IP Office 8.0

Administering one-X Portal for IP Office

15-601139 Issue 05a - (Friday, December 09, 2011)

© 2011 AVAYA All Rights Reserved.

Notices
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
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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 End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

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

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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

Avaya fraud intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com
Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks
Avaya and Aura are trademarks of Avaya, Inc.
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(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(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.

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

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

1. Maintenance

1.1 Preferred Edition License 5
1.2 Manually Starting the Service 6
1.3 Adding an Additional IP Office 6
1.4 Changing IP Office Details 9
1.5 Adding an LDAP External Directory Source 10
1.6 Adding/Deleting Users 11
1.7 Editing User Settings 11
1.8 Backing Up the Database 14
1.9 Restoring a Previous Backup 15
1.10 Checking and Updating the System Directory 15
1.11 Checking the External LDAP Directory 16
1.12 Upgrading one-X Portal for IP Office 17
1.13 Downgrading one-X Portal for IP Office 17
1.14 Removing one-X Portal for IP Office 18
1.15 Remote Logging 20
1.16 Troubleshooting 23
1.17 Agent Gadget Control 24
1.18 Enabling or Disabling Openfire Admin Console 24

2. Administration

2.1 Log in 27
2.2 Log out 28
2.3 Health 28
2.3.1 Component Status 28
2.3.2 Key Recent Events 28
2.3.3 Active Sessions 29
2.3.4 Environment 29
2.4 Configuration 30
2.4.1 Providers 30
2.4.2 Users 34
2.4.3 Backups 36
2.4.4 CSV 36
2.4.5 Branding 37
2.4.6 IM/Presence 37
2.4.7 Exchange service 37
2.5 Diagnostics 39
2.5.1 Logging Configuration 39
2.5.2 Logging Viewer 40
2.5.3 Network Routes 40
2.5.4 IP Office Connections 40
2.5.5 Database Integrity 41
2.5.6 User Data Validation 41
2.6 Directory Integration 42
2.6.1 Directory Synchronisation 42
2.6.2 System Directory 43
2.6.3 LDAP Directory Search 43
2.7 Gadget configuration 44
2.7.1 External gadget list 44
2.8 Help & Support 48

3. Backup/Restore

3.1 Superuser Log in 51
3.2 System Status 51
3.3 Configuration 52
3.4 DB Operations 52
3.4.1 Backup 52
3.4.2 Restore 53

4. Glossary

Index 58

Chapter 1. Maintenance

1. Maintenance

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

- Preferred Edition License 5
- Manually Starting the Service 6
- Adding an Additional IP Office 6
- Changing an IP Office Details 9
- Adding/Deleting Users 11
- Editing User Settings 11
- Adding an LDAP Directory Source 10
- Checking the External LDAP Directory 16
- Backing Up the Database 14
- Restoring a Previous Backup 15
- Checking and Updating the System Directory 15
- Upgrading one-X Portal for IP Office 17
- Downgrading one-X Portal for IP Office 17
- Removing one-X Portal for IP Office 18
- Remote Logging 20
- Agent Gadget Control 24
- Enabling or Disabling Openfire Admin Console 24

1.1 Preferred Edition License

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

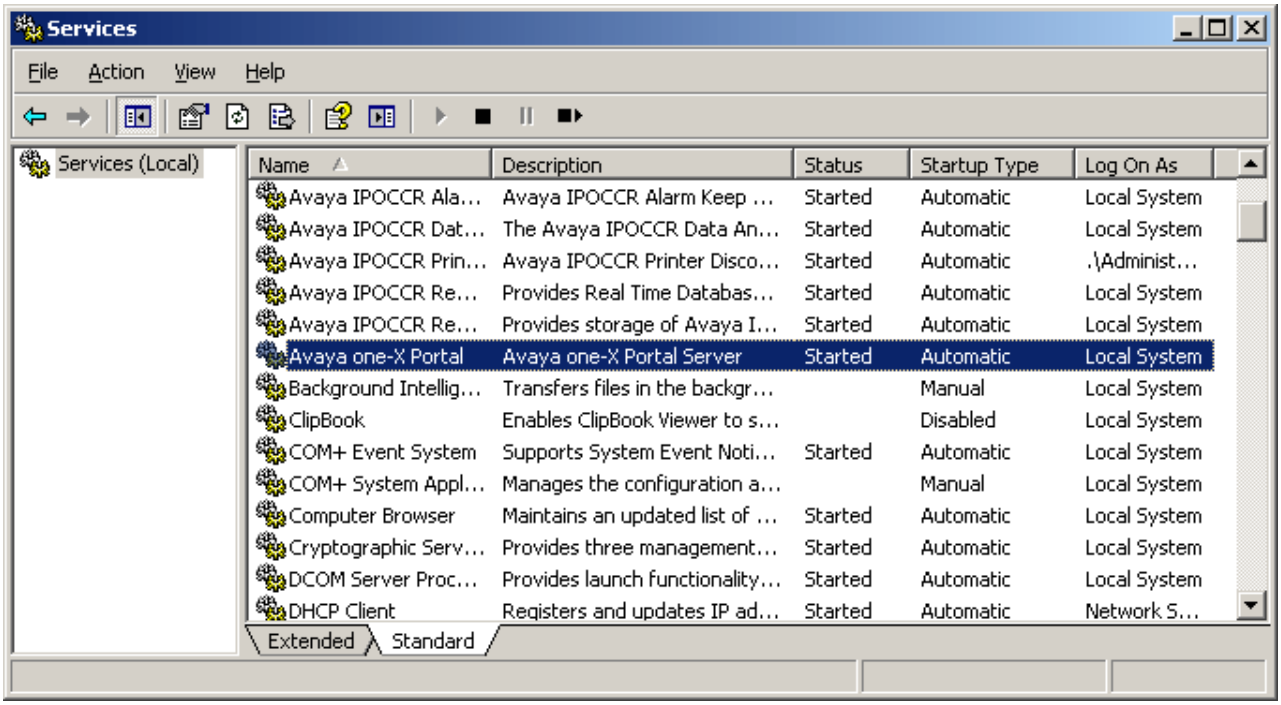
Note: During installation or upgrade, no information message regarding Preferred Edition license will be displayed.

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.

1.2 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 23.

1.3 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.

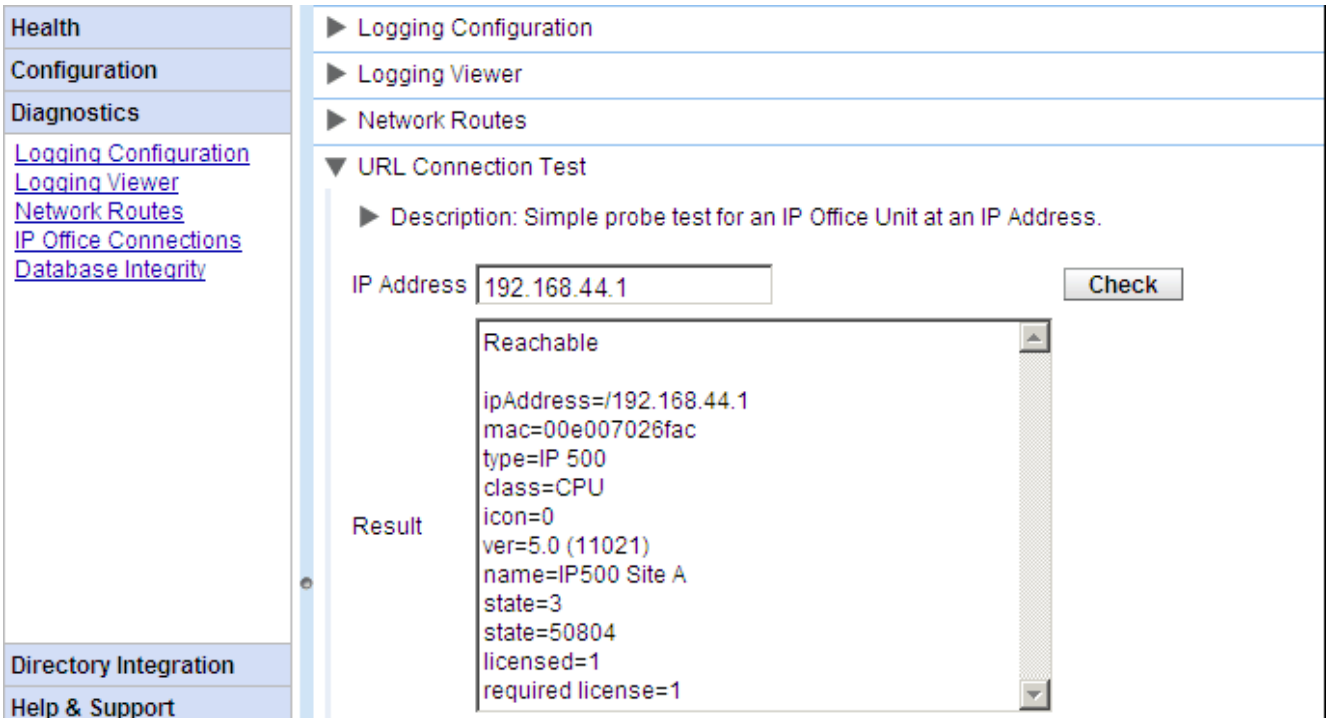
1. Before adding another IP Office to the one-X Portal for IP Office configuration:

- 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 27 to the administrator menus.
3. Check that the IP Office can be seen from the one-X Portal for IP Office server.

a. Select **Diagnostics** and then **IP Office Connections**.

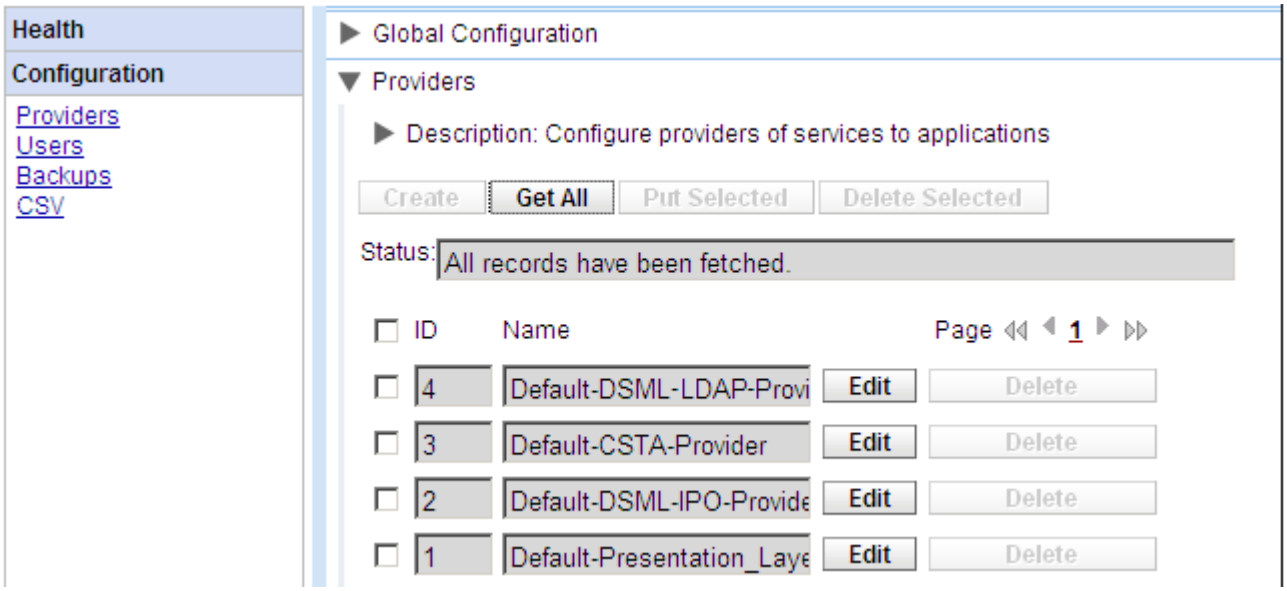
b. Enter the **IP Address** of the target IP Office and click on **Check**.



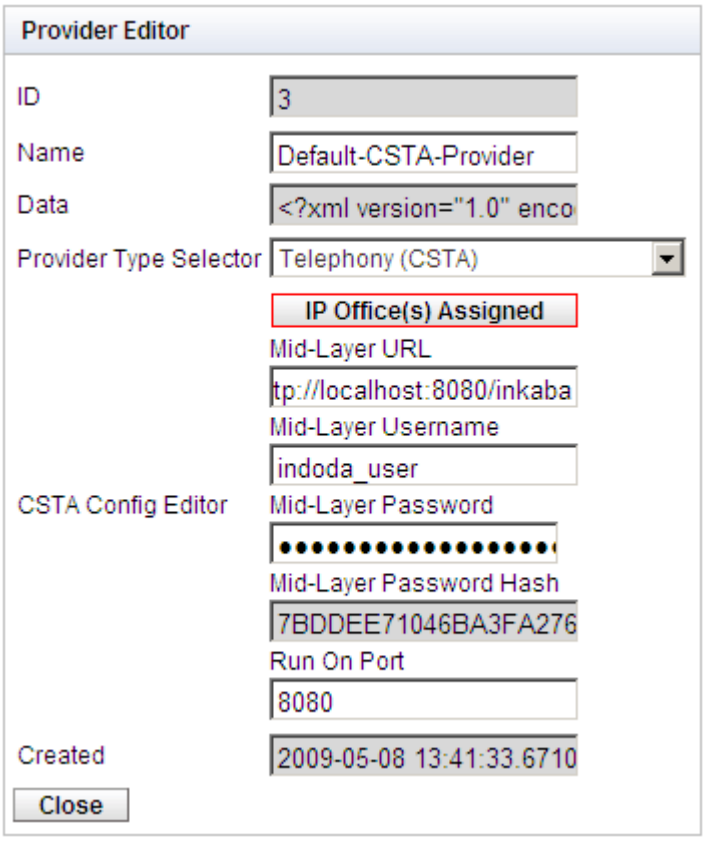
c. If the IP Office is reachable, the results will include base information about the IP Office system.

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

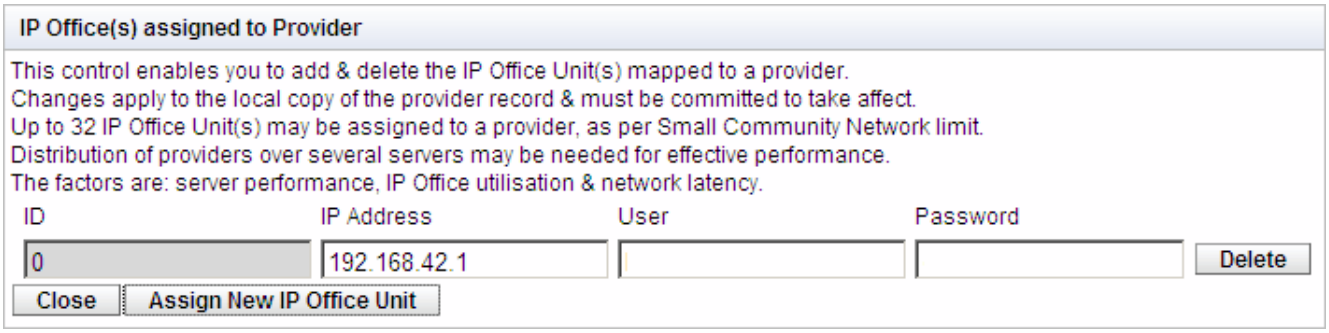
5. Click on **Get All** to retrieve the current provider records from the one-X Portal for IP Office database.



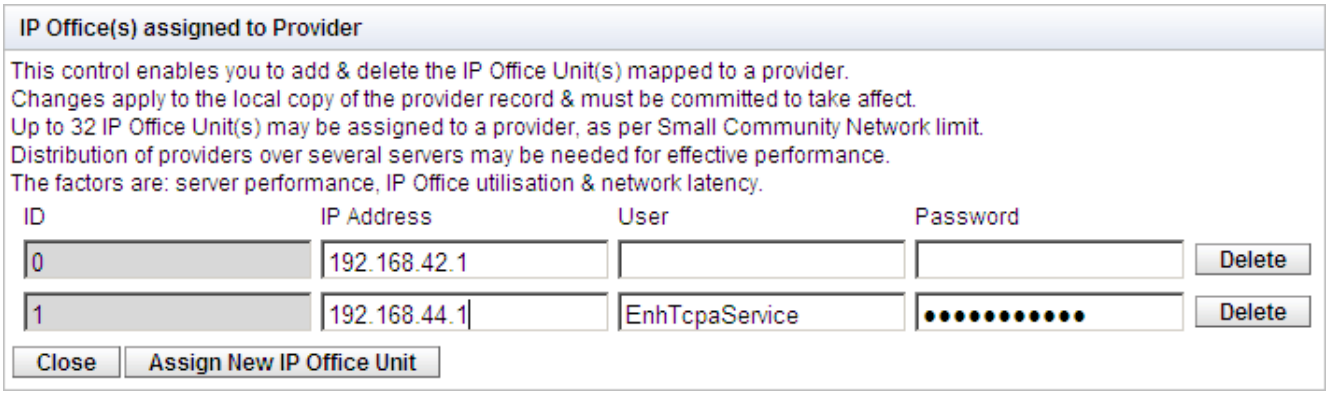
6. Next to the **Default-CSTA-Provider**, click on **Edit**.



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

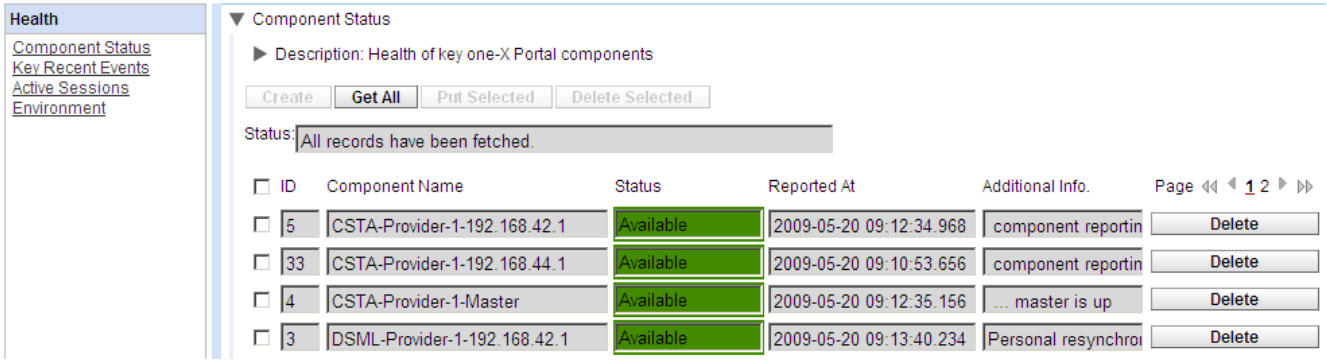


8. Click on **Assign New IP Office Unit**.



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 on **Put Selected**. This writes the new settings of the CSTA 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 6.
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.



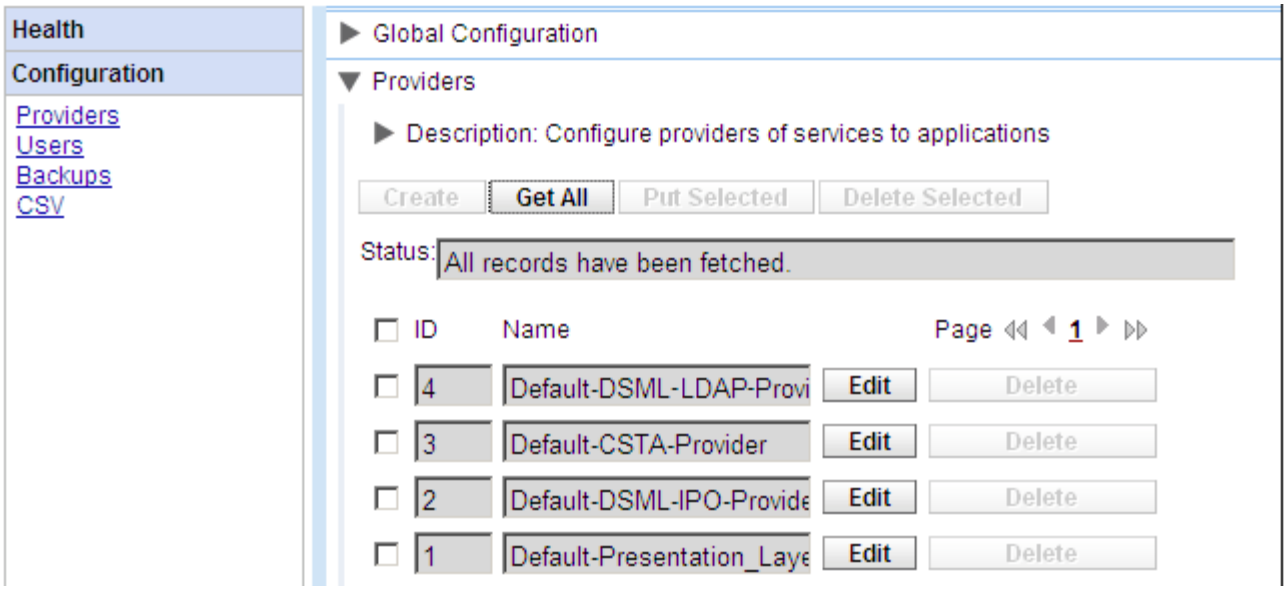
19. Select **Directory Integration**. Check that the new IP Office system's users are listed. If not, select **Directory Synchronization | Force a resynchronization with IP Office Directories** and wait 5 minutes.
20. Select **Configuration** and then **Users**. Click **Get All**. Check that the new IP Office system's users are listed.

