IP Office 7.0

one-X Portal for IP Office Installation

15-601139 Issue 05b - (04 August 2011)

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. one-X Portal for IP Office

2. Installation

3. Maintenance

4. Administration

5. Backup/Restore

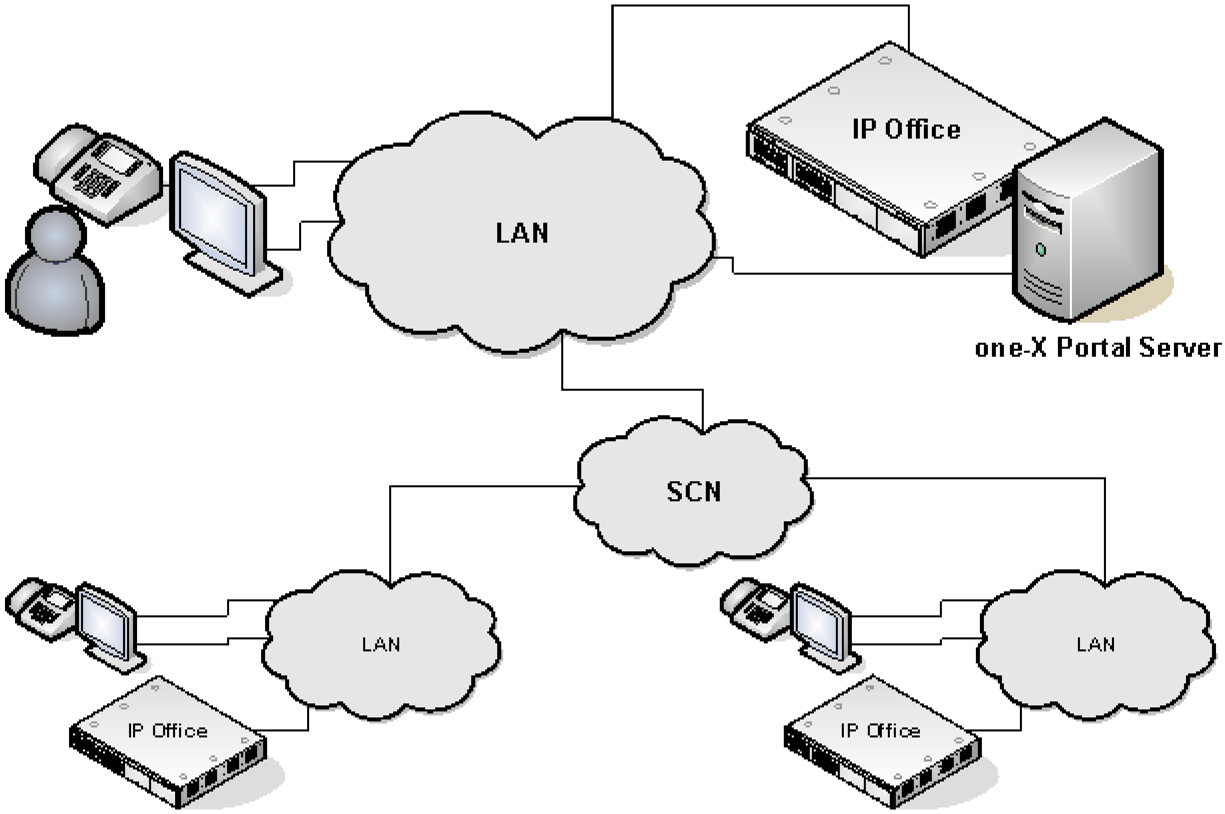
6. Glossary

Chapter 1. one-X Portal for IP Office

1. one-X Portal for IP Office

one-X Portal for IP Office is a server application that allows IP Office users to control their phone and various telephony settings through a web browser. A single one-X Portal for IP Office server can support multiple IP Offices when they are connected in a single IP Office Small Community Network 8 (SCN). one-X Portal for IP Office supports up to 500 simultaneous sessions.

The one-X Portal for IP Office application software is installed onto a Window server. Alternatively it can be installed as one of the Linux components on the IP Office Application Server, for full details of that installation refer to the IP Office Application Server manuals.



one-X Portal for IP Office installs as a service with an integral web server. Both user and administrator access to one-X Portal for IP Office is via web browser to the one-X Portal for IP Office server. The one-X Portal for IP Office service communicates with the IP Office system using the IP Office's TSPI (Telephony Service Provider Interface) service. This service is configured through the security settings of the IP Office control units.

one-X Portal for IP Office is a licensed application, with each IP Office requiring licenses for those users configured 21 to use one-X Portal for IP Office.

1.1 Server Requirements

one-X Portal for IP Office is currently supported with all components installed on a single server meeting the following requirements:

- **Administrator Account:** During installation you must be logged in using an account with full administrator rights.
- **Operating System:** Windows 2003 or Windows 2008 (32-bit and 64-bit).
- **Processor:** Intel Pentium D945 Dual Core or AMD Athlon64 4000+ or better.
- **RAM Memory:** 2GB minimum.
- **Available Hard Disk Space:** 10GB.
- **TCP/IP Port:**
  The default ports are 8080 and 8666. These can be changed if required during installation of the server software if necessary. See Checking Available Ports 22.
- **Firewall Exceptions**
  Exceptions should be added to the server firewall for incoming access on the TCP ports above. If the firewall is also used to control outgoing access, an exception for access to TCP port 50814 on the IP Office IP address should also be added.

1.2 Small Community Network Support

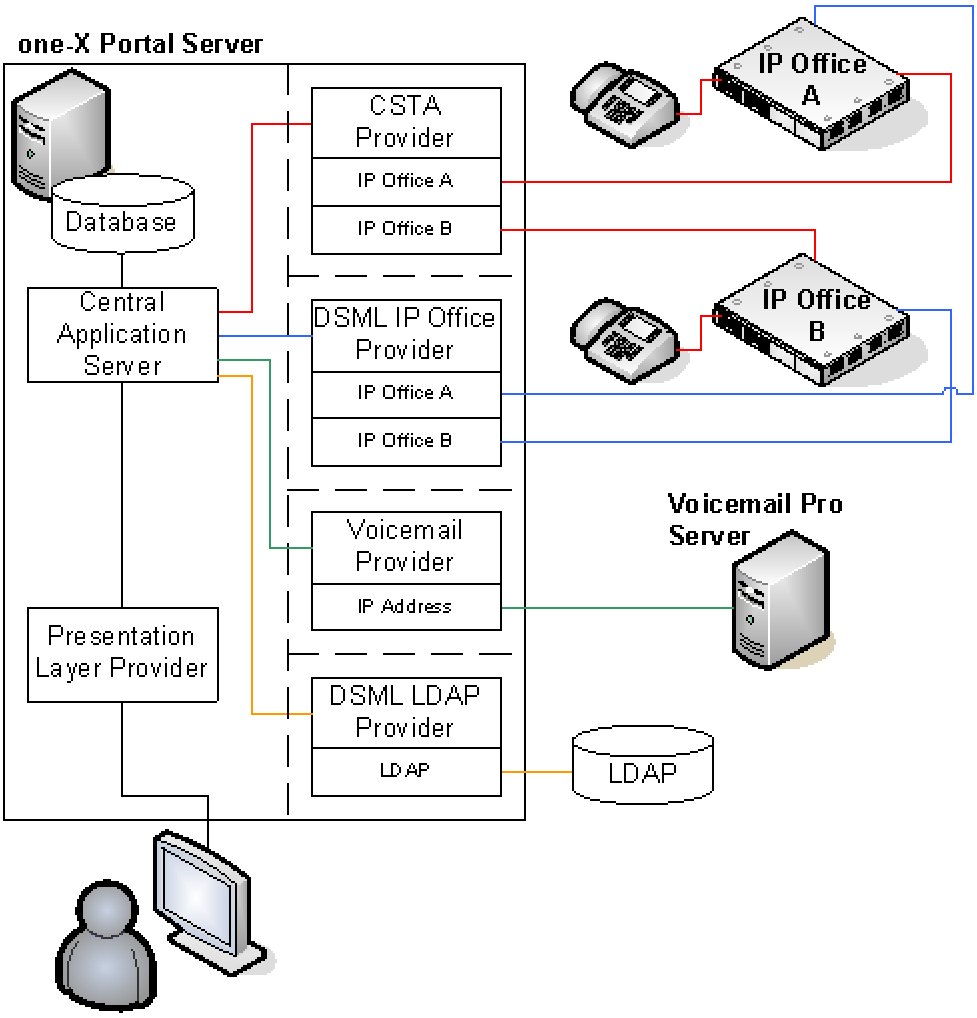
one-X Portal for IP Office is supported within a Small Community Network (SCN) of IP Office systems.

- In a Small Community Network, only a single server running one-X Portal for IP Office is supported. This one-X Portal for IP Office can support up to 500 simultaneous user sessions.
- Each IP Office on which one-X Portal for IP Office users are located must meet the requirements for one-X Portal for IP Office. That includes systems to which one-X Portal for IP Office users may temporarily hot desk.
- In a Small Community Network, one Voicemail Pro server is used as the centralized voicemail server for all telephone systems in the network. The one-X Portal for IP Office must be configured to use that voicemail server.
  - Voicemail configuration does allow additional voicemail servers in a Small Community Network in roles as distributed voicemail server. However the one-X Portal for IP Office should only be configured to use the centralized voicemail server.
- one-X Portal for IP Office does not provide additional Small Community Network features. It only supports features that are supported by each user's IP Office systems. For example, the system park buttons controls provided by one-X Portal for IP Office are not supported between different systems in an Small Community Network. This means that one-X Portal for IP Office users can only park and unpark calls on the IP Office system on which they are registered.

1.3 Providers

A key idea to understand one-X Portal for IP Office is providers. Providers are components of one-X Portal for IP Office, each of which performs a specific role. The different types of provider are:

- **Presentation Level Provider**
  This type of provider handles the browser connections between users and the one-X Portal for IP Office server.
- **Telephony CSTA Provider**
  This type of provider handles telephony communications to and from the IP Office systems assigned to it.
- **Directory DSML IP Office Provider**
  This type of provider handles obtaining directory information from the IP Office phone systems assigned to it.
- **Directory DSML LDAP Provider**
  Handles obtaining LDAP directory information from an LDAP source. LDAP sources are assigned to the provider during installation.
- **Voicemail Provider**
  Handles direct interaction with the voicemail server for features such as message playback via the browser.



During installation:

- One provider of each type is created.
- The IP Offices indicated during installation are assigned to the Telephony CSTA and Directory DSML providers. Following installation, additional IP Offices can be assigned 36 as they are added to the Small Community Network.
- A Directory DSML LDAP provider is created even if no LDAP source is assigned. The actual LDAP sources can be assigned after installation.
- A Voicemail provider is created but needs to be configured to the appropriate IP address of the voicemail server.

1.4 one-X Portal for IP Office Settings

The sections below detail which user and directory data is stored by the one-X Portal for IP Office server and which is stored by the telephone systems.

Directories

The various directories available to a one-X Portal for IP Office user are taken from a number of sources:

- **Personal Directory**
  As personal directory records are added, they are stored by both the one-X Portal for IP Office application and by the telephone system and kept in synch. The telephone system can only store up to 100 personal directory entries per user (subject to its own system limits), any additional entries beyond that are stored by one-X Portal for IP Office only.
  - 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.
  - Users with a 1608, 1616, 9400, 9500 or 9600 phones can edit or delete contacts through the phone's menus (primary phone number only). Users with 1608, 1616 or 9600 Series phones can edit or delete contacts through the phone's menus (primary phone number only).
- **System Directory**
  The system directory contains records for all the users and groups on the IP Office systems assigned to one-X Portal for IP Office plus the system directory entries stored in the configuration of those systems. It does not include directory records those systems obtain by LDAP and or HTTP import.
  - In an IP Office Small Community Network, the system directory entries configured on one IP Office system can be dynamically shared by other IP Offices in the network. This is a Centralized System Directory. The IP Office used to store the system directory used by the other systems should be one of those also assigned to one-X Portal for IP Office.
  - If multiple IP Office systems are configured to operate with one-X Portal for IP Office, the system directories of each are combined by one-X Portal for IP Office into a single system directory for use by one-X Portal for IP Office users. If the same name exists in more than one IP Office system directory, that name will exist as multiple records in the one-X Portal for IP Office system directory. If this is undesirable, the centralized system directory feature supported by IP Office 5.0 and higher systems should be used to have the system directory record configured on just one IP Office but shared by HTTP import on the other IP Offices.
  - Since the system directories are available to all one-X Portal for IP Office users, the number must be dialable by all one-X Portal for IP Office users. Alternatively, short codes should be used to ensure that numbers selected from the one-X Portal for IP Office system directory are interpreted correctly by the user's own IP Office
  - The one-X Portal for IP Office administrator can add System Directory contacts 76 that are stored as part of the one-X Portal for IP Office configuration rather than IP Office configuration. These contacts can have multiple phone numbers and email addresses in the same way as user's Personal Directory contacts, but are available to all one-X Portal for IP Office users.
- **External Directory**
  The external directory is not stored by one-X Portal for IP Office. Instead one-X Portal for IP Office performs a live search of the external directory source configured 41 for one-X Portal for IP Office usage.

User Settings

User settings for telephony operation are mainly stored by the IP Office system on which that user is configured. Only a small number of settings are stored by the one-X Portal for IP Office server.

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. • Users with a 1608, 1616, 9400, 9500 or 9600 phones can edit or delete contacts through the phone's menus (primary phone number only). Users with 1608, 1616 or 9600 Series phones 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 is may alter 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.

Note that those settings stored by one-X Portal for IP Office are lost if one-X Portal for IP Office is reinstalled 51 rather than upgraded 49.

1.5 Telephony Notes

While the one-X Portal for IP Office displays information about calls and allows the user to perform actions such as answer or make call, all control of the user's phone and call is still performed via the telephone system.

Incoming Calls

The calls that reach the one-X Portal for IP Office user are still fully controlled by the IP Office system settings. For example, the user's call waiting settings, number of call appearance buttons, etc. This applies to both user calls and calls to hunt groups of which the user is a member. Issues with incoming calls not alerting the one-X Portal for IP Office user will be down to IP Office system configuration settings.

Outgoing Calls

The outgoing calls that the one-X Portal for IP Office user can make will be subject to the user's IP Office configuration settings. The one difference is that the user can use one-X Portal for IP Office to make additional calls. For example, when all the appearance buttons on a user's phone are in use, they can still use one-X Portal for IP Office to make additional calls.

On some type of phones, the call log shown by the phone and the phone's redial function use information stored by the phone. When that is the case, those functions will not include calls made using the one-X Portal for IP Office.

Call Gadget Buttons

Within the sub-tab shown for each call being handled by the one-X Portal for IP Office users, a number of buttons are included. The buttons indicate actions that the user can perform or initiate and vary according to factors such as the type of phone, the current state of the call, whether the user already has other calls connected or held, etc.

It is important to understand that it is not the one-X Portal for IP Office application that controls which buttons are displayed. The actions currently performable on each call are indicated to one-X Portal for IP Office as part of the information from the IP Office system.

When the user is using a phone that the IP Office system cannot force off-hook, the following differences are applicable.

- When an incoming calls is presented while the phone is on-hook, one-X Portal for IP Office will not enable the **Answer** button. The user needs to manually take the phone off hook to answer the call using the phone's own controls.
- When making a call from one-X Portal for IP Office with the phone is on-hook (for example after entering a number and clicking on **Call** or having selected to play a voicemail message), the IP Office will call the user's phone and will only make the outgoing call when answered.

Some phones allow actions such as entering the number to call without going off-hook. This is called en-bloc dialing. The IP Office system, and therefore the one-X Portal for IP Office, is unaware of such activity until the prepared digits are sent from the phone.

- This typically applies to phones on DECT systems and to SIP extensions.
- Avaya 1400, 1600, 9400, 9500 and 9600 Series phones can be optionally set to use en-bloc dialing.

Chapter 2. Installation

2. Installation

This section covers the installation of a one-X Portal for IP Office server using default settings. This is the recommended option except for installers with advanced one-X Portal for IP Office experience.

- **Important**
  Installation of one-X Portal for IP Office is greatly simplified if each IP Office contains at least one user already licensed and configured for one-X Portal for IP Office operation. It is also vital to check the security settings of each IP Office.

Installation Process

The basic installation process consists of the following stages:

1. Check the installation requirements 15
2. Check IP Office Security Settings 18
3. Add User Licenses 20
4. Configure Users 21
5. Checking Available Ports 22
6. Install the one-X Portal for IP Office Software 23
7. Initial Server Configuration 26
8. Test User Connection 30

2.1 Installation Requirements

Ensure that the following requirements are met before beginning installation of the one-X Portal for IP Office software on the server PC. Failure to do so will cause the one-X Portal for IP Office server to operate incorrectly.

IP Office Software

- □ **IP Office Applications DVD**
  For a Windows based server installation, the IP Office Applications DVD includes the software for installation of one-X Portal for IP Office. It also includes software for installation of IP Office Manager and the IP Office System Status Application which are required during one-X Portal for IP Office installation.

- □ **IP Office Application Server DVD**
  For a Linux based server installation, the one-X Portal for IP Office application is included as one of the applications that can be selected during the IP Office Application server installation. A copy of the IP Office Application DVD is still required for the IP Office Manager application.

-

IP Office System Requirements

- □ **IP Office System**
  If the system running pre-IP Office Release 7.0 software, it must be upgraded as per the relevant IP Office Technical Bulletins before proceeding.

- Users licensed and configured with the ***Office User***, ***Teleworker User*** or ***Power User*** profiles can be configured for as one-X Portal for IP Office users. Those licensed and configured for with ***Teleworker User*** or ***Power User*** profiles can also be enabled for one-X Portal for IP Office telecommuter mode.

  - For systems being upgraded from IP Office Release 5, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for IP Office for users set to the ***Basic User*** profile.

Server PC Requirements

one-X Portal for IP Office is currently supported with all components installed on a single server meeting the following requirements:

- **Administrator Account:** During installation you must be logged in using an account with full administrator rights.

- **Operating System:** Windows 2003 or Windows 2008 (32-bit and 64-bit).

- **Processor:** Intel Pentium D945 Dual Core or AMD Athlon64 4000+ or better.

- **RAM Memory:** 2GB minimum.

- **Available Hard Disk Space:** 10GB.

- **TCP/IP Port:**
  The default ports are 8080 and 8666. These can be changed if required during installation of the server software if necessary. See Checking Available Ports 22.

- **Firewall Exceptions**
  Exceptions should be added to the server firewall for incoming access on the TCP ports above. If the firewall is also used to control outgoing access, an exception for access to TCP port 50814 on the IP Office IP address should also be added.

Voicemail Server Requirements

The playback of a user's messages through their phone is supported using embedded voicemail or Voicemail Pro. Voicemail playback through the one-X Portal for IP Office user's browser and personalized greeting recording and control requires a Voicemail Pro voicemail server.

If using a Windows based Voicemail Pro server, the server must be installed as follows:

- □ Microsoft IIS should be installed and running before installation of the Voicemail Pro voicemail server software. The following IIS options should be enabled:
  - □ **Enable Direct Metabase Edit**.
  - □ **IIS6 Configuration Compatibility**.
  - □ SSL should be disabled for the default website.
- □ The Voicemail Pro voicemail server installation should include the **Web Voicemail (UMS)** component.
- □ The voicemail server must be in the same subnet as the one-X Portal for IP Office server.
- Check that the IIS on the voicemail server can be browsed by server name from the one-X Portal for IP Office server PC. Enter ***http://<voicemail_server_name>/localstart.asp*** into a browse. If the IIS server does not response resolve the DNS routing between the servers before proceeding with the one-X Portal for IP Office installation.

Information Required

- □ For the server PC:
  - □ **IP Address**.
  - □ **User Account:** A user account with full administrator rights. This account should be used for the software installation.
  - □ **Computer Name:** This name will become part of the URL users use to access one-X Portal for IP Office.
- □ For each IP Office system:
  - □ IP Address.
  - □ Name and password for security settings access.
  - □ Name and password for configuration settings access.
  - □ Users who will be using one-X Portal for IP Office including IP Office user name and password.
  - □ The IP address of the Voicemail Pro voicemail server being used by the IP Office.

LDAP Information

To enabled the External tab in the one-X Portal for IP Office Directory gadget, details of the customer's LDAP server and an search configuration details are required.

- □ LDAP Server URL.
- □ User name and password.
- □ Base DN/Search Base.
- □ Field names.

User Requirements

- □ **Browser**
  Web browser with LAN access to the one-X Portal for IP Office server. one-X Portal for IP Office is tested using the current versions of the **Google Chrome**, **Internet Explorer**, **Mozilla Firefox** and **Safari** browsers.

  - □ The browser must have JavaScript enabled.

  - □ The **Remember me on this computer** option requires the browser to allow cookies.

  - □ For sounds to be used, for example ringing for a call waiting, or voicemail playback through the computer, a media player such as **Windows Media Player** or **Quick Time** must be installed. When using a browser other than Internet Explorer, Windows Media Player can be supported by the addition of the Firefox Windows Media Play plugin. This plugin is available from http://port25.technet.com/pages/windows-media-player-firefox-plugin-download.aspx. Currently this plugin is useable with Google Chrome, Mozilla Firefox and Windows Safari.

  - □ The playback of voicemail messages on the user computer may require the user browser to have the IP address of the voicemail server added to the proxy server exceptions.

