



IP Office™ Platform 9.1

Administering Avaya one-X Portal for IP Office

Notice

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

Documentation disclaimer

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a 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 IF YOU PURCHASE A 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](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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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. Note that 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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies 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](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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](http://WWW.MPEGLA.COM).

Compliance with Laws

Customer acknowledges and agrees that it is responsible 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

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>).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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

1. one-X Portal for IP Office Administration

1.1 Log in	7
1.2 Log out	7

2. Admin Menus

2.1 Health	12
2.1.1 Component Status	12
2.1.2 IM/Presence Server Status	12
2.1.3 Key Recent Events	13
2.1.4 Active Sessions	13
2.1.5 Environment	14
2.2 Configuration	15
2.2.1 Providers	15
2.2.2 Users	21
2.2.3 CSV	22
2.2.4 Branding	22
2.2.5 IM/Presence	23
2.2.6 Exchange Service	24
2.2.7 Conference Dial-In	25
2.2.8 SMTP Configuration	26
2.2.9 Syslog	27
2.2.10 Conference Clean Up	28
2.2.11 Auto Provisioning	28
2.3 Security	29
2.3.1 Protocol	29
2.3.2 Certificate	30
2.4 Diagnostics	30
2.4.1 Logging Configuration	30
2.4.2 Logging Viewer	32
2.4.3 Network Routes	32
2.4.4 IP Office Connections	33
2.4.5 Database Integrity	33
2.4.6 User Data Validation	34
2.4.7 Call/Conference Scheduling	35
2.5 Directory Integration	36
2.5.1 Directory Synchronisation	36
2.5.2 LDAP Directory Search	36
2.5.3 System Directory	37
2.6 Gadget configuration	38
2.6.1 External gadget list	38
2.6.2 Importing gadgets	38
2.6.3 Exporting Gadgets	39
2.7 IM Archive	40
2.7.1 Search Archive	40
2.8 Web Conferences	41
2.8.1 Monitor Conferences	41
2.9 Help & Support	42

3. Maintenance Tasks

3.1 Manually Starting the Service	44
3.2 Call Log Configuration	45
3.3 IP Office Switch	45
3.3.1 Adding an Additional IP Office	45
3.3.2 Changing IP Office Details	48
3.4 Gadgets	50

3.4.1 Fetching a gadget URL	50
3.4.2 Importing gadgets	51
3.4.3 Exporting Gadgets	53
3.4.4 Adding an external gadget	54
3.4.5 Editing an external gadget	54
3.4.6 Enabling an external gadget	55
3.4.7 Disabling an external gadget	55
3.4.8 Deleting an external gadget	55
3.5 Users	56
3.5.1 Adding/Deleting Users	56
3.5.2 Editing User Settings	56
3.6 Directories	58
3.6.1 Adding an LDAP External Directory Source	58
3.6.2 Checking the External LDAP Directory	59
3.6.3 Checking and Updating the System Directory ...	60
3.7 Upgrade/Downgrade	61
3.7.1 Upgrading one-X Portal for IP Office	61
3.7.2 Downgrading one-X Portal for IP Office	62
3.7.3 Removing one-X Portal for IP Office	63
3.8 Instant Messaging/Presence	64
3.8.1 IM Server Configuration	65
3.8.2 User IM Configuration	66
3.8.3 Starting the IM Server	66
3.8.4 Searching the IM Archive	66
3.8.5 Exchange Calendar Integration	67
3.8.6 Enabling the XMPP Admin Console	68
3.8.7 Enabling IM archiving	69
3.8.8 Disabling IM archiving	70
3.8.9 Disabling the XMPP Admin Console	70
3.9 Conferences	71
3.9.1 Viewing Conferences	71
3.9.2 Deleting a Scheduled Conference	71
3.9.3 Conference Notification Message	72
3.9.4 Conference Emails	73
3.10 Remote Logging	74
3.11 Troubleshooting	78
3.12 Migrating from Phone Manager to one-X Portal for IP Office	79
3.13 Adding Additional Administrators	79

4. AFA Menus

4.1 Log in	81
4.2 System Status	82
4.3 Configuration	83
4.4 DB Operations	84
4.4.1 Backup	84
4.4.2 Restore	85

5. Document History

Index	89
-------------	----

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, Linux based one-X Portal for IP Office servers use **Referred Authentication**. That means that the portal administration rights are assigned to security users configured in the security configuration of the IP Office service running on the same server. By default that is the **Administrator** user, however additional service users can also be configured for portal administrator access. If referred authentication is disabled, the portal uses its own local administrator account in the same as for a Windows based server as below.

Windows based servers use a local **Administrator** account stored in the portal's own settings (or **Superuser** for the AFA menus). The default password is changed by the installer as part of the installation process.

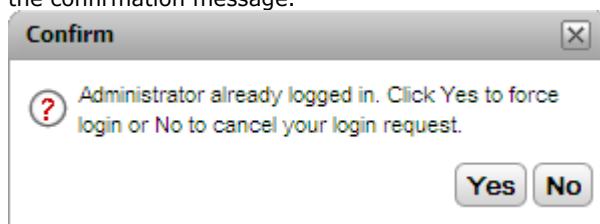
To log in:

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 will be either **9443** or **8443** for HTTPS access.
- You can use **http://** rather than **https://** and **8080** as the port if unsecure access has been configured. See [Protocol](#) ^[29].
- 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.

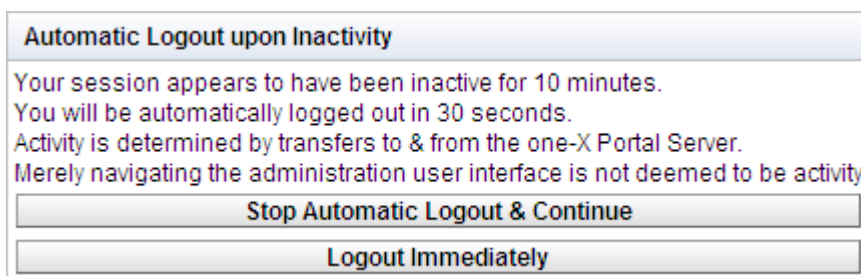


3. Click **Login**.

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	Component Status ¹²	List the last status change of the server components.
	IM/Presence server status ¹²	Shows the current status of the instant messaging server component.
	Key Recent Events ¹³	View the last 20 events on the server.
	Active Sessions ¹³	Show how many sessions are cached by one-X Portal for IP Office.
	Environment ¹⁴	Show a summary of the one-X Portal for IP Office server PC.
Configuration	Providers ¹⁵	View and edit the providers.
	Users ²¹	View and edit user one-X Portal for IP Office settings.
	CSV ²²	Export the user directory and system directory.
	Branding ²²	Specify the text that is displayed on the one-X Portal for IP Office pages after a user has logged in.
	IM/Presence ²³	Monitor the status of the IM/Presence server as a Administrator.
	Exchange service ²⁴	Configure the Exchange server to avail the calendar mining and presence information of the users.
	Conference Dial-in ²⁵	Set the fixed text to include in scheduled conference notifications.
	SMTP Configuration ²⁶	Set the email details used for emailing conference notifications.
	Syslog ²⁷	For Windows based servers, enable Syslog reporting to a remote address.
	Conference Clean Up ²⁸	Configure how long conference details are retained.
	Auto Provisioning ²⁸	Configure whether the server automatically manages providers for other IP Office systems in the network. (<i>IP Office Server Edition only</i>)
Security	Protocol ²⁹	Set whether the server uses HTTPS or HTTP and HTTP.
	Certificate ³⁰	For Windows based servers, import the security certificate to be used for secure IM/presence access.
Diagnostics	Logging Configuration ³⁰	Configure the level and method of logging supported.
	Logging Viewer ³²	Install and launch Chainsaw for log viewing.
	Network Routes ³²	Test the IP connection path to an IP address.
	IP Office Connections ³³	Test the IP connection path to an IP Office.
	Database Integrity ³³	Test the structure of the database.
	User Data Validation ³⁴	Identify possible cause of user login failure or user data corruption and reset the corrupt data.
	Call/Conference Scheduling ³⁵	Delete a scheduled conference.
Directory Integration	Directory Synchronization ³⁶	Force a system directory update by the server.
	System Directory ³⁷	View the one-X Portal for IP Office system directory.
	LDAP Directory Search ³⁸	View the external directory for which the one-X Portal for IP Office server has been configured.
Gadgets Configuration	External Gadgets List ³⁸	The external gadgets that are in the system are listed.
	Import External Gadgets ⁵¹	Import external gadgets.
	Export External Gadgets	Export external gadgets.
Web Conferences	Monitor Conferences ⁴¹	See details of any web conferences currently running on the server.
IM Archive	Search Archive	Search for the IM conversations between the system contacts.
Help & Support	Help ⁴²	Access one-X Portal for IP Office help installed on the server.
	Avaya Support ⁴²	Access the Avaya support web site for Avaya applications.

Menu	Sub-Menu	Description
	About 	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.

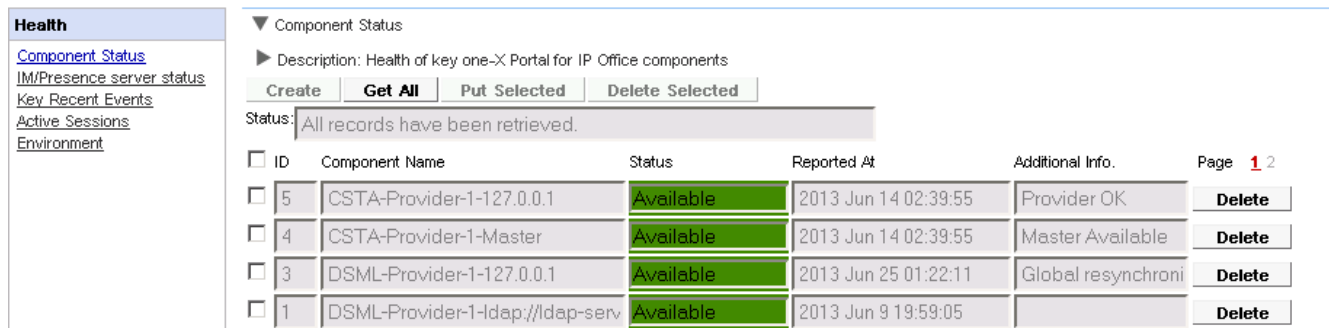
2.1 Health

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

2.1.1 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.

There should be a CSTA Provider Master plus 1 CSTA Provider for each IP Office system assigned, a DSML Provider Master plus 1 DSML Provider for each IP Office, and one DSML LDAP Provider.



Health

- [Component Status](#)
- [IM/Presence server status](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

▼ Component Status

► Description: Health of key one-X Portal for IP Office components

Create Get All Put Selected Delete Selected

Status: All records have been retrieved.

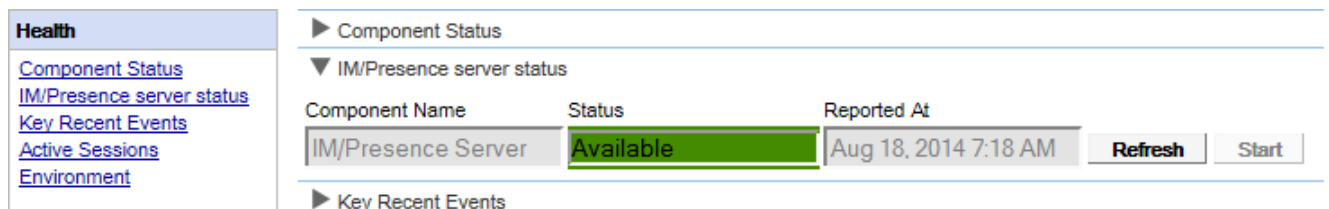
<input type="checkbox"/>	ID	Component Name	Status	Reported At	Additional Info.	Page 1 2
<input type="checkbox"/>	5	CSTA-Provider-1-127.0.0.1	Available	2013 Jun 14 02:39:55	Provider OK	Delete
<input type="checkbox"/>	4	CSTA-Provider-1-Master	Available	2013 Jun 14 02:39:55	Master Available	Delete
<input type="checkbox"/>	3	DSML-Provider-1-127.0.0.1	Available	2013 Jun 25 01:22:11	Global resynchroni	Delete
<input type="checkbox"/>	1	DSML-Provider-1-ldap://ldap-serv	Available	2013 Jun 9 19:59:05		Delete

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.

2.1.2 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](#)^[64].



Health

- [Component Status](#)
- [IM/Presence server status](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

► Component Status

▼ IM/Presence server status

Component Name	Status	Reported At		
IM/Presence Server	Available	Aug 18, 2014 7:18 AM	Refresh	Start

► Key Recent Events

2.1.3 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.

Health

- Component Status
- Key Recent Events**
- Active Sessions
- Environment

Component Status

Key Recent Events

Description:

Create Get All Put Selected Delete Selected

Status: All records have been fetched.

ID	What Happened?	Significance	When	Additional Info.	Page 1 2
<input type="checkbox"/> 1	Administrator	Low	2009-08-03 13:35:53.328	Administrator logged in	Delete
<input type="checkbox"/> 2	Installation	Medium	2009-08-03 13:45:41.078	DSML Provider is re	Delete
<input type="checkbox"/> 3	Password Changed	Medium	2009-08-03 13:46:15.812	Administrator password	Delete
<input type="checkbox"/> 4	Administrator	Low	2009-08-03 14:11:00.906	Administrator logged in	Delete

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.

2.1.4 Active Sessions

The **Active Session** menu displays the number of current browser sessions connected to the one-X Portal for IP Office server.

Health

- Component Status
- Key Recent Events
- Active Sessions**
- Environment

Component Status

Key Recent Events

Active Sessions

Description: one-X Portal for IP Office Utilisation

Refresh

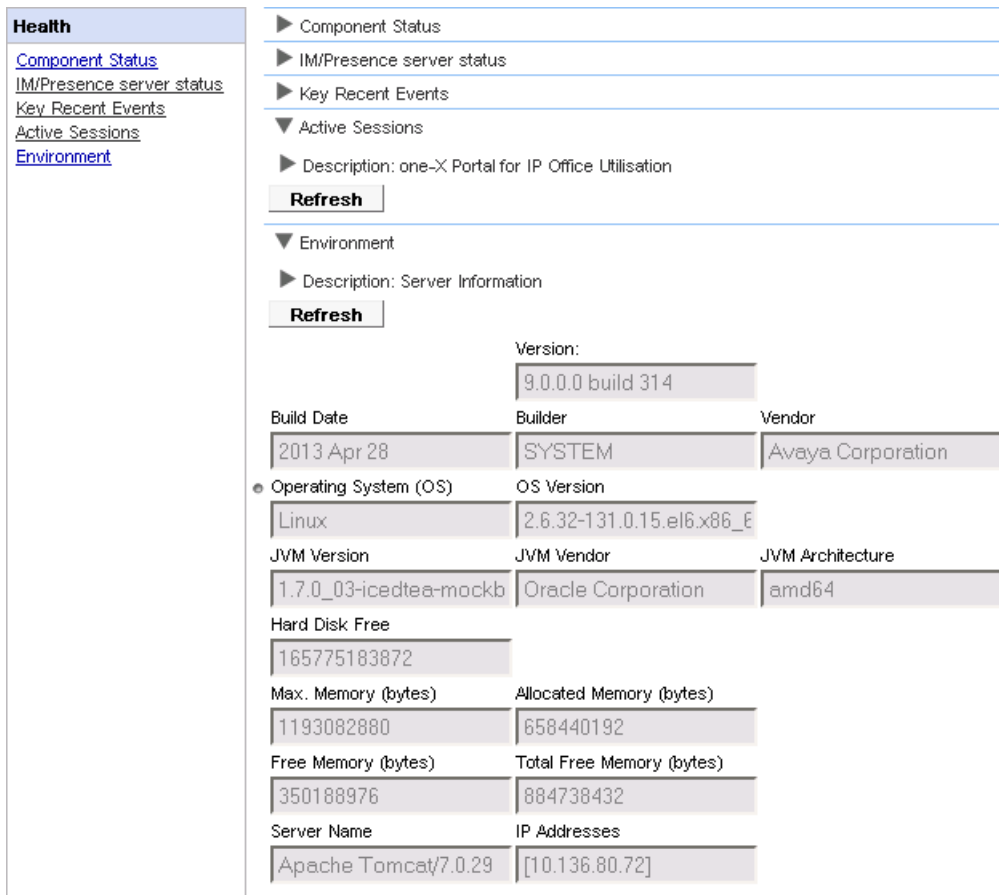
Total	User	Administrator	Application
3	0	1	2

To view the active sessions:

1. Select **Health** and then **Active Sessions**. Click **Refresh**.
2. Click on **Refresh**.

2.1.5 Environment

The **Environment** menu display information about the one-X Portal for IP Office server PC.