1.4 Changing IP Office Details

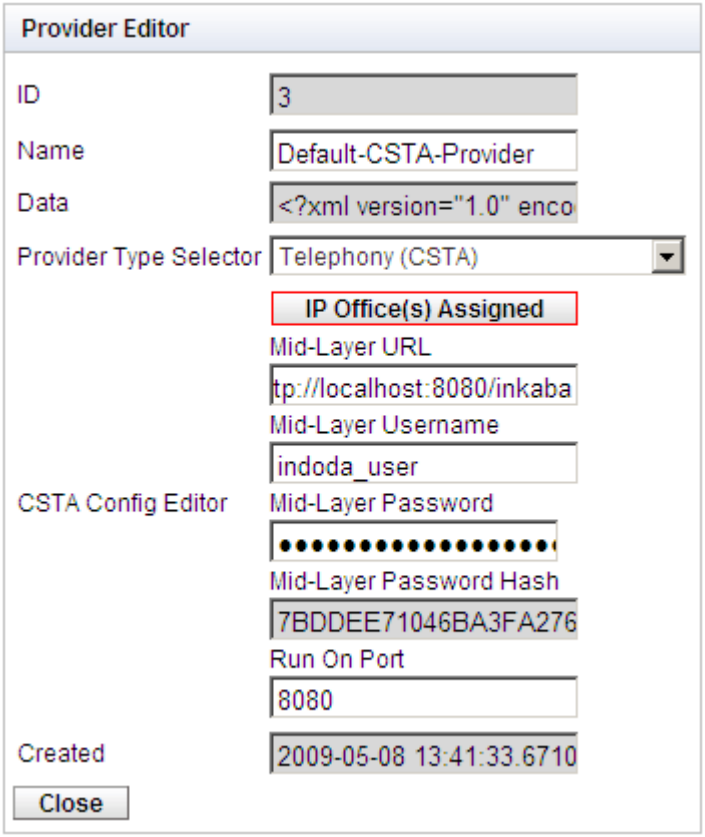
If the details (IP address, TCPA service user name or password) of an assigned IP Office are changed, the IP Office settings within the one-X Portal for IP Office providers must be updated to match.

- **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.

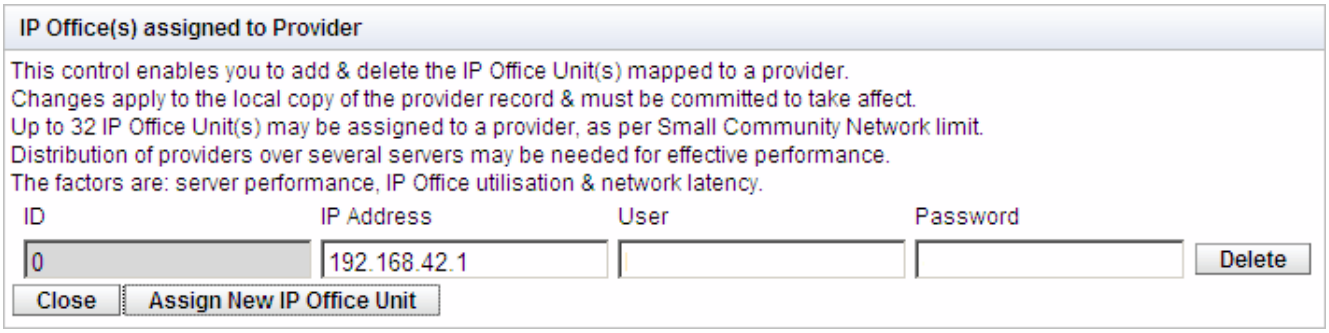
1. Log in 27 to the administrator menus.
2. If it is the IP Office IP address that has changed, check that the IP Office can be seen from the one-X Portal for IP Office server.
   a. Select **Diagnostics** and then **IP Office Connections**.
   b. Enter the **IP Address** of the target IP Office and 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 on **Put Selected**. This writes the new settings of the CSTA 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.

1.5 Adding an LDAP External Directory Source

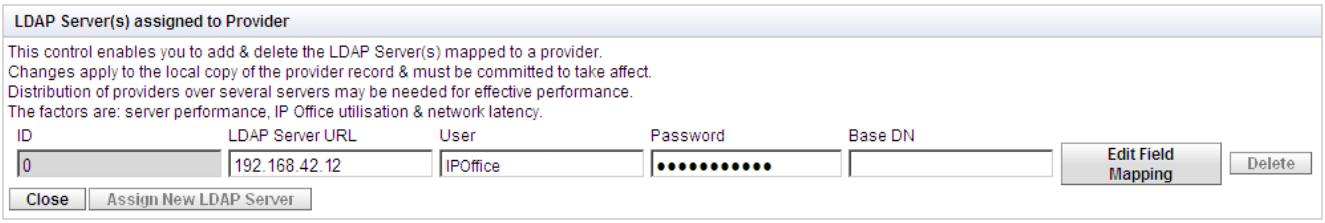
An LDAP provider is created by default during installation but not configured for connection to an LDAP sever (unless an Advanced Installation is selected and the LDAP provider settings altered). The process below changes the LDAP provider settings to allow LDAP operation.

LDAP operation can be tested through the **Directory Integration | LDAP Directory Search** 43 option in the administrator menus.

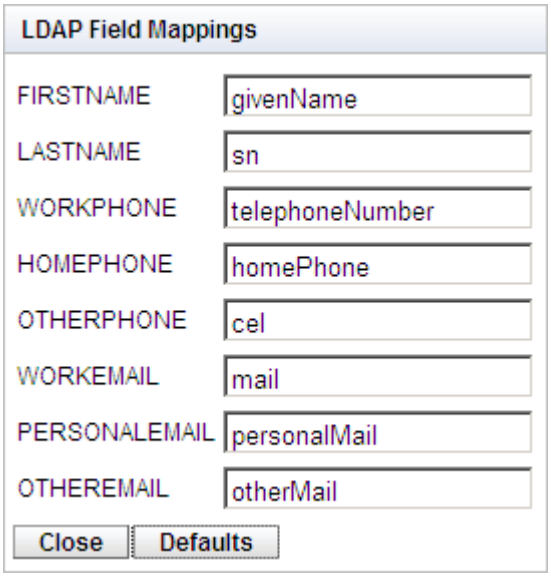
Unlike the LDAP support in the IP Office, the one-X Portal for IP Office sever does not import records from the LDAP source and then use those records as a directory. Instead, when a one-X Portal for IP Office user enters characters in the External Directory tab of the Directory gadget, the one-X Portal 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.



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.



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 6.

1.6 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 after approximately 5 minutes.

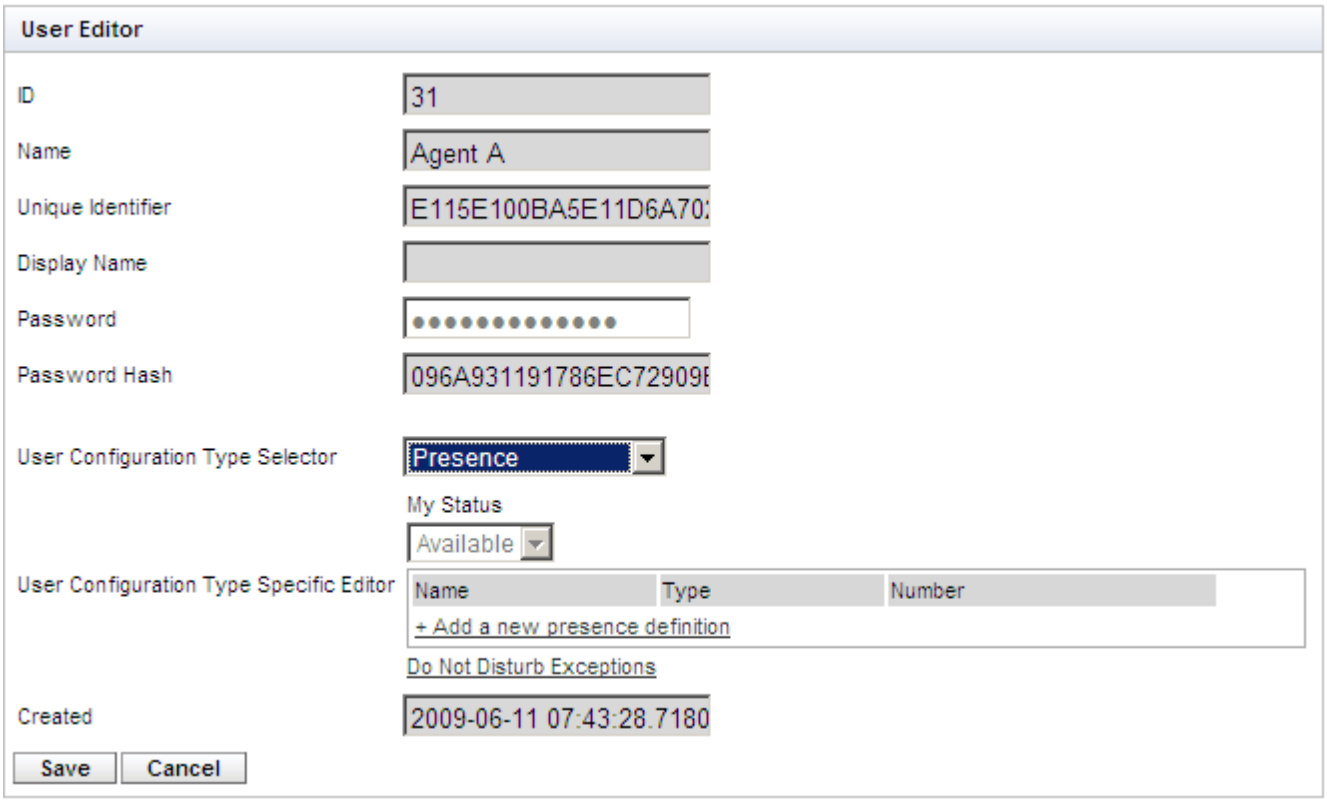
1.7 Editing User Settings

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. • Personal directory records stored by one-X Portal for IP Office can contain several numbers, with one selected as the **Primary phone** number. The matching records stored in the IP Office configuration contains just one number, that being the one selected as the **Primary phone** number. Changing the Primary phone number selection in one-X Portal for IP Office will update the number stored in the IP Office configuration to match. • The system limit for total personal directory records depends on the IP Office control unit being used. When this limit is reached, additional personal directory records are stored by one-X Portal for IP Office only. • **IP500/IP500v2:** 10800 total personal directory records. • For users with a 1608, 1616, 9500 or 9600 phones, they can edit or delete contacts through the phone's menus (primary phone number only).
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

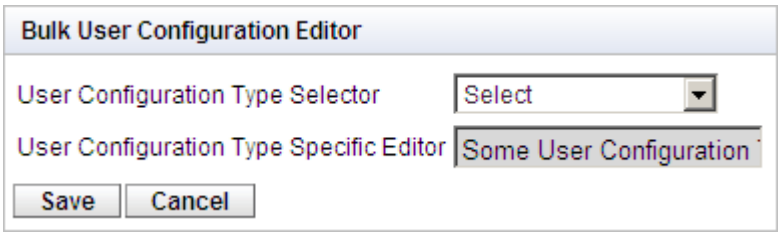
1. Select **Configuration** and then **Users**.
2. Click on **Get All**. and browse through the users.
3. Click on the **Edit** button next to the user you want to edit. The user configuration settings are displayed.



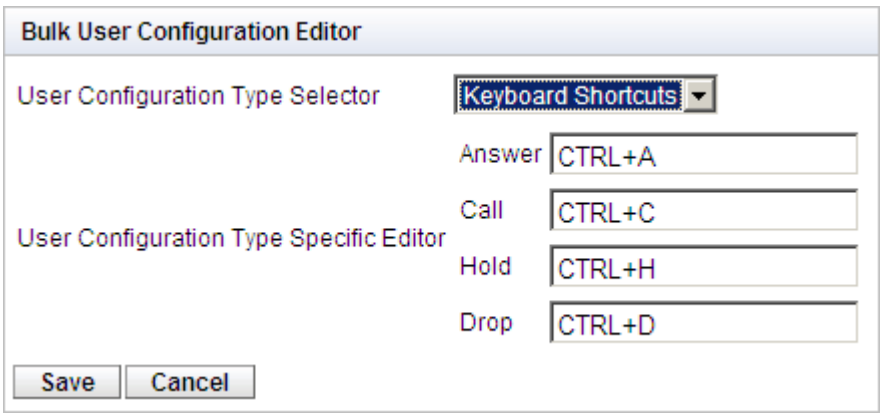
4. Use the **User Configuration Type Selector** to select the user settings you want to view/edit. If required edit the settings.
5. Click **Save**.
6. To commit the edited settings back to the one-X Portal for IP Office database, select the check box next to the user and click on **Put Selected**.

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**.



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

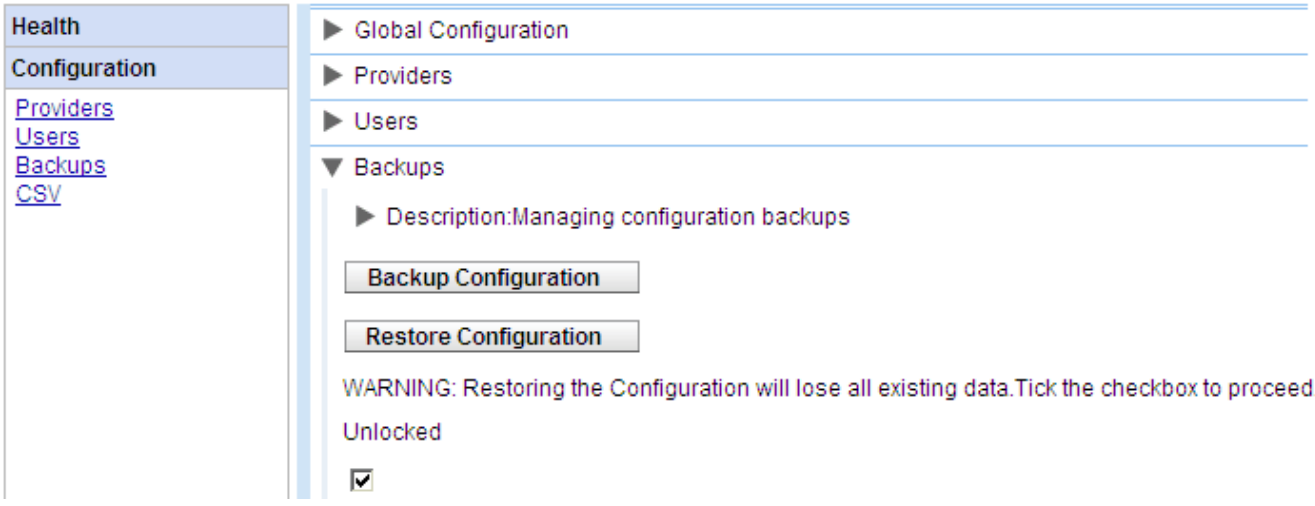


6. When you have completed editing, click **Save**.
7. Click **Put Selected** to send the changes back to the one-X Portal for IP Office database.

1.8 Backing Up the Database

You can backup the one-X Portal for IP Office database of settings. The resulting file can be restored 15.

1. Select **Configuration** and then **Backups**.

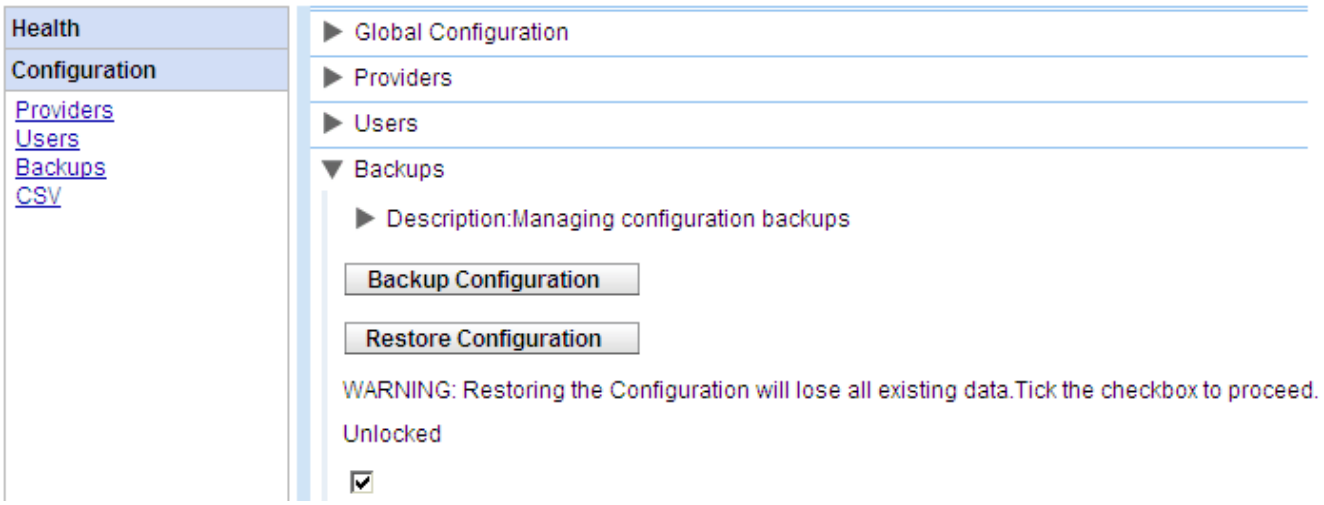


2. Click on **Backup Configuration**.
3. The configuration is backed up as ***backup.sql*** in the bin folder of the one-X Portal for IP Office application (default C:\Program Files\Avaya\oneXportal\Tomcat\appache-tomcat-6.0.18\\bin\backup.sql).

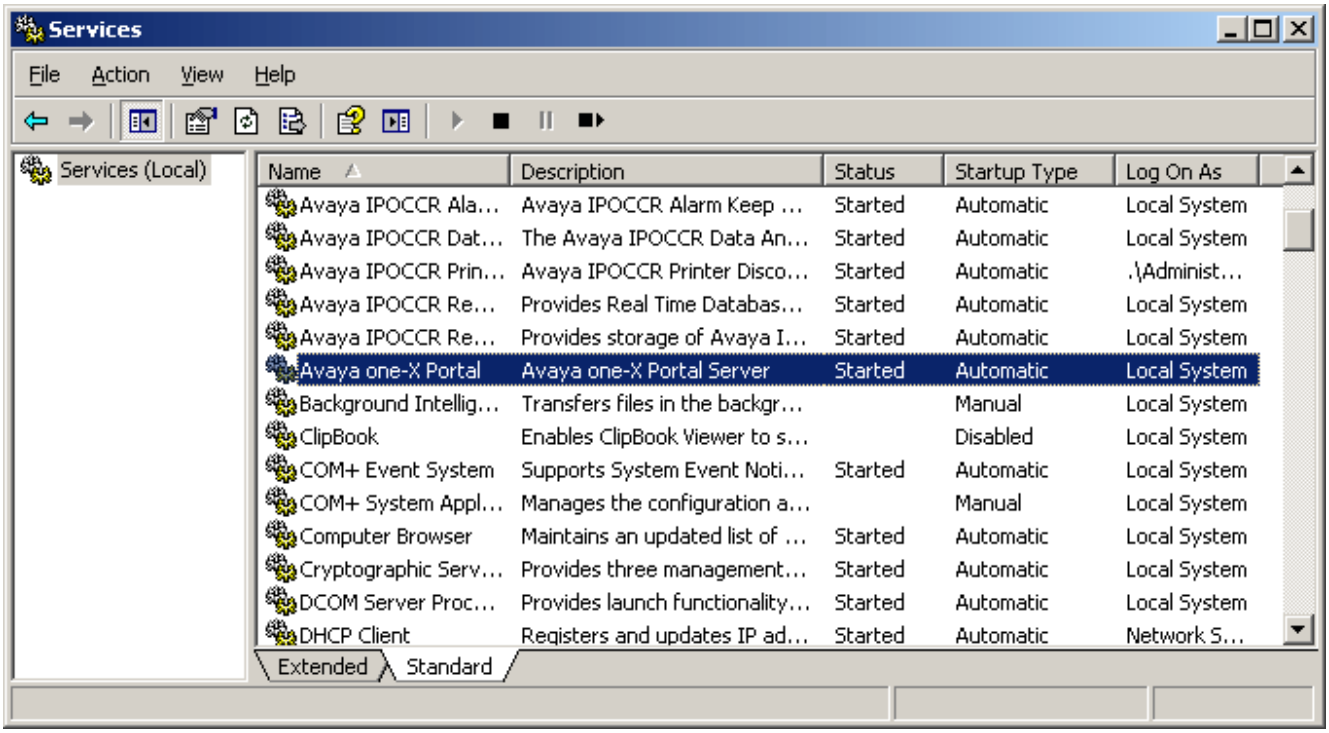
1.9 Restoring a Previous Backup

This process will override the current one-X Portal for IP Office configuration. It needs to be followed by a restart of the one-X Portal for IP Office service. It requires the one-X Portal for IP Office settings to have been previously backed up to a file called ***backup.sql*** . That file needs to be in the bin folder of the one-X Portal for IP Office application (default C:\Program Files\Avaya\oneXportal\Tomcat\appache-tomcat-6.0.18\\bin\backup.sql) for restoration.

1. Select **Configuration** and then **Backups**.



2. Select **Unlocked**.
3. Click on **Restore Configuration**.
4. The one-X Portal for IP Office server will indicate if the restore was completed.
5. In order to clear cached data and settings from the previous configuration, you must restart the one-X Portal for IP Office server service.



