



IP Office 9.0.3

Administering 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: <http://www.avaya.com/support> 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://SUPPORT.AVAYA.COM/LICENSEINFO), 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 Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, 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.

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

Shrinkwrap License (SR). 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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

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 Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: <http://support.avaya.com>, or such successor site as designated by Avaya.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <http://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: <http://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. Administration

1.1 Log in	8
1.2 Log out	9
1.3 Health	10
1.3.1 Component Status.....	10
1.3.2 IM/Presence server status.....	11
1.3.3 Key Recent Events.....	11
1.3.4 Active Sessions.....	12
1.3.5 Environment.....	12
1.4 Configuration.....	13
1.4.1 Providers.....	13
1.4.2 Users.....	18
1.4.3 CSV.....	20
1.4.4 Branding.....	21
1.4.5 IM/Presence.....	22
1.4.6 Exchange service.....	23
1.5 Diagnostics.....	24
1.5.1 Logging Configuration.....	24
1.5.2 Logging Viewer.....	26
1.5.3 Network Routes.....	26
1.5.4 IP Office Connections.....	27
1.5.5 Database Integrity.....	27
1.5.6 User Data Validation.....	28
1.6 Directory Integration.....	29
1.6.1 Directory Synchronisation.....	29
1.6.2 System Directory.....	30
1.6.3 LDAP Directory Search.....	30
1.7 Gadget configuration.....	32
1.7.1 External gadget list.....	32
1.8 IM Archive.....	39
1.8.1 Searching for IM conversations in the archive....	39
1.8.2 Enable/Disable IM Archive.....	39
1.9 Help & Support.....	41

2. Maintenance

2.1 Preferred Edition License.....	44
2.2 Manually Starting the Service.....	44
2.3 Adding an Additional IP Office.....	45
2.4 Changing IP Office Details.....	48
2.5 Adding an LDAP External Directory Source.....	50
2.6 Adding/Deleting Users.....	51
2.7 Editing User Settings	51
2.8 Checking and Updating the System Directory.....	54
2.9 Checking the External LDAP Directory.....	55
2.10 Upgrading one-X Portal for IP Office	56
2.11 Downgrading one-X Portal for IP Office.....	57
2.12 Removing one-X Portal for IP Office.....	58
2.13 Remote Logging.....	59
2.14 Troubleshooting.....	63
2.15 Agent Gadget Control.....	63
2.16 Enabling or Disabling Admin console of XMPP Server	64
2.16.1 Enabling Admin console of XMPP Server.....	64
2.16.2 Disabling Admin console of XMPP Server.....	65
2.17 Migrating from Phone Manager 7.0 to one-X Portal for IP Office 8.0.....	65

3. Backup/Restore

3.1 Superuser Log in.....	67
3.2 System Status.....	67
3.3 Configuration.....	68
3.4 DB Operations.....	69
3.4.1 Backup.....	69
3.4.2 Restore.....	70

4. Glossary

5. Document History

Index	76
-------------	----

Chapter 1.

Administration

1. Administration

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 	List the last status change of the server components.
	Key Recent Events 	View the last 20 events on the server.
	Active Sessions 	Show how many sessions are cached by one-X Portal for IP Office.
	Environment 	Show a summary of the one-X Portal for IP Office server PC.
Configuration 	Providers 	View and edit the providers.
	Users 	View and edit user one-X Portal for IP Office settings.
	CSV 	Export the user directory and system directory.
	Branding 	Specify the text that is displayed on the one-X Portal for IP Office pages after a user has logged in.
	IM/Presence 	Monitor the status of the IM/Presence server as a Administrator.
	Exchange service 	Configure the Exchange server to avail the calendar mining and presence information of the users.
Diagnostics 	Logging Configuration 	Configure the level and method of logging supported.
	Logging Viewer 	Install and launch Chainsaw for log viewing.
	Network Routes 	Test the IP connection path to an IP address.
	IP Office Connections 	Test the IP connection path to an IP Office.
	Database Integrity 	Test the structure of the database.
	User Data Validation 	Identify possible cause of user login failure or user data corruption and reset the corrupt data.
Directory Integration 	Directory Synchronization 	Force a system directory update by the server.
	System Directory 	View the one-X Portal for IP Office system directory.
	LDAP Directory Search 	View the external directory for which the one-X Portal for IP Office server has been configured.
Gadgets Configuration 	External Gadgets List 	The external gadgets that are in the system are listed.
	Import External Gadgets 	Import external gadgets.
	Export External Gadgets 	Export external gadgets.
IM Archive 	Search Archive 	Search for the IM conversations between the system contacts.
Help & Support 	Help 	Access one-X Portal for IP Office help installed on the server.
	Avaya Support 	Access the Avaya support web site for Avaya applications.
	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   icon next to Description can be used to show/hide a short description of the menus function and content.

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. If the one-X Portal for IP Office server already has an administrator connection in progress, it will display a warning.

1. Browse to **http://<server name>:<server port>/onexportal-admin.html**, where *<server name>* is the name or the IP address of the server, and *<server port>* is the port number selected during one-X Portal for IP Office software installation (the default is 8080). The one-X Portal for IP Office login menu appears.

Note: one-X Portal for IP Office 8.1 continues to support the URL **http://<server name>:<server port>/inyama/inyama.html?admin=true**

2. Enter the one-X Portal for IP Office administrator name and password as configured during installation.
3. If there is already a session connected as an administrator, the following confirmation message box appears:



4. Do one of the following:
 - To end the session of the logged in administrator and log in with your administrator credentials, click **Yes** in the confirmation message.
 - To login later without disrupting the current administrator session, click **No** in the confirmation message.

one-X Portal for IP Office 8.1 supports **English(US and UK), French, German, Italian, Dutch, Brazilian Portuguese, Latin Spanish, Russian** and **Simplified Chinese**. You can set the language in the login page as an **Administrator** or as a **User**. Set the language only when you are accessing the one X portal for the first time on a browser. To set the language of your preference do the following:

1. Log in as an Administrator.
2. Choose the language listed under **Language**.
3. Click **Login**.

Note: The language that you set is applicable only to the one X Portal. This setting does not affect the language of other websites that you access using the browser.

one-X Portal for IP Office displays the Change Administrator Default Password window.

4. Do one of the following:

- To change the default administrator password assigned to you, type your password in **New Password** and re-type your password in **Confirm New Password**, and then click **Change password**. The Change password button enables only when the passwords you type match.

Change Administrator Default Password

You should change the password from its default value.

New Password:

Confirm New Password:

Passwords match.

Password strength not enforced.

Change password

Skip this time

- If you do not want to change the administrator password assigned to you, click **Skip this time**. However, the Change Administrator Default Password window appears every time you log into one-X Portal for IP Office until you change the assigned administrator password.

Change Administrator Default Password

You should change the password from its default value.

New Password:

Confirm New Password:

Passwords match.

Password strength not enforced.

Change password

Skip this time

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.

Automatic Logout upon Inactivity

Your session appears to have been inactive for 10 minutes.

You will be automatically logged out in 30 seconds.

Activity is determined by transfers to & from the one-X Portal Server.

Merely navigating the administration user interface is not deemed to be activity

Stop Automatic Logout & Continue

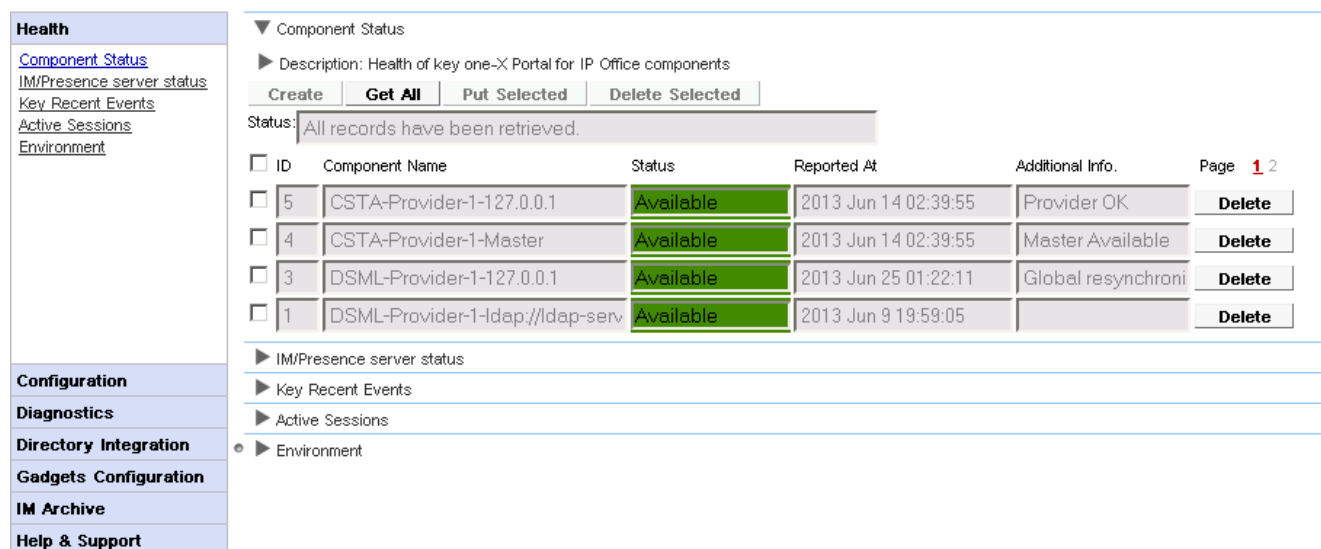
Logout Immediately

1.3 Health

1.3.1 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](#)

Configuration

Diagnostics

Directory Integration

Gadgets Configuration

IM Archive

Help & Support

▼ 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
☐	5	CSTA-Provider-1-127.0.0.1	Available	2013 Jun 14 02:39:55	Provider OK	Delete
☐	4	CSTA-Provider-1-Master	Available	2013 Jun 14 02:39:55	Master Available	Delete
☐	3	DSML-Provider-1-127.0.0.1	Available	2013 Jun 25 01:22:11	Global resynchroni	Delete
☐	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

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.

1.3.2 IM/Presence server status

You can monitor the status of the IM/Presence server as a Administrator.

IM/Presence server status	Description
Available	The system displays the XMPP presence status of all the users.
Failed	The system does not display the XMPP presence status of all the users.
Starting	The system is starting the component.

Procedure:

To start IM/Presence server when it is non-functional:

1. Select **Health**.

2. Select **IM/Presence server status**.

The system displays the status of the IM/Presence server.

3. Click **Start**.

Note: If the database is corrupt then, the system displays a message that reads: *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 backup the database every eight hours.

Note: You can not start the IM/presence server without restoring the corrupt database. If you click **No**. The system displays a warning message that reads: *IM/Presence server can not be started with corrupted database. The IM/Presence features will be unavailable.*

Result:

The system restarts the IM/Presence server.

1.3.3 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.