  - **Language**
    one-X Portal for IP Office currently supports ***English***, ***French***, ***German***, ***Italian***, ***Dutch***, ***Brazilian Portuguese***, ***Latin Spanish***, ***Russian*** and ***Simplified Chinese***. The language it uses will be the best match to the browser language preferences.

- □ **Phone**
  one-X Portal for IP Office can be used with most phones supported by the telephone system except Phone Manager PC Softphone. The operation of analog and SIP phones does affect the method of operation of the one-X Portal for IP Office application, see Telephone Notes 12.

  - For analog phone users, the user's **Call Waiting On** and **Off Hook Station** settings should be selected in the user's IP Office configuration.

2.2 Check the IP Office Security Settings

Before attempting to connect an IP Office to a one-X Portal for IP Office server you must check the IP Office security settings. one-X Portal for IP Office uses a specific service and security service user account for the connection. This service is not necessarily present by default.

- **Important: Perform this Process from the one-X Portal for IP Office Server PC**
  It is strongly recommended that this and other IP Office configuration actions are performed using IP Office Manager installed on the server PC. That then also tests the network routing between the server PC and the IP Office system.

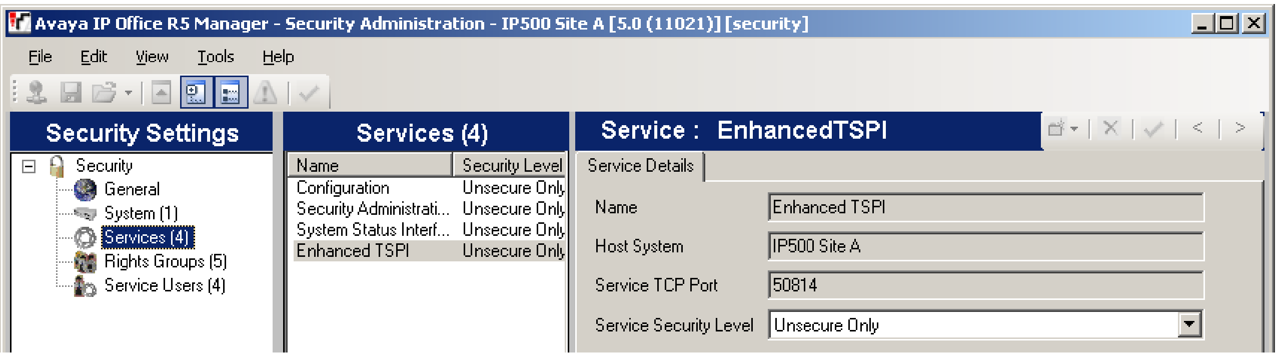
- **Important: Security Name and Password**
  This process uses the default security name and password assumed by one-X Portal for IP Office installation for TCPA/TSPI access to an IP Office 5.0+ system. If using the **Advanced** option during one-X Portal for IP Office installation, alternate names and passwords can be used. However, that is only recommended for installers with experience of previous one-X Portal for IP Office installations.

1. Start IP Office Manager and select **File | Advanced | Security Settings**.

2. Select the IP Office system and click **OK**.

3. Enter the user name and password for access to the IP Office's security settings.

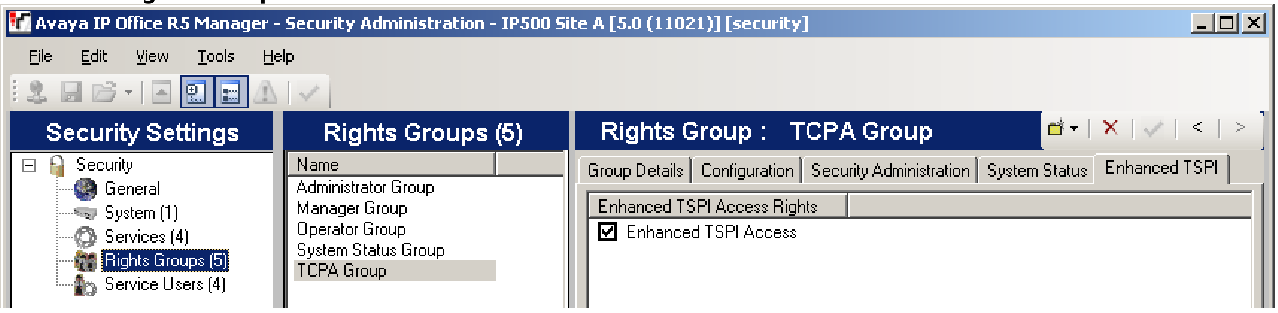
4. Select **Services**. On systems running IP Office 5.0+ software the list of services will include an entry for an ***Enhanced TSPI*** service. This is the service used by the one-X Portal for IP Office service to access the IP Office. You need to ensure that the IP Office security configuration includes a Service User and Right Group configured to use this service.



Name	Security Level
Configuration	Unsecure Only
Security Administrati...	Unsecure Only
System Status Interf...	Unsecure Only
Enhanced TSPI	Unsecure Only

Name: Enhanced TSPI
Host System: IP500 Site A
Service TCP Port: 50814
Service Security Level: Unsecure Only

5. Select **Rights Groups**.

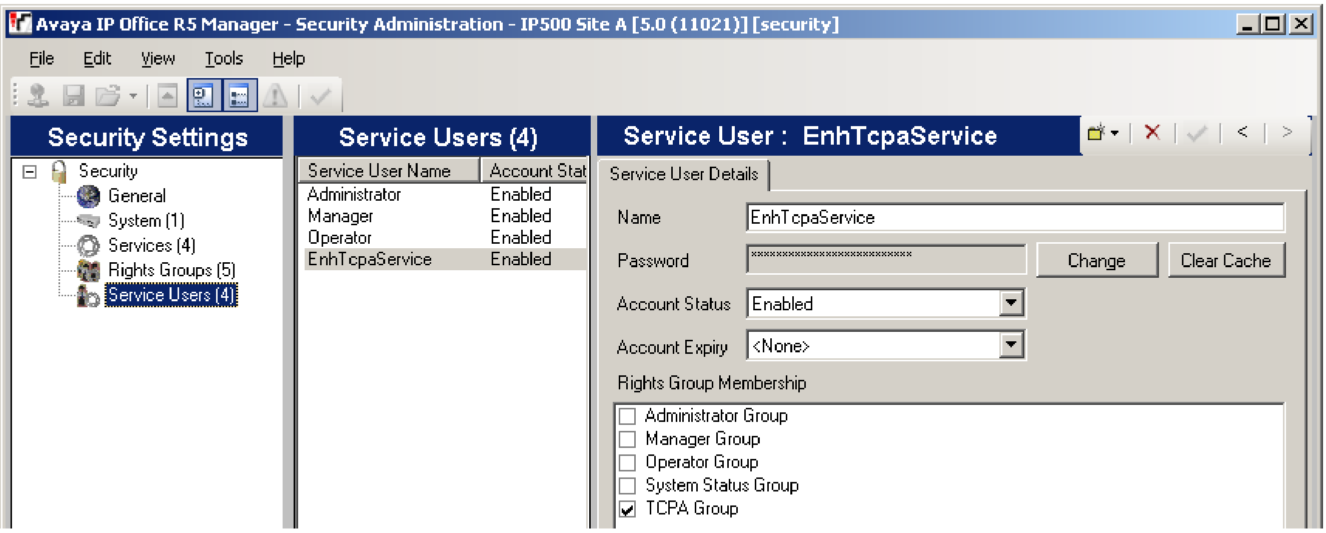


Name
Administrator Group
Manager Group
Operator Group
System Status Group
TCPA Group

Enhanced TSPI Access Rights
☑ Enhanced TSPI Access

6. The list of **Rights Groups** should contain a group called ***TCPA Group***. Select this group and then the **Enhanced TSPI** tab. The option for **Enhanced TSPI Access** should be selected as shown above. If this is not the case correct the security settings, creating a new group of necessary.

7. Select **Service Users**.



Avaya IP Office R5 Manager - Security Administration - IP500 Site A [5.0 (11021)] [security]

Security Settings

- Security
  - General
  - System (1)
  - Services (4)
  - Rights Groups (5)
  - Service Users (4)

Service Users (4)

Service User Name	Account Stat
Administrator	Enabled
Manager	Enabled
Operator	Enabled
EnhTcpaService	Enabled

Service User : EnhTcpaService

Service User Details

Name: EnhTcpaService

Password: ************************** Change Clear Cache

Account Status: Enabled

Account Expiry: <None>

Rights Group Membership

□ Administrator Group
□ Manager Group
□ Operator Group
□ System Status Group
☑ TCPA Group

8. The list of **Service Users** should include a user called ***EnhTcpaService***. In the service user details this user should be set as a member of the **TCPA Group**. If this is not the case correct the security settings, creating a new user if necessary. The user password should be ***EnhTcpaPwd1***.

9. If you have had to make changes to the security settings, click on the 💾 icon to save the new security settings.

2.3 Add Licenses

Each user for one-X Portal for IP Office must be configured to a user profile 21 that includes support for one-X Portal for IP Office. User profiles other than ***Basic User***, which does not include support for one-X Portal for IP Office usage, required an appropriate user profile license in the IP Office system configuration.

It is strongly recommended that these licenses are added to the IP Office configuration and validated before one-X Portal for IP Office is installed. Each license is specific to the serial number of the IP Office system's Feature Key serial number and licenses a specific number of users. Multiple licenses can be added for a larger total number of users.

- Users licensed and configured with the ***Office User***, ***Teleworker User*** or ***Power User*** profiles can be configured for as one-X Portal for IP Office users. Those licensed and configured for with ***Teleworker User*** or ***Power User*** profiles can also be enabled for one-X Portal for IP Office telecommuter mode.
  - For systems being upgraded from IP Office Release 5, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for IP Office for users set to the ***Basic User*** profile.
- Users can refresh their browser without being logged out. All data will be retrieved from the server as if they had just logged in again. The user can also navigate to another website and back to one-X Portal for IP Office and still be logged in. If the user presses the **Esc** button, they will be prompted whether they wish to log out. If they do not, the browser will be refreshed. With some browsers, for example Firefox, if a user closes the browser without logging out, when they reopen the browser they will be logged straight back in. If a user closes their browser rather than logging out, the license they were using will remain consumed by them for up to 6 hours.

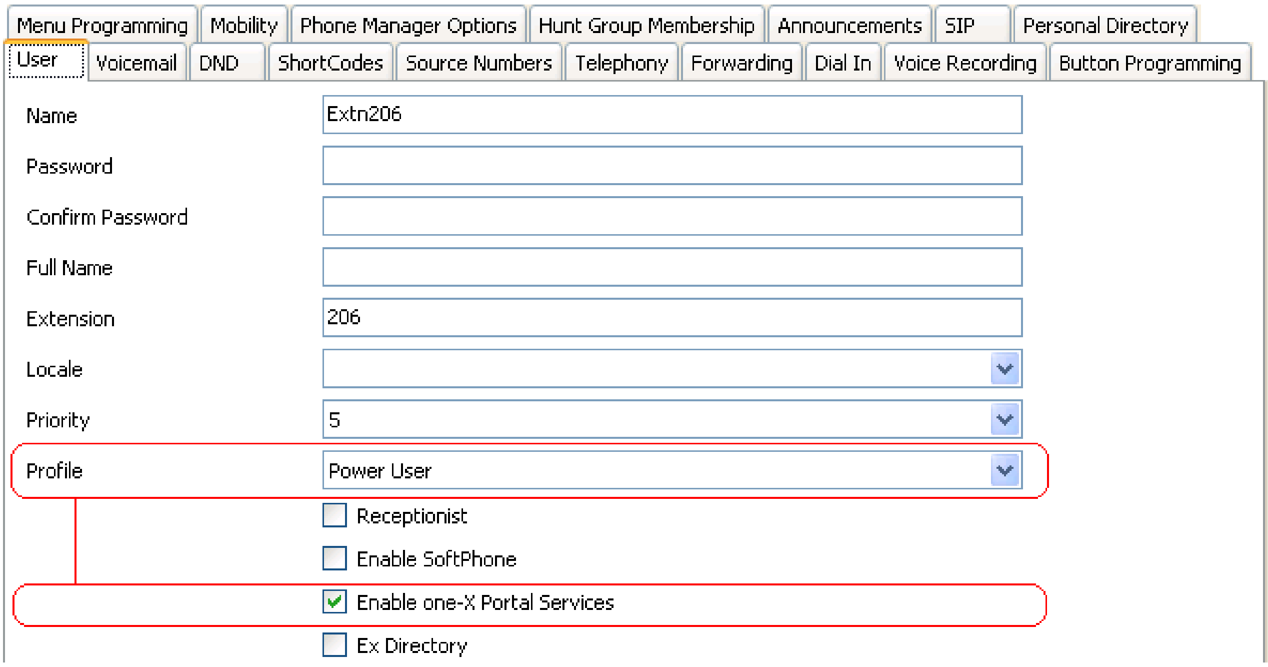
1. Start IP Office Manager and click on the icon.
2. Select the IP Office and click **OK**.
3. Enter the user name and password for access to the IP Office's configuration settings.
4. Click on **License**.
5. Click on to enter a new license.
6. Enter the license or licenses provided for one-X Portal for IP Office operation on that system.
7. If the license has been entered correctly, the **License Type** will shown. The **License Status** will be ***Unknown***. The **Instances** will show the number of users who can now be configured for one-X Portal for IP Office operation using that license.
8. Click on 💾 to save the updated configuration back to the IP Office system.
9. Reload the IP Office configuration and select **License** again.
10. Check that the **License Status** is now ***Valid***.
11. Repeat this process for any other IP Office's that will be supported by the one-X Portal for IP Office server.

2.4 Configure Users

Once the appropriate licenses have been added to the IP Office system's configuration, selected user's can have the user one-X Portal for IP Office option enabled. It is strongly recommended that at least one user on each IP Office system to be supported is configured as a one-X Portal for IP Office user before the one-X Portal for IP Office server is installed.

- Users licensed and configured with the ***Office User***, ***Teleworker User*** or ***Power User*** profiles can be configured for as one-X Portal for IP Office users. Those licensed and configured for with ***Teleworker User*** or ***Power User*** profiles can also be enabled for one-X Portal for IP Office telecommuter mode.
    - For systems being upgraded from IP Office Release 5, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for IP Office for users set to the ***Basic User*** profile.

1. Start IP Office Manager and click on the icon.
2. Select the IP Office and click **OK**.
3. Enter the user name and password for access to the IP Office's configuration settings.
4. Click on **User**.
5. Select the user who you want to enable for one-X Portal for IP Office operation.
6. Select the **User** tab.



Name	Extn206
Password	
Confirm Password	
Full Name	
Extension	206
Locale	
Priority	5
Profile	Power User

□ Receptionist

□ Enable SoftPhone

☑ Enable one-X Portal Services

□ Ex Directory

7. Select the **Profile** which you want the user to use and for which the IP Office system has licenses. For one-X Portal for IP Office, the supported profiles are ***Office User***, ***Teleworker User*** or ***Power User***. The later two are also able to support the one-X Portal for IP Office telecommuter features.
8. Check that the **Enable one-X Portal Services** check box is selected.
9. Note the user **Name** and **Password**. These are used by the user to login to one-X Portal for IP Office.
    - For analog phone users, the user's **Call Waiting On** and **Off Hook Station** settings should be selected in the user's IP Office configuration.
10. Repeat the process for any other users who will be using one-X Portal for IP Office services.
11. Click on to save the updated configuration back to the IP Office system.

2.5 Checking Available Server Ports

The one-X Portal for IP Office application installs as a service (*Avaya one-X Portal*) listening on a port. By default it uses port 8080. The backup and restore service 80 also use port 8666 by default.

It is important to check that these ports are not already in use by other applications. If they are, a different unused port number should be specified during the one-X Portal for IP Office software installation. The only way to change the ports following installation is to remove and then reinstall the software 51.

Whichever ports are selected, ensure that incoming TCP access to those ports is allowed in the server's firewall exceptions.

- **Ports Used by the one-X Portal for IP Office**
  In addition to the ports used to access the one-X Portal for IP Office server from a browser client, various components of the one-X Portal for IP Office also use ports to communicate. The full set of ports used by one-X Portal for IP Office are listed below.
  - **4560** - This port is used by log4j socket appender.
  - **8080** - Default HTTP browser access port. This port number can be changed during installation.
  - **8443** - Used for HTTPS access to one-X Portal
  - **8005** - Used by the Tomcat shutdown listener
  - **9092** - The database component of the one-X Portal for IP Office uses this port.
  - **8666** - This port is used by the JVMX component of the one-X Portal for IP Office. This port number can be changed during installation.

- **Listing Ports Already in Use**
  To check which ports are already in use on the server, the command **netstat -an > ports.txt** can be used. This will create a text file ***ports.txt*** listing all the ports on which the server is currently listening. Check that none of the ports required by one-X Portal for IP Office are already in use. If they are, there will be a conflict between the application already using the port and one-X Portal for IP Office when one-X Portal for IP Office is installed.

- **Reserved Ports**
  There are a number of ports used by other Avaya IP Office applications. If any of these are specified during installation, the installer will ignore the selection and default to installing on port 8080. Examples of reserved ports are:
  - **8089** - Default port used by IP Office Conferencing Center application.
  - **8888** - Default port used by ContactStore for IP Office.

- **Other Commonly Used Ports**
  Ports in the 8000 range are also frequently used by other applications.
  - **8081** - Default port used by IIS for Sharepoint Administration access.

2.6 Install the one-X Portal for IP Office Software

Linux Server

The Linux based version of one-X Portal for IP Office is installed as one of the selectable application in the IP Office Application Server installation process. For details of that process refer to the IP Office Application Server Installation Manual.

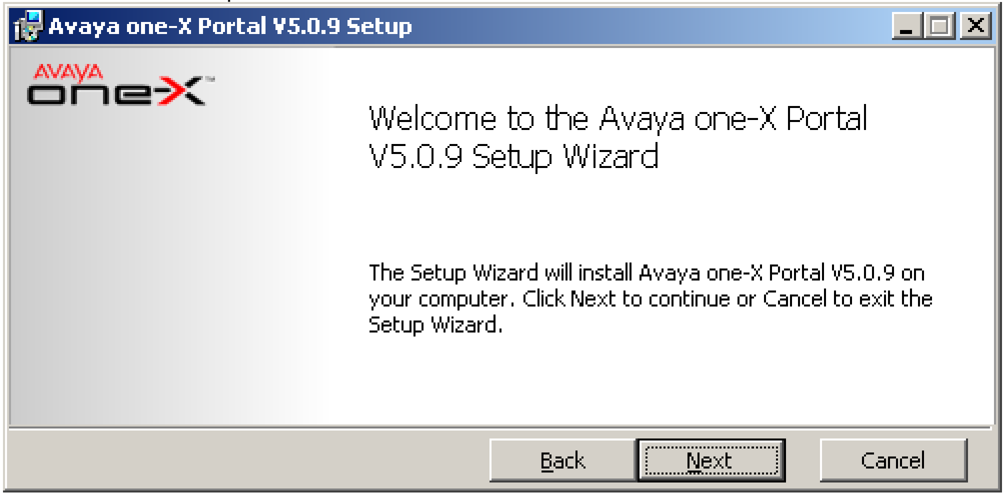
Windows Server

The following process is used for installation of the one-X Portal for IP Office software on a Windows server. It is strongly recommended that you do not start software installation until the previous installation steps (IP Office security settings 18, one-X Portal for IP Office licenses 20, user configuration 21) have been completed.

1. Check that you have logged in on the server using an account with full administrator rights.

   - **! WARNING: Windows 2008 Server Installation**
     For installation on a Windows 2008 server, ensure that **User Account Control (UAC)** is switched off before beginning the installation. This is done through the **User Accounts** section of the Windows Control Panel. When doing this you may be required to restart the server. Failure to switch off UAC during installation will cause operating system issues. It can be re-enabled once installation is complete.

2. On the IP Office Application DVD, locate and double-click on the file **one-Xportal.msi** file to start the server software installation process.

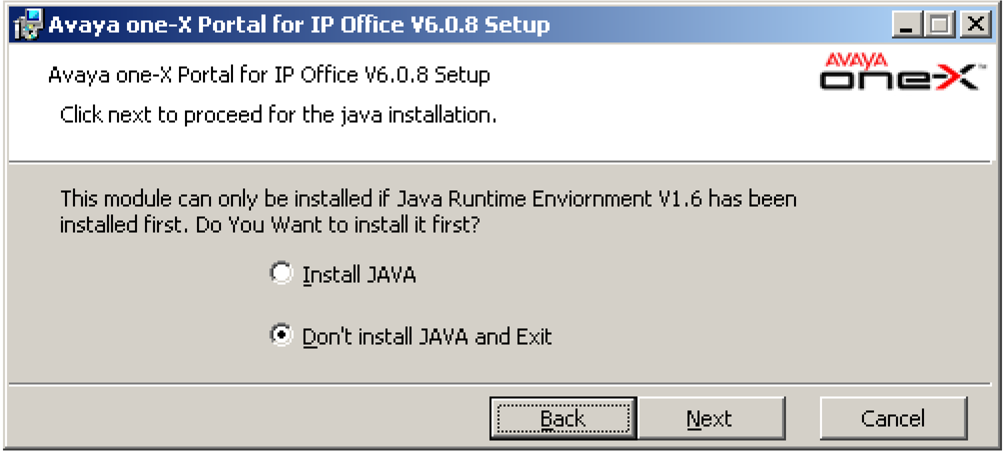


Avaya one-X Portal V5.0.9 Setup

Welcome to the Avaya one-X Portal V5.0.9 Setup Wizard

The Setup Wizard will install Avaya one-X Portal V5.0.9 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Click **Next**. If Java is not installed on the server, the one-X Portal for IP Office installer will offer to install it.