1.10 Checking and Updating the System Directory

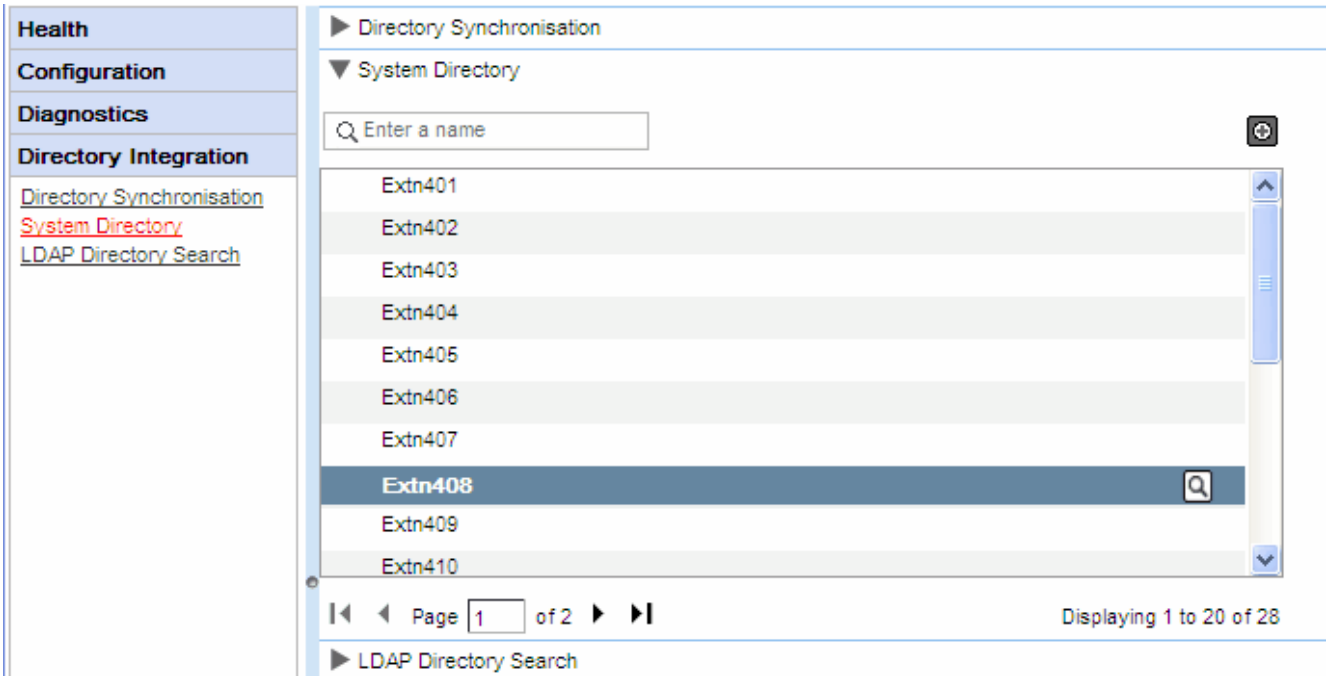
The system directory shown to one-X Portal for IP Office users is a combination of the users, groups and directory entries from all the IP Office systems with which one-X Portal for IP Office has been configured to operate.

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.

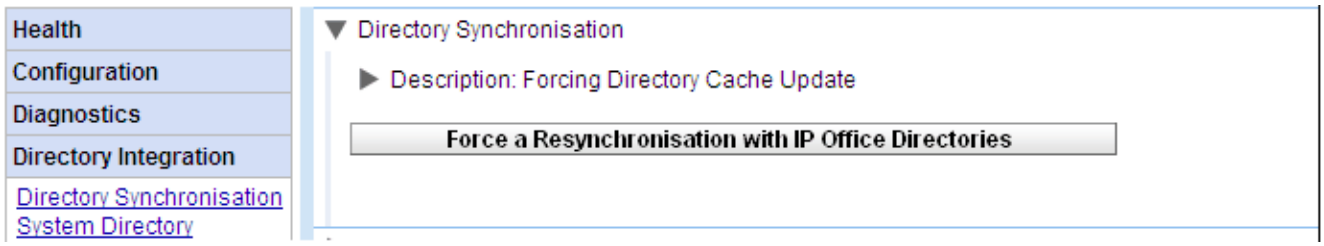
You can also search the external directory in the same way as one-X Portal for IP Office users.

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**.

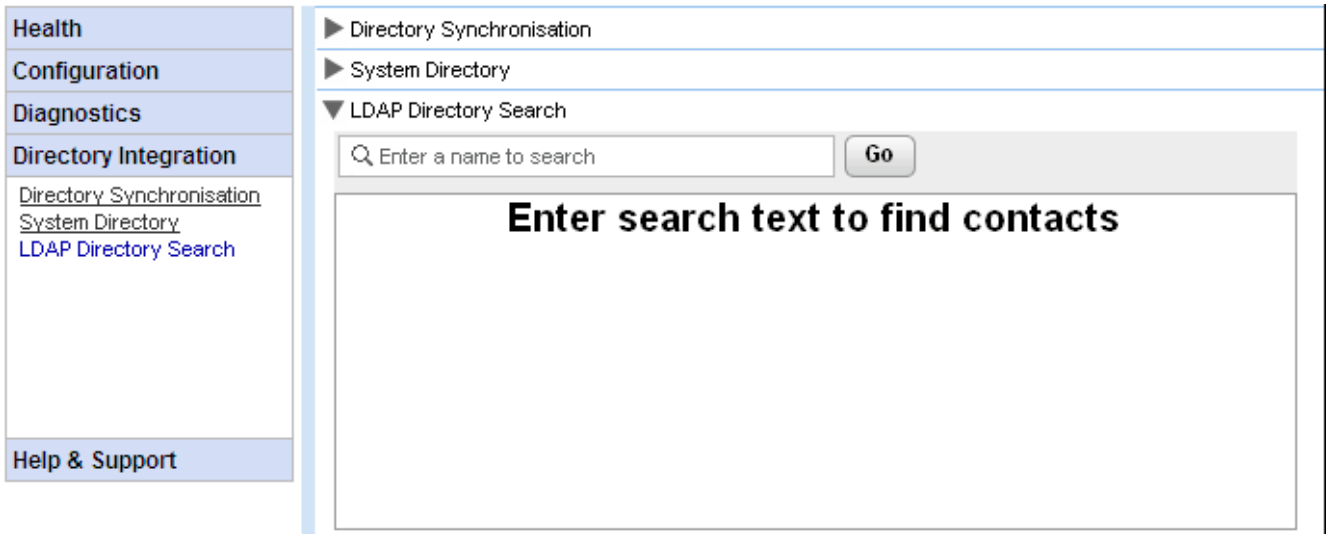


4. Click on **Force a Resynchronization to all IP Office Directories**.

1.11 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.

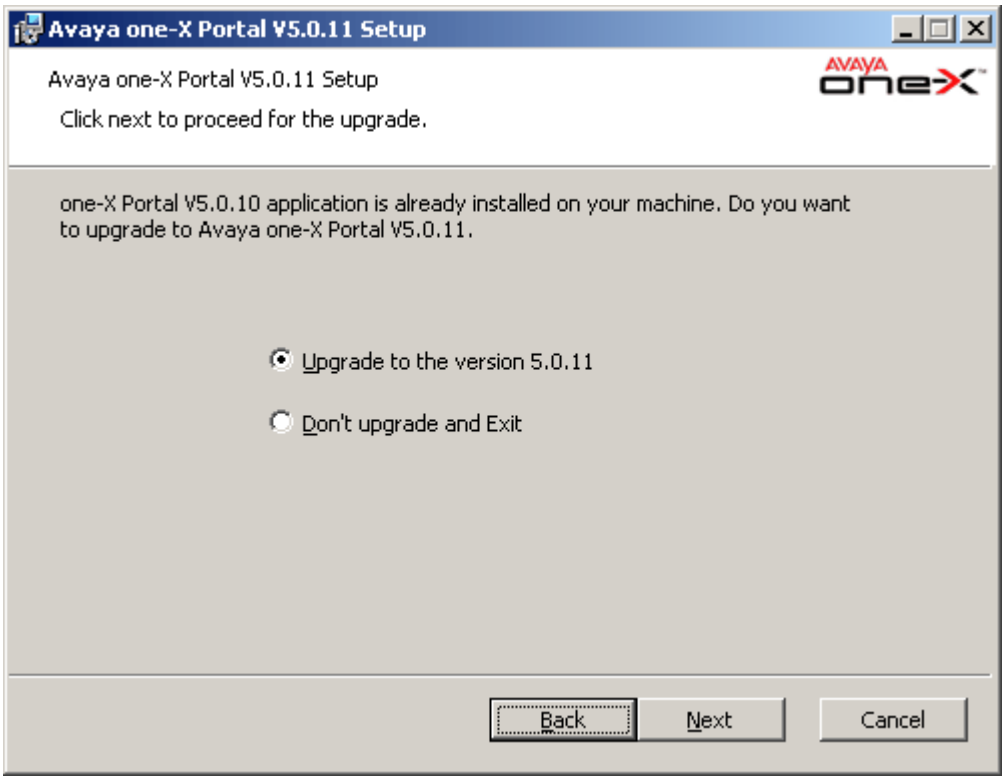


1.12 Upgrading one-X Portal for IP Office

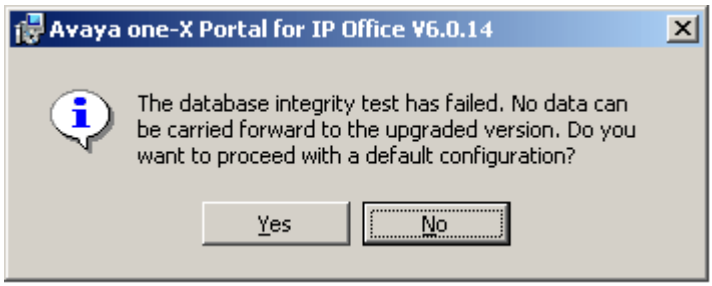
Before upgrading one-X Portal for IP Office ensure that you have read the Avaya IP Office Technical Bulletin for the release of one-X Portal for IP Office software to which you want to install or the IP Office software release in which it was included. The Technical Bulletin will include details of any 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 greyed 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 17 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. Refer to Backing Up the Database 14 for details of creating a full backup.

1.13 Downgrading one-X Portal for IP Office

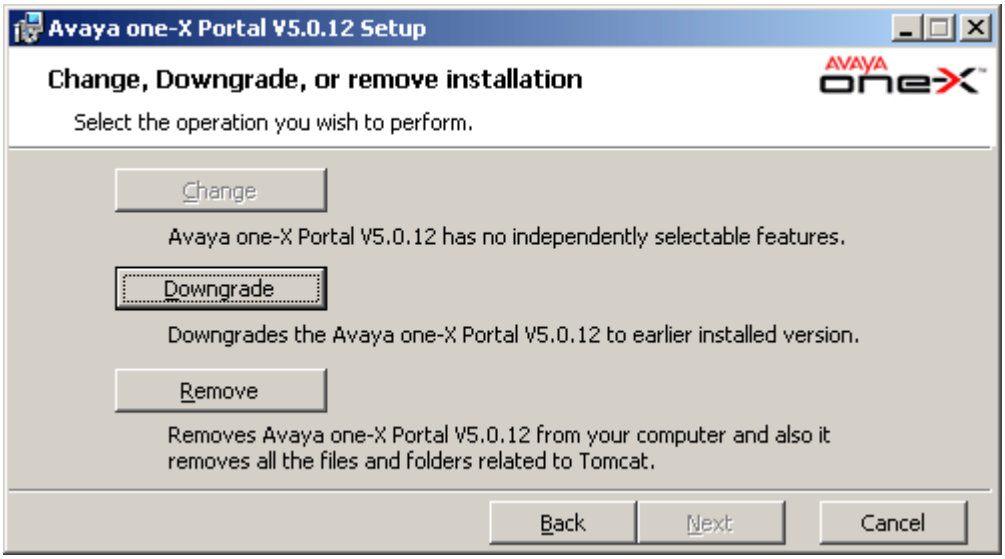
If the one-X Portal for IP Office application software has been upgraded using the upgrade process 17, it is also possible to downgrade back to the original installed version.

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.

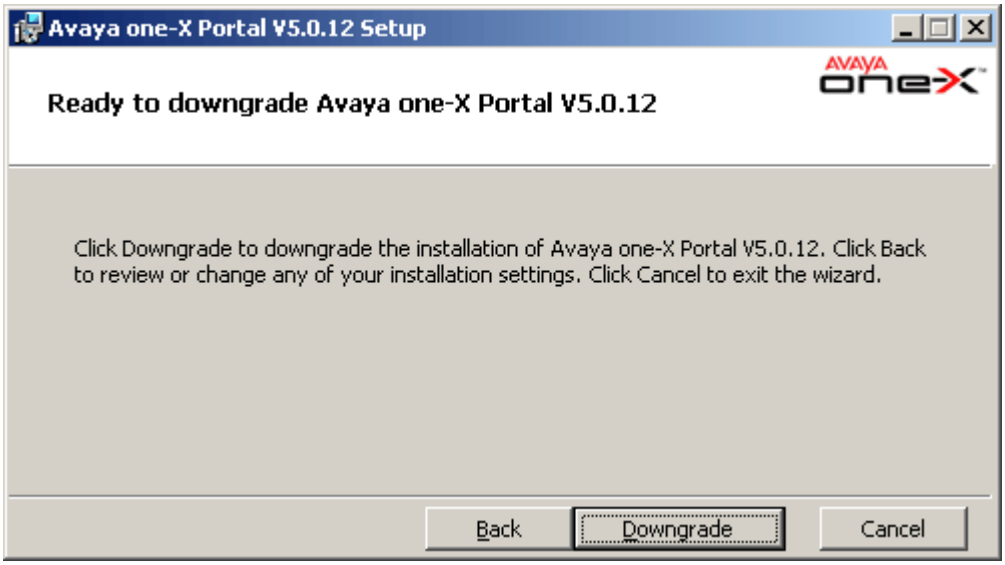
Before downgrading one-X Portal for IP Office ensure that you have read the Avaya IP Office Technical Bulletin for the one-X Portal for IP Office software releases. The Technical Bulletin will include details of any special requirements and additional steps that are not in this documentation.

- **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 6.

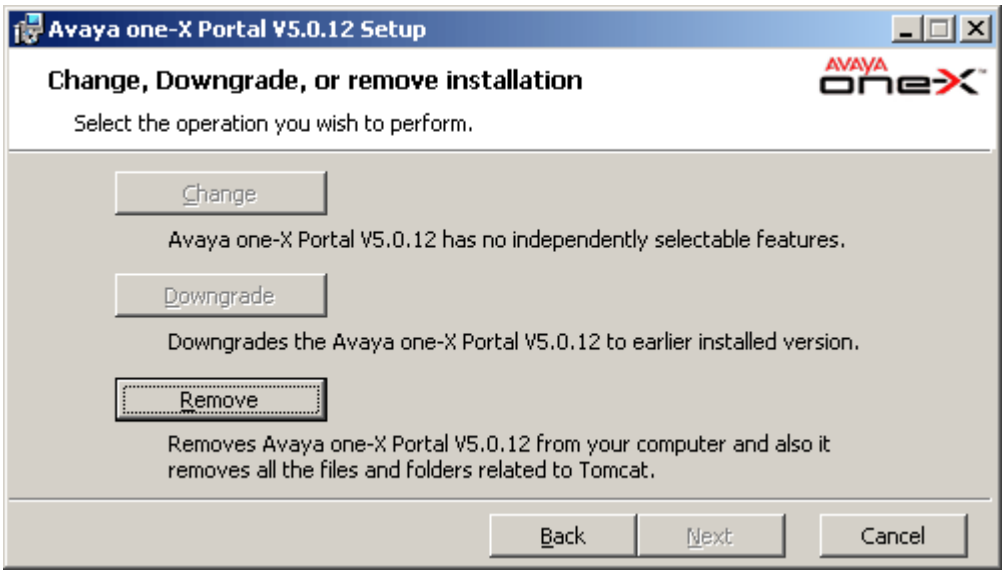
1.14 Removing one-X Portal for IP Office

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

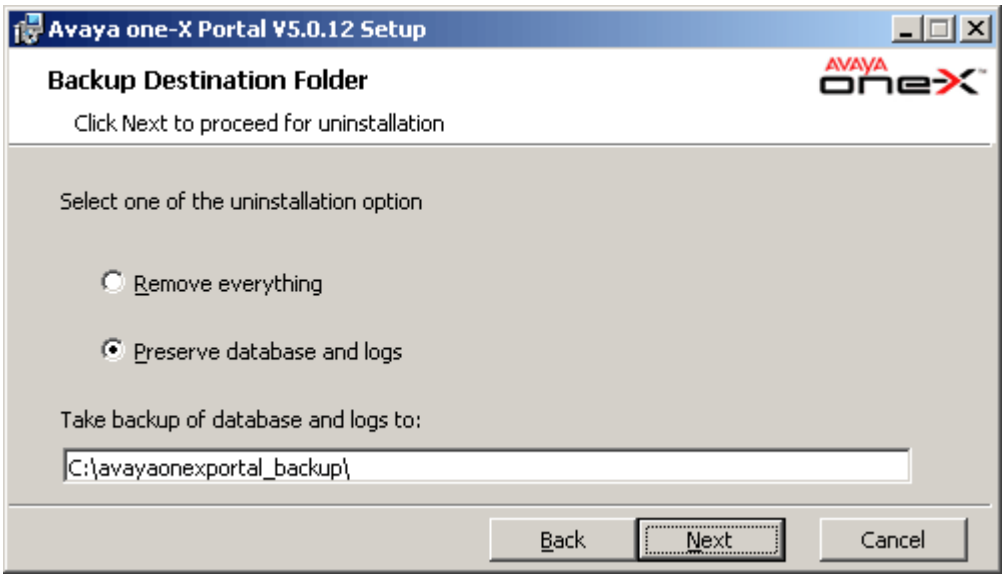
Uninstalling one-X Portal for IP Office

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

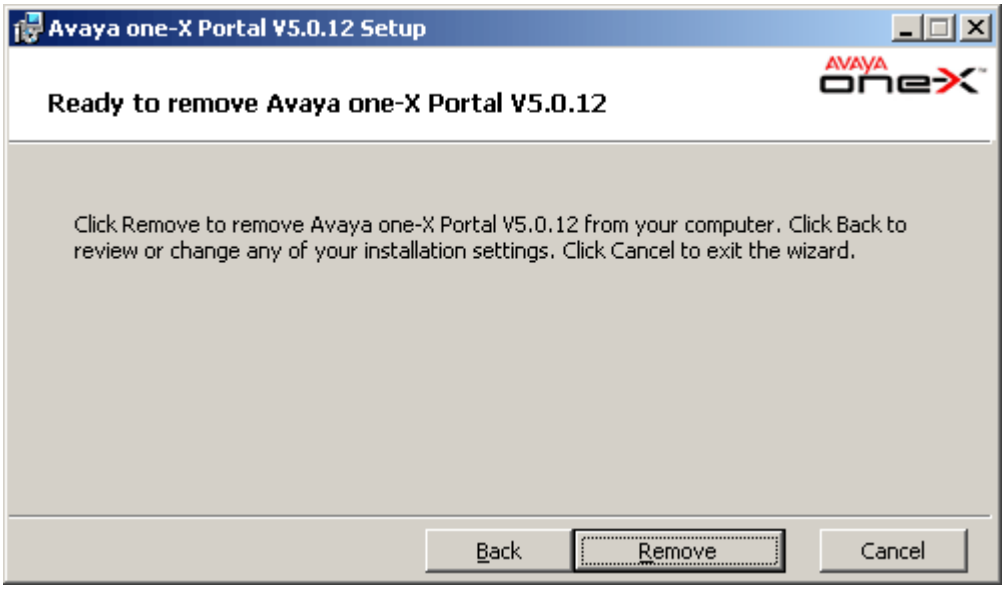
1. Select **Start | All Programs | IP Office | one-X Portal | Uninstall one-X Portal**.



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:\avayaonexportal_backup***.