The screenshot shows the 'Health' section with a sidebar containing links: Component Status, Key Recent Events (selected), Active Sessions, and Environment. The main content area is titled 'Component Status' and 'Key Recent Events'. Below the title, there are buttons: Create, Get All, Put Selected, and Delete Selected. A status bar indicates 'All records have been fetched.' Below this is a table with the following data:

ID	What Happened?	Significance	When	Additional Info.	Page 1 2
☐ 1	Administrator	Low	2009-08-03 13:35:53.328	Administrator logged in	Delete
☐ 2	Installation	Medium	2009-08-03 13:45:41.078	DSML Provider is re	Delete
☐ 3	Password Changed	Medium	2009-08-03 13:46:15.812	Administrator passw	Delete
☐ 4	Administrator	Low	2009-08-03 14:11:00.906	Administrator logged	Delete

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.

1.3.4 Active Sessions

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

The screenshot shows the 'Health' menu on the left with options: Component Status, Key Recent Events, Active Sessions (selected), and Environment. The main content area shows 'Component Status', 'Key Recent Events', and 'Active Sessions'. Under 'Active Sessions', there is a description 'Description: one-X Portal for IP Office Utilisation', a 'Refresh' button, and a table with session counts.

Total	User	Administrator	Application
3	0	1	2

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

1.3.5 Environment

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

The screenshot shows the 'Health' menu on the left with options: Component Status, IM/Presence server status, Key Recent Events, Active Sessions, and Environment (selected). The main content area shows 'Component Status', 'IM/Presence server status', 'Key Recent Events', 'Active Sessions', and 'Environment'. Under 'Environment', there is a description 'Description: Server Information', a 'Refresh' button, and a table with system information.

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]

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

1.4 Configuration

1.4.1 Providers

This menu shows the service providers configured on the one-X Portal for IP Office server.

Health

Configuration

[Providers](#)

[Users](#)

[CSV](#)

[Branding](#)

[IM/Presence](#)

[Exchange service](#)

▼ Providers

► Description: Configure providers of services to applications

Get All **Put Selected** **Delete Selected**

Status: All records have been retrieved.

☐ ID	Name		Page 1 2
☐ 4	Default-CSTA-Provider	Edit Delete	
☐ 2	Default-DSML-IPO-Prov	Edit Delete	
☐ 3	Default-DSML-LDAP-Pr	Edit Delete	
☐ 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.

1.4.1.1 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: 3

Name: Default-CSTA-Provider

Data: <?xml version="1.0" enco

Provider Type Selector: Telephony (CSTA)

IP Office(s) Assigned

Mid-Layer URL: tp://localhost:8080/inkaba

Mid-Layer Username: indoda_user

Mid-Layer Password:

Mid-Layer Password Hash: 7BDDEE71046BA3FA276

Run On Port: 8080

Created: 2009-05-08 13:41:33.6710

Close

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	
0	192.168.42.1			Delete

Close
Assign New IP Office Unit

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

1.4.1.2 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	3
Name	Default-CSTA-Provider
URL	tp://localhost:8080/indoda
Data	<?xml version="1.0" enco
Provider Type Selector	Directory Source (DSML IP-Office) ▼
	<div>IP Office(s) Assigned</div>
	Mid-Layer URL
	tp://localhost:8080/inkaba
	Mid-Layer Username
	indoda_user
	Mid-Layer Password
	
	Mid-Layer Password Hash
	7BDDEE71046BA3FA276
	Run On Port
	8080
Created	2009-05-08 13:41:33.6710

Close

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	
0	192.168.42.1			Delete

Close
Assign New IP Office Unit

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

1.4.1.3 DSML (LDAP) Provider

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

The screenshot shows the 'Provider Editor' window. It contains the following fields and values:

- ID:** 3
- Name:** Default-CSTA-Provider
- URL:** tp://localhost:8080/indoda
- Provider Type Selector:** Directory Source (DSML LDAP)
- LDAP Server(s) Assigned:** (button)
- Mid-Layer URL:** tp://localhost:8080/inkaba
- Mid-Layer Username:** indoda_user
- Mid-Layer Password:** (masked with dots)
- Mid-Layer Password Hash:** 7BDDEE71046BA3FA276
- Run On Port:** 8080
- Created:** 2009-05-08 13:41:33.6710
- Close:** (button)

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.

The screenshot shows the 'LDAP Server(s) assigned to Provider' window. It contains the following information:

- Header:** LDAP Server(s) assigned to Provider
- Description:** 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.
- Fields:**
 - ID:** 0
 - LDAP Server URL:** 192.168.42.12
 - User:** IPOffice
 - Password:** (masked with dots)
 - Base DN:** (empty)
- Buttons:** Edit Field Mapping, Delete, Close, Assign New LDAP Server

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.

The screenshot shows the 'LDAP Field Mappings' window. It contains the following mappings:

- FIRSTNAME:** givenName
- LASTNAME:** sn
- WORKPHONE:** telephoneNumber
- HOMEPHONE:** homePhone
- OTHERPHONE:** cel
- WORKEMAIL:** mail
- PERSONALEMAIL:** personalMail
- OTHEREMAIL:** otherMail
- Buttons:** Close, Defaults

1.4.1.4 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.

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

You can 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

6. Click the **Assign New Voicemail Server Unit** button to add a new row.

7. Enter the *ID* and *VoiceMail server IP Address*.

Note: Ensure that you enter the IP Address of the VoiceMail server because some of the functions such as playing messages using one-X Portal for IP Office browser client will not work if you leave the field blank.

8. Click **Close**.

9. 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.

1.4.2 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. You can not edit user settings stored in the IP Office.

Note: The maximum active user capacity on a primary server is 300 and on a dedicated server it is 750. Also, the maximum extension capacity is 1500.

1. Click **Configuration**, in the left navigation pane.
2. Click **Users**.
3. Click **Get All**.
4. Click **Edit** to edit the settings of the users. You can also select multiple users and then click **Bulk Edit** to edit several users at the same time. **Note:** You cannot edit the **Alternate IM ID** when you select **Bulk Edit**.
5. In the **User Configuration Type Selector** select the user settings that you want to edit. The options are **Screen Popping**, **Park Slots**, **Bridge Number**, and **IM/Presence Configuration**.
 - If you select **IM/Presence**, then you can set the various options for users such as **Send conference entry IM**, **Send conference exit IM**, **Voice message begin IM**, **Voice message end IM**, **Alternate IM ID**, **Advertise on call status**, and **Advertise calendar status**.
6. The **User Role Configuration** is currently used in conjunction with Customer Call Reporter. You can enter the name and password of a user set as **Manager** in the configuration of Customer Call Reporter. These details enable the Customer Call Reporter feature for forcing agent states.
7. After making the the changes click **Save**.
8. Click **Put Selected** to update the changes that you made to the user records in the one-X Portal for IP Office database.

Field	Options	Description
IM/Presence	Send conference entry IM	mybuddy sends an IM to you when someone joins your <i>MeetMe</i> conference.
	Send conference exit IM	mybuddy sends an IM to you when someone leaves your <i>MeetMe</i> conference.
	Voice message begin IM	mybuddy sends an IM to you when someone begins to leave a message in your voice mailbox.
	Voice message end IM	mybuddy sends an IM to you after someone leaves a message in your voice mailbox.
	Alternate IM ID	mybuddy sends the notifications about your Send conference entry IM , Send conference exit IM , Voice message begin IM , and Voice message end IM to the alternate IM ID that you set in this field. If IM server to server federation has been set up then this ID could be an external ID such as a Google Talk ID. In this way, you can get a notification on your google talk client. Notifications to the Alternate IM ID are in addition to notifications to mybuddy via the one-X Portal for IP Office.
	Advertise on call status	You can set the status of this field to reflect your call status: <ul style="list-style-type: none">• If you set the status of this field to Presence and Message, your presence will be changed to DND and your status message set to indicate you are on a call.• If you set the status of this field to Message Only, the system will update your status message to indicate you are on the phone. You cannot set or edit the <i>on the phone</i> status message.• If you set the status of this field to None, the system does not alter your status message or presence indicator while you are on the phone.
	Advertise calendar status	You can set the status of this field to reflect your calendar status: <ul style="list-style-type: none">• If you set the status of this field to Presence and Message, the system updates your status message to indicate you are in a meeting or at an appointment. Additionally, the system sets your presence to DND.• If you set the status of this field as Message Only, the system displays only your calendar message.

Field	Options	Description
		<ul style="list-style-type: none">If you set the status of this field to None, the system does not alter your status message or presence indicator while you are in a meeting or at an appointment.

If you think that the user records do not match the users configured on the IP Office systems, the [Directory Integration | Directory Synchronization](#)  menu can be used to force an update from the IP Office systems.

Note: The mybuddy command language is based on the language configured for a specific user by the administrator in IP Office Manager.

1.4.3 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.

Health	► Providers
Configuration	► Users
Providers	▼ CSV
Users	A control for exporting the user list and directory as a CSV file.
CSV	CSV import is not supported.
Branding	The exported filenames are hardcoded as exportUser.csv & exportDirectoryEntry.csv
IM/Presence	These get written to the underlying Tomcat/bin folder.
Exchange service	Export Configuration
	► Branding
	► IM/Presence Server
	► IM/Presence Exchange Service
Diagnostics	
Directory Integration	
Gadgets Configuration	
IM Archive	
Help & Support	

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**

1.4.4 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 'one-X Portal for IP Office' interface. On the left is a navigation menu with 'Health' and 'Configuration' sections. Under 'Configuration', there are links for 'Providers', 'Users', 'Backups', 'CSV', and 'Branding' (which is highlighted). The main content area shows the 'Branding' configuration. It includes a 'Refresh' button, a description: '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.', a text input field labeled 'Branding Name' containing 'one-X Server', and a 'Save' button.

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



1.4.5 IM/Presence

one-X Portal for IP Office can be configured for IM/Presence.

Before you begin

Note: XMPP accounts will not be created for users who have special characters (&,',<,>) in the user fields. Such users will not be able to use the IM/Presence features in all XMPP clients, including the one-X Portal for IP Office.

Extensible Messaging and Presence Protocol (XMPP) domain name: The XMPP domain name should be a domain name that the DNS can resolve. However, if you have not set a XMPP domain name that the DNS can resolve then you can use the IP address of the one-X Portal for IP Office server.

Note: You can set the [XMPP domain name](#)^[22] at any point in time. If you use the IP address then the one-X Portal for IP Office cannot federate with remote server such as Google Talk because the external servers will not be able to recognize the IP address of one-X Portal for IP Office.

To ensure that the IM/Presence server of one-X Portal for IP Office is configured to any remote XMPP server you have to set these configurations in one-X Portal for IP Office:

1. Enable **Server to Server Federation**.
2. To disconnect the Server to server configuration when the system is idle enable **Disconnect on Idle**.
3. To enable anyone to connect to the IM/Presence Server enable **Anyone can connect**.
4. Set the timeout time for the system in **Idle timeout**.
5. Set the XMPP domain name in **XMPP Domain Name**.
6. Click **Save**.

1.4.5.1 XMPP domain name configuration

As an administrator, you can specify sources of user lists, directories, and telephony services.

Configuring the XMPP domain name:

1. Select **Configuration > IM/Prsence**
2. In the **XMPP Domain Name**, set the XMPP domain name. By default, the value is *127.0.0.1*.