Health

- [Component Status](#)
- [IM/Presence server status](#)
- [Key Recent Events](#)
- [Active Sessions](#)

▶ Description: one-X Portal for IP Office Utilisation

Refresh

▼ Environment

▶ Description: Server Information

Refresh

Version:	9.0.0.0 build 314	
Build Date	Builder	Vendor
2013 Apr 28	SYSTEM	Avaya Corporation
● Operating System (OS)	OS Version	
Linux	2.6.32-131.0.15.el6.x86_64	
JVM Version	JVM Vendor	JVM Architecture
1.7.0_03-icedtea-mockb	Oracle Corporation	amd64
Hard Disk Free	165775183872	
Max. Memory (bytes)	Allocated Memory (bytes)	
1193082880	658440192	
Free Memory (bytes)	Total Free Memory (bytes)	
350188976	884738432	
Server Name	IP Addresses	
Apache Tomcat/7.0.29	[10.136.80.72]	

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.

Health	
Configuration	
Providers	▼ Providers
Users	► Description: Configure providers of services to applications
CSV	Get All Put Selected Delete Selected
Branding	Status: All records have been retrieved.
IM/Presence	<input type="checkbox"/> ID Name Page 1 2
Exchange service	<input type="checkbox"/> 4 Default-CSTA-Provider Edit Delete
	<input type="checkbox"/> 2 Default-DSML-IPO-Prov Edit Delete
	<input type="checkbox"/> 3 Default-DSML-LDAP-Pr Edit Delete
	<input type="checkbox"/> 1 Default-Presentation_La Edit Delete

During one-X Portal for IP Office, one provider of each type is created. 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.

Provider Editor

ID	<input type="text" value="3"/>
Name	<input type="text" value="Default-CSTA-Provider"/>
Data	<input 1.0"="" enco"="" type="text" value="<?xml version="/>
Provider Type Selector	<input type="text" value="Telephony (CSTA)"/> <div style="border: 1px solid #ccc; padding: 2px; width: fit-content; margin-top: 2px;"> IP Office(s) Assigned </div>
	Mid-Layer URL
	<input type="text" value="tp://localhost:8080/inkaba"/>
	Mid-Layer Username
	<input type="text" value="indoda_user"/>
CSTA Config Editor	Mid-Layer Password
	<input type="password" value="....."/>
	Mid-Layer Password Hash
	<input type="text" value="7BDDEE71046BA3FA276"/>
	Run On Port
	<input type="text" value="8080"/>
Created	<input type="text" value="2009-05-08 13:41:33.6710"/>

The **IP Office(s) Assigned** button can be used to display which IP Office systems are assigned to the provider. Additional IP Offices can be assigned while existing assignments can be deleted. Each IP Office system should only be assigned to one provider of each type (CSTA and DSML) at any time.

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
 Changes apply to the local copy of the provider record & must be committed to take affect.
 Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
 Distribution of providers over several servers may be needed for effective performance.
 The factors are: server performance, IP Office utilisation & network latency.

ID	IP Address	User	Password	
<input type="text" value="0"/>	<input type="text" value="192.168.42.1"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>

The **User** and **Password** details used must match the TCPA service user configured in the IP Office system's security configuration settings.

2.2.1.2 DSML (IP Office) Provider

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

Provider Editor

ID:

Name:

URL:

Data:

Provider Type Selector: ▼

IP Office(s) Assigned

Mid-Layer URL:

Mid-Layer Username:

DSML(IPO) Config Editor Mid-Layer Password:

Mid-Layer Password Hash:

Run On Port:

Created:

The **IP Office(s) Assigned** button can be used to display which IP Office systems are assigned to the provider. Additional IP Offices can be assigned while existing assignments can be deleted. Each IP Office system should only be assigned to one provider of each type (CSTA and DSML) at any time.

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider. Changes apply to the local copy of the provider record & must be committed to take affect. Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit. Distribution of providers over several servers may be needed for effective performance. The factors are: server performance, IP Office utilisation & network latency.

ID	IP Address	User	Password	
<input type="text" value="0"/>	<input type="text" value="192.168.42.1"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>

The **User** and **Password** details used must match the TCPA service user configured in the IP Office system's security configuration settings.

2.2.1.3 DSML (LDAP) Provider

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

Provider Editor

ID:

Name:

URL:

Provider Type Selector:

LDAP Server(s) Assigned

Mid-Layer URL:

Mid-Layer Username:

DSML(LDAP) Config Editor Mid-Layer Password:

Mid-Layer Password Hash:

Run On Port:

Created:

The **LDAP Server(s) Assigned** button can be used to configure the LDAP connection. This can include adding additional LDAP sources and configuring the LDAP directory fields to the one-X Portal for IP Office directory display fields.

LDAP Server(s) assigned to Provider

This control enables you to add & delete the LDAP Server(s) mapped to a provider. Changes apply to the local copy of the provider record & must be committed to take affect. Distribution of providers over several servers may be needed for effective performance. The factors are: server performance, IP Office utilisation & network latency.

ID	LDAP Server URL	User	Password	Base DN	
<input type="text" value="0"/>	<input type="text" value="192.168.42.12"/>	<input type="text" value="IPOffice"/>	<input type="password" value="....."/>	<input type="text"/>	<input type="button" value="Edit Field Mapping"/> <input type="button" value="Delete"/>

The **Edit Field Mapping** button displays a menu which can be used to set which LDAP field should be obtained and into which one-X Portal for IP Office directory fields the values should be displayed.

LDAP Field Mappings

FIRSTNAME:

LASTNAME:

WORKPHONE:

HOMEPHONE:

OTHERPHONE:

WORKEMAIL:

PERSONALEMAIL:

OTHEREMAIL:

2.2.1.4 Voicemail Provider

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

• Voicemail Provider

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider
Provider's Mid-Layer Username	<input type="text" value="izwi_user"/>			
Provider's Mid-Layer Password	<input type="password" value="....."/>			
Provider runs on Port	<input type="text" value="8080"/>			

Assign New Voicemail Server Unit

ID	VoiceMailServer IP Address	
<input type="text" value="0"/>	<input type="text" value="EnterValidIPAddress"/>	<input type="button" value="Delete"/>

To update or change the VMPRO Provider details in the one-X Portal for IP Office interface:

1. Log on to the one-X Portal for IP Office.
2. In the left navigation pane, click on **Configuration > Providers**.
3. On the right side, click the **Get All** button. The system displays a list of providers.

AVAYA one-X Portal for IP Office

Providers

Description: Configure Providers of services to applications

Status: All records have been retrieved.

<input type="checkbox"/>	ID	Name	Page
<input checked="" type="checkbox"/>	5	Default-VMPRO-Provider	1 2

4. Select **Default-VMPRO-Provider**.
5. Click **Edit**. The system displays the **Provider Editor** dialog box.

Provider Editor

ID	<input type="text" value="5"/>
Name	<input type="text" value="Default-VMPRO-Provider"/>
URL	<input type="text" value="http://localhost:8080/izwi"/>
Provider Type Selector	VoiceMailServer (VMPRO)
<input type="button" value="VoiceMail Server Assigned"/>	
Mid-Layer URL	<input type="text" value="http://localhost:8080/inkat"/>
Mid-Layer Username	<input type="text" value="izwi_user"/>
VoiceMail Config Editor	midLayerPassword
	<input type="password" value="....."/>
Mid-Layer Password Hash	<input type="text" value="7BDDEE71046BA3FA276"/>
Run On Port	<input type="text" value="8080"/>
Created	<input type="text" value="2011-09-20 14:16:09.0800"/>

6. Click the **VoiceMail Server Assigned** button to add or delete the Voicemail server Units.

Voicemail Server Assigned to Provider

This control enables you to add & delete the Voicemail server Unit(s).
Changes apply to the local copy of the VMPro provider record & must be committed to take affect.

ID	VoiceMailServer IP Address	
0	135.11.196.10	Delete
1	Enter valid ip address	Delete

7. Click the **Assign New Voicemail Server Unit** button to add a new row and enter the IP address of the voicemail server.

9. Click **Close**. After verifying the VMPro provider details in the **Provider Editor** dialog box, click **Close**.

10. Click the checkbox next to the provider just edited and then click on **Put Selected**. This writes the new settings of the provider back to the one-X Portal for IP Office database.

- **Note:** After updating or changing the Voicemail Pro provider details, the one-X Portal for IP Office should be restarted.

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.

You can edit some of the user settings stored in the one-X Portal for IP Office, see [Editing User Settings](#)^[56]. You can not edit user settings stored in the IP Office.

Health

Configuration

[Providers](#)

[Users](#)

[CSV](#)

[Branding](#)

[IM/Presence](#)

[Exchange service](#)

[Conference Dial-in](#)

[SMTP Configuration](#)

Security

Diagnostics

Directory Integration

Gadgets Configuration

Web Conferences

IM Archive

Help & Support

► Providers

▼ Users

► Configure supplementary application settings for users

[Create](#) [Get All](#) [Put Selected](#) [Delete Selected](#)

Status: 10 Records from 12 have been fetched.

<input type="checkbox"/>	ID	Name	Role	Bulk Edit	Page 1 2
<input type="checkbox"/>	1	Administrator	ADMINISTRATOR	Edit	Delete
<input type="checkbox"/>	3	csta_provider_user	APPLICATION	Edit	Delete
<input type="checkbox"/>	4	dsml_ipo_provider_user	APPLICATION	Edit	Delete
<input type="checkbox"/>	5	dsml_ldap_provider_u	APPLICATION	Edit	Delete
<input type="checkbox"/>	12	Extn210	USER	Edit	Delete
<input type="checkbox"/>	11	Extn211	USER	Edit	Delete
<input type="checkbox"/>	10	Extn212	USER	Edit	Delete
<input type="checkbox"/>	6	indoda_user	APPLICATION	Edit	Delete
<input type="checkbox"/>	7	inyama_user	APPLICATION	Edit	Delete
<input type="checkbox"/>	8	izwi_user	APPLICATION	Edit	Delete

To view users:

1. Click **Configuration** and select **Users**.
2. Click **Get All**.

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\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\bin**). Any existing file is overwritten.

The screenshot shows the configuration page for CSV export. On the left is a navigation menu with 'Health' and 'Configuration' sections. Under 'Configuration', there are links for 'Providers', 'Users', 'CSV', 'Branding', 'IM/Presence', and 'Exchange service'. The main content area shows a tree view with 'Providers', 'Users', and 'CSV' expanded. The 'CSV' section contains the following text: 'A control for exporting the user list and directory as a CSV file. CSV import is not supported. The exported filenames are hardcoded as exportUser.csv & exportDirectoryEntry.csv These get written to the underlying Tomcat/bin folder.' Below this text is an 'Export Configuration' button. At the bottom of the main content area, there are links for 'Branding', 'IM/Presence Server', and 'IM/Presence Exchange Service'.

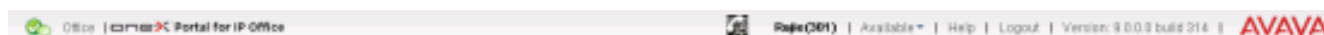
1. Select **Configuration** and then **CSV**.
2. Click **Export Configuration**.
3. Two files are created in the folder the **/bin** sub-folder of the application directory (by default **C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\bin**).
 - **exportUser.csv**
 - **exportDirectoryEntry.csv**

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 screenshot shows the configuration page for Branding. The navigation menu on the left includes 'Branding' under the 'Configuration' section. The main content area shows a tree view with 'Branding' expanded. The text in the 'Branding' section reads: 'A control for configure Branding Name so that it will shown at One-X Portal user login page. Maximum 40 characters allowed for Branding Name.' Below this text is a 'Refresh' button and a text input field labeled 'Branding Name' containing the text 'one-X Server'. To the right of the input field is a 'Save' button.

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](#) ^[64].

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▼ IM/Presence Server
Branding	Server to Server Federation <input checked="" type="checkbox"/>
IM/Presence	Disconnect on Idle <input type="checkbox"/>
Exchange service	Anyone can connect <input checked="" type="checkbox"/>
Conference Dial-in	Port number <input type="text" value="5269"/>
SMTP Configuration	Idle timeout <input type="text" value="3600"/>
	MyBuddy username <input type="text" value="mybuddy"/>
	XMPP Domain Name <input type="text" value="localhost.localdomain"/>
	<input type="button" value="Save"/>

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 may 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, for example with one-X Mobile.
- 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 server such as Google Talk.
- For Linux based servers (IP Office Server Edition, IP Office Application Server and Unified Communications Module), 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.

3. Click **Save**.

2.2.6 Exchange Service

one-X Portal for IP Office can be configured with the Exchange server to avail the calendar mining and presence information of the users. Only Microsoft Exchange Server 2007 and Microsoft Exchanger Server 2010 can be configured with one-X Portal for IP Office .

This section only provides a summary of the settings. Refer to the "*Implementing one-X Portal for IP Office*" manual for full details of Microsoft Exchange server integration.

Health	► Providers
Configuration	► Users
Providers	► CSV
Users	► Branding
CSV	► IM/Presence Server
Branding	▼ IM/Presence Exchange Service
IM/Presence	Exchange service account name <input type="text" value="AvayaAdmin"/>
Exchange service	Exchange service account password <input type="password" value="●●●●●●"/>
Conference Dial-in	Exchange service Host <input type="text"/>
SMTP Configuration	Exchange Port number <input type="text" value="6669"/>
	Exchange service proxy host <input type="text"/>
	Exchange proxy port <input type="text"/>
	Test Email Address (e.g. user@example.com) <input type="text"/>
	<input type="button" value="Save"/> <input type="button" value="Validate Exchange Service Configuration"/>
Security	
Diagnostics	
Directory Integration	
Gadgets Configuration	
IM Archive	
Web Conferences	
Help & Support	

Note:

- Test email address is required for MS Exchange 2013 for validation purpose only.
- It is not possible to execute the batch file by placing it on the desktop.
- Please make sure that the batch file is not stored on the desktop.
- Save the file on any local drives, for example C drive. To download the file, right click on the link below and select "Save Link As...".

[Download Powershell script](#)

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 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, web collaboration URL). It can also include the fixed text set through the **Conference Dial-in** menu.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▶ IM/Presence Exchange Service
Exchange service	▼ Conference Dial-in Information
Conference Dial-in	The following audio conference dial-in information will be displayed to the web conference participants:
SMTP Configuration	<div style="border: 1px solid #ccc; padding: 5px; min-height: 80px;"> <p>To access conferences, dial 01555 220637 if external or 637 if internal, and follow the spoken prompts.</p> </div>
	Dial-in
	<input type="button" value="Save"/>

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**.

2.2.8 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.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▶ IM/Presence Exchange Service
IM/Presence	▶ Conference Dial-in Information
Exchange service	▼ SMTP Configuration
Conference Dial-in	Following SMTP configuration will be used to send emails for conference scheduling feature
SMTP Configuration	Server Address <input type="text"/>
Conference Clean Up	Port number <input type="text" value="25"/> *Default SMTP Port is 25
Auto Provisioning	Email From Address <input type="text"/>
Security	Use STARTTLS <input type="checkbox"/>
Diagnostics	● Server Requires Authentication <input type="checkbox"/>
Directory Integration	User Name <input type="text"/>
Gadgets Configuration	Password <input type="text"/>
IM Archive	<input type="button" value="Save"/>
Web Conferences	
Help & Support	

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 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. Enter the fixed text that should be included in all conference notifications.
4. Click **Save**.

2.2.9 Syslog

For Windows based portal servers, this menu allows enabling of Syslog reporting. For Linux based servers, Syslog reporting for applications is managed through that server's web management menus.

The Windows server supports reporting of:

- User and administrator logins including failed login attempts.
- Starts and stops of the OpenFire component used by the portal application.