Avaya one-X Portal for IP Office V6.0.8 Setup

Avaya one-X Portal for IP Office V6.0.8 Setup

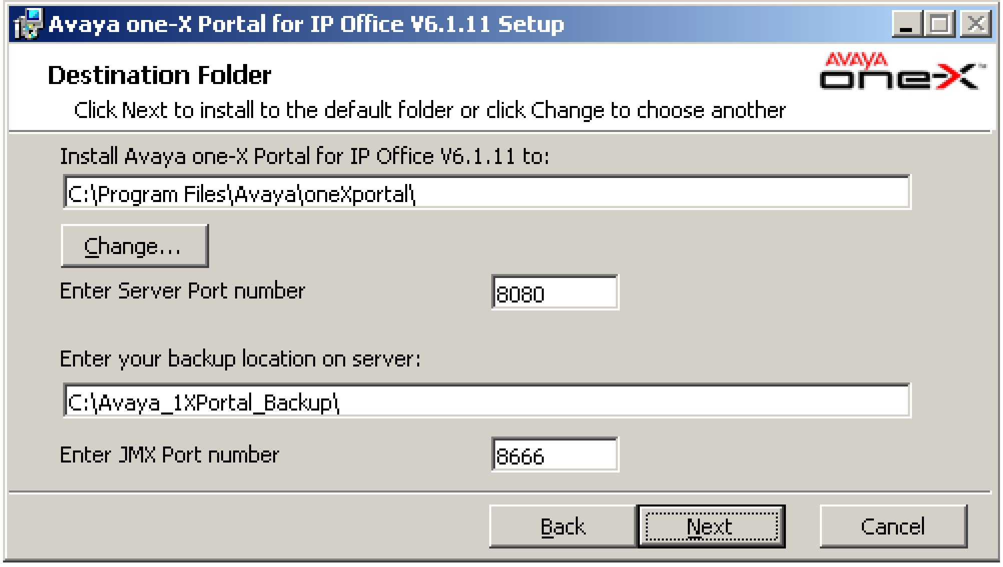
Click next to proceed for the java installation.

This module can only be installed if Java Runtime Enviornment V1.6 has been installed first. Do You Want to install it first?

○ Install JAVA

● Don't install JAVA and Exit

4. Select **Install Java** and click **Next**. Unless there is a reason to do otherwise, we recommend that you leave the default installation paths unchanged.



Avaya one-X Portal for IP Office V6.1.11 Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another

Install Avaya one-X Portal for IP Office V6.1.11 to:

C:\Program Files\Avaya\oneXportal\

Change...

Enter Server Port number: 8080

Enter your backup location on server:

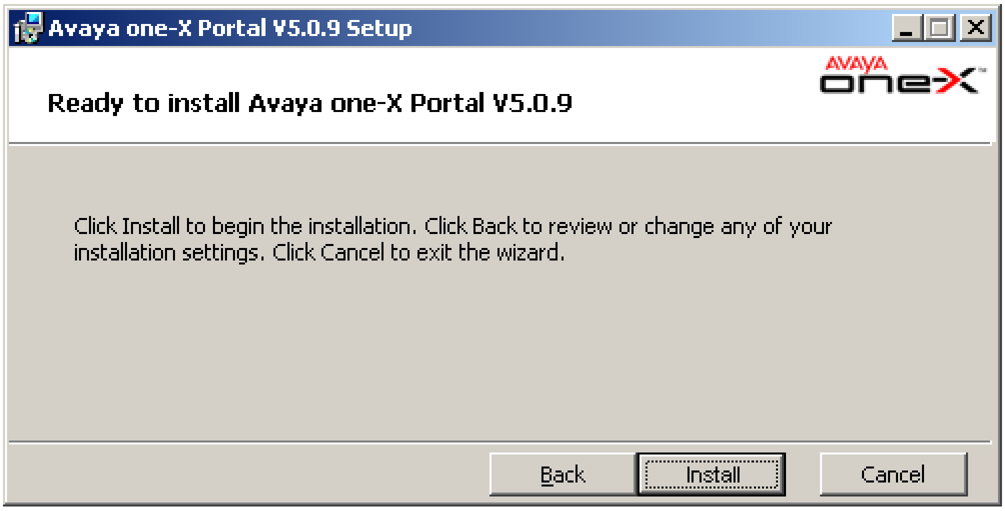
C:\Avaya_1XPortal_Backup\

Enter JMX Port number: 8666

- **Enter Server Port number:** *Default = 8080*
  If the server PC already has services using port 8080 (see Checking Available Ports 22), enter a new unused port number here. Note that once one-X Portal for IP Office is installed, the port number can only be changed by removing and then reinstalling the one-X Portal for IP Office software.

- **Enter JMX Port Number:** *Default = 8666*
  This is the port used for the one-X Portal for IP Office's backup and restore 80 services.

5. Click **Next**.

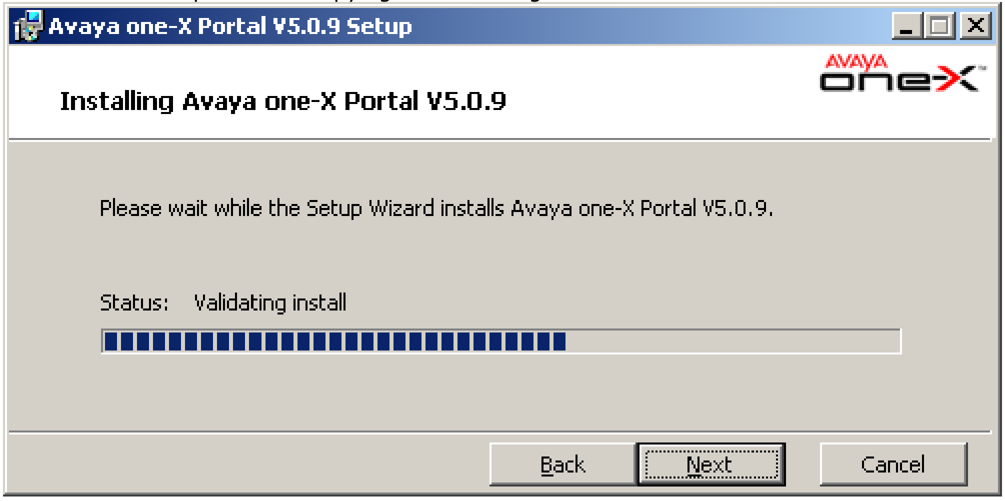


Avaya one-X Portal V5.0.9 Setup

Ready to install Avaya one-X Portal V5.0.9

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

6. Click **Install**. The process of copying and installing files is started.



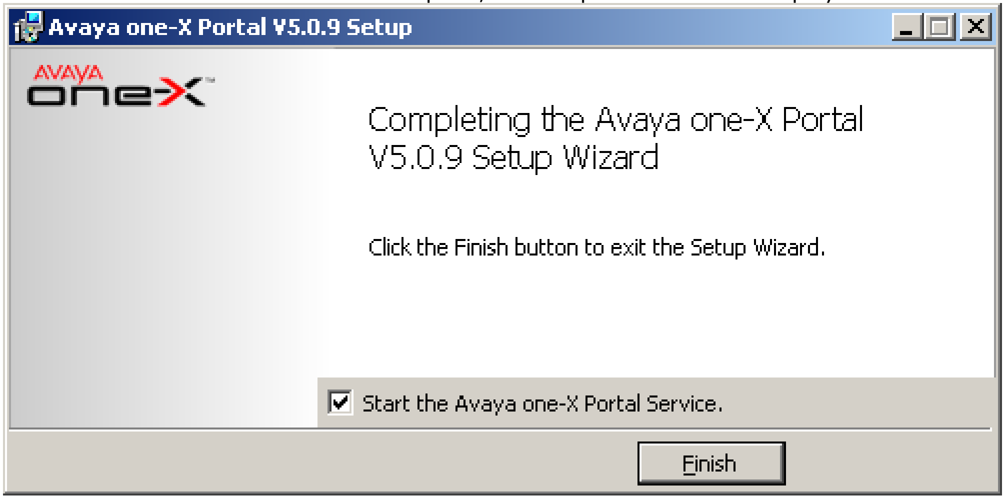
Avaya one-X Portal V5.0.9 Setup

Installing Avaya one-X Portal V5.0.9

Please wait while the Setup Wizard installs Avaya one-X Portal V5.0.9.

Status: Validating install

7. When installation of the software is complete, the completion screen is displayed.



Avaya one-X Portal V5.0.9 Setup

Completing the Avaya one-X Portal V5.0.9 Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Start the Avaya one-X Portal Service.

8. Select **Start the Avaya one-X Portal Service**. If you do not select this option, the Avaya one-X Portal service will need to be started manually 35 before it can be configured.

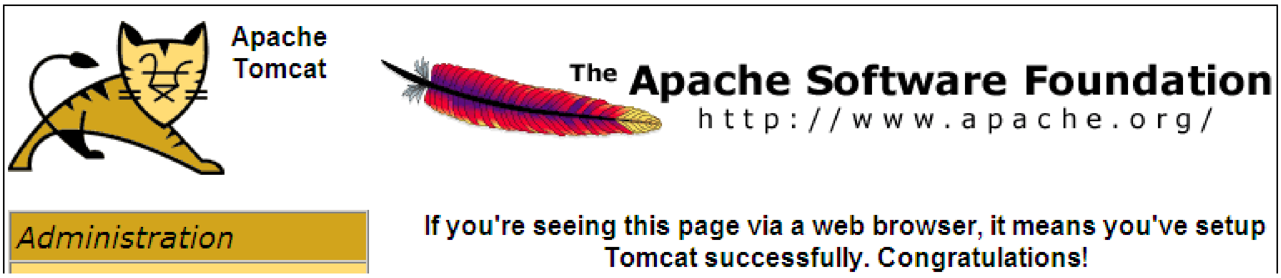
9. Click on **Finish**.

10. Proceed to Initial Server Configuration 26.

2.7 Initial Server Configuration

At this stage, the one-X Portal for IP Office server software has been installed 23 and the service started. However the one-X Portal for IP Office server still requires initial configuration. During this configuration it will connect to the IP Office systems.

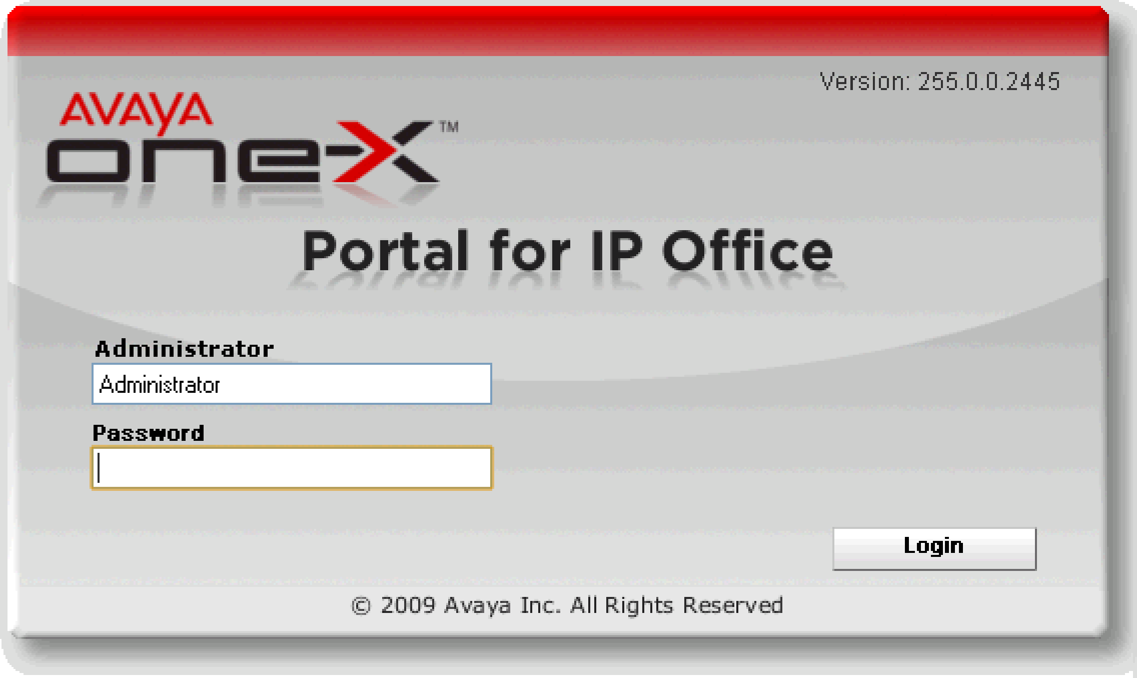
1. Enter the address of the one-X Portal for IP Office server with :8080 added, that is ***http://<server_address>:8080***. The web server installed as part of the one-X Portal for IP Office should respond with its default web page. If using a browser on the server PC, enter ***http://127.0.0.1:8080***. If the software was installed using a different port number, replace the 8080 with that port number.



If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

- If the services has only just been started, you will have to wait a while. This can take up to 15 minutes. One way to monitor progress is to use Windows Task Manager. Typically the **PF Usage** will gradually increase. Once is reaches approximately 2.3GB, the services will have started.

2. Add ***inyama/inyama.html?admin=true*** to the browser address. This is the login path for the administrator access to the one-X Portal for IP Office application.



Version: 255.0.0.2445

Administrator: Administrator

Password

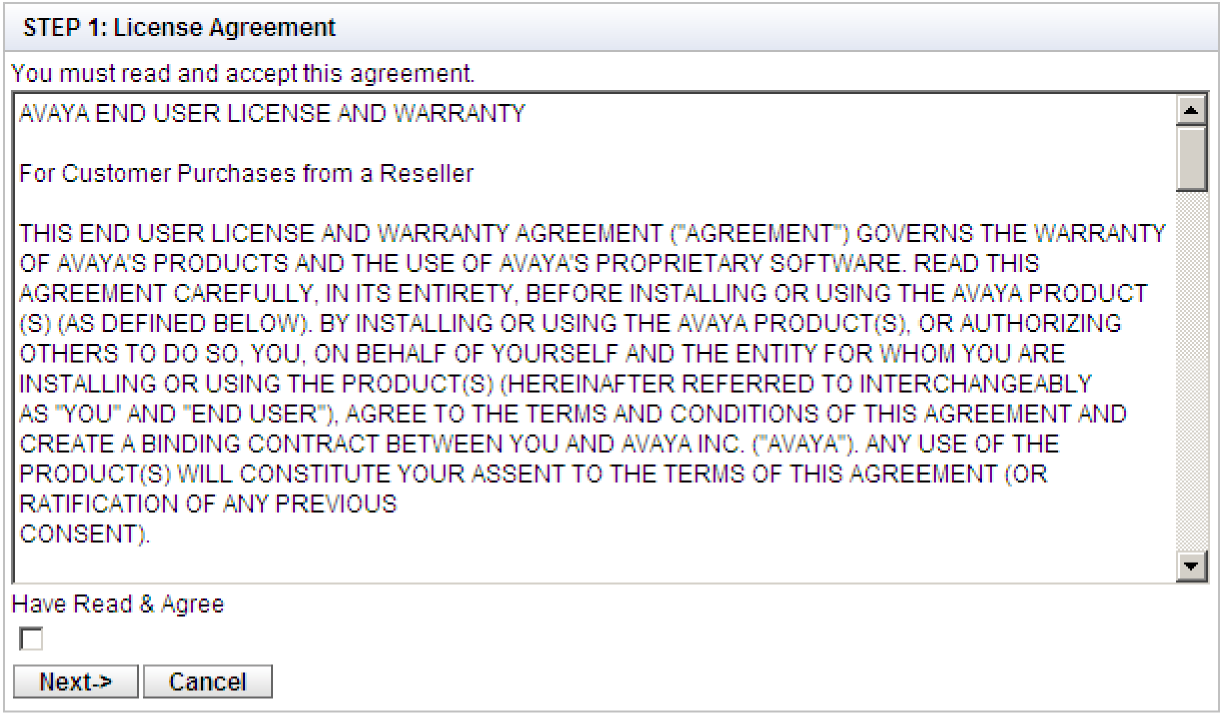
© 2009 Avaya Inc. All Rights Reserved

3. The message ***System is currently unavailable - please wait*** may be displayed if the one-X Portal for IP Office application is still starting. When the message disappears approximately 15 minutes after the one-X Portal for IP Office service was started, you can login.

4. Check that the version reported matches the version expected. If not refer to the Troubleshooting 57 section.

5. Enter the default administrator name (***Administrator***) and password (***Administrator***) and click **Login**.

6. The **License Agreement** page is displayed.



STEP 1: License Agreement

You must read and accept this agreement.

AVAYA END USER LICENSE AND WARRANTY

For Customer Purchases from a Reseller

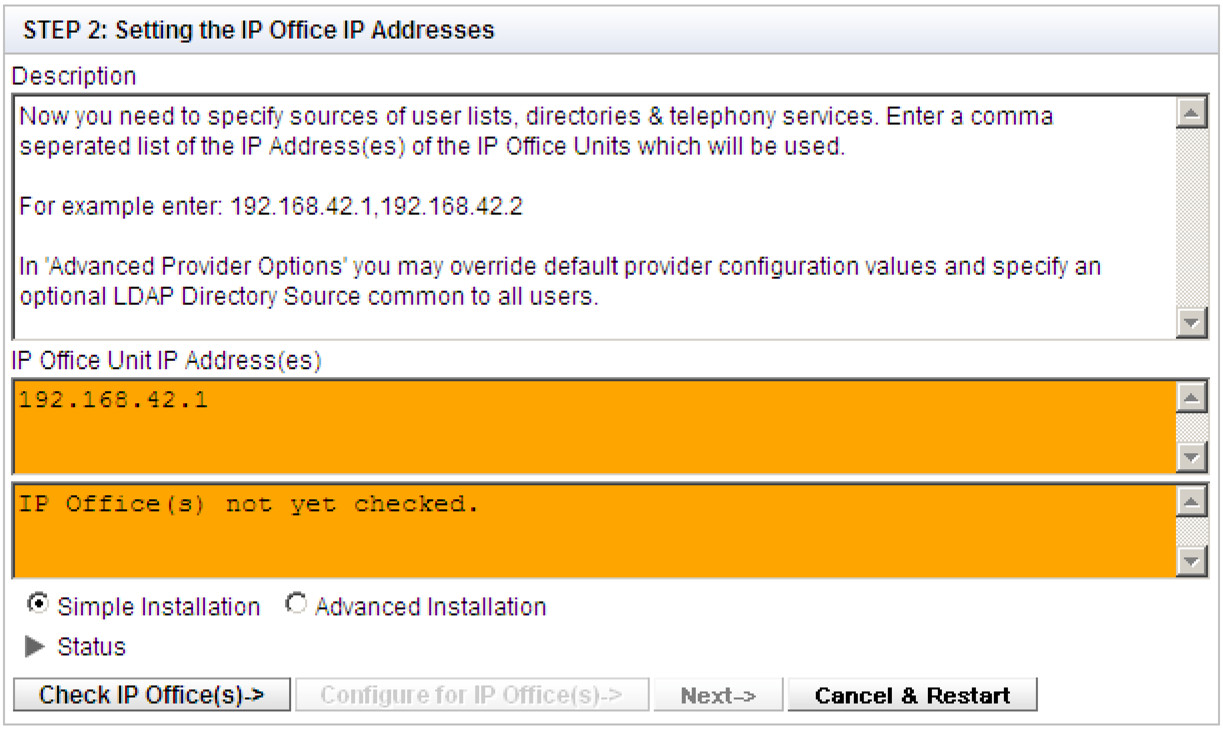
THIS END USER LICENSE AND WARRANTY AGREEMENT ("AGREEMENT") GOVERNS THE WARRANTY OF AVAYA'S PRODUCTS AND THE USE OF AVAYA'S PROPRIETARY SOFTWARE. READ THIS AGREEMENT CAREFULLY, IN ITS ENTIRETY, BEFORE INSTALLING OR USING THE AVAYA PRODUCT (S) (AS DEFINED BELOW). BY INSTALLING OR USING THE AVAYA PRODUCT(S), OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING OR USING THE PRODUCT(S) (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. ("AVAYA"). ANY USE OF THE PRODUCT(S) WILL CONSTITUTE YOUR ASSENT TO THE TERMS OF THIS AGREEMENT (OR RATIFICATION OF ANY PREVIOUS
CONSENT).

Have Read & Agree

□

7. When you have read the license, select **Have Read & Agree** and then click on **Next**.

8. The menu now allows entry of the IP addresses of the IP Office systems to which you want the one-X Portal for IP Office server to connect.



STEP 2: Setting the IP Office IP Addresses

Description

Now you need to specify sources of user lists, directories & telephony services. Enter a comma seperated list of the IP Address(es) of the IP Office Units which will be used.

For example enter: 192.168.42.1,192.168.42.2

In 'Advanced Provider Options' you may override default provider configuration values and specify an optional LDAP Directory Source common to all users.