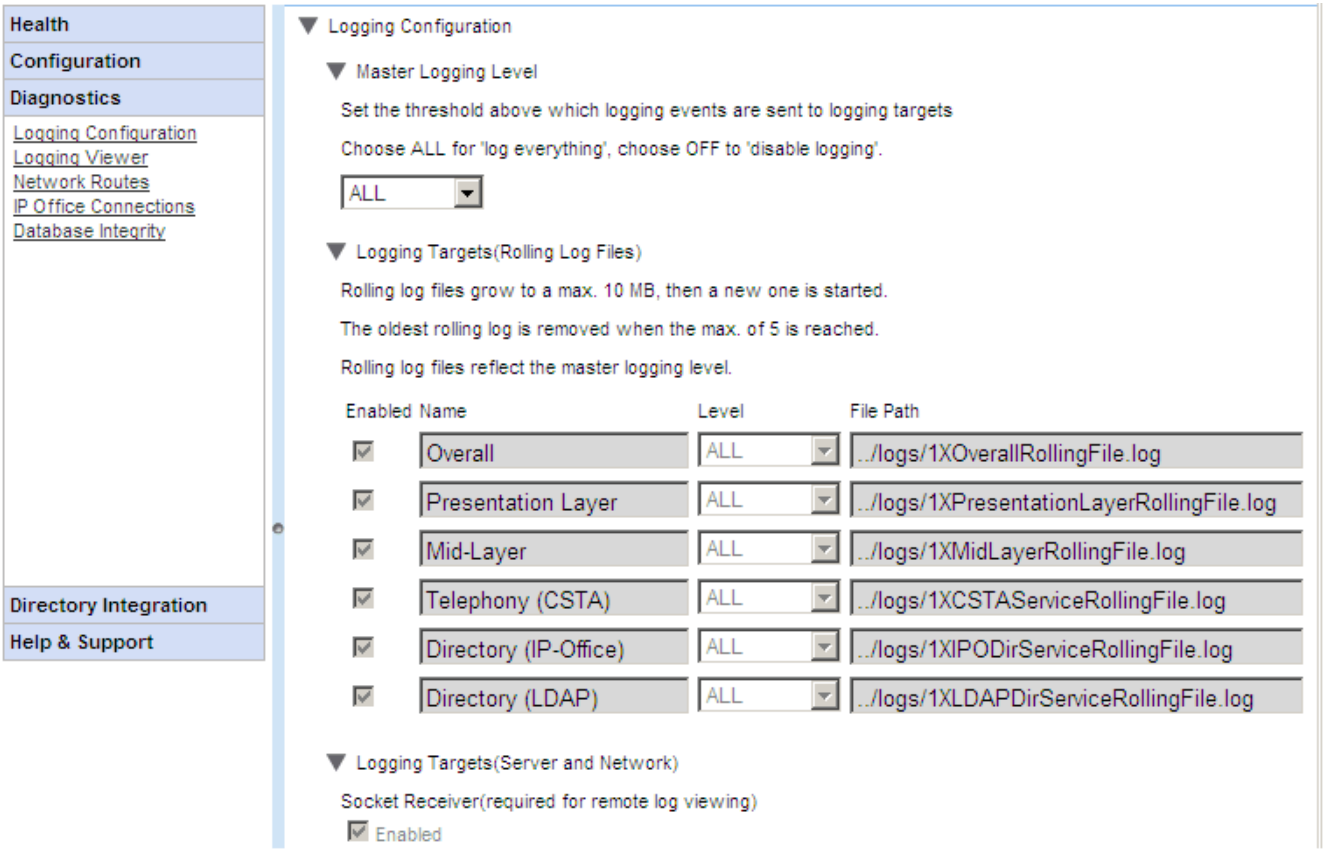
1. Start the standard Windows Control Panel.
2. Select **Add or Remove Programs**.
3. Select **one-X Portal** and then click **Remove**.
   - If the one-X Portal for IP Office has been upgraded at some stage, there will be a program entry for both the original one-X Portal for IP Office installation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

1.15 Remote Logging

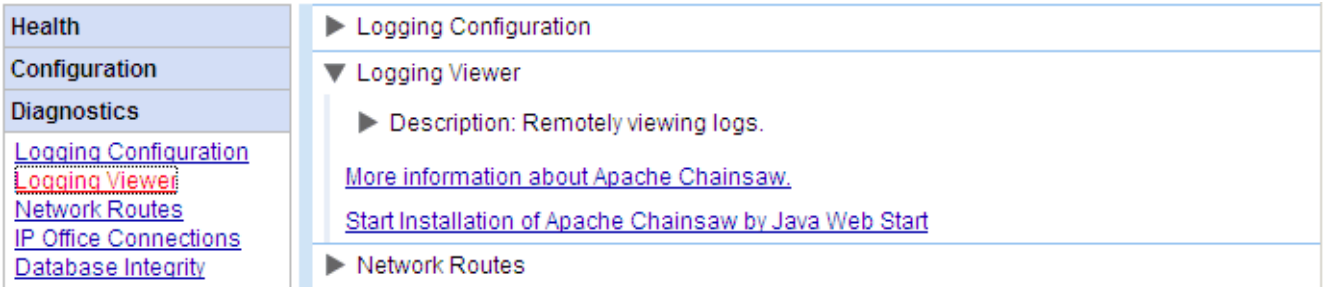
The one-X Portal for IP Office server can be configured to allow logging applications to connect on port 4560 to collect logging output. The output is in Log4j format. The one-X Portal for IP Office server administrator interface includes links to install Apache Chainsaw.

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

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



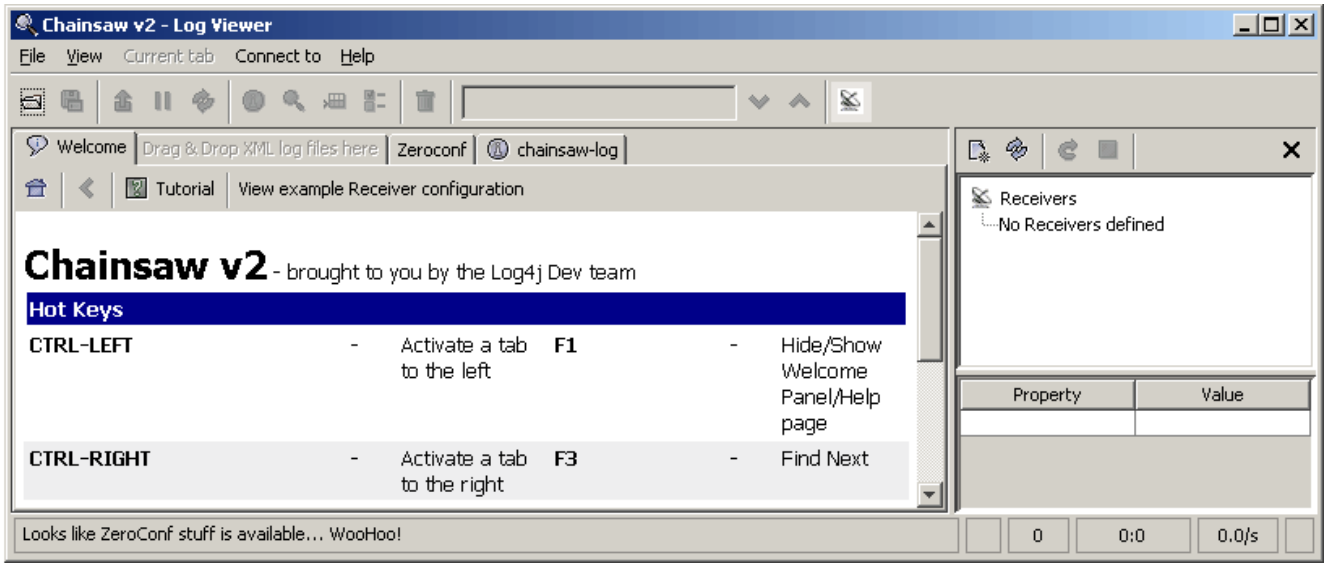
2. Check that **Socket Receiver** is enabled.
3. Select **Logging Viewer**.



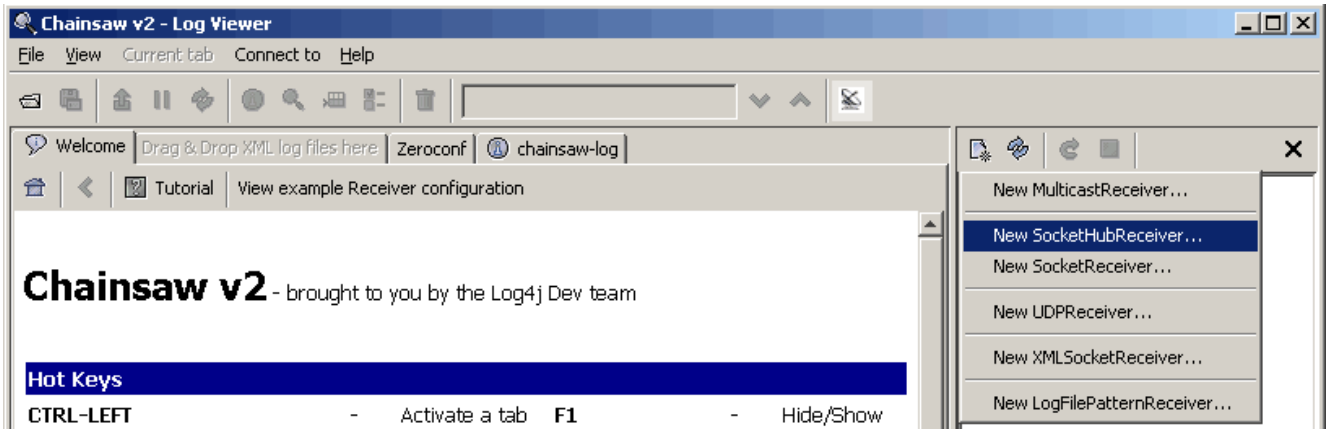
4. Click on **Start Installation of Apache Chainsaw by Java Web Start**.

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

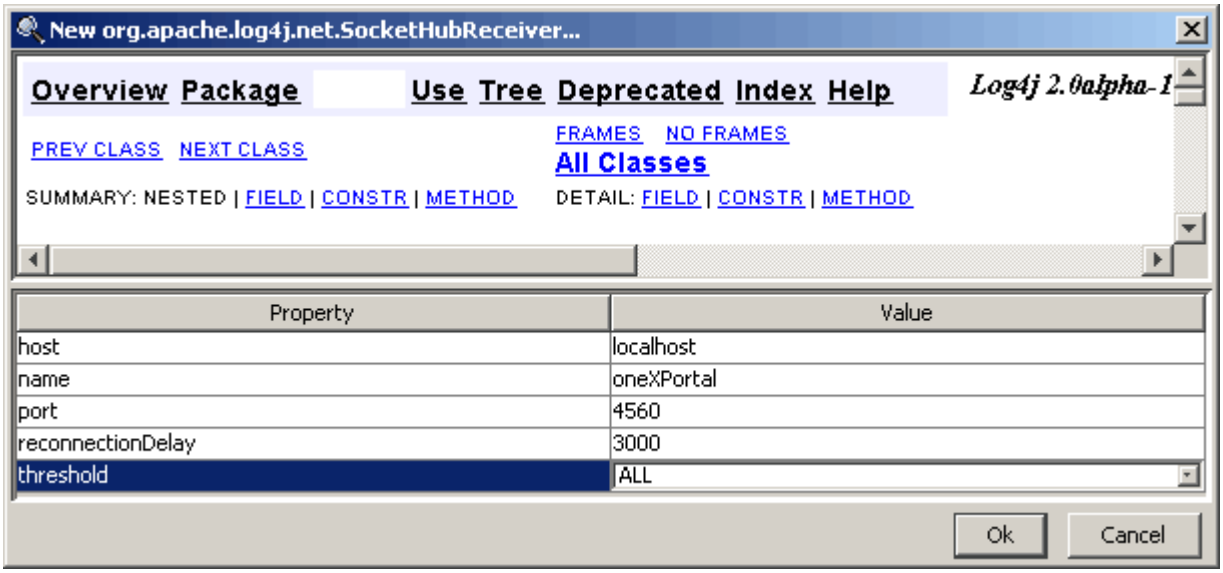
6. The Receivers panel should be visible on the right. If not click on the button in the top toolbar.



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



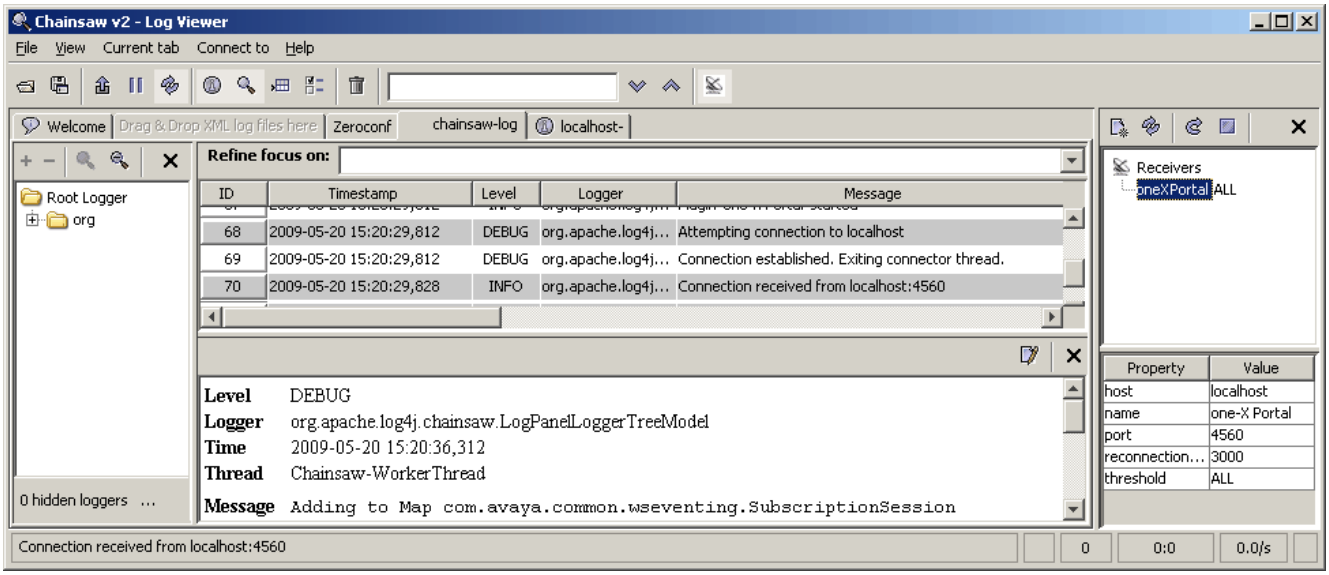
8. Enter the details for the one-X Portal for IP Office server.



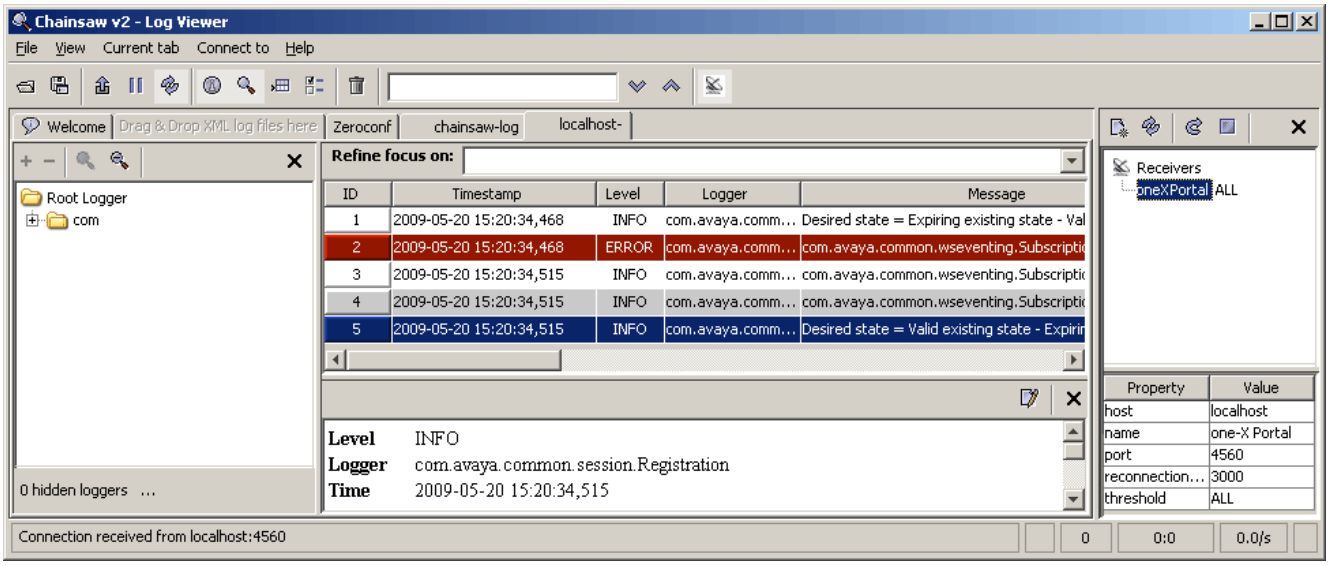
host	This field sets the address of the one-X Portal for IP Office server. In the example above chainsaw is being run on the one-X Portal for IP Office server PC.

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

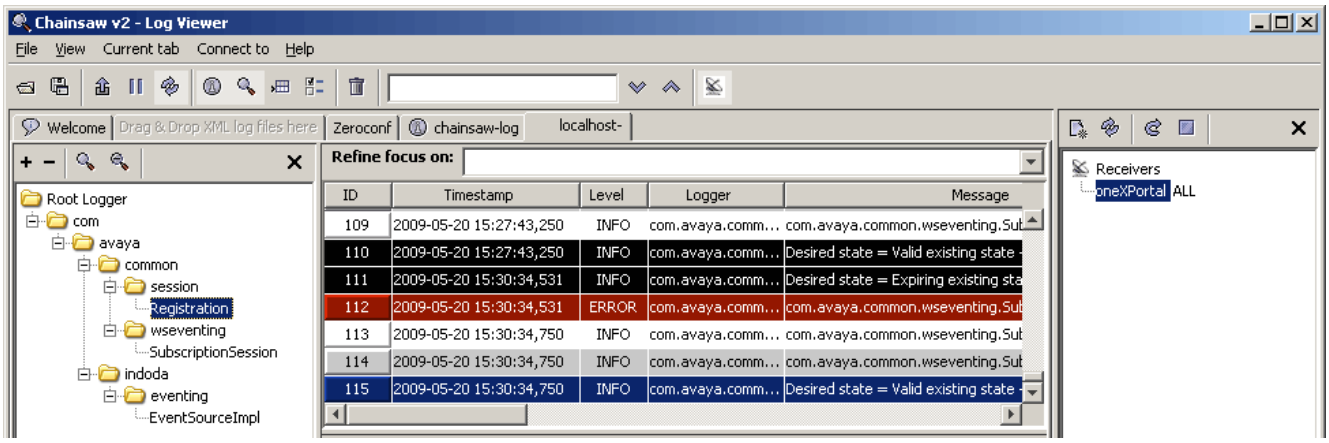
9. When you have completed the fields, click OK. After a few seconds the receiver should start and connect to the one-X Portal for IP Office server. The process will appear as log events on the chainsaw-log tab and when completed the receiver will be displayed as a new tab.



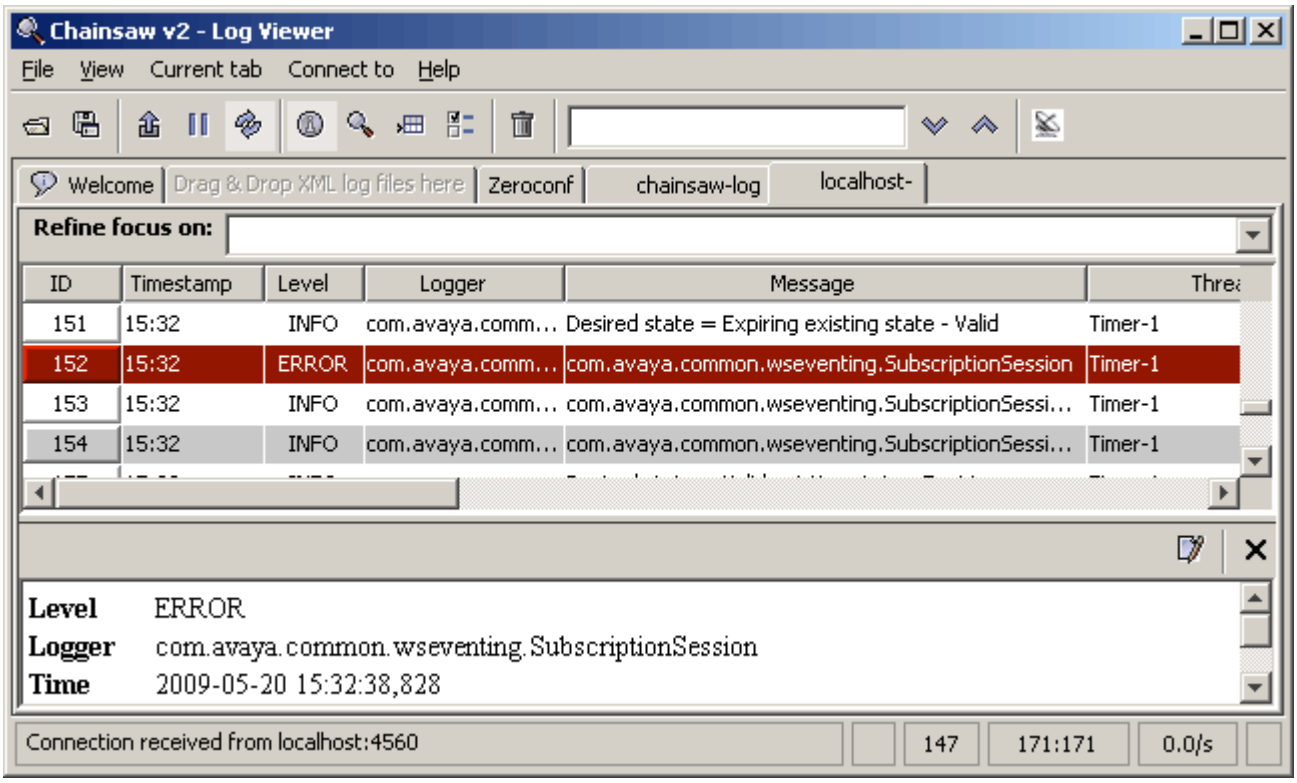
10. Click on the new receiver tab to view the one-X Portal for IP Office log records.



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



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



1.16 Troubleshooting

Version Mismatch Problem

Symptoms	• Database integrity 41 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 | Unistall V***X.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	1. Remove one-X Portal for IP Office 18. 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 a locked. 3. Install the new version of one-X Portal for IP Office.

one-X Portal for IP Office Does Not Start

Symptoms	• 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	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 18. 4. Install one-X Portal for IP Office.

1.17 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.

1.18 Enabling or Disabling Openfire Admin Console

You can use the *Command Prompt* in Windows and *Linux Terminal* in Linux to enable or disable the Openfire admin console.

To enable or disable the Openfire admin console (For Windows):

1. In *Command Prompt*, navigate to the path **<one-X Portal for IP Office install dir>/openfire/bin**.
2. To enable the Openfire admin console, execute the batch file **AdminConsoleManager.bat** with the **enable** option.

For example, **AdminConsoleManager.bat enable**.

3. To disable the Openfire admin console, execute the batch file **AdminConsoleManager.bat** with the **disable** option.

For example, **AdminConsoleManager.bat disable**.

To enable or disable the Openfire admin console (For Linux):

1. In *Linux Terminal*, navigate to the path **opt/Avaya/oneXPortal/openfire/bin**.
2. To enable the Openfire admin console, execute the script **AdminConsoleManager.sh** with the **enable** option.

For example,**./AdminConsoleManager.sh enable**.

3. To disable the Openfire admin console, execute the script with **AdminConsoleManager.sh** with the **disable** option.

For example,**./AdminConsoleManager.sh disable**.

The aforementioned changes are reflected when you restart the one-X Portal for IP Office.