The screenshot shows the Syslog configuration page. On the left is a navigation menu with the following items: Configuration (selected), Providers, Users, CSV, Branding, IM/Presence, Exchange service, Conference Dial-in, SMTP Configuration, and Syslog. Below these are Security, Diagnostics, and Directory Integration. The main content area shows the Syslog configuration options: Enable Remote Syslog (checkbox), Syslog Server IP Address (text input), and Syslog Server UDP Port (text input). A Save button is at the bottom.

- **Enable Remote Syslog**
If selected, enables the sending of Syslog reports to the remote server details specified.
- **Syslog Server IP Address**
Set the destination IP address or domain name of the server which can receive Syslog reports.
- **Syslog Server UDP Port**
Set the port on which the remote server listens for Syslog reports.

2.2.10 Conference Clean Up

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

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▶ IM/Presence Exchange Service
IM/Presence	▶ Conference Dial-in Information
Exchange service	▶ SMTP Configuration
Conference Dial-in	▼ Conference Clean Up
SMTP Configuration	Enter number of days after the conferences are cleaned up: <input type="text" value="0"/> <input type="button" value="Save"/>
Conference Clean Up	
Auto Provisioning	▶ Auto Provisioning Configuration
Security	
Diagnostics	

2.2.11 Auto Provisioning

For a Linux based one-X Portal for IP Office server supporting IP Office Server Edition, the server can automatically add providers for additional IP Office systems when they are added to the network.

- **IP Office Server Edition Auto-Provisioning**

For a Linux based portal server supporting a IP Office Server Edition network, the server can be informed by the primary IP Office system about others systems in a network. It then automatically add or removes the appropriate providers for those other systems. This is done using the [Auto Provisioning Configuration](#) setting, which is on by default for new installations. When enabled, manual configuration of providers for additional IP Office systems is not necessary.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▶ IM/Presence Exchange Service
IM/Presence	▶ Conference Dial-in Information
Exchange service	▶ SMTP Configuration
Conference Dial-in	▶ Conference Clean Up
SMTP Configuration	▼ Auto Provisioning Configuration
Conference Clean Up	AutoProvisioningConfiguration <input checked="" type="checkbox"/>
Auto Provisioning	<input type="button" value="Save"/>
Security	Note:
Diagnostics	● Auto provisioning is a feature provided only for IP Office Server Edition platform.
Directory Integration	● Once Auto Provisioning is enabled, the new IP Office nodes in SCN will be automatically provisioned with one-X Portal.
Gadgets Configuration	● Auto provisioning will create the CSTA and DSML providers for respective IP Office nodes.
IM Archive	● If an IP Office node is removed from SCN, the corresponding provider and component status records will have to be manually removed from one-X Portal. For changes to take effect, please restart one-X Portal service.
Web Conferences	
Help & Support	

2.3 Security

2.3.1 Protocol

By default, the server installs with support for secure HTTPS access only; that is port 9443 on a Linux server, port 8443 on Windows server. This menu can be used to also enable insecure HTTP access on port 8080.

Health	▼ Protocol
Configuration	Select protocol option
Security	<input type="radio"/> Secure Connection (HTTPS)
Protocol	<input checked="" type="radio"/> Unsecure and Secure (HTTP and HTTPS)
	HTTP is insecure and prone to eavesdropping attacks.
	<input type="button" value="Save"/>
	Note: Changes to Secure Connection settings require one-X Portal server restart. The one-X Portal will NOT function till the service is restarted.

2.3.2 Certificate

For Windows based servers, this menu allows the portal to import a certificate for use with IM and presence. This is necessary for applications that want to use secure TLS connection to the portal, for example Avaya Communicator.

Health

Configuration

Security

[Protocol](#)

[Certificate](#)

▶ Protocol

▼ Certificate

Import Certificate Chain

Certificate File

Store Password

Source Alias

Note:

- Changes to Certificate Import settings are NOT applicable until one-X Portal service is restarted.
- Certificate file needs to be in PKCS12 format.

2.4 Diagnostics

This section allow you to run various diagnostic checks.

2.4.1 Logging Configuration

one-X Portal for IP Office supports a wide range of log output methods which selection of the level of logging required.

Health

Configuration

Diagnostics

[Logging Configuration](#)

[Logging Viewer](#)

[Network Routes](#)

[IP Office Connections](#)

[Database Integrity](#)

▼ Logging Configuration

▼ Master Logging Level

Set the threshold above which logging events are sent to logging targets

Choose ALL for 'log everything', choose OFF to 'disable logging'.

▼ Logging Targets(Rolling Log Files)

Rolling log files grow to a max. 10 MB, then a new one is started.

The oldest rolling log is removed when the max. of 5 is reached.

Rolling log files reflect the master logging level.

Enabled	Name	Level	File Path
<input checked="" type="checkbox"/>	Overall	ALL	../logs/1XOverallRollingFile.log
<input checked="" type="checkbox"/>	Presentation Layer	ALL	../logs/1XPresentationLayerRollingFile.log
<input checked="" type="checkbox"/>	Mid-Layer	ALL	../logs/1XMidLayerRollingFile.log
<input checked="" type="checkbox"/>	Telephony (CSTA)	ALL	../logs/1XCSTAServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (IP-Office)	ALL	../logs/1XIPODirServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (LDAP)	ALL	../logs/1XLDAPDirServiceRollingFile.log

▼ Logging Targets(Server and Network)

Socket Receiver(required for remote log viewing)

Enabled

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

- **Note:** When you install **one-X Portal for IP Office 8.1** on Windows and Linux for the first time, the default log level is **ERROR**. When you upgrade **one-X Portal for IP Office** to 8.1 on Windows, the default log level is set to **ERROR**. When you upgrade **one-X Portal for IP Office** to 8.1 on Linux, the system retains the same log level that you set before the upgrade.

2. Use the settings to enable the level and type of logging required:

- **Master Logging Level**
This field is used to select the minimum level of event to log or to disable any logging by selecting **Off**. This field is used as the default setting for the specific logging options below. They can be set to the same level or higher.

- **Logging Targets (Rolling Log Files)**

These fields are used to configure logging to file. The default is to log to files stored in a */logs* sub-folder of the application directory (by default *C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\logs*). Each log file can grow to approximately 10MB before a new file is started. When there are 5 files of a particular type, the oldest file is deleted when a new file is started.

- **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.

- **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.

- **IMPresence:** *1XSCSServicesRollingFile.log*

This log captures IP Office IM and Presence information.

- **Directory (LDAP):** *1XLDAPDirServiceRollingFile.log*

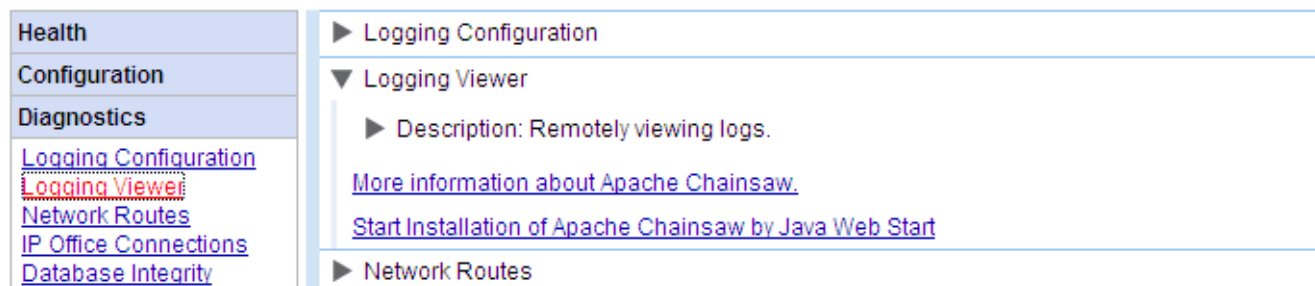
This log captures LDAP directory information.

- **Socket Receiver (required for remote log viewing)**

If enabled, an external logging application can connect to port 4560 on the server to receive logging output. The output is in log4j format and can be received by logging application such as Apache Chainsaw.

2.4.2 Logging Viewer

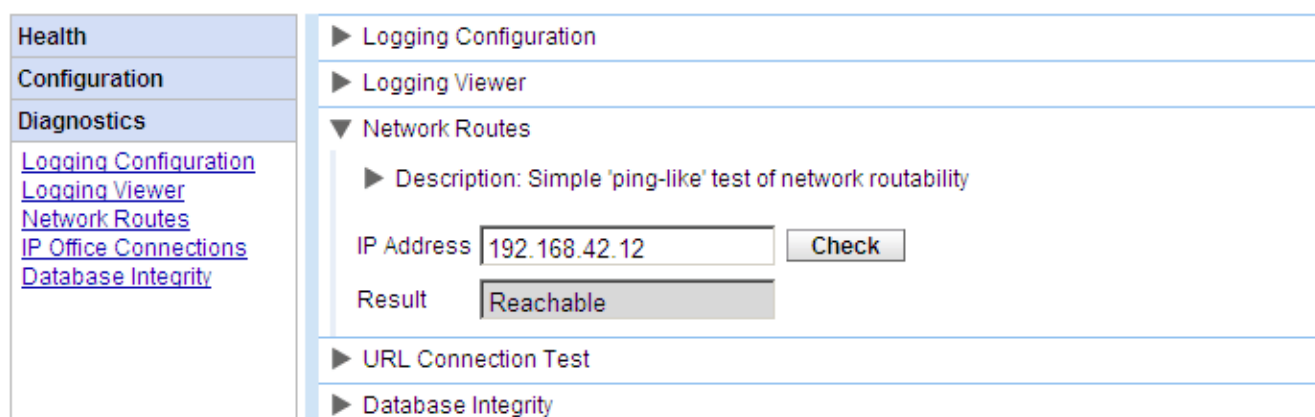
In addition to logging to files, the logging messages output by the components of one-X Portal for IP Office can also be viewed using a remote logging application that supports the Log4j format. The **Diagnostics | Logging Viewer** menu provides links for information about and [installing Apache Chainsaw](#)^[74] which is a suitable logging application .



The screenshot shows a navigation menu on the left with 'Diagnostics' selected. Under 'Diagnostics', the following links are listed: [Logging Configuration](#), [Logging Viewer](#), [Network Routes](#), [IP Office Connections](#), and [Database Integrity](#). The main content area on the right shows a tree view with 'Logging Viewer' expanded. It contains a description: 'Remotely viewing logs.', a link for 'More information about Apache Chainsaw', and a link for 'Start Installation of Apache Chainsaw by Java Web Start'. Below this, 'Network Routes' is also visible in the tree view.

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](#)^[33] should be used instead.



The screenshot shows the 'Diagnostics | Network Routes' menu. The left navigation menu has 'Diagnostics' selected, with links for [Logging Configuration](#), [Logging Viewer](#), [Network Routes](#), [IP Office Connections](#), and [Database Integrity](#). The main content area shows 'Network Routes' expanded. It includes a description: 'Simple 'ping-like' test of network routability'. Below the description is a form with an 'IP Address' field containing '192.168.42.12' and a 'Check' button. The 'Result' field shows 'Reachable'. Below the form are links for 'URL Connection Test' and 'Database Integrity'.

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).

The screenshot shows the 'IP Office Connections' diagnostic tool. On the left is a navigation menu with 'Diagnostics' selected, and sub-links for 'Logging Configuration', 'Logging Viewer', 'Network Routes', 'IP Office Connections', and 'Database Integrity'. The main area shows the 'URL Connection Test' section. It includes a description: 'Simple probe test for an IP Office Unit at an IP Address.' Below this is an input field for 'IP Address' containing '192.168.44.1' and a 'Check' button. A 'Result' window is open, displaying the following information:

```

Reachable
ipAddress=/192.168.44.1
mac=00e007026fac
type=IP 500
class=CPU
icon=0
ver=5.0 (11021)
name=IP500 Site A
state=3
state=50804
licensed=1
required license=1
  
```

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. If **Fail** is reported refer to the [Troubleshooting](#) section for known issues and resolutions.

The screenshot shows the 'Database Integrity' diagnostic tool. The left navigation menu is the same as in the previous screenshot. The main area shows the 'Database Integrity' section with the description: 'This invokes a 'sanity' check of the configuration database.' Below this is a 'Database Integrity Check' button. A table displays the results of the check:

Expected Result	Calculated Result	Result
D26D2C06BD65B000B508D09BB1	D26D2C06BD65B000B508D09BB1	Pass

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.

The screenshot shows the 'one-X Portal for IP Office' interface. On the left is a navigation menu with 'Diagnostics' selected, containing links for 'Logging Configuration', 'Logging Viewer', 'Network Routes', 'IP Office Connections', 'Database Integrity', and 'User Data Validation'. The main content area shows a tree view with 'User Data Validation' expanded. Below this is a form with 'Enter User Name' containing 'Extn5506' and a 'Validate' button. The results are displayed in a table:

Field	Status	Value/Message
Marked Deleted ?	No	
UI Preferences :	Valid	No UI Preference xml is configured for User.
CSTA Configuration :	Valid	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><Data><Password></Password><deviceID switchingSubDomainInformationElem
User Configuration :	Valid	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><arrayListWrapper xmlns:ns2="http://com.avaya.inkaba

A 'Reset' button is located to the right of the UI Preferences field.

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.

- **Conference ID**

To delete a conference requires the conference ID.

Health	▶ Logging Configuration
Configuration	▶ Logging Viewer
Security	▶ Network Routes (Not for IP Offices)
Diagnostics	▶ IP Office Connections
Logging Configuration	▶ Database Integrity
Logging Viewer	▶ User Data Validation
Network Routes	▼ Call/Conference Scheduling
IP Office Connections	
Database Integrity	
User Data Validation	
Call/Conference Scheduling	

Enter Scheduled Conference ID to delete:

To delete a scheduled conference:

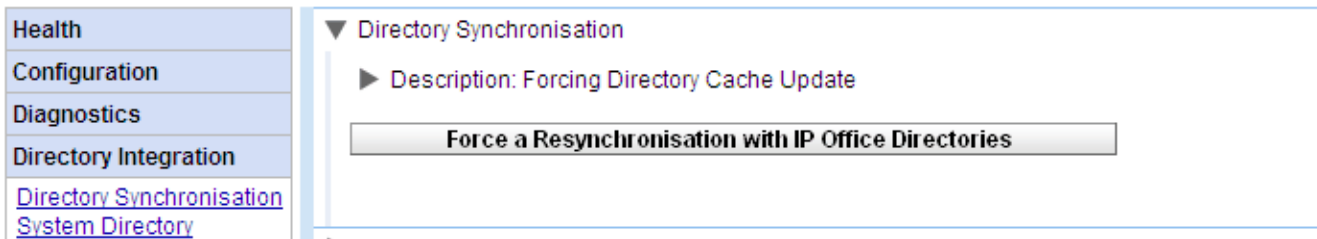
1. Click **Diagnostics** and select **Call/Conference Scheduling**.
2. Enter the ID of the future conference to delete from the scheduled conferences.
3. Click **Delete**.

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.




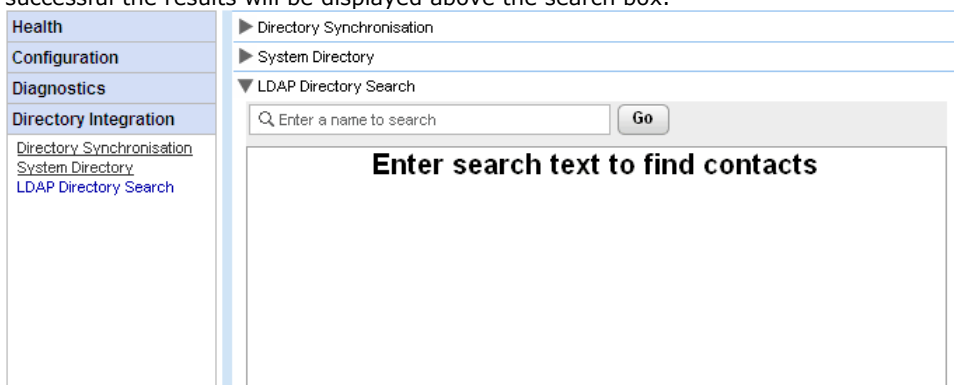
- **Force a Resynchronization with IP Office Directories**
Requests an update of the system directory entries stored in the configurations of the IP Office systems. The entries in the **System Directory** can also be viewed and checked through the [Directory Integration | System Directory](#) option.

