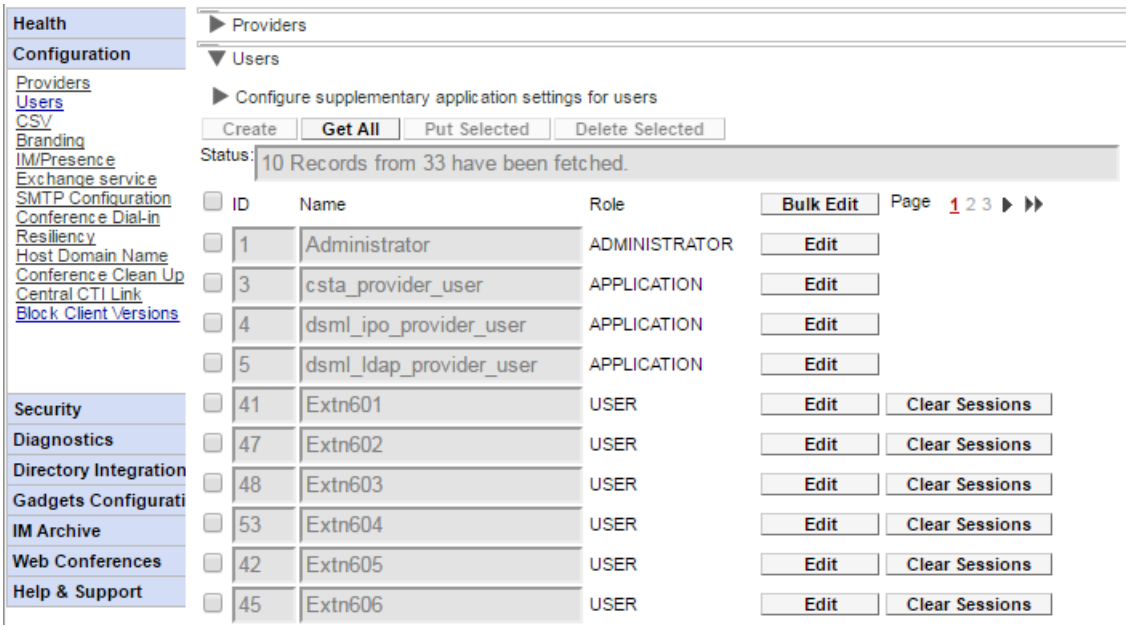
To edit the provider, click on the edit icon.

Any changes to provider settings requires you to restart the portal service 48.

2.2.2 Users

You can view the users of IP Office in the **Users** menu. It lists all IP Office users, not just those enabled for one-X Portal for IP Office operation. Note that during normal operation the portal server only resynchronizes its list of known users with the telephone system every 5 minutes.

You can edit some of the user settings stored in the one-X Portal for IP Office, see Editing User Settings 61. You can not edit user settings stored in the IP Office.

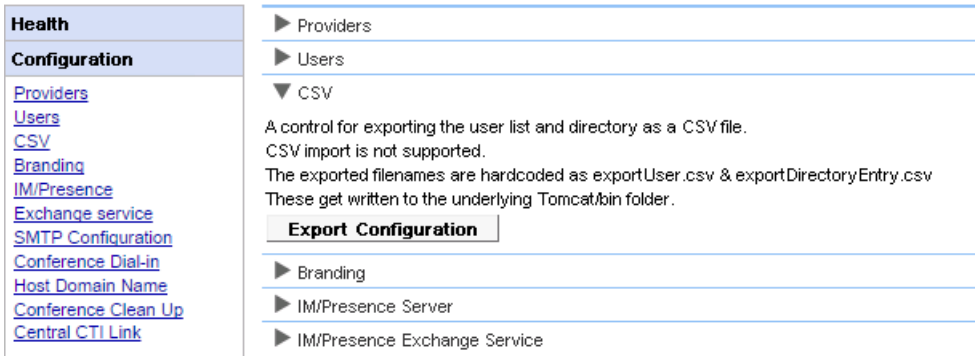


To view users:

1. Click **Configuration** and select **Users**.
2. Click **Get All**.
3. The **Clear Sessions** button next to each user can be used to disconnect any currently connected clients that user has running.

2.2.3 CSV

This menu allows you to export the user information and system directories being used by the one-X Portal for IP Office server to .csv format files. The files are exported to the ***/bin*** sub-folder of the application directory (by default ***C:\Program Files (x86)\Avaya\onexportal\Tomcat\Server\\bin***). Any existing file is overwritten.

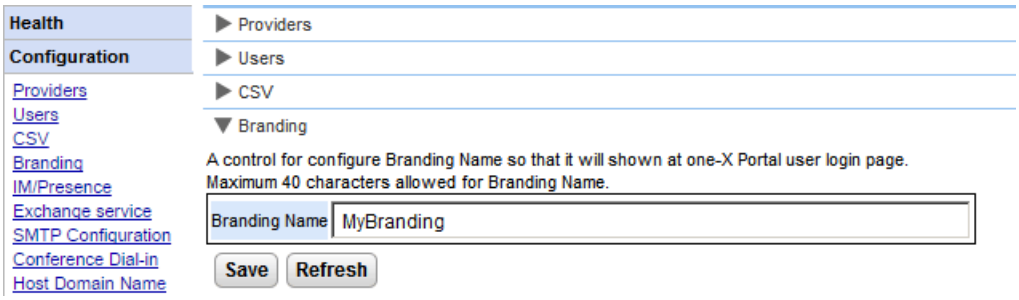


To export:

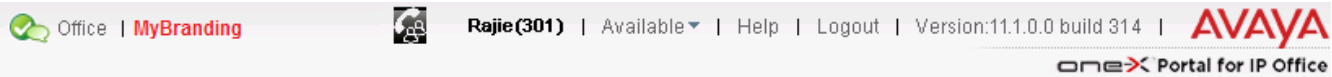
1. Select **Configuration** and then **CSV**.
2. Click **Export Configuration**.
3. Two files are created in the folder the ***/bin*** sub-folder of the application directory. By default, a path similar to ***/opt/Avaya/oneXportal/10.1.0_136//apache-tomcat/bin***.
   - ***exportUser.csv***
   - ***exportDirectoryEntry.csv***

2.2.4 Branding

This menu allows you to specify some text that is then displayed on the one-X Portal for IP Office pages after a user has logged in.

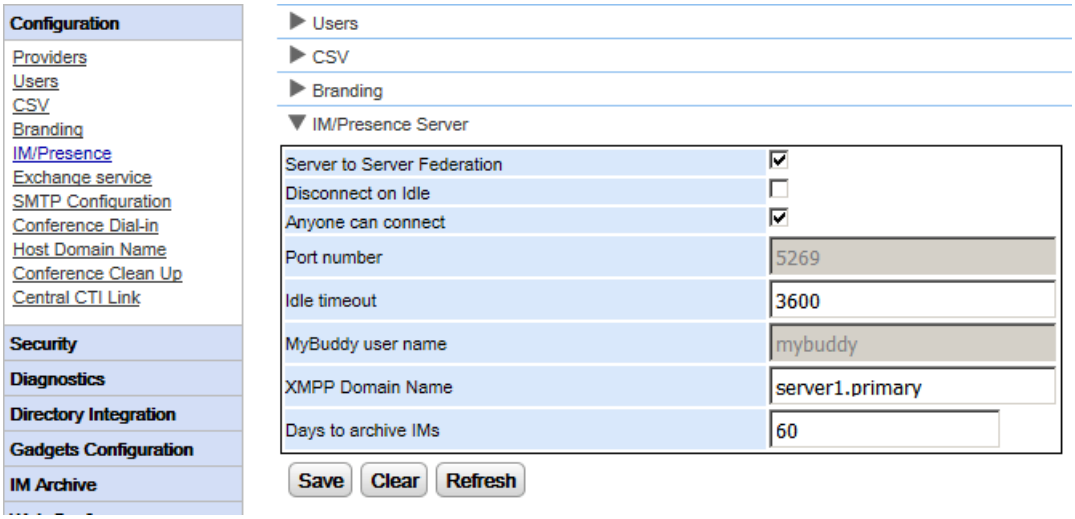


The text is displayed in the one-X Portal for IP Office title bar as shown below.



2.2.5 IM/Presence

The portal includes a component that acts as its instant messaging/presence server. The IM/presence server can be separately configured. See Instant Messaging/Presence 67.

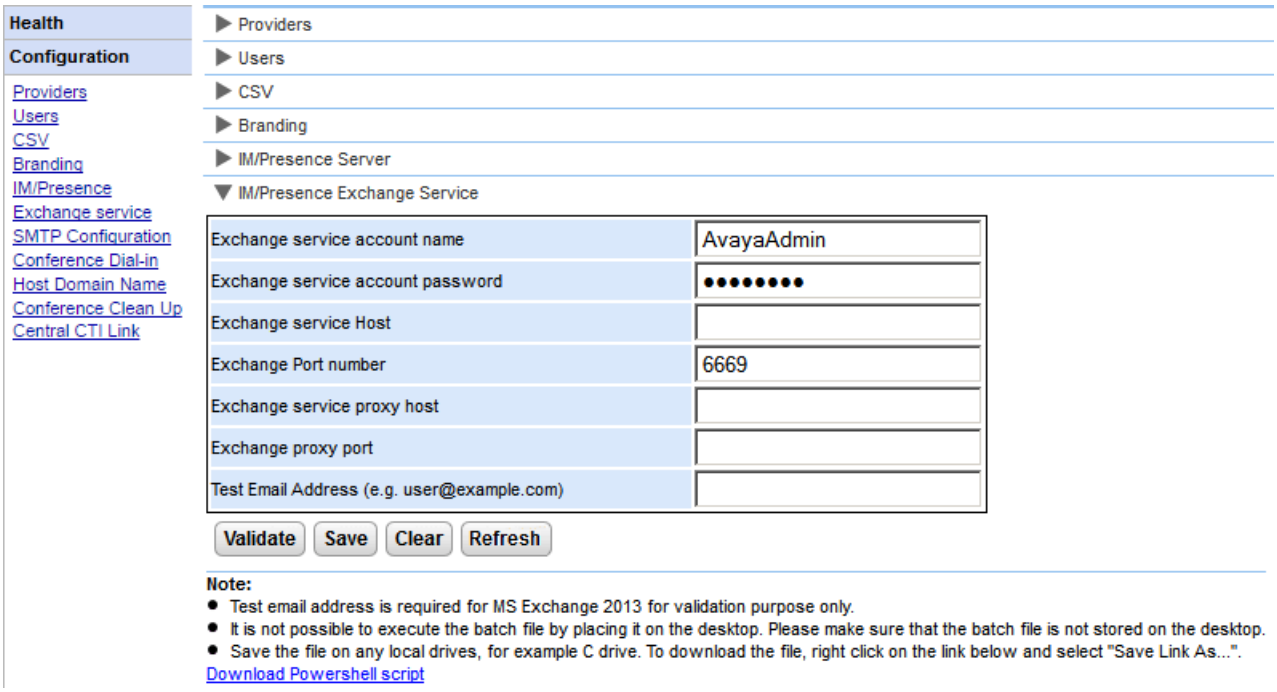


To configure the IM/Presence server:

1. Click **Configuration** and select **IM/Presence Server**.
2. Select the required server settings:
   - **Server to Server Federation**
     If selected, the portal's presence server is able to exchange presence information with other presence servers.
   - **Disconnect on Idle**
     If selected, server to server connections are disconnected if idle for the **Idle timeout** period.
   - **Anyone can connect**
     Allow anyone to connect to IM/presence services.
   - **Port number**
     This is fixed as ***5269***.
   - **Idle timeout**
     This is the timeout in seconds used for **Disconnect on Idle** if selected.
   - **MyBuddy user name**
     This field is fixed as ***mybuddy***. The value my be needed when integrating presence details with other IM/presence services.
   - **XMPP Domain Name**
     This sets the DNS domain name used for IM/presence functions:
     - The XMPP domain name should be a domain name that the DNS can resolve. You can set the XMPP domain name at any point in time. The domain name must be reachable from the internet if you wish to use presence outside of your LAN.
     - Avaya recommends that you use a split DNS so that the server name outside of your LAN is resolved into the public IP address of the NAT or firewall whilst inside your network it is resolved into the private IP address of the server on the LAN.
     - If you cannot set a resolvable DNS domain name, you can use the IP address of the one-X Portal for IP Office server for internal only IM/presence. In this case the one-X Portal for IP Office cannot federate with remote servers.
     - You must use the server's **Web Control** menus to configure their network settings so that the auto-configuration email link uses the FQDN instead of the IP address of the server. In **Web Control**, navigate to **Settings > System > Host Name** to change the network settings. If you change the domain name any other way, the email links might not work properly.
   - **Days to archive IMs**
     This field sets how long the server should retain messages in the IM archive before deleting those messages. The default setting is 182 days (6 months). If necessary, you can disable IM archiving 73 using the XMPP admin console. The IM/Presence server must be available (see IM/Presence Server Status 13) to change this setting.
3. Click **Save**.

2.2.6 Exchange Service

one-X Portal for IP Office can be configured with the Exchange server to the presence information of the users.

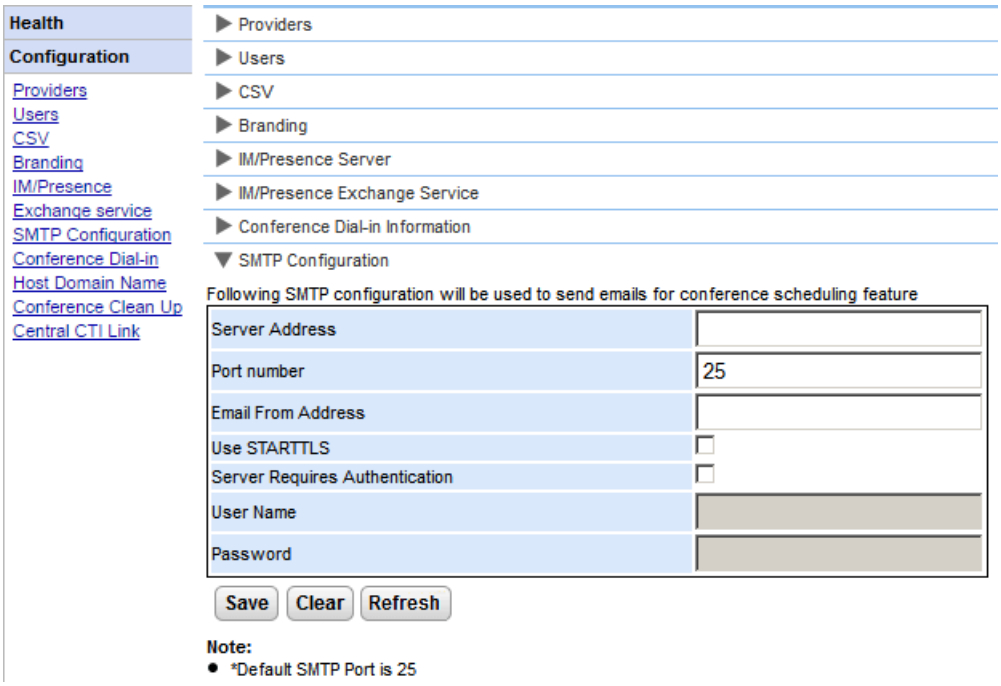


To configure Exchange services:

1. Click **Configuration**, in the left navigation pane.
2. Click **Exchange service**.
   a. Type ***AvayaAdmin*** in the **Exchange service account name**. Ensure that this name is the same as the ***AvayaAdmin*** account that you created on the exchange server.
   b. Type the password that was set for the **AvayaAdmin** in **Exchange service account password**.
   c. Type the IP address of the exchange service host in **Exchange service Host**.
   d. Type the port number of the exchange service in **Exchange Port number**.
   e. Type the domain name of the proxy server that is used to connect to the exchange server in **Exchange service proxy host**.
   f. Type the port number of the proxy server for exchange service in **Exchange proxy port**.
   g. Set a **Test Email Address** using a valid email address.
3. Click on **Validate Exchange Service Configuration** to view whether the provided exchange details are valid.
4. Click **Save**.

2.2.7 SMTP Configuration

The conference invites to participant can use both instant messaging and email. For email, the conference email settings must be configured as below. The email address used for each individual participant is set in the telephone system configuration.

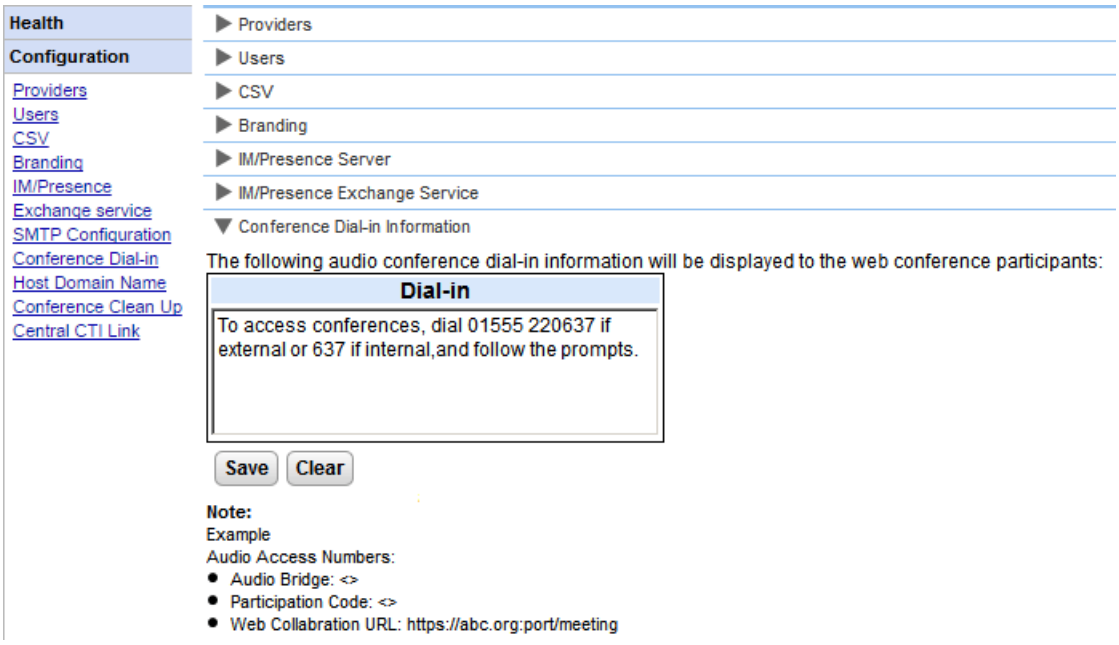


To set the conference notification fixed text:

1. Select **Configuration** and then **SMTP Configuration**.
2. Set the SMTP email details that the server should use:
   - **Server Address**
     The IP address of the customer's SMTP server.
   - **Port Number**
     The SMTP listening port of the server. The default is 25.
   - **Email From Address**
     This is the address that will be used by the server. Some email servers will only relay messages from recognized or addresses in the same domain.
   - **Use STARTTLS**
     Select this field to enable TLS/SSL encryption. Encryption allows voicemail-to-email integration with hosted email providers that only permit SMTP over more secure transport.
   - **Server Requires Authentication**
     If the server requires a user account to receive and send emails, enter the details of an account configured on that server for use by the IP Office.
     - **User Name**
       The account name to use if Server Requires Authentication is selected.
     - **Password**
       The account password to use if Server Requires Authentication is selected.
3. Click **Save**.

2.2.8 Conference Dial-In

When a user schedules a conference, the server sends the invited participants a conference notification using email and instant messaging. That notification includes the details of the conference set by the user (bridge number, participant code). It can also include the fixed text set through the **Conference Dial-in** menu.



To set the conference notification fixed text:

1. Select **Configuration** and then **Conference Dial-in**.
2. Enter the fixed text that should be included in all conference notifications.
3. Click **Save**.

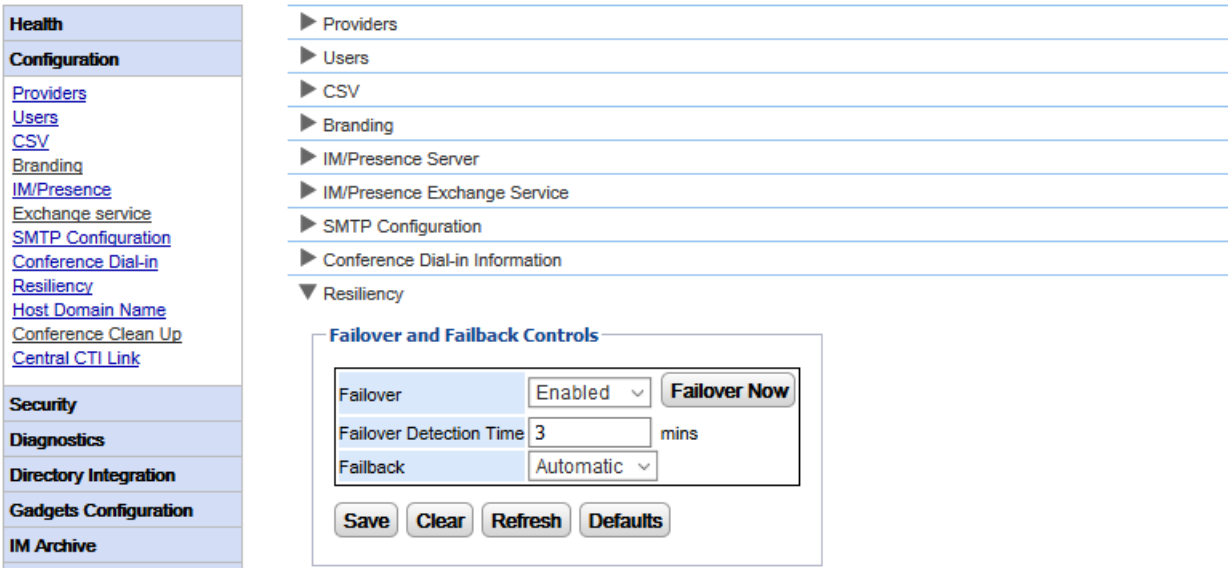
2.2.9 Resiliency

This menu is available on portal servers supporting a IP Office Server Edition Select network. It provides additional settings for the portal server for it to take part in portal server resiliency. See Resiliency 53.

- On existing non-IP Office Server Edition Select mode systems that have then been switched to IP Office Server Edition Select mode, it may be necessary to restart the portal services for resiliency settings to become available. Similarly it may be necessary to restart the portal services after first configuring portal resiliency in the IP Office system configuration.