Chapter 2. Administration

2. 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 28	Component Status 28	List the last status change of the server components.
	Key Recent Events 28	View the last 20 events on the server.
	Active Sessions 29	Show how many sessions are cached by one-X Portal for IP Office.
	Environment 29	Show a summary of the one-X Portal for IP Office server PC.
Configuration 30	Providers 30	View and edit the providers.
	Users 34	View and edit user one-X Portal for IP Office settings.
	Backups 36	Backup the one-X Portal for IP Office configuration database. Also restore a previous backup.
	CSV 36	Export the user directory and system directory.
Diagnostics	Logging Configuration 39	Configure the level and method of logging supported.
	Logging Viewer 40	Install and launch Chainsaw for log viewing.
	Network Routes 40	Test the IP connection path to an IP address.
	IP Office Connections 40	Test the IP connection path to an IP Office.
	Database Integrity 41	Test the structure of the database.
Directory Integration 42	Directory Synchronization 42	Force a system directory update by the server.
	System Directory 43	View the one-X Portal for IP Office system directory.
	LDAP Directory Search 43	View the external directory for which the one-X Portal for IP Office server has been configured.
Help & Support 48	Help 48	Access one-X Portal for IP Office help installed on the server.
	Avaya Support 48	Access the Avaya support web site for Avaya applications.
	About 48	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.

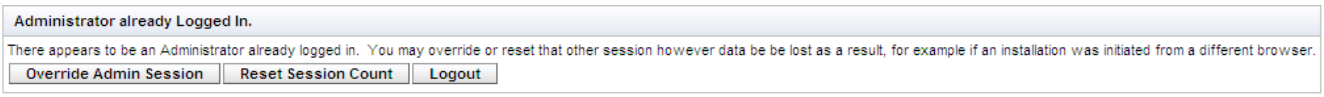
2.1 Log in

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 8.0 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, a warning appears:



one-X Portal for IP Office 8.0 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:

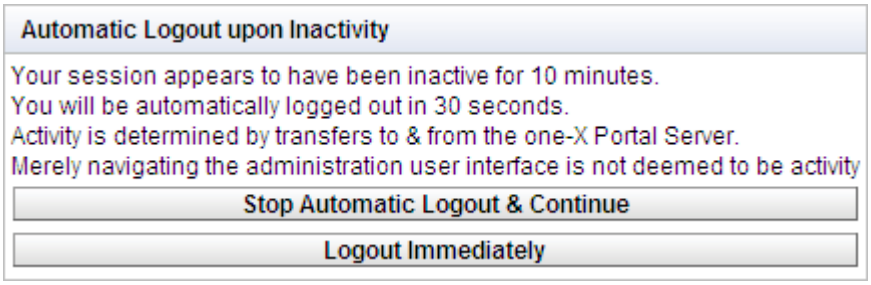
1. Log in as an Administrator.
2. Choose the language listed under **Language**.
3. Click **Login**.

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.

2.2 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.

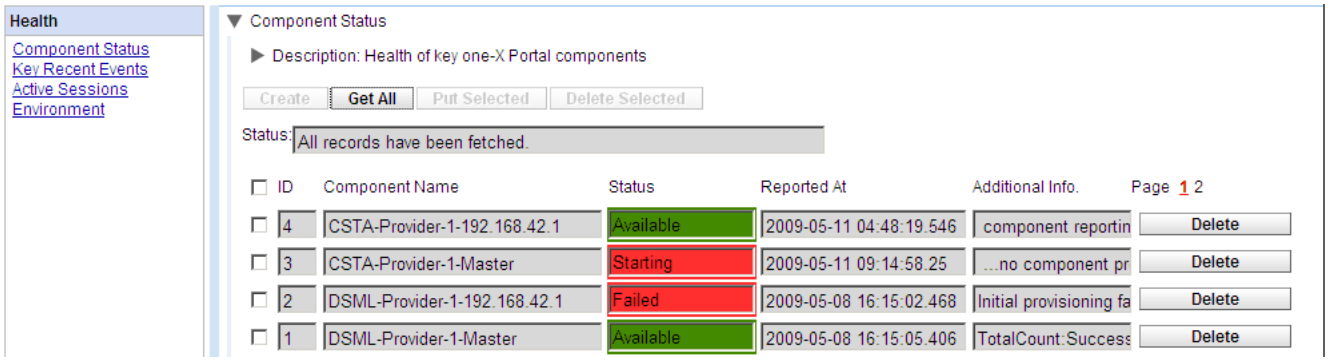


2.3 Health

2.3.1 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.

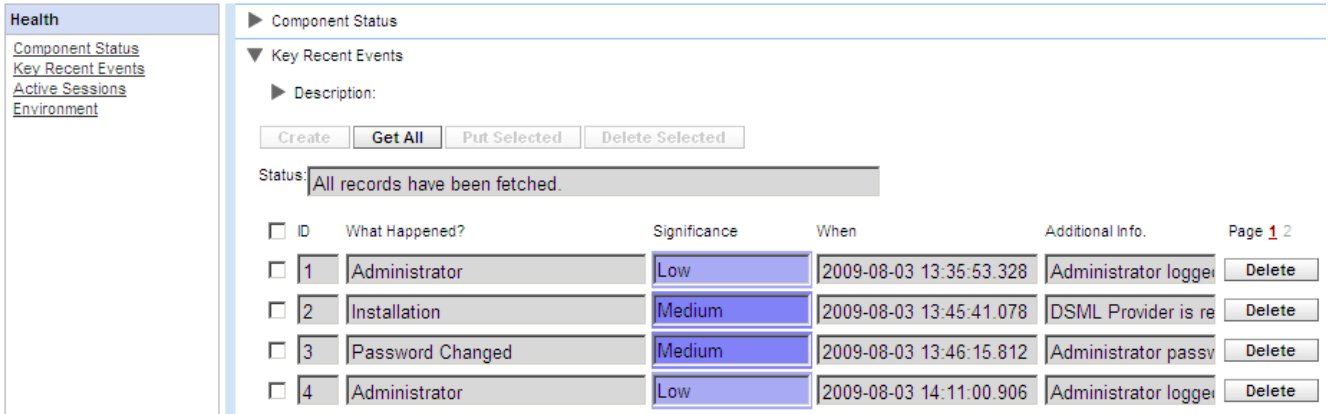
There should be a CSTA Provider Master plus 1 CSTA Provider for each IP Office system assigned, a DSML Provider Master plus 1 DSML Provider for each IP Office, and one DSML LDAP Provider.



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

2.3.2 Key Recent Events

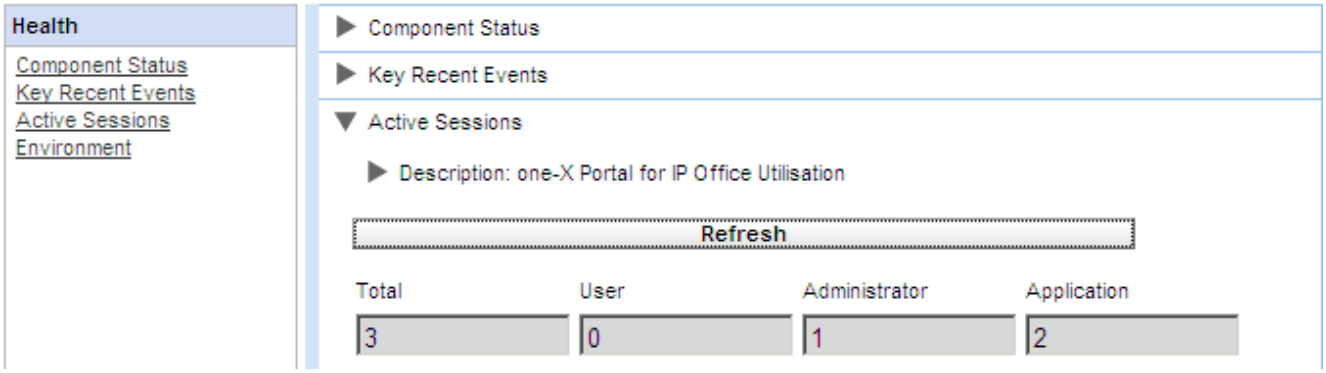
The **Key Recent Events** menu displays the last 20 events recorded by the one-X Portal for IP Office application. These can be actions performed by the one-X Portal for IP Office service and also administration actions such as administrator log in/log out, administrator password changes, provider changes,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



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

2.3.3 Active Sessions

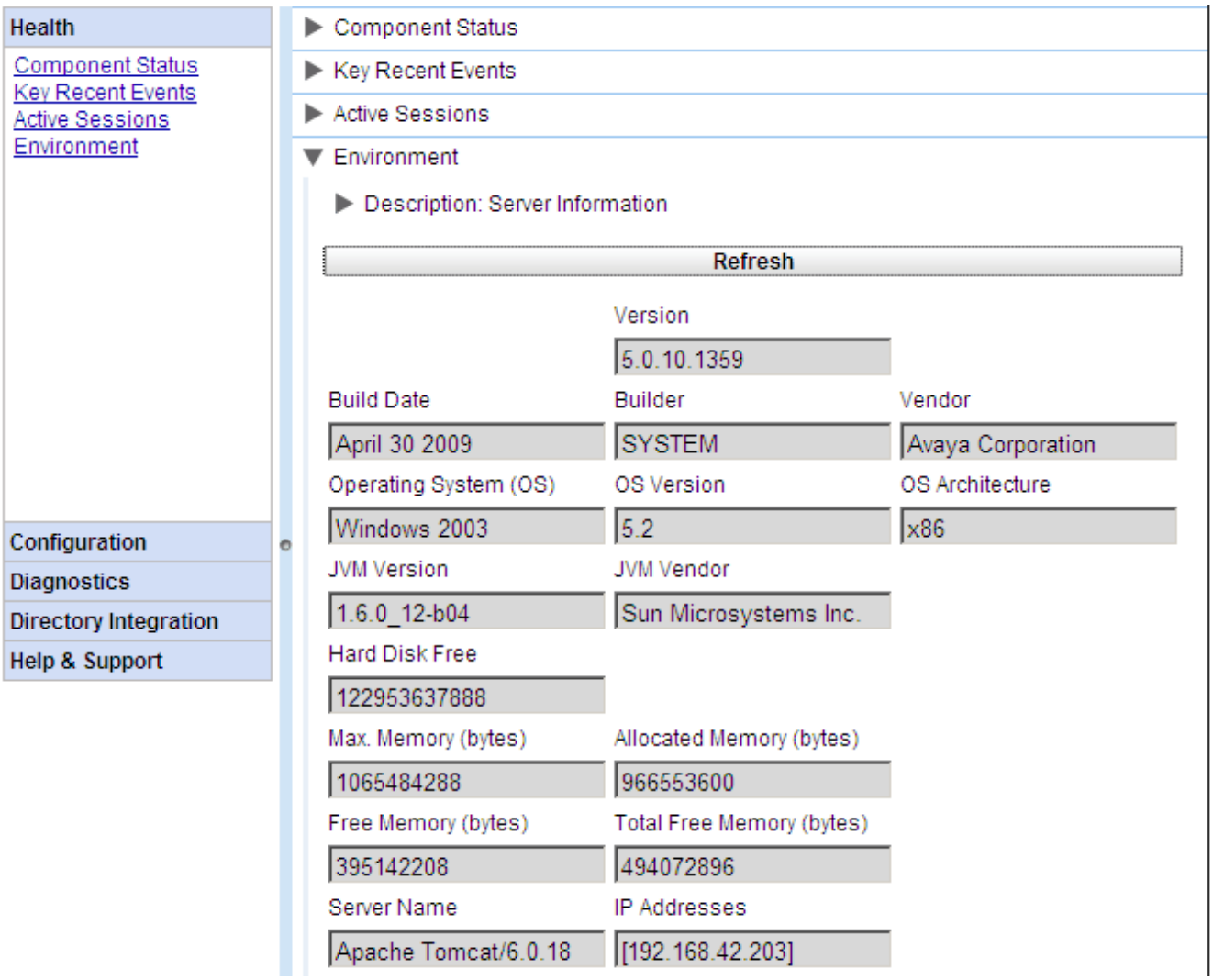
The **Active Session** menu displays the number of current browser sessions connected to the one-X Portal for IP Office server.



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

2.3.4 Environment

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

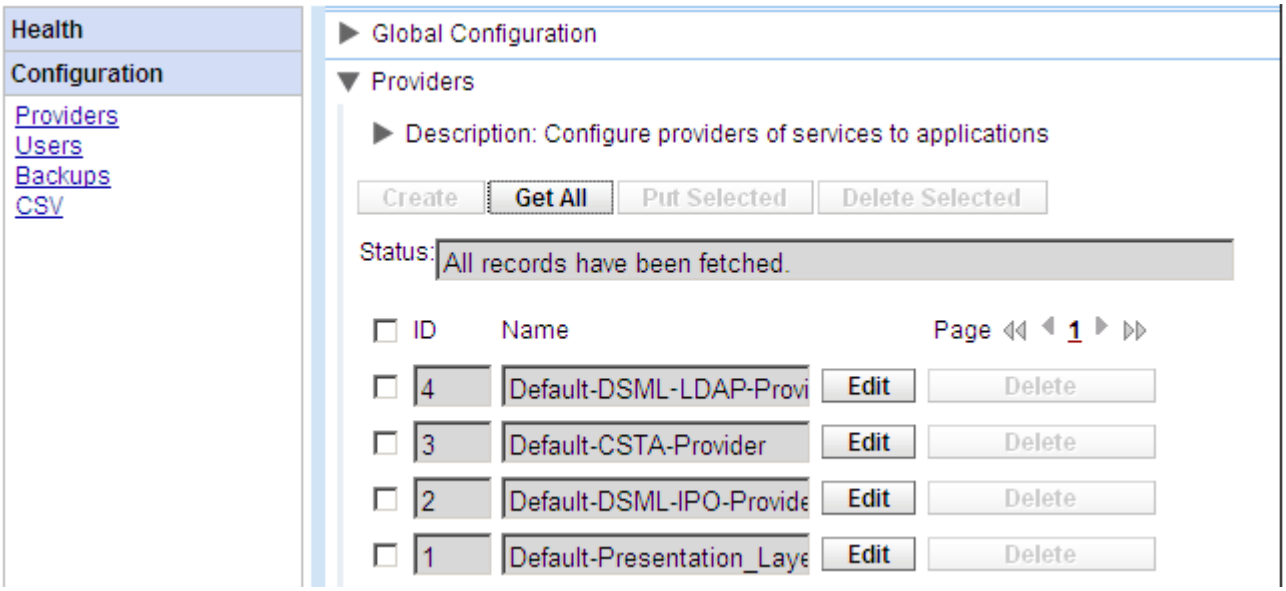


1. Select **Health** and then **Environment**.
2. Click on **Refresh**.

2.4 Configuration

2.4.1 Providers

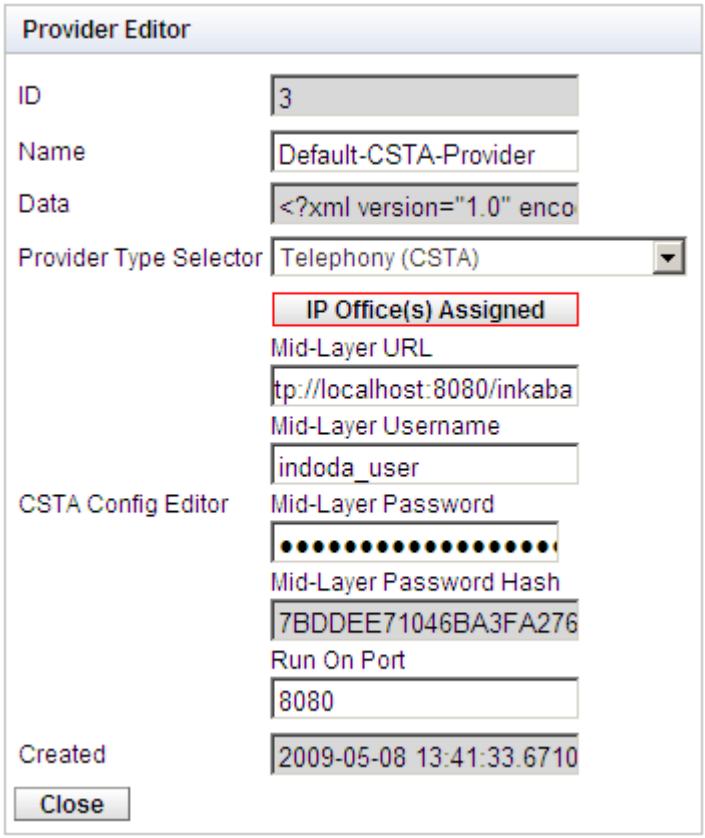
This menu shows the service providers configured on the one-X Portal for IP Office server.



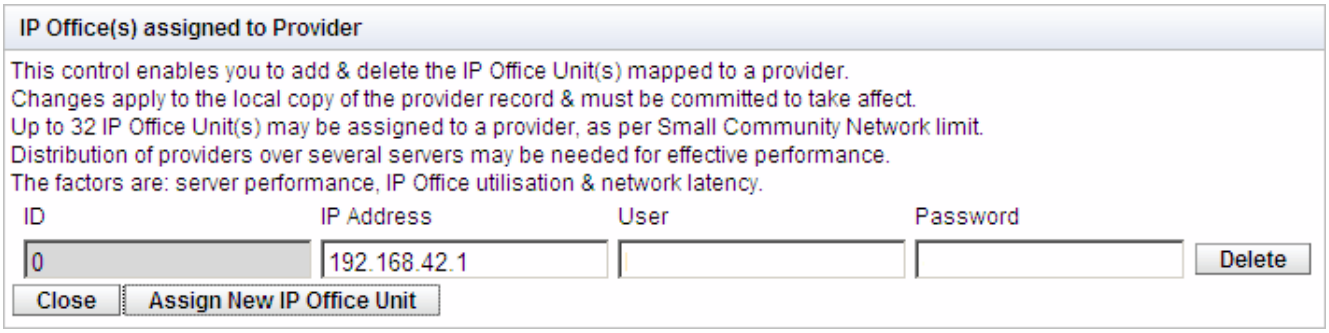
During one-X Portal for IP Office, one provider of each type is created. The Providers menu allows editing of which IP Offices and LDAP servers are assigned to the providers.

2.4.1.1 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.



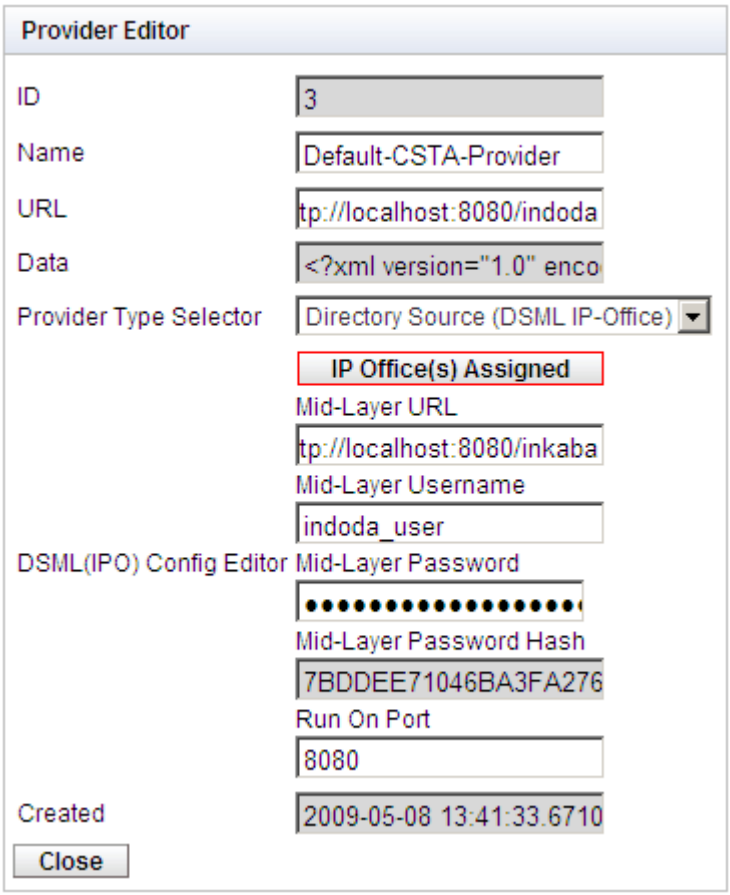
The **IP Office(s) Assigned** button can be used to display which IP Office systems are assigned to the provider. Additional IP Offices can be assigned while existing assignments can be deleted. Each IP Office system should only be assigned to one provider of each type (CSTA and DSML) at any time.



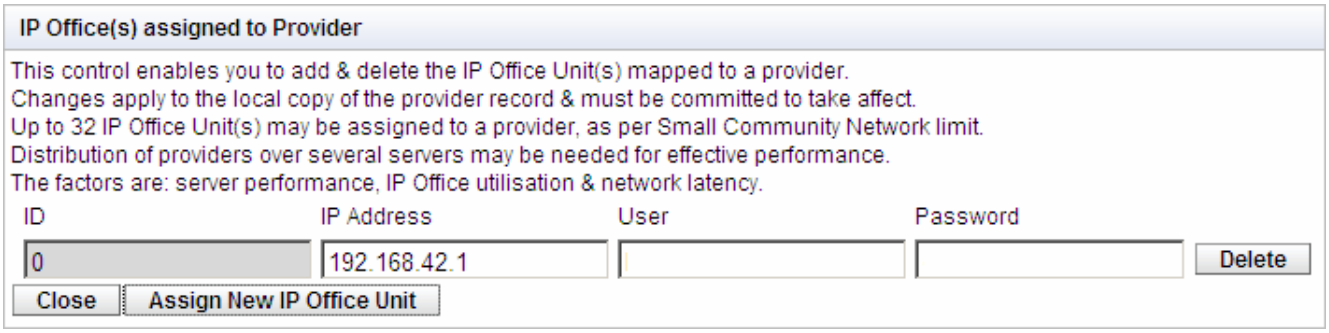
The **User** and **Password** details used must match the TCPA service user configured in the IP Office system's security configuration settings.