Note: You can change the value to *localhost*, *FQDN*, or *machine name*. The FQDN must be reachable from the internet if you wish to use the one-X Mobile application outside of your WLAN. Avaya recommends that you use a split DNS so that the server name outside of your WLAN is resolved into the public IP address of the NAT or firewall. The server name inside your network is resolved into the private IP address on the LAN.

Note: On Server Edition systems, UCM, and Application servers that are on a Linux platform, you must use the Web Control 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**.

1.4.5.2 Configuring IM/Presence Fedration with Google Talk

As an administration, you can configure one-X Portal for IP Office to federate with Google Talk and establish chat communication between Google Talk and one-X Portal for IP Office contact. To ensure that one-X Portal for IP Office is federated with Google Talk, set the following configurations:

1. To enable one-X Portal for IP Office federation with Google Talk server, set the **Port number** to 5269.
2. Set the fully qualified domain name of the Google Talk server. Ensure that the Google Talk server is accessible to one-X Portal for IP Office for communication.

1.4.6 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 .

Some of the settings that you need to configure as an Administrator of one-X Portal for IP Office are:

1. Click **Configuration**, in the left navigation pane.
2. Click **Exchange service**.
3. 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.
4. Type the password that was set for the **AvayaAdmin** in **Exchange service account password**.
5. Type the IP address of the exchange service host in **Exchange service Host**.
6. Type the port number of the exchange service in **Exchange Port number**.
7. Type the domain name of the proxy server that is used to connect to the exchange server in **Exchange service proxy host**.
8. Type the port number of the proxy server for exchange service in **Exchange proxy port**.
9. Click on **Validate Exchange Service Configuration** to view whether the provided exchange details are valid.
10. Click **Save**.

AVAYA one-X Portal for IP Office

Configuration

- Providers
- Users
- Backups
- CSV
- Branding
- IM/Presence Server
- IM/Presence Exchange Service

Exchange service account name: AvayaAdmin

Exchange service account password:

Exchange service Host:

Exchange Port number: 6669

Exchange service proxy host:

Exchange proxy port:

Save **Validate Exchange Service Configuration**

Note: 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. Locate the file under any main drive, for example it can be C drive. To download right click on below link and click "Save link As..".
[Download Powershell script](#)

Note: You can **Download Powershell script** to provide impersonation rights to the users.

1.5 Diagnostics

1.5.1 Logging Configuration

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

Enabled	Name	Level	File Path
☒	Overall	ALL	../logs/1XOverallRollingFile.log
☒	Presentation Layer	ALL	../logs/1XPresentationLayerRollingFile.log
☒	Mid-Layer	ALL	../logs/1XMidLayerRollingFile.log
☒	Telephony (CSTA)	ALL	../logs/1XCSTAServiceRollingFile.log
☒	Directory (IP-Office)	ALL	../logs/1XIPODirServiceRollingFile.log
☒	Directory (LDAP)	ALL	../logs/1XLDAPDirServiceRollingFile.log

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.

1.5.2 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](#)^[59] which is a suitable logging application .

Health	▶ Logging Configuration
Configuration	▼ Logging Viewer
Diagnostics	▶ Description: Remotely viewing logs.
Logging Configuration	More information about Apache Chainsaw.
Logging Viewer	Start Installation of Apache Chainsaw by Java Web Start
Network Routes	
IP Office Connections	▶ Network Routes
Database Integrity	

1.5.3 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](#)^[27] should be used instead.

Health	▶ Logging Configuration
Configuration	▶ Logging Viewer
Diagnostics	▼ Network Routes
Logging Configuration	▶ Description: Simple 'ping-like' test of network routability
Logging Viewer	IP Address <input type="text" value="192.168.42.12"/> <input type="button" value="Check"/>
Network Routes	Result <input type="text" value="Reachable"/>
IP Office Connections	▶ URL Connection Test
Database Integrity	▶ Database Integrity

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**.

1.5.4 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).

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.

1.5.5 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](#) ^[63] section for known issues and resolutions.

1.5.6 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.

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.

AVAYA one-X Portal for IP Office

Welcome Administrator

Health
▶ Logging Configuration
▶ Logging Viewer

Configuration
▶ Network Routes (Not for IP Offices)
▶ IP Office Connections
▶ Database Integrity

Diagnostics
▼ User Data Validation

Enter User Name:

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><switchingSubDomainInformationElement>

User Configuration : Valid
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><arrayListWrapper xmlns:ns2="http://com.avaya.inkaba">

Following are the fields that are validated:

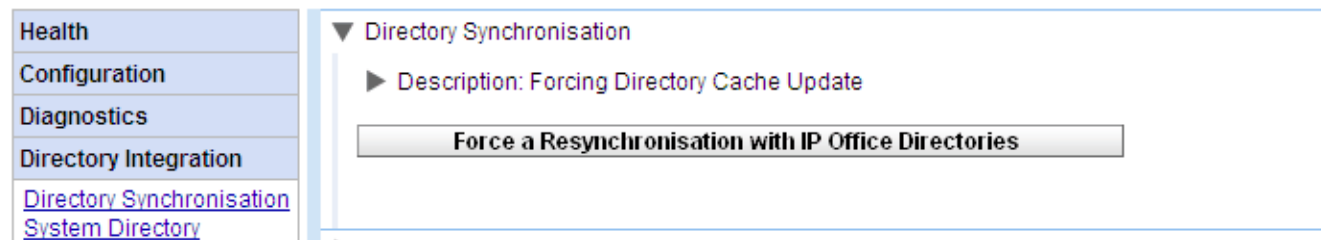
- **Marked Deleted?:** If the user record is marked as deleted or not.
- **UI Preferences:** If UI preference data is valid or not along with the corresponding XML. A 'Reset' button is provided for the Administrator to reset the data if it is corrupt. The UI preference is restored to default factory 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.

Note: The CSTA Configuration and User Configuration do not have the 'Reset' option. The Administrator can copy the information from these two fields and send it to Avaya Backbone Support group for investigation.

1.6 Directory Integration

1.6.1 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.

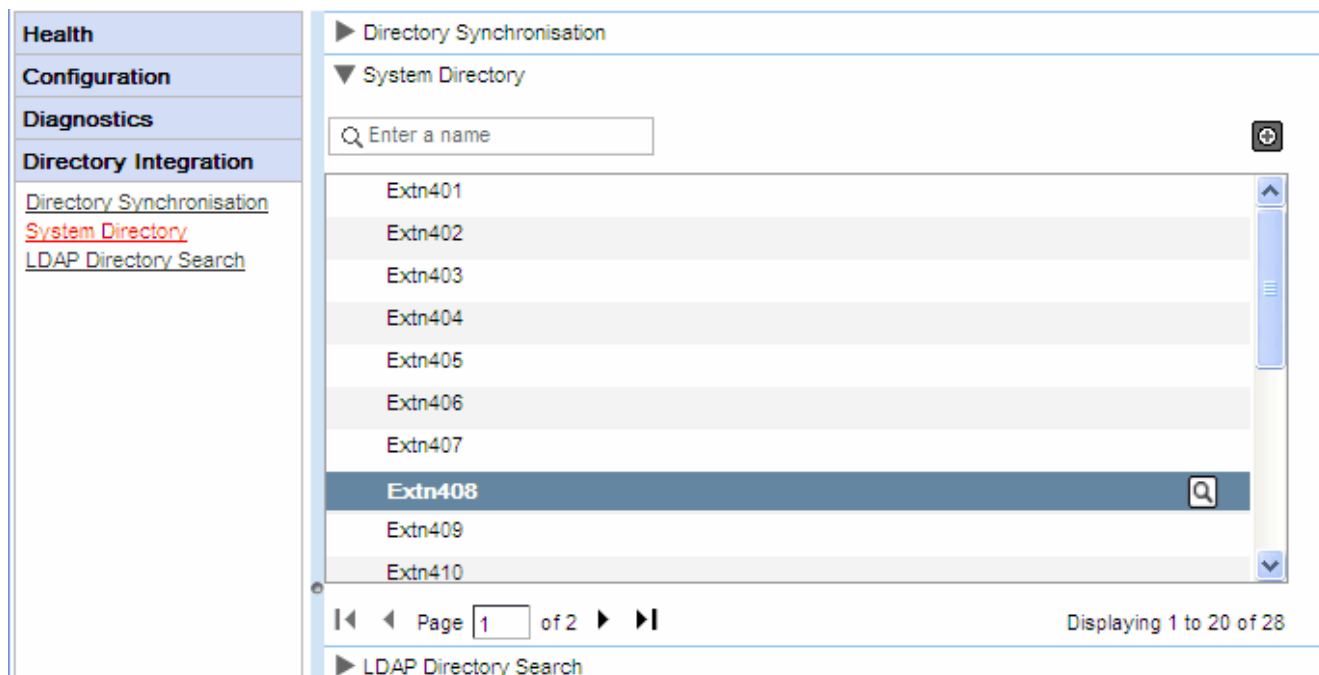


- **Force a Resynchronization with IP Office Directories**

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.

1.6.2 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: By default, the system displays only Hunt groups such as CCR agent group and Centralized group that the *Administrator* for IP Office system has created. The system does not display an XMPP Hunt group created by the *Administrator* of IP Office system. If the *Administrator* of IP Office system has enabled the "Ex-directory" option for a Hunt group in IP Office Manager, then the system does not display those Hunt groups.

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](#) ^[29] 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.

1.6.3 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](#) ^[50].

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.

Health	► Directory Synchronisation
Configuration	► System Directory
Diagnostics	▼ LDAP Directory Search
Directory Integration	<input type="text" value="Enter a name to search"/> <input type="button" value="Go"/>
Directory Synchronisation	Enter search text to find contacts
System Directory	
LDAP Directory Search	
Help & Support	

1.7 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.

1.7.1 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](#)^[32] or [import external gadgets](#)^[36] for the user.

1.7.1.1 Adding an external gadget

Prerequisites:

Gadget URL: To add the gadgets you need the URL of the gadgets. For more information about how to get the URL of the gadgets see [Fetching the URL of an external gadget - Example](#)^[33]

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 and click **Save**.

The system updates the external gadgets that you added in the one-X Portal for IP Office database.

Add or Edit Gadget field description

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.

1.7.1.1.1 Fetching the URL of an external gadget - Example

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

Note: This is just an example and the instructions to fetch the URL of the gadget varies depending on the 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 the following:

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

The text that is within the " " (quotes) is the URL for the gadget.

1.7.1.2 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.

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. 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.

Add or Edit Gadget field description

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
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.

1.7.1.3 Deleting 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.

1.7.1.4 Enabling an external gadget

Note: 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.

1.7.1.5 Disabling an external gadget

Note: When you disable a gadget all the users of one-X Portal for IP Office 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 the 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.

1.7.1.6 Importing a third party gadget

Third party gadgets can be added to the one-X Portal for IP Office by the Administrator. You can upload a maximum of 50 gadgets at a time.

A gadget represents the following parameters:

- 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).

Gadget configuration file specification and validation:

- Configuration file must be in an XML file format.
- File size must not exceed 2 MB.