Primary Server Settings

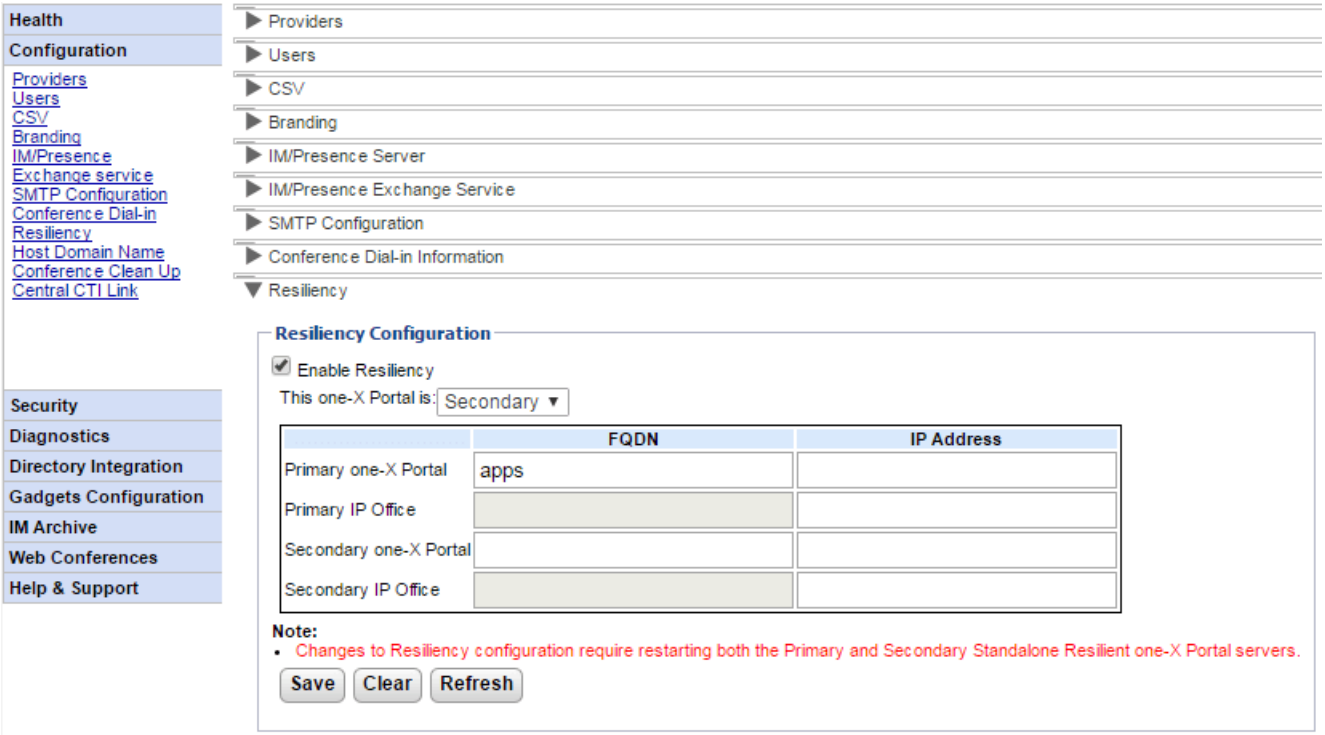
The settings shown on the primary server are:



- **Failover**
  Select whether the server should support failover. If enabled, the domain name of the secondary portal server should be set in the Host Domain Name 30 form.
  - **Failover Now**
    This control can be used to manually initiate the failover process.
- **Failover Detection Time**
  Sets the time in minutes before failover occurs when potential issues are detected. The default (3 minutes) stops failover being initiated by normal maintenance restarts of services.
- **Failback**
  Sets whether the failback process should be initiated automatically when possible. If set to manual, then a restart of the portal services is required to complete failback.

Application Server Settings

The settings also appear on an application server. When that server is being used in a IP Office Server Edition Select network, it can act the portal server for the primary or secondary server, replacing the embedded portal service on that server.

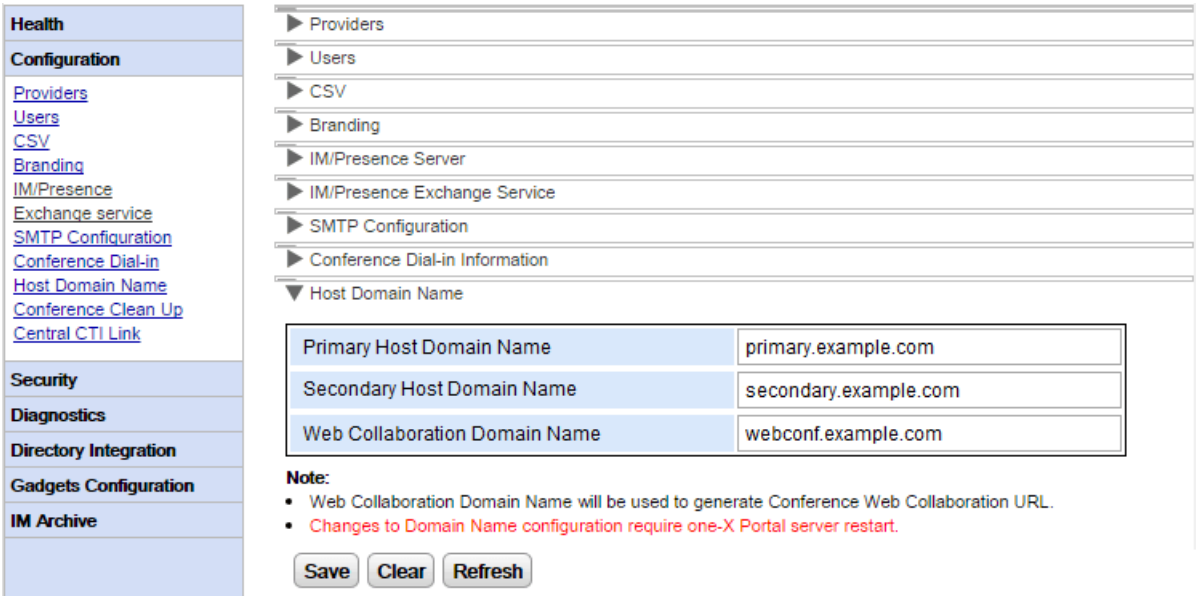


- **Enable Resiliency**
  If selected, enables portal resiliency and displays the additional fields required to define the addresses of the other servers in the resiliency setup and the role of the servers. If resiliency is not enabled, then the portal service on secondary server is automatically stopped and cannot be manually restarted.
  - **This one-X Portal:**
    Define the role of this server.
    - **Primary**
      Select if this server is intended to act as the primary portal server.
    - **Secondary**
      Select if this server is intended to act as the backup/fallback portal server if the primary portal is not available.
- **FQDN/IP Address**
  Use this table to enter the fully qualified domain names or IP addresses of the all the portals and IP Office servers in the resiliency set.

2.2.10 Host Domain Name

The **Configuration | Host Domain Name** menu is used to set the domain name used for access to the portal services and between portal servers. The number of domain names required depends on the type of portal server.

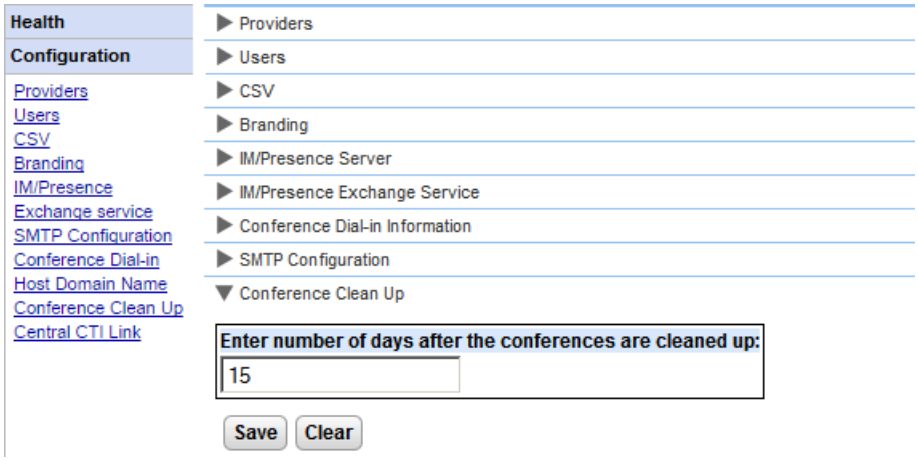
Note that changing the domain names requires the portal service to be restarted for the changes to take effect.



- The web collaboration URL is used as the default for conference invitations when scheduling a conference. The web collaboration service is not supported with R12.0 and higher.

2.2.11 Conference Clean Up

This menu allows the configuration of how many days conference details are retained by the server.



2.2.12 Central CTI Link

IP Office Server Edition portal servers can use centralized CTI mode. In this mode, the portal service only needs to be linked to one Linux-based IP Office system in order to provide services to all the IP Office systems in the network. This includes an IP Office Application Server being used with IP Office Server Edition.

- This option is not available for an IP Office Application Server supporting an IP500 V2 system.

In centralized CTI link mode, the portal service automatically provides call services to all IP Office systems in the network. It obtains system directory entries from all systems and automatically about systems added to or removed from the network. Additionally, the portal automatically obtains information about the central voicemail server.

- **Central CTI Link**
  This setting is used to enabled or disable centralized CTI mode. Note that the one-X Portal for IP Office service must be restarted if the setting is changed.
  - **If enabled:**
    When this setting is enabled, the portal service uses centralized CTI mode. This means:
    - The portal connects with only one IP Office system. CSTA and DSML providers are created only for that system. However, the connections to that system are used to learn about and provide services for all other IP Office systems in the network.
    - The link to the IP Office system is also used to discover the voicemail server settings and automatically create the necessary provider.
    - If IP Office Server Edition resilience 53 is also enabled, then CSTA providers are created for both the primary and secondary IP Office systems.
    - Each individual IP Office system known to the portal server is still shown in the **Component Status** 13 menu.
    - The portal obtains IP Office server information and system directories from the primary IP Office system.
    - Personal directory records are still obtained from each user's host IP Office system.
  - **If disabled:**
    When this setting is not enabled:
    - CSTA and DSML providers must be manually configured for each IP Office system in the network. This is done during installation and/or through the **Providers** 17 menus. However, the voicemail provider is provisioned automatically based on information from the connected IP Office system.
    - This is the default setting for system upgraded to IP Office Release 10.

Auto Provisioning

Systems upgraded from Release 9.1, display their original **Auto Provisioning** setting and use that instead of **Central CTI Link**. If **Auto Provisioning** is enabled, the initial CSTA provider connected is used to automatically create additional providers and maintain CSTA and DSML providers for all other systems in the network. In Release 10.0, the voicemail provider is also automatically configured using the information from the telephone system.

Systems using **Auto Provisioning** can be converted to using **Central CTI Link** by clicking the **Convert to Central CTI Link** button. This process cannot be reversed.

2.2.13 Block Client Versions

This menu can be used to create a list of client versions that the portal server will not support. This is done by adding the client version and build to the lists of blocked clients.

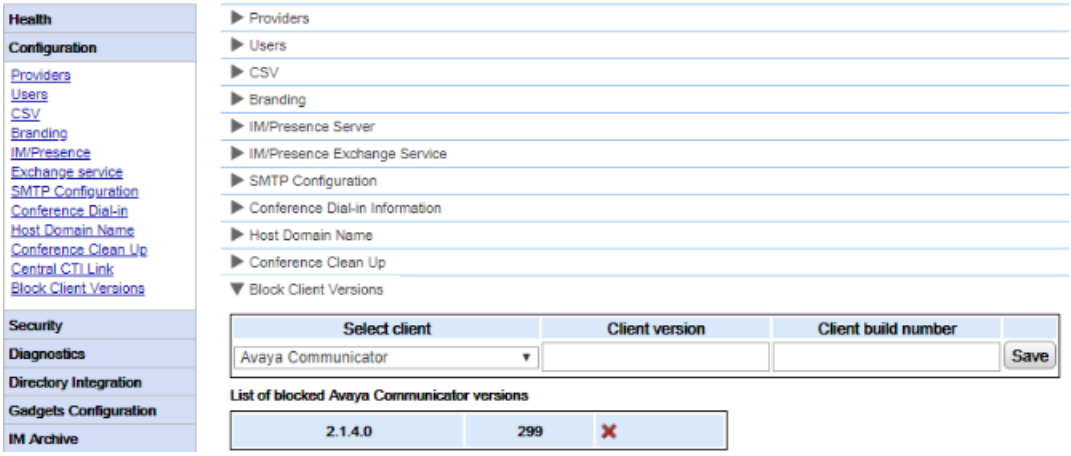
The affect of being blocked by the portal varies depending on the client:

- **Avaya IP Office Plug-In, Avaya one-X Call Assistant:**
  If blocked, these clients are not able to log in. If already logged in, they will continue to work until they log out.

- **SoftConsole:**
  If blocked, these clients can still log-in as they login directly to the IP Office for telephony services. However, they will not receive IM and presence support from the one-X Portal for IP Office server.

For each client, a maximum of 15 version/build combinations can be blocked.

- Details of the clients being used and their versions can be seen on the **Active Sessions** 16 menu.
- The versions reported by clients when connected may differ from that shown to the user within the clients menus (for example the client's **Help | About**).
- When using this menu to block particular clients, it is important to also test and ensure that you have not also blocked versions of the client that you want to support.



To add a new blocked client:

1. Use the **Select client** drop-down to select the client.
2. Enter the **Client version** and **Client build** number values. Both values must be set.
3. Click **Save**.

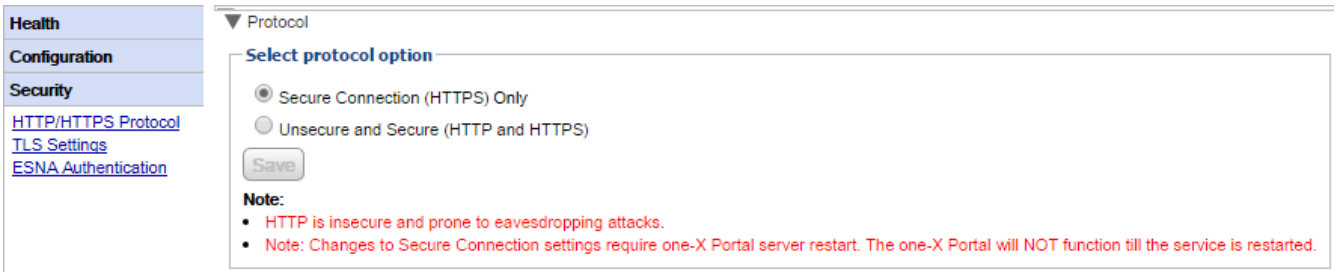
To removed a blocked client:

1. Click on the cross icon

2.3 Security

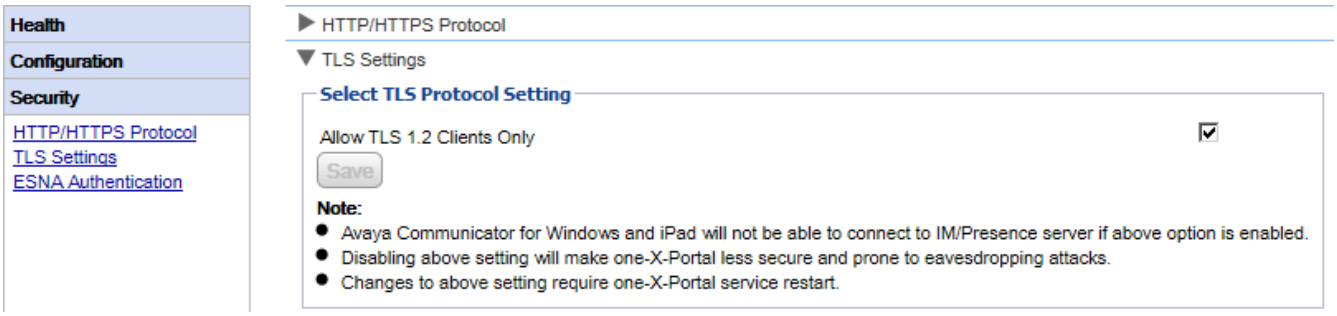
2.3.1 HTTP/HTTPS Protocol

By default, the server installs with support for encrypted HTTPS access only; that is port 9443 on a Linux server. This menu can be used to also enable HTTP access on port 8080.



2.3.2 TLS Settings

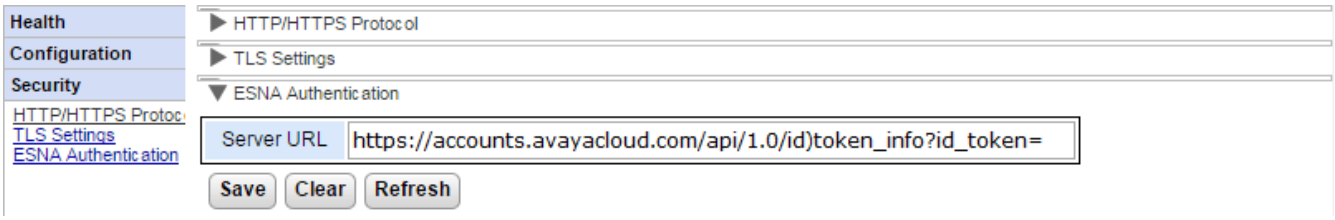
The portal server supports user and applications connecting using TLS. That can be restricted to connections that use TLS 1.2.



- **Allow TLS 1.2 Clients Only**
  If enabled, the TLS support provided by the portal server is restricted to TLS 1.2. If this setting is changed, you must restart the portal service 48 for the change to take effect.

2.3.3 ESNA Authentication

Users connecting using an Avaya Cloud (formerly ESNA) account require authentication against Avaya Cloud's servers.



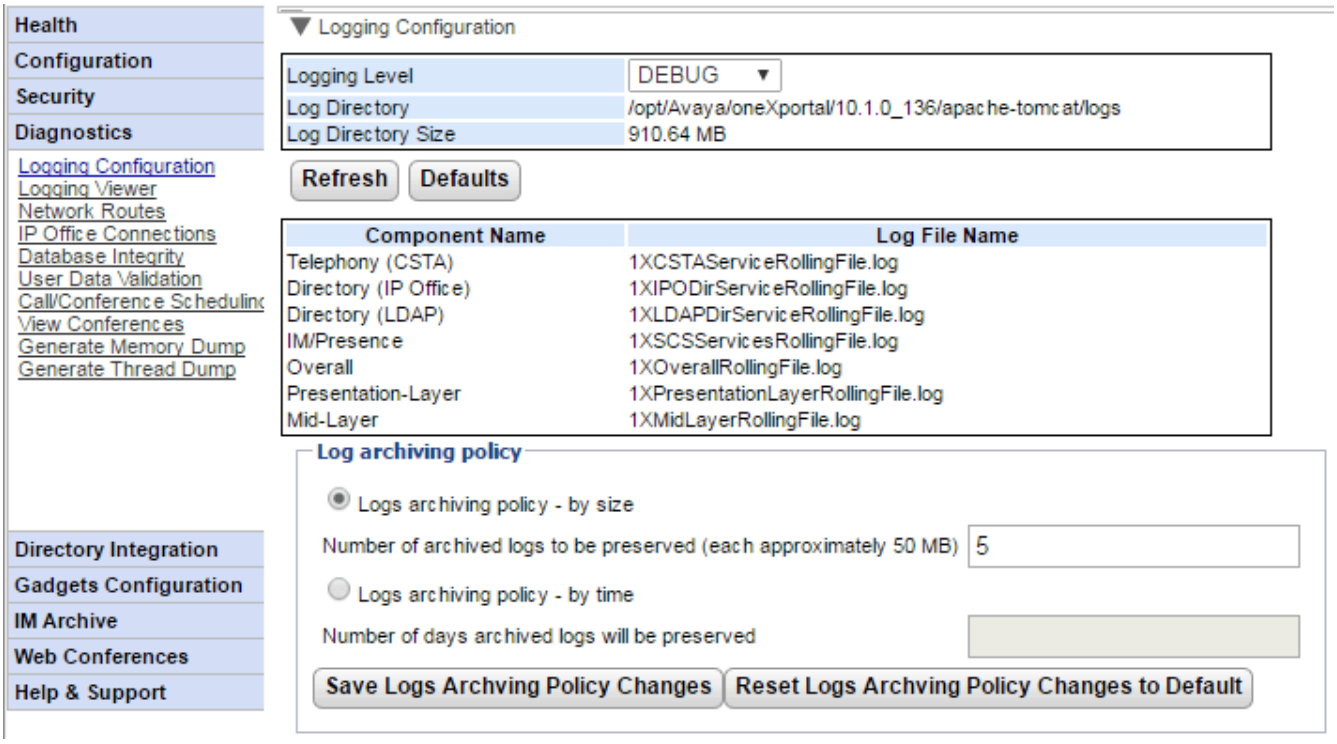
- **Server URL**
  This field sets the URL used to redirect user authentication requests to Avaya Cloud for authentication. The value is automatically configured during original installation and does not need to be changed.

2.4 Diagnostics

This section allow you to run various diagnostic checks.

2.4.1 Logging Configuration

This menu is used to configure the one-X Portal for IP Office logging outputs. Actual logs can be downloaded through the servers web control/platform view menus.



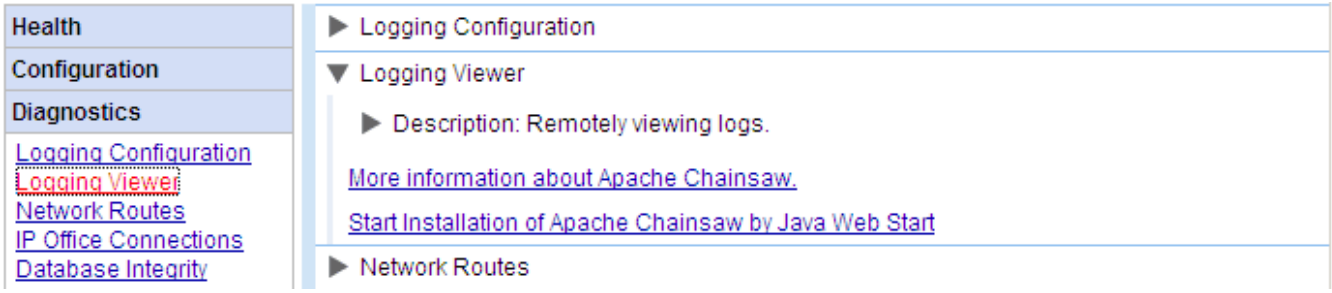
- **Master Logging Level**
  This field is used to select the minimum level of event to log or to disable any logging by selecting ***OFF***.
  - The default logging level for new installations is ***ERROR***.
  - For all systems, the logging level ***ERROR*** is used during service start-up, regardless of the configured setting. Once the service has started, the configured level is applied.
  - A warning regarding logging of personal data is displayed when selecting a logging level other than ***ERROR*** or ***OFF***.
- **Log Directory**
  The directory to which the server saves its log files. Not changeable.
- **Log Directory Size**
  The current total size of the log files.
- **Refresh**
  When clicked, updates the information displayed.
- **Default**
  When clicked, return the **Master Logging Level** to the default value of ***ERROR***.
- **Log File Descriptions:**
  This table shows the log files used by the different components of one-X Portal for IP Office.
  - **Telephony (CSTA):** *1XCSTAServiceRollingFile.log*
    This log captures telephony information. That includes obtaining user and licensing information from the IP Offices.
  - **Directory (IP-Office):** *1XIPODirServiceRollingFile.log*
    This log captures IP Office directory information.
  - **Directory (LDAP):** *1XLDAPDirServiceRollingFile.log*
    This log captures LDAP directory information.
  - **IM/Presence:** *1XSCSServicesRollingFile.log*
    This log captures IP Office IM and Presence information.

- **Overall:** *1XOverallRollingFile.log*
  This is an overall log file of all types of logged events.
- **Presentation Layer:** *1XPresentationLayerRollingFile.log*
  This log captures user browser activity information/
- **Mid-Layer:** *1XMidLayerRollingFile.log*
  This log captures interaction between the various one-X Portal for IP Office components including the IP Offices.

- **Log archiving policy**
  These settings allow you to configure how log file retention is controlled by the server. The default is to retain the last 5 log files.
  - **Logs archiving policy - by size**
    If selected, the number of log files setting is used to determine which files to keep. When a new file is started (files are automatically rolled over when they reach approximately 50MB), the oldest file is automatically deleted if the number of files to retain has been exceeded.
    - **Number of archived logs to be preserved**
      Sets the number of files to retain if **Logs archiving policy - by size** is selected. The default setting is 5 files.
  - **Logs archiving policy - by time**
    If selected, the log file age in days is used to determine which files are kept. Older files are automatically deleted.
    - **Number of days archived logs will be preserved**
      Sets the number of days to retain a log file if **Logs archiving policy - by time** is selected. The default setting is 5 days.

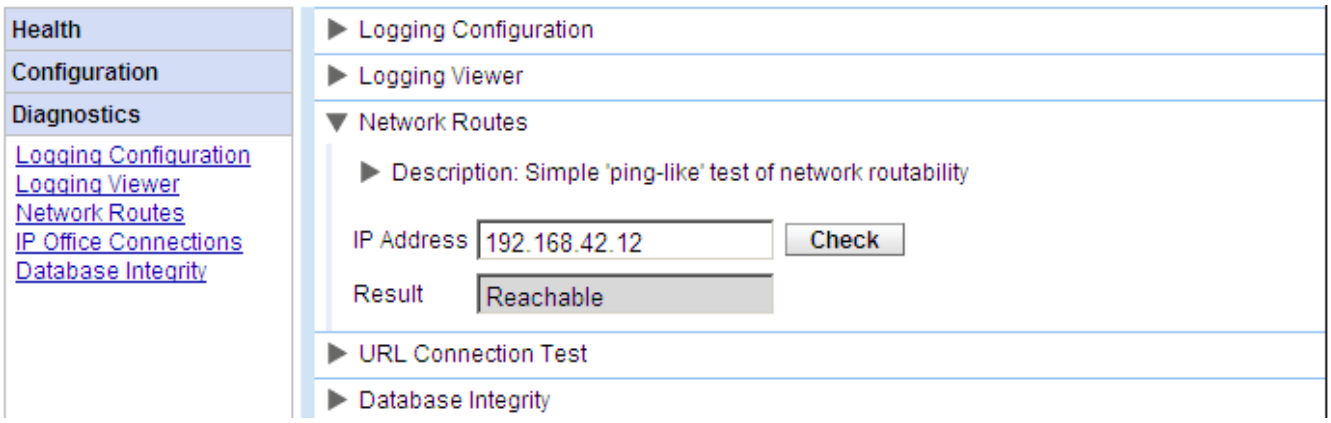
2.4.2 Logging Viewer

In addition to logging to files, the logging messages output by the components of one-X Portal for IP Office can also be viewed using a remote logging application that supports the Log4j format. The **Diagnostics | Logging Viewer** menu provides links for information about and installing Apache Chainsaw 78 which is a suitable logging application .