2.4.1.2 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.



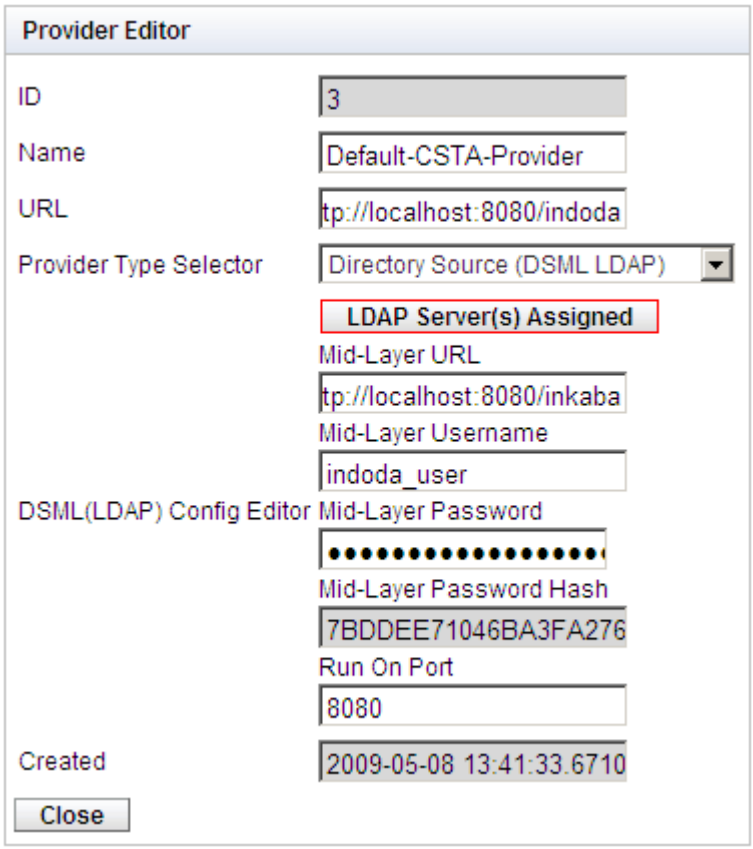
The **IP Office(s) Assigned** button can be used to display which IP Office systems are assigned to the provider. Additional IP Offices can be assigned while existing assignments can be deleted. Each IP Office system should only be assigned to one provider of each type (CSTA and DSML) at any time.



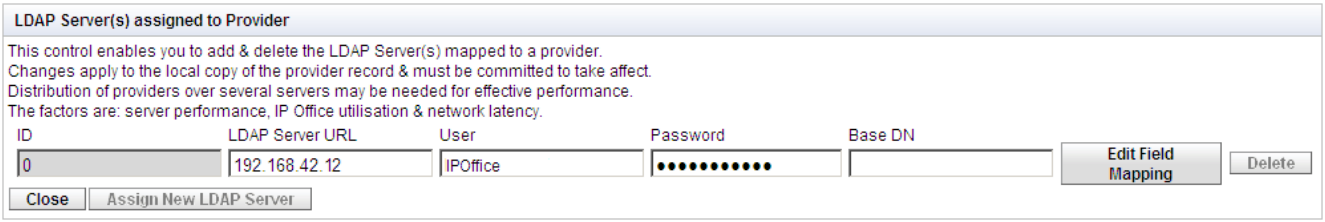
The **User** and **Password** details used must match the TCPA service user configured in the IP Office system's security configuration settings.

2.4.1.3 DSML (LDAP) Provider

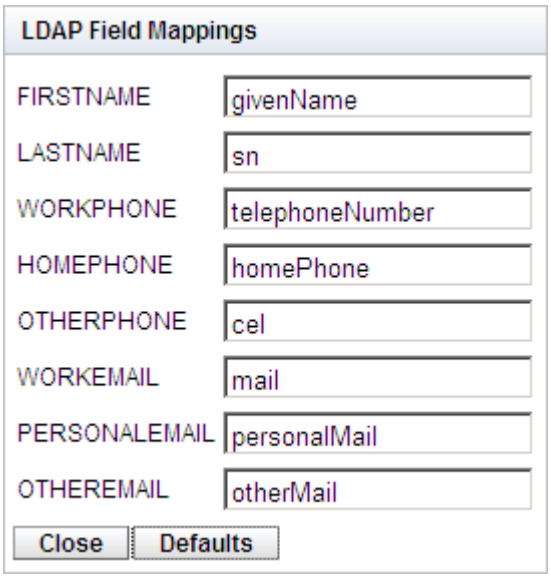
The settings below are shown for a **Directory (DSML LDAP)** provider.



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.



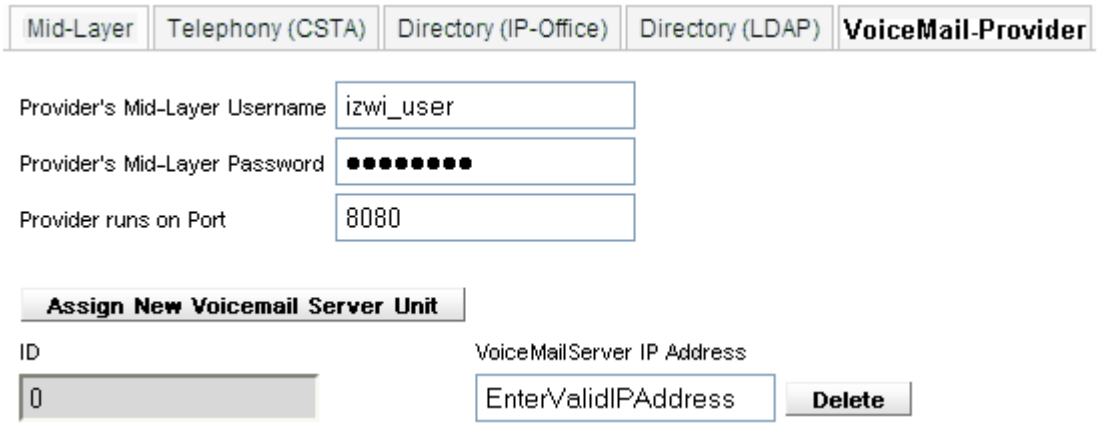
The **Edit Field Mapping** button displays a menu which can be used to set which LDAP field should be obtained and into which one-X Portal for IP Office directory fields the values should be displayed.



2.4.1.4 Voicemail Provider

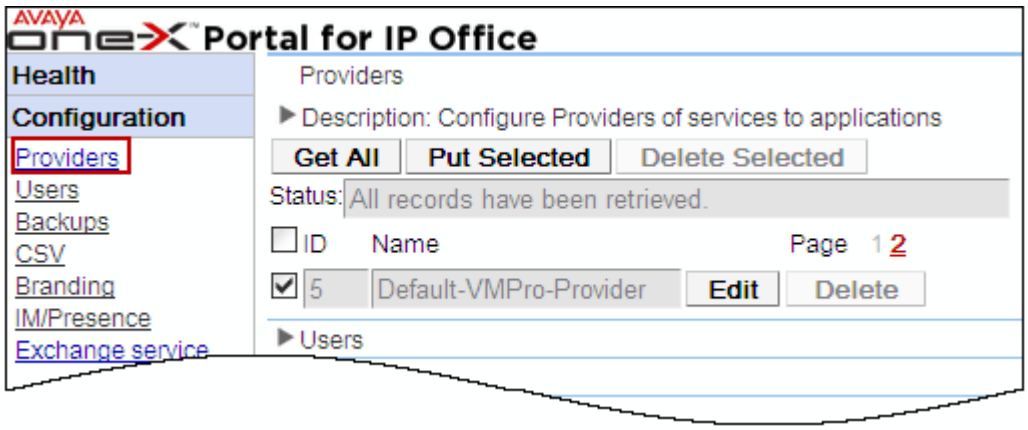
The settings below are shown for a **Voicemail** provider.

- **Voicemail Provider**

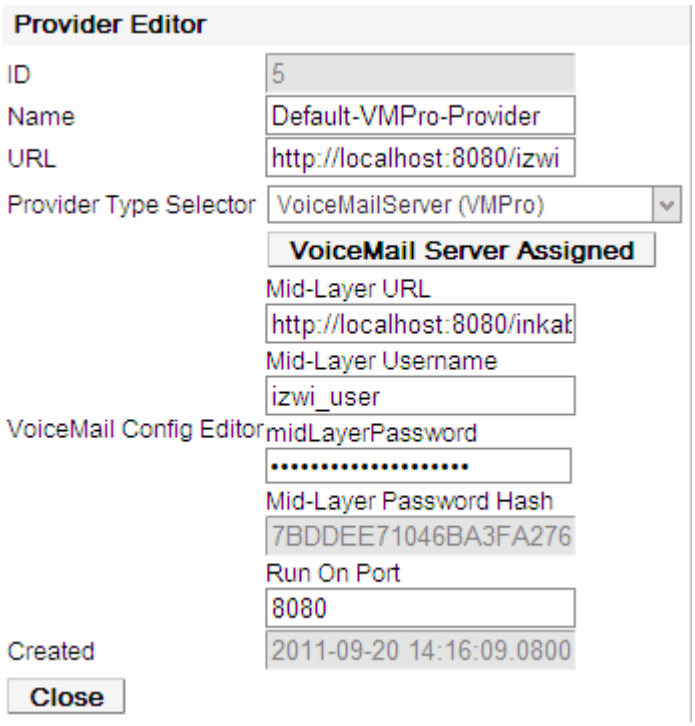


To update or change the VMPro Provider details in the one-X Portal for IP Office interface:

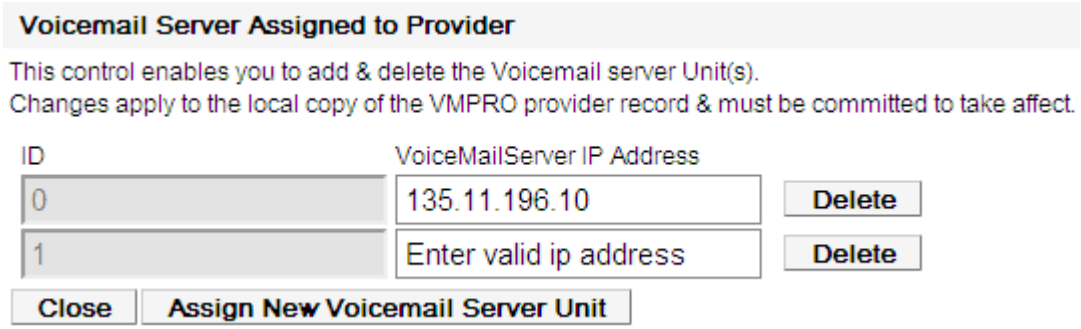
1. Log on to the one-X Portal for IP Office.
2. In the left navigation pane, click on **Configuration > Providers**.
3. On the right side, click the **Get All** button. The system displays a list of providers.



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.



6. Click the **Assign New Voicemail Server Unit** button to add a new row.
7. Enter *the ID* and *VoiceMail server IP Address.*
8. Click **Close**.
9. After verifying the VMPro provider details in the **Provider Editor** dialog box, click **Close**.
10. Check the **Default-VMPro-Provider** and click the **Put Selected** button. The system updates the details of the VMPro provider in the database of the one-X Portal for IP Office

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

2.4.2 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.

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**.

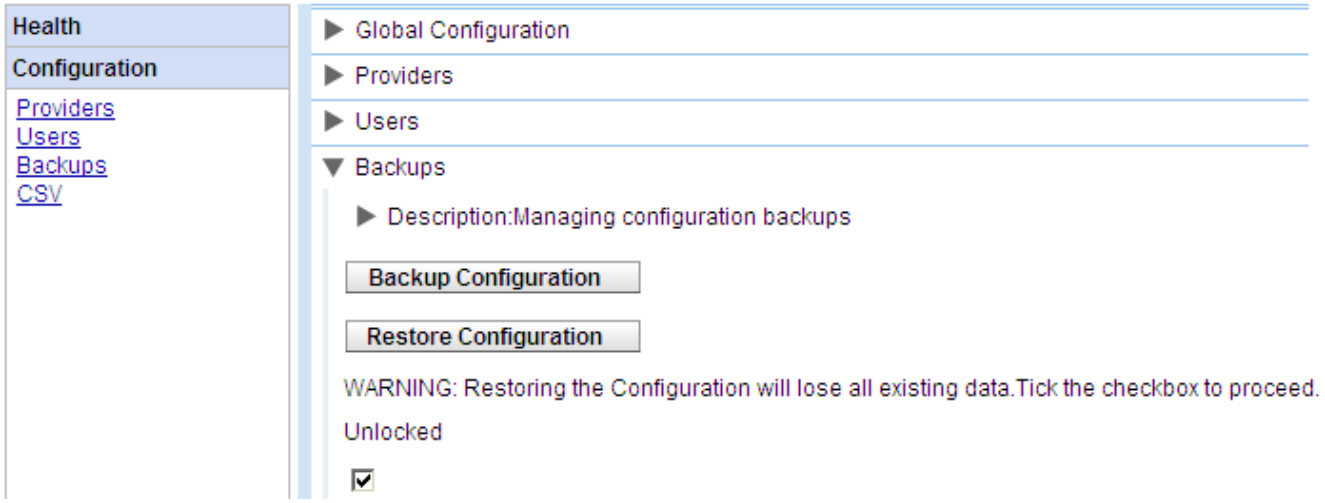
8. Click **Put Selected** to update the changes that you made to the user records in the one-X Portal for IP Office database.

Field	Options	Description
IM/Presence	Send conference entry IM	MyBuddy sends an IM to you when someone joins your *MeetMe* conference.
	Send conference exit IM	MyBuddy sends an IM to you when someone leaves your MeetMe 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: • 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 *on the phone* 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: • 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. • 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** 42 menu can be used to force an update from the IP Office systems.

2.4.3 Backups

This menu provided options to backup [14] the one-X Portal for IP Office configuration. It can also be used to restore [15] a previous backed up configuration.



Note that this is only intended as a simply backup and restore to allow rollback of server changes while making and testing administration changes. For one-X Portal for IP Office a more sophisticated set of backup and restore [51] options are available.

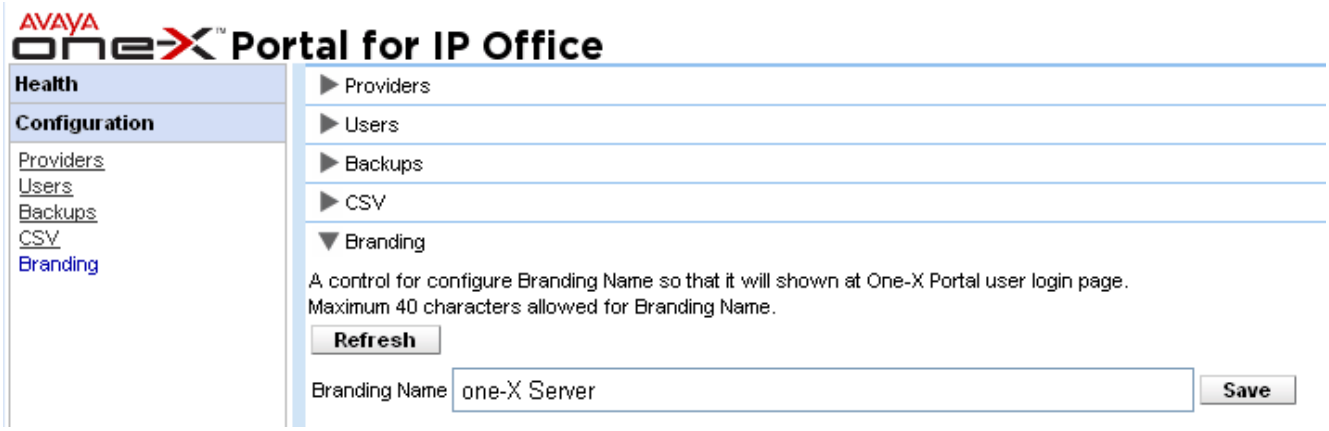
2.4.4 CSV

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\appache-tomcat-6.0.18\\bin***). Any existing file is overwritten.

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\appache-tomcat-6.0.18\\bin***).
   - ***exportUser.csv***
   - ***exportDirectoryEntry.csv***

2.4.5 Branding

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



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

2.4.6 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 server.

Note: You can set the XMPP domain name 37 only for the first time you initialize the configuration. If you use the IP address then the one-X Portal for IP Office cannot federate with remote server such as GTalk 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**.

2.4.6.1 XMPP domain name configuration

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

Configuring the XMPP domain name:

1. You can configure the XMPP domain name in the **IM Presence** tab. By default, the value is *127.0.0.1*.
2. You can change the value to *localhost*, *FQDN,* or *machine name*.

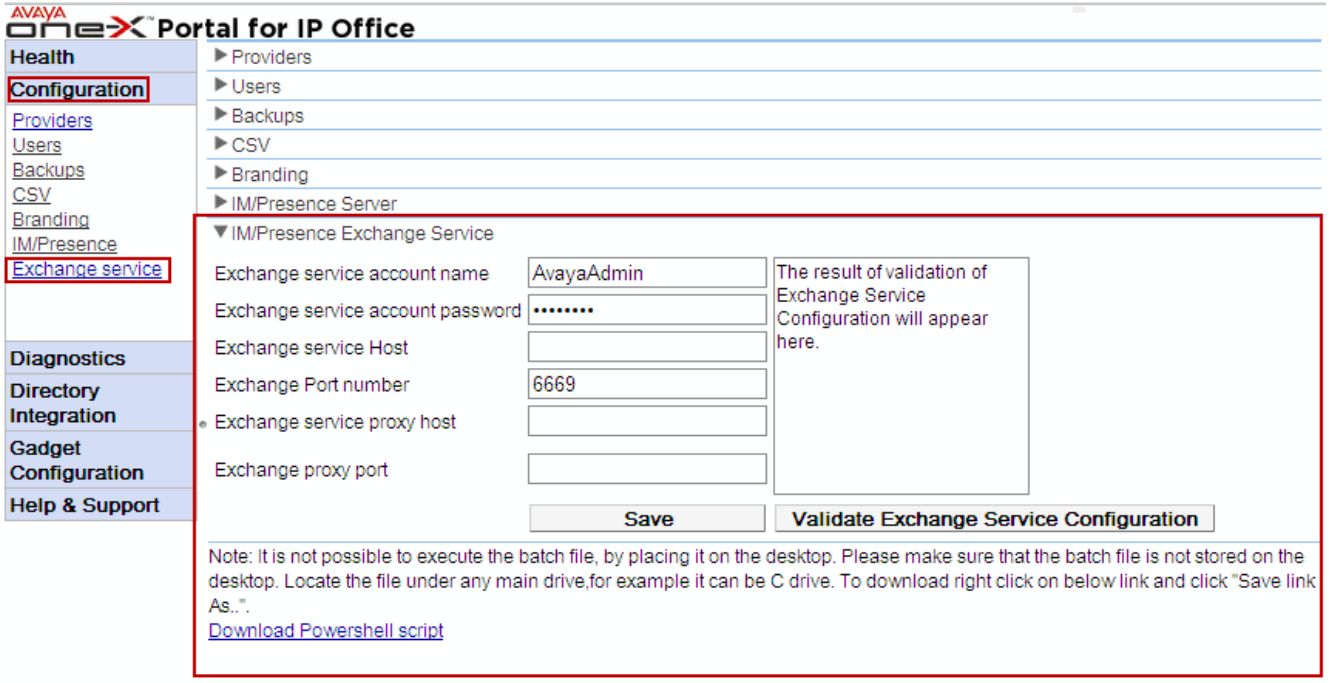
2.4.7 Exchange service

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**.

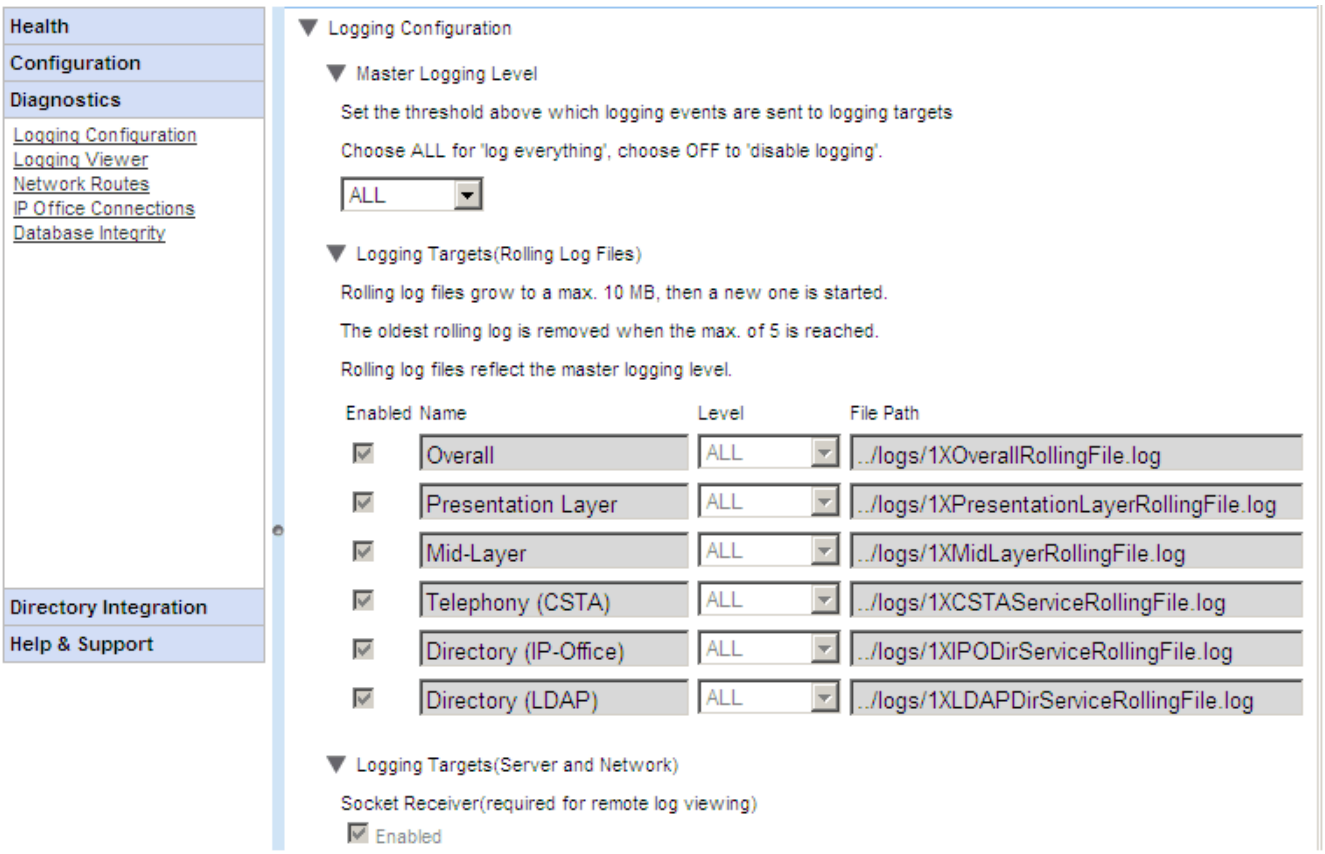


Note: You can **Download Powershell script** to provide impersonation rights to the users.