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
<name>Angry Birds</name>
<toolbarText><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry Birds</en_US><en_GB>Angry Bi
<tooltip><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry Birds</en_US><en_GB>Angry Birds<
<url>http://www.gmodules.com/ig/ifr?url=http://www.forumforyou.it/google_gadget_angry_birds.xml&amp;synd=open&amp;w
</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:

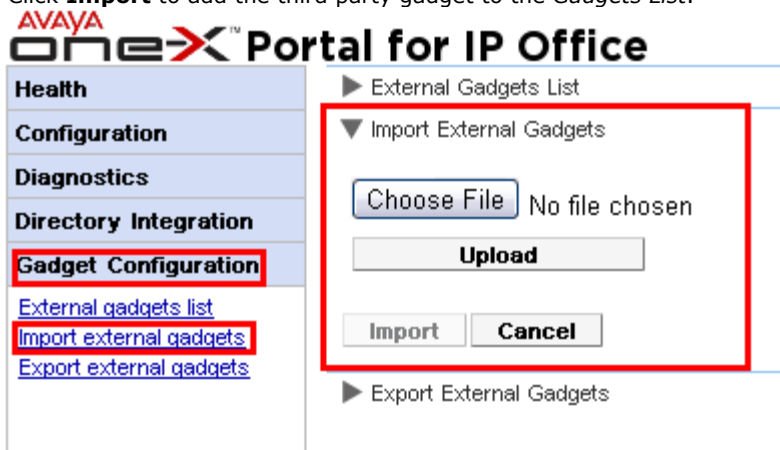
Element	Description
<created>	The date you created the file.
<defaultToolbarIcon>	Specify the default toolbar icon that the system displays when you minimize the gadget is minimized. The system displays the icon in the toolbar of the user.
<downToolbarIcon>	Specify the toolbar that system displays when 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 ^[33]

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

As an Administrator, you can add a third party gadget to the one-X Portal for IP Office by importing the configuration 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*.



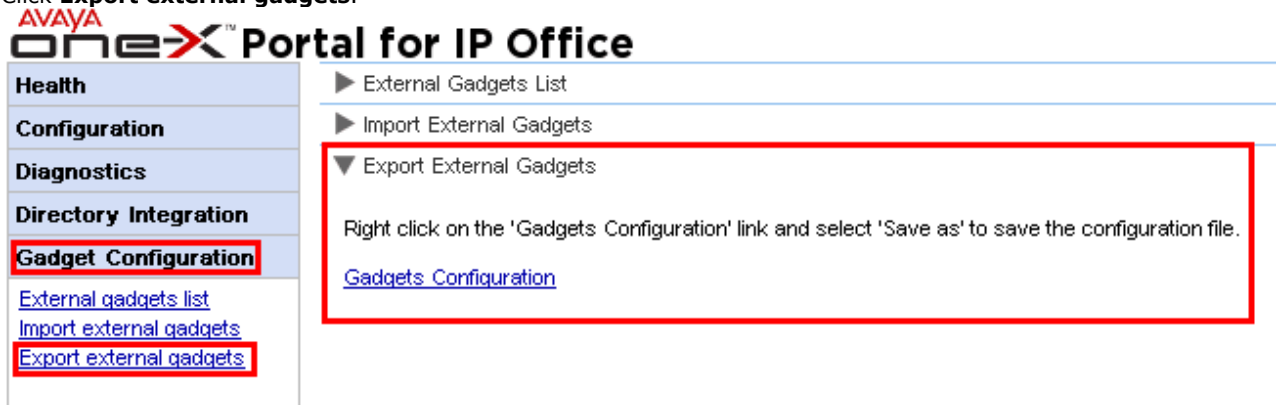
The next time the user logs into the one-X Portal for IP Office, the third party gadget is displayed.

1.7.1.7 Exporting a third party gadget

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. As an Administrator, you can save the configuration file on a machine used to access the admin interface.

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.

You can add this set of gadgets to the one-X Portal for IP Office of another user by [importing](#)  the saved configuration file.

Note: No separate mechanism is provided to move the files between one-X Portal for IP Office deployments directly.

1.8 IM Archive

As an administrator of one-X Portal for IP Office you can search the IM conversations of all the users.

1.8.1 Searching for IM conversations in the archive

You can search for the IM conversations between the system contacts.

Note: All the fields in the search panel are optional.

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.

1. In the left panel, select the **IM Archive**.
2. Click **Search Archive**.
 - The system displays the search panel where you can specify the search criteria.
 - The system lists all conversations based on your search.
3. Click on the conversation that you want to open.
 - The system opens the conversation.

1.8.2 Enable/Disable IM Archive

IM Archive is enabled by default.

To disable archival of IM, do the following:

1. [Enabling Admin console of XMPP Server](#) ⁶⁴
2. [Using XMPP Server to disable IM archiving settings](#) ⁴⁰
3. [Disabling Admin console of XMPP Server](#) ⁶⁵

To enable archival of IM, do the following:

1. [Enabling Admin console of XMPP Server](#) ⁶⁴
2. [Using XMPP Server to enable IM archiving settings](#) ⁴⁰
3. [Disabling Admin console of XMPP Server](#) ⁶⁵

1.8.2.1 Using XMPP Server to disable IM archiving settings

To disable IM archiving settings in XMPP Server:

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.*

1.8.2.2 Using XMPP Server to enable IM archiving settings

To disable IM archiving settings in XMPP Server:

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. Enable 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.*

1.9 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.

Health

Configuration

Diagnostics

Directory Integration

Help & Support

Help

Avaya Support

About

Avaya one-X Portal for IP Office
Copyright 2011 Avaya Inc. All Rights Reserved.

Version:
7.0.25.1419

Links to the licenses of the third-party software components used in one-X Portal for IP Office.

[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 2.

Maintenance

2. Maintenance

This section covers various post installation activities that are to be performed.

- [Preferred Edition License](#) ⁴⁴
- [Manually Starting the Service](#) ⁴⁴
- [Adding an Additional IP Office](#) ⁴⁵
- [Changing an IP Office Details](#) ⁴⁸
- [Adding/Deleting Users](#) ⁵¹
- [Editing User Settings](#) ⁵¹
- [Adding an LDAP Directory Source](#) ⁵⁰
- [Checking the External LDAP Directory](#) ⁵⁵
- [Checking and Updating the System Directory](#) ⁵⁴
- [Upgrading one-X Portal for IP Office](#) ⁵⁶
- [Downgrading one-X Portal for IP Office](#) ⁵⁷
- [Removing one-X Portal for IP Office](#) ⁵⁸
- [Remote Logging](#) ⁵⁹
- [Agent Gadget Control](#) ⁶³
- [Enabling or Disabling Openfire Admin Console](#) ⁶⁴

2.1 Preferred Edition License

A Preferred Edition License is required to use the one-X Portal for IP Office.

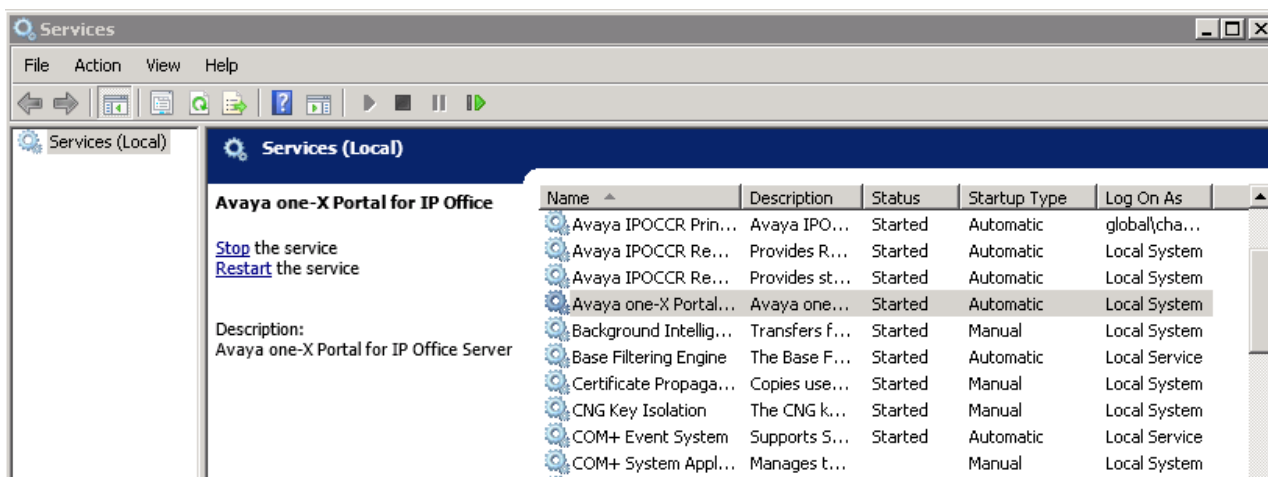
Note: During installation or upgrade, no information message regarding Preferred Edition license will be displayed.

As an Administrator, you can login and provision IPO irrespective of preferred edition license availability. No warning is displayed during IPO provisioning. However, after you log into the one-X Portal for IP Office, an error message is displayed stating that *No Preferred Edition license available* for each IPO not having a preferred edition license. The information is displayed in the CSTA Provider status screen.

When a user logs in for the first time, the one-X Portal for IP Office checks the availability of the preferred edition license for that user. If the license is not available, the one-X Portal for IP Office user login screen displays the error message: *No Preferred Edition license available, Please contact Administrator*. The user can login only if the Preferred Edition License is added later. The removal of the license restricts the user from logging into the one-X Portal for IP Office.

2.2 Manually Starting the Service

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](#) ⁶³.

2.3 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.

- **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](#) 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**.

one-X Portal for IP Office

Health

Configuration

Diagnostics

[Logging Configuration](#)

[Logging Viewer](#)

[Network Routes](#)

[IP Office Connections](#)

[Database Integrity](#)

[User Data Validation](#)

Directory Integration

Gadgets Configuration

IM Archive

Help & Support

▼ Logging Configuration

► Master Logging Level

► Logging Targets (Rolling Log Files)

► Logging Targets (Server and Network)

► Logging Viewer

► Network Routes (Not for IP Offices)

▼ IP Office Connections

► Description: Simple probe test for an IP Office Unit at an IP Address.

IP Address: **Check**

Result

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.

one-X Portal for IP Office

Health

Configuration

[Providers](#)

[Users](#)

[CSV](#)

[Branding](#)

[IM/Presence](#)

[Exchange service](#)

▼ Providers

► Description: Configure providers of services to applications

Get All **Put Selected** **Delete Selected**

Status: All records have been retrieved.

Page 1 2

ID	Name	Edit	Delete
4	Default-CSTA-Provider	Edit	Delete
2	Default-DSML-IPO-Prov	Edit	Delete
3	Default-DSML-LDAP-Pr	Edit	Delete
1	Default-Presentation_La	Edit	Delete

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

Provider Editor

ID: 4

Name: Default-CSTA-Provider

URL: http://localhost:8080/index

Provider Type Selector: Telephony (CSTA)

IP Office(s) Assigned

Mid-Layer URL: http://localhost:8080/index

Mid-Layer Username: indoda_user

CSTA Config Editor

Mid-Layer Password: [REDACTED]

Mid-Layer Password Hash: 7BDDEE71046BA3FA27

Run On Port: 8080

Created: 2012-03-27 11:09:06.9350

Close

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	[REDACTED]	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	[REDACTED]	Delete
1	Enter valid ip address	EnhTcpaService	[REDACTED]	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 TCPA 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
☐	5	CSTA-Provider-1-127.0.0.1	Available	2013 Jun 14 02:39:55	Provider OK	Delete
☐	4	CSTA-Provider-1-Master	Available	2013 Jun 14 02:39:55	Master Available	Delete
☐	3	DSML-Provider-1-127.0.0.1	Available	2013 Jun 24 23:22:11	Global resynchroni	Delete
☐	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

Configuration
Diagnostics
Directory Integration

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.