IP Office Unit IP Address(es)

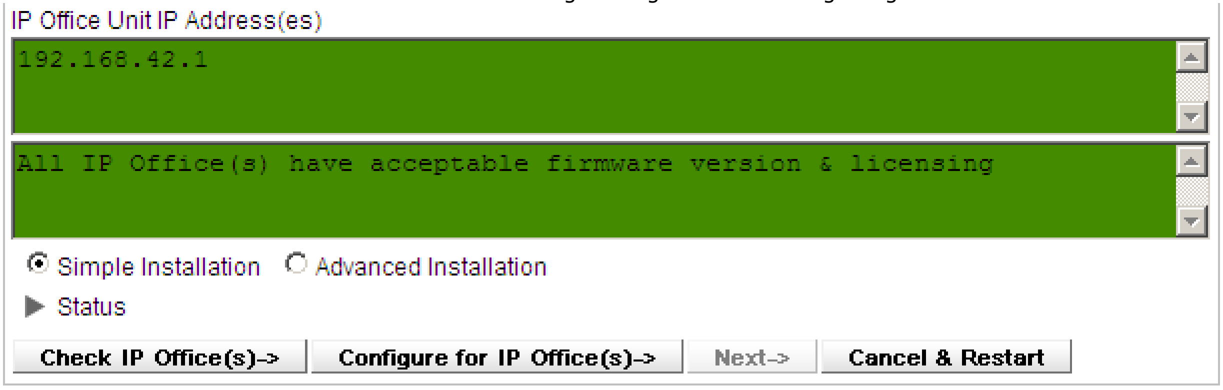
```
192.168.42.1
```

```
IP Office(s) not yet checked.
```

● Simple Installation ○ Advanced Installation

- In the following menus, the ▶ **Status** icon can be used to show/hide status messages about the actions being performed by the installation process.

9. Enter the addresses in the form and select **Check IP Office(s)**. The one-X Portal for IP Office server will attempt to connect to each of the indicated IP Offices. The orange background will change to green is this is successful.



IP Office Unit IP Address(es)

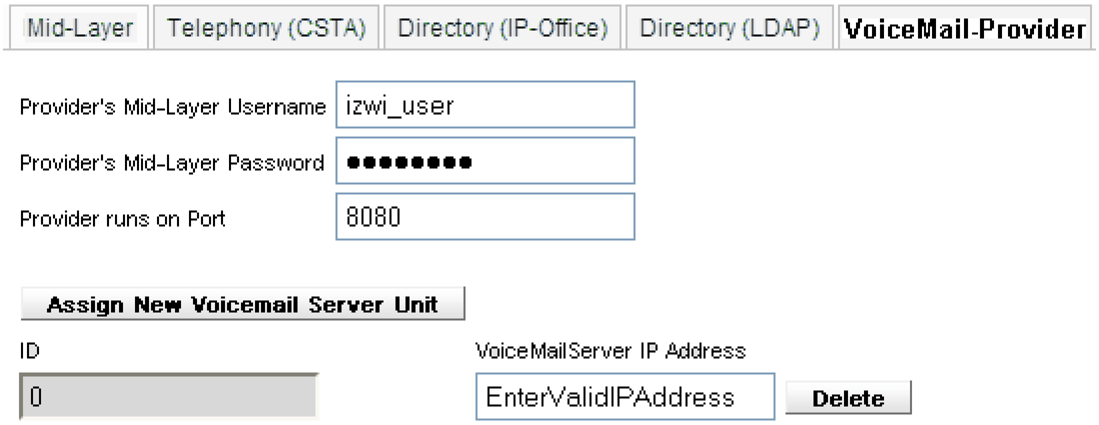
192.168.42.1

All IP Office(s) have acceptable firmware version & licensing

● Simple Installation ○ Advanced Installation

10. If the customer has a Voicemail Pro voicemail server, click on **Advanced Installation**.

- Click on the **Voicemail Provider** tab and enter the IP address of the Voicemail Pro voicemail server. For IP Offices in a Small Community this should be the address of the centralized voicemail server (not that of the backup or any distributed voicemail servers). For embedded voicemail enter the IP Office system's own IP address.



Provider's Mid-Layer Username: izwi_user

Provider's Mid-Layer Password: ●●●●●●●●●

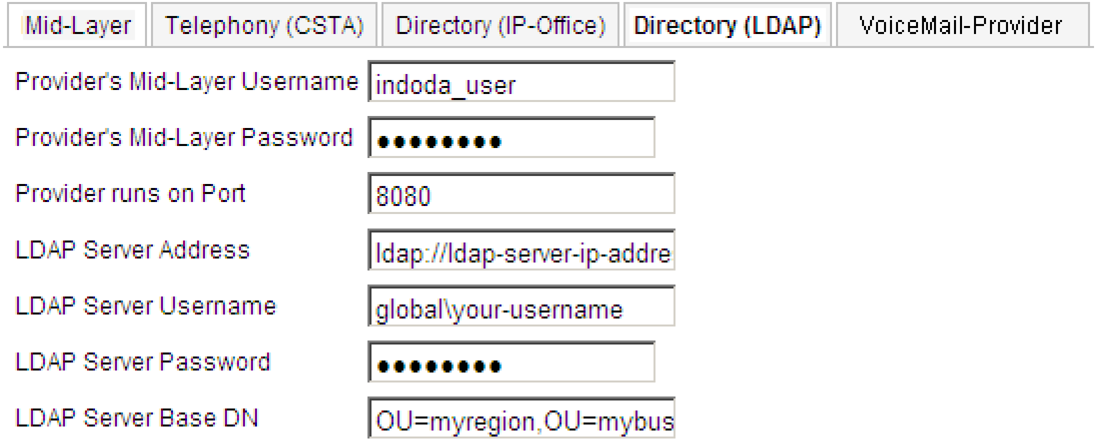
Provider runs on Port: 8080

ID: 0

VoiceMailServer IP Address: EnterValidIPAddress

11. If the customer has provided details of an LDAP directory source, click on **Advanced Installation** if not already selected.

- Click on the **Directory (LDAP)** tab. Enter the LDAP server information into the fields labeled LDAP.



Provider's Mid-Layer Username: indoda_user

Provider's Mid-Layer Password: ●●●●●●●●

Provider runs on Port: 8080

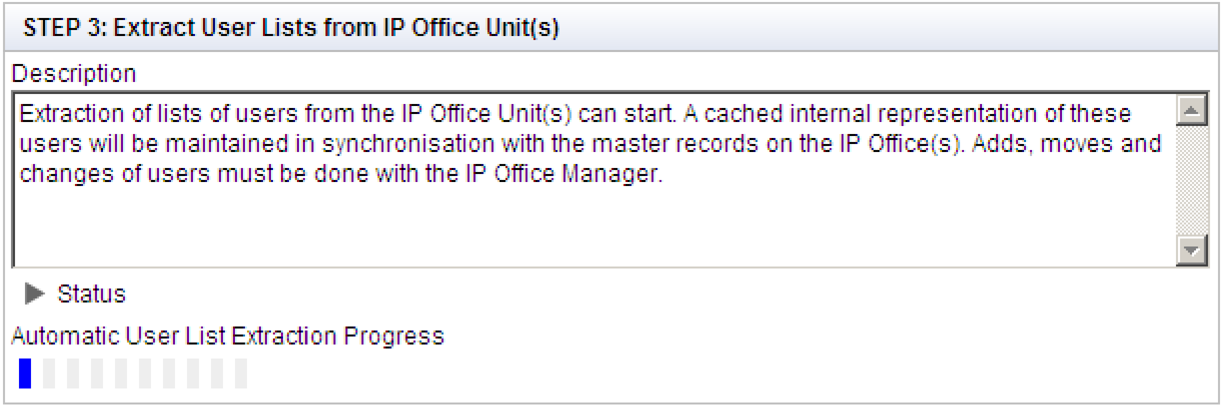
LDAP Server Address: ldap://ldap-server-ip-addre

LDAP Server Username: global\your-username

LDAP Server Password: ●●●●●●●●

LDAP Server Base DN: OU=myregion,OU=mybus

12. Click on **Configure for IP Office(s)**. The one-X Portal for IP Office server will connect with each IP Office and automatically extract details of the IP Office users. If **Simple Installation** was selected, the installer will go through this and the following steps automatically. If **Advanced Installation** was selected, the installer will require you to select **Next** after each step.



STEP 3: Extract User Lists from IP Office Unit(s)

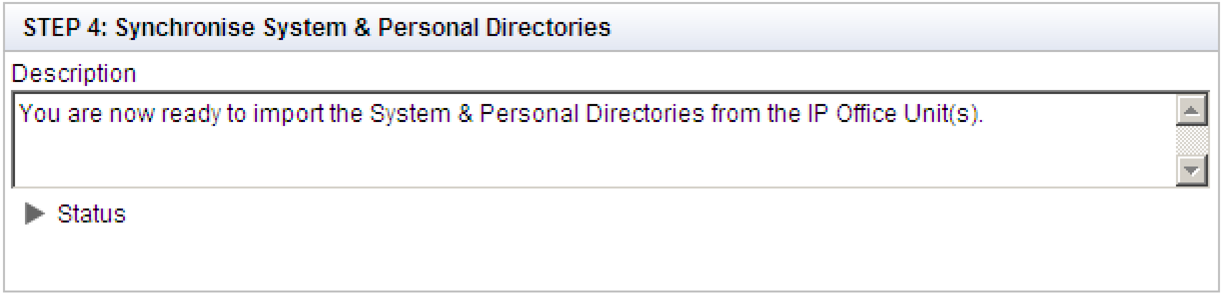
Description

Extraction of lists of users from the IP Office Unit(s) can start. A cached internal representation of these users will be maintained in synchronisation with the master records on the IP Office(s). Adds, moves and changes of users must be done with the IP Office Manager.

▶ Status

Automatic User List Extraction Progress

13. Having extracted user details, the one-X Portal for IP Office server will extract directory details from the IP Office systems.



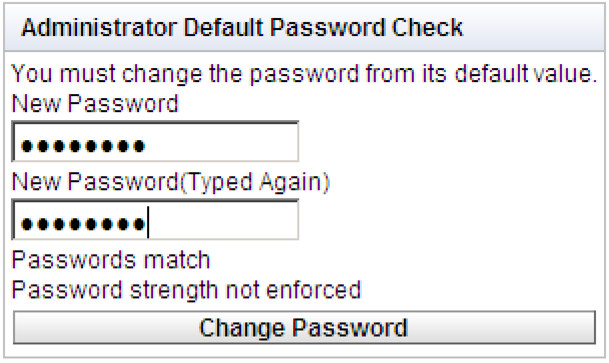
STEP 4: Synchronise System & Personal Directories

Description

You are now ready to import the System & Personal Directories from the IP Office Unit(s).

▶ Status

14. The one-X Portal for IP Office server will now prompt you to change the password used for administrator access.



Administrator Default Password Check

You must change the password from its default value.

New Password: ●●●●●●●●

New Password(Typed Again): ●●●●●●●●●

Passwords match

Password strength not enforced

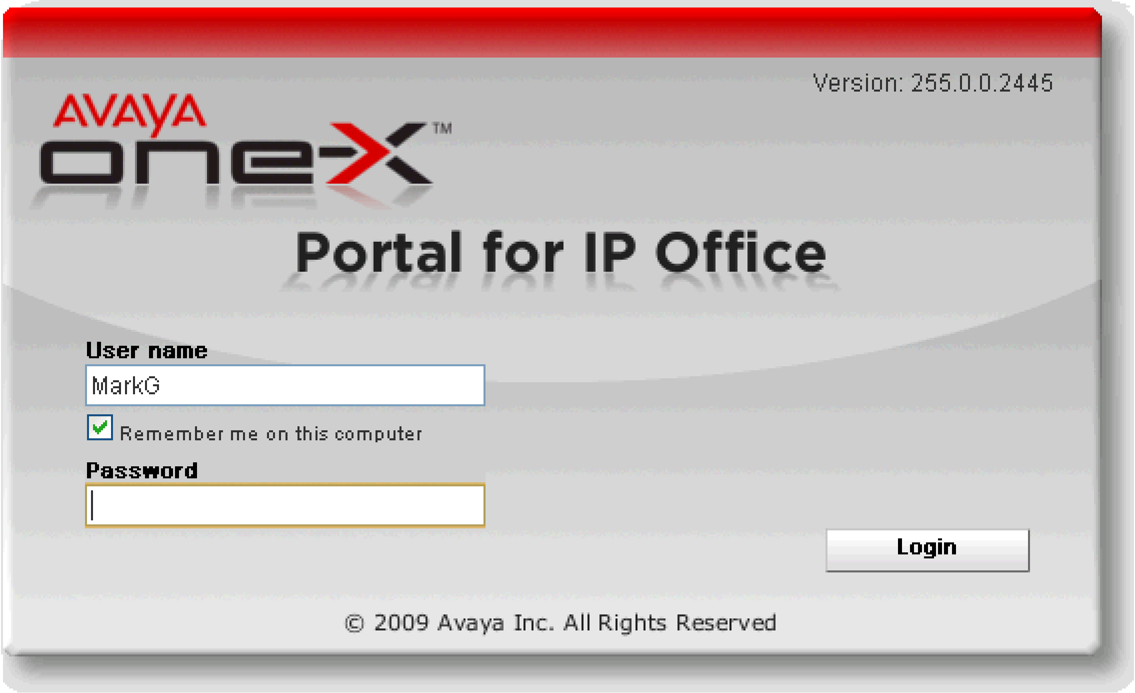
15. Enter a new password and click **Change Password**.

16. The initial configuration is complete. Note that it will still be at least another 5 minutes before the one-X Portal for IP Office is usable by end users.

2.8 Test User Connnection

From a user PC rather than the server PC, check that a user can login to one-X Portal for IP Office and use it to make and answer calls on their phone.

1. From a user PC, uses a web browser to browse to the one-X Portal for IP Office server. Do not add the ***?admin=true*** part to the URL as that is only used for administrator access.



2. Enter the user's name and password.
3. Check that the user can see the system directories and, if configured, search the external directory.
4. Check that the user can see and edit their personal directory.
5. Make a call to the user's extension. The call should be shown within the **Calls** gadget. Answer the call using the **Calls** gadget.
6. Check that the answered call appears in the **Call Log** gadget.
7. Make a call using the **Calls Gadget**.
8. If the IP Office system includes a voicemail server, check that the **Messages** gadget shows messages in the user's mailbox (leave them a message if necessary).
9. Select **Logout** and thank the user nicely.

2.9 Disable Java Updates

one-X Portal for IP Office uses Java and will install Java if not already present on the server. However it is strongly recommended that Java automatic updates are turned off once one-X Portal for IP Office is installed. This can be done through the Java option in the Windows Control Panel.

Chapter 3. Maintenance

3. Maintenance

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

one-X Portal for IP Office 6.1 and higher supports an additional set of backup and restore 80 options.

3.1 Manually Starting the Service

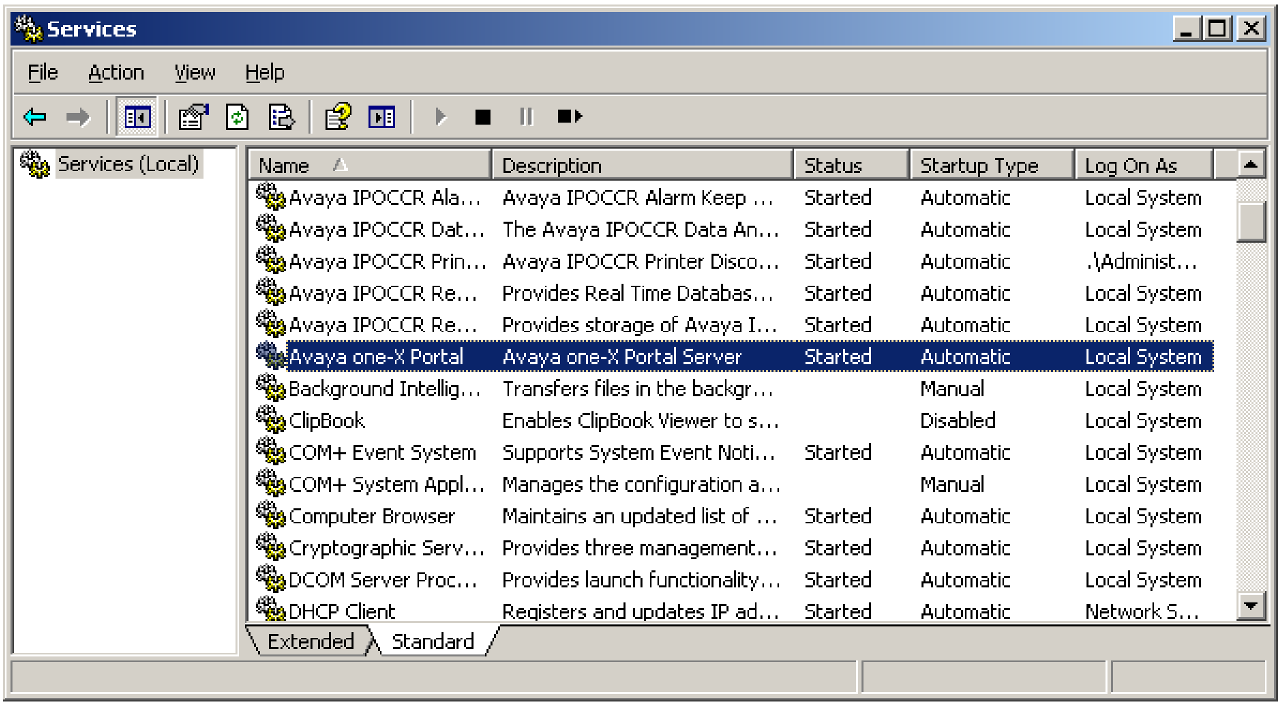
Linux Server

Log into the web controls pages of the IP Office Application server hosting the one-X Portal for IP Office application. The initial **Home** page displays the status of all the applications installed on the server. If the one-X Portal for IP Office application is ***Stopped***, click on the **Start** button to start the application.

The **Auto Start** checkbox can be selected to ensure that the application is always started after any restart of the server.

Windows Server

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



Name	Description	Status	Startup Type	Log On As
Avaya IPOCCR Ala...	Avaya IPOCCR Alarm Keep ...	Started	Automatic	Local System
Avaya IPOCCR Dat...	The Avaya IPOCCR Data An...	Started	Automatic	Local System
Avaya IPOCCR Prin...	Avaya IPOCCR Printer Disco...	Started	Automatic	.\Administ...
Avaya IPOCCR Re...	Provides Real Time Databas...	Started	Automatic	Local System
Avaya IPOCCR Re...	Provides storage of Avaya I...	Started	Automatic	Local System
Avaya one-X Portal	Avaya one-X Portal Server	Started	Automatic	Local System
Background Intellig...	Transfers files in the backgr...		Manual	Local System
ClipBook	Enables ClipBook Viewer to s...		Disabled	Local System
COM+ Event System	Supports System Event Noti...	Started	Automatic	Local System
COM+ System Appl...	Manages the configuration a...		Manual	Local System
Computer Browser	Maintains an updated list of ...	Started	Automatic	Local System
Cryptographic Serv...	Provides three management...	Started	Automatic	Local System
DCOM Server Proc...	Provides launch functionality...	Started	Automatic	Local System
DHCP Client	Registers and updates IP ad...	Started	Automatic	Network S...

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.

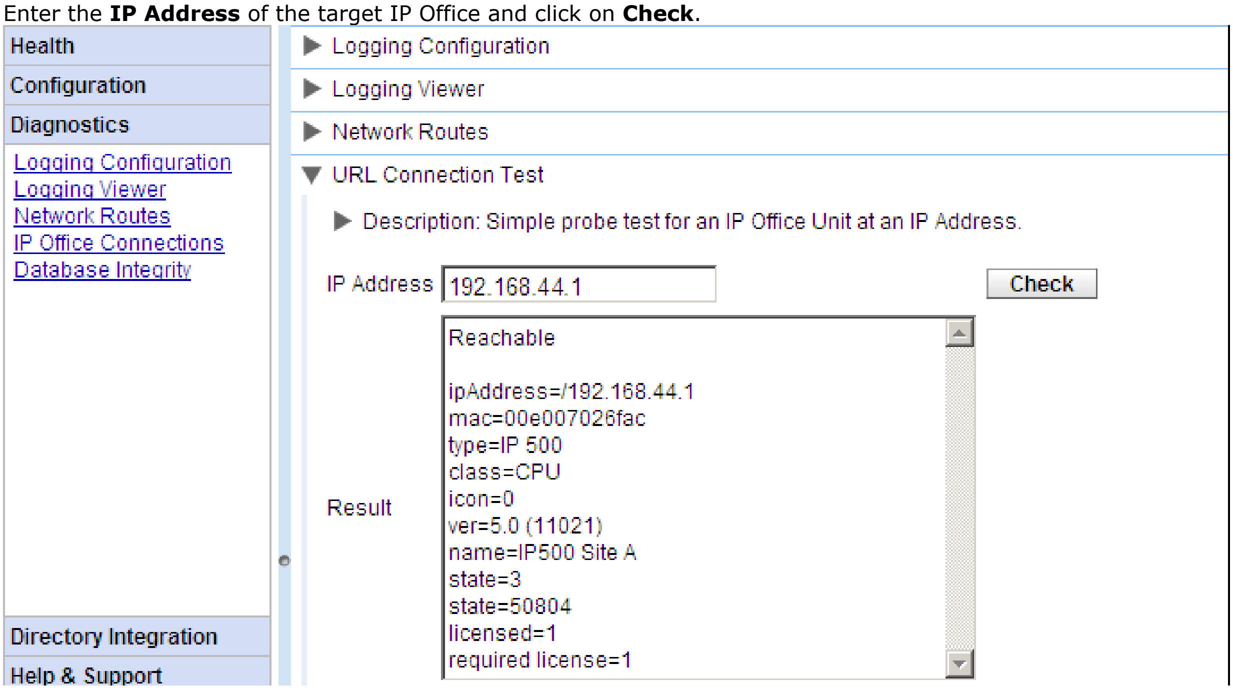
- **No Service !**
  If the service is not present, the most likely cause is a port conflict or Java problem. Refer to Troubleshooting 57.