2.5 Diagnostics

2.5.1 Logging Configuration

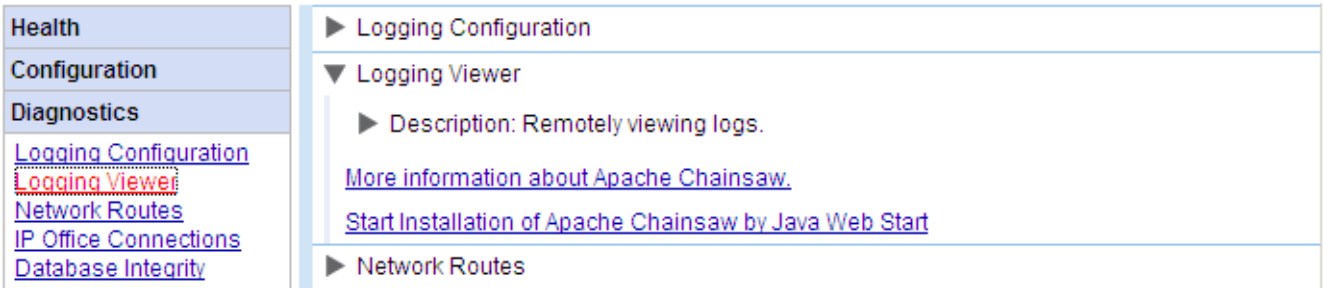
one-X Portal for IP Office supports a wide range of log output methods which selection of the level of logging required.



1. Select **Diagnostics** and then **Logging Configuration**.
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\appache-tomcat-6.0.18\ \logs***). Each log file can grow to approximately 10MB before a new file is started. When there are 5 files of a particular type, the oldest file is deleted when a new file is started.
   - **Overall:** *1XOverallRollingFile.log*
     This is an overall log file of all types of logged events.
   - **Presentation Layer:** *1XPresentationLayerRollingFile.log*
     This log captures user browser activity information/
   - **Mid-Layer:** *1XMidLayerRollingFile.log*
     This log captures interaction between the various one-X Portal for IP Office components including the IP Offices.
   - **Telephony (CSTA):** *1XCSTAServiceRollingFile.log*
     This log captures telephony information. That includes obtaining user and licensing information from the IP Offices.
   - **Directory (IP Office):** *1XIPODirServiceRollingFile.log*
     This log captures IP Office directory information.
   - **IMPresence:** *1XSCSServicesRollingFile.log*
     This log captures IP Office IM and Presence information.
   - **Directory (LDAP):** *1XLDAPDirServiceRollingFile.log*
     This log captures LDAP directory information.
   - **Socket Receiver (required for remote log viewing)**
     If enabled, an external logging application can connect to port 4560 on the server to receive logging output. The output is in log4j format and can be received by logging application such as Apache Chainsaw.

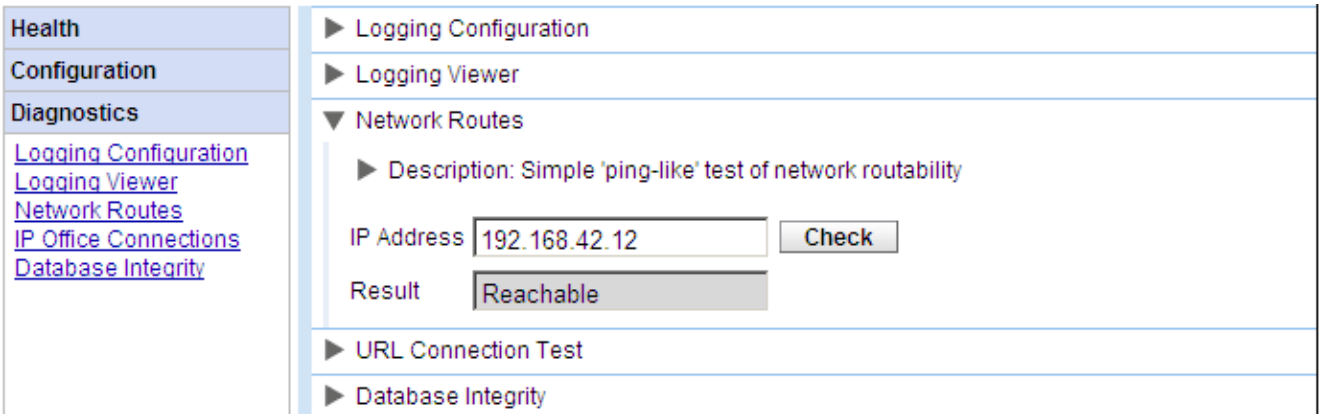
2.5.2 Logging Viewer

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 20 which is a suitable logging application .



2.5.3 Network Routes

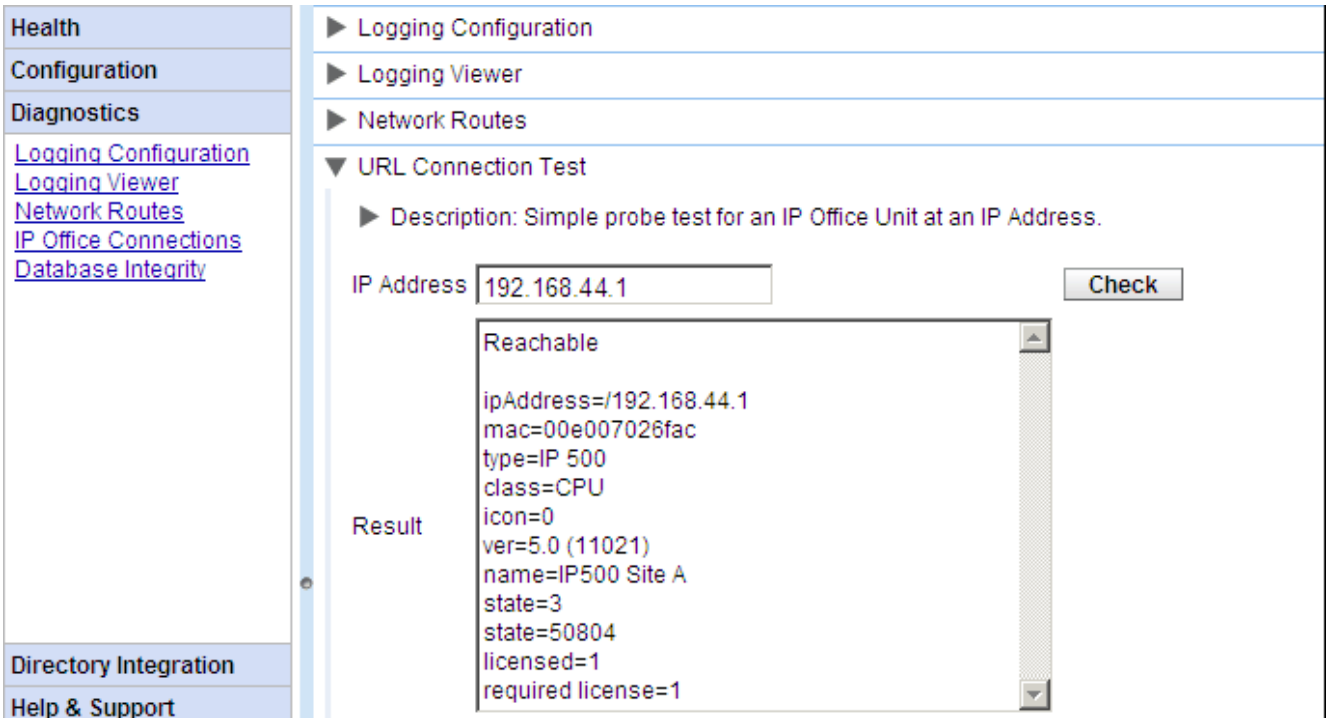
This menu can be used to test routing from the one-X Portal for IP Office server to an IP Office address. It uses TCP to port 7 (Echo service) on the target IP address. Note that this does not work with IP Office control units, for which the IP Office Connections 40 should be used instead.



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

2.5.4 IP Office Connections

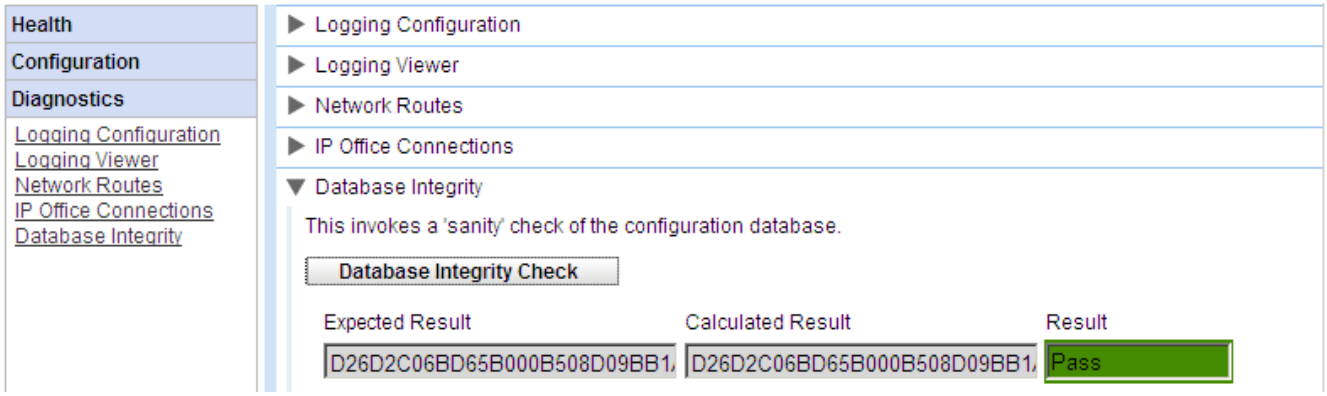
This menu can be used to check the connection between the one-X Portal for IP Office server and a particular IP Office. The connection check uses the standard discovery method used by IP Office applications such as IP Office Manager (connection to port 50804 of the IP Office control unit).



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.

2.5.5 Database Integrity

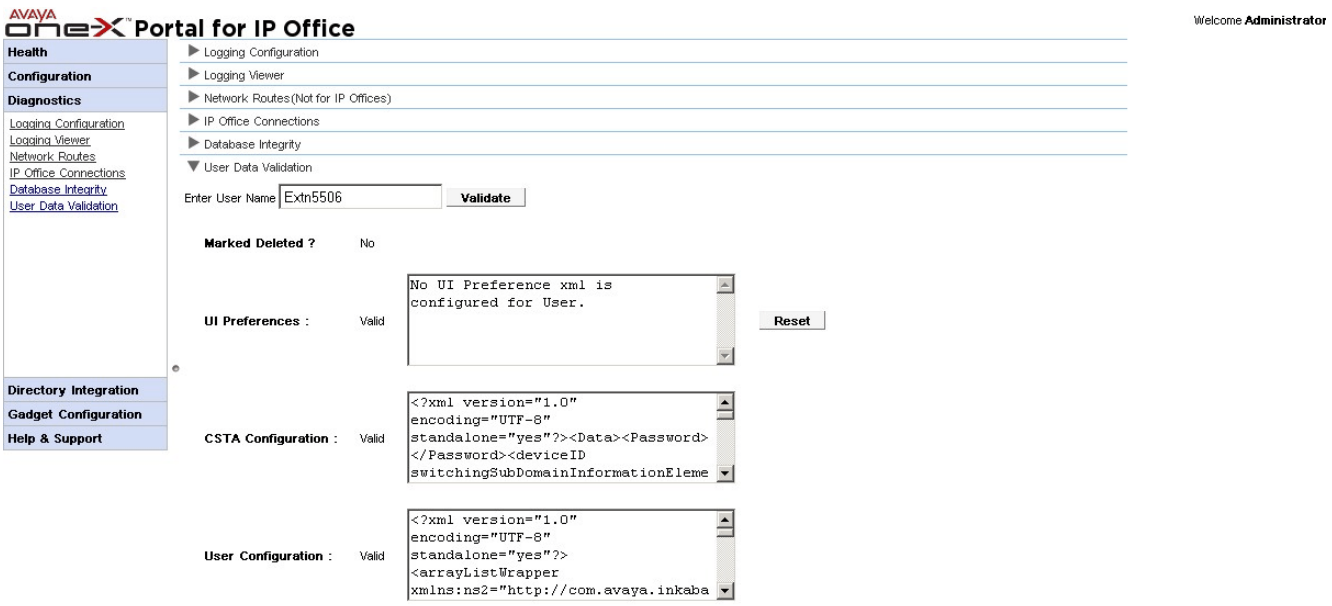
This menu can be used to check the database structure. It will return **Pass** if the tables and fields within the database are as expected for the particular version of one-X Portal for IP Office. It does not check the data within the fields. If **Fail** is reported refer to the Troubleshooting 23 section for known issues and resolutions.



2.5.6 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.



Following are the fields that are validated:

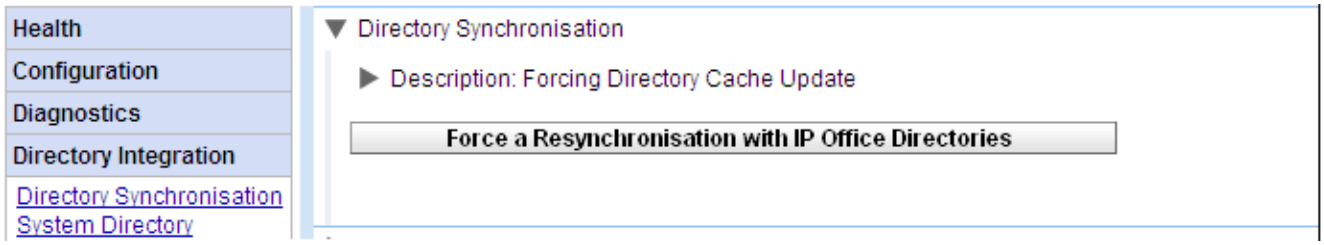
- **Marked Deleted?:** If the user record is marked as deleted or not.
- **UI Preferences:** If UI preference data is valid or not along with the corresponding XML. A 'Reset' button is provided for the Administrator to reset the data if it is corrupt. The UI preference is restored to default factory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

2.6 Directory Integration

2.6.1 Directory Synchronisation

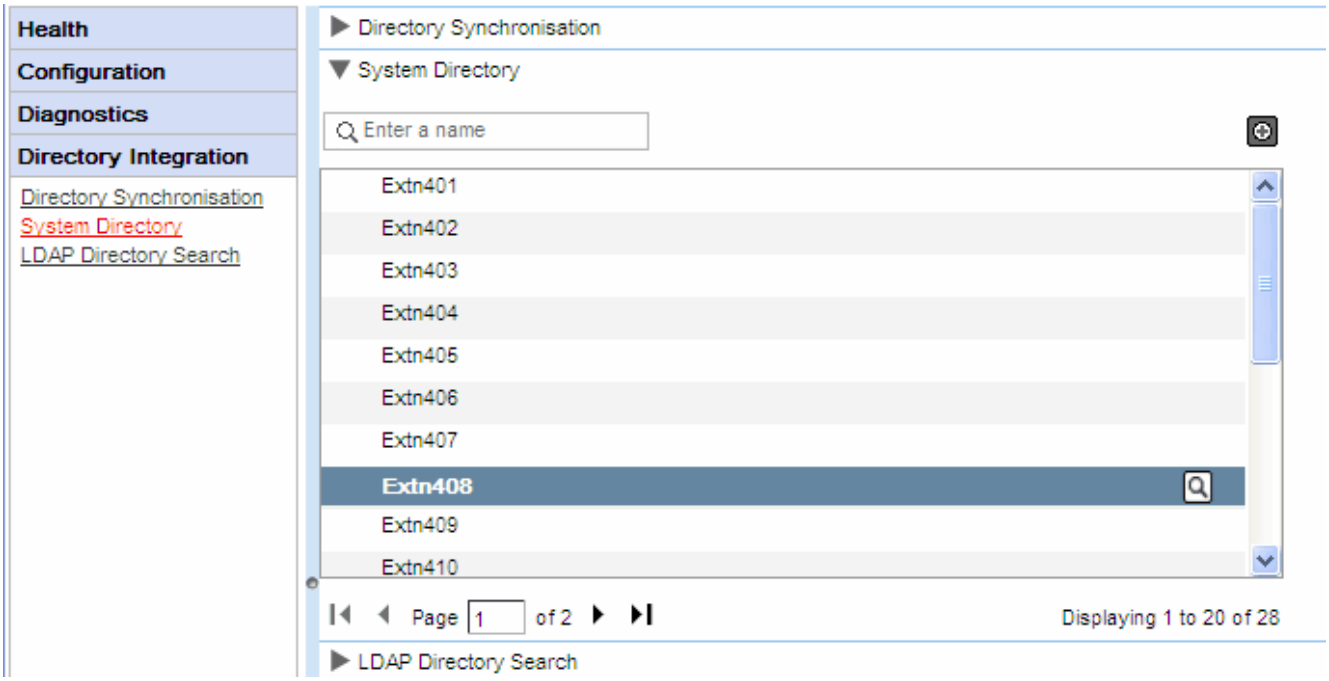
During normal operation, the one-X Portal for IP Office server updates the records every 300 seconds approximately. However, this menu can be used to force an update of the system directory and IP Office users.



- **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** 43 option.

2.6.2 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 was 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. 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** 42 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.

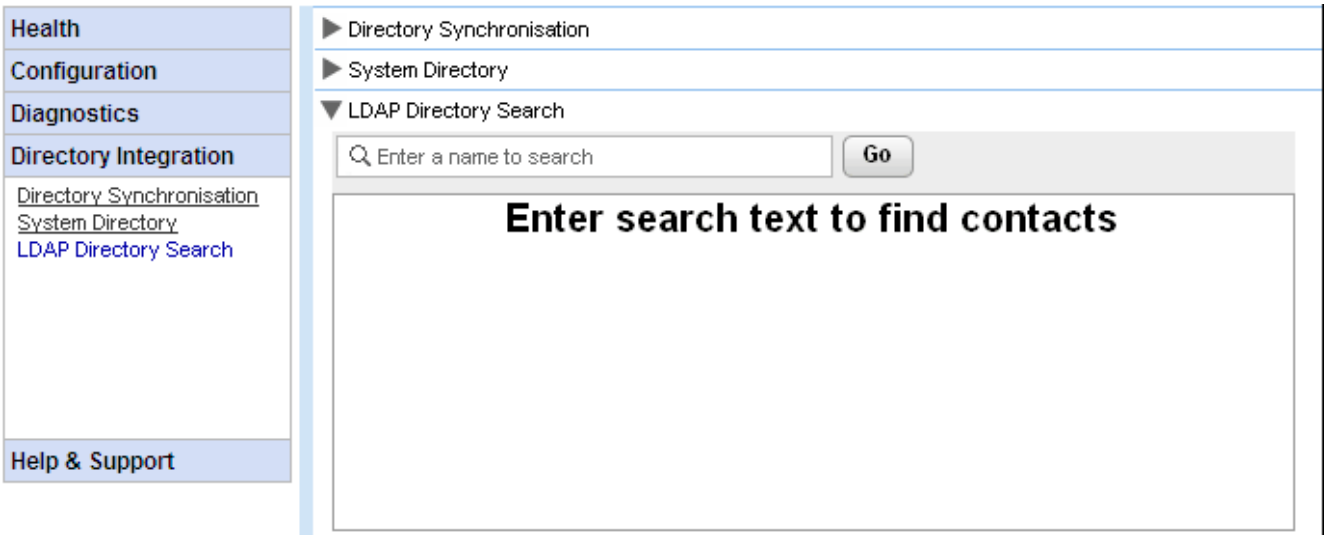
State	Icon	Description
Available		The normal state for a user showing that their work extension is not in use.
Busy		The normal state for a user showing that their work extension is currently on a call.
Do Not Disturb		The user has set **Do Not Disturb**. Calls to them will go to voicemail if enabled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

You can use the icon to add a new system directory contact. Note that contacts added in this way are stored by one-X Portal for IP Office only are 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 select **Delete** in the contact details.

2.6.3 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 10.

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



2.7 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.

2.7.1 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 44 or import external gadgets 46 for the user.

2.7.1.1 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 45

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.