2.4 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.

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

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.

2.5 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](#)^[30] 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.

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.

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.

Field Name	Mapping
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].

2.6 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, Flare and others after 10 minutes of the synchronization time and users should also be logged in after the synchronization.

2.7 Editing User Settings

Most of the settings set by one-X Portal for IP Office users through their **Configuration** tab, for example **Profile** definitions, are stored as part of the one-X Portal for IP Office database. As the one-X Portal for IP Office administrator you can view and edit those settings. The exception is DND Exception numbers which are part of the user's configuration read from the IP Office system.

Setting	one-X Portal for IP Office	IP Office	Source/Storage
Personal Directory	✓	✓	A user's personal directory is stored in the configuration of both one-X Portal for IP Office and their IP Office. Changes in either are synchronized where possible.
Call Log	✗	✓	A user's call log is stored in the configuration of their IP Office.
Voicemail Messages	✗	✓	Details of the user's voicemail messages are taken from the voicemail server via the IP Office.
Profiles	✓	✗	A user's profiles are stored by the one-X Portal for IP Office server. When a profile is made active, it alters various user settings on the IP Office. If the IP Office configuration settings are altered by another method, the user's profile is changed to 'Detected'.
DND Exceptions	✗	✓	A user's Do Not Disturb exception numbers are stored in the configuration of their IP Office.
Keyboard Shortcuts	✓	✗	A user's keyboard shortcuts are stored by one-X Portal for IP Office.
Sound Configuration	✓	✗	A user's one-X Portal for IP Office sound preference is stored by one-X Portal for IP Office.
Park Slots	✓	✗	The park slot numbers used for a user's one-X Portal for IP Office park buttons are stored by one-X Portal for IP Office.

Editing 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.

User Editor

ID: 13

Name: Extn101

Unique Identifier: B7462000CEEC11DB80

Display Name: Extn101

Password: [Masked]

Password Hash: 7B295DC8FA34A5BE93

User Role: User

User Configuration Type Selector: Select

User Configuration Type Specific Editor: [Empty]

User Role Configuration:
☒ User
☐ Manager

Created: 2013-05-14 01:29:06.1600

Save Cancel

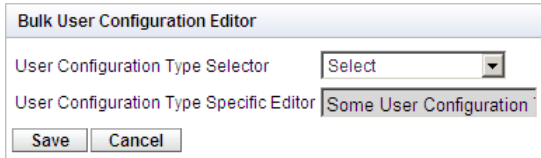
4. Use the **User Configuration Type Selector** to select the user settings you want to view/edit. If required edit the settings.

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**.

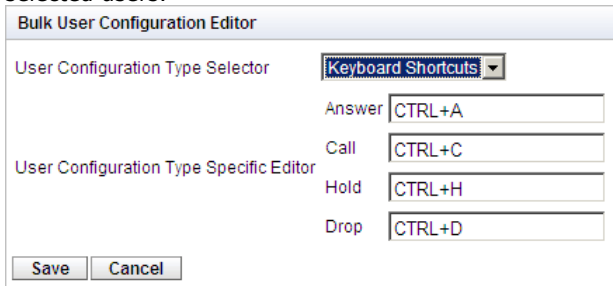
Bulk Editing

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, "User Configuration Type Selector", has a dropdown menu currently set to "Select". The second section, "User Configuration Type Specific Editor", has a text field containing "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 menu is now set to "Keyboard Shortcuts". Below this, there are four rows of configuration options, each with a label and a text field: "Answer" with "CTRL+A", "Call" with "CTRL+C", "Hold" with "CTRL+H", and "Drop" with "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.

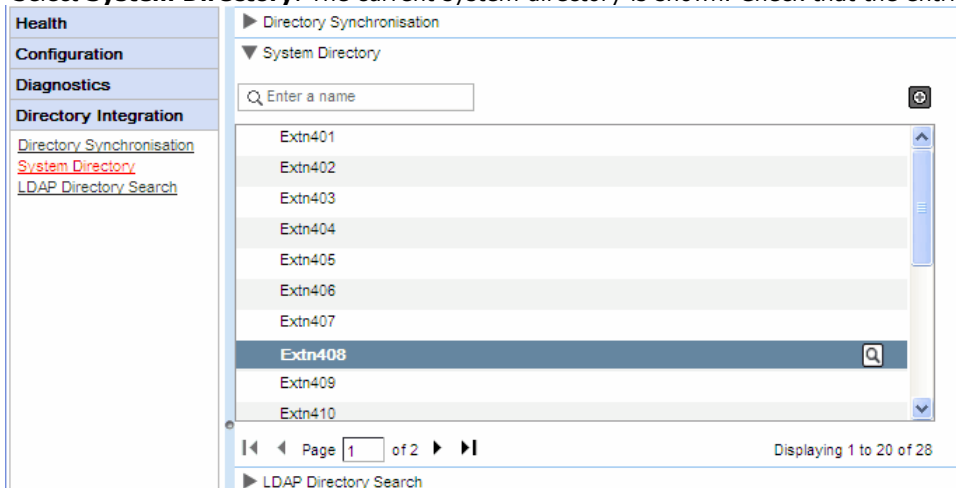
2.8 Checking and Updating the System Directory

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.

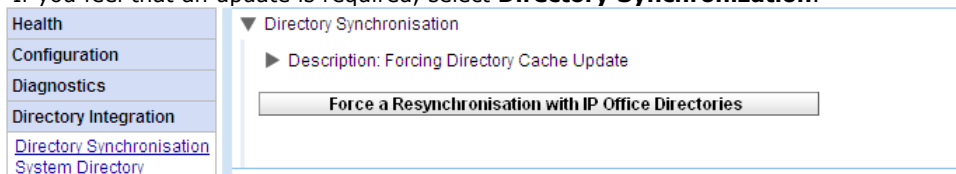
By default, the one-X Portal for IP Office application updates the system directory records every 300 seconds approximately. Through the one-X Portal for IP Office administrator menus you can view the system directory and force an update.

You can also search the external directory in the same way as one-X Portal for IP Office users.

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**.

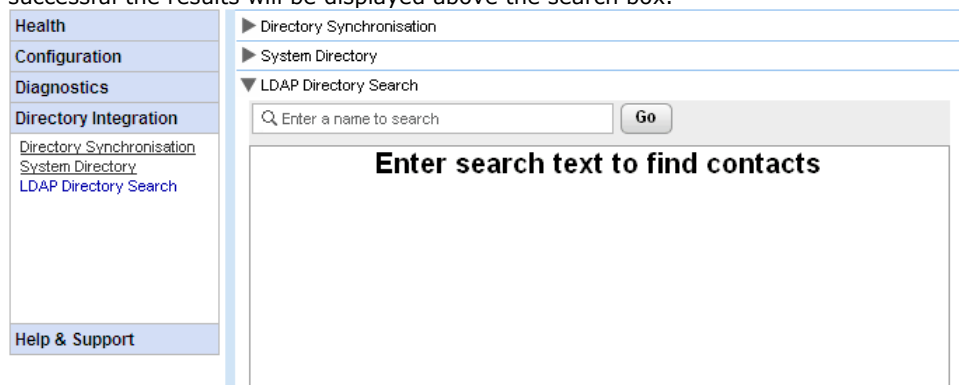


4. Click on **Force a Resynchronization to all IP Office Directories**.

2.9 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.

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 administrator interface. On the left is a sidebar menu with the following items: Health, Configuration, Diagnostics, Directory Integration (highlighted), Directory Synchronisation, System Directory, LDAP Directory Search, and Help & Support. The main content area has a breadcrumb trail: Directory Synchronisation > System Directory > LDAP Directory Search. Below the breadcrumb is a search input field with the placeholder text 'Enter a name to search' and a 'Go' button. Below the search field is a large rectangular box containing the text 'Enter search text to find contacts'.

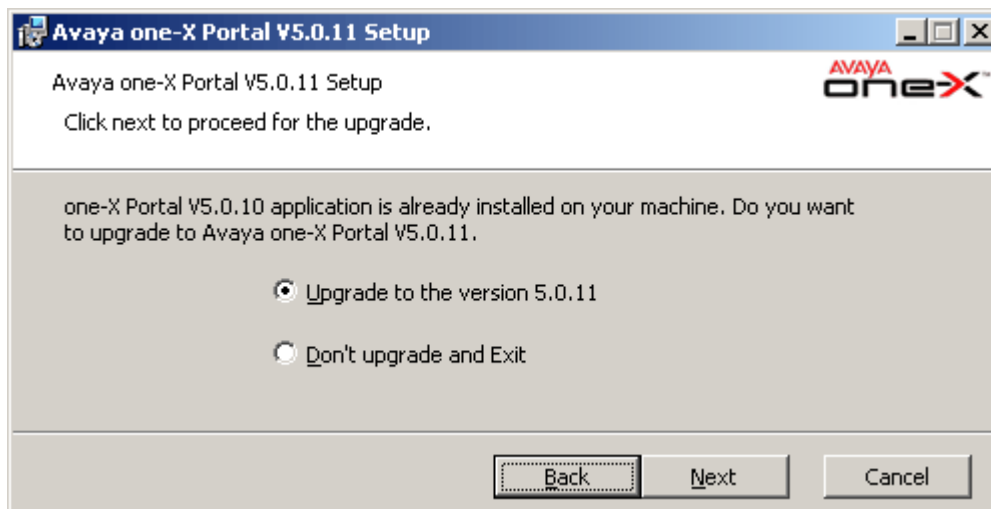
2.10 Upgrading one-X Portal for IP Office

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.

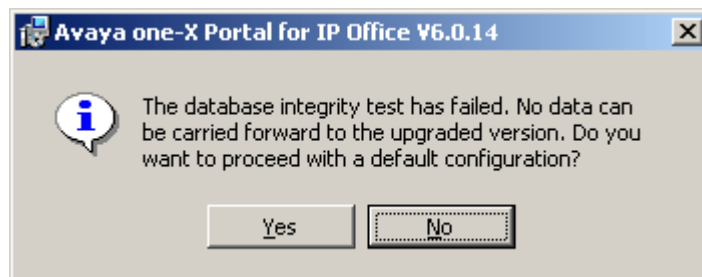
If one-X Portal for IP Office is already installed on a server PC and the installation file for a later version is run, the existing version will be detected and you will be prompted whether to upgrade or not. If you select to upgrade, the process is similar to normal software installation, however some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

2.11 Downgrading one-X Portal for IP Office

If the one-X Portal for IP Office application software has been upgraded using the [upgrade process](#)^[56], it is also possible to downgrade back to the original installed version.