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](#) option.

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 on the  icon. If the search is successful the results will be displayed above 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 XMPP Hunt groups. It also does not show 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](#) ^[36] 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.
Ringling		This icon is used for an internal contact that is currently ringing.

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 and 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 **Delete** in the contact details.

2.6 Gadget configuration

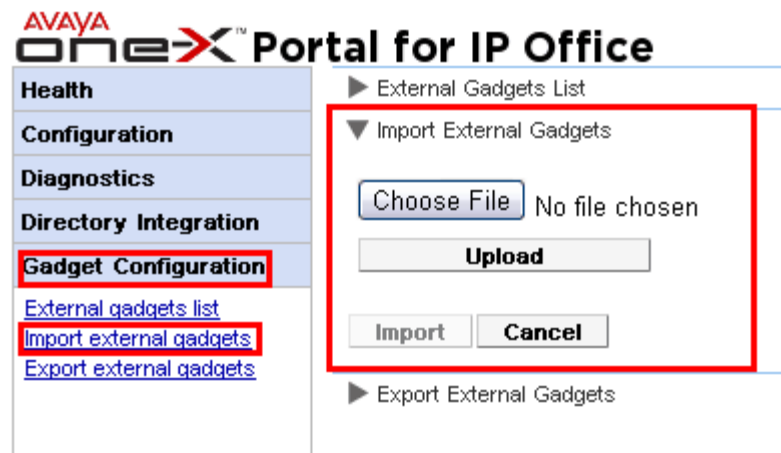
As an administrator of one-X Portal for IP Office you can configure a list of external gadgets in the system. You can enable, edit, and delete the gadgets that the user of one-X Portal for IP Office can add. The user of one-X Portal for IP Office can add only those external gadgets that the administrator 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](#)^[54] or [import external gadgets](#)^[51] 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](#)^[51].



To import a gadgets file:

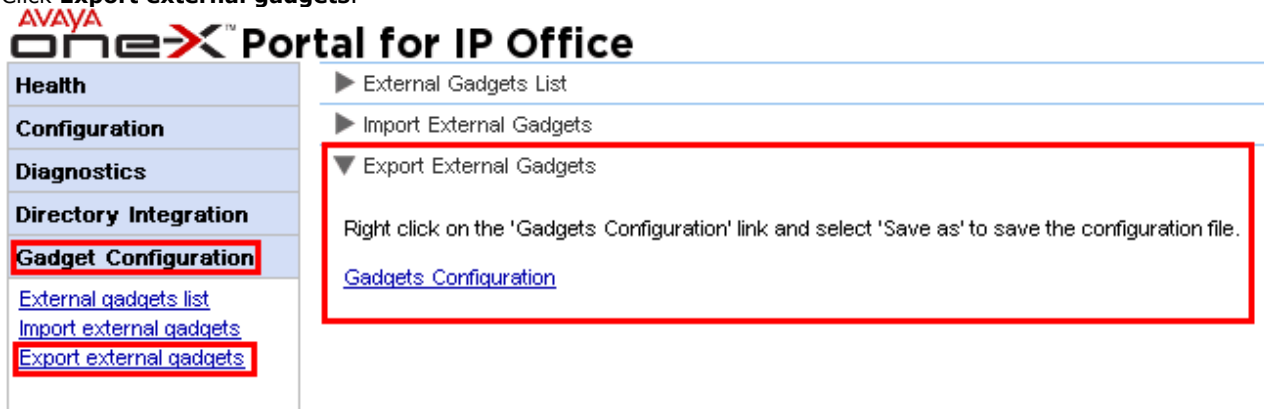
1. Click **Gadget Configuration** and select **Import external gadgets**.
2. Click **Choose File** to browse for the configuration file.
3. Click **Upload**. The system uploads the XML file on the one-X Portal for IP Office.
4. Click **Import** to add the third party gadget to the *Gadgets List*.
5. 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](#) 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](#) ^[64].

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.

- Health
- Configuration
- Security
- Diagnostics
- Directory Integration
- Gadgets Configuration
- Web Conferences
- IM Archive**
- [Search Archive](#)

Participants

Start

Keywords

End

Participants	Start	Count
Extn210 mybuddy	Aug 15, 2014 12:00 PM	4
Extn210 Extn211	Aug 15, 2014 8:05 AM	2
Extn210 everyone	Aug 14, 2014 2:13 PM	1

Participants: Extn210, Extn211
 Date: Aug 15, 2014 8:05 AM
 Keyword:

7:59 Extn210 : Morning. How are the updates going?
 8:5 Extn211 : Okay now we have the system running. Tell you how far we got at the end of today.

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 Web Conferences

On suitable licensed systems, the one-X Portal for IP Office server also supports web conferencing services for users.

2.8.1 Monitor Conferences

This menu allows you see details of any 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).

AVAYA one-X Portal for IP Office

Host	User Name	Extension	Join Time	Leave Time
Peter Power				
	Peter Power	239	Jul 23, 2014 4:19 PM	
	Gary Guest	5555555	Jul 23, 2014 4:22 PM	
Lync01(230)				
	Lync01	230	Jul 23, 2014 4:20 PM	
	Getrude Guest	666666	Jul 23, 2014 4:23 PM	

IM Archive
Help & Support

Refresh

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.

2.9 Help & Support

Help | Help

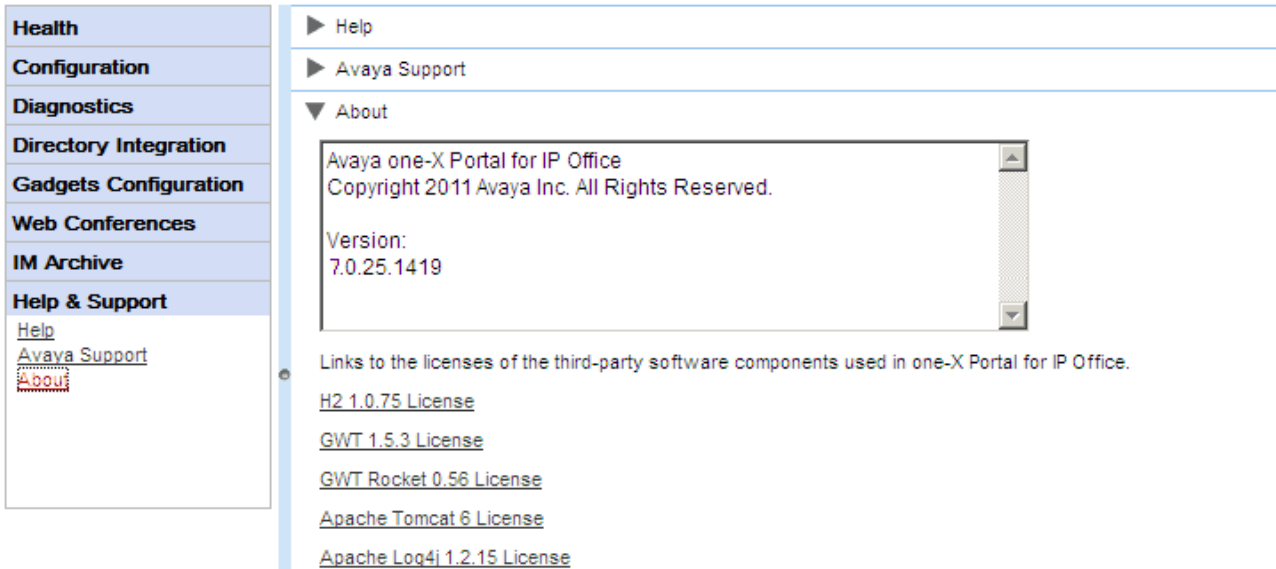
Provides links to both the one-X Portal for IP Office user help and to this document as help.

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.



The screenshot displays a web interface with a left-hand navigation menu and a main content area. The navigation menu includes categories like Health, Configuration, Diagnostics, and Help & Support. Under 'Help & Support', there are links for 'Help', 'Avaya Support', and 'About'. The 'About' page is active, showing the following content:

- ▶ Help
- ▶ Avaya Support
- ▼ About
 - Avaya one-X Portal for IP Office
Copyright 2011 Avaya Inc. All Rights Reserved.
 - Version:
7.0.25.1419

Below the version information, there is a text block: "Links to the licenses of the third-party software components used in one-X Portal for IP Office." followed by a list of license links:

- [H2 1.0.75 License](#)
- [GWT 1.5.3 License](#)
- [GWT Rocket 0.56 License](#)
- [Apache Tomcat 6 License](#)
- [Apache Log4j 1.2.15 License](#)

Chapter 3.

Maintenance Tasks

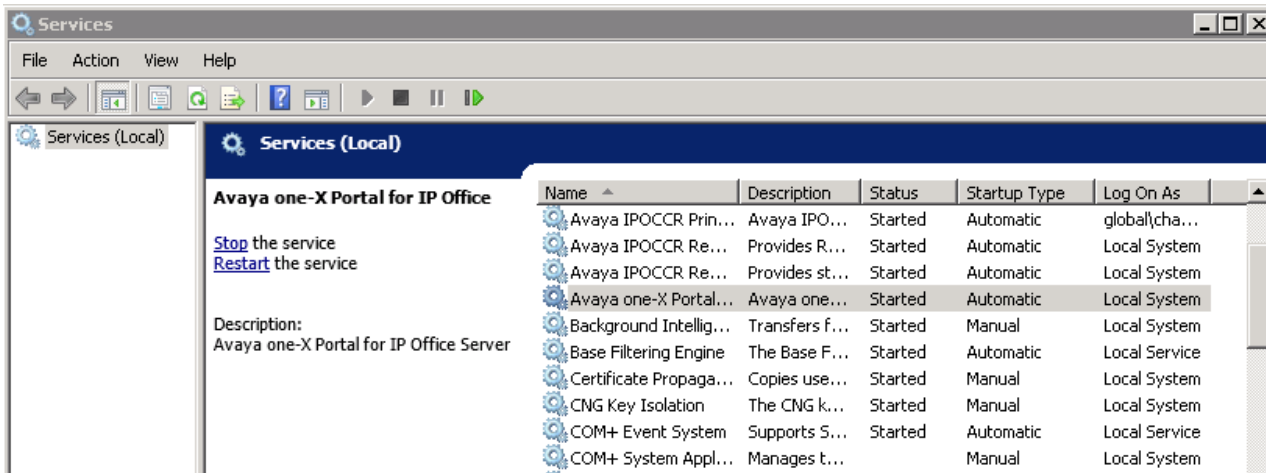
3. Maintenance Tasks

3.1 Manually Starting the Service

The method for starting/stopping the one-X Portal for IP Office service depends on whether the application is installed on a Windows or Linux server.

Windows Based Server

The one-X Portal for IP Office application installs as a service called Avaya one-X Portal. It can be started and stopped through the standard Windows Services control panel.



Note that when starting or restarting the service, even though the Avaya one-X Portal service will report itself as started within a few seconds, it will be up to 15 minutes before the application is fully operational. One way to monitor progress is to use Windows Task Manager. Typically as one-X Portal for IP Office is starting, the **PF Usage** will gradually increase to approximately 2.3GB before one-X Portal for IP Office has started.

- **No Service !**

If the service is not present, the most likely cause is a port conflict or Java problem. Refer to [Troubleshooting](#)⁷⁸.

Linux Based Server

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 1400, 1600, 9500 or 9600 Series phone with a **Call Log** or **History** button, or an M-Series or T-Series phone, 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) provider and to the Directory (DSML IP Office) provider.

- **IP Office Server Edition Auto-Provisioning**

For a Linux based portal server supporting a IP Office Server Edition network, the server can be informed by the primary IP Office system about others systems in a network. It then automatically add or removes the appropriate providers for those other systems. This is done using the [Auto Provisioning Configuration](#) ⁽²⁸⁾ setting, which is on by default for new installations. When enabled, manual configuration of providers for additional IP Office systems is not necessary.

To add another IP Office system:

- **Warning**

This process requires the Avaya one-X Portal service to be restarted. During the restart one-X Portal for IP Office will not be available to all 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](#) ⁽⁷⁾ 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**.

The screenshot shows the 'one-X Portal for IP Office' interface. On the left is a navigation menu with 'Diagnostics' selected. The main content area shows 'Logging Configuration' expanded, with 'IP Office Connections' selected. Below this, there is a 'Description: Simple probe test for an IP Office Unit at an IP Address.' and a form with 'IP Address' set to '10.136.80.72' and a 'Check' button. The 'Result' section shows a 'Reachable' status with the following details:

```

Reachable
IP Address=10.136.80.72
mac=001bb9f94fb4
type=IPO-MediaServer
class=Internal
icon=0
version=9.0.0 (242)
name=DocPrimarySE
state=3
baseport=50804
licensed=7
required license=7
    
```

c. If the IP Office is reachable, the results will include base information about the IP Office system.

4. Select **Configuration** and then **Providers**.

5. Click on **Get All** to retrieve the current provider records from the one-X Portal for IP Office database.

The screenshot shows the 'Providers' configuration page. The left navigation menu has 'Configuration' selected, and 'Providers' is highlighted. The main content area shows a description: 'Configure providers of services to applications'. There are buttons for 'Get All', 'Put Selected', and 'Delete Selected'. The 'Status' bar indicates 'All records have been retrieved.' Below this is a table of providers:

ID	Name	Page	1	2
<input type="checkbox"/>	4	Default-CSTA-Provider	Edit	Delete
<input type="checkbox"/>	2	Default-DSML-IPO-Prov	Edit	Delete
<input type="checkbox"/>	3	Default-DSML-LDAP-Pr	Edit	Delete
<input type="checkbox"/>	1	Default-Presentation_La	Edit	Delete

6. Next to the **Default-CSTA-Provider**, click on **Edit**.

The screenshot shows the 'Provider Editor' form for the 'Default-CSTA-Provider'. The form contains the following fields:

- ID: 4
- Name: Default-CSTA-Provider
- URL: http://localhost:8080/ind
- Provider Type Selector: Telephony (CSTA)
- IP Office(s) Assigned: (button)
- Mid-Layer URL: http://localhost:8080/ink
- Mid-Layer Username: indoda_user
- Mid-Layer Password: (masked with dots)
- Mid-Layer Password Hash: 7BDDEE71046BA3FA27
- Run On Port: 8080
- Created: 2012-03-27 11:09:06.9350

A 'Close' button is located at the bottom left of the form.

7. Click on **IP Office(s) Assigned.**

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
 Changes apply to the local copy of the provider record & must be committed to take affect.
 Up to 64 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
 Distribution of providers over several servers may be needed for effective performance.
 The factors are: server performance, IP Office utilisation & network latency.

ID	IP Address	User	Password	
0	127.0.0.1	EnhTcpaService	●●●●●●●●	Delete

Close Assign New IP Office Unit

8. Click on **Assign New IP Office Unit.**

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
 Changes apply to the local copy of the provider record & must be committed to take affect.
 Up to 64 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
 Distribution of providers over several servers may be needed for effective performance.
 The factors are: server performance, IP Office utilisation & network latency.

ID	IP Address	User	Password	
0	127.0.0.1	EnhTcpaService	●●●●●●●●	Delete
1	Enter valid ip address	EnhTcpaService	●●●●●●●●	Delete

Close Assign New IP Office Unit

9. Enter the **IP Address** of the IP Office control unit.

10. Enter the **User** name and **Password** that match the T CPA security user configured in the IP Office system.

11. Click **Close**.

12. Click **Close** again.

13. Click the checkbox next to the provider just edited and then click on **Put Selected**. This writes the new settings of the provider back to the one-X Portal for IP Office database.

14. Repeat the process but this time adding the new IP Office to the IP Offices assigned to the **Default- DSML-IPO-Provider**. Again end with **Put Selected**.

15. [Restart the Avaya one-X Portal service](#) ^[44].

16. When the service has fully restarted, log in to the administrator menus again.

17. Select **Health** and then **Component Status**.

18. 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.

Health

- [Component Status](#)
- [IM/Presence server status](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

▼ Component Status

► Description: Health of key one-X Portal for IP Office components

Create **Get All** Put Selected Delete Selected

Status: All records have been retrieved.