2.7.1.1.1 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&amp;up_def_fro
m=USD&amp;up_def_to=EUR&amp;synd=open&amp;w=320&amp;h=170&amp;title=Currency+Converter&amp;bo
rder=%23ffffff%7C0px%2C1px+solid+%2382CAFA%7C0px%2C2px+solid+%23BDEDFF%7C0px%2C3px+solid+%
23E0FFFF&amp;output=js"></script>
```

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

2.7.1.2 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.

2.7.1.3 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.

2.7.1.4 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.

2.7.1.5 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.

2.7.1.6 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
- Height (optional)
- Toolbar icons for the gadget. It is recommended to provide toolbar icons for all gadgets specified in gadgets.xml. However, if the zip file does not contain any specified icon images, the system uses the default icons.
- 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:

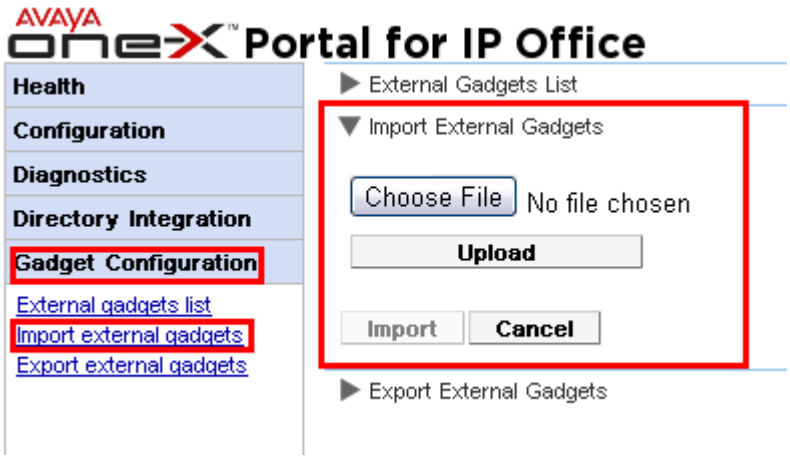
```
<gadgets>
<gadget>
<url>
https://accounts.zoho.com/iam/login?load_ifr=true&serviceurl=http%3A%2F%2Fgadgets.zoho.com%2Fembed%
2Fcalendar%3Ftitle%3DZoho%20Calendar
</url>
<name locale="en">Zoho Calendar</name>
<height>500</height>
<toolbar-icons>
<default>zoho-calendar-default.png</default>
```

```
<mouse-hover>zoho-calendar-hover.png</mouse-hover>
<mouse-press>zoho-calendar-press.png</mouse-press>
</toolbar-icons>
<toolbar-texts>
<label locale="en">My Calendar</label>
<tooltip locale="en">Zoho Calendar</tooltip>
</toolbar-texts>
</gadget>
<gadget>
<url>
http://www.gmodules.com/ig/ifr?url=http://www.donalobrien.net/apps/google/currency.xml&up_def_from=
USD&up_def_to=EUR&synd=open&w=320&h=170&title=Currency+Converter&border=%23ffffff%7C3px%2C1px+solid
+%23999999&output=js
</url>
<name locale="en">Currency Converter</name>
<height>170</height>
<toolbar-icons>
<default>currency-converter-default.gif</default>
<mouse-hover>currency-converter-hover.gif</mouse-hover>
<mouse-press>currency-converter-press.gif</mouse-press>
</toolbar-icons>
<toolbar-texts>
<label locale="en">Cur Converter</label>
<tooltip locale="en">Currency Converter</tooltip>
</toolbar-texts>
</gadget>
</gadgets>
```

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*.



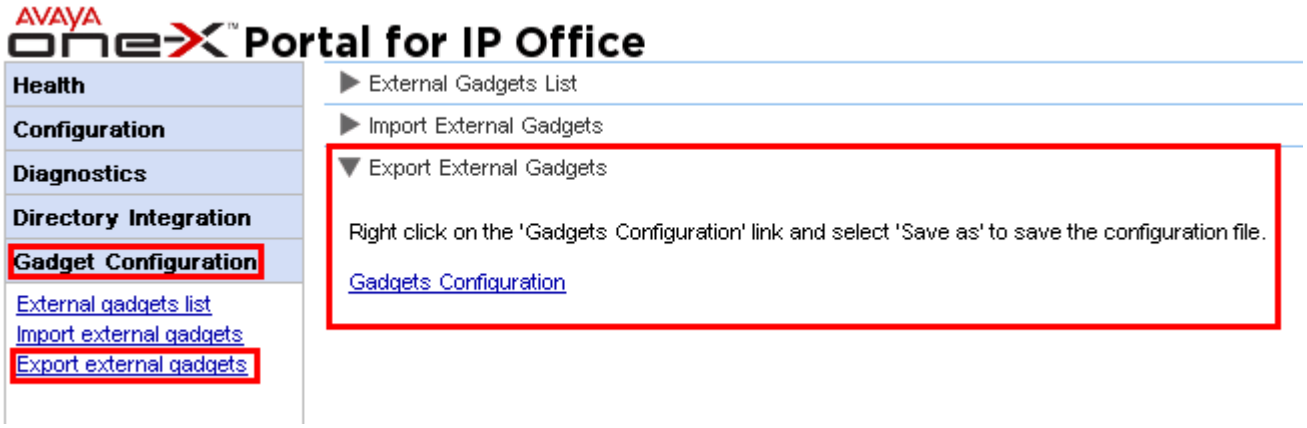
The next time the user logs into the one-X Portal for IP Office, the third party gadget is displayed.

2.7.1.7 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 [46] the saved configuration file.

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

2.8 Help & Support

Help | Help

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

Help | Avaya Support

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

Help | About

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

Chapter 3. 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.

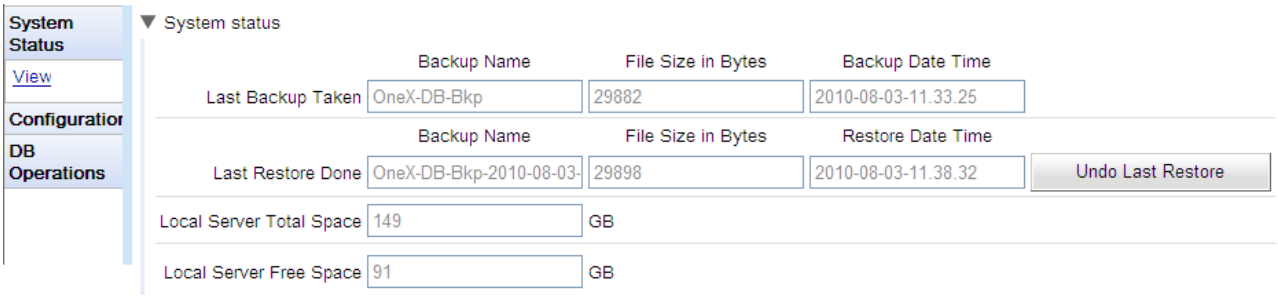
Note: One-X Portal for IP Office 8.0 continues to support the URL **http://<server name>:<server port>/induna/induna.html.**

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.
- **Backup Folder**
  This is the path to be used for backup and restore operations on the one-X Portal for IP Office server. Note that even if backing up and restoring to and from an FTP or local PC folder, this server folder is still used for temporary file storage.

3.2 System Status

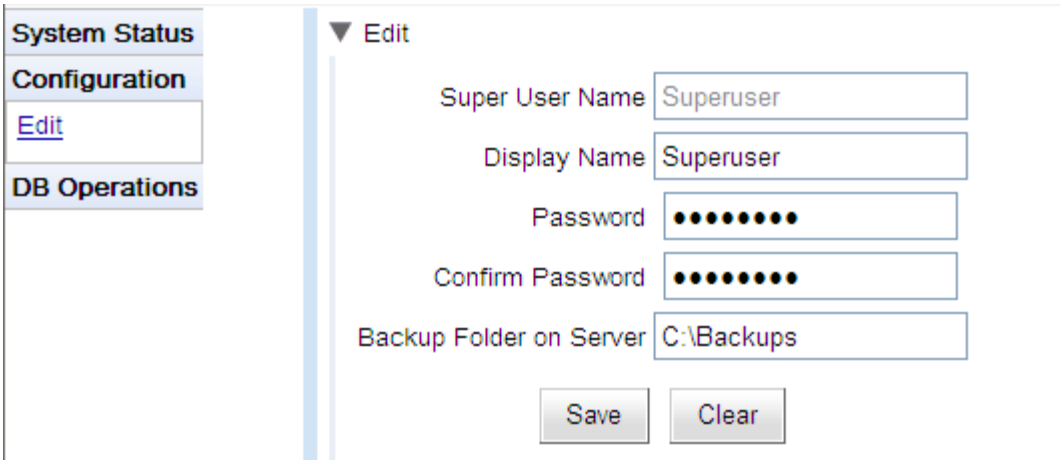
This menu gives a summary of the previous usage of the Superuser menus. It also allows the rollback of the last previous restore operation.



- **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 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.



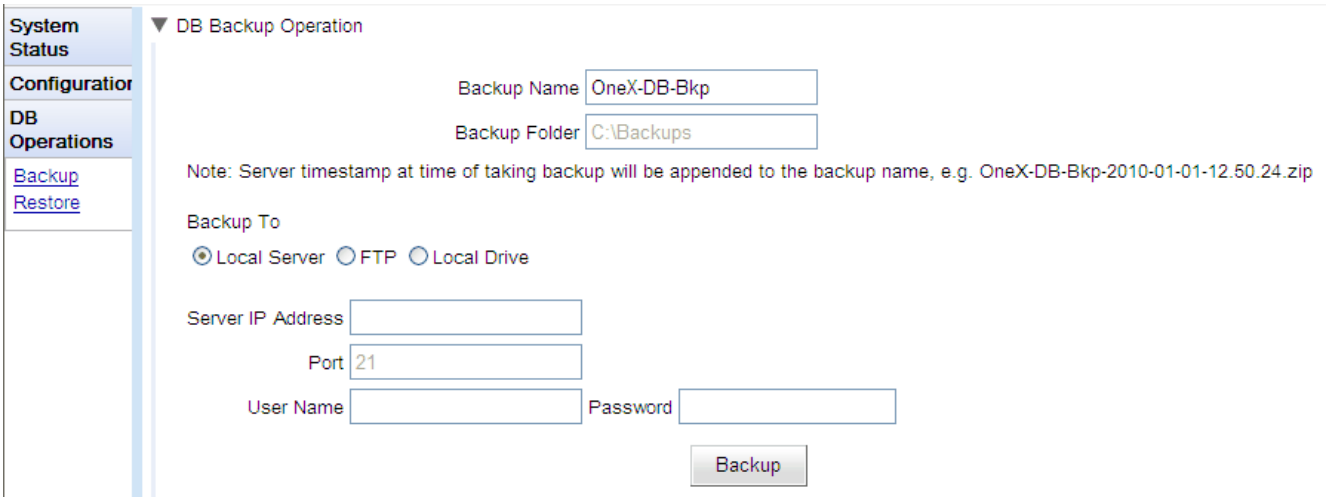
- **Super User Name**
  This is a fixed name and cannot be changed. It is the name used for the login.
- **Display Name**
  Enter a name for display in the one-X Portal for IP Office menus.
- **Password/Confirm Password**
  Enter a password that will be used for future ***Superuser*** access.
- **Backup Folder**
  This is the path to be used for backup and restore operations on the one-X Portal for IP Office server. Note that even if backing up and restoring to and from an FTP or local PC folder, this server folder is still used for temporary file storage.

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.

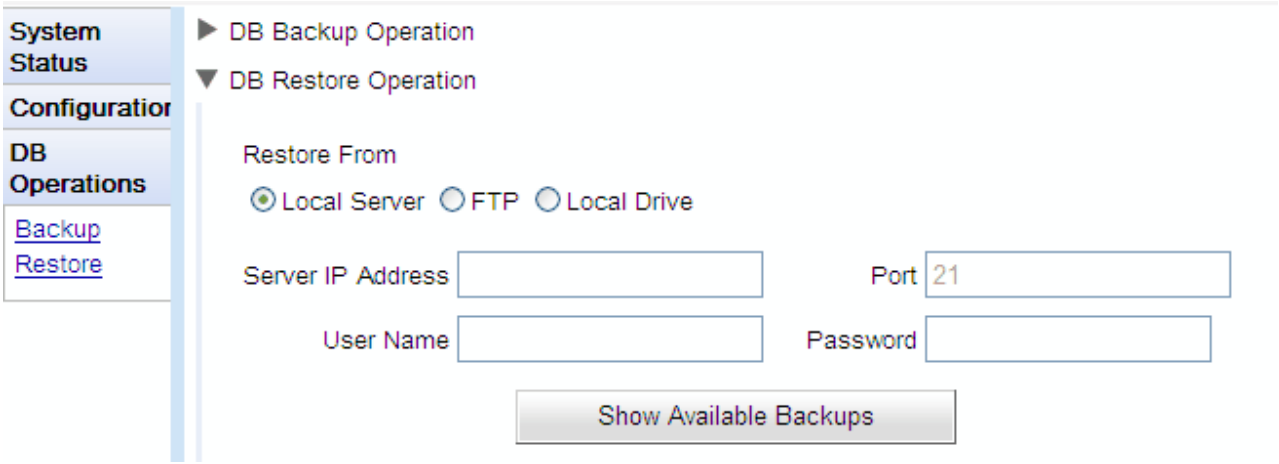


- **Backup Name**
  This name is used for the backup zip files. The date and time of the backup is also added to the file name. For example, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Backup Folder**
  This is the path to be used for backup and restore operations on the one-X Portal for IP Office server. Note that even if backing up and restoring to and from an FTP or local PC folder, this server folder is still used for temporary file storage.
- **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**.

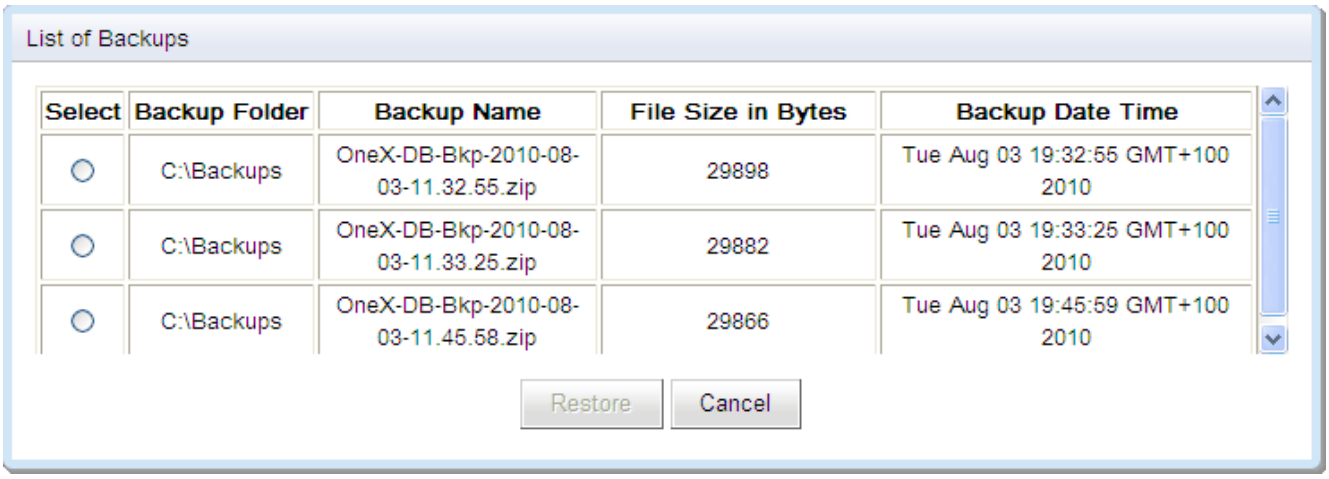
- **FTP**
  If this option is selected, the backup file is temporarily created in the **Backup Folder**. It is then sent to the specified FTP server address.
- **Local Drive**
  If this option is selected, the backup file is temporarily created in the **Backup Folder**. It is then offered for download 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

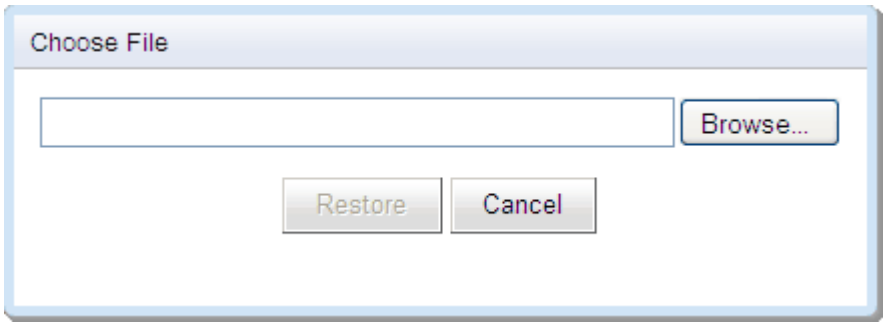
This menu is used to select a previous backup file and then use that file for a restore operation. Before the restoration occurs, a backup of the current configuration is made and stored in the **Backup Folder** for use with the **Undo Last Restore** 51 control. Restoration is only supported from a backup of the same one-X Portal for IP Office version.



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



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



Chapter 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.

Index

4

4560 20

A

About 27
Active Sessions 27, 29
Add
  IP Office 6
  LDAP 10
  User 11
Administrator
  Help 48
  Name 27
Agent 24
Apache
  Chainsaw 20, 40
Assign
  IP Office 6, 9
  IP Office (CSTA) 30
  IP Office (Directory) 31
  LDAP Provider 32
  Providers 30
Automatic logout 28
Avaya Support 27

B

Backup 14, 36
  Restore 15
Backups 27
Base DN 10
Bulk Edit 11, 34
  User 11

C

Call Log 11
Chainsaw 20, 40
Component Status 27, 28
Computer Supported Telecommunications Application 57
Configuration 27
  Backup 14
  Backups 36
  Bulk Edit 11
  CSV 36
  Export 36
  Providers 30
  Restore 15, 36
  Users 34
Control Panel 18
CSTA 30, 57
CSTA (IP Office) Provider 30
CSV 27, 36

D

Database
  Backup 14, 36
  Check 41
  Restore 15, 36
  Sanity Check 41
Database Integrity 27
Deinstall 18
Delete
  IP Office 9
  User 11
Diagnostics 27
  Connections 40
  Database Integrity 41
  IP Office Connections 40
  Logging Configuration 20, 39
  Logging Viewer 20, 40
  Network Routes 40
Directory
  Export 36
  Resynch 15, 42
Directory (DSML IP Office) 31
Directory (DSML LDAP) 32
Directory Integration 27
  Directory Synchronization 15, 42
Directory Intergration
  LDAP 16, 43
  System Directory 15, 43
Directory Search
  LDAP 16, 43
  System Directory 15, 43
Directory Synchronization 27
DND Exceptions 11
Downgrading 17
DSML (IP Office) Provider 31
DSML (LDAP) Provider 32

E

Echo 40
Edit
  Bulk Edit 11
  IP Office settings 9
  User settings 11, 34
Environment 27
Events 28
Exceptions 11
Export Configuration 36
exportDirectoryEntry.csv 36
exportUser.csv 36
External Directory
  Search 16, 43

F

Field Mapping 10, 32
Force a Resynchronization 15, 42

G

Group 24

H

Health 27
  Active Sessions 29
  Component Status 28
  Environment 29
  Key Recent Events 28
Help 27
  About 48
  Avaya Support 48
  Help 48
Hunt Group 24

I

Immediate logout 28
IP Office
  Connections 27
  CSTA Provider 30
  Directory Provider 31

J

Java Web Start 20

K

Key Recent Events 27, 28
Keyboard Shortcuts 11

L

LDAP
- Assign 10
- Directory Search 16, 27, 43
- Provider 32

Log Files 39
Log4j format 20
Logging 20
- Configuration 27
- Level 39
- Targets 39
- Viewer 20, 27

Logging Configuration 20
Login 27
Logout 28

M

Maintenance 5
Master Logging Level 39
Membership 24
Messages 11

N

Network Routes 27, 40
Not Reachable 40

O

Override Admin Session 27

P

Park Slots 11
Password 27
Personal Directory 11
PING 40
Port
- 4560 20
- 7 40

Presence 11
Provider 27
- Assign 30
- CSTA (IP Office) 30
- Directory (DSML IP Office) 31
- Directory (DSML LDAP) 32
- DSML (IP Office) 31
- DSML (LDAP) 32
- View 30

R

Reachable 40
Recent Events 28
Remote Logging 20
Remove
- IP Office 9
- one-X Portal for IP Office 18
- User 11

Reset Session Count 27
Restart Service 6
Restore 15, 36
- Backup 14

Resynchronization 15, 42
Rolling Log Files 39
Routes 40

S

Sanity 41
Search
- LDAP 16, 43
- System Directory 15, 43

Search Base 10
Server
- Information 29
- Version 29

Service
- Restart 6

Sessions 29
Settings
- Backup 14
- Bulk Edit 11
- Restore 15

Shortcuts 11
Socket Receiver 20, 39
Start Service 6
Status 28
Synchronization 15, 42
System Directory 27
- Directory Search 15, 43
- Export 36
- Resynch 15, 42

T

TCP Port 7 40
TCPA 57
Telephony Service Provider Interface 57
Test
- External Directory 16, 43
- IP Office connection 40
- LDAP Directory 16, 43
- Network Route 40
- System Directory 15, 43

Thin Client Productivity Application 57
TSPI 57

U

Uninstall 18
Upgrading 17
User
- Add 11
- Bult Edit 11
- Delete 11
- Edit settings 11
- Export 36
- Help 48

Users 27
- Active 29
- Edit settings 34
- Resynch 15, 42
- View 34

V

Version 29
View
- Component Status 28
- Key Recent Events 28
- Providers 30

Voicemail Messages 11

Performance figures and data quoted in this document are typical, and must be specifically confirmed in writing by Avaya before they become applicable to any particular order or contract. The company reserves the right to make alterations or amendments to the detailed specifications at its discretion. The publication of information in this document does not imply freedom from patent or other protective rights of Avaya or others.

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

This document contains proprietary information of Avaya and is not to be disclosed or used except in accordance with applicable agreements.

© 2011 Avaya Inc. All rights reserved.