2.4.3 Network Routes

This menu can be used to test routing from the one-X Portal for IP Office server to an IP Office address. It uses TCP to port 7 (Echo service) on the target IP address. Note that this does not work with IP Office control units, for which the IP Office Connections 37 should be used instead.

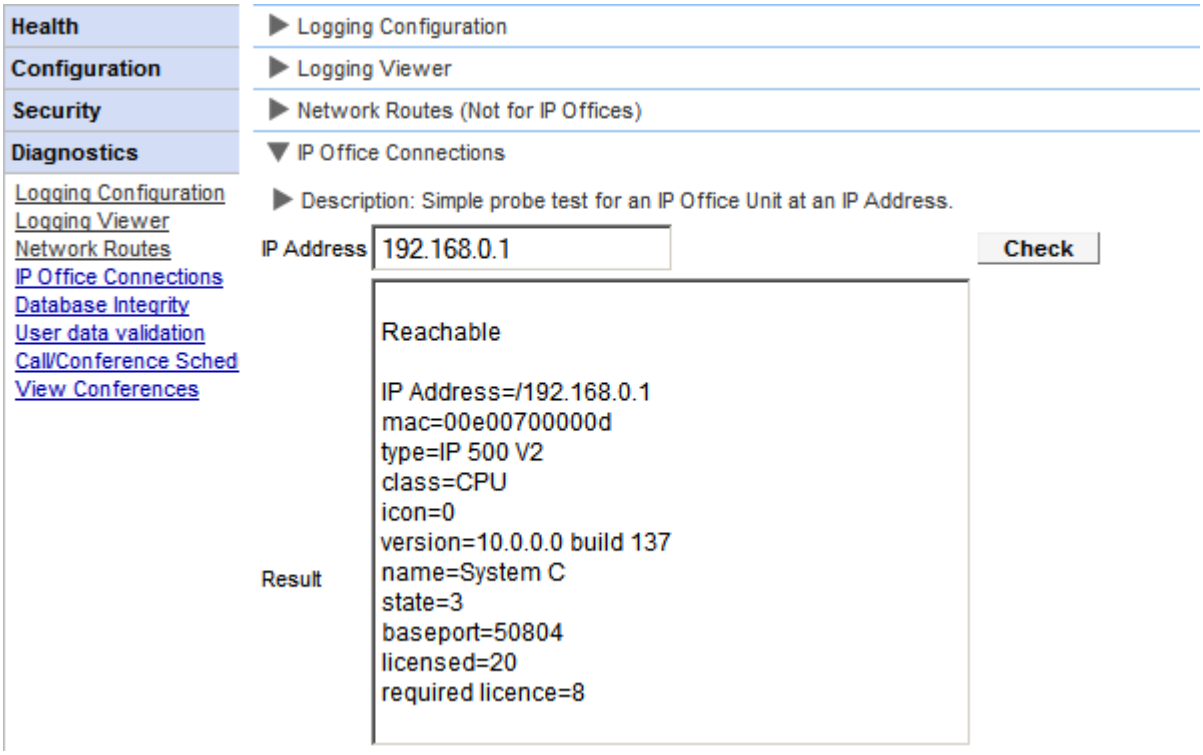


To check a network route:

1. Select **Diagnostics** and then **Network Routes**.
2. Enter the **IP Address** of the target and click on **Check**.
3. The one-X Portal for IP Office server will report whether the target is ***Reachable*** or ***Not Reachable***.

2.4.4 IP Office Connections

This menu can be used to check the connection between the one-X Portal for IP Office server and a particular IP Office. The connection check uses the standard discovery method used by IP Office applications such as IP Office Manager (connection to port 50804 of the IP Office control unit).

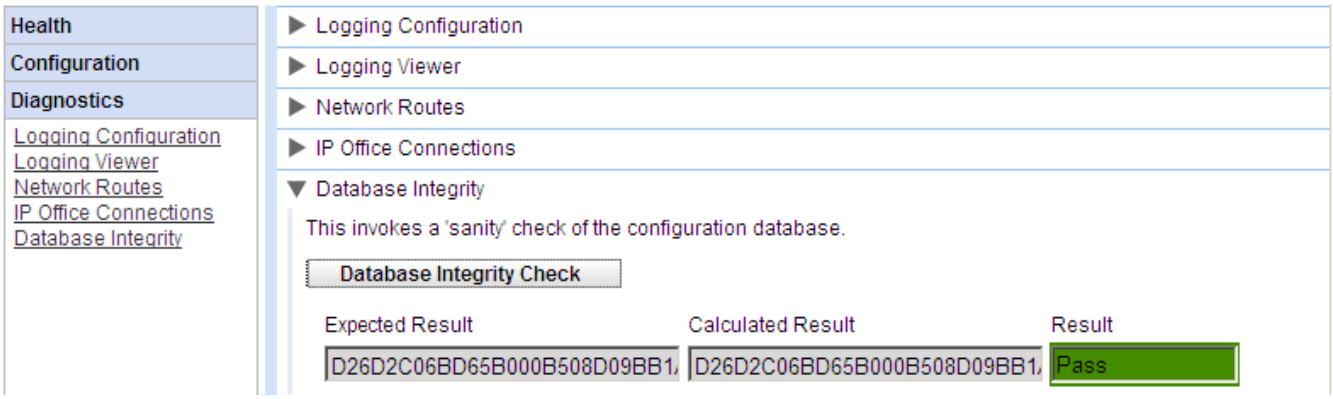


To test the IP Office connection:

1. Select **Diagnostics** and then **IP Office Connections**.
2. Enter the **IP Address** of the target IP Office and click on **Check**.
3. If the IP Office is reachable, the results will include base information about the IP Office system.

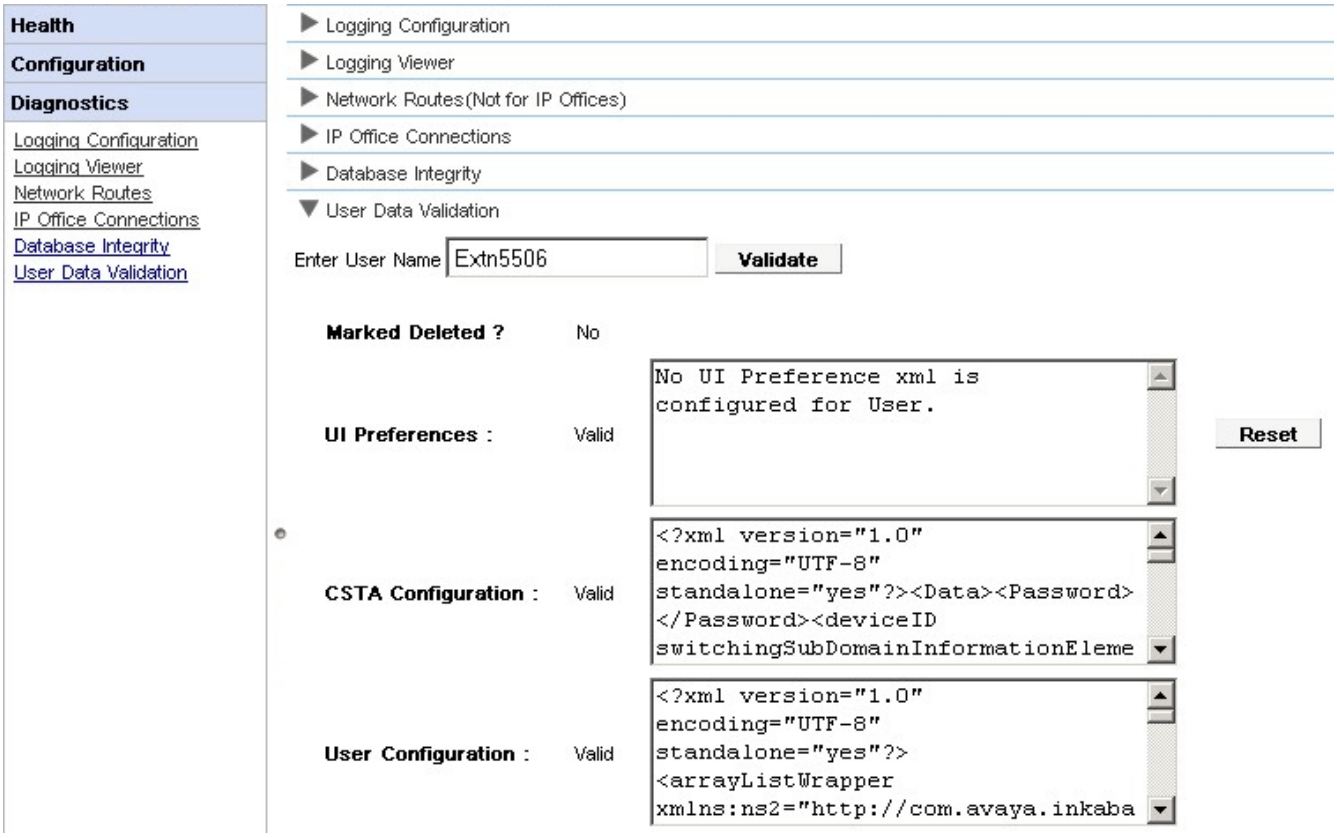
2.4.5 Database Integrity

This menu can be used to check the database structure. It will return **Pass** if the tables and fields within the database are as expected for the particular version of one-X Portal for IP Office. It does not check the data within the fields.



2.4.6 User Data Validation

The Administrator and Avaya Backbone Support group can identify possible cause of user login failure or user data corruption and reset the corrupt data using the diagnostic feature in one-X Portal for IP Office.

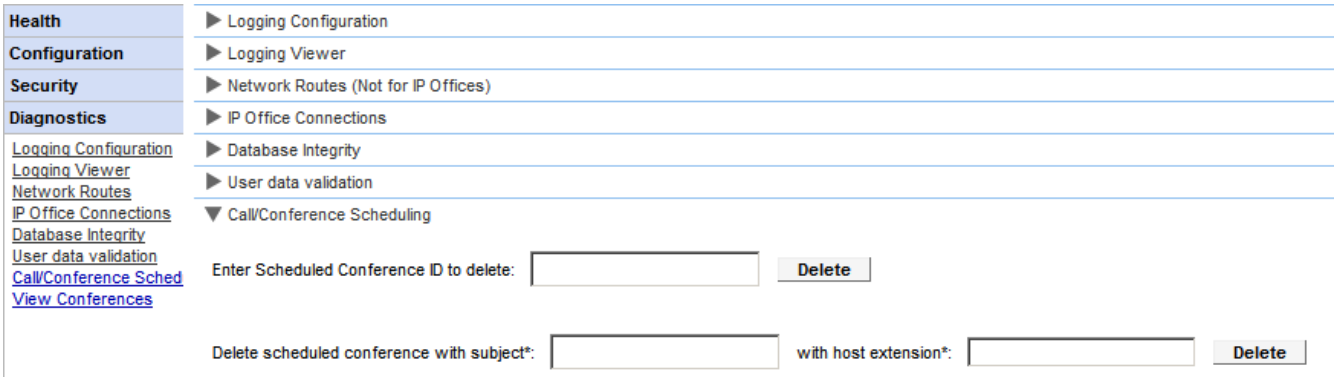


To view the user data validation:

1. In the Administrator interface of one-X Portal for IP Office, click **Diagnostic**.
2. Select **User Data Validation** to display a corresponding form on the right.
3. **Enter the User Name** of the user whose data has to be validated. This field has auto-complete feature as a drop-down menu.
4. Click **Validate**. The system validates certain fields of the user data in the database and displays the result. The fields validated are:
   - **Marked Deleted?:** If the user record is marked as deleted or not.
   - **UI Preferences:** If UI preference data is valid or not along with the corresponding XML. A **Reset** button is provided to reset the data if it is corrupt. The UI preference is restored to default factory settings. The user has to re-login to access the one-X Portal for IP Office.
   - **CSTA Configuration:** If CSTA configuration data is valid or not along with the corresponding XML.
   - **User Configuration:** If User configuration data is valid or not along with the corresponding XML.

2.4.7 Call/Conference Scheduling

You can delete a future scheduled conference. If the conference is a recurring conference, all occurrences of the conference are deleted.

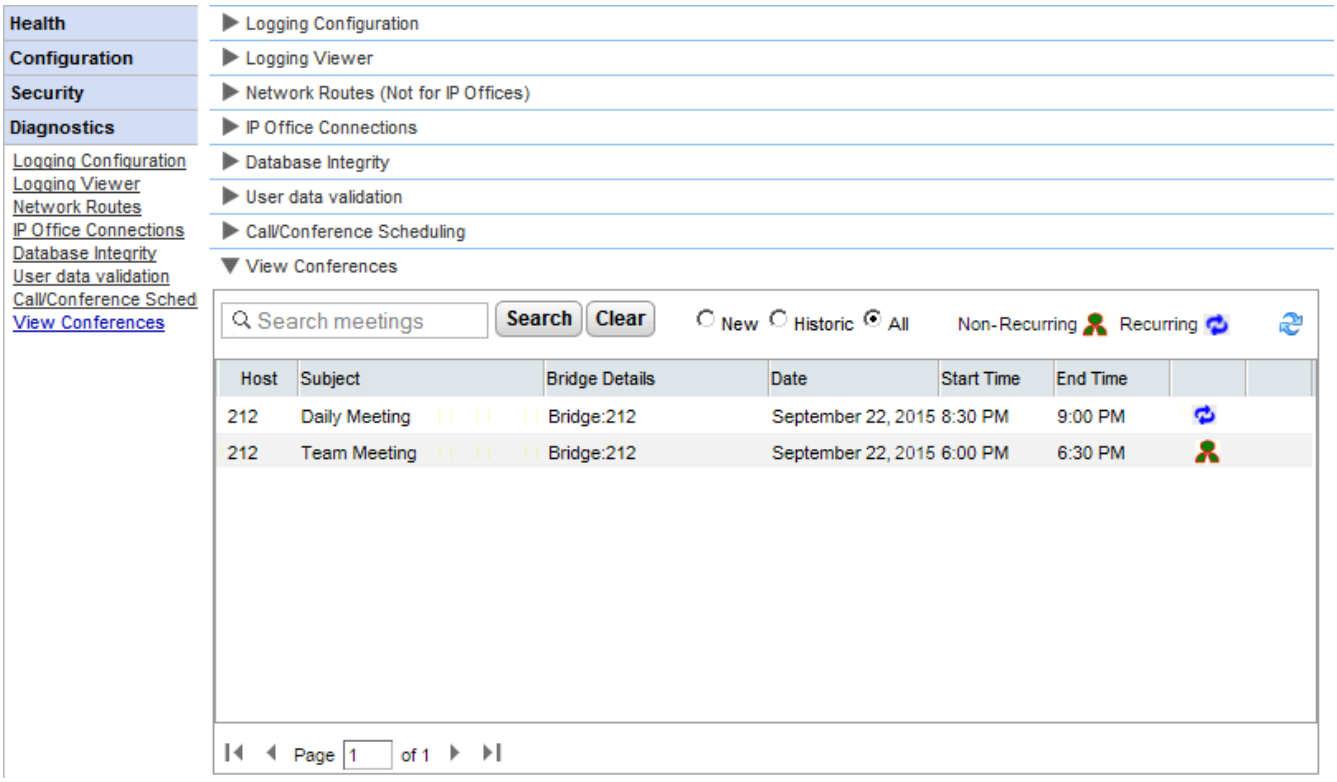


To delete a scheduled conference or conferences:

1. Click **Diagnostics** and select **Call/Conference Scheduling**.
2. Enter the host extension and a subject. If you leave the subject blank, all conferences scheduled by the host are deleted.
3. Click **Delete**.

2.4.8 View Conferences

This menu displays the calendar for scheduled conference similar to that seen and used by individual one-X Portal for IP Office users. The difference however is that is shows the scheduled conferences for all users. You can use this menu to delete a scheduled conference and to modify the details of future conferences.



2.4.9 Generate Memory Dump

In order to diagnose issues, Avaya may request a memory dump. This menu creates a memory dump log file for the server's current state of operation. The file is named based on the date and time, suffixed with **.hprof**.

Any existing memory dump files are included in the log files downloadable from the server's web control/platform view menus (**Logs | Download**).

2.4.10 Generate Thread Dump

In order to diagnose issues, Avaya may request a thread dump. This menu creates a thread dump log file for the server's current state of operation. The file is ***onex_thread_dump*** plus the date and time, suffixed with **.log**.

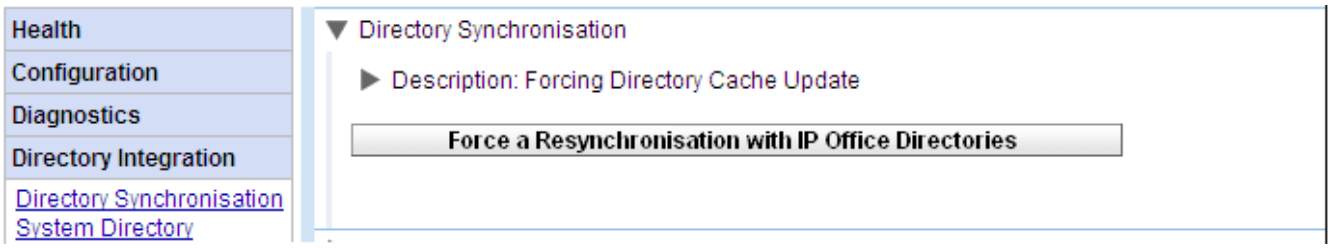
Any existing memory dump files are included in the log files downloadable from the server's web control/platform view menus (**Logs | Download**).

2.5 Directory Integration

This section allows you to view and check the servers integration with the directories that it uses.

2.5.1 Directory Synchronisation

During normal operation, the one-X Portal for IP Office server updates the records every 300 seconds approximately. However, this menu can be used to force an update of the system directory and IP Office users.



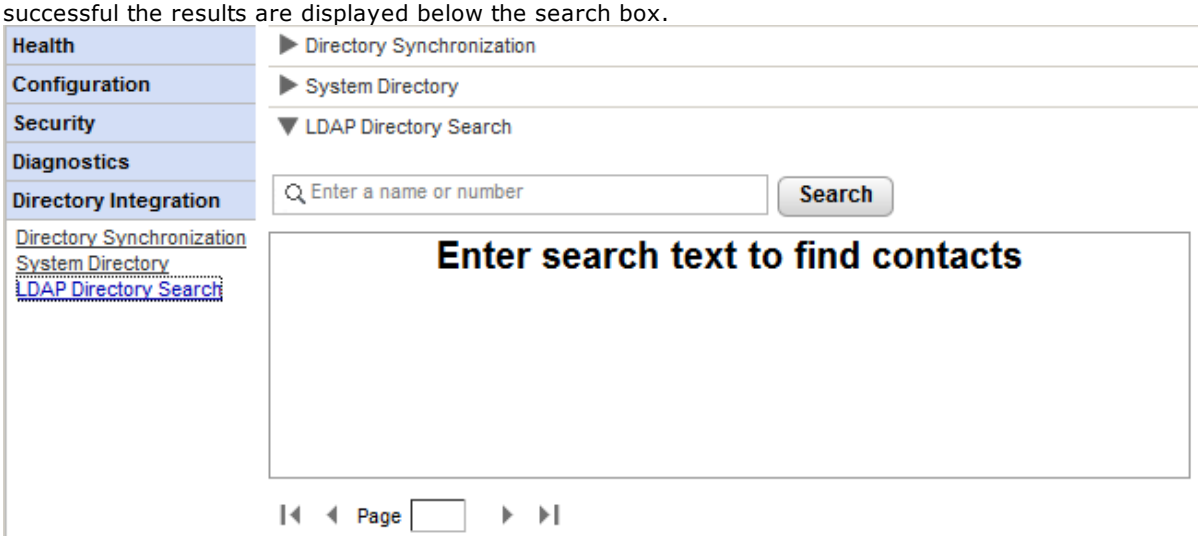
- **Force a Resynchronization with IP Office Directories**
  Requests an update of the system directory entries stored in the configurations of the IP Office systems. The entries in the **System Directory** can also be viewed and checked through the **Directory Integration | System Directory** 42 option.

2.5.2 LDAP Directory Search

This option allows you to search the external directory in the same way as one-X Portal for IP Office users. This allows you to test the operation of the LDAP Provider 63.

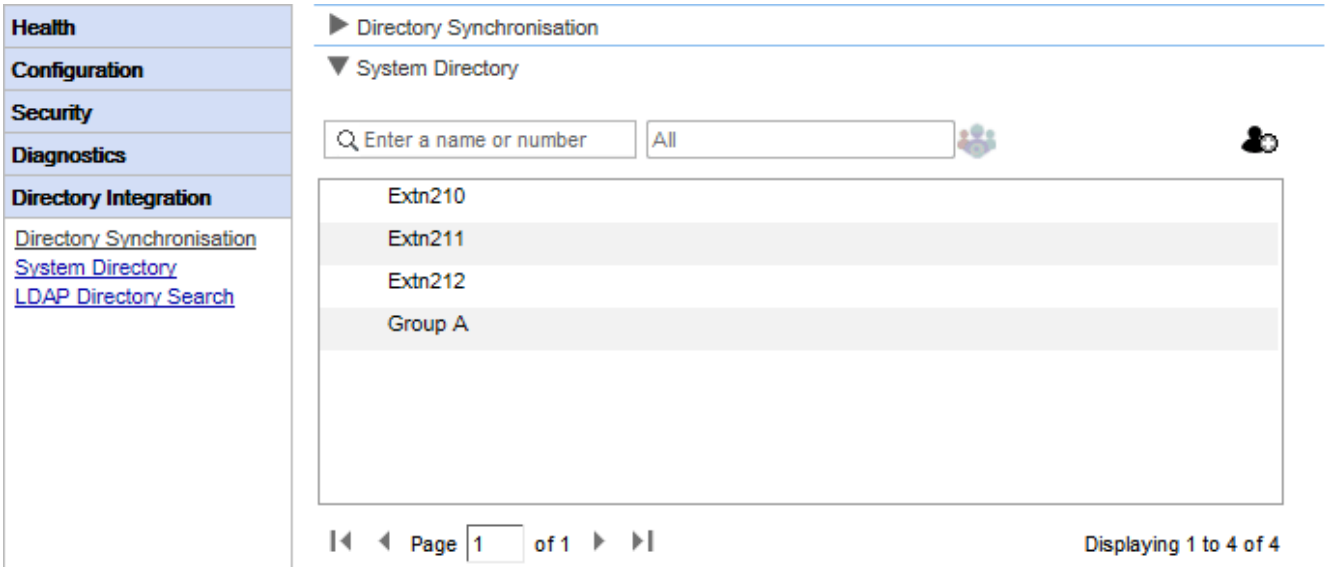
To search the LDAP directory:

1. Select **Directory Integration**.
2. Select **LDAP Directory Search**.
3. Enter a name or number that you know is in the external directory and click **Search**. If the search is successful the results are displayed below the search box.



2.5.3 System Directory

This option shows you the system directory as being shown to the one-X Portal for IP Office users. You can search the directory in the same way as if you were using the one-X Portal for IP Office client.



You can use this menu to verify the directory is as expected, with users, groups and directory entries from each IP Office being supported.

- **Note:** The system does not display hunt groups set as *"Ex-directory"* in the telephone system configuration.

The one-X Portal for IP Office server updates system and personal directory records every 300 seconds approximately. You can force an update using the **Directory Synchronization** 41 option.