ID	Component Name	Status	Reported At	Additional Info.	Page 1 2
<input type="checkbox"/>	5 CSTA-Provider-1-127.0.0.1	Available	2013 Jun 14 02:39:55	Provider OK	Delete
<input type="checkbox"/>	4 CSTA-Provider-1-Master	Available	2013 Jun 14 02:39:55	Master Available	Delete
<input type="checkbox"/>	3 DSML-Provider-1-127.0.0.1	Available	2013 Jun 24 23:22:11	Global resynchroni	Delete
<input type="checkbox"/>	1 DSML-Provider-1-ldap://ldap-serv	Available	2013 Jun 9 19:59:05		Delete

► IM/Presence server status

► Key Recent Events

► Active Sessions

► Environment

19. 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.

20. 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**

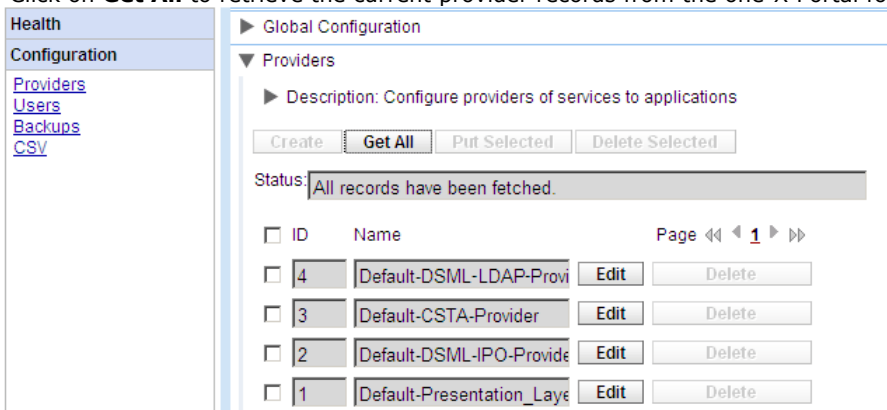
This process requires the Avaya one-X Portal service to be restarted. During the restart one-X Portal for IP Office will not be available to all users for up to 15 minutes.

- **IP Office Server Edition Auto-Provisioning**

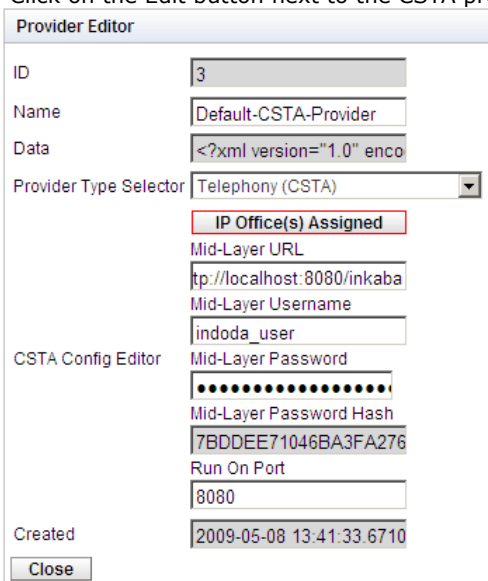
For a Linux based portal server supporting a IP Office Server Edition network, the server can be informed by the primary IP Office system about others systems in a network. It then automatically add or removes the appropriate providers for those other systems. This is done using the [Auto Provisioning Configuration](#) ²⁸ setting, which is on by default for new installations. When enabled, manual configuration of providers for additional IP Office systems is not necessary.

To change the IP Office details:

1. [Log in](#) ⁷⁴ to the administrator menu.
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 **Get All** to retrieve the current provider records from the one-X Portal for IP Office database.



5. Click on the Edit button next to the CSTA provider to which the IP Office was assigned.



6. Edit the details displayed to match the new settings of the IP Office system.

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
Distribution of providers over several servers may be needed for effective performance.
The factors are: server performance, IP Office utilisation & network latency.

ID	IP Address	User	Password	
0	192.168.42.1			Delete

Close Assign New IP Office Unit

7. Click **Close**.
8. Click **Close** again.
9. Click the checkbox next to the provider just edited and then click on **Put Selected**. This writes the new settings of the provider back to the one-X Portal for IP Office database.
10. Repeat the process but this time updating the details for the DSML IP-Office provider to which the IP Office was previously assigned. Again end with **Put Selected**.
11. Restart the Avaya one-X Portal service.

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&up_def_from
=USD&up_def_to=EUR&synd=open&w=320&h=170&title=Currency+Converter&border=
%23ffffff%7C0px%2C1px+solid+%2382CAFA%7C0px%2C2px+solid+%23BDEDF%7C0px%2C3px+solid+%23
E0FFFF&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><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry Birds</ru><zh>Angry
Birds</zh></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><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry Birds</ru><zh>Angry
Birds</zh></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><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry Birds</ru><zh>Angry
Birds</zh></names></tooltip>
<url>http://www.gmodules.com/ig/ifr?url=http://www.forumforyou.it/google_gadget_angry_birds.xml&synd=open
&w=820&h=680&title=Angry+Birds&border=%23ffffff%7C3px%2C1px+solid+%23999999&ou
tput=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

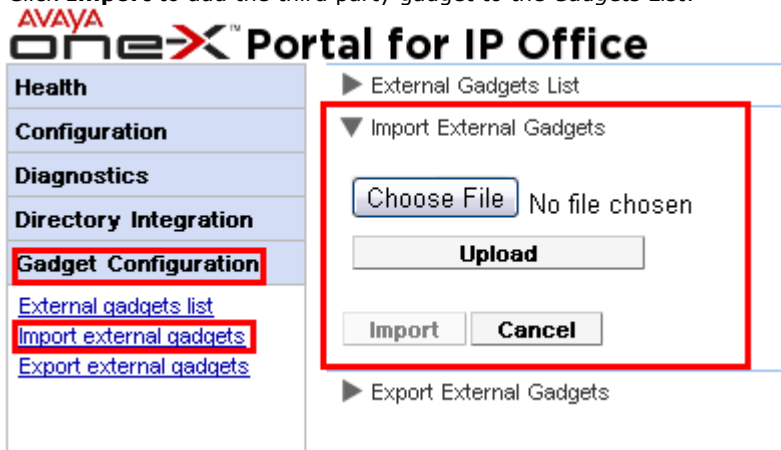
5. Details of other elements:

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 ^[50]

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*.



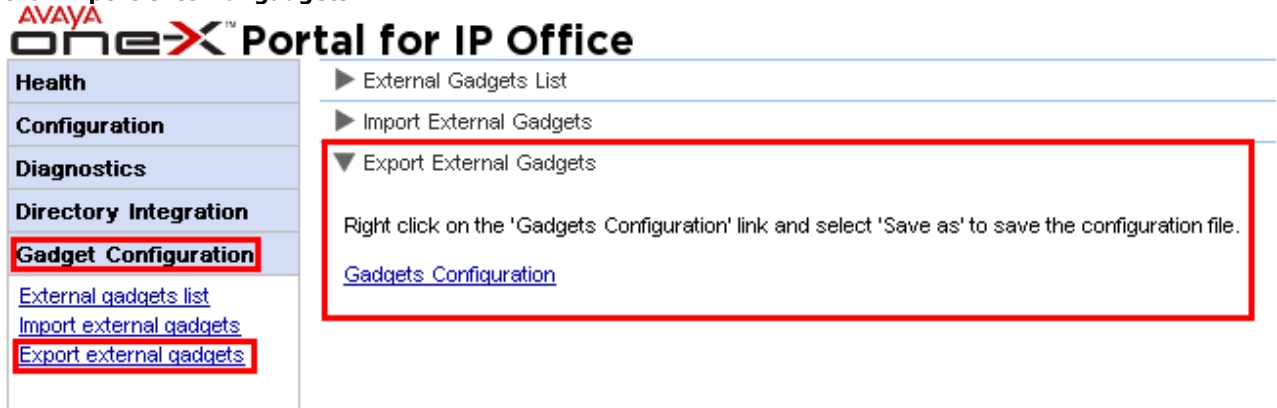
6. The next time the user logs into the one-X Portal for IP Office, the third party gadget is available to user to add to their portal.

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](#) 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](#)^[50].

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](#)^[54] 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 Avaya clients such as mobility, Avaya Communicator and others after 10 minutes of the synchronization time and users should also be logged in after the synchronization.

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.

The screenshot shows a 'User Editor' form with the following fields and values:

ID	13
Name	Extn101
Unique Identifier	B7462000CEEC11DB80
Display Name	Extn101
Password
Password Hash	7B295DC8FA34A5BE93
User Role	User
User Configuration Type Selector	Select
User Configuration Type Specific Editor	
User Role Configuration	<input checked="" type="radio"/> User <input type="radio"/> Manager
Created	2013-05-14 01:29:06.1600

Buttons: Save, Cancel

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.

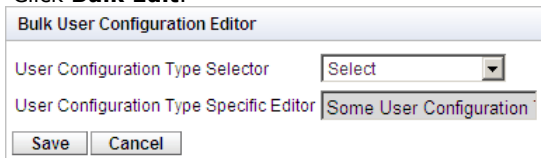
- **IM/Presence Configuration**

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**.

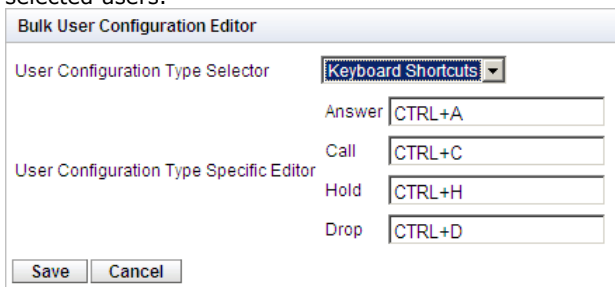
To bulk edit user settings:

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**.



The dialog box is titled "Bulk User Configuration Editor". It contains two main sections. The first section is "User Configuration Type Selector" with a dropdown menu currently set to "Select". The second section is "User Configuration Type Specific Editor" with a dropdown menu currently set to "Some User Configuration". At the bottom of the dialog are two buttons: "Save" and "Cancel".

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



The dialog box is titled "Bulk User Configuration Editor". The "User Configuration Type Selector" dropdown is now set to "Keyboard Shortcuts". Below this, there are four input fields for specific settings: "Answer" (CTRL+A), "Call" (CTRL+C), "Hold" (CTRL+H), and "Drop" (CTRL+D). The "User Configuration Type Specific Editor" section is empty. At the bottom are "Save" and "Cancel" buttons.

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](#)³⁶ 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 the Avaya one-X Portal service to be restarted. During the restart one-X Portal for IP Office will not be available to all 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. Click on **Get All** to retrieve the current provider records from the one-X Portal for IP Office database.
4. Click on the **Edit** button next to the LDAP provider.
5. Click on **LDAP Server(s) Assigned**. This will list the LDAP source already assigned.

The screenshot shows a window titled "LDAP Server(s) assigned to Provider". It contains a table with columns: ID, LDAP Server URL, User, Password, and Base DN. The first row has values: 0, 192.168.42.12, IPOffice, a masked password, and an empty Base DN field. There are buttons for "Close", "Assign New LDAP Server", "Edit Field Mapping", and "Delete".

ID	LDAP Server URL	User	Password	Base DN
0	192.168.42.12	IPOffice	

6. 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*.

7. Click on **Edit Field Mapping**. 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.

The screenshot shows a window titled "LDAP Field Mappings". It contains a table with columns: Field Name and LDAP Field Name. The first row has values: FIRSTNAME and givenName. There are buttons for "Close" and "Defaults".


Field Name	LDAP Field Name
FIRSTNAME	givenName
LASTNAME	sn
WORKPHONE	telephoneNumber
HOMEPHONE	homePhone
OTHERPHONE	cel
WORKEMAIL	mail
PERSONALEMAIL	personalMail
OTHEREMAIL	otherMail

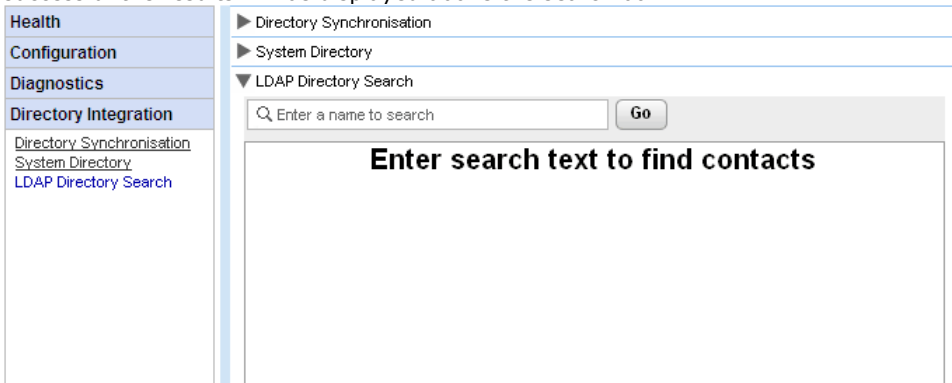
8. Click **Close**.
9. Select the check box next to the new entry and click on **Put Selected**.
10. [Restart the Avaya one-X Portal service](#)⁴⁴.

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 on the  icon. If the search is successful the results will be displayed above the search box.



The screenshot shows the Avaya one-X Portal administrator interface. On the left is a navigation menu with the following items: Health, Configuration, Diagnostics, Directory Integration (highlighted), Directory Synchronisation, System Directory, and LDAP Directory Search. The main content area shows a tree view with 'Directory Synchronisation', 'System Directory', and 'LDAP Directory Search' (expanded). Below the tree is a search box with the placeholder text 'Enter a name to search' and a 'Go' button. Below the search box is a large empty box with the text 'Enter search text to find contacts'.

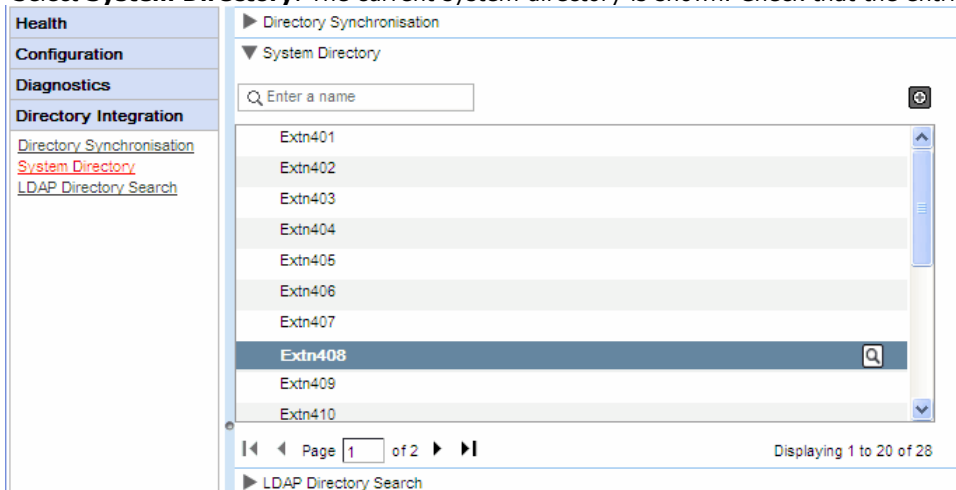
3.6.3 Checking and Updating the System Directory

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.

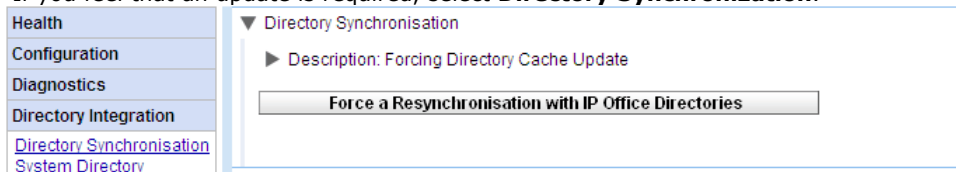
By default, the one-X Portal for IP Office application updates the system directory records every 300 seconds approximately. Through the one-X Portal for IP Office administrator menus you can view the system directory and force an update.