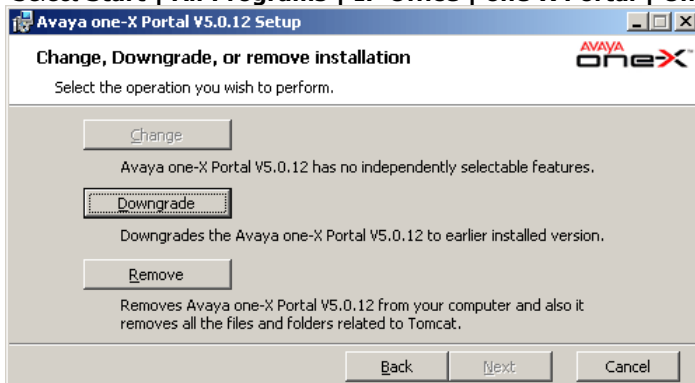
Note: The installation of one-X Portal for IP Office and the last upgrade to one-X Portal for IP Office are both be listed in the Windows Control Panel **Add and Remove Programs** list. Note however that removing either of these will remove the whole application.

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.

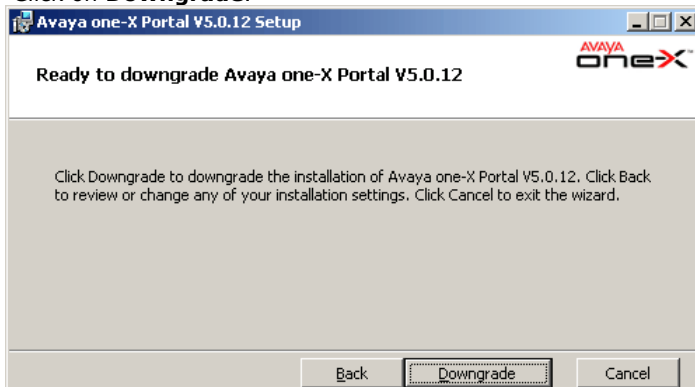
- **Warning**

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.

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].

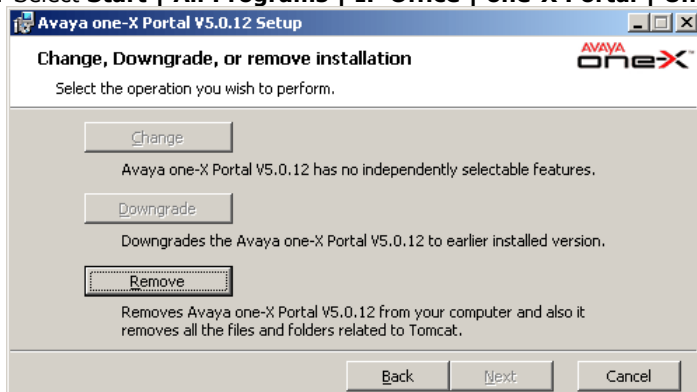
2.12 Removing one-X Portal for IP Office

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

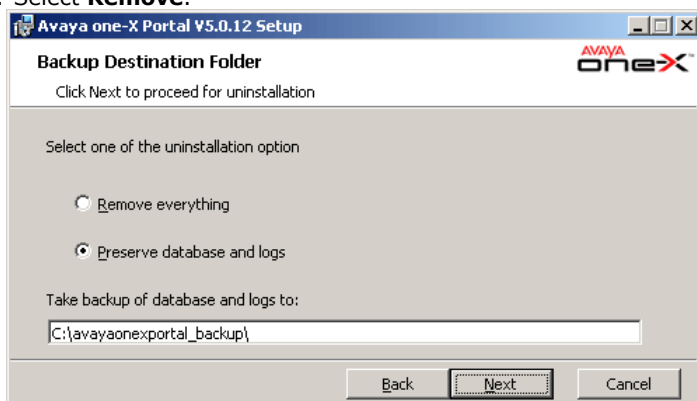
Uninstalling one-X Portal for IP Office

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

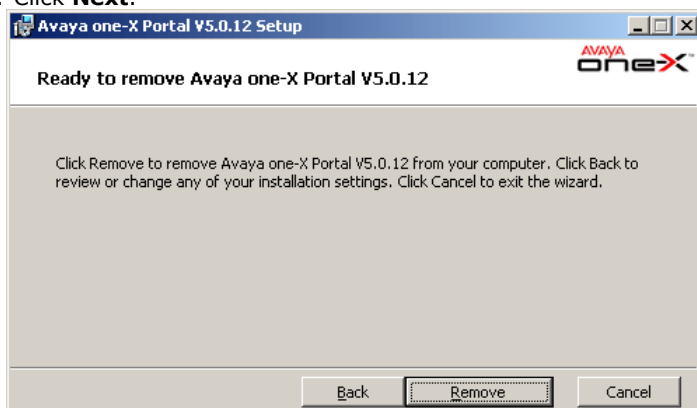
1. Select **Start | All Programs | IP Office | one-X Portal | Uninstall one-X Portal**.



2. Select **Remove**.



3. Click **Next**.



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

Removing one-X Portal for IP Office via the 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:\avayaonexpportal_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.

2.13 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**.

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'.

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.

Enabled	Name	Level	File Path
☒	Overall	ALL	../logs/1XOverallRollingFile.log
☒	Presentation Layer	ALL	../logs/1XPresentationLayerRollingFile.log
☒	Mid-Layer	ALL	../logs/1XMidLayerRollingFile.log
☒	Telephony (CSTA)	ALL	../logs/1XCSTAServiceRollingFile.log
☒	Directory (IP-Office)	ALL	../logs/1XIPODirServiceRollingFile.log
☒	Directory (LDAP)	ALL	../logs/1XLDAPDirServiceRollingFile.log

▼ Logging Targets(Server and Network)

Socket Receiver(required for remote log viewing)

☒ Enabled

2. Check that **Socket Receiver** is enabled.

3. Select **Logging Viewer**.

Logging Viewer

► 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

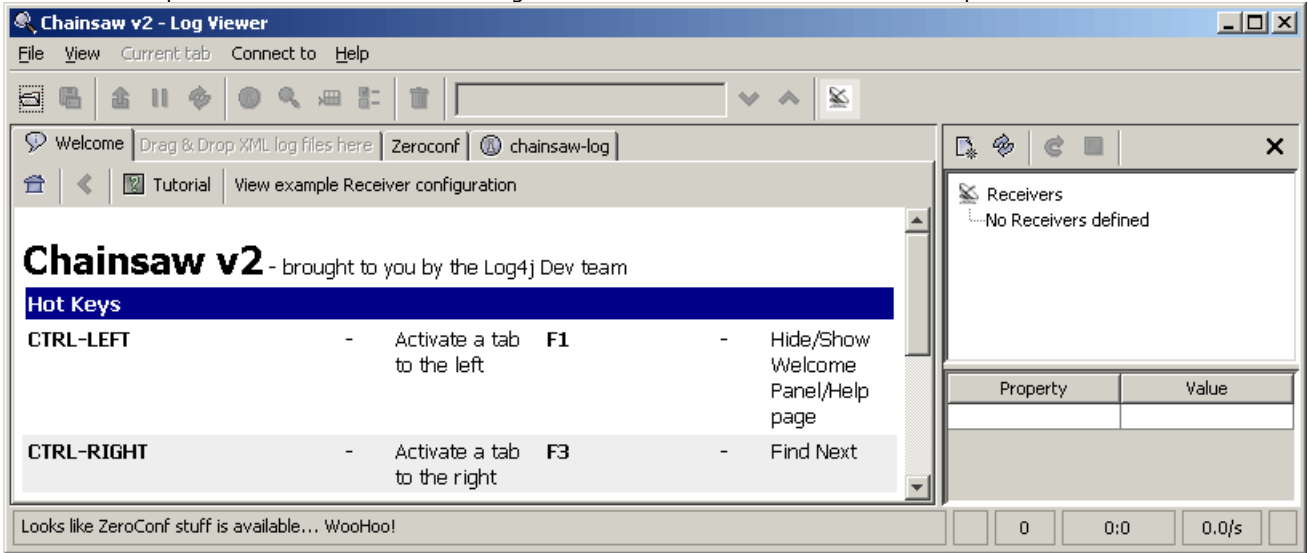
► Database Integrity

► User Data Validation

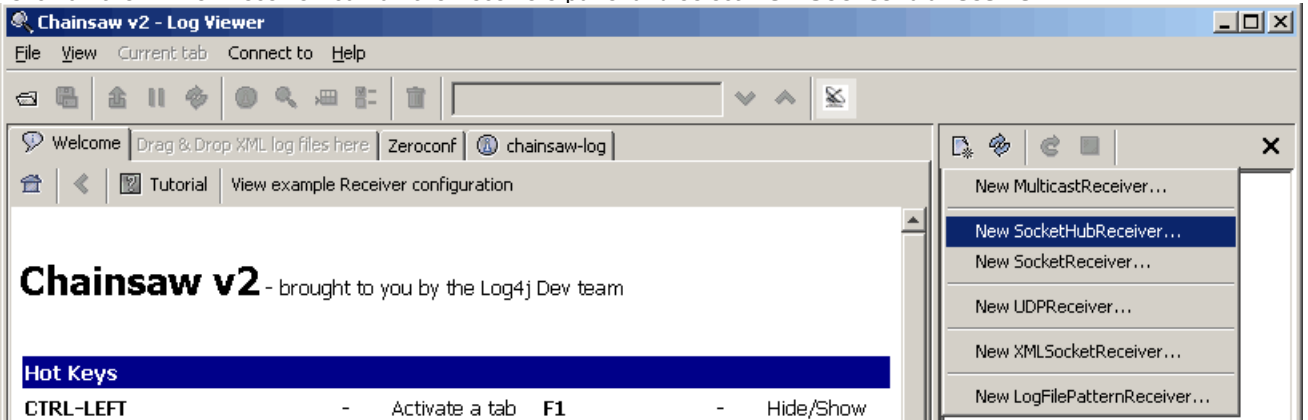
4. Click on **Start Installation of Apache Chainsaw by Java Web Start**.

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**.

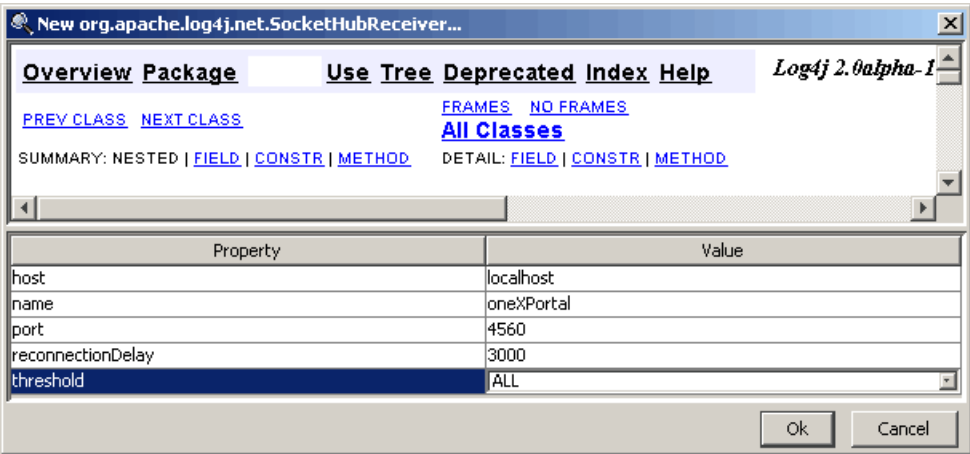
6. The Receivers panel should be visible on the right. If not click on the  button in the top toolbar.