- For some directory contacts, one-X Portal for IP Office indicates the contacts current status by using different icons. For contacts that have multiple telephone numbers, the status is based that of the work number.

State	Icon	Description
Available		The normal state for a user showing the status of their work extension in use.
Busy		The normal state for a user showing that their work extension is currently on a call.
Do Not Disturb		The user has set **Do Not Disturb**. Calls to them will go to voicemail if enabled or else get busy tone unless you are in the user's **Do Not Disturb exception list**.
Logged Out		The user has logged out from their phone. Calls to them will most likely go to voicemail if available.
Other		This icon is used when the status is not known or cannot be known, i.e. external numbers.
Ringing		This icon is used for an internal contact that is currently ringing.

Adding and Editing Portal Contacts

You can use the icon to add a new system directory contact. Note that contacts added in this way are stored by one-X Portal for IP Office only are accessible by users through one-X Portal for IP Office only. These contacts can have multiple phone numbers and email addresses configured if required.

To delete contacts that have been added in this way, click on the contact and select the delete icon.

2.6 Gadget configuration

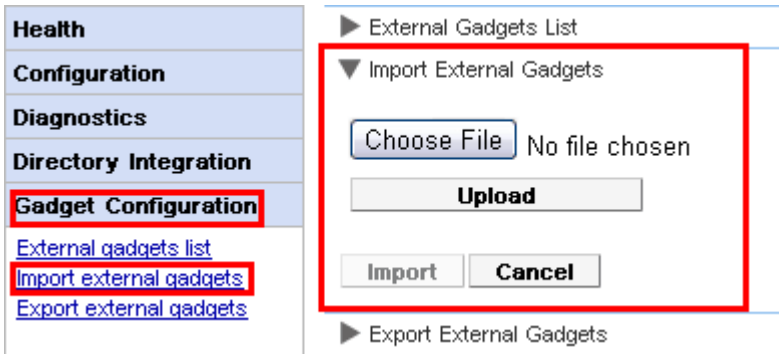
As an administrator of one-X Portal for IP Office you can configure a list of external gadgets in the system. You can enable, edit, and delete the gadgets that the user of one-X Portal for IP Office can add. The user of one-X Portal for IP Office can add only those external gadgets that the administrator enables.

2.6.1 External gadget list

All the external gadgets that are in the system are listed in the **External gadgets list**. By default, there are no external gadgets configured on the one-X Portal for IP Office. As an Administrator, you can add an external gadget 59 or import external gadgets 56 for the user.

2.6.2 Importing gadgets

You can import external gadgets as an XML file. Those gadgets are then available for users to select. See Importing gadgets 56.



To import a gadgets file:

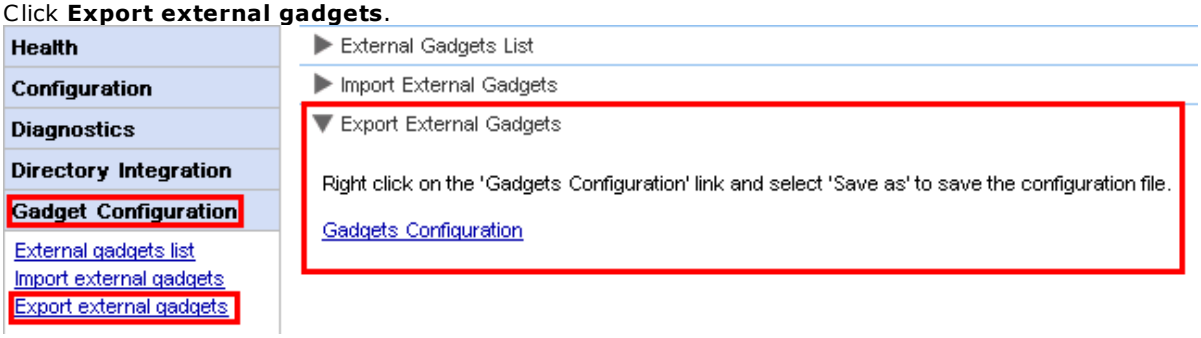
1. Click **Gadget Configuration** and select **Import external gadgets**.
2. Click **Choose File** to browse for the configuration file.
3. Click **Upload**. The system uploads the XML file on the one-X Portal for IP Office.
4. Click **Import** to add the third party gadget to the *Gadgets List*.
5. The next time the user logs into the one-X Portal for IP Office, the third party gadget is available to user to add to their portal.

2.6.3 Exporting Gadgets

The existing set of external gadgets in the one-X Portal for IP Office can be exported as a configuration file. The configuration file is in an XML format. The configuration file contains information about the gadget parameters. You can add this set of gadgets to the one-X Portal for IP Office of another user by importing 56 the saved configuration file.

To export a third party gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **Export external gadgets**.



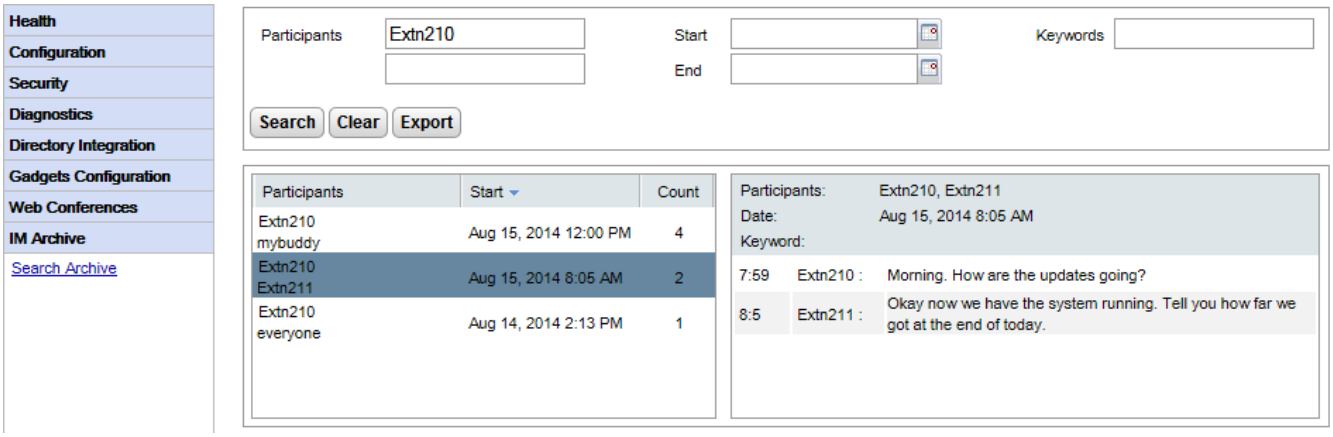
3. Right click on the **Gadgets Configuration** link.
4. Select ***Save as*** to save the configuration file.

2.7 IM Archive

As an administrator of one-X Portal for IP Office you can search the IM conversations of all the users. See Enabling/Disabling IM Archiving 67.

2.7.1 Search Archive

You can search for the instant message conversations between the users and from the system to a user. All the fields in the search panel are optional. The number of days that the server retains an IM in the archive is set by the Days to archive IMs 68 setting.



To search the IM archive:

1. In the left panel, select the **IM Archive**.
2. Click **Search Archive**.
3. Enter the search criteria and click Search.

Field	Description
Participants	Type the name of the participant in the IM conversation.
Keywords	Type the keywords in the IM conversation.
Start	Select the date from which the conversations need to be listed. If you do not select a date, the system displays from the earliest conversation that the system has retained.
End	Select the date until which the conversations need to be listed. If you do not select a date, the system displays until the latest conversation.

4. Click on the conversation that you want to open. The system displays the conversation.

2.8 Help & Support

Help | Help

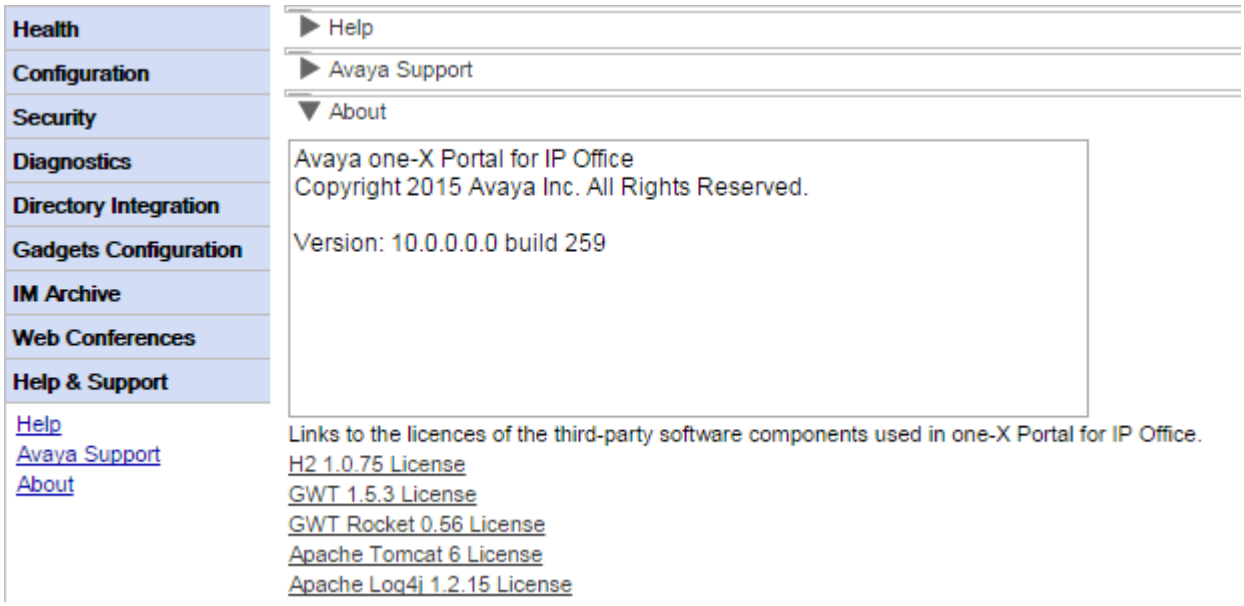
Provides links to both the one-X Portal for IP Office user help and to this document as help.

Help | Avaya Support

Loads a link to the Avaya support website (http://support.avaya.com).

Help | About

Shows basic version information for the one-X Portal for IP Office installation.



Chapter 3.
Maintenance Tasks

3. Maintenance Tasks

3.1 Restarting the Service

The one-X Portal for IP Office service can be stopped and restarted in a number of ways.

- Do not restart the one-X Portal for IP Office service whilst any Voicemail Pro client is connected to the voicemail server. Doing so will cause conference access and scheduling features to not operate correctly as the portal service needs administrator access to the voicemail server during a restart.

From the portal Administrator menus

You can click the icon at the top of the administrator menus to restart the portal. Note that this icon appears automatically if you make any changes that require a restart.

From the server menus

1. Through the web management menus for the server, select **Solution**.
2. Click on the ☰ icon and select **Platform View**.
3. In the platform view, the status of the one-X Portal service is shown on the **System** tab. To stop the service, click **Stop** or **Force Stop**. To start the service, click **Start**.

3.2 Call Log Configuration

The user call log shown by one-X Portal for IP Office is stored on the telephone system as part of the user's settings. Up to 30 records are stored, with new records replacing the old ones when the limit is reached. However, for repeated call to or from the same number, the existing record is updated and the number of calls count increased.

For incoming call, by default, only personal calls (non hunt group) to the user that were answered by the user or which went unanswered anywhere are included in the call log.

- **Missed Calls**
  Calls that the user does not answer but are answered by voicemail or another extension are not normally logged as missed calls. To enable the logging of missed calls, the system-wide setting **Log Missed Calls Answered at Coverage** (**System | Telephony | Call Log**) should be enabled in the IP Office telephone system configuration.
- **Missed Hunt Group Calls**
  By default, only hunt group calls that the user answers are logged. To enable the logging of missed hunt group calls, the system-wide setting **Log Missed Huntgroup Calls** should also be enabled in the IP Office telephone system configuration. The user must also be configured in the telephone systems with the hunt groups for which their call log can include missed calls (**User | Telephony | Call Log**).
- **Automatic Deletion**
  Old call records are automatically deleted when the call log capacity is reached and a new call record needs to be added. In addition, through the telephone system configuration you can configure the telephone system to delete log entries after a set period. Select **Delete entries after** (**User | Telephony | Call Log**).

Phone Conversation History

For users using Avaya phones with a **Call Log** or **History** button, by default the same call log as shown by the portal is also shown on the phone. You can then use and edit the call log from the phone or from one-X Portal for IP Office. The two change in parallel.

Users, using any other type of phone that has a call log, that call log is stored by the phone itself and so does not necessarily match the call log shown in one-X Portal for IP Office. For example, calls made using the one-X Portal for IP Office do not appear in the phone's call log and vice versa.

In either case, the one-X call log is limited to displaying 255 records.

3.3 IP Office Switch

3.3.1 Adding an Additional IP Office

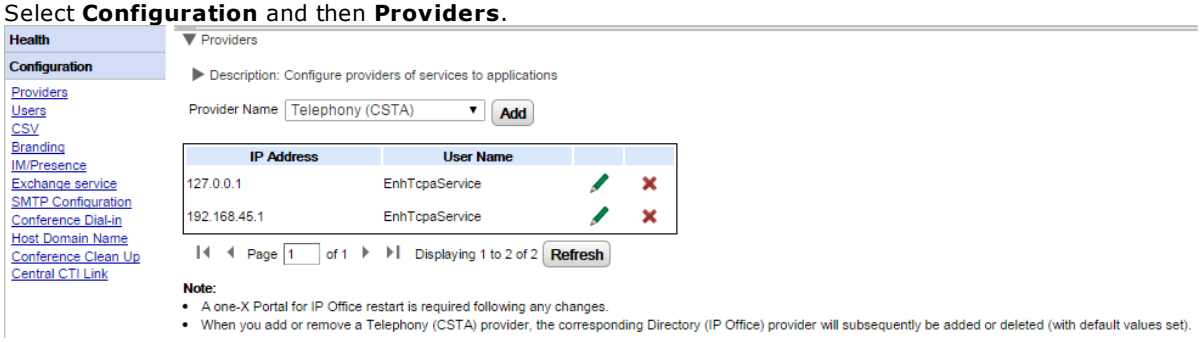
To add an additional IP Office within the Small Community Network, its IP address needs to be assigned to the **Telephony (CSTA)** and **Directory (IP Office)** providers.

- **Automatic Provisioning/Centralized CTI Mode** 31
  For a portal server supporting a Linux-based IP Office network, the server can be informed by the primary IP Office system about other IP Office systems in the network and about the voicemail server. It then automatically adds or removes the appropriate providers for those other systems. This is done using the **Central CTI Link setting** 31, which is on by default for new installations. When enabled, manual configuration of providers for additional IP Office systems is not necessary. In centralized CTI mode:
  - If not using resilience, the server only requires a DSML provider to the primary IP Office system.
  - If using resilience, the server only requires a DSML provider to the primary and secondary IP Office systems.
  - The server only requires a CSTA provider to the primary IP Office system unless using portal resilience in which case it also needs a CSTA provider to the secondary IP Office system.

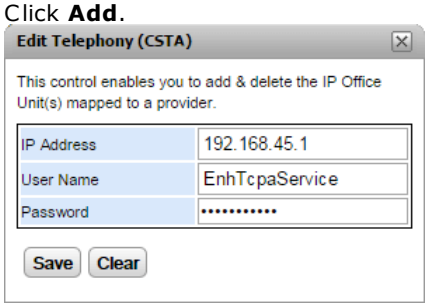
To add another IP Office system:

- **Warning**
  This process requires you to restart the portal service 48 for the changes to take effect. During the restart, the portal may not be available to users for up to 15 minutes.

1. Before adding another IP Office to the one-X Portal for IP Office configuration:
   - Check that the IP Office has been configured with the security settings for one-X Portal for IP Office operation.
   - Check that the IP Office is licensed for one-X Portal for IP Office.
   - Check that at least one user on the IP Office has been enabled for one-X Portal for IP Office.
2. Log in 8 to the administrator menus.
3. Check that the IP Office can be seen from the one-X Portal for IP Office server.
   a. Select **Diagnostics** and then **IP Office Connections**.
   b. Enter the **IP Address** of the target IP Office and click on **Check**.
   c. If the IP Office is reachable, the results will include information about the IP Office system.
4. Select **Configuration** and then **Providers**.



5. Click **Add**.



6. Enter the **IP Address** of the new IP Office system.

7. Enter the **User** name and **Password** that match the TCPA security user configured in the IP Office system.
8. Click **Save**.
9. Restart the Avaya one-X Portal service 48. When the service has fully restarted, log in to the administrator menus again.
10. Select **Health** and then **Component Status**.
11. Click on **Get All**. New CSTA and DSML components for the IP address of the newly added IP Office should be included. The status of these should be available.
12. Select **Directory Integration**. Check that the new IP Office system's users are listed. If not, select **Directory Synchronization | Force a resynchronization with IP Office Directories** and wait 5 minutes.
13. Select **Configuration** and then **Users**. Click **Get All**. Check that the new IP Office system's users are listed.

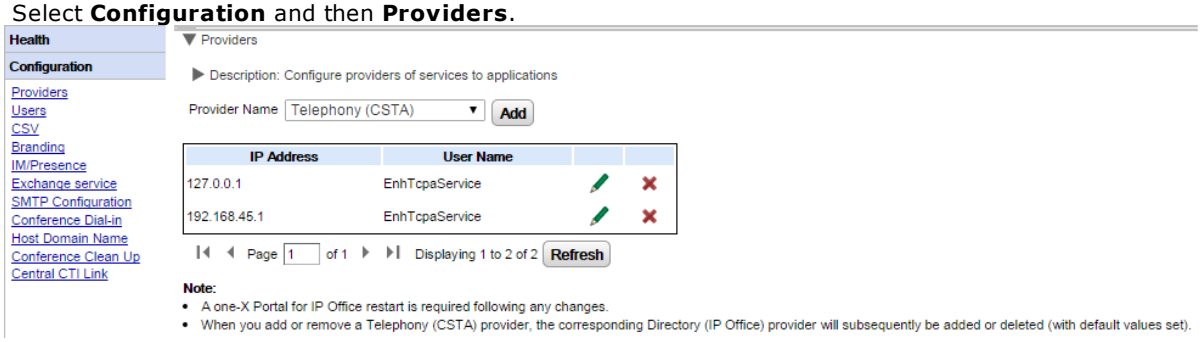
3.3.2 Changing IP Office Details

If the details (IP address, TCPA service user name or password) of an assigned IP Office are changed, the IP Office settings within the one-X Portal for IP Office providers must be updated to match.

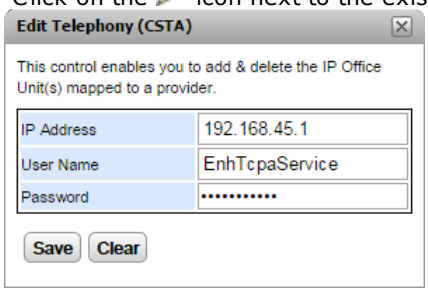
- **Warning**
  This process requires you to restart the portal service 48 for the changes to take effect. During the restart, the portal may not be available to users for up to 15 minutes.

To change the IP Office details:

1. Log in 8 to the administrator menus.
2. If it is the IP Office IP address that has changed, check that the IP Office can be seen from the one-X Portal for IP Office server.
   a. Select **Diagnostics** and then **IP Office Connections**.
   b. Enter the **IP Address** of the target IP Office and click on **Check**.
   c. If the IP Office is reachable, the results will include base information about the IP Office system.
3. Select **Configuration** and then **Providers**.



4. Click on the icon next to the exising CSTA provider to which the IP Office was assigned.



5. Edit the details displayed to match the new settings of the IP Office system and click **Save**.
6. Restart the portal service 48.

3.3.3 Resilience

For IP Office Release 10 and higher, the portal service is also installed by default on the IP Office Server Edition secondary server. This allows that secondary server to act as the portal server for users when, for some reason, the primary server is not available.

- Portal resilience is supported in IP Office Server Edition Select mode. Portal resilience can also be configured when using an IP Office Application Server in place of the primary or secondary server's portal service.
  - On existing non-IP Office Server Edition Select mode systems that have then been switched to IP Office Server Edition Select mode, it may be necessary to restart the portal services for resiliency settings to become available. Similarly it may be necessary to restart the portal services after first configuring portal resiliency in the IP Office system configuration.
- Resilience is only supported between primary and secondary servers running the same version of portal software.
- During normal operation (both servers running and connected), user and administrator changes made on the primary server are automatically synchronized to the secondary server. However, during resilience, changes made on either server are not synchronized and may be lost when the servers return to normal operation.
  - Scheduled conferences are currently an exception to the above. Conferences scheduled on the primary do not occur when running in failover. Conferences scheduled on the secondary are lost when failback occurs.
- Within the platform view (web control panel) of each server:
  - the active portal server is displayed as 'Available' (a green icon).
  - the passive portal server is displayed as 'Starting' (an amber icon).
- Portal client applications such as one-X Portal Call Assistant are not automatically redirected. The user has to enter the address of the secondary server in order to login.

When portal resilience is configured:

- **On primary server portal failure**
  If the primary server's portal service stops for some reason, the portal service on the secondary server automatically becomes available.
  - Users who were logged into the portal on the primary are able to login again on the secondary server.
    - If the primary IP Office service is still running, those portal users are automatically redirected.
    - If the user has not previously accessed the secondary portal server, they may need to accept the security certificate or create an exception which will interrupt automatic re-connection.
  - The same applies for users who were logged into one of the portal clients such as the Outlook Plug-in
  - New users wanting to login will have to use the address of the secondary server.
- **On primary server IP Office failure:**
  If the primary server's IP Office service stops for some reason, portal services are automatically transferred to the secondary server as above.
  - When IP Office core is not up, users belonging to that IP Office core cannot update or delete personal contacts from the portal directory gadget.
- **On network failure:**
  If the network connection between the primary and secondary server fails for some reason, both portal servers become active and can be logged into. Again user and admin changes on secondary portal server are not copied to primary when the network connection recovers. This is referred as "Standalone Mode".
- **On primary server portal recovery:**
  When the primary server's portal service is available again, the portal service on the secondary server stops supporting login.
  - Users who were logged into the portal on the secondary are automatically re-directed to login again on the primary server.
  - Users who were logged into one of the portal clients such as the Outlook Plug-in are automatically connected to the primary server.
  - New users wanting to log in are redirected to the primary.
- **On primary server IP Office recovery:**
  When the primary server's IP Office service is available again, portal service support also returns to the primary server as above.

To configure resilience:

1. **Enable Centralized CTI Link Mode**
   Both portal servers must be set to use centralized CTI link mode. That is the default for a new installation but must be manually enabled for existing systems upgraded to IP Office Release 10 or higher.

   a. Centralized CTI link mode is enabled through the **Central CTI Link** 31 menu.

   b. If the setting is changed, the portal service must be restarted for the change to take effect.

   c. The setting must be enabled on both the primary and secondary servers.

2. **Enable Portal Server Resilience**
   The primary portal server needs to be configured for resiliency through its **Resilience Configuration** 28 menus.

3. **Restart the Portal Services**
   If any changes are made in the steps above.

4. **Enable Portal Backup on Network Trunks**
   The SCN trunks between the primary and secondary IP Office severs need to have the setting for portal backup enabled.

   a. Using IP Office Manager, load the configuration from the IP Office Server Edition IP Office systems.

   b. In the settings of the primary, locate the IP Office line from the primary to the secondary IP Office system.

   c. On the **Line** tab, in the **SCN Resiliency Options**, check that **Supports Resiliency** and **Backs up my one-X Portal** are selected.

   d. Save the configuration changes.

3.4 Gadgets

3.4.1 Fetching a gadget URL

Google provides a range of gadgets that you can add to your webpage.

Example: To get the URL of a Google gadget:

1. To get a list of gadgets that Google provides go to: http://www.google.com/ig/directory?synd=open
2. Select the gadget that you would like to add to your webpage.
3. Click **Add to your webpage**.
4. Click **Get the Code**. The system displays a string similar to that shown below. The text that is within the " " quotes is the URL for the gadget.:

```
<script src="http://www.gmodules.com/ig/ifr?
url=http://www.donalobrien.net/apps/google/currency.xml&amp;up_def_from=USD&amp;up_def_to=EUR&amp;
synd=open&amp;w=320&amp;h=170&amp;title=Currency+Converter&amp;border=%23ffffff%7C0px%
2C1px+solid+%2382CAFA%7C0px%2C2px+solid+%23BDEDFF%7C0px%2C3px+solid+%
23E0FFFF&amp;output=js"></script>
```

3.4.2 Importing gadgets

Third party gadgets can be added to the one-X Portal for IP Office using an XML file. You can upload a maximum of 50 gadgets at a time. The file size must not exceed 2MB.