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 Upgrade/Downgrade

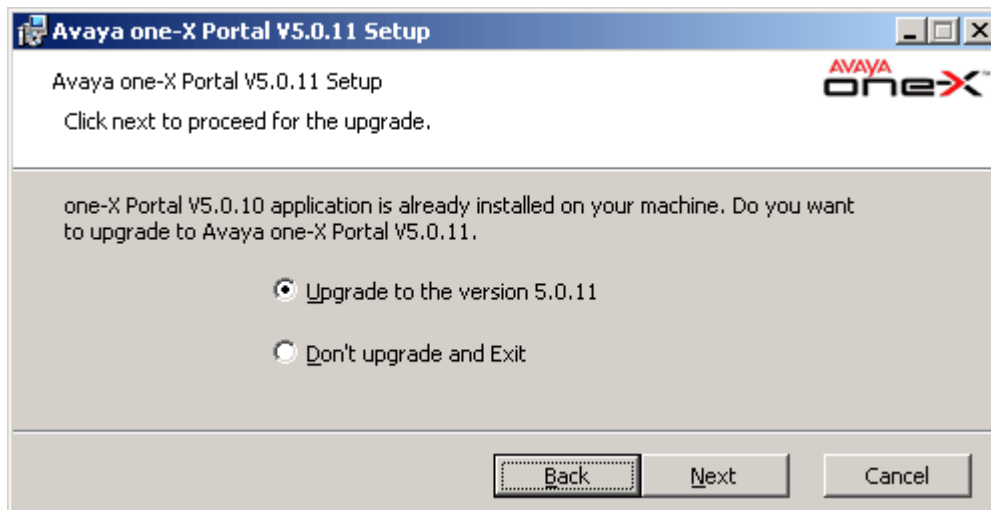
3.7.1 Upgrading one-X Portal for IP Office

Before upgrading one-X Portal for IP Office ensure that you have read the Avaya IP Office Technical Bulletin for the release of one-X Portal for IP Office software to which you want to install or the IP Office software release in which it was included. The Technical Bulletin will include details of any special requirements and additional steps that are not in this documentation.

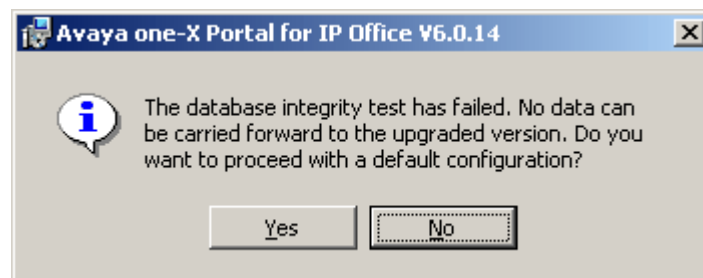
If one-X Portal for IP Office is already installed on a server PC and the installation file for a later version is run, the existing version will be detected and you will be prompted whether to upgrade or not. If you select to upgrade, the process is similar to normal software installation, however some installation options will be grayed out as the existing settings cannot be changed.

- **Warning**

This process requires the Avaya one-X Portal service to be restarted. During the restart one-X Portal for IP Office will not be available to all users for up to 15 minutes.



- If the existing one-X Portal for IP Office database cannot be upgraded a warning will be displayed. If you select Yes, the existing database is replaced with a defaulted database. If you select No you will need to rerun the installer in order to [downgrade](#) back to the version of one-X Portal for IP Office that is compatible with the database.



During the upgrade process a backup file is created (backup.sql). This is not a full backup of the one-X Portal for IP Office system and should not be used for restoration of setting.

3.7.2 Downgrading one-X Portal for IP Office

If the one-X Portal for IP Office application software has been upgraded using the [upgrade process](#)^[61], it is also possible to downgrade back to the original installed version.

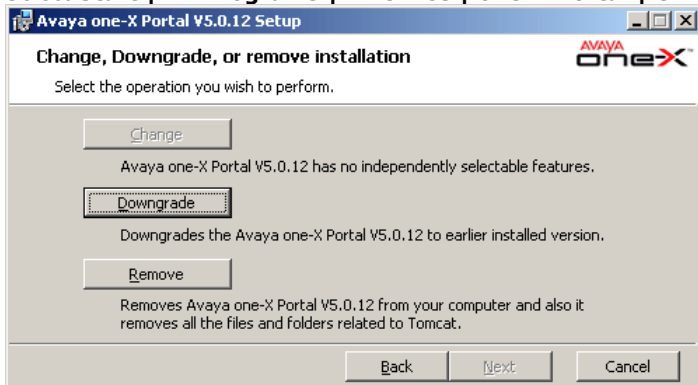
- **Note:** The installation of one-X Portal for IP Office and the last upgrade to one-X Portal for IP Office are both be listed in the Windows Control Panel **Add and Remove Programs** list. Note however that removing either of these will remove the whole application.

Before downgrading one-X Portal for IP Office ensure that you have read the Avaya IP Office Technical Bulletin for the one-X Portal for IP Office software releases. The Technical Bulletin will include details of any special requirements and additional steps that are not in this documentation.

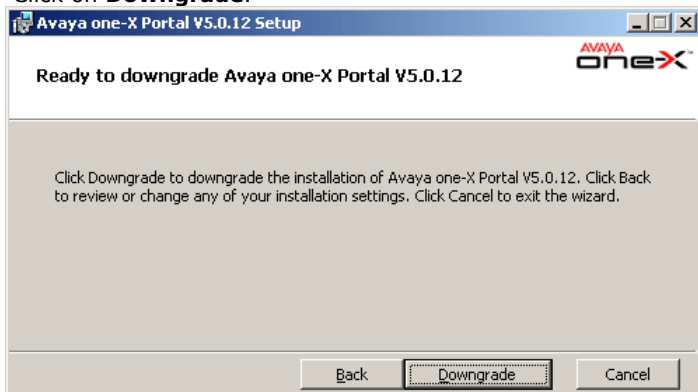
- **Warning**
This process requires the Avaya one-X Portal service to be restarted. During the restart one-X Portal for IP Office will not be available to all users for up to 15 minutes.

To downgrade one-X Portal for IP Office:

1. Select **Start | All Programs | IP Office | one-X Portal | Uninstall one-X Portal**.



2. Click on **Downgrade**.



3. When the downgrade has been completed, the Avaya one-X Portal needs to be [restarted manually](#)^[44].

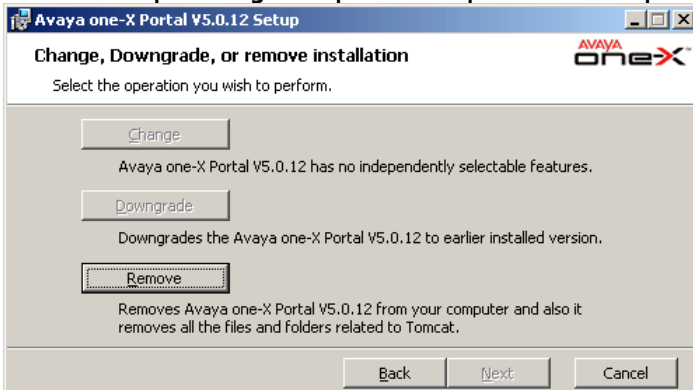
3.7.3 Removing one-X Portal for IP Office

There are 2 methods for removing the one-X Portal for IP Office application.

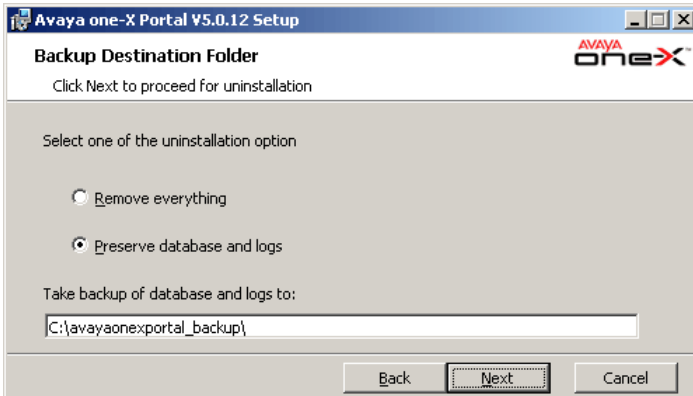
To uninstall one-X Portal for IP Office:

This method of removal allows selection of whether backups of the database and log files should be kept.

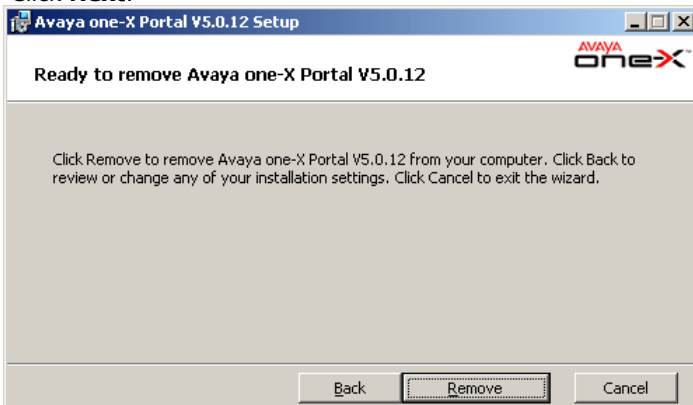
1. Select **Start | All Programs | IP Office | one-X Portal | Uninstall one-X Portal**.



2. Select **Remove**.



3. Click **Next**.



4. Click **Remove** to start the process of removing files.

To removing one-X Portal for IP Office via the Windows Control Panel:

The **Add or Remove Programs** option in the Windows Control Panel can be used to remove one-X Portal for IP Office. This method automatically makes backup copies of the database and log files in the folder **c:\avayaonportal_backup**.

1. Start the standard Windows Control Panel.
2. Select **Add or Remove Programs**.
3. Select **one-X Portal** and then click **Remove**.
 - If the one-X Portal for IP Office has been upgraded at some stage, there will be a program entry for both the original one-X Portal for IP Office installation and the most recent upgrade. Select the upgrade installation and then click Remove. This will remove both the upgrade and the original installation.

3.8 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](#) ^[65]
- [Starting the IM Server](#) ^[66]
- [Searching the IM Archive](#) ^[66]
- [Exchange Calendar Integration](#) ^[67]

To disable IM archiving:

1. [Enabling Admin console of XMPP Server](#) ^[68]
2. [Using XMPP Server to disable IM archiving settings](#) ^[70]
3. [Disabling Admin console of XMPP Server](#) ^[70]

To enable IM archiving:

1. [Enabling Admin console of XMPP Server](#) ^[68]
2. [Using XMPP Server to enable IM archiving settings](#) ^[69]
3. [Disabling Admin console of XMPP Server](#) ^[70]

Changes to Default XMPP Operation

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

Issue: New User Not Appearing in XMPP Group

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).

3.8.1 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](#) ^[64].

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▼ IM/Presence Server
Branding	Server to Server Federation <input checked="" type="checkbox"/>
IM/Presence	Disconnect on Idle <input type="checkbox"/>
Exchange service	Anyone can connect <input checked="" type="checkbox"/>
Conference Dial-in	Port number <input type="text" value="5269"/>
SMTP Configuration	Idle timeout <input type="text" value="3600"/>
	MyBuddy username <input type="text" value="mybuddy"/>
	XMPP Domain Name <input type="text" value="localhost.localdomain"/>
	<input type="button" value="Save"/>

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 may 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, for example with one-X Mobile.
- 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 server such as Google Talk.
- For Linux based servers (IP Office Server Edition, IP Office Application Server and Unified Communications Module), 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.

3. Click **Save**.

3.8.2 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.

When adding a new user to the IP Office configuration, the user should be added and the configuration saved before the user is then also added to any XMPP groups. This ensures correct synchronization of users known to the portal server and the IM/presence rights of those users.

3.8.3 Starting the IM Server

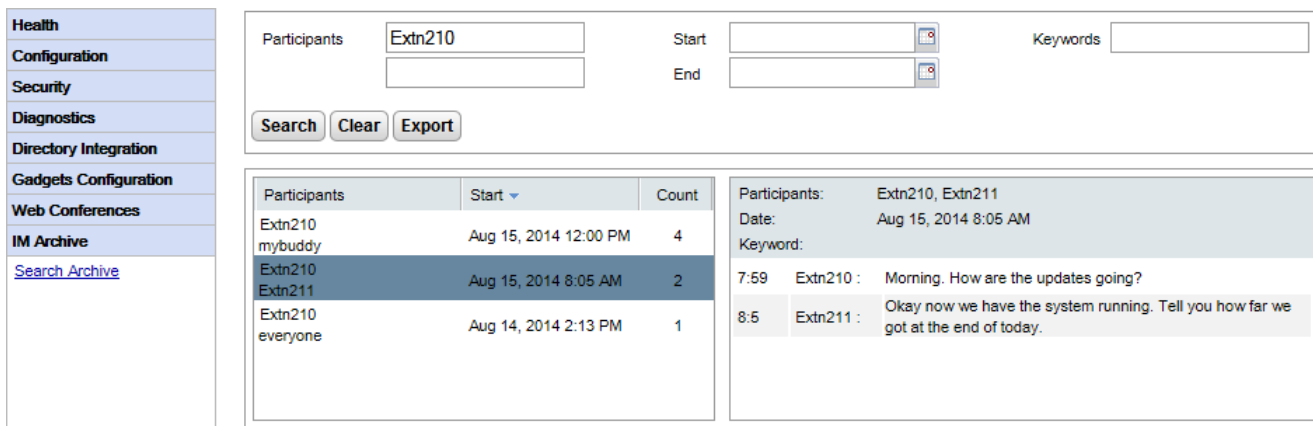
You can check the status of the IM/presence server through the [IM/presence server status](#) ¹² menu. If the IM/presence server is not running, you can use the process below to start the service.

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"*.

3.8.4 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.



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.

3.8.5 Exchange Calendar Integration

one-X Portal for IP Office can be configured with the Exchange server to avail the calendar mining and presence information of the users. Only Microsoft Exchange Server 2007 and Microsoft Exchanger Server 2010 can be configured with one-X Portal for IP Office .

This section only provides a summary of the settings. Refer to the "*Implementing one-X Portal for IP Office*" manual for full details of Microsoft Exchange server integration.

Health	<ul style="list-style-type: none"> ▶ Providers ▶ Users ▶ CSV ▶ Branding ▶ IM/Presence Server ▼ IM/Presence Exchange Service 	
Configuration		
Providers Users CSV Branding IM/Presence Exchange service Conference Dial-in SMTP Configuration		
Security		
Diagnostics		
Directory Integration		
Gadgets Configuration		
IM Archive		
Web Conferences		
Help & Support		

Exchange service account name	<input type="text" value="AvayaAdmin"/>	The result of validation of Exchange Service Configuration will appear here.
Exchange service account password	<input type="password" value="●●●●●●"/>	
Exchange service Host	<input type="text"/>	
Exchange Port number	<input type="text" value="6669"/>	
Exchange service proxy host	<input type="text"/>	
Exchange proxy port	<input type="text"/>	
Test Email Address (e.g. user@example.com)	<input type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Validate Exchange Service Configuration"/>		

Note:

- Test email address is required for MS Exchange 2013 for validation purpose only.
- It is not possible to execute the batch file by placing it on the desktop.
- Please make sure that the batch file is not stored on the desktop.
- Save the file on any local drives, for example C drive. To download the file, right click on the link below and select "Save Link As...".

[Download Powershell script](#)

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**.

3.8.6 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](#) again afterwards.

To disable Admin console in a Linux platform:

1. Login as 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`

To disable Admin console in a Windows platform:

1. Go to command prompt.
2. Go to the directory where one-X Portal for IP Office is installed, for example `cd C:\Program Files\Avaya\oneXportal`.
- **Note:** The installation path will be different on a 32-bit and 64-bit installation
3. Enter `cd \openfire\bin`
4. At the command prompt, type: `AdminConsoleManager.bat enable`
5. Restart Avaya one-X Portal.

3.8.7 Enabling IM archiving

To enable IM archiving settings in XMPP Server:

1. [Enable the XMPP admin console](#)^[68].
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](#)^[70].