3.2 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 18 for one-X Portal for IP Office operation.
   - Check that the IP Office is licensed 20 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 21.
2. Log in 61 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**.



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

IP Address 192.168.44.1

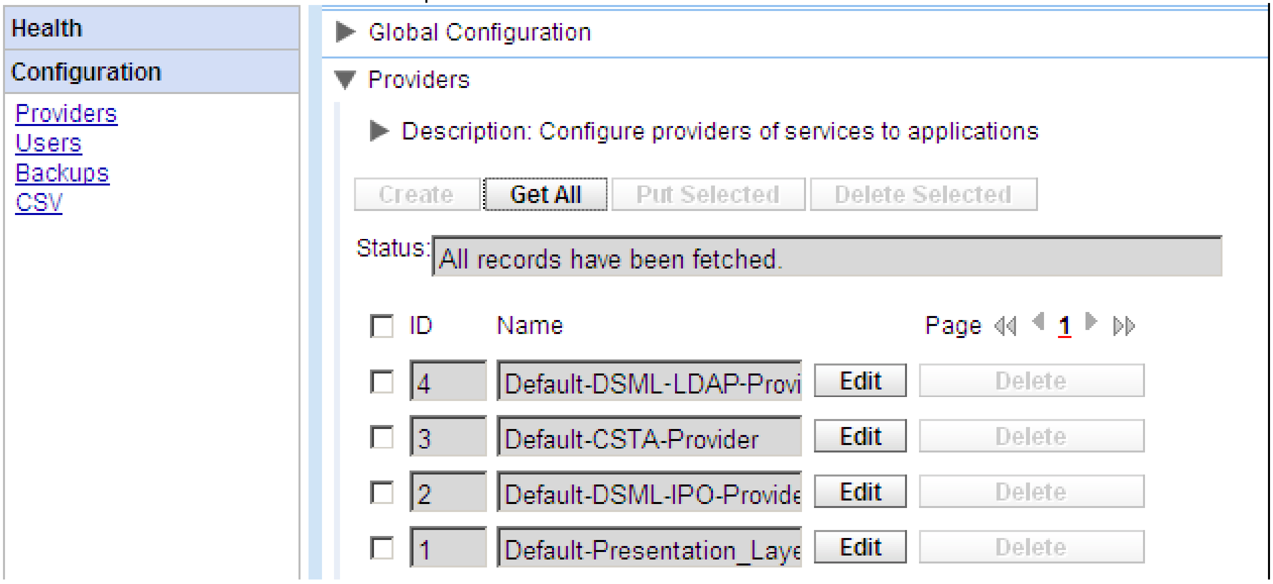
Result

```
Reachable

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

   c. If the IP Office is reachable, the results will include base information about the IP Office system.
4. Select **Configuration** and then **Providers**.

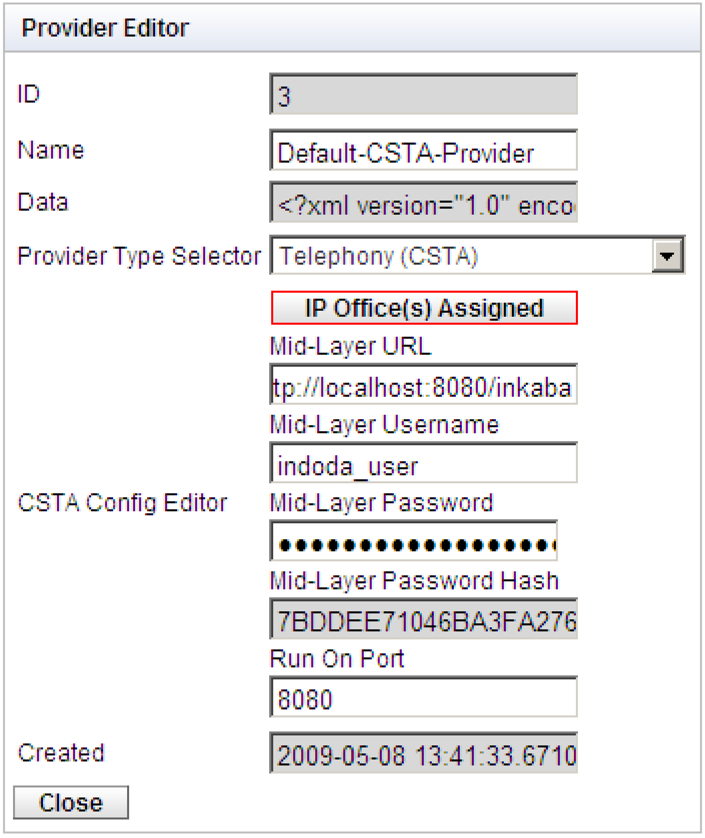
5. Click on **Get All** to retrieve the current provider records from the one-X Portal for IP Office database.



Status: All records have been fetched.

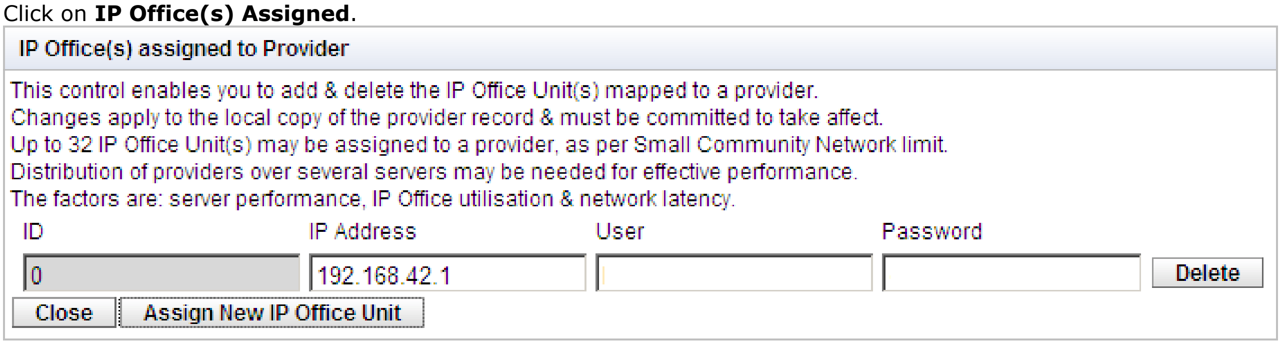
	ID	Name		
□	4	Default-DSML-LDAP-Provi	Edit	Delete
□	3	Default-CSTA-Provider	Edit	Delete
□	2	Default-DSML-IPO-Provide	Edit	Delete
□	1	Default-Presentation_Laye	Edit	Delete

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



ID	3	
Name	Default-CSTA-Provider	
Data	<?xml version="1.0" enco	
Provider Type Selector	Telephony (CSTA)	
CSTA Config Editor	Mid-Layer URL	tp://localhost:8080/inkaba
	Mid-Layer Username	indoda_user
	Mid-Layer Password	•••••••••••••••••
	Mid-Layer Password Hash	7BDDEE71046BA3FA276
	Run On Port	8080
Created	2009-05-08 13:41:33.6710	

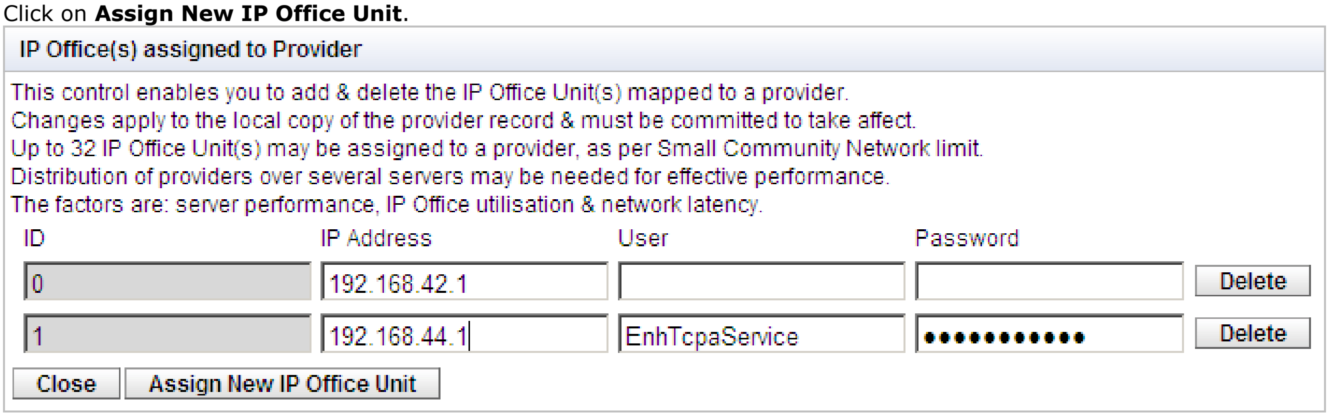
7. Click on **IP Office(s) Assigned**.



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

ID	IP Address	User	Password
0	192.168.42.1		

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



IP Office(s) assigned to Provider

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

ID	IP Address	User	Password	
0	192.168.42.1			Delete
1	192.168.44.1	EnhTcpaService	●●●●●●●●●●●	Delete

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.

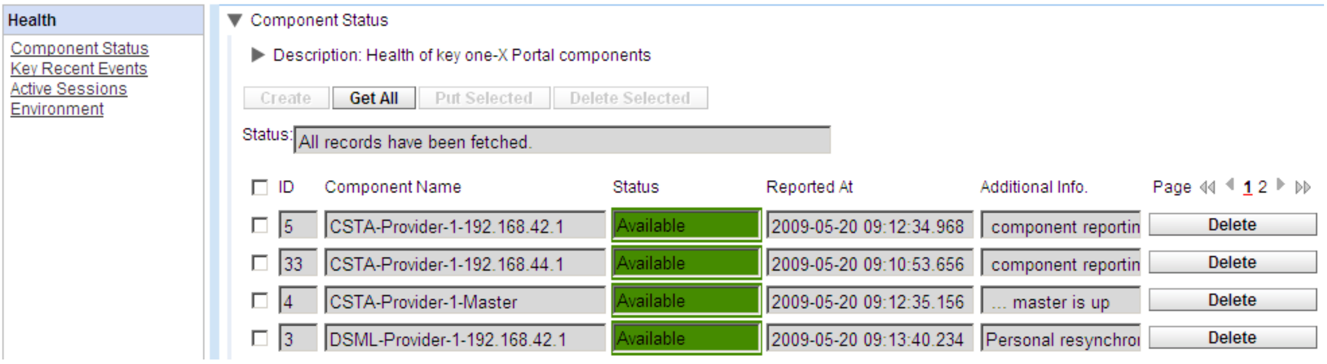
14. Repeat the process but this time adding the new IP Office to the IP Offices assigned to the ***Default- DSML-IPO-Provider***. Again end with **Put Selected**.

15. Restart the Avaya one-X Portal service 35.

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.



Status: All records have been fetched.

□ ID	Component Name	Status	Reported At	Additional Info.	Page ◀◀ ◀ 1 2 ▶ ▶▶
□ 5	CSTA-Provider-1-192.168.42.1	Available	2009-05-20 09:12:34.968	component reportin	Delete
□ 33	CSTA-Provider-1-192.168.44.1	Available	2009-05-20 09:10:53.656	component reportin	Delete
□ 4	CSTA-Provider-1-Master	Available	2009-05-20 09:12:35.156	... master is up	Delete
□ 3	DSML-Provider-1-192.168.42.1	Available	2009-05-20 09:13:40.234	Personal resynchroi	Delete

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

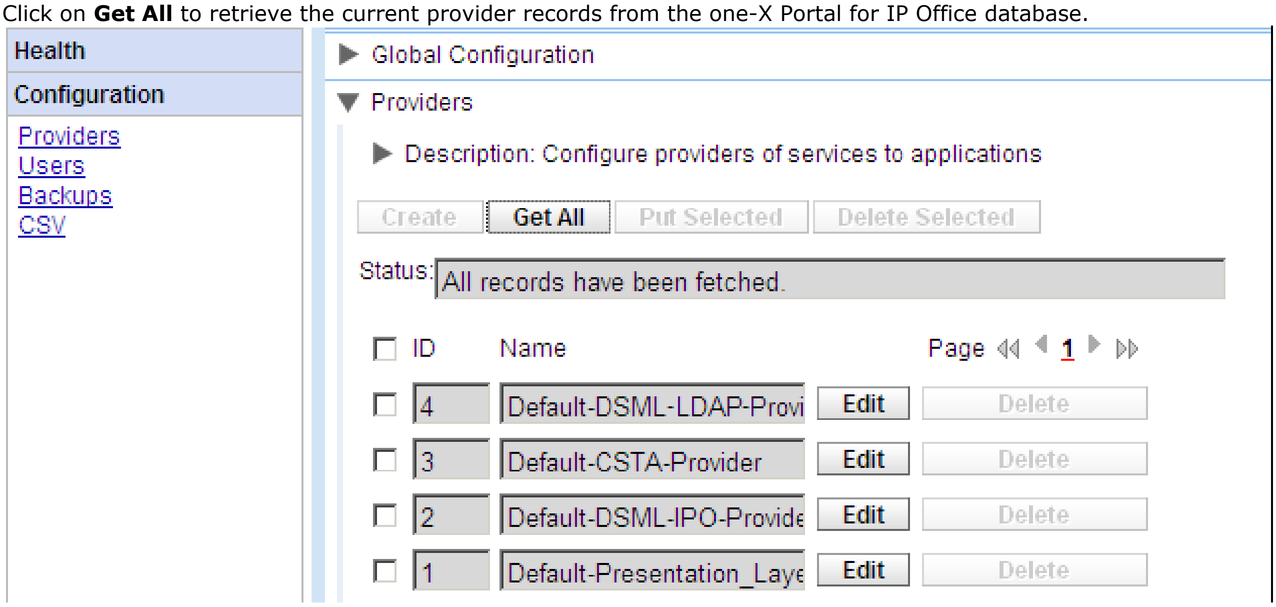
20. Select **Configuration** and then **Users**. Click **Get All**. Check that the new IP Office system's users are listed.

3.3 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.

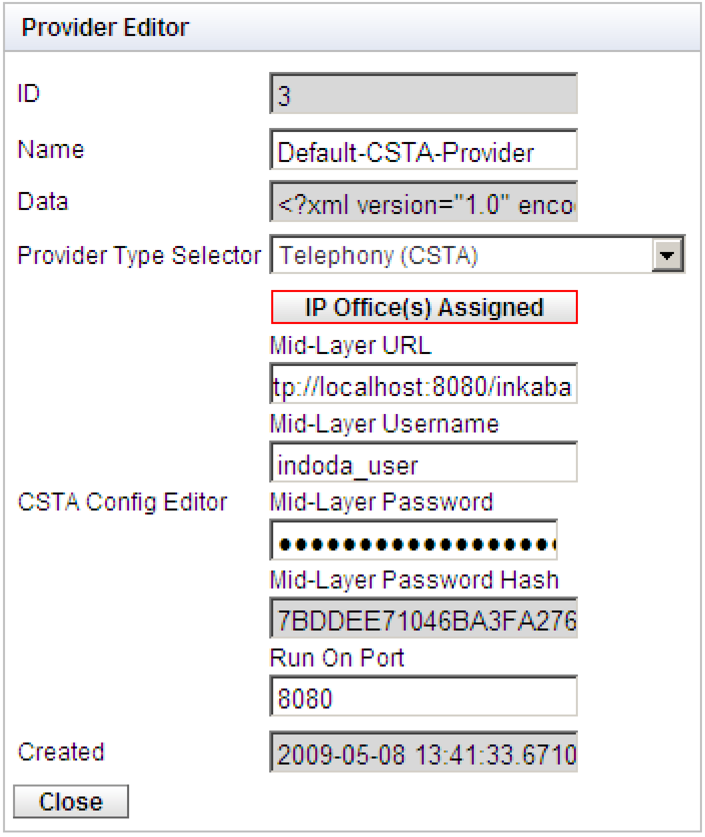
1. Log in 61 to the administrator menus.
2. If it is the IP Office IP address that has changed, check that the IP Office can be seen from the one-X Portal for IP Office server.
   a. Select **Diagnostics** and then **IP Office Connections**.
   b. Enter the **IP Address** of the target IP Office and 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.



Status: All records have been fetched.

	ID	Name		
□	4	Default-DSML-LDAP-Provi	Edit	Delete
□	3	Default-CSTA-Provider	Edit	Delete
□	2	Default-DSML-IPO-Provide	Edit	Delete
□	1	Default-Presentation_Laye	Edit	Delete

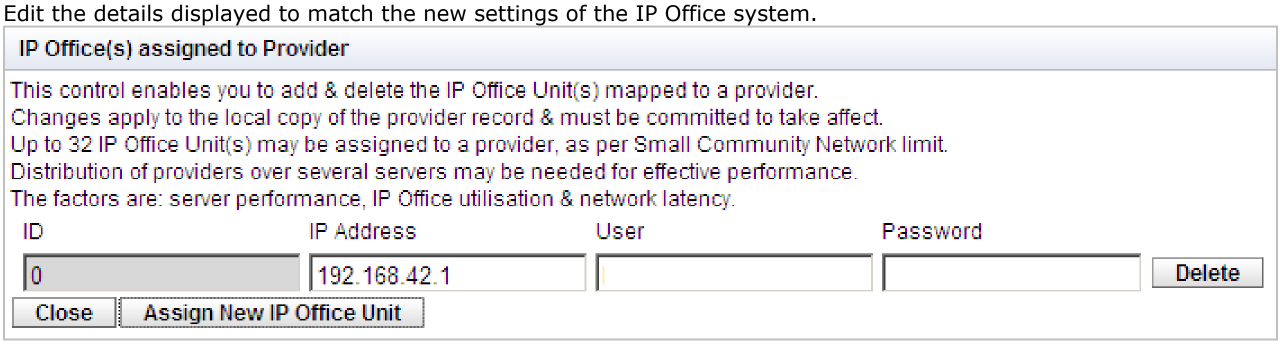
5. Click on the Edit button next to the CSTA provider to which the IP Office was assigned.



Provider Editor

ID	3
Name	Default-CSTA-Provider
Data	<?xml version="1.0" enco
Provider Type Selector	Telephony (CSTA)
	IP Office(s) Assigned
CSTA Config Editor	Mid-Layer URL tp://localhost:8080/inkaba Mid-Layer Username indoda_user Mid-Layer Password •••••••••••••••••• Mid-Layer Password Hash 7BDDEE71046BA3FA276 Run On Port 8080
Created	2009-05-08 13:41:33.6710

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



IP Office(s) assigned to Provider

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

ID	IP Address	User	Password	
0	192.168.42.1			Delete

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.

3.4 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 77 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.

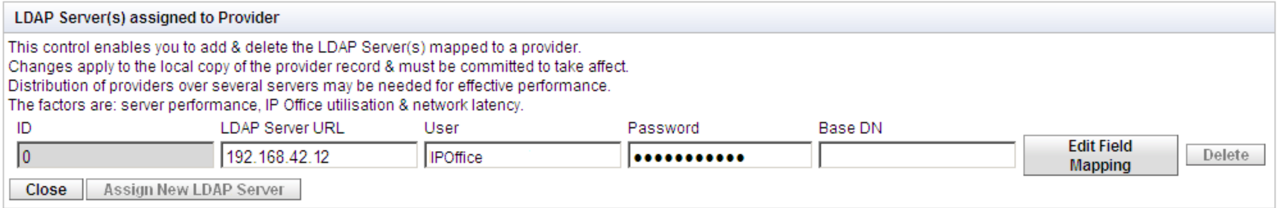
1. Login to the administrator menus.

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.



LDAP Server(s) assigned to Provider

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

ID	LDAP Server URL	User	Password	Base DN		
0	192.168.42.12	IPOffice	●●●●●●●●●●●		Edit Field Mapping	Delete

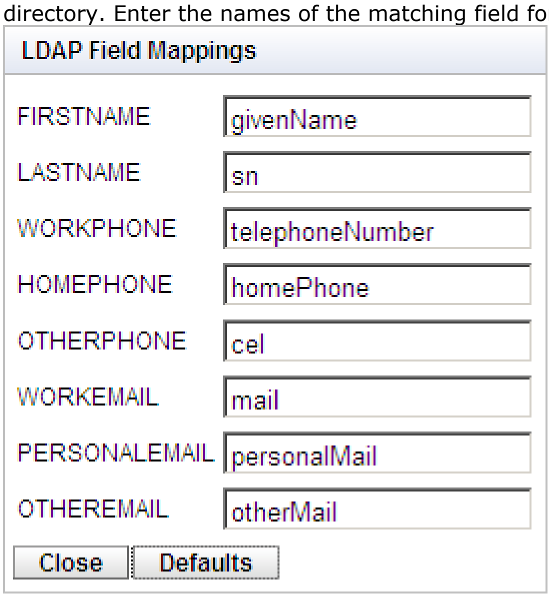
6. Change the details to match the LDAP server source that you want to use.

   - **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.



LDAP Field Mappings

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