For each gadget, the following parameters need to be specified:

- URL of the gadget, that is, the source of gadget and its content
- Name of the gadget displayed on the gadget title bar
- Toolbar icons for the gadget. It is recommended to provide toolbar icons for all gadgets specified in gadgets.xml.
- Gadget toolbar texts (the tool tip text and the text that appears below the toolbar icon).

An example of a gadgets XML file format:

```
<GadgetsConfigurationImpl>
<gadgetRecords>
<entry>
<key>1</key>
<value>
<categorys>1</categorys>
<categorys>2</categorys>
<created>2012-08-10</created>
<defaultToolbarIcon />
<downToolbarIcon />
<deleted />
<enable>true</enable><external>true</external><height>300</height><id>1</id>
<localizedName><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB></names></localizedName>
<name>Angry Birds</name>
<toolbarText><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB></names></toolbarText>
<tooltip><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB></names></tooltip>
<url>http://www.gmodules.com/ig/ifr?
url=http://www.forumforyou.it/google_gadget_angry_birds.xml&amp;synd=open&amp;w=820&amp;h=680&amp;title
=Angry+Birds&amp;border=%23ffffff%7C3px%2C1px+solid+%23999999&amp;output=js</url>
</value>
</entry>
</gadgetRecords>
</GadgetsConfigurationImpl>
```

Note: Ensure the following in the .xml file:

1. Place each of the gadget within the <entry></entry> element.
2. The element <key></key> should be unique and it should match with <id></id>. This is a unique gadget id used for internal purpose.
3. The element <value></value> should contain gadget information.
4. The element <categorys></categorys> indicates the category of the gadget. The IDs and codes for the categories are as follows:

Code	Category
1	ALL
2	COMMUNICATION
3	TOOLS
4	PRODUCTIVITY
5	FINANCE
6	TECHNOLOGY
7	ZOHO

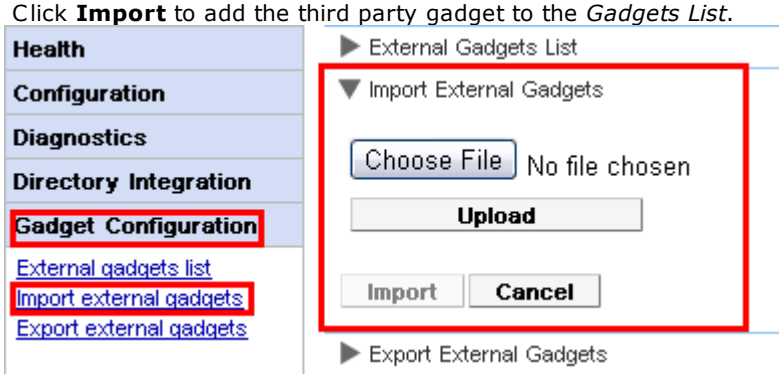
5. Details of other elements:

Element	Description
<created>	The date you created the file.
<defaultToolbarIcon>	Specify the default toolbar icon that the system displays when you minimize the gadget is minimized. The system displays the icon in the toolbar of the user.
<downToolbarIcon>	Specify the toolbar that system displays when the user clicks the gadgets icon.
<enable>	Specify the value to true if you want the user to view the gadget.
<external>	Set the value as true for all external gadgets.
<height>	Set the height of the gadget in pixel.
<id>	ID of the gadget.
<localizedName>	Specify the localized name for each locale.
<name>	Specify a unique name for the gadget.
<toolbarText>	The text that the system displays in the gadget toolbar.
<tooltip>	The text that the system displays in the gadget tool tip.
<url>	The URL of the gadget. For more information see, Fetching the URL of an external gadget - Example 55

Note: Appropriate error messages are displayed if the configuration file does not support any of the aforementioned criteria.

To import a gadgets file:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **Import external gadgets**.
3. Click **Choose File** to browse for the configuration file.
4. Click **Upload**. The system uploads the XML file on the one-X Portal for IP Office.
5. Click **Import** to add the third party gadget to the *Gadgets List*.



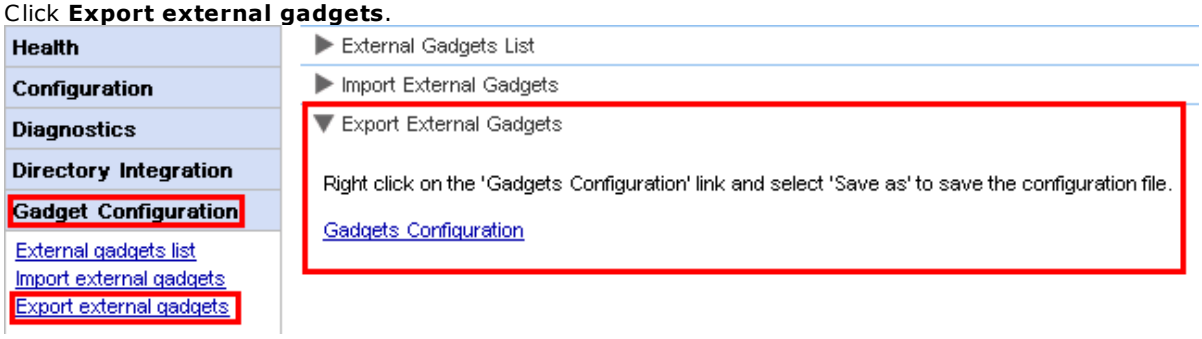
6. The next time the user logs into the one-X Portal for IP Office, the third party gadget is available to user to add to their portal.

3.4.3 Exporting Gadgets

The existing set of external gadgets in the one-X Portal for IP Office can be exported as a configuration file. The configuration file is in an XML format. The configuration file contains information about the gadget parameters. You can add this set of gadgets to the one-X Portal for IP Office of another user by importing 56 the saved configuration file.

To export a third party gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **Export external gadgets**.



3. Right click on the **Gadgets Configuration** link.
4. Select ***Save as*** to save the configuration file.

3.4.4 Adding an external gadget

To add a single gadget you need the URL of the gadget. For more information about how to get the URL of gadget see Fetching the URL of an external gadget - Example 55.

To add an external gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **External gadgets list**.
3. Click **Add**. The system displays **Add Gadget** dialog box.
4. Add the details of the gadget (see below) and click **Save**. The system updates the external gadget that you added in the one-X Portal for IP Office database.

Gadget Fields

Field name	Description
Gadget name	The system displays the name that you specify in this field on the title bar of the gadget. Ensure that the name of the gadget does not exceed 50 characters.
Gadget URL	Contains the URL of the gadget. The URL that you provide should conform to the standards URL specification of http://www.w3.org/Addressing/URL/url-spec.txt. The system uses the URL that you specify to display the gadget.
Localized gadget name	The system displays the localized name that you specify in this field on the title bar of the gadget. The system displays the localized name only if the user of one-X Portal for IP Office selects a language while logging in.
Toolbar icon label	The system displays the text that you set in this field as the label of the gadget in the toolbar. If you do not specify the text, the system displays the entire gadget name.
Toolbar icon tool tip text	The system displays the tool tip that you set in this field for the gadget when the user hovers over the gadget icon in the toolbar.
Toolbar icon	The system displays the icon that you set in this field on the toolbar. Ensure that the image type is only png, gif, or jpeg, the dimension of the image is 37*37 pixels, and the maximum size of the image is 10KB. If you do not set an icon, the system displays the default image.
Toolbar icon on mouse click	The system displays the icon that is set in this field when you click the icon in the toolbar. Ensure that the image type is only png, gif, or jpeg, the dimension of the image is 37*37 pixels, and the maximum size of the image is 10KB.
Enabled	The system enables the gadget for all the users of one-X Portal for IP Office.
Gadget height	The system displays the height of the gadget to the height that you set in this field. The default height of the gadget window is set to 300 pixels in this field. You can set the height of the gadget window only when you add a gadget. You can not edit the height of the gadget after you add a gadget.

3.4.5 Editing an external gadget

You can edit the details of a gadget such as the name of the gadget, the URL of the gadget, the text that appears in the toolbar, tool tip, icon that appear in the toolbar, and the icon that appears on a mouse click.

To edit an external gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **External gadgets list**.
3. Click **Get All**. The system displays a list of all the external gadgets that are available in the system.
4. Click **Edit** to edit the details of the gadget. The system displays **Edit Gadget** dialog box.
5. See Adding an External Gadget 59 for details of the gadget fields. Update the changes that you would like to make and click **Save**.
6. Click **Put Selected**. The system updates the external gadgets that you edited in the one-X Portal for IP Office database.

3.4.6 Enabling an external gadget

When you enable a gadget, all the users of one-X Portal for IP Office can add that gadget.

To enable an external gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **Externals gadget list**.
3. Click **Get All**. The system displays a list of all the external gadgets that are available in the system.
4. Enable the gadget that the users of one-X Portal for IP Office can add to the one-X Portal for IP Office window.
5. Click **Put Selected**. The system updates the external gadgets that you enabled in the one-X Portal for IP Office database.

3.4.7 Disabling an external gadget

When you disable a gadget, one-X Portal for IP Office users cannot add that gadget to the one-X Portal for IP Office window. If you disable a gadget that the users have already added to their one-X Portal for IP Office window, the system does not display gadget when the users log in the next time.

To disable an external gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **External gadgets list**.
3. Click **Get All**. The system displays a list of all the external gadgets that are available in the system.
4. Disable the gadget that you do not want the users of one-X Portal for IP Office to the one-X Portal for IP Office window.
5. Click **Put Selected**. The system updates the external gadgets that you disabled in the one-X Portal for IP Office database.

3.4.8 Deleting an external gadget

To delete an external gadget:

1. Click **Gadget Configuration**, in the left navigation pane.
2. Click **External gadgets list**.
3. Click **Get All**. The system displays a list of all the external gadgets that are available in the system.
4. Select the gadget that you would like to delete.
5. Click **Delete**.
6. Click **Yes** to confirm that you would like to delete the gadget. The system updates the external gadgets that you deleted in the one-X Portal for IP Office database.

3.5 Users

3.5.1 Adding/Deleting Users

The one-X Portal for IP Office server is synchronized with the users that exist on the IP Office systems. Users are added and or deleted through the IP Office configuration. Changes to users on the IP Office systems will be updated within one-X Portal for IP Office and other clients using the portal after approximately 10 minutes.

3.5.2 Editing User Settings

You can use the portal administration menus to view and edit a number of user settings.

To edit user settings:

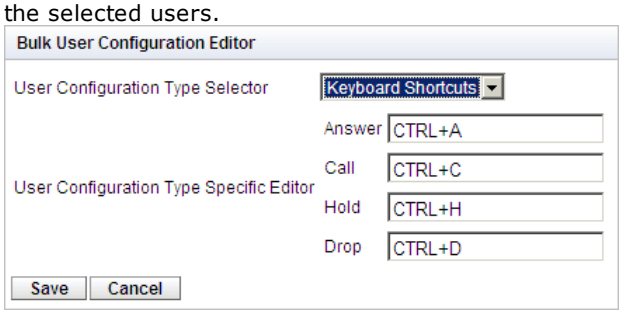
1. Select **Configuration** and then **Users**.
2. Click on **Get All**. and browse through the users.
3. Click on the **Edit** button next to the user you want to edit. The user configuration settings are displayed.

4. Use the **User Configuration Type Selector** to select the user settings you want to view/edit. If required edit the settings.
   - **Screen Popping**
     Displays the link for downloading the desktop client installation software used for one-X Portal Call Assistant and Outlook Plug-in.
   - **Park Slot**
     Allows configuration of the park slot numbers associated with the user's park buttons.
   - **Bridge Number**
     Allows configuration of the user's bridge number for their personal meet me conferences.
   - **TeleCommuter Mode**
     Allows selection of telecommute mode for the user and configuration of their home/mobile number to be used when that mode is active.
   - **IM/Presence Configuration**
     Allows configuration of the users IM/presence settings. Note that the user still needs to enable notifications through their own one-X Portal for IP Office session.
5. Click **Save**.
6. To commit the edited settings back to the one-X Portal for IP Office database, select the check box next to the user and click on **Put Selected**.

To bulk edit user settings:

1. Select **Configuration** and then **Users**.
2. Click on **Get All** and browse through the users.
3. Select the check box next to each of the users that you want to edit.
4. Click **Bulk Edit**.

5. Use the **User Configuration Type Selector** to select which user configuration settings you want to edit for all the selected users.



6. When you have completed editing, click **Save**.
7. Select the check box next to each of the users that you edited and click **Put Selected** to send the changes back to the one-X Portal for IP Office database.

3.6 Directories

3.6.1 Adding an LDAP External Directory Source

An LDAP provider is created by default during installation but not configured for connection to an LDAP sever (unless an Advanced Installation is selected and the LDAP provider settings altered). The process below changes the LDAP provider settings to allow LDAP operation.

LDAP operation can be tested through the **Directory Integration | LDAP Directory Search** 41 option in the administrator menus.

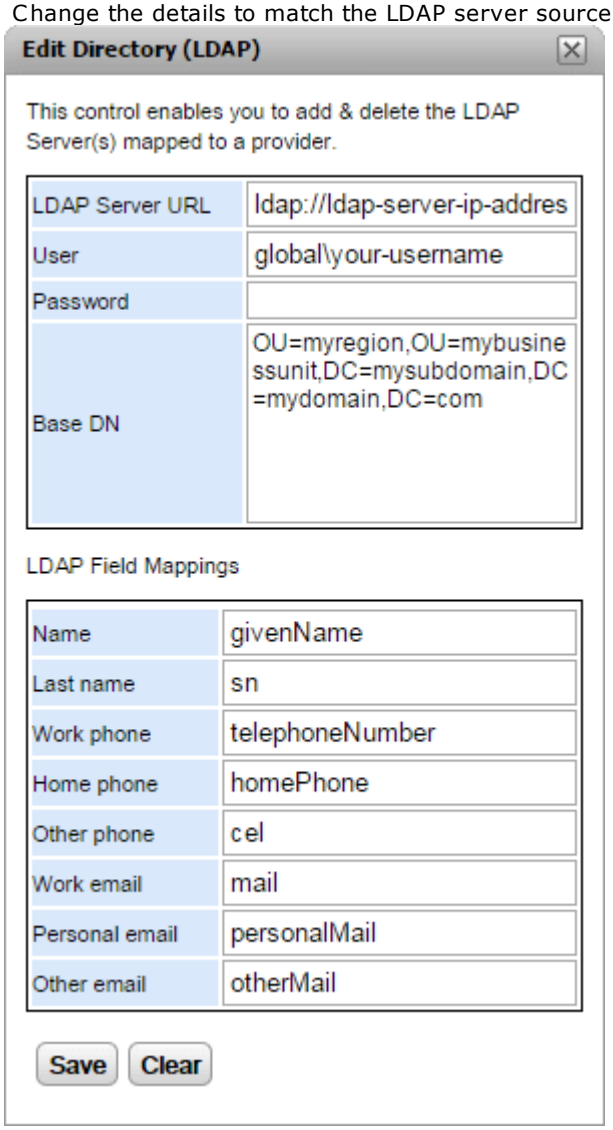
Unlike the LDAP support in the IP Office, the one-X Portal for IP Office sever does not import records from the LDAP source and then use those records as a directory. Instead, when a one-X Portal for IP Office user enters characters in the External Directory tab of the Directory gadget, the one-X Portal for IP Office server uses the LDAP source settings to do a live search of the LDAP source records. The one-X Portal for IP Office server therefore does not need to regularly update its LDAP records.

- **Warning**
  This process requires you to restart the portal service 48 for the changes to take effect. During the restart, the portal may not be available to users for up to 15 minutes.

To add an external LDAP directory:

1. Login to the administrator menus.
2. Select **Configuration** and then **Providers**.
3. From the **Provider Name** drop-down list select ***Directory (LDAP)***.
4. Click on the icon next to the LDAP provider.

5. Change the details to match the LDAP server source that you want to use.



- **LDAP Server URL**
  The URL of the LDAP directory source, for example ***ldap:\\ldap.example.com***.
- **User/Password**
  The user name and password for access to the LDAP server.
- **Base DN**
  This is also called the **Search Base**. It defines which set of records in the LDAP source should be used for searches. The LDAP sever administrator will provide a suitable string, for example *ou=Users,dc=global,dc=example,ddc=com*.
- **LDAP Field Mappings**
  The field names (on the left) are the fields shown in the one-X Portal for IP Office directory. Enter the names of the matching field for each in the LDAP sources records.

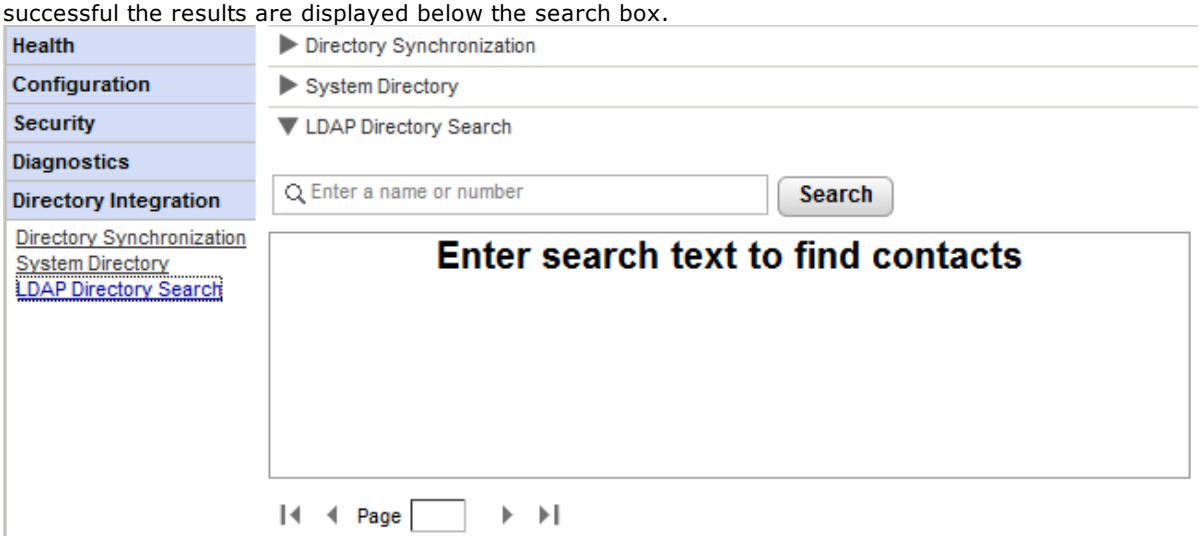
6. Click **Save**.
7. Restart the Avaya one-X Portal service 48.

3.6.2 Checking the External LDAP Directory

If you have configured an LDAP external directory source, access to it by one-X Portal for IP Office can be tested from within the administrator menus.

To check the LDAP directory:

1. Select **Directory Integration**.
2. Select **LDAP Directory Search**.
3. Enter a name or number that you know is in the external directory and click **Search**. If the search is successful the results are displayed below the search box.



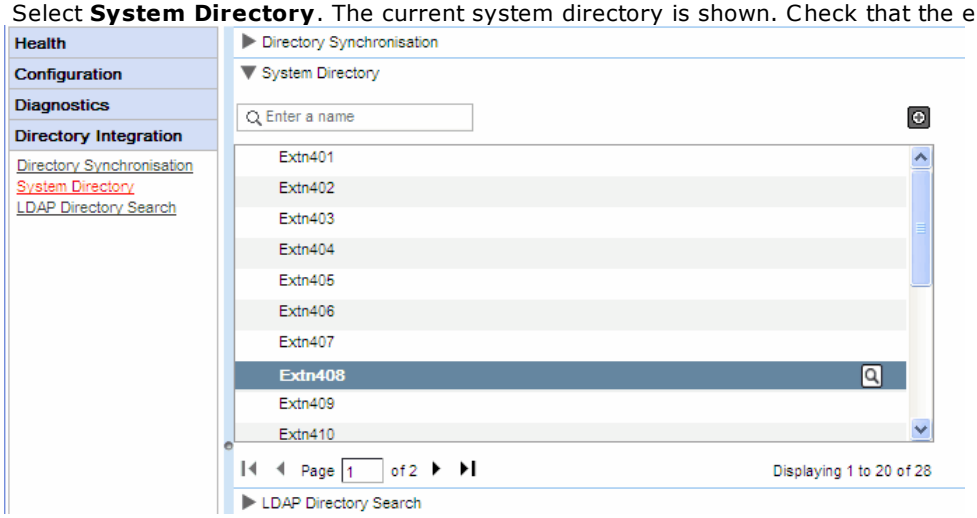
3.6.3 Checking and Updating the System Directory

The system directory shown to one-X Portal for IP Office users is a combination of the users, groups and directory entries from all the IP Office systems with which one-X Portal for IP Office has been configured to operate.

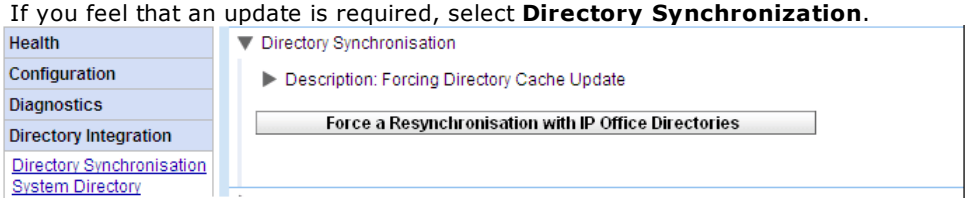
By default, the one-X Portal for IP Office application updates the system directory records every 300 seconds approximately. Through the one-X Portal for IP Office administrator menus you can view the system directory and force an update.

To check the system directory:

1. Select **Directory Integration**.
2. Select **System Directory**. The current system directory is shown. Check that the entries are as expected.



3. If you feel that an update is required, select **Directory Synchronization**.



4. Click on **Force a Resynchronization to all IP Office Directories**.

3.7 Instant Messaging/Presence

The one-X Portal for IP Office server includes an XMPP server as a component which is enabled by default. This server allows the users to IM each other and to share their IM presence.

Archiving of instant messages is also enabled by default, allowing you to search user's previous messages.

- IM Server Configuration 68
- Starting the IM Server 69
- Searching the IM Archive 70
- Setting the duration of IM Archiving 68
- Exchange Presence Integration 71

To disable IM archiving:

1. Enabling Admin console of XMPP Server 72
2. Using XMPP Server to disable IM archiving settings 73
3. Disabling Admin console of XMPP Server 73

To enable IM archiving:

1. Enabling Admin console of XMPP Server 72
2. Using XMPP Server to enable IM archiving settings 72
3. Disabling Admin console of XMPP Server 73

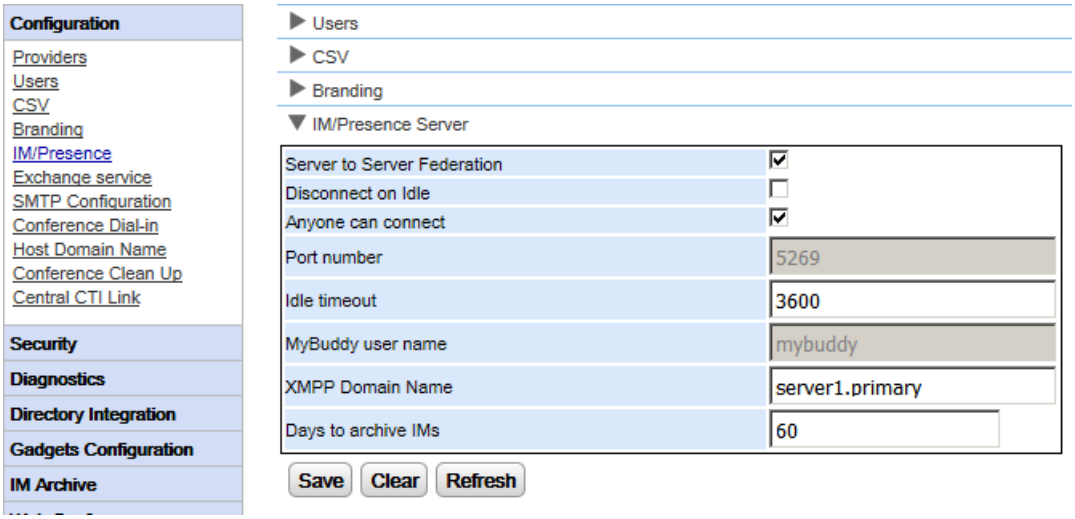
Changes to Default XMPP Operation

Prior to IP Office Release 9.1, each IP Office system had a default XMPP group that contained every IP Office user as a member. As a result, each user was able to automatically see other user's IM presence.