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

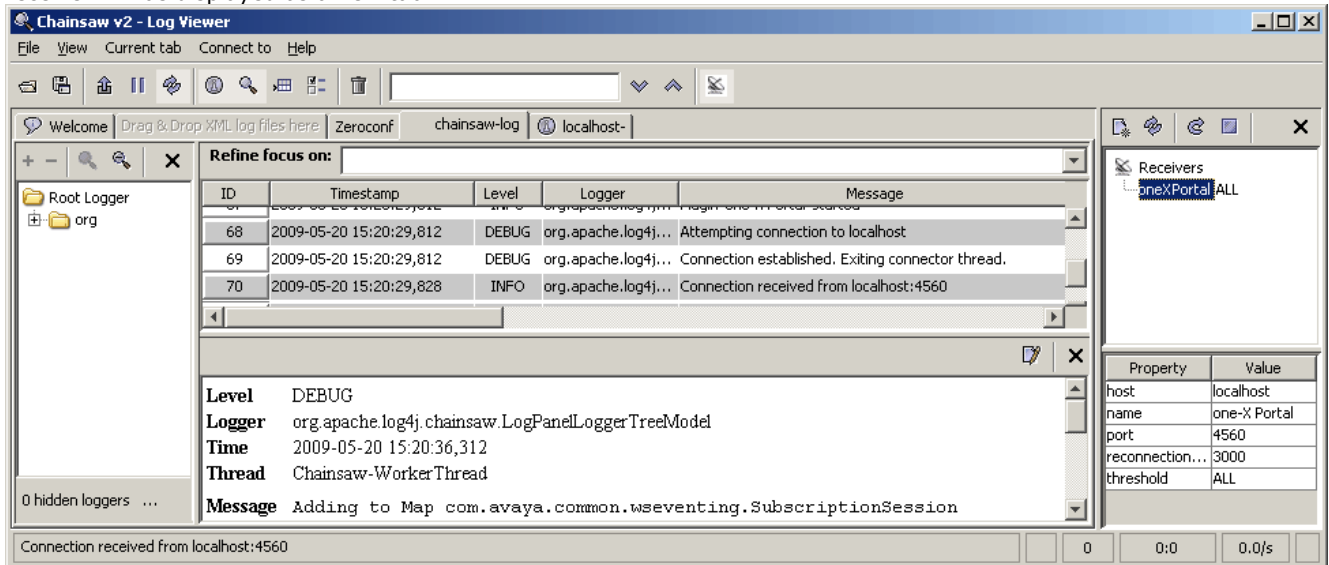


8. Enter the details for the one-X Portal for IP Office server.

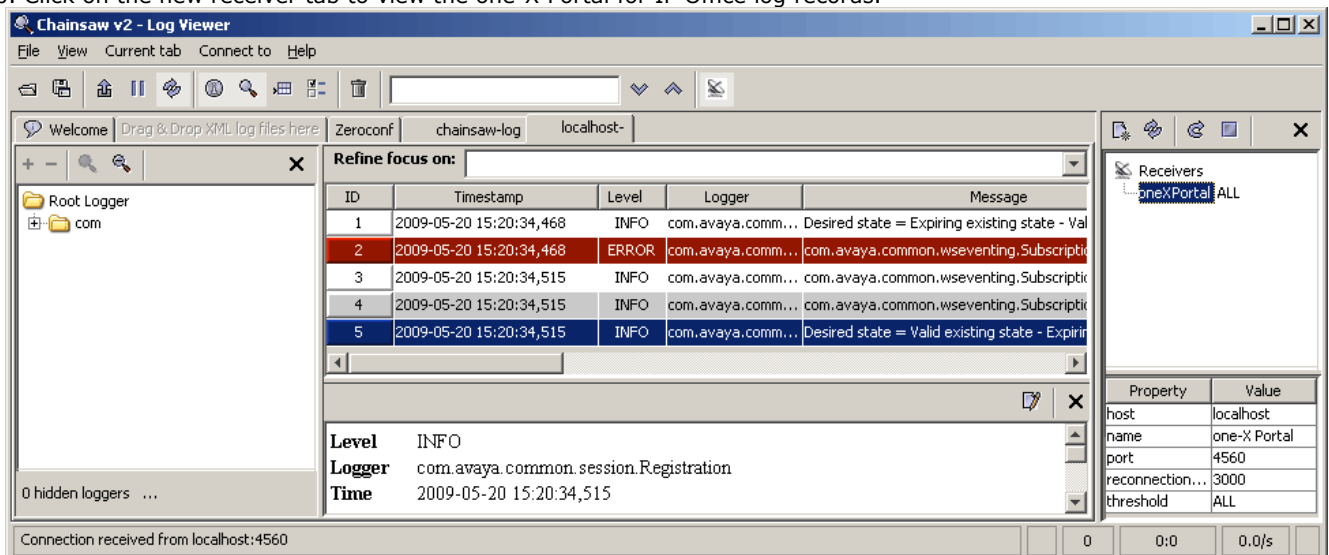


host	This field sets the address of the one-X Portal for IP Office server. In the example above chainsaw is being run on the one-X Portal for IP Office server PC.
name	This field is for display only. Enter a name for the receiver entry in Chainsaw.
port	Set this to 4560. This is the port to which one-X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

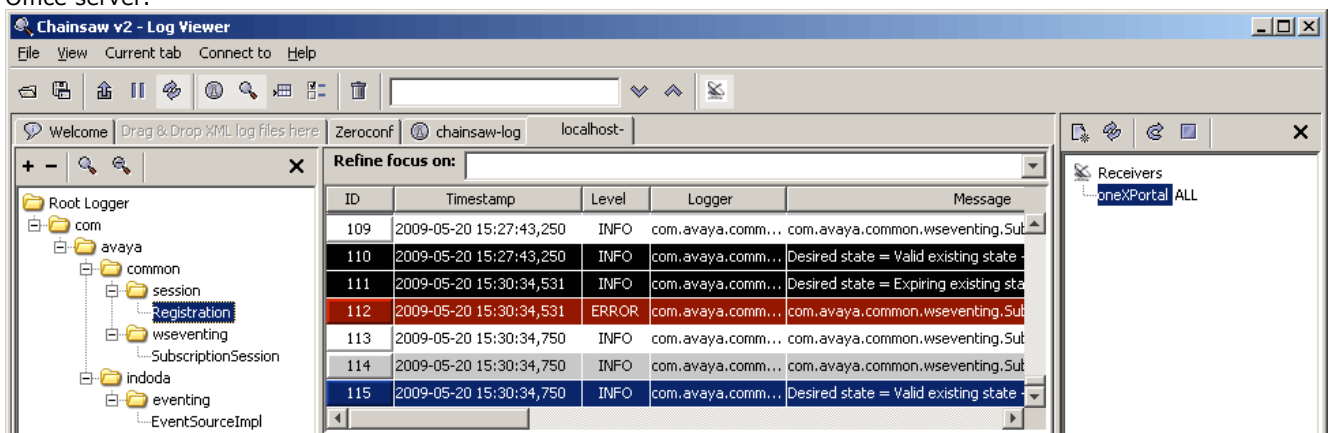
9. When you have completed the fields, click OK. After a few seconds the receiver should start and connect to the one-X Portal for IP Office server. The process will appear as log events on the chainsaw-log tab and when completed the receiver will be displayed as a new tab.



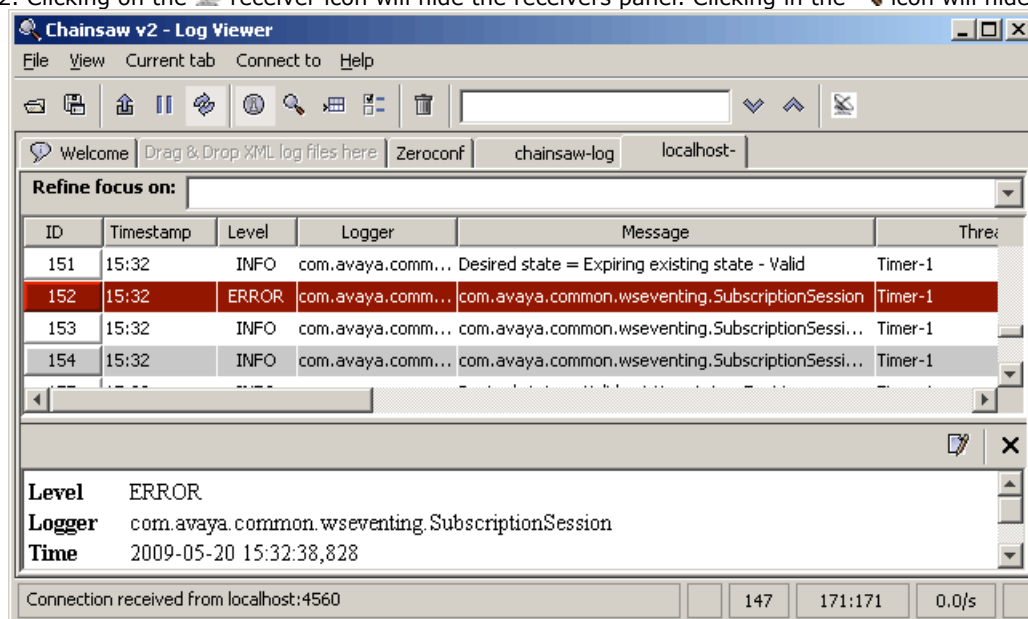
10. Click on the new receiver tab to view the one-X Portal for IP Office log records.



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



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



2.14 Troubleshooting

Version Mismatch Problem

Symptoms	<ul style="list-style-type: none"> • Database integrity ²⁷ 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 ⁵⁸. 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 ⁵⁸. 4. Install one-X Portal for IP Office.

2.15 Agent Gadget Control

Those users configured as CCR Agents within the IP Office configuration are shown the one-X Portal for IP Office Agent Control gadget. They can use this to control various settings including enabling or disabling their membership of various hunt groups.

Through the IP Office configuration, you can select for which groups the user is able to control their group membership. This will affect both the one-X Portal for IP Office and also the group control menu options on some phones (1400, 1600, 9500 and 9600 Series).

1. Using IP Office Manager, receive the configuration from the IP Office system.
2. Select  **User** and select the user whose setting you want to change.
3. Select the **Menu Programming** tab and then the **Hunt Group** sub-tab.
4. The menu displays the hunt groups of which the user is a member and the functions that the user can perform for each of those groups.
5. To allow the user to enable or disable their group membership for a particular group, select the **Can Change Membership** option for that group.
6. Save the configuration back to the IP Office system.