3.8.8 Disabling IM archiving

To disable IM archiving:

1. Open the XMPP Server in the browser, type: *http://<server IP address>:9094*
2. Login to XMPP Server with the following default credentials:
 - Username: admin
 - Password: admin
3. Click **Server** tab.
4. Click **Archiving** tab.
5. In the left panel select **Archiving Settings**.
6. Disable the following check boxes:
 - **Conversation State Archiving**
 - **Archive one-to-one chats**
 - **Archive group chats**
7. Click **Update Settings** button. The system saves the settings and displays the following message: *Archive Settings have been saved.*

3.8.9 Disabling the XMPP Admin Console

To disable Admin console in a Linux platform:

1. Login as 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`

To disable Admin console in a Windows platform:

1. Go to command prompt.
2. Go to the directory where one-X Portal for IP Office is installed, for example `cd C:\Program Files\Avaya\oneXportal`.
 - **Note:** The installation path will be different on a 32-bit and 64-bit installation
3. Enter `cd \openfire\bin`
4. At the command prompt, type: `AdminConsoleManager.bat disable`
5. Restart Avaya one-X Portal.

3.9 Conferences

The portal can include a component that provides support for conferencing functions, those being conference scheduling and web collaboration sessions in parallel with conferences.

3.9.1 Viewing Conferences

This menu allows you see details of any 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).

Host	User Name	Extension	Join Time	Leave Time
Peter Power				
	Peter Power	239	Jul 23, 2014 4:19 PM	
	Gary Guest	5555555	Jul 23, 2014 4:22 PM	
Lync01(230)				
	Lync01	230	Jul 23, 2014 4:20 PM	
	Getrude Guest	6666666	Jul 23, 2014 4:23 PM	

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.

3.9.2 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.

- **Conference ID**

To delete a conference requires the conference ID.

To delete a scheduled conference:

1. Click **Diagnostics** and select **Call/Conference Scheduling**.
2. Enter the ID of the future conference to delete from the scheduled conferences.
3. Click **Delete**.

3.9.3 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, web collaboration URL). It can also include the fixed text set through the **Conference Dial-in** menu.

The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes 'Health' and 'Configuration'. Under 'Configuration', there are links for 'Providers', 'Users', 'CSV', 'Branding', 'IM/Presence', 'Exchange service', 'Conference Dial-in', and 'SMTP Configuration'. The main content area has a tree view with expandable items: 'Providers', 'Users', 'CSV', 'Branding', 'IM/Presence Server', 'IM/Presence Exchange Service', and 'Conference Dial-in Information'. The 'Conference Dial-in Information' item is expanded, showing a text box with the following text: 'To access conferences, dial 01555 220637 if external or 637 if internal, and follow the spoken prompts.' Below the text box is a 'Dial-in' label and a 'Save' button.

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**.

3.9.4 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.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▶ IM/Presence Exchange Service
IM/Presence	▶ Conference Dial-in Information
Exchange service	▼ SMTP Configuration
Conference Dial-in	Following SMTP configuration will be used to send emails for conference scheduling feature
SMTP Configuration	Server Address <input type="text"/>
Conference Clean Up	Port number <input type="text" value="25"/> *Default SMTP Port is 25
Auto Provisioning	Email From Address <input type="text"/>
Security	Use STARTTLS <input type="checkbox"/>
Diagnostics	● Server Requires Authentication <input type="checkbox"/>
Directory Integration	User Name <input type="text"/>
Gadgets Configuration	Password <input type="text"/>
IM Archive	<input type="button" value="Save"/>
Web Conferences	
Help & Support	

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 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. Enter the fixed text that should be included in all conference notifications.
4. Click **Save**.

3.10 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**.

The screenshot shows the 'Logging Configuration' page. On the left, a navigation menu has 'Diagnostics' selected, with 'Logging Configuration' as a sub-link. The main content area is titled 'Logging Configuration' and contains several sections:

- Logging Configuration** (expanded):
 - Master Logging Level**: Set the threshold above which logging events are sent to logging targets. Choose ALL for 'log everything', choose OFF to 'disable logging'. A dropdown menu is set to 'ALL'.
 - Logging Targets (Rolling Log Files)**: Rolling log files grow to a max. 10 MB, then a new one is started. The oldest rolling log is removed when the max. of 5 is reached. Rolling log files reflect the master logging level. Below this is a table of logging targets:

Enabled	Name	Level	File Path
<input checked="" type="checkbox"/>	Overall	ALL	../logs/1XOverallRollingFile.log
<input checked="" type="checkbox"/>	Presentation Layer	ALL	../logs/1XPresentationLayerRollingFile.log
<input checked="" type="checkbox"/>	Mid-Layer	ALL	../logs/1XMidLayerRollingFile.log
<input checked="" type="checkbox"/>	Telephony (CSTA)	ALL	../logs/1XCSTAServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (IP-Office)	ALL	../logs/1XIPODirServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (LDAP)	ALL	../logs/1XLDAPDirServiceRollingFile.log

- Logging Targets (Server and Network)**:
 - Socket Receiver (required for remote log viewing)**: Enabled

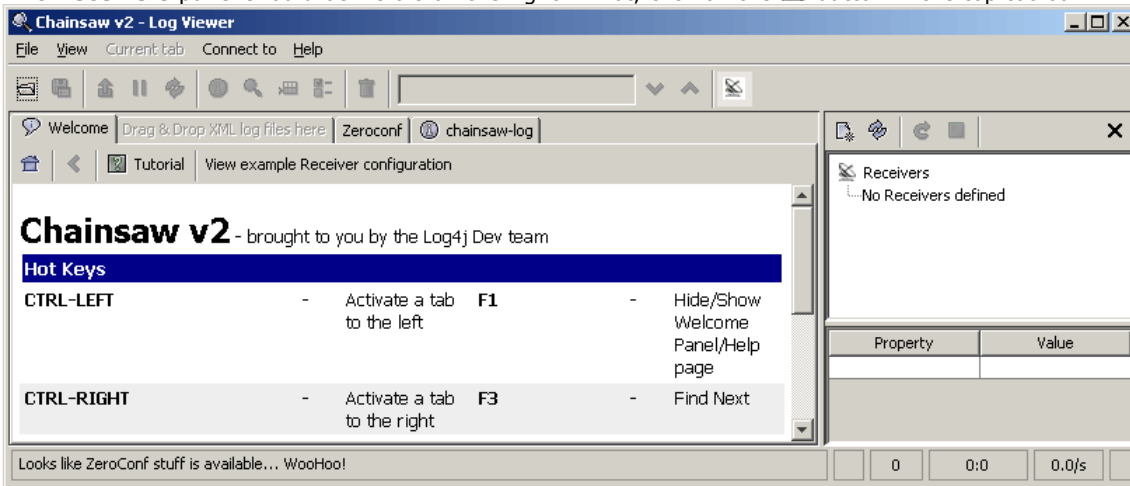
2. Select **Logging Targets** and check that **Socket Receiver** is enabled.
3. Select **Logging Viewer**.


The screenshot shows the 'Logging Viewer' page. On the left, a navigation menu has 'Diagnostics' selected, with 'Logging Viewer' as a sub-link. The main content area is titled 'Logging Viewer' and contains:

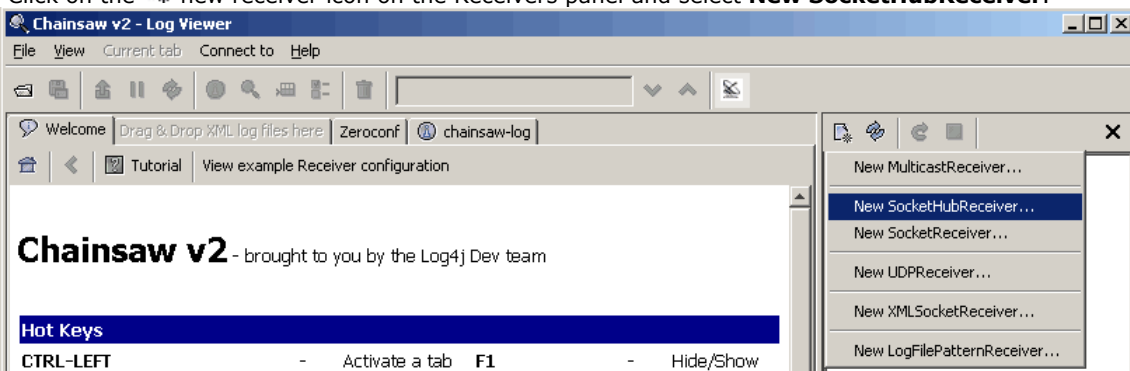
- Logging Viewer** (expanded):
 - Description: Remotely viewing logs.
 - More information about Apache Chainsaw.
 - Start Installation of Apache Chainsaw by Java Web Start
 - Network Routes (Not for IP Offices)
 - IP Office Connections
 - Database Integrity
 - User Data Validation

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**.

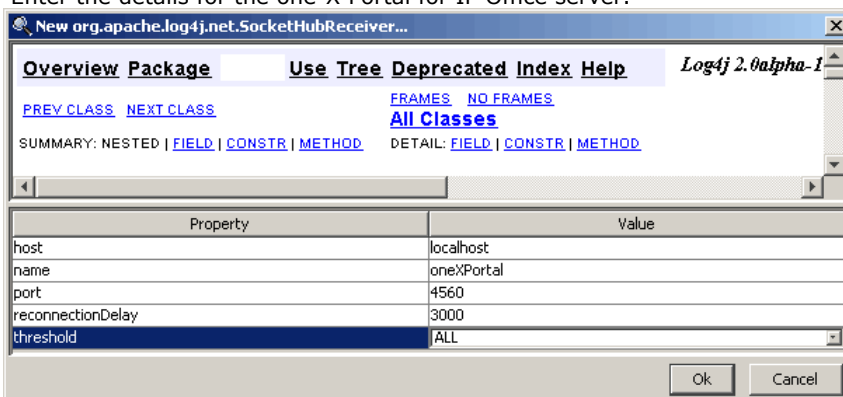
6. The **Receivers** panel should be visible on the right. If not, click on the  button in the top toolbar.



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

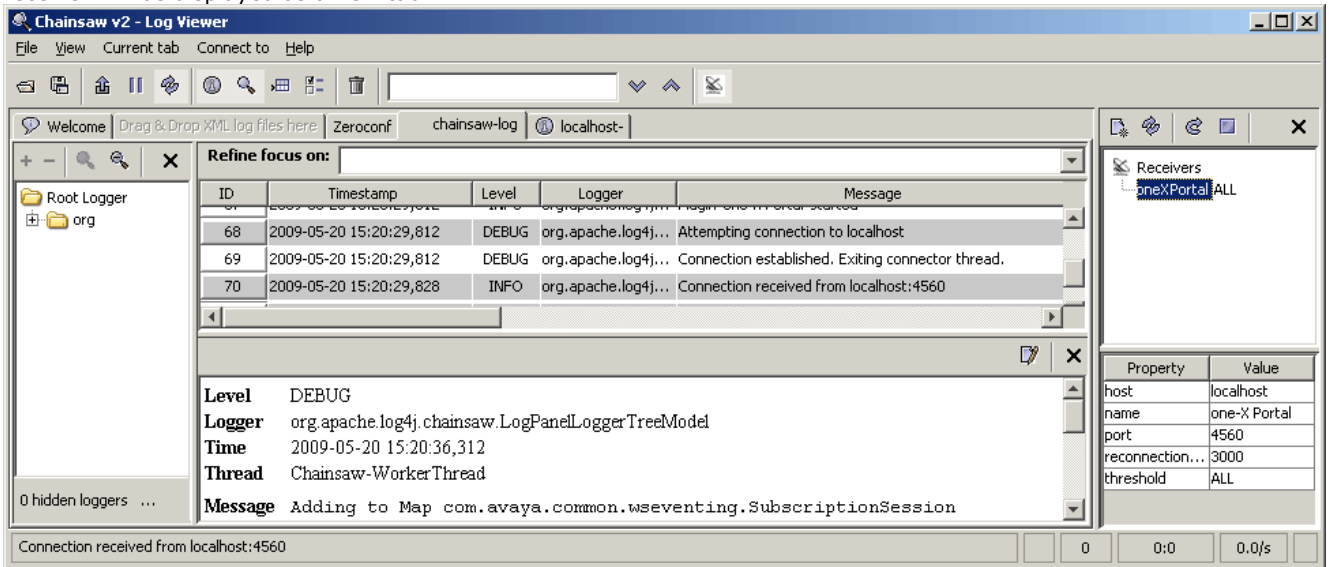


8. Enter the details for the one-X Portal for IP Office server.

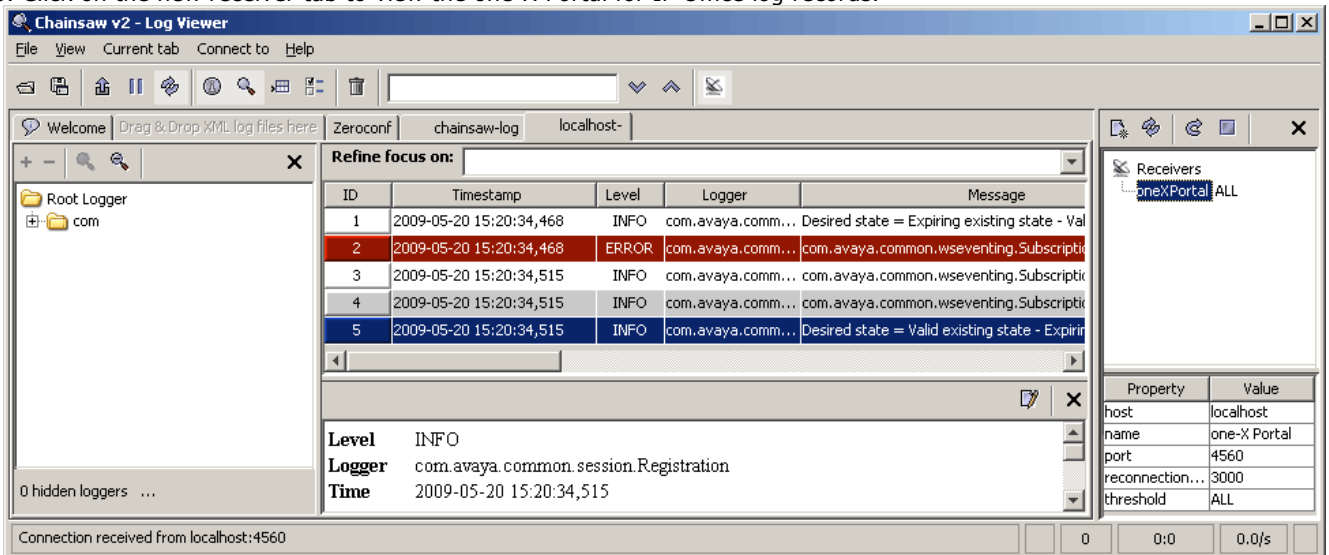


host	This field sets the address of the one-X Portal for IP Office server. In the example above chainsaw is being run on the one-X Portal for IP Office server PC.
name	This field is for display only. Enter a name for the receiver entry in Chainsaw.
port	Set this to 4560. This is the port to which one-X 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.

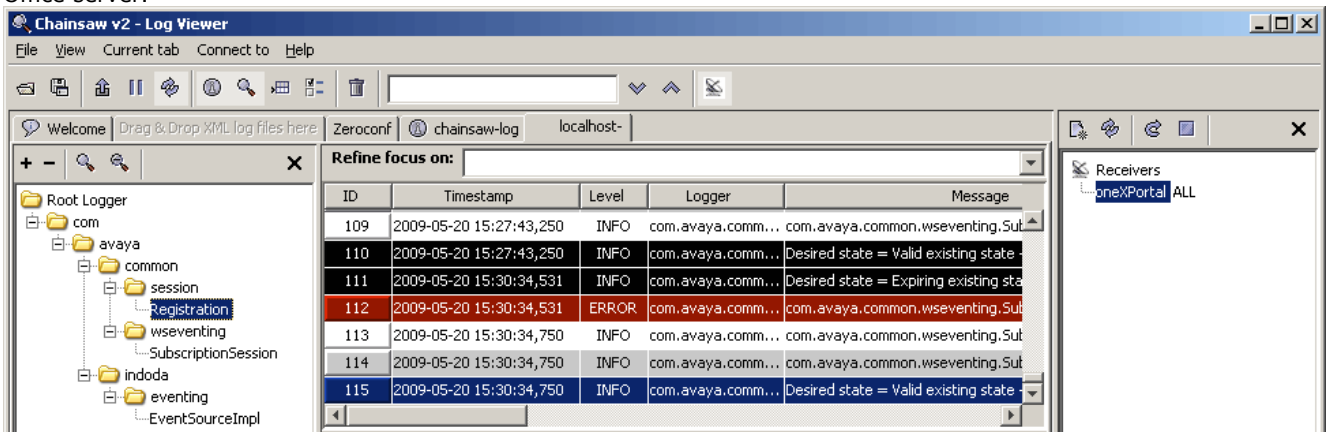
- When you have completed the fields, click OK. After a few seconds the receiver should start and connect to the one-X Portal for IP Office server. The process will appear as log events on the chainsaw-log tab and when completed the receiver will be displayed as a new tab.