For IP Office Release 9.1 the above no longer applies. The sharing of IM/presence between users requires the manual configuration of XMPP groups containing those users in the IP Office system configuration (refer to the IP Office Manager help or documentation).

3.7.1 IM Server Configuration

The portal includes a component that acts as its instant messaging/presence server. The IM/presence server can be separately configured. See Instant Messaging/Presence 67.



To configure the IM/Presence server:

1. Click **Configuration** and select **IM/Presence Server**.
2. Select the required server settings:
   - **Server to Server Federation**
     If selected, the portal's presence server is able to exchange presence information with other presence servers.
   - **Disconnect on Idle**
     If selected, server to server connections are disconnected if idle for the **Idle timeout** period.
   - **Anyone can connect**
     Allow anyone to connect to IM/presence services.
   - **Port number**
     This is fixed as ***5269***.
   - **Idle timeout**
     This is the timeout in seconds used for **Disconnect on Idle** if selected.
   - **MyBuddy user name**
     This field is fixed as ***mybuddy***. The value my be needed when integrating presence details with other IM/presence services.
   - **XMPP Domain Name**
     This sets the DNS domain name used for IM/presence functions:
     - The XMPP domain name should be a domain name that the DNS can resolve. You can set the XMPP domain name at any point in time. The domain name must be reachable from the internet if you wish to use presence outside of your LAN.
     - Avaya recommends that you use a split DNS so that the server name outside of your LAN is resolved into the public IP address of the NAT or firewall whilst inside your network it is resolved into the private IP address of the server on the LAN.
     - If you cannot set a resolvable DNS domain name, you can use the IP address of the one-X Portal for IP Office server for internal only IM/presence. In this case the one-X Portal for IP Office cannot federate with remote servers.
     - You must use the server's **Web Control** menus to configure their network settings so that the auto-configuration email link uses the FQDN instead of the IP address of the server. In **Web Control**, navigate to **Settings > System > Host Name** to change the network settings. If you change the domain name any other way, the email links might not work properly.
   - **Days to archive IMs**
     This field sets how long the server should retain messages in the IM archive before deleting those messages. The default setting is 182 days (6 months). If necessary, you can disable IM archiving 73 using the XMPP admin console. The IM/Presence server must be available (see IM/Presence Server Status 13) to change this setting.
3. Click **Save**.

3.7.2 User IM Configuration

Two IP Office users can only see each other's presence status and exchange instant messages if they are members of the same XMPP group in the IP Office system configuration. Each user can be a member of one or more XMPP groups.

If a new IP Office user is added as a single action (add user, add new user to XMPP group, save configuration), the user is not seen in the portal view of the XMPP group. The resolution is to then make some further XMPP group configuration change or to restart the portal service.

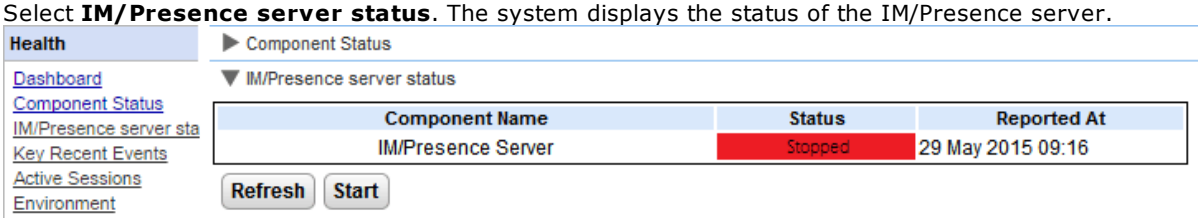
To avoid this, you should save the configuration between each action (add user, save configuration, add new user to XMPP group, save configuration).

3.7.3 Starting the IM Server

You can check the status of the IM/presence server through the IM/presence server status 13 menu. If the IM/presence server is not running, you can use the process below to start the service.

To start the IM/presence server:

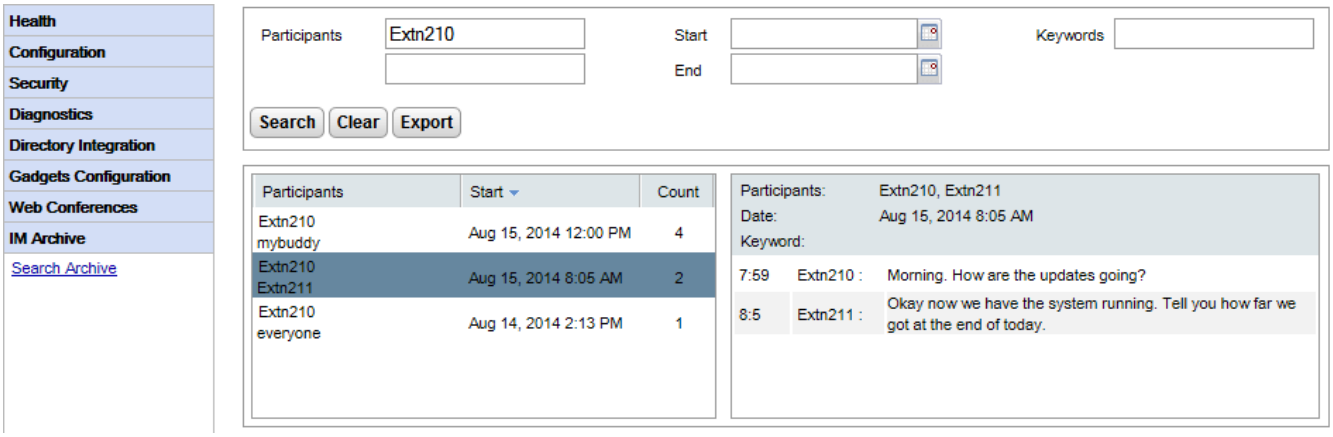
1. Select **Health**.
2. Select **IM/Presence server status**. The system displays the status of the IM/Presence server.



3. Click **Start**.
   - If the database is corrupt, the system displays *"IM/Presence server database is corrupt and needs to be restored. Would you like to restore it?"*.
     - To restore the database and start the IM/Presence server, click **Yes**. The system restores the database from the backup folder. The system automatically backs up the database every eight hours. You can not start the IM/presence server without restoring the corrupt database.
     - If you click **No**. The system displays *"IM/Presence server can not be started with corrupted database. The IM/Presence features will be unavailable"*.

3.7.4 Searching the IM Archive

You can search for the instant message conversations between the users and from the system to a user. All the fields in the search panel are optional. The number of days that the server retains an IM in the archive is set by the Days to archive IMs 68 setting.



To search the IM archive:

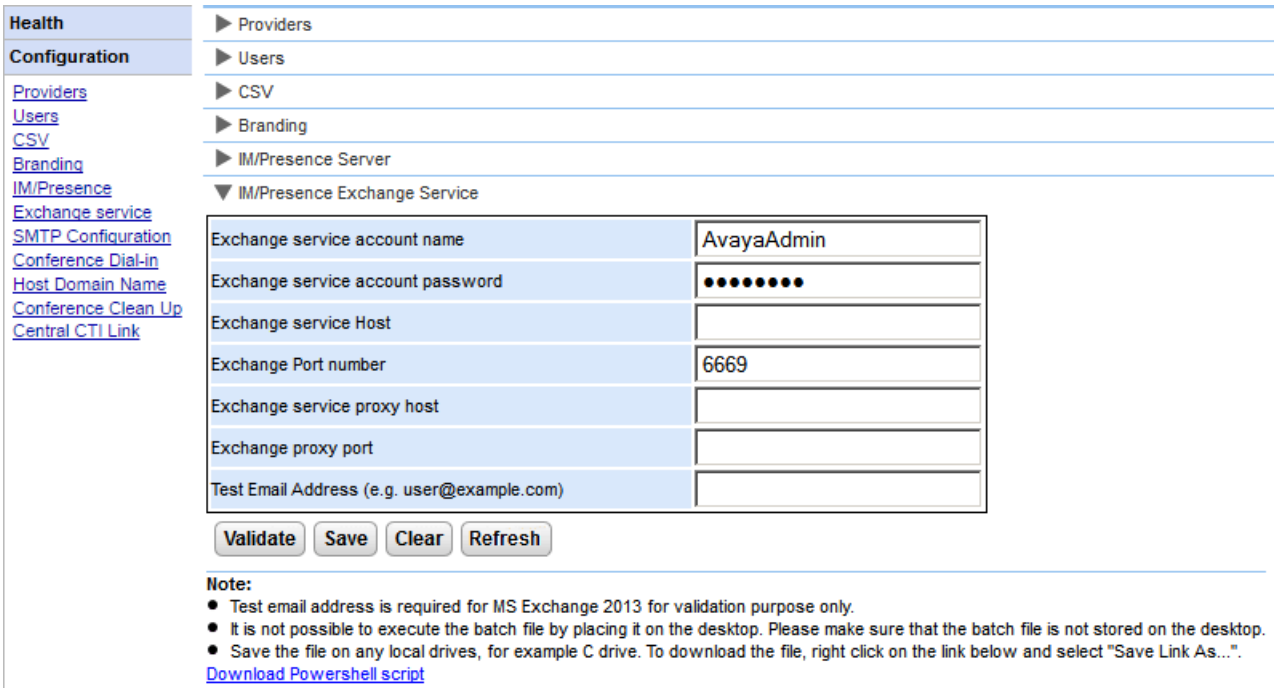
1. In the left panel, select the **IM Archive**.
2. Click **Search Archive**.
3. Enter the search criteria and click Search.

Field	Description
Participants	Type the name of the participant in the IM conversation.
Keywords	Type the keywords in the IM conversation.
Start	Select the date from which the conversations need to be listed. If you do not select a date, the system displays from the earliest conversation that the system has retained.
End	Select the date until which the conversations need to be listed. If you do not select a date, the system displays until the latest conversation.

4. Click on the conversation that you want to open. The system displays the conversation.

3.7.5 Exchange Presence Integration

one-X Portal for IP Office can be configured with the Exchange server to the presence information of the users.



To configure Exchange services:

1. Click **Configuration**, in the left navigation pane.
2. Click **Exchange service**.
   a. Type ***AvayaAdmin*** in the **Exchange service account name**. Ensure that this name is the same as the ***AvayaAdmin*** account that you created on the exchange server.
   b. Type the password that was set for the **AvayaAdmin** in **Exchange service account password**.
   c. Type the IP address of the exchange service host in **Exchange service Host**.
   d. Type the port number of the exchange service in **Exchange Port number**.
   e. Type the domain name of the proxy server that is used to connect to the exchange server in **Exchange service proxy host**.
   f. Type the port number of the proxy server for exchange service in **Exchange proxy port**.
   g. Set a **Test Email Address** using a valid email address.
3. Click on **Validate Exchange Service Configuration** to view whether the provided exchange details are valid.
4. Click **Save**.

3.7.6 Enabling the XMPP Admin Console

For security, the XMPP admin console is not enabled by default. If enabled for maintenance or troubleshooting, you must disable the admin console 73 again afterwards.

To enable the Admin console:

1. Login locally as the root user.
2. Enter `cd /opt/Avaya/oneXportal/openfire/bin`
3. At the prompt, enter: `sh AdminConsoleManager.sh enable`
4. To restart the service, enter: `service onexportal restart`

3.7.7 Enabling IM archiving

To enable IM archiving settings in XMPP Server:

1. Enable the XMPP admin console 72.
2. Open the admin console in a browser by entering *http://<server IP address>:9094*
3. Login with the username and password ***admin***.
4. Click **Server** tab.
5. Click **Archiving** tab.
6. In the left panel select **Archiving Settings**.
7. Enable the following check boxes:
   - **Conversation State Archiving**
   - **Archive one-to-one chats**
   - **Archive group chats**
8. Click **Update Settings** button. The system saves the settings and displays the following message: *Archive Settings have been saved.*
9. Disable the XMPP admin console 73.

3.7.8 Disabling IM archiving

To disable IM archiving:

1. Enable the XMPP admin console 72.
2. Open the admin console in a browser by entering *http://<server IP address>:9094*
3. Login with the username and password ***admin***.
4. Click **Server** tab.
5. Click **Archiving** tab.
6. In the left panel select **Archiving Settings**.
7. Disable the following check boxes:
   - **Conversation State Archiving**
   - **Archive one-to-one chats**
   - **Archive group chats**
8. Click **Update Settings** button. The system saves the settings and displays the following message: *Archive Settings have been saved.*
9. Disable the admin console 73.

3.7.9 Disabling the XMPP Admin Console

For security, the XMPP admin console is not enabled by default. If enabled for maintenance or troubleshooting, you must disable the admin console again afterwards.

To disable the Admin console:

1. Login locally as the root user.
2. Enter `cd /opt/Avaya/oneXportal/openfire/bin`
3. At the prompt, enter: `sh AdminConsoleManager.sh disable`
4. To restart the service, enter: `service onexportal restart`

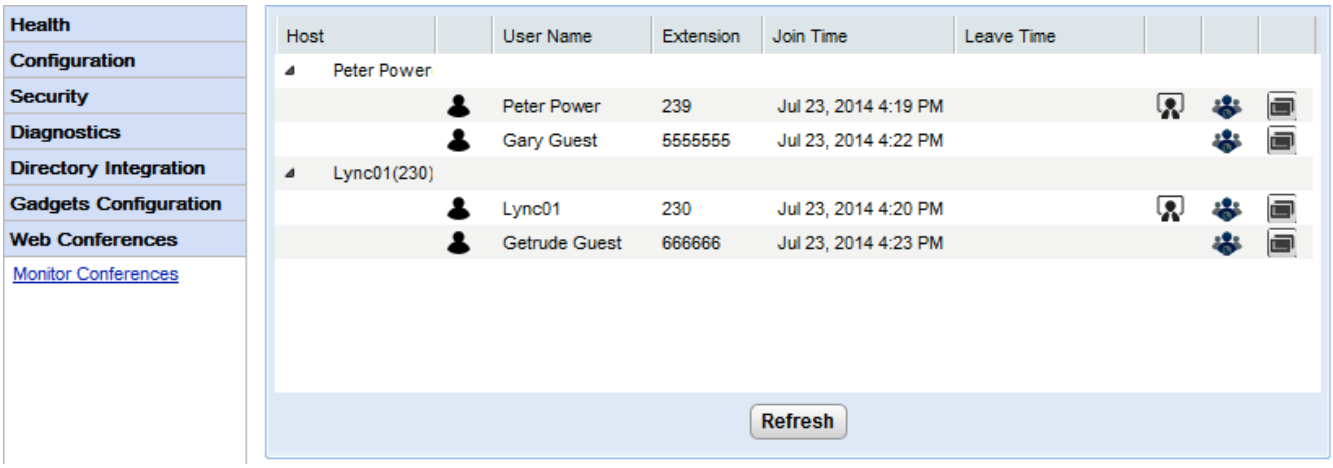
3.8 Conferences

The portal can include a component that provides support for conferencing scheduling in parallel with conferences.

3.8.1 Viewing Conferences

This menu allows you see details of web collaboration conferences being hosted by the server. It lists the members of the conferences, when they last joined and what their participation is (presenter, audio conference member, web conference member).

- The web collaboration service is not supported with R12.0 and higher.

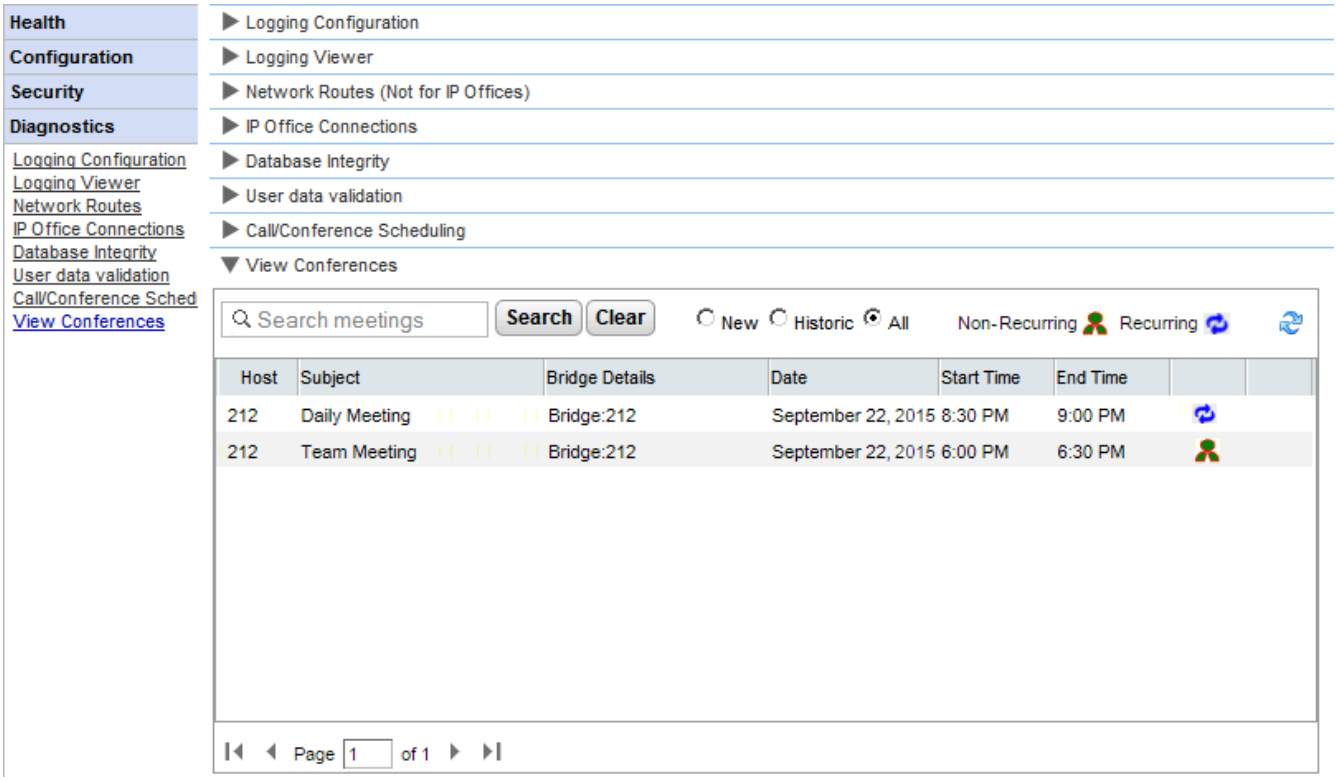


To view current conferences:

1. Select **Web Conferences** and then **Monitor Conferences**.
2. The current web conference are listed.
3. Click on the **Host** to expand the conference and view details of the participants.

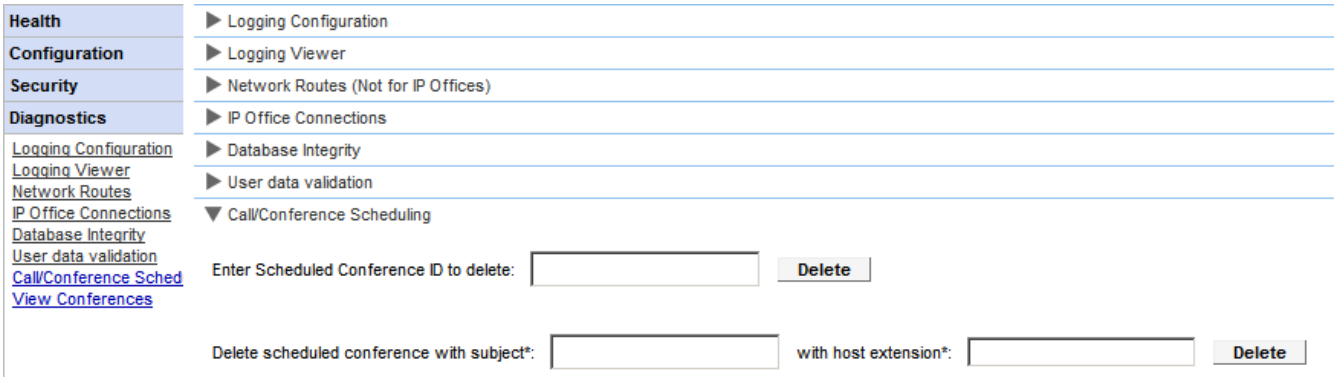
3.8.2 View Scheduled Conferences

This menu displays the calendar for scheduled conference similar to that seen and used by individual one-X Portal for IP Office users. The difference however is that is shows the scheduled conferences for all users. You can use this menu to delete a scheduled conference and to modify the details of future conferences.



3.8.3 Deleting a Scheduled Conference

You can delete a future scheduled conference. If the conference is a recurring conference, all occurrences of the conference are deleted.

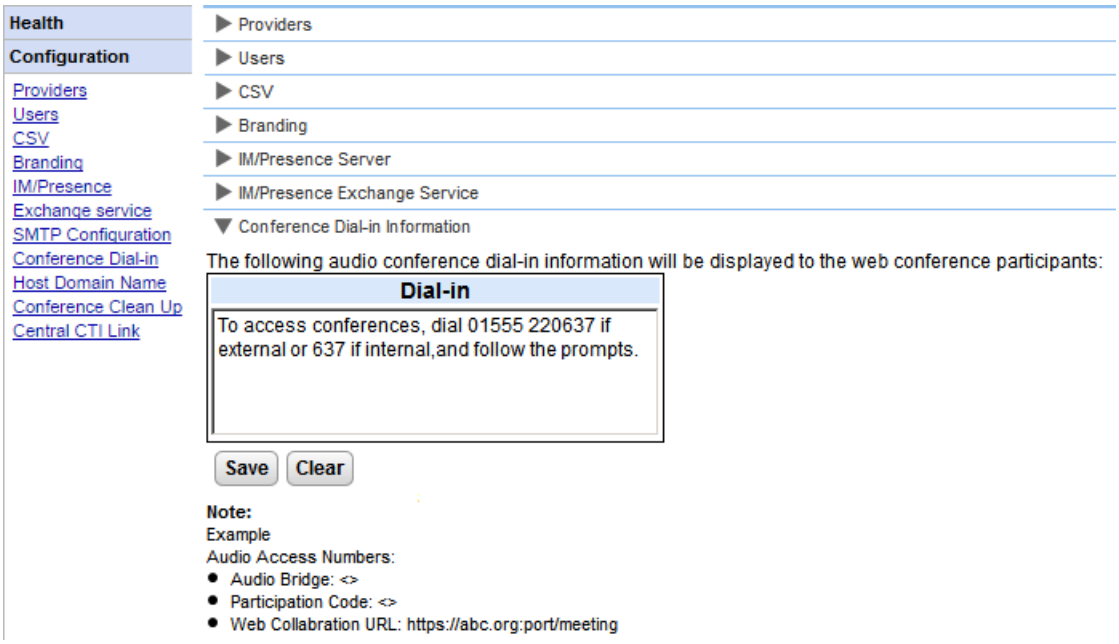


To delete a scheduled conference or conferences:

1. Click **Diagnostics** and select **Call/Conference Scheduling**.
2. Enter the host extension and a subject. If you leave the subject blank, all conferences scheduled by the host are deleted.
3. Click **Delete**.

3.8.4 Conference Notification Message

When a user schedules a conference, the server sends the invited participants a conference notification using email and instant messaging. That notification includes the details of the conference set by the user (bridge number, participant code). It can also include the fixed text set through the **Conference Dial-in** menu.