8. Click **Close**.

9. Select the check box next to the new entry and click on **Put Selected**.

10. Restart the Avaya one-X Portal service 35.

3.5 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.

3.6 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.

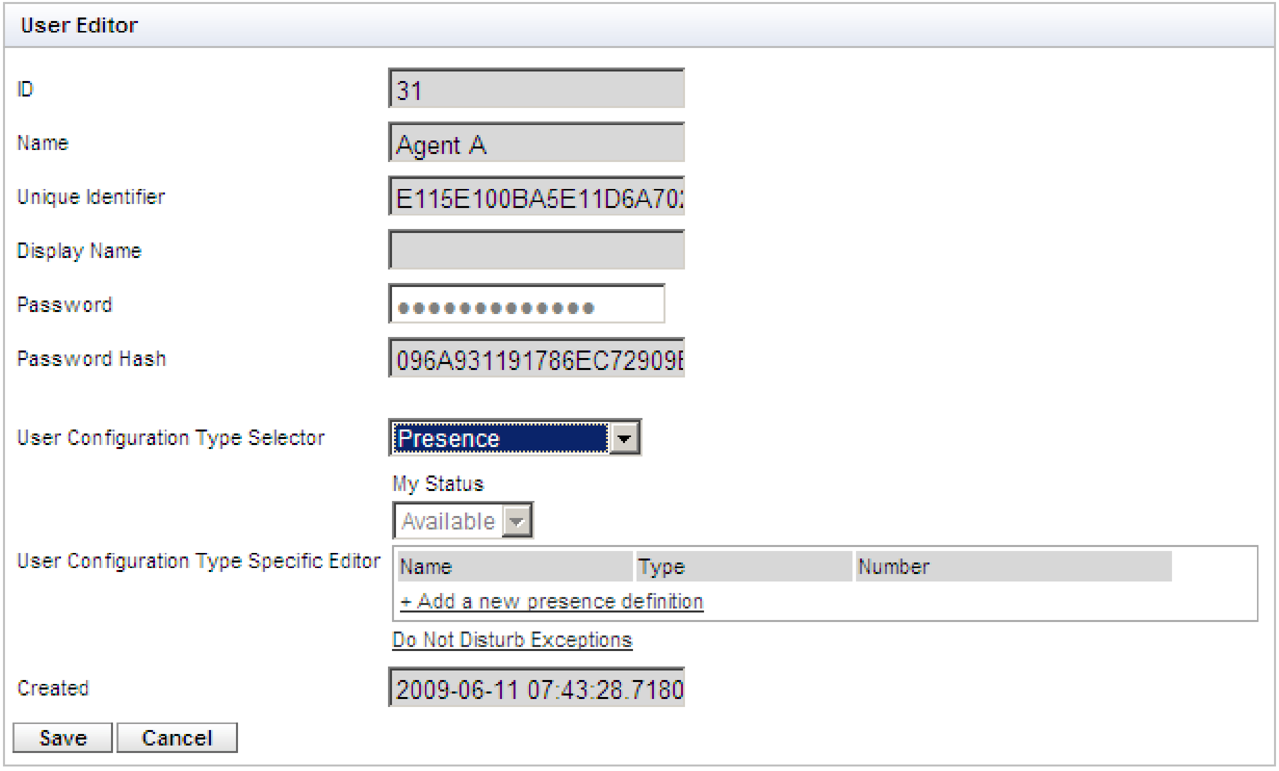
Setting	one-X Portal for IP Office	IP Office	Source/Storage
Personal Directory	✓	✓	A user's personal directory is stored in the configuration of both one-X Portal for IP Office and their IP Office. Changes in either are synchronized where possible. • Personal directory records stored by one-X Portal 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. • Users with a 1608, 1616, 9400, 9500 or 9600 phones can edit or delete contacts through the phone's menus (primary phone number only). Users with 1608, 1616 or 9600 Series phones 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 is may alter various user settings on the IP Office. If the IP Office configuration settings are altered by another method, the user's profile is changed to 'Detected'.
DND Exceptions	−	✓	A user's Do Not Disturb exception numbers are stored in the configuration of their IP Office.
Keyboard Shortcuts	✓	−	A user's keyboard shortcuts are stored by one-X Portal for IP Office.
Sound Configuration	✓	−	A user's one-X Portal for IP Office sound preference is stored by one-X Portal for IP Office.
Park Slots	✓	−	The park slot numbers used for a user's one-X Portal for IP Office park buttons are stored by one-X Portal for IP Office.

Editing User Settings

1. Select **Configuration** and then **Users**.

2. Click on **Get All**. and browse through the users.

3. Click on the **Edit** button next to the user you want to edit. The user configuration settings are displayed.



User Editor

ID	31
Name	Agent A
Unique Identifier	E115E100BA5E11D6A70
Display Name	
Password	●●●●●●●●●●●●●
Password Hash	096A931191786EC72909
User Configuration Type Selector	Presence
User Configuration Type Specific Editor	My Status: Available
Created	2009-06-11 07:43:28.7180

Name	Type	Number

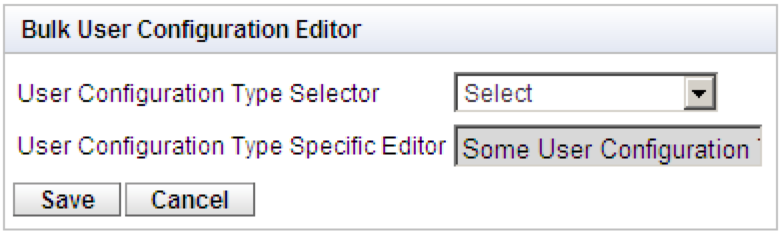
4. Use the **User Configuration Type Selector** to select the user settings you want to view/edit. If required edit the settings.

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**.

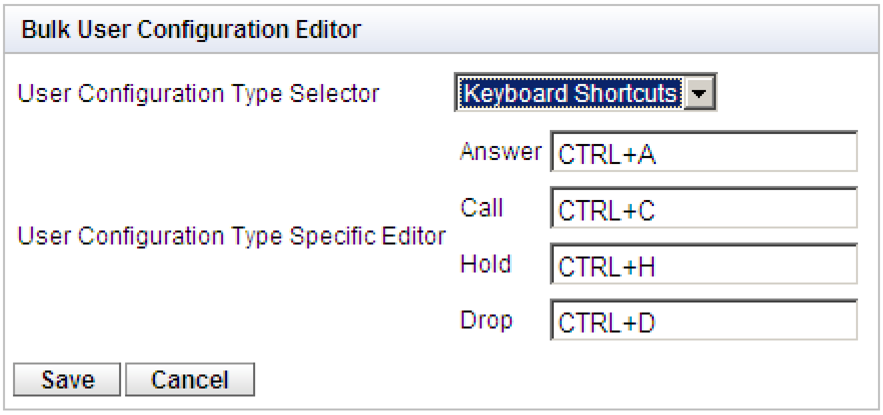


Bulk User Configuration Editor

User Configuration Type Selector: Select

User Configuration Type Specific Editor: Some User Configuration

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



Bulk User Configuration Editor

User Configuration Type Selector: Keyboard Shortcuts

User Configuration Type Specific Editor

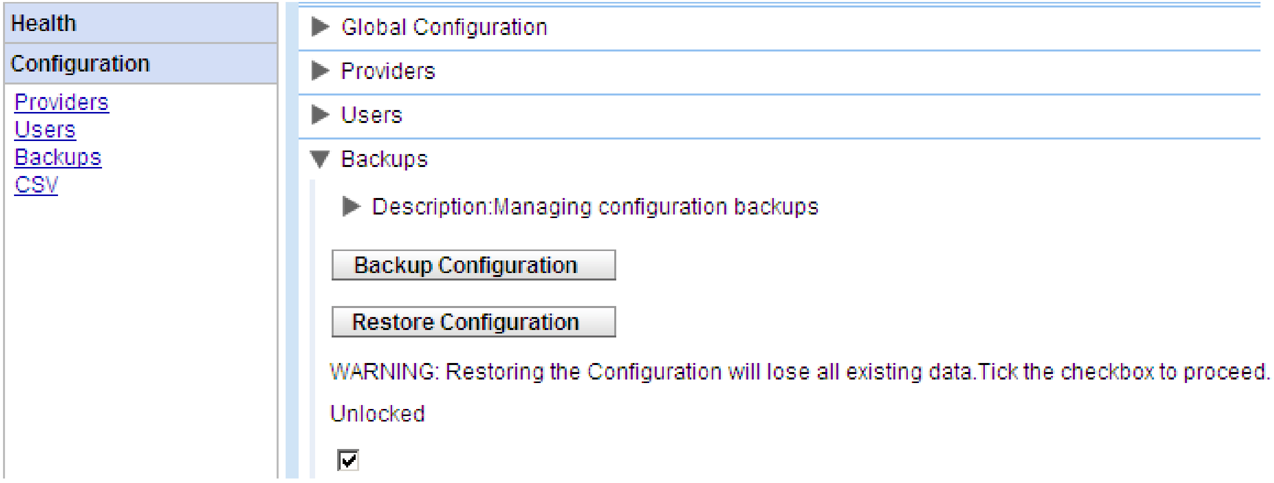
Answer	CTRL+A
Call	CTRL+C
Hold	CTRL+H
Drop	CTRL+D

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.

3.7 Backing Up the Database

You can backup the one-X Portal for IP Office database of settings. The resulting file can be restored 46 if necessary.

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

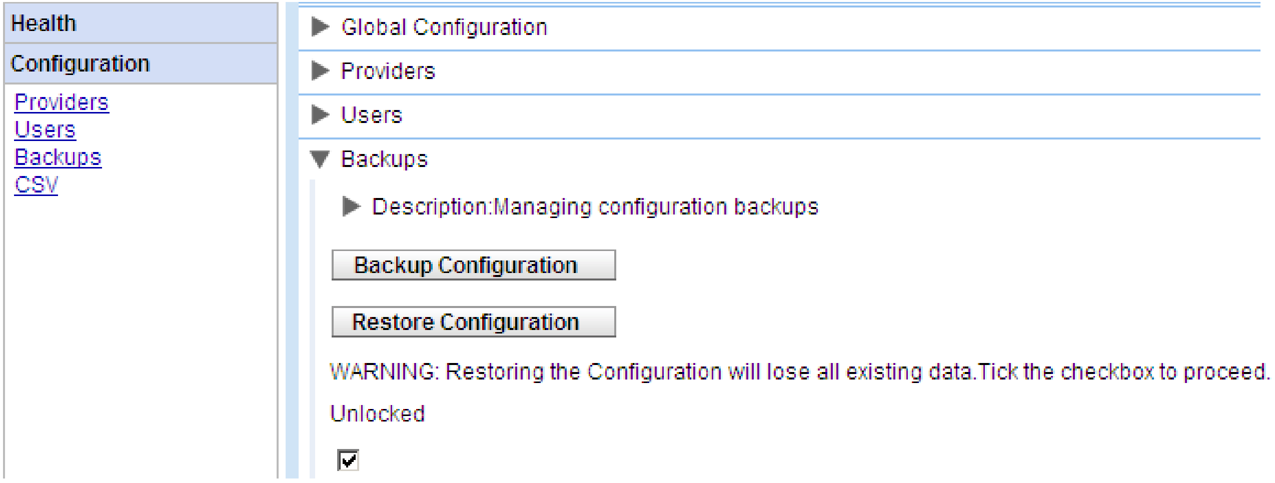

Health
Configuration
Providers
Users
Backups
CSV
Global Configuration
Providers
Users
Backups
Description:Managing configuration backups
Backup Configuration
Restore Configuration
WARNING: Restoring the Configuration will lose all existing data.Tick the checkbox to proceed.
Unlocked
☑

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).

3.8 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**.



WARNING: Restoring the Configuration will lose all existing data.Tick the checkbox to proceed.

Unlocked

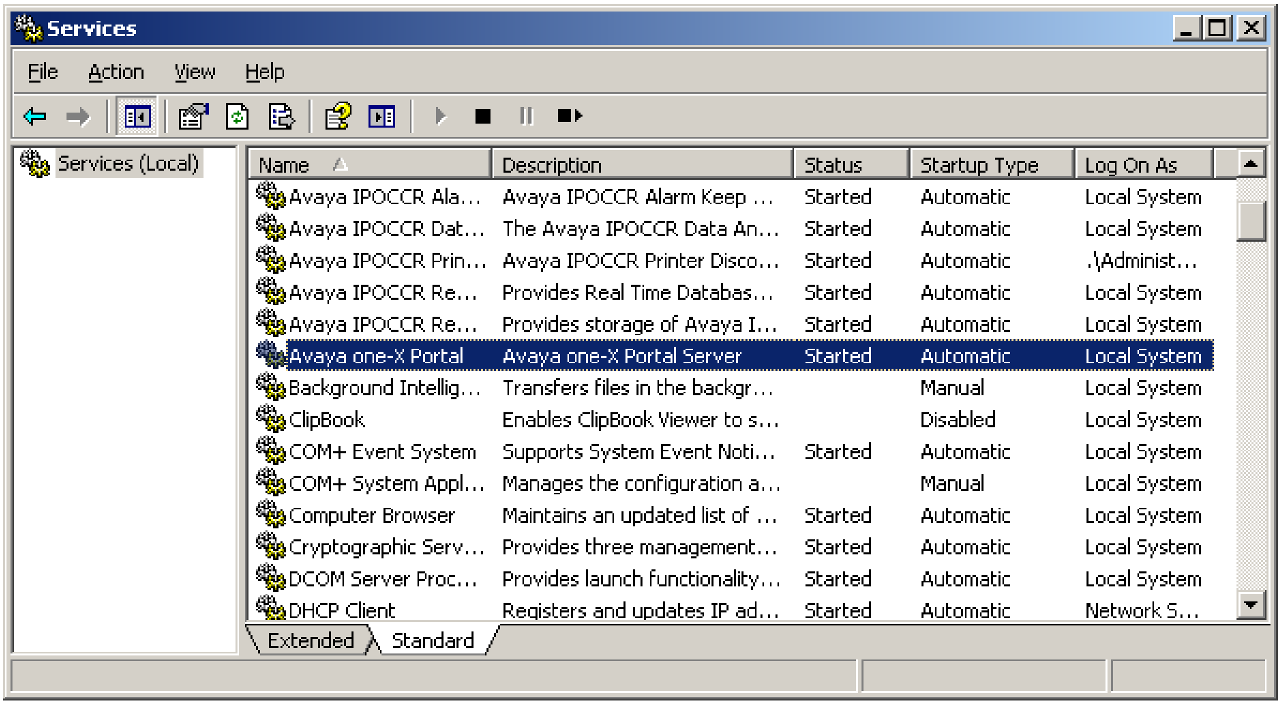
☑

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.



Name	Description	Status	Startup Type	Log On As
Avaya IPOCCR Ala...	Avaya IPOCCR Alarm Keep ...	Started	Automatic	Local System
Avaya IPOCCR Dat...	The Avaya IPOCCR Data An...	Started	Automatic	Local System
Avaya IPOCCR Prin...	Avaya IPOCCR Printer Disco...	Started	Automatic	.\Administ...
Avaya IPOCCR Re...	Provides Real Time Databas...	Started	Automatic	Local System
Avaya IPOCCR Re...	Provides storage of Avaya I...	Started	Automatic	Local System
Avaya one-X Portal	Avaya one-X Portal Server	Started	Automatic	Local System
Background Intellig...	Transfers files in the backgr...		Manual	Local System
ClipBook	Enables ClipBook Viewer to s...		Disabled	Local System
COM+ Event System	Supports System Event Noti...	Started	Automatic	Local System
COM+ System Appl...	Manages the configuration a...		Manual	Local System
Computer Browser	Maintains an updated list of ...	Started	Automatic	Local System
Cryptographic Serv...	Provides three management...	Started	Automatic	Local System
DCOM Server Proc...	Provides launch functionality...	Started	Automatic	Local System
DHCP Client	Registers and updates IP ad...	Started	Automatic	Network S...

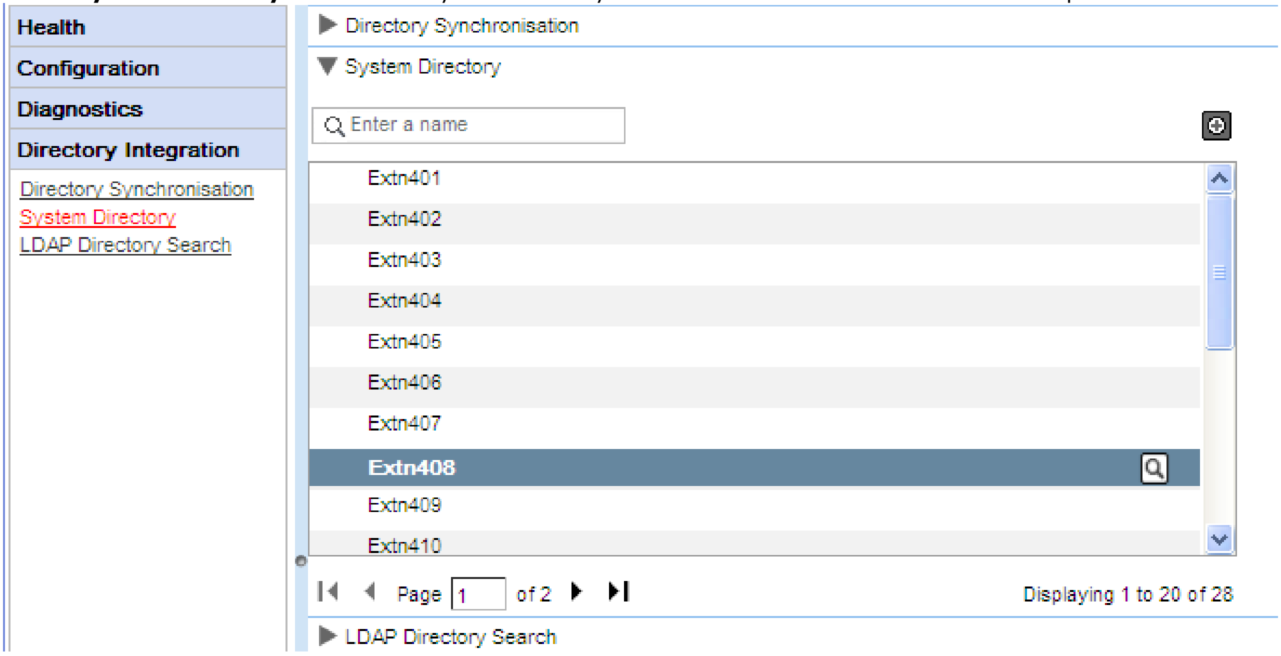
3.9 Checking and Updating the System Directory

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.

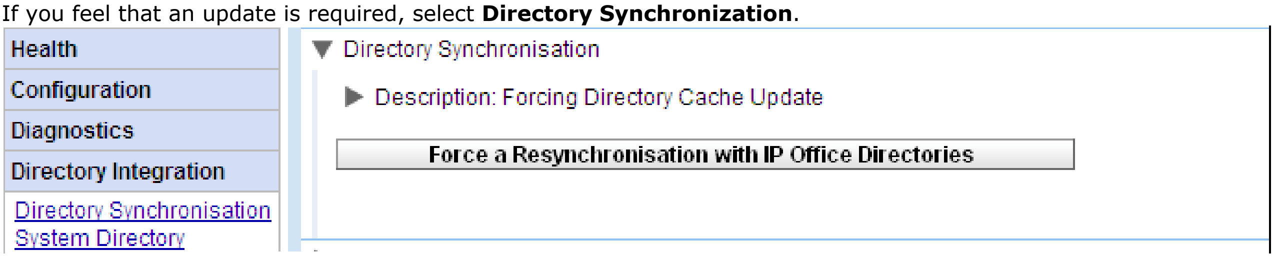