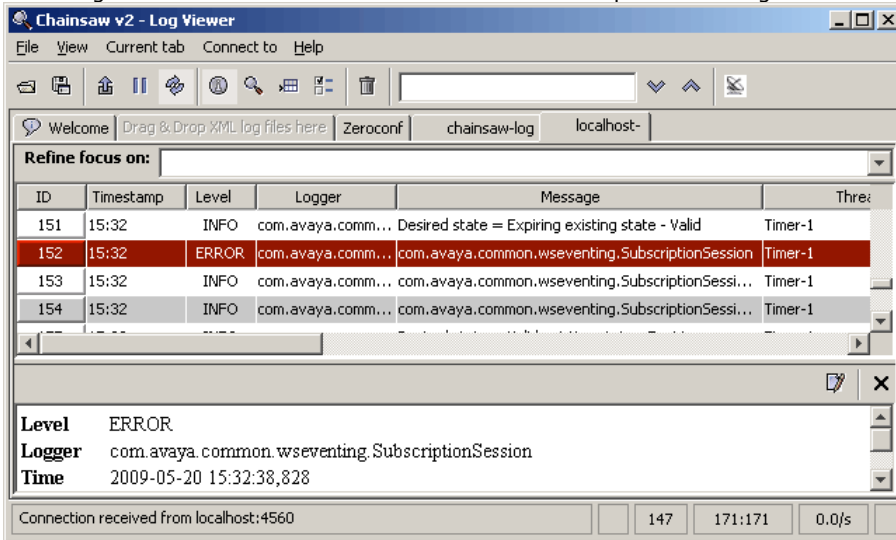
- Click on the new receiver tab to view the one-X Portal for IP Office log records.



- 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.



3.11 Troubleshooting

Version Mismatch Problem

Symptoms	<ul style="list-style-type: none">• Database integrity ^[33] check fails.• When starting one-X Portal for IP Office, the version shown on the login page is the previous version and differs from that reported by Windows (Start Programs IP Office Avaya one-X Portal for IP Office Uninstall VX.XX) menu.
Cause	Normally the one-X Portal for IP Office installer will automatically stop any Tomcat web server associated with a previous installation of one-X Portal for IP Office. However it has been found that it in some cases it fails to stop the Tomcat server but will still report successful completion of the installation process. This leads to a version mismatch between components.
Resolution	<ol style="list-style-type: none">1. Remove one-X Portal for IP Office ^[63].2. Manually delete the one-X Portal for IP Office application folder (by default C:\Program Files\Avaya\oneXportal). You need to reboot the server if the folder is reported as locked.3. Install the new version of one-X Portal for IP Office.

one-X Portal for IP Office Does Not Start

Symptoms	<ul style="list-style-type: none">• one-X Portal for IP Office fails to start.• Prorun Error appears in the Tomcat server log files.• Other Java applications fail to run on the server (for example the IP Office System Status Application).
Resolution	<ol style="list-style-type: none">1. Check for a port conflict. If one exists either remove the other application or install one-X Portal for IP Office using a different port.2. Using the Windows Add or Remove Programs applet, remove Java.3. Remove one-X Portal for IP Office ^[63].4. Install one-X Portal for IP Office.

3.12 Migrating from Phone Manager to one-X Portal for IP Office

With a Avaya Phone Manager Pro (per seat) license, you can migrate to one-X Portal for IP Office 8.0 or later and activate the Office Worker user profile to start using one-X Portal for IP Office. With one-X Portal for IP Office, you can use all the Phone Manager features except PC softphone.

To migrate from Phone Manager Pro to one-X Portal for IP Office:

1. Open IP Office Manager and log in as Administrator.
2. In the navigation pane, select the system to which you want to add the PhoneManager license.
3. In the navigation pane, right-click **License** and click **New**.
4. In the right pane, enter the Phone Manager Pro (per seat) license and click **OK**.
5. Under System, right-click **User** and click **New**.
6. In the **User** tab, enter the appropriate user information in the fields. For information on configuring a user, see the *IP Office Manager* user guide available at the Avaya support website www.support.avaya.com.
7. From the **Profile** list, select **Office Worker User**.
8. Click **Enable one-X Portal** and other options appropriately.
9. Click **OK**. You can log into one-X Portal for IP Office using the new user credentials created and start using one-X Portal for IP Office. For more information on licenses, see the IP Office Product Description on the Avaya support website www.support.avaya.com.



3.13 Adding Additional Administrators

By default, Linux based one-X Portal for IP Office servers use **Referred Authentication**. That means that the portal administration rights are assigned to security users configured in the security configuration of the IP Office service running on the same server. By default that is the **Administrator** user, however additional service users can also be configured for portal administrator access. If referred authentication is disabled, the portal uses its own local administrator account in the same as for a Windows based server as below.


Windows based servers use a local **Administrator** account stored in the portal's own settings (or **Superuser** for the AFA menus). The default password is changed by the installer as part of the installation process.

The process below illustrates how to configured portal administration rights for additional security 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.

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**

For portal being run on a Linux based server, the portal can be included in the backup and restore functions provided through the Linux 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 as the Superuser at any time.

By default, Linux based one-X Portal for IP Office servers use **Referred Authentication**. That means that the portal administration rights are assigned to security users configured in the security configuration of the IP Office service running on the same server. By default that is the **Administrator** user, however additional service users can also be configured for portal administrator access. If referred authentication is disabled, the portal uses its own local administrator account in the same as for a Windows based server as below.

Windows based servers use a local **Administrator** account stored in the portal's own settings (or **Superuser** for the AFA menus). The default password is changed by the installer as part of the installation process.

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 will be either **9443** or **8443** for HTTPS access.
- You can use ***http://*** rather than ***https://*** and **8080** as the port if unsecure access has been configured. See [Protocol](#)^[29].
- Alternatively, from the normal user login menu, select **AFA Login**.

2. At the login menu, enter the password:

- On a Linux based server, enter the password of an IP Office security user [configured for one-X Portal Super User](#)^[79] access. By default that is the **Administrator** user.
- On a Windows based server, enter the name **Superuser** and enter the associated password.
 - 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.

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.

System Status View Configurator DB Operations	System status		
	Last Backup Taken		
	Backup Name	File Size in Bytes	Backup Date Time
	OneX-DB-Bkp	29882	2010-08-03-11.33.25
Last Restore Done			
Backup Name	File Size in Bytes	Restore Date Time	
OneX-DB-Bkp-2010-08-03-	29898	2010-08-03-11.38.32	
<input type="button" value="Undo Last Restore"/>			
Local Server Total Space			
149	GB		
Local Server Free Space			
91	GB		

- **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.

The screenshot shows a web interface for configuring the Superuser. On the left is a navigation menu with 'System Status', 'Configuration', 'DB Operations', and an 'Edit' link. The main area is titled 'Edit' and contains four input fields: 'Super User Name' (pre-filled with 'Superuser'), 'Display Name' (pre-filled with 'aditya'), 'Password' (masked with three dots), and 'Confirm Password' (masked with three dots). At the bottom are 'Save' and 'Clear' buttons.

- **Super User Name**
This is a fixed name and cannot be changed. It is the name used for the login.
- **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.

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.

System Status

Configuration

DB Operations

Backup

Restore

Backup

Backup Name

Note: Server timestamp at time of taking backup will be appended to the backup name, e.g. OneX-DB-Bkp-2010-01-18-12.50.24.zip

Backup To

Local Server FTP Local Drive

Server IP Address

Port

User Name Password

Backup

- **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

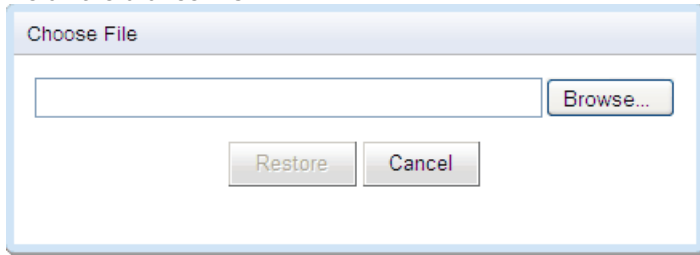
This menu is used to select a previous backup file and then use that file for a restore operation. Before the restoration occurs, a backup of the current configuration is made and stored in the **Backup Folder** for use with the **Undo Last Restore** control. Restoration is only supported from a backup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

Select	Backup Folder	Backup Name	File Size in Bytes	Backup Date Time
<input type="radio"/>	C:\Backups	OneX-DB-Bkp-2010-08-03-11.32.55.zip	29898	Tue Aug 03 19:32:55 GMT+100 2010
<input type="radio"/>	C:\Backups	OneX-DB-Bkp-2010-08-03-11.33.25.zip	29882	Tue Aug 03 19:33:25 GMT+100 2010
<input type="radio"/>	C:\Backups	OneX-DB-Bkp-2010-08-03-11.45.58.zip	29866	Tue Aug 03 19:45:59 GMT+100 2010

- **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.

Document History

5. Document History

Date	Issue	Change Summary
30th October 2014	10b	<ul style="list-style-type: none"> Update for IP Office Release 9.1
24th November 2014	10c	<ul style="list-style-type: none"> Correct document title.
16th April 2015	10d	<ul style="list-style-type: none"> Correct appearance of old Avaya Communicator product name.
7th May 2015	10e	<ul style="list-style-type: none"> Note added regarding the lack in 9.1 of a default XMPP group. [84595] Certificate menu was incorrectly lists as a sub-menu of configuration. Moved to Security. [87017]
26th November 2015	10f	<ul style="list-style-type: none"> Removed the errant 'Draft' label from previous issue. Advice of cause of new IP Office user not appearing in portal XMPP group [64], [102625] Clarification of difference between first time AFA login [81] for Linux or Windows server. [98969] Help page added for Security Certificate [30] menu. [98228]
4th December 2015	10g	<ul style="list-style-type: none"> Replace errant <<<Link>>> marking with actual link.
7th December 2015	10h	<ul style="list-style-type: none"> Correct font size icon issue in online help.
8th December 2015	10i	<ul style="list-style-type: none"> Refresh of Openfire console instruction (link using console to enabling console).
5th January 2016	10j	<ul style="list-style-type: none"> Update to the notes on how Referred Authentication is used on Linux based servers.
14th January 2016	10k	<ul style="list-style-type: none"> Description of XMPP groups and their usage added. [102625]

Index

4

4560 74

A

About 10

Active Sessions 10, 13

Add

Gadget 54

IP Office 45

LDAP 58

User 56

Administrator

Help 42

Name 7

Anyone can connect. 65

Apache

Chainsaw 32, 74

Archive

IM Sessions 64

Assign

IP Office 45, 48

IP Office (CSTA) 16

IP Office (Directory) 17

LDAP Provider 18

Providers 15

Voicemail provider 19

Audio conference 41

Automatic logout 7

Avaya Support 10

B

Backups 10

Base DN 58

Branding 22

Bulk Edit 21, 56

User 56

C

Calendar 24, 67

Call Log 56

Chainsaw 32, 74

Component Status 10, 12

Conference 41

Configuration 10

Branding 22

Bulk Edit 56

CSV 22

Export 22

IM 65

Presence 65

Providers 15

Users 21

Control Panel 63

CSTA 16

CSTA (IP Office) Provider 16

CSV 10, 22

D

Data validation 34

Database

Check 33

Sanity Check 33

Database Integrity 10

Deinstall 63

Delete

Gadget 55

IP Office 48

User 56

Diagnostics 10

Connections 33

Database Integrity 33

IP Office Connections 33

Logging Configuration 30, 74

Logging Viewer 32, 74

Network Routes 32

Directory

Export 22

Resynch 36, 60

Directory (DSML IP Office) 17

Directory (DSML LDAP) 18

Directory Integration 10

Directory Synchronization 36, 60

Directory Intergration

LDAP 36, 59

System Directory 37, 60

Directory Search

LDAP 36, 59

System Directory 37, 60

Directory Synchronization 10

Disconnect on Idle. 65

DND Exceptions 56

Domain name

XMPP domain name 65

Downgrading 62

DSML (IP Office) Provider 17

DSML (LDAP) Provider 18

E

Echo 32

Edit

Bulk Edit 56

Gadget 54

IP Office settings 48

User settings 21, 56

Enable

External gadget 55

Environment 10

Events 13

Exceptions 56

Exchange 24, 67

Export

Gadgets 39, 53

Export Configuration 22

exportDirectoryEntry.csv 22

exportUser.csv 22

External Directory

Search 36, 59

F

Field Mapping 18, 58

Force a Resynchronization 36, 60

G

Gadget

Delete 55

Disable 55

Edit 54

Enable 55

Export 39, 53

Import 51

URL 50

Gadgets

List external gadgets 38

H

Health 10

- Health 10
 - Active Sessions 13
 - Component Status 12
 - Environment 14
 - Key Recent Events 13
- Help 10
 - About 42
 - Avaya Support 42
 - Help 42
- I**
- Idle timeout. 65
- IM**
 - Archiving 64
 - Configuration 65
 - Search sessions 40, 66
 - Status 66
- Immediate logout 7
- Import
 - Gadgets 51
- IP Office
 - Connections 10
 - CSTA Provider 16
 - Directory Provider 17
- J**
- Java Web Start 74
- K**
- Key Recent Events 10, 13
- Keyboard Shortcuts 56
- L**
- LDAP 59
 - Assign 58
 - Directory Search 10, 36, 59
 - Provider 18
- Log Files 30
- Log4j format 74
- Logging 74
 - Configuration 10
 - Level 30
 - Targets 30
 - Viewer 10, 74
- Logging Configuration 74
- Login 7
- Logout 7
- M**
- Master Logging Level 30
- Messages 56
- Monitor 41
- N**
- Network Routes 10, 32
- Not Reachable 32
- O**
- Override Admin Session 7
- P**
- Park Slots 56
- Participants 41
- Password 7
- Personal Directory 56
- PING 32
- Port
 - 4560 74
 - 7 32
- Presence 56
 - Configuration 65
- Exchange 24, 67
 - Status 66
- Provider 10
 - Assign 15
 - CSTA (IP Office) 16
 - Directory (DSML IP Office) 17
 - Directory (DSML LDAP) 18
 - DSML (IP Office) 17
 - DSML (LDAP) 18
 - View 15
 - Voicemail 19
- R**
- Reachable 32
- Recent Events 13
- Remote Logging 74
- Remove
 - IP Office 48
 - one-X Portal for IP Office 63
 - User 56
- Reset Session Count 7
- Restart Service 44
- Resynchronization 36, 60
- Rolling Log Files 30
- Routes 32
- S**
- Sanity 33
- Search
 - IM sessions 40, 66
 - LDAP 36, 59
 - System Directory 37, 60
- Search Base 58
- Server
 - Information 14
 - Version 14
- Service
 - Restart 44
- Sessions 13
- Settings
 - Bulk Edit 56
- Shortcuts 56
- Socket Receiver 30, 74
- Start Service 44
- Status
 - Component 12
 - IM 66
 - Presence 66
- Synchronization 36, 60
- System Directory 10
 - Directory Search 37, 60
 - Export 22
 - Resynch 36, 60
- T**
- TCP Port 7 32
- Test
 - External Directory 36, 59
 - IP Office connection 33
 - LDAP Directory 36, 59
 - Network Route 32
 - System Directory 37, 60
- U**
- Uninstall 63
- Upgrading 61
- User
 - Add 56
 - Bult Edit 56

User

- Data validation 34
- Delete 56
- Edit settings 56
- Export 22
- Help 42

Users 10

- Active 13
- Edit settings 21
- Resynch 36, 60
- View 21

V**Version 14****View**

- Component Status 12
- Conference 41
- Key Recent Events 13
- Providers 15

Voicemail

- Provider 19

Voicemail Messages 56**W****Web conference 41****X****XMPP domain name 65**