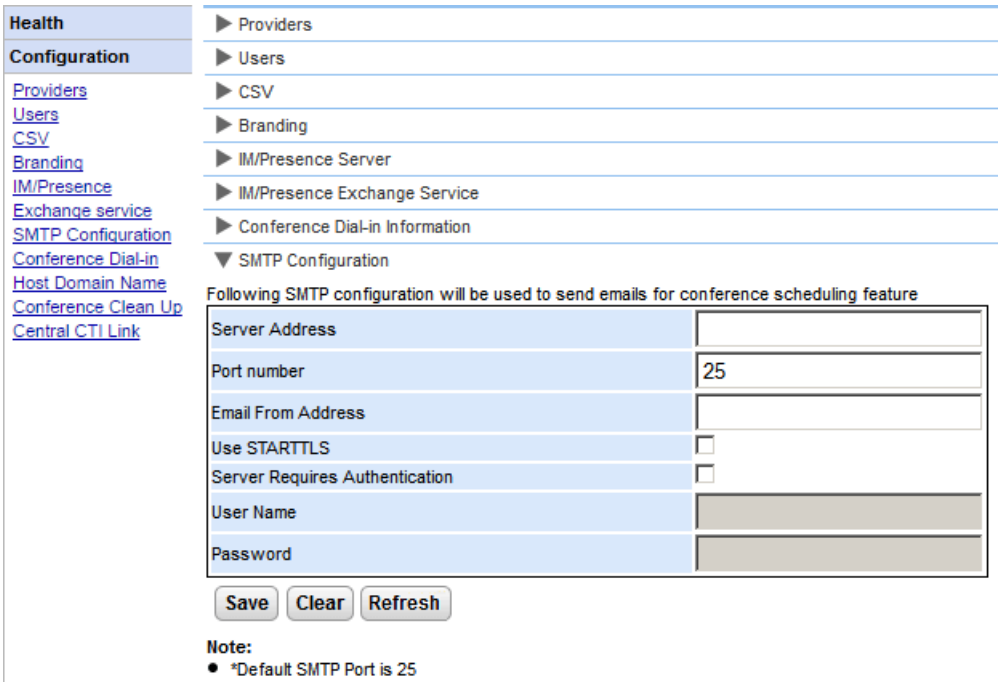


To set the conference notification fixed text:

1. Select **Configuration** and then **Conference Dial-in**.
2. Enter the fixed text that should be included in all conference notifications.
3. Click **Save**.

3.8.5 Conference Emails

The conference invites to participant can use both instant messaging and email. For email, the conference email settings must be configured as below. The email address used for each individual participant is set in the telephone system configuration.



To set the conference notification fixed text:

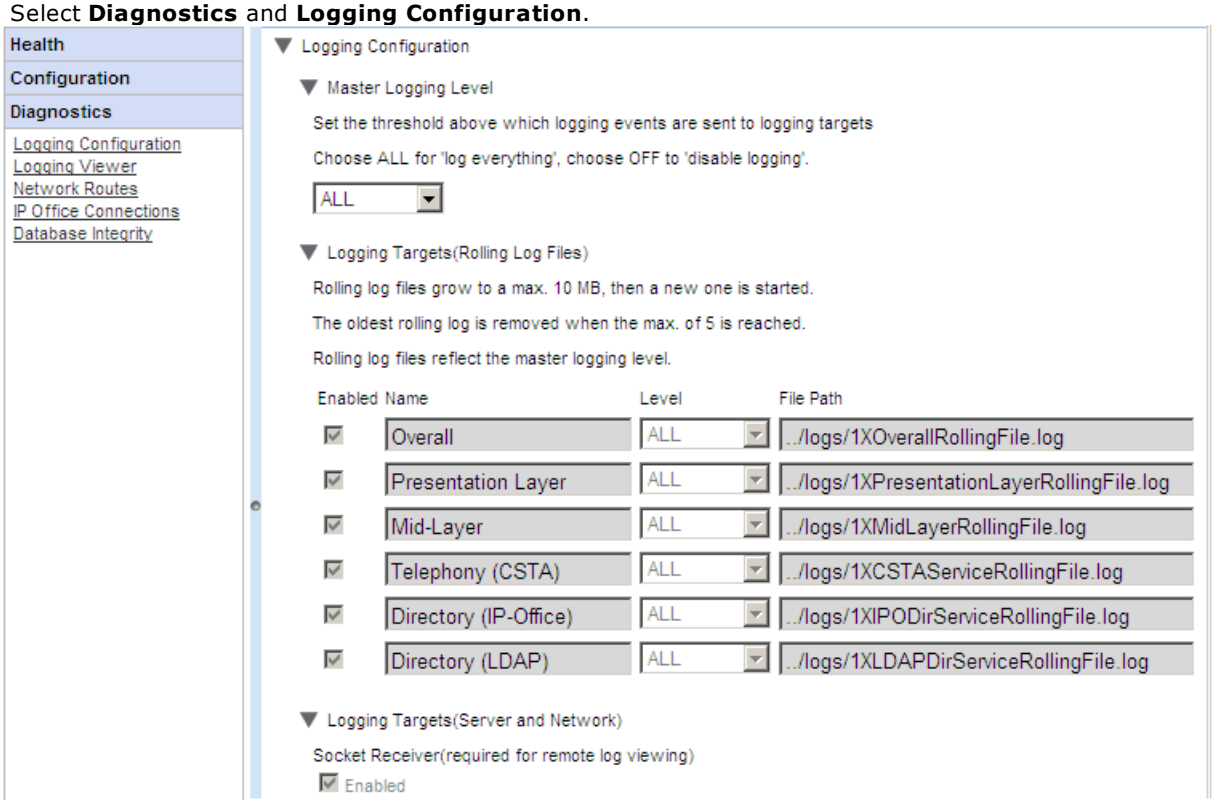
1. Select **Configuration** and then **SMTP Configuration**.
2. Set the SMTP email details that the server should use:
   - **Server Address**
     The IP address of the customer's SMTP server.
   - **Port Number**
     The SMTP listening port of the server. The default is 25.
   - **Email From Address**
     This is the address that will be used by the server. Some email servers will only relay messages from recognized or addresses in the same domain.
   - **Use STARTTLS**
     Select this field to enable TLS/SSL encryption. Encryption allows voicemail-to-email integration with hosted email providers that only permit SMTP over more secure transport.
   - **Server Requires Authentication**
     If the server requires a user account to receive and send emails, enter the details of an account configured on that server for use by the IP Office.
     - **User Name**
       The account name to use if Server Requires Authentication is selected.
     - **Password**
       The account password to use if Server Requires Authentication is selected.
3. Click **Save**.

3.9 Remote Logging

The one-X Portal for IP Office server can be configured to allow logging applications to connect on port 4560 to collect logging output. The output is in Log4j format. The one-X Portal for IP Office server administrator interface includes links to install Apache Chainsaw.

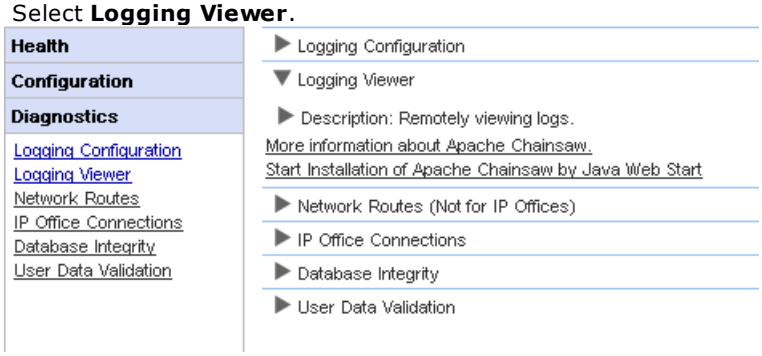
This process assumes that the PC from which it is being run has an Internet connection. If that is not the case, Apache Chainsaw can be downloaded and installed following the instructions on the Apache Chainsaw website (http://logging.apache.org/chainsaw).

1. Select **Diagnostics** and **Logging Configuration**.



2. Select **Logging Targets** and check that **Socket Receiver** is enabled.

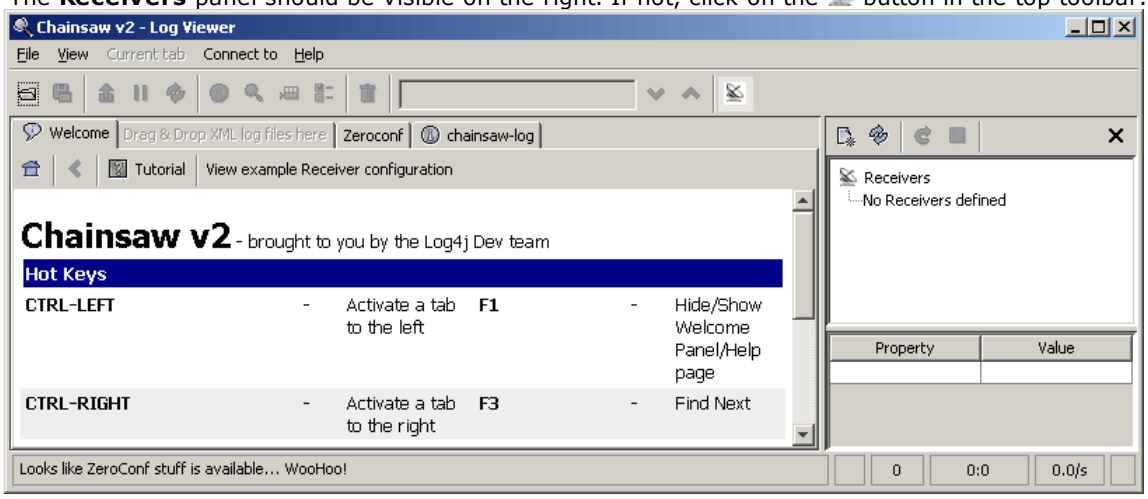
3. Select **Logging Viewer**.



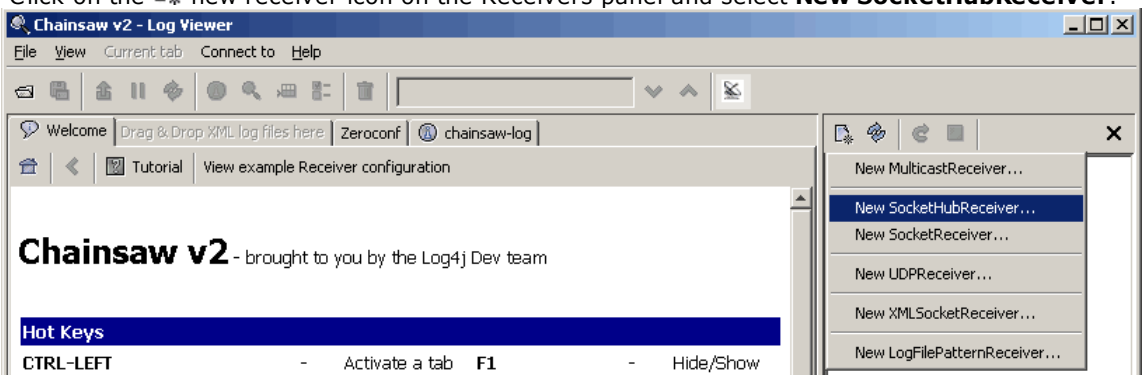
4. Click on **Start Installation of Apache Chainsaw by Java Web Start**.

5. The process for downloading and installing Chainsaw is largely automatic. Chainsaw is started. If the message ***Warning: You have no Receivers defined...*** appears, select ***I'm fine thanks, don't worry*** and ***Don't show me this again*** and click **OK**.

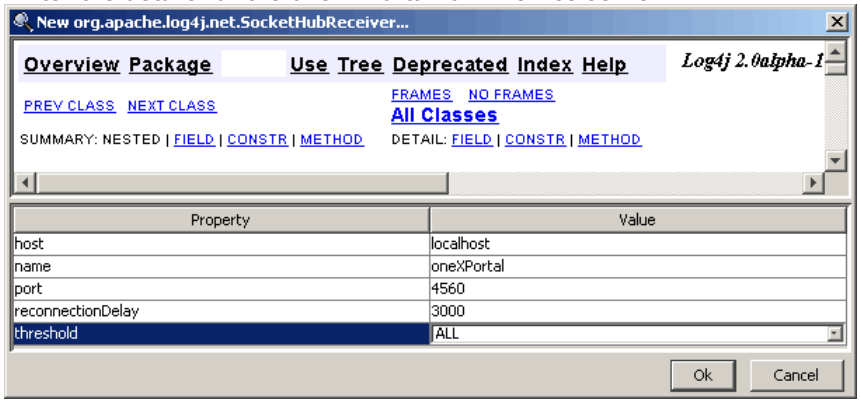
6. The **Receivers** panel should be visible on the right. If not, click on the button in the top toolbar.



7. Click on the new receiver icon on the Receivers panel and select **New SocketHubReceiver**.

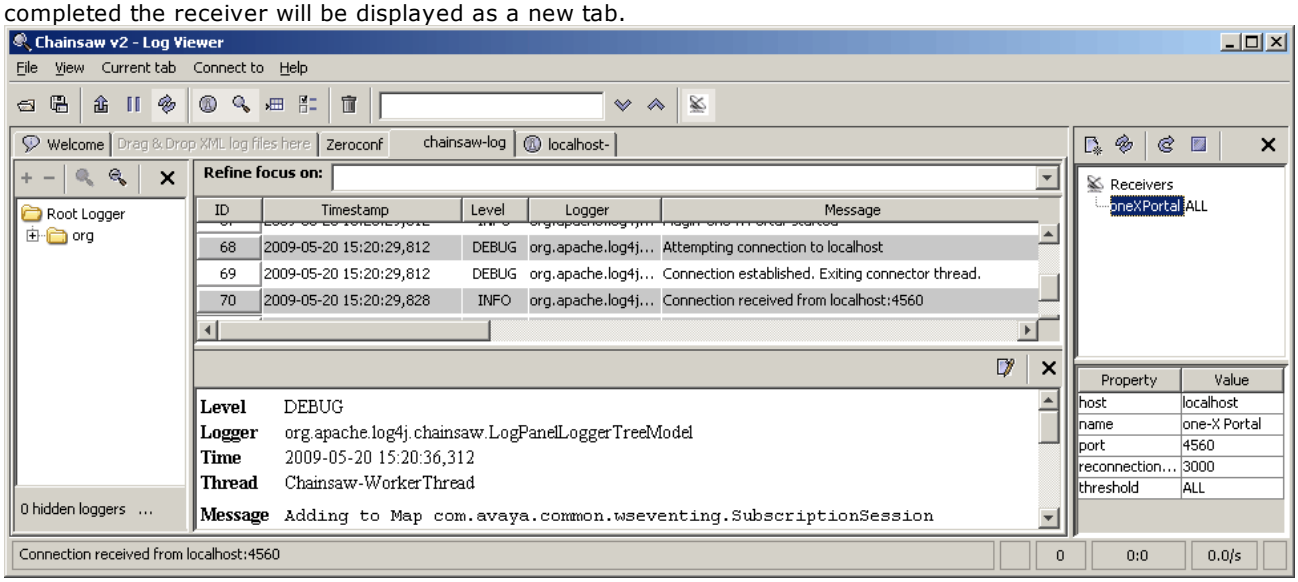


8. Enter the details for the one-X Portal for IP Office server.

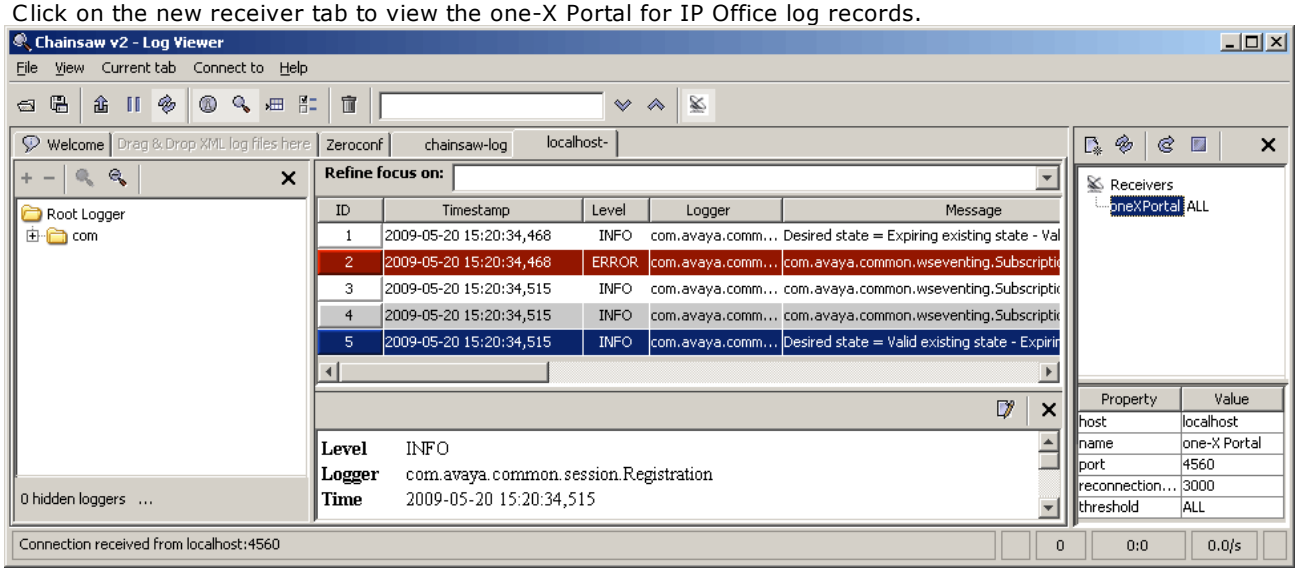


host	This field sets the address of the one-X Portal for IP Office server. In the example above chainsaw is being run on the one-X Portal for IP Office server PC.
name	This field is for display only. Enter a name for the receiver entry in Chainsaw.
port	Set this to 4560. This is the port to which one-X Portal for IP Office outputs log records for collection by remote logging applications.
reconnectionDelay	This field sets the how long (in milliseconds) the receiver should wait if it suspects it has lost connection before reattempting connection.
threshold	This field sets the minimum level of logging message to receive or All or Off.

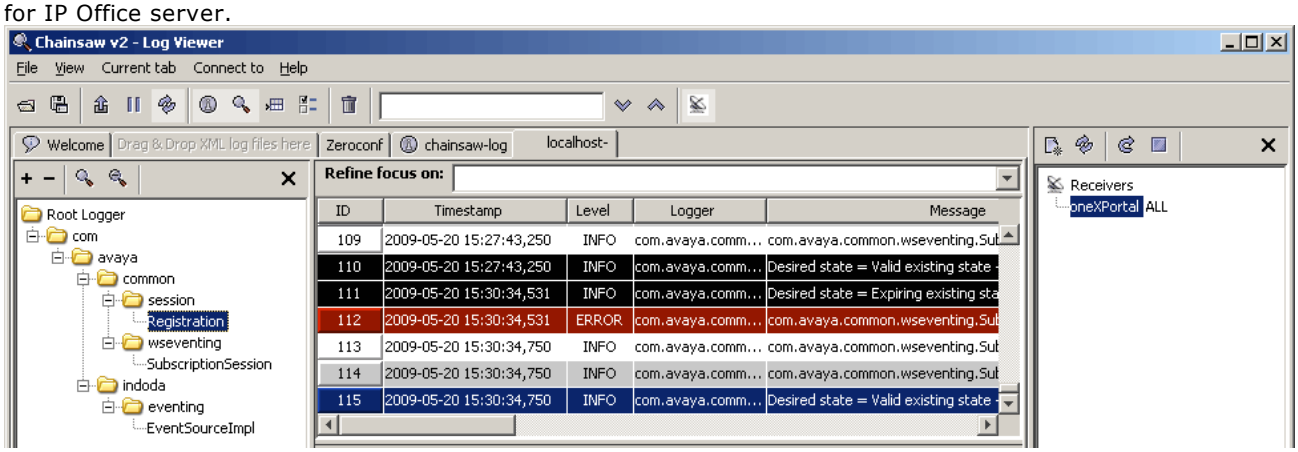
9. When you have completed the fields, click OK. After a few seconds the receiver should start and connect to the one-X Portal for IP Office server. The process will appear as log events on the chainsaw-log tab and when completed the receiver will be displayed as a new tab.



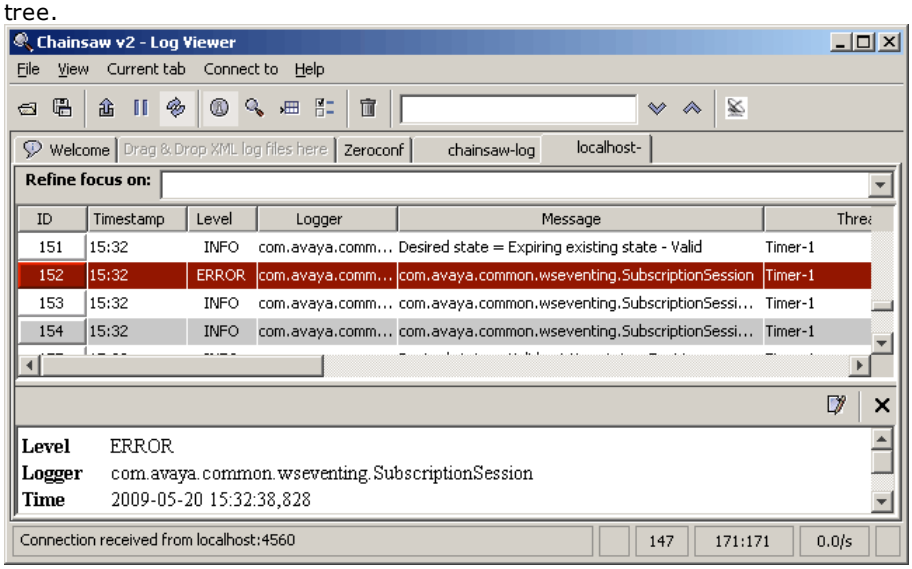
10. Click on the new receiver tab to view the one-X Portal for IP Office log records.



11. The navigation tree on the left can be used to focus the log view onto a particular component of one-X Portal for IP Office server.



12. Clicking on the receiver icon will hide the receivers panel. Clicking in the icon will hide the navigation tree.



3.10 Adding Additional Administrators

The process below illustrates how to configured portal administration rights for additional IP Office service users. Each IP Office service user is a member of one or several rights groups. It is the rights group settings that control what the service user can do, including their level of one-X Portal for IP Office server access.

- By default, the one-X Portal for IP Office server uses "referred authentication". That means that the portal administration access rights are assigned to IP Office service users configured in the security settings of the IP Office service running on the same server.
- If "referred authentication" is disabled on the IP Office, the portal uses its own local ***Administrator*** account for access to the administration menus, and a local ***Superuser*** account for access to the AFA menus. The passwords for these local accounts are stored by the portal service and are not part of the IP Office security settings.

To view and adjust rights group settings:

1. Using IP Office Manager, select **File | Advanced | Security Settings**.
2. Select the IP Office system and click **OK**.
3. Enter the name and password for access to the IP Office system's security settings.
4. Select **Rights Groups**.
5. Select the **External** tab. This tab include settings for level of portal access allowed to members of the rights group.
   - **One-X Portal Administrator**
     Access to the portal administrator menus.
   - **One-X Portal Super User**
     Access to the portal AFA menus.
6. Select a particular rights group in the list to see what level of access the rights group has.
7. If you make any changes, click **OK**.
8. Click on the to save the changes.

To change a service user's rights group memberships:

1. Using IP Office Manager, select **File | Advanced | Security Settings**.
2. Select the IP Office system and click **OK**.
3. Enter the name and password for access to the IP Office system's security settings.
4. Select **Service Users**.
5. Select the service user. The details shows the rights group of which that service user is a member.

Chapter 4.
AFA Menus

4. AFA Menus

one-X Portal for IP Office supports a set of menus for the backup and restoration of one-X Portal for IP Office configuration settings. These allow backup and restoration using the one-X Portal for IP Office server, an FTP server or your own browser PC as the destination for the backup files.

The menus are also intended to allow backup and restoration between an old and a new installation of one-X Portal for IP Office on a new server. However, it is not supported for backup and restoration between different versions of one-X Portal for IP Office, for example from 6.1 to 7.0.

Access to the advanced backup and restore menus is controlled by a separate user and password from other administrator access.

- **Linux Based Servers**
  The portal can be included in the backup and restore functions provided through the IP Office server's web management menus. Those options include support for backup to HTTP. HTTPS and SFTP servers and scheduled backups.

4.1 Log in

Only one user can be logged in to the AFA menus at any time.