2.16 Enabling or Disabling Admin console of XMPP Server

2.16.1 Enabling Admin console of XMPP Server

To enable Admin console in a Linux platform:

1. Login as root user.
2. To go to the directory, in the command line type:

```
cd /opt/Avaya/oneXportal/openfire/bin
```

3. At the prompt, type:

```
sh AdminConsoleManager.sh enable
```

4. To restart the service type:

```
service onexportal restart
```

Note: The system applies these changes only after you restart Avaya one-X Portal.

To enable Admin console in a Windows platform:

1. Go to command prompt.
2. To go to the directory where one-X Portal for IP Office is installed, type: C:\Program Files\Avaya\oneXportal

Note:

The installation path will be different on a 32 bit and 64 bit installation

3. To go to openfire directory, type: cd \openfire\bin
4. At the command prompt, type: AdminConsoleManager.bat enable
5. Restart Avaya one-X Portal.

Note: The system applies these changes only after you restart Avaya one-X Portal.

2.16.2 Disabling Admin console of XMPP Server

To disable Admin console in a Linux platform:

1. Login as root user.

2. To go to the directory, in the command line type:

```
cd /opt/Avaya/oneXportal/openfire/bin
```

3. At the prompt, type:

```
sh AdminConsoleManager.sh disable
```

4. To restart the service, type:

```
service onexportal restart
```

Note: The system applies these changes only after you restart Avaya one-X Portal.

To disable Admin console in a Windows platform:

1. Go to command prompt.

2. To go to the directory where one-X Portal for IP Office is installed, type: C:\Program Files\Avaya\oneXportal

Note:

The installation path will be different on a 32 bit and 64 bit installation

3. To go to openfire directory, type: cd \openfire\bin

4. At the command prompt, type: AdminConsoleManager.bat disable

5. Restart Avaya one-X Portal.

Note: The system applies these changes only after you restart Avaya one-X Portal.

2.17 Migrating from Phone Manager 7.0 to one-X Portal for IP Office 8.0

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 SoftPhone. However, you can use the Avaya Power User solution that includes the IP Office Video SoftPhone application and make VoIP calls.

To use the IP Office Video SoftPhone application and Telecommuter feature, you must purchase the Power User license.

To use the CCR Agent feature, you must purchase the CCR Agent license.

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 Manager Administration guide at the Avaya support website www.support.avaya.com.

Chapter 3.

Backup/Restore

3. Backup/Restore

one-X Portal for IP Office supports a new 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.

3.1 Superuser Log in

Only one user can be logged in as the Superuser at any time.

1. Enter the browser address ***http://<server name>:<server port>/onexportal-afa.html***, where *<server name>* is the name or the IP address of the server, and *<server port>* is the port number assigned to the server.

- **Note:** one-X Portal for IP Office 8.1 continues to support the URL ***http://<server name>:<server port>/induna/induna.html***.

2. At the login menu, 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.

3.2 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			
System Status			
View			
Configurator			
DB Operations			
	Backup Name	File Size in Bytes	Backup Date Time
Last Backup Taken	OneX-DB-Bkp	29882	2010-08-03-11.33.25
	Backup Name	File Size in Bytes	Restore Date Time
Last Restore Done	OneX-DB-Bkp-2010-08-03-	29898	2010-08-03-11.38.32
	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.

3.3 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, a sidebar contains three main sections: 'System Status', 'Configuration', and 'DB Operations'. The 'Configuration' section is active, showing an 'Edit' link. The main content area 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). Below these fields are two buttons: 'Save' and 'Clear'.

- **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.

3.4 DB Operations

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

3.4.1 Backup

This menu is used to create backup files.

System Status ▾ Backup

Configuration

DB Operations

[Backup](#)

[Restore](#)

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

[Restore](#)

- 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.

3.4.2 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.

The screenshot shows the 'DB Restore Operation' configuration window. On the left is a sidebar with 'System Status', 'Configuration', 'DB Operations', 'Backup', and 'Restore'. The 'DB Restore Operation' section is active, showing 'Restore From' options: 'Local Server' (selected), 'FTP', and 'Local Drive'. Below these are input fields for 'Server IP Address', 'Port' (set to 21), 'User Name', and 'Password'. A 'Show Available Backups' button is at the bottom.

- **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.

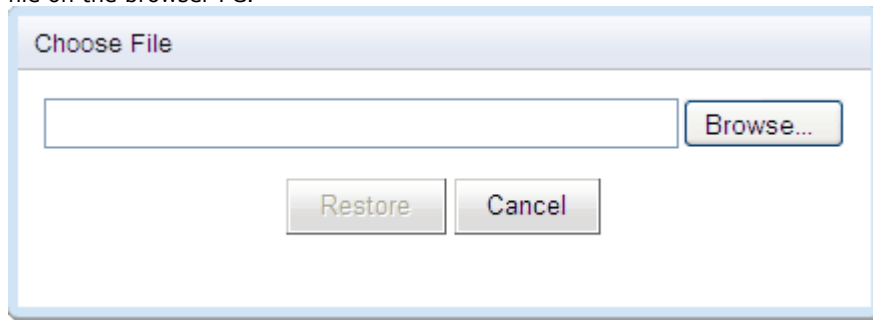
The screenshot shows the 'List of Backups' dialog box. It contains a table with the following data:

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

At the bottom of the dialog are 'Restore' and 'Cancel' buttons.

- **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.

A screenshot of a 'Choose File' dialog box. The dialog has a title bar with the text 'Choose File'. Inside, there is a text input field on the left and a 'Browse...' button on the right. Below these, there are two buttons: 'Restore' and 'Cancel'.

Chapter 4.

Glossary

4. Glossary

CSTA - Computer Supported Telecommunications Application.

Indoda - The Zulu word for 'man'.

Induna - The Zulu word for 'advisor', 'great leader' or 'ambassador'.

Inyama - The Zulu word for 'meat' or, when applied to people, 'flesh'. For example 'inyama nenyama' is 'face to face' or 'in the flesh'.

Inkaba - The Zulu word for 'navel' or 'centre'. For example 'inkaba yedolobha' is 'town centre'.

Izwi - The Zulu word for 'voice'.

TCPA - Thin Client Productivity Application.

TSPI - Telephony Service Provider Interface.

XMPP - Extensible Messaging and Presence Protocol.

XML RPC - XML Remote Procedure Call.

Chapter 5.

Document History

5. Document History

17th July 2014	09c	<ul style="list-style-type: none">• Fix for access to administrator help in 9.0.4.
3rd October 2014	09d	<ul style="list-style-type: none">• Added missing step to confirm changed entries are selected before using "Put Selected".
8th December 2015	09e	<ul style="list-style-type: none">• General refresh and update.

Index

4

4560 59

A

About 7

Active Sessions 7, 12

Add

IP Office 45

LDAP 50

User 51

Administrator

Help 41

Name 8

Agent 63

Apache

Chainsaw 26, 59

Assign

IP Office 45, 48

IP Office (CSTA) 13

IP Office (Directory) 14

LDAP Provider 15

Providers 13

Automatic logout 9

Avaya Support 7

B

Backups 7

Base DN 50

Bulk Edit 18, 51

User 51

C

Call Log 51

Chainsaw 26, 59

Component Status 7, 10

Computer Supported Telecommunications Application 73

Configuration 7

Bulk Edit 51

CSV 20

Export 20

Providers 13

Users 18

Control Panel 58

CSTA 13, 73

CSTA (IP Office) Provider 13

CSV 7, 20

D

Database

Check 27

Sanity Check 27

Database Integrity 7

Deinstall 58

Delete

IP Office 48

User 51

Diagnostics 7

Connections 27

Database Integrity 27

IP Office Connections 27

Logging Configuration 24, 59

Logging Viewer 26, 59

Network Routes 26

Directory

Export 20

Resynch 29, 54

Directory (DSML IP Office) 14

Directory (DSML LDAP) 15

Directory Integration 7

Directory Synchronization 29, 54

Directory Intergration

LDAP 30, 55

System Directory 30, 54

Directory Search

LDAP 30, 55

System Directory 30, 54

Directory Synchronization 7

DND Exceptions 51

Downgrading 57

DSML (IP Office) Provider 14

DSML (LDAP) Provider 15

E

Echo 26

Edit

Bulk Edit 51

IP Office settings 48

User settings 18, 51

Environment 7

Events 11

Exceptions 51

Export Configuration 20

exportDirectoryEntry.csv 20

exportUser.csv 20

External Directory

Search 30, 55

F

Field Mapping 15, 50

Force a Resynchronization 29, 54

G

Group 63

H

Health 7

Active Sessions 12

Component Status 10

Environment 12

Key Recent Events 11

Help 7

About 41

Avaya Support 41

Help 41

Hunt Group 63

I

Immediate logout 9

IP Office

Connections 7

CSTA Provider 13

Directory Provider 14

J

Java Web Start 59

K

Key Recent Events 7, 11

Keyboard Shortcuts 51

L

LDAP

Assign 50

Directory Search 7, 30, 55

Provider 15

Log Files 24

Log4j format 59

Logging 59

- Logging 59
 - Configuration 7
 - Level 24
 - Targets 24
 - Viewer 7, 59
- Logging Configuration 59
- Login 8
- Logout 9
- M**
- Maintenance 43
- Master Logging Level 24
- Membership 63
- Messages 51
- N**
- Network Routes 7, 26
- Not Reachable 26
- O**
- Override Admin Session 8
- P**
- Park Slots 51
- Password 8
- Personal Directory 51
- PING 26
- Port
 - 4560 59
 - 7 26
- Presence 51
- Provider 7
 - Assign 13
 - CSTA (IP Office) 13
 - Directory (DSML IP Office) 14
 - Directory (DSML LDAP) 15
 - DSML (IP Office) 14
 - DSML (LDAP) 15
 - View 13
- R**
- Reachable 26
- Recent Events 11
- Remote Logging 59
- Remove
 - IP Office 48
 - one-X Portal for IP Office 58
 - User 51
- Reset Session Count 8
- Restart Service 44
- Resynchronization 29, 54
- Rolling Log Files 24
- Routes 26
- S**
- Sanity 27
- Search
 - LDAP 30, 55
 - System Directory 30, 54
- Search Base 50
- Server
 - Information 12
 - Version 12
- Service
 - Restart 44
- Sessions 12
- Settings
 - Bulk Edit 51
- Shortcuts 51
- Socket Receiver 24, 59
- Start Service 44
- Status 10
- Synchronization 29, 54
- System Directory 7
 - Directory Search 30, 54
 - Export 20
 - Resynch 29, 54
- T**
- TCP Port 7 26
- TCPA 73
- Telephony Service Provider Interface 73
- Test
 - External Directory 30, 55
 - IP Office connection 27
 - LDAP Directory 30, 55
 - Network Route 26
 - System Directory 30, 54
- Thin Client Productivity Application 73
- TSPI 73
- U**
- Uninstall 58
- Upgrading 56
- User
 - Add 51
 - Built Edit 51
 - Delete 51
 - Edit settings 51
 - Export 20
 - Help 41
- Users 7
 - Active 12
 - Edit settings 18
 - Resynch 29, 54
 - View 18
- V**
- Version 12
- View
 - Component Status 10
 - Key Recent Events 11
 - Providers 13
- Voicemail Messages 51