By default, the one-X Portal for IP Office application updates the system directory records every 300 seconds approximately. Through the one-X Portal for IP Office administrator menus you can view the system directory and, if necessary, force an update.

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**.


Health
Configuration
Diagnostics
Directory Integration
Directory Synchronisation
System Directory
Directory Synchronisation
Description: Forcing Directory Cache Update
Force a Resynchronisation with IP Office Directories

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

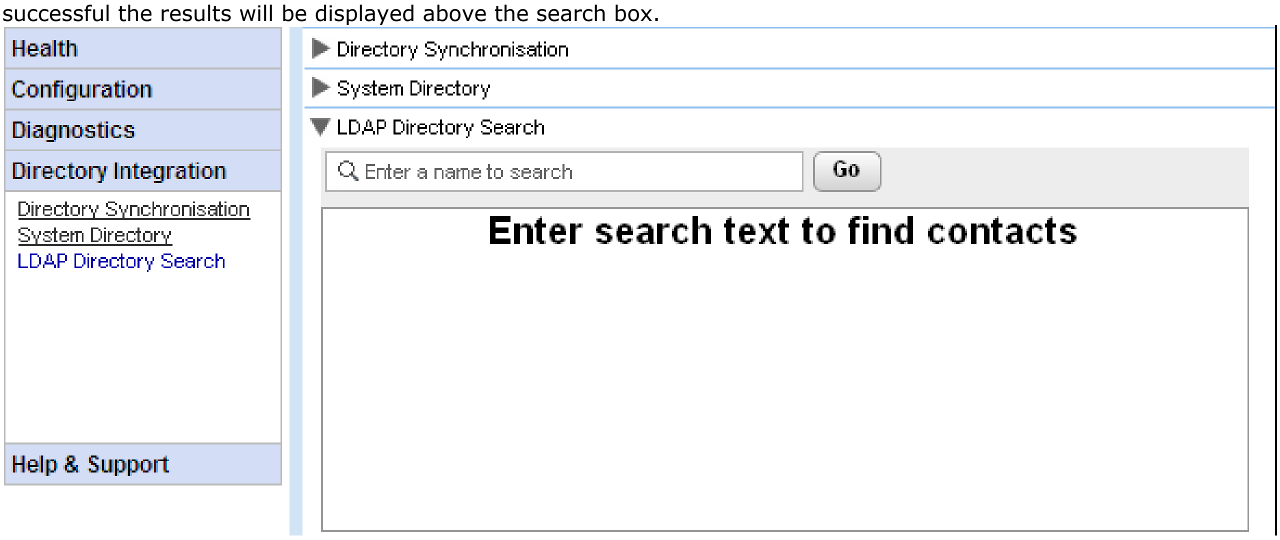
3.10 Checking the External LDAP Directory

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.

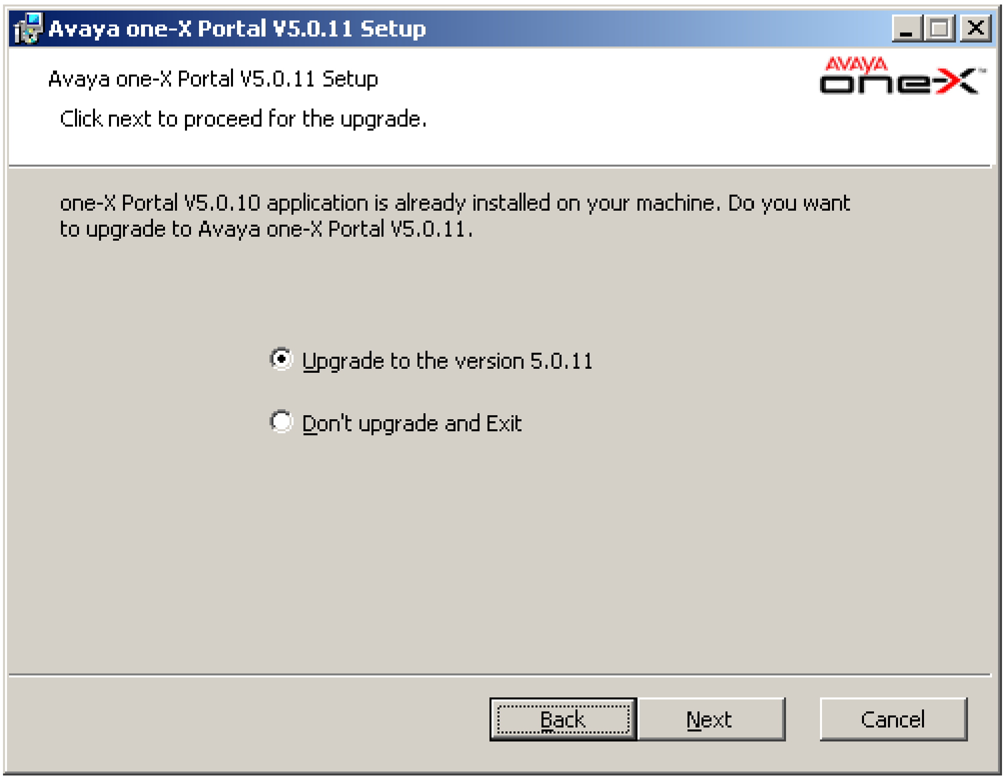


3.11 Upgrading one-X Portal for IP Office

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 may not be 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.



Avaya one-X Portal V5.0.11 Setup

Avaya one-X Portal V5.0.11 Setup

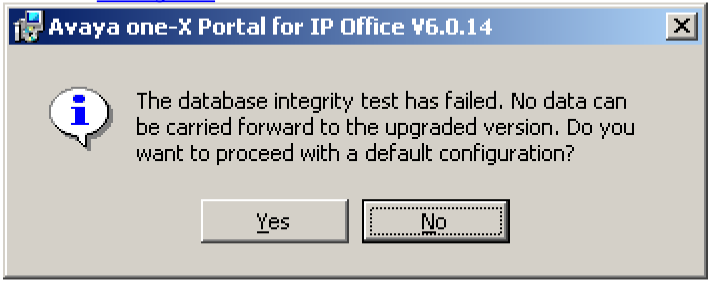
Click next to proceed for the upgrade.

one-X Portal V5.0.10 application is already installed on your machine. Do you want to upgrade to Avaya one-X Portal V5.0.11.

● Upgrade to the version 5.0.11

○ Don't upgrade and Exit

- 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 50 back to the version of one-X Portal for IP Office that is compatible with the database.



Avaya one-X Portal for IP Office V6.0.14

The database integrity test has failed. No data can be carried forward to the upgraded version. Do you want to proceed with a default configuration?

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 45 for details of creating a full backup.

3.12 Downgrading one-X Portal for IP Office

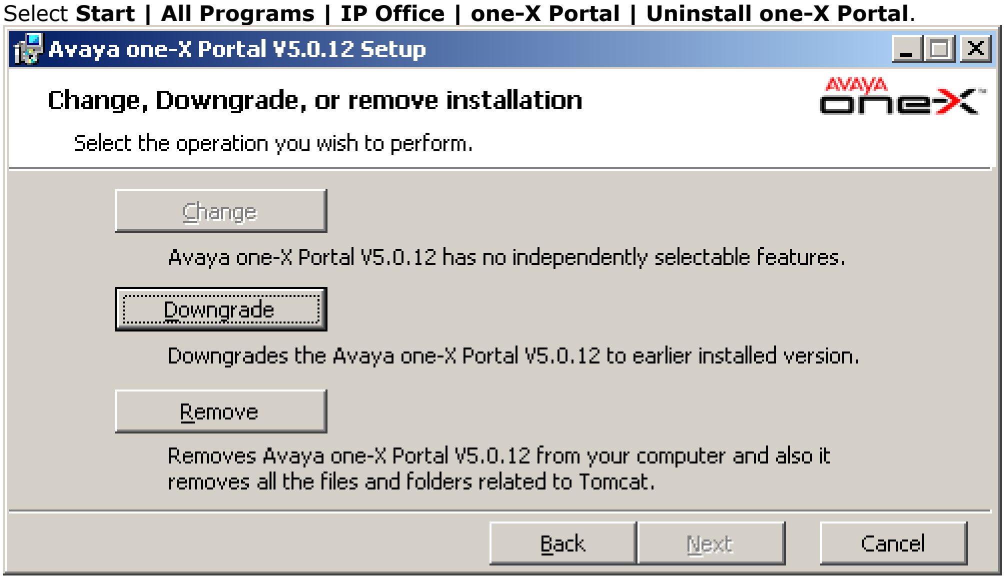
If the one-X Portal for IP Office application software has been upgraded using the upgrade process 49, it is also possible to downgrade back to the original installed version.

- 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 may not be 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**.



Avaya one-X Portal V5.0.12 Setup

Change, Downgrade, or remove installation

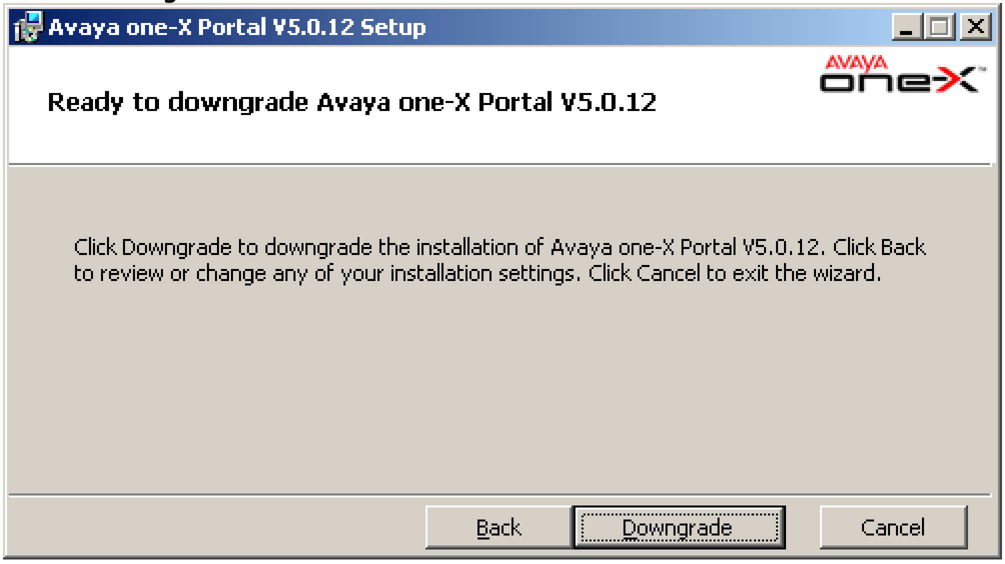
Select the operation you wish to perform.

Avaya one-X Portal V5.0.12 has no independently selectable features.

Downgrades the Avaya one-X Portal V5.0.12 to earlier installed version.

Removes Avaya one-X Portal V5.0.12 from your computer and also it removes all the files and folders related to Tomcat.

2. Click on **Downgrade**.



Avaya one-X Portal V5.0.12 Setup

Ready to downgrade Avaya one-X Portal V5.0.12

Click Downgrade to downgrade the installation of Avaya one-X Portal V5.0.12. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

3. When the downgrade has been completed, the Avaya one-X Portal needs to be restarted manually 35.

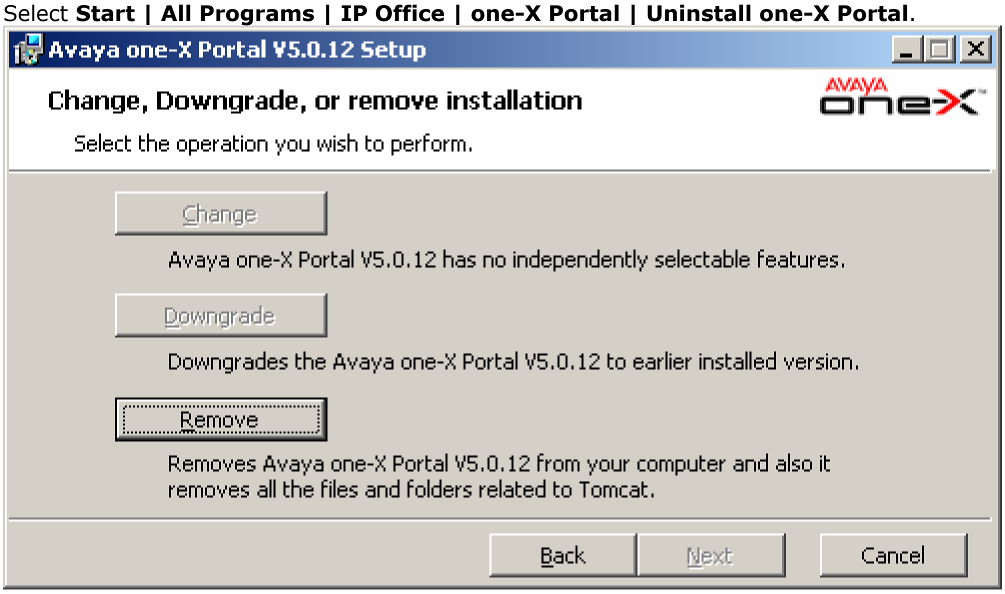
3.13 Removing one-X Portal for IP Office

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**.



Avaya one-X Portal V5.0.12 Setup

Change, Downgrade, or remove installation

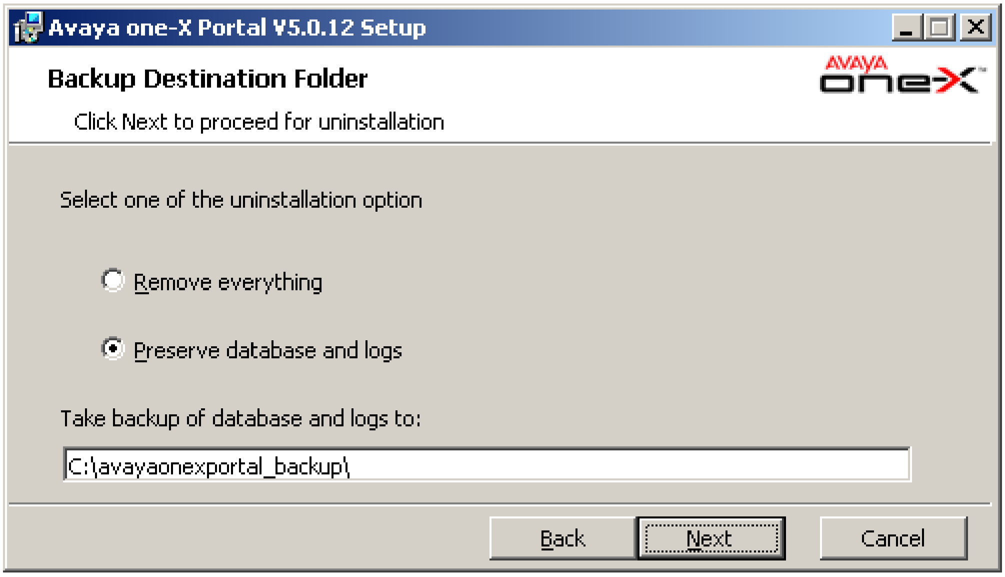
Select the operation you wish to perform.

Avaya one-X Portal V5.0.12 has no independently selectable features.

Downgrades the Avaya one-X Portal V5.0.12 to earlier installed version.

Removes Avaya one-X Portal V5.0.12 from your computer and also it removes all the files and folders related to Tomcat.

2. Select **Remove**.



Avaya one-X Portal V5.0.12 Setup

Backup Destination Folder

Click Next to proceed for uninstallation

Select one of the uninstallation option

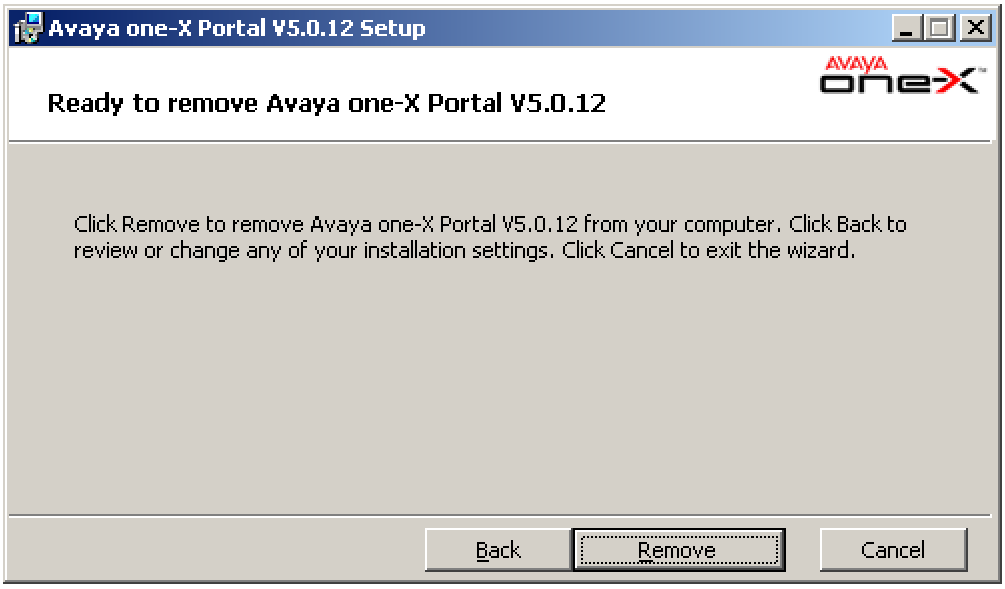
○ Remove everything

● Preserve database and logs

Take backup of database and logs to:

C:\avayaonexportal_backup\

3. Click **Next**.



Avaya one-X Portal V5.0.12 Setup
Ready to remove Avaya one-X Portal V5.0.12
AVAYA one-X

Click Remove to remove Avaya one-X Portal V5.0.12 from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

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**.

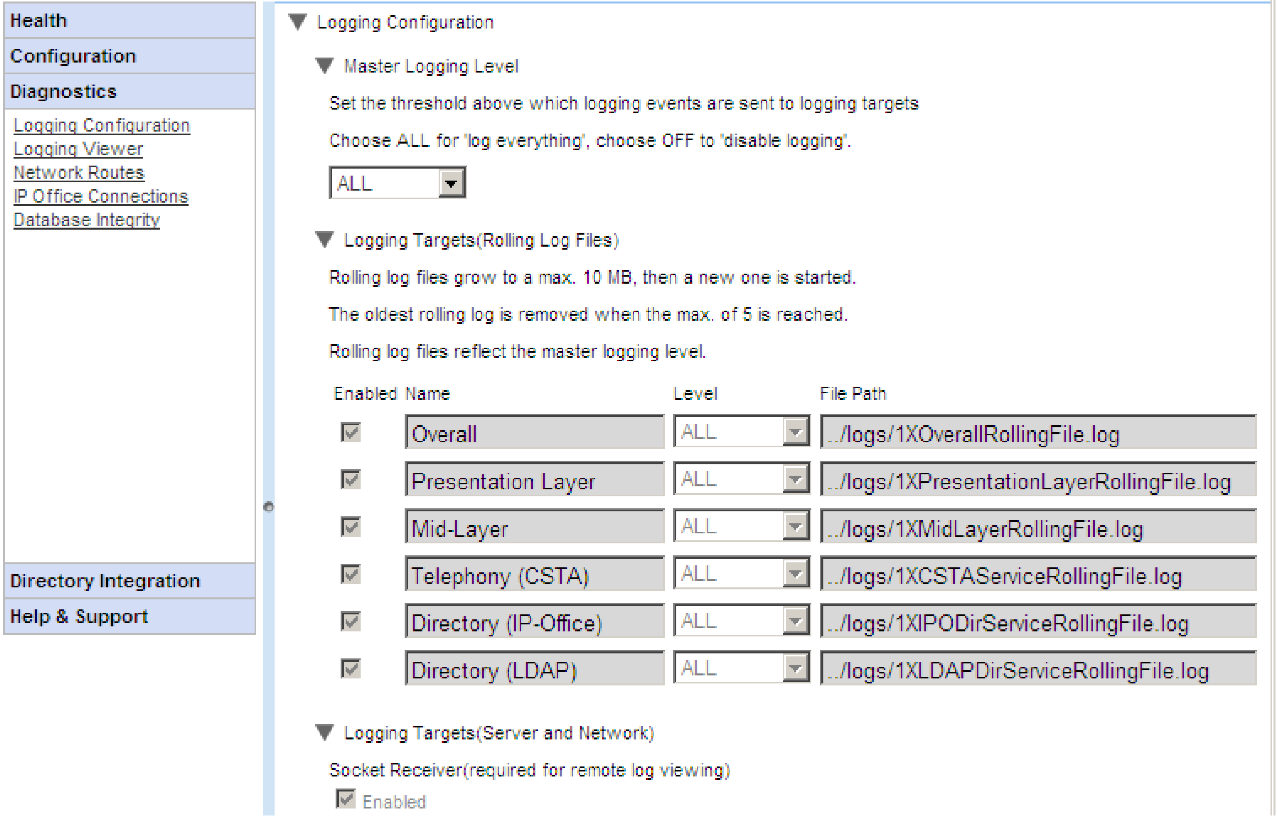
   - If the one-X Portal for IP Office has been upgraded at some stage, there will be a program entry for both the original one-X Portal for IP Office installation and the most recent upgrade. Select the upgrade installation and then click Remove. This will remove both the upgrade and the original installation.

3.14 Remote Logging

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

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

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



▼ Logging Configuration

▼ Master Logging Level

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

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

ALL

▼ Logging Targets(Rolling Log Files)

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

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

Rolling log files reflect the master logging level.

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

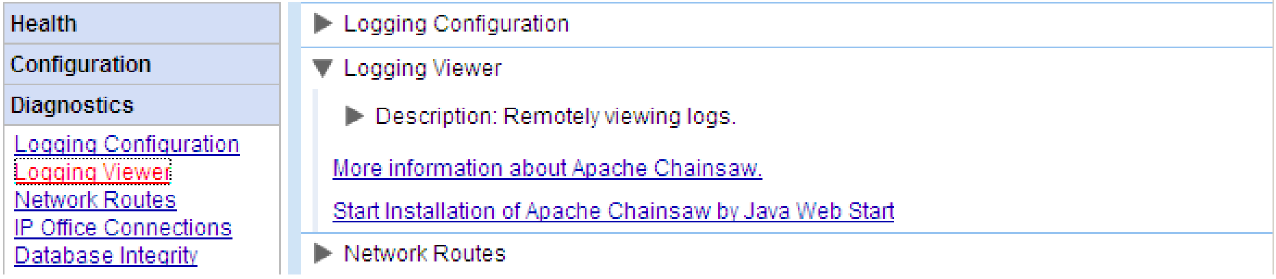
▼ Logging Targets(Server and Network)

Socket Receiver(required for remote log viewing)

☑ Enabled

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

3. Select **Logging Viewer**.



▶ Logging Configuration

▼ Logging Viewer

▶ Description: Remotely viewing logs.

More information about Apache Chainsaw.

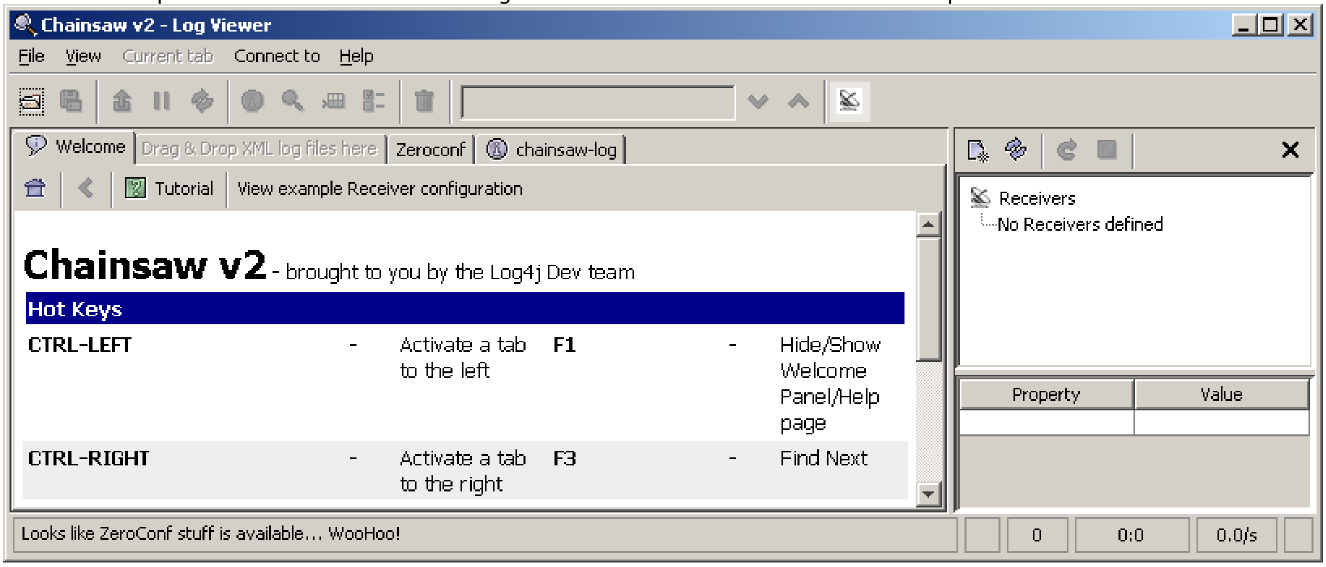
Start Installation of Apache Chainsaw by Java Web Start

▶ Network Routes

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.

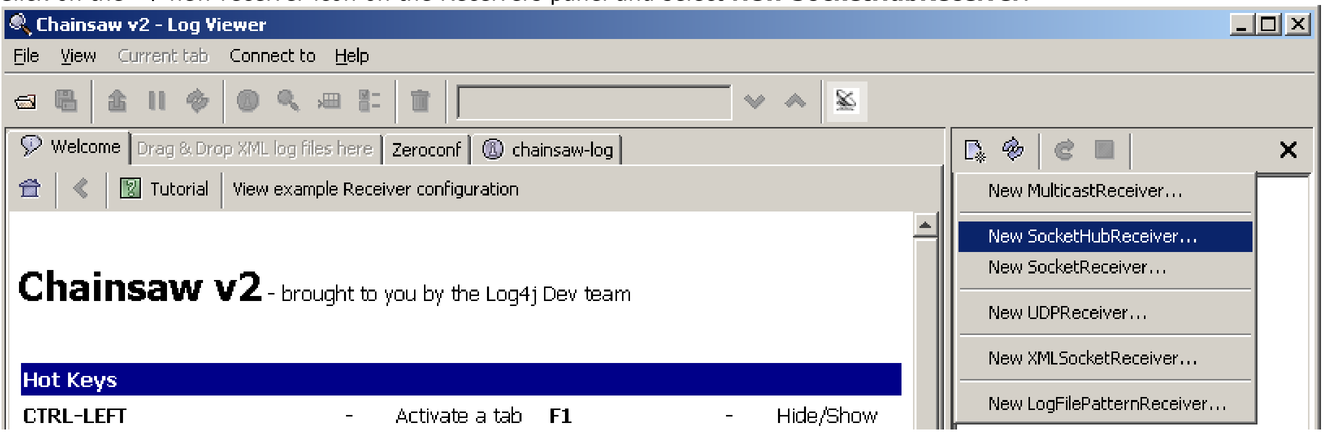

Chainsaw v2 - Log Viewer
File View Current tab Connect to Help
Welcome
Drag & Drop XML log files here
Zeroconf
chainsaw-log
Tutorial
View example Receiver configuration
Receivers
No Receivers defined
Property
Value

Chainsaw v2 - brought to you by the Log4j Dev team

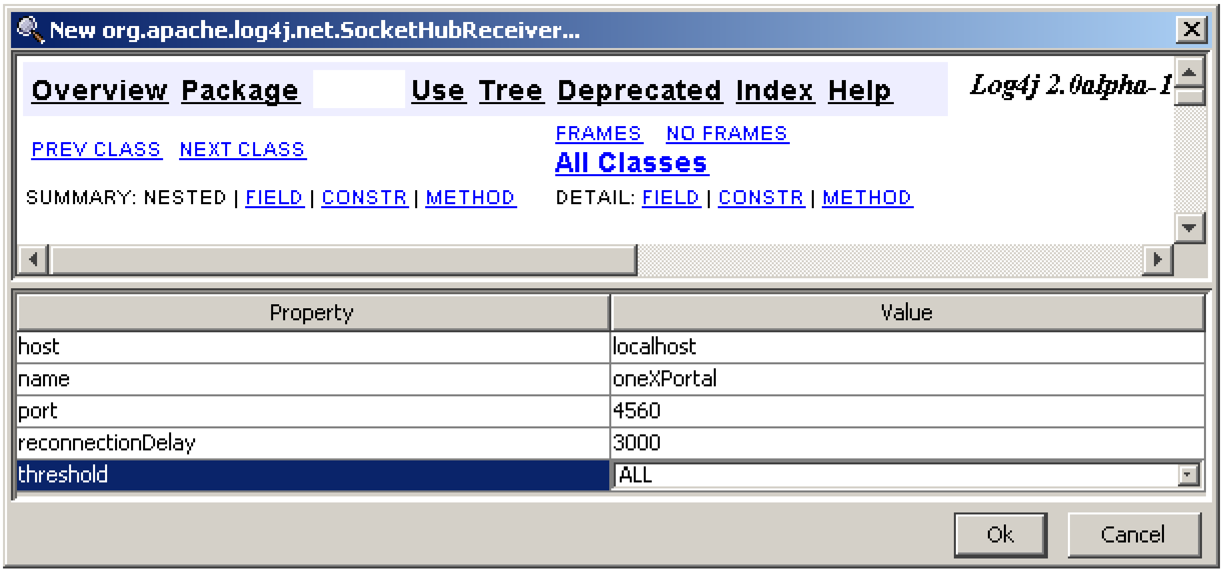
Hot Keys					
CTRL-LEFT	-	Activate a tab to the left	F1	-	Hide/Show Welcome Panel/Help page
CTRL-RIGHT	-	Activate a tab to the right	F3	-	Find Next

Looks like ZeroConf stuff is available... WooHoo!

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


Chainsaw v2 - Log Viewer
File View Current tab Connect to Help
Welcome
Drag & Drop XML log files here
Zeroconf
chainsaw-log
Tutorial
View example Receiver configuration
Chainsaw v2 - brought to you by the Log4j Dev team
Hot Keys
CTRL-LEFT - Activate a tab F1 - Hide/Show
New MulticastReceiver...
New SocketHubReceiver...
New SocketReceiver...
New UDPReceiver...
New XMLSocketReceiver...
New LogFilePatternReceiver...

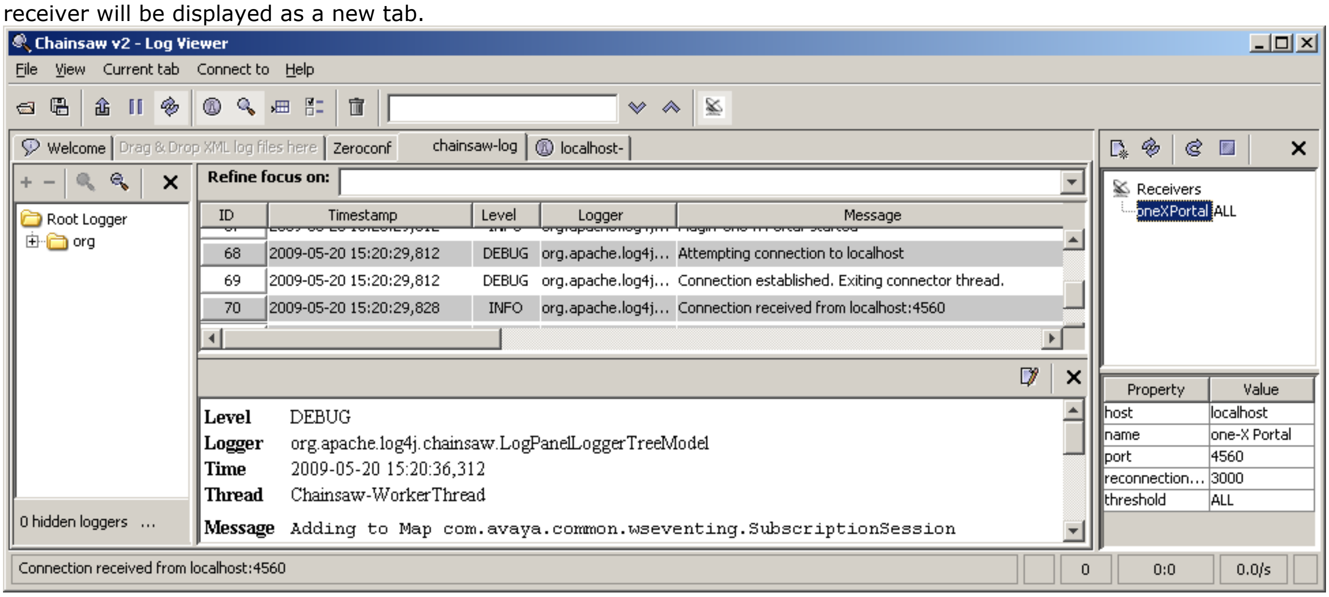
8. Enter the details for the one-X Portal for IP Office server.


New org.apache.log4j.net.SocketHubReceiver...
Overview Package Use Tree Deprecated Index Help
Log4j 2.0alpha-1
PREV CLASS NEXT CLASS
FRAMES NO FRAMES
All Classes
SUMMARY: NESTED | FIELD | CONSTR | METHOD
DETAIL: FIELD | CONSTR | METHOD
Ok
Cancel

Property	Value
host	localhost
name	oneXPortal
port	4560
reconnectionDelay	3000
threshold	ALL

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.



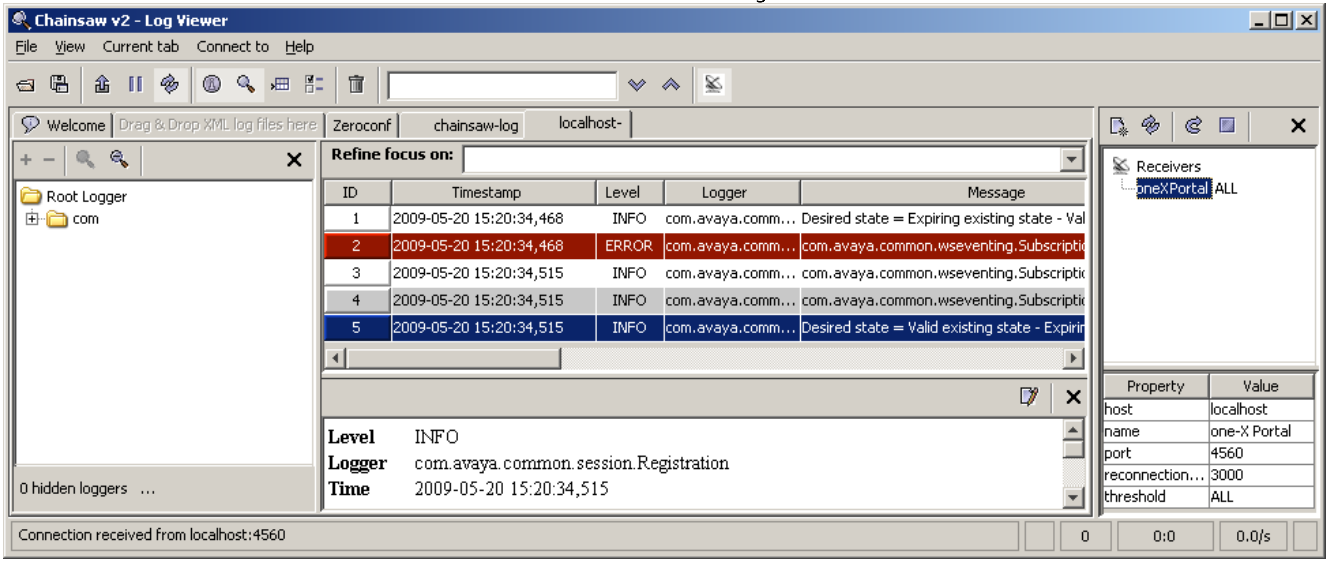
ID	Timestamp	Level	Logger	Message
68	2009-05-20 15:20:29,812	DEBUG	org.apache.log4j...	Attempting connection to localhost
69	2009-05-20 15:20:29,812	DEBUG	org.apache.log4j...	Connection established. Exiting connector thread.
70	2009-05-20 15:20:29,828	INFO	org.apache.log4j...	Connection received from localhost:4560

Level DEBUG
Logger org.apache.log4j.chainsaw.LogPanelLoggerTreeModel
Time 2009-05-20 15:20:36,312
Thread Chainsaw-WorkerThread
Message `Adding to Map com.avaya.common.wseventing.SubscriptionSession`

Property	Value
host	localhost
name	one-X Portal
port	4560
reconnection...	3000
threshold	ALL

Connection received from localhost:4560 | 0 | 0:0 | 0.0/s

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



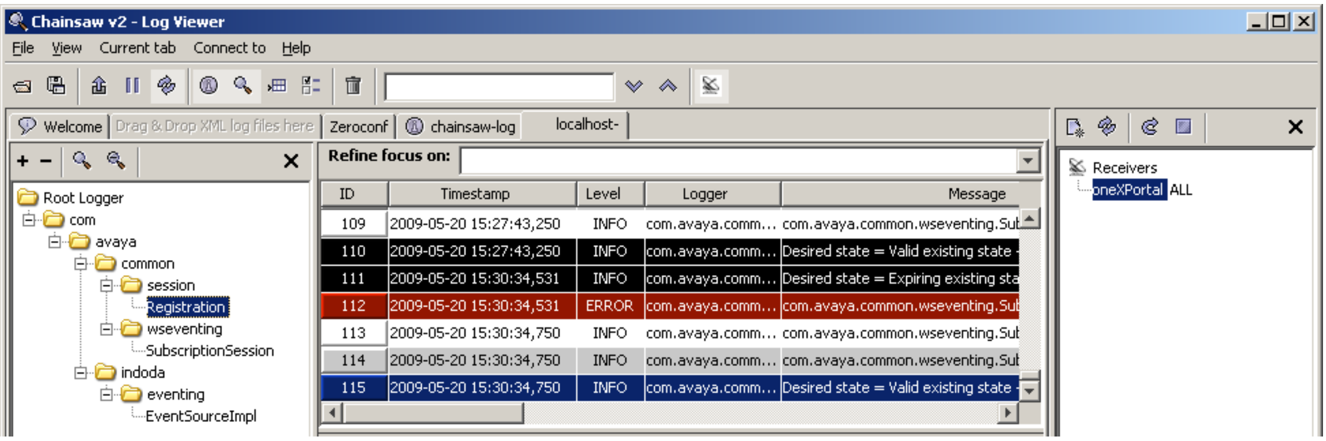
ID	Timestamp	Level	Logger	Message
1	2009-05-20 15:20:34,468	INFO	com.avaya.comm...	Desired state = Expiring existing state - Val
2	2009-05-20 15:20:34,468	ERROR	com.avaya.comm...	com.avaya.common.wseventing.Subscriptio
3	2009-05-20 15:20:34,515	INFO	com.avaya.comm...	com.avaya.common.wseventing.Subscriptio
4	2009-05-20 15:20:34,515	INFO	com.avaya.comm...	com.avaya.common.wseventing.Subscriptio
5	2009-05-20 15:20:34,515	INFO	com.avaya.comm...	Desired state = Valid existing state - Expirin

Level INFO
Logger com.avaya.common.session.Registration
Time 2009-05-20 15:20:34,515

Property	Value
host	localhost
name	one-X Portal
port	4560
reconnection...	3000
threshold	ALL

Connection received from localhost:4560 | 0 | 0:0 | 0.0/s

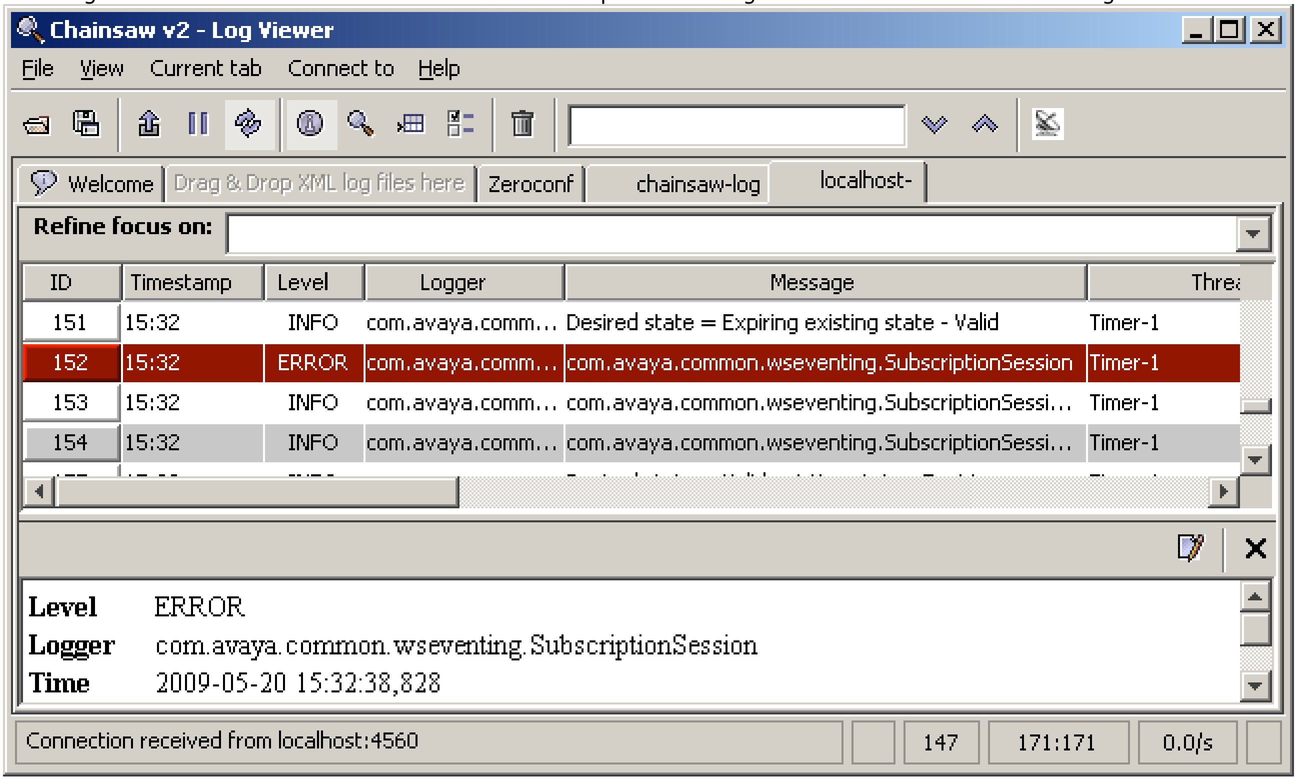
11. The navigation tree on the left can be used to focus the log view onto a particular component of one-X Portal for IP Office server.



Root Logger
- com
  - avaya
    - common
      - session
        - Registration
      - wseventing
        - SubscriptionSession
    - indoda
      - eventing
        - EventSourceImpl

ID	Timestamp	Level	Logger	Message
109	2009-05-20 15:27:43,250	INFO	com.avaya.comm...	com.avaya.common.wseventing.Sul
110	2009-05-20 15:27:43,250	INFO	com.avaya.comm...	Desired state = Valid existing state -
111	2009-05-20 15:30:34,531	INFO	com.avaya.comm...	Desired state = Expiring existing sta
112	2009-05-20 15:30:34,531	ERROR	com.avaya.comm...	com.avaya.common.wseventing.Sul
113	2009-05-20 15:30:34,750	INFO	com.avaya.comm...	com.avaya.common.wseventing.Sul
114	2009-05-20 15:30:34,750	INFO	com.avaya.comm...	com.avaya.common.wseventing.Sul
115	2009-05-20 15:30:34,750	INFO	com.avaya.comm...	Desired state = Valid existing state -

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



ID	Timestamp	Level	Logger	Message	Threa
151	15:32	INFO	com.avaya.comm...	Desired state = Expiring existing state - Valid	Timer-1
152	15:32	ERROR	com.avaya.comm...	com.avaya.common.wseventing.SubscriptionSession	Timer-1
153	15:32	INFO	com.avaya.comm...	com.avaya.common.wseventing.SubscriptionSessi...	Timer-1
154	15:32	INFO	com.avaya.comm...	com.avaya.common.wseventing.SubscriptionSessi...	Timer-1

Level ERROR
Logger com.avaya.common.wseventing.SubscriptionSession
Time 2009-05-20 15:32:