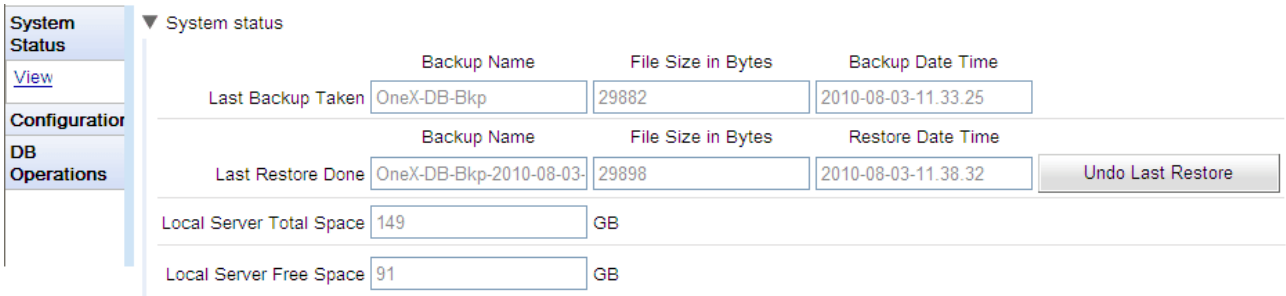
- By default, the one-X Portal for IP Office server uses "referred authentication". That means that the portal administration access rights are assigned to IP Office service users configured in the security settings of the IP Office service running on the same server.
- If "referred authentication" is disabled on the IP Office, the portal uses its own local ***Administrator*** account for access to the administration menus, and a local ***Superuser*** account for access to the AFA menus. The passwords for these local accounts are stored by the portal service and are not part of the IP Office security settings.

To login:

1. Enter the browser address ***http://<server name>:<server port>/onexportal-afa.html***, where:
   - ***<server name>*** is the name or the IP address the one-X Portal for IP Office server.
   - ***<server port>*** is the port number used by the one-X Portal for IP Office. This is 9443 for HTTPS access.
   - You can use ***http://*** rather than ***https://*** and ***8080*** as the port if unsecure access has been configured. See Protocol 33.
   - Alternatively, from the normal user login menu, select **AFA Login**.
2. At the login menu, enter the password:
   - Enter the password of an IP Office security user configured for one-X Portal Super User 82 access. By default that is the **Administrator** user.
   - Otherwise:
     - When you log in for the first time, use the default password ***MyFirstLogin1_0***. After logging in, you will be prompted to enter a new password for the ***Superuser*** account plus additional information.
   - **Display Name**
     Enter a name for display in the one-X Portal for IP Office menus.
   - **Password/Confirm Password**
     Enter a password that will be used for future ***Superuser*** access. This password is used on servers not using **Referred Authentication**.

4.2 System Status

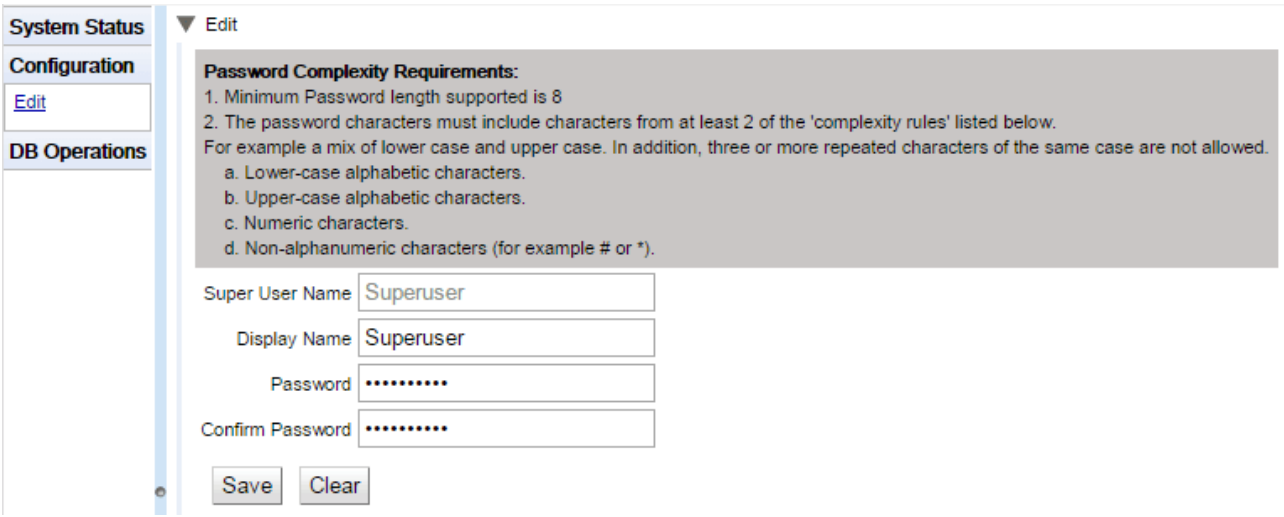
This menu gives a summary of the previous usage of the Superuser menus. It also allows the rollback of the last previous restore operation.



- **Last Backup Taken**
  This section gives details of the last backup taken using the Backup menu. The backup file name will have been a zip file named with the **Backup Name** plus the **Backup Date Time**. For example, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Last Restore Done**
  This section gives details of the last restore operation. The time and date of the restore are shown and the name of the file used for that operation. The Undo Last Restore control can be used to rollback the restore action.
- **Local Server Total Space**
  Shows the approximate disk space on the one-X Portal for IP Office server.
- **Local Server Free Space**
  Shows the approximate free disk space remaining on the one-X Portal for IP Office server.

4.3 Configuration

This menu is used to set the basic settings for ***Superuser*** access.



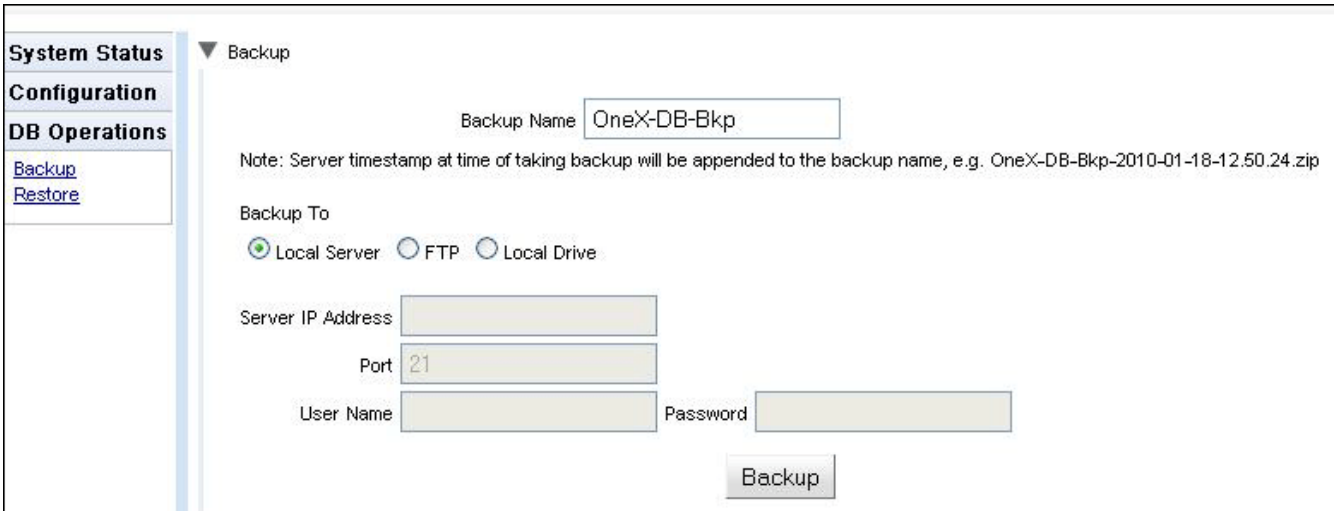
- **Super User Name**
  This is a fixed name and cannot be changed.
  - **Display Name**
    Enter a name for display in the one-X Portal for IP Office menus.
  - **Password/Confirm Password**
    Enter a password that will be used for future ***Superuser*** access. This password is used on servers not using **Referred Authentication**.

4.4 DB Operations

These menus are used to create backup files and to restore the settings from a previous backup file.

4.4.1 Backup

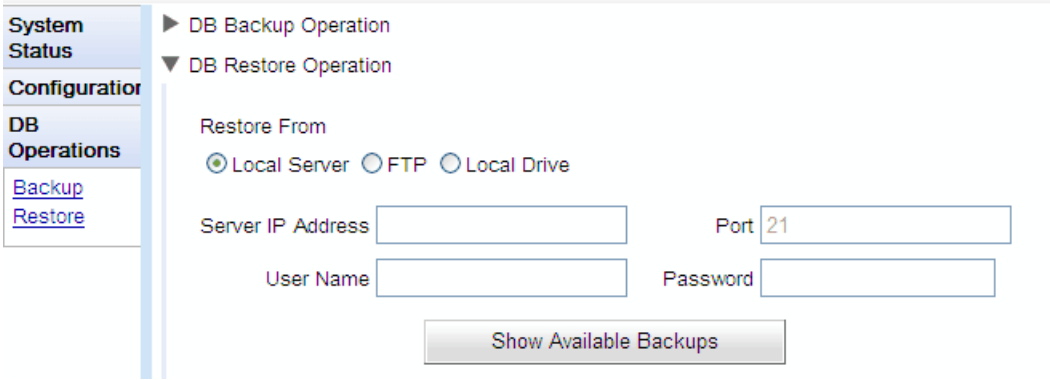
This menu is used to create backup files.



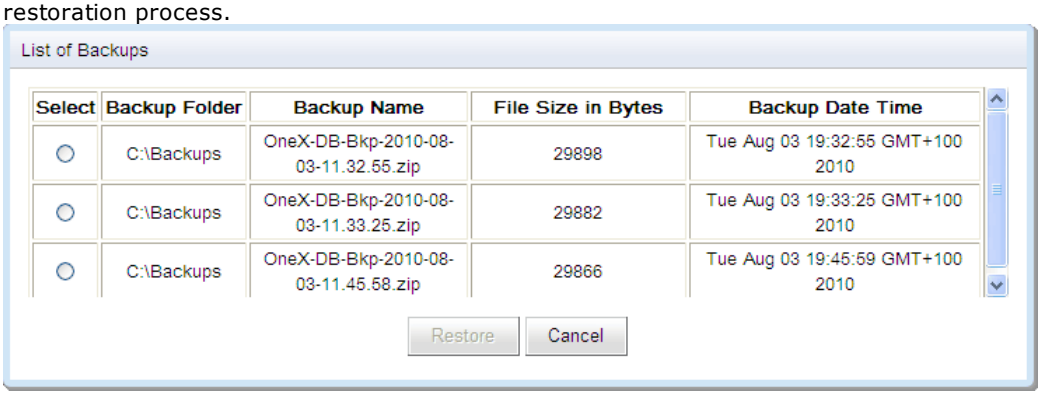
- **Backup Name**
  This name is used for the backup zip files. The date and time of the backup is also added to the file name. For example, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Backup To**
  This setting is used to select the destination for the backup file.
- **Local Server**
  If this options is selected, the backup file is created in the **Backup Folder**.
- **FTP**
  If this option is selected, the backup file is temporarily created in the **Backup Folder**. It is then sent to the specified FTP server address.
- **Local Drive**
  If this option is selected, the backup file is temporarily created in the **Backup Folder**. It is then offered for download by the browser.
- **FTP Settings**
  The following settings are used if the destination for the backup file is set to **FTP**.
- **Server IP Address**
  The address, including file path, of the FTP server.
- **Port**
  The FTP port on the server. The normal default is port 21.
- **User Name** / **Password**
  The user name and password for file access to the specified FTP server.
- **Backup**
  This button is used to initiate a backup using the settings above.

4.4.2 Restore

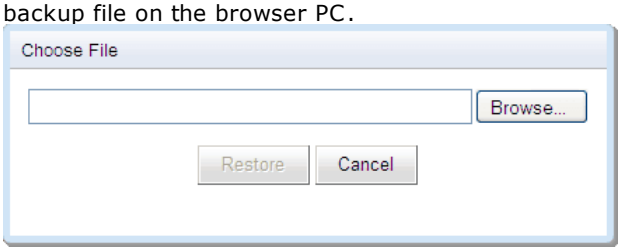
This menu is used to select a previous backup file and then use that file for a restore operation. Before the restoration occurs, a backup of the current configuration is made and stored in the **Backup Folder** for use with the **Undo Last Restore** 85 control. Restoration is only supported from a backup of the same one-X Portal for IP Office version.



- **Restore From**
  This setting is used to select the destination from which the previous backup file should be selected.
- **Local Server**
  If this options is selected, the backup file for the restore is selected from the configured **Backup Folder**.
- **FTP**
  If this option is selected, the backup file for the restore is selected from the specified FTP server address.
- **Local Drive**
  If this option is selected, the backup file for the restore is selected using a file browse menu to locate a file on the browser PC.
- **FTP Settings**
  The following settings are used if the destination for the backup file is set to **FTP**.
- **Server IP Address**
  The address, including file path, of the FTP server.
- **Port**
  The FTP port on the server. The normal default is port 21.
- **User Name** / **Password**
  The user name and password for file access to the specified FTP server.
- **Show Available Backups**
  This button is shown when **Restore From** option is set to **Local Server** or **FTP**. When clicked, a list of the available backup files at the selected location is shown. Select a file and click **Restore** to begin the restoration process.



- **Choose File**
  This button is available when the **Restore From** option is set to **Local Drive**. It allows you to Browse to backup file on the browser PC.



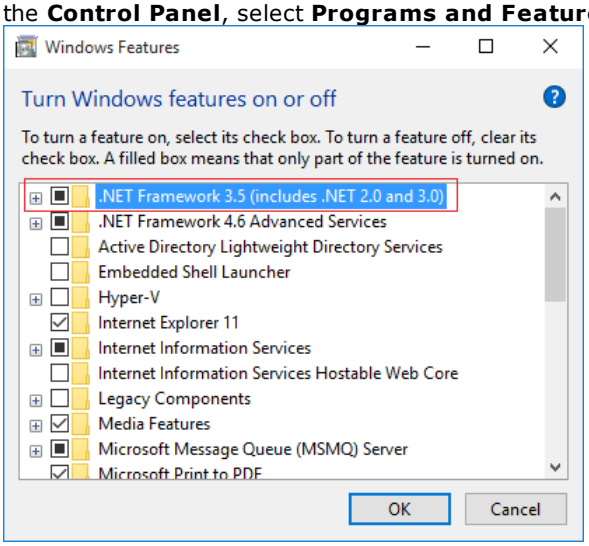
Chapter 5.

Desktop Client Group Policy Installation

5. Desktop Client Group Policy Installation

You can install Avaya IP Office Desktop Clients through group policy. This tutorial describes how to deploy a MSI on multiple machines using a group policy.

- **Prerequisite:**
  Ensure that the following are present on all the remote PCs:
  - **.NET Framework 4.5.2**
    The install package for this can be downloaded from the **Configure | Desktop Integration** page within one-X Portal for IP Office.
  - **.NET Framework 3.5**
    Support for .NET Framework 3.5 must also be enabled within the Windows Features on the user PC (from the **Control Panel**, select **Programs and Features | Turn Windows features on or off**).



  - **Microsoft Office 2007 PIA**
  - **Microsoft VSTO 2010 Runtime v4.0 (10.0.40303 or later)**

Deployment Methods

Group policy supports two methods of deploying an MSI package:

- **Assign software**
  A program can be assigned per-user or per-machine. If it is assigned per-user, the program is installed when the user logs on. If it is assigned per-machine, the program is installed for all users when that machine starts.
- **Publish software**
  A published program is added to the **Add or Remove Programs** list and the user is able to install it from there.

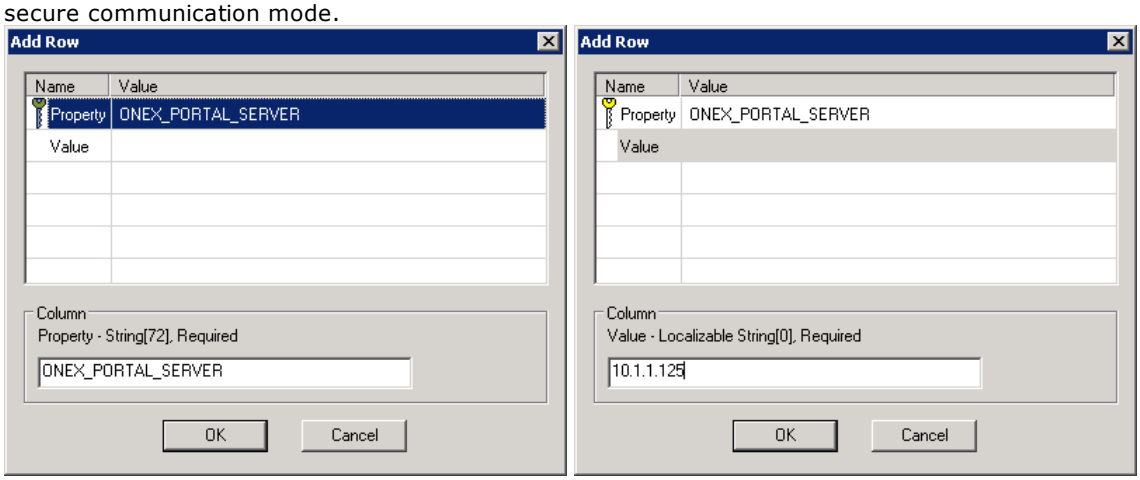
Deployment Summary

5.1 Creating a Distribution Point

The first step in deploying an MSI is to create a distribution point on the publishing server.

To create a distribution point:

1. Log on to the server as an Administrator.
2. Create a shared network folder to contain the MSI package.
3. Set the permissions on this folder allow remote access to the distribution package
4. In the shared folder, perform an administrative install of the desktop client executable. The command line for an administrative installation is ***AvayaOneXDesktopClients.exe /a***
5. Download the open source ORCA tool from: http://www.softpedia.com/progDownload/Orca-Download-79861.html. This creates an MSI package.
6. After downloading and installing ORCA, right-click on the MSI file and select **Edit with Orca**.
7. From the left-hand **Table** item select **Property Table**.
8. From the list of tables select **Property**. Scroll to the bottom of the table, right-click and select **Add Row**.
9. Add the following Properties with corresponding values to specify one-X Portal server address, port and secure communication mode.



- ONEX_PORTAL_SERVER = <Server IP address or fully qualified domain name>
- PORT_NUMBER = <Server port number>
- SECUREMODE = <1 for enabled or 0 for disabled>

10. After adding all the properties, save the MSI file and close the ORCA tool.

5.2 Creating a Group Policy Object

An MSI package is deployed (distributed) using a Group Policy Object.

To create a Group Policy Object:

1. Create a **Container** or **Organizational Unit**.
2. Open the **Active Directory Users and Computers** window.
3. In the console tree, right-click your domain, and then select **New**.
4. Select **Organizational Unit**.
5. Provide a name for the container and uncheck the checkbox **Protect container from accidental deletion** so as to be able to delete this container later. If checkbox is marked, it is not possible to delete this container.
6. In the same **Active Directory Users and Computers** window, add to the Container the users and machines for which the policy needs to be applied. New domain users and computers can be created in this container.
   - Alternatively you can move the users from the **USERS** account to the container and machine accounts from **COMPUTERS** account to the container. Moving the users or machines prompts a warning.
7. Click on the **Start** button.
8. Go to **Programs**.
9. Select **Administrative Tools** and then select **Group Policy Management**.
10. Expand the tree for your domain and select the newly created container or organizational unit.
11. Right-click and select **Create a GPO in this domain, and Link it here...**.
12. Provide a name for the GPO and click the **OK** button to close the window. The GPO is added to the container and also to the Group Policy Objects list.
13. Right-click the GPO in the container and select **Edit** to open the **Group Policy Management Editor**. Select how you want the policy installed. If you assign the application to a user, it is installed when the user logs on to the computer. If you assign the application to a computer, it is installed when the computer starts.

5.3 Assigning an MSI Package

A package can be assigned per-user or per-machine. Assigned packages are automatically silently installed.

To assign a package:

1. In the **Group Policy Management Editor**, go to **Computer Configuration** and select **Policies and Software Settings**.
2. Select **Software Installation**.
3. Right-click and select **New** and then select **Package**.
4. In the open dialog box, make sure to type the full UNC path of the shared installer package. For example: *\\<machine_name>\MyGPO\DesktopClients.msi*
5. Click **Open** and **Select the Deployment Method** as Assign and click **OK**.
6. From the command-line window, run the command to force update of group policy.
   gpupdate/Force

5.4 Publishing an MSI Package

You can publish a package in order to allow the target user to install it by using Add or Remove programs.

To publish a package:

1. In the **Group Policy Management Editor**, go to **Computer Configuration**.
2. Select **Policies and Software Settings**.
3. Select **Software Installation**.
4. Right-click and select **New** then select **Package**.
5. In the open dialog box, make sure to type the full UNC path of the shared installer package. For example: *\\<machine_name>\MyGPO\DesktopClients.msi*
6. Click **Open**.
7. Select the **Deployment Method** as **Publish** and click **OK**.
8. From the command-line window, run the command to force update of group policy.
   gpupdate/Force

5.5 Redeploying an MSI Package

Sometimes you may need to redeploy a package, for example when doing an upgrade.

To redeploy a package:

1. In the **Group Policy Management Editor**, go to **Computer Configuration** and select **Policies and Software Settings**.
2. Select **Software Installation**.
3. Right-click and select **Existing GPO**.
4. Right click and click **Redeploy application**.
5. Click the **Yes** button for reinstalling the application wherever it is installed.
6. Close the **Group Policy** snap-in.
7. Click **OK** and exit the **Group Policy Management** snap-in.
8. From the command-line window, run the command to force update of group policy.
   gpupdate/Force

5.6 Removing an MSI Package

Group Policy allows you to remove packages which have been deployed in the past. For more details read http://support.microsoft.com/kb/816102.

To remove a package:

1. Click on the **Start** button.
2. Go to **Programs**.
3. Select **Administrative Tools** and then select **Active Directory Users and Computers**.
4. Right-click your domain name in the console tree and select the **Properties**.
5. Select the **Group Policy** tab.
6. Select the object you used to deploy the package and click **Edit**.
7. Expand the **Software Settings** element (per-user or per-machine) which contains the deployed package
8. Expand the **Software Installation** element which contains the deployed package
9. Right-click the package in the right pane of the **Group Policy** window
10. Select the **All Tasks** menu and click **Remove**
11. Select from the following options:
    - **Immediately uninstall the software from users and computers**
    - **Allow users to continue to use the software but prevent new installations**
12. Click the **OK** button to continue .
13. Close the **Group Policy** snap-in.
14. Click **OK** and exit the **Active Directory Users and Computers** snap-in.

5.7 Silent Installation Commands

You can install the Avaya IP Office Plug-in silently on a PC using the following command line options:

- **Install only Call Assistant:**
  AvayaOneXDesktopClients.exe /s /v"/qn SECUREMODE=<1 or 0> PORT_NUMBER=<PORTNUMBER> ONEX_PORTAL_SERVER=<one-X Portal Server IP or FQDN> ADDLOCAL=callAssistant,ChangeARP"
- **Install only Outlook plug-in:**
  AvayaOneXDesktopClients.exe /s /v"/qn SECUREMODE=<1 or 0> PORT_NUMBER=<PORTNUMBER> ONEX_PORTAL_SERVER=<one-X Portal Server IP or FQDN> ADDLOCAL=OutlookPlugin,ChangeARP"
- **Install Both:**
  AvayaOneXDesktopClients.exe /s /v"/qn SECUREMODE=<1 or 0> PORT_NUMBER=<PORTNUMBER> ONEX_PORTAL_SERVER=<one-X Portal Server IP or FQDN>"

Note: If the user does not want to provide value of one-X Portal server or port number then do not include those properties. Do not add a space before or after the "=" in property values. A SECUREMODE value other than 0 or 1 defaults to 0.

Chapter 6.
Document History

6. Document History

Date	Issue	Change Summary
4th April 2024	**19a**	Updates for IP Office R12.0.
17th April 2024	**19b**	• UCM not supported for IP Office R12.0.

Index

U

V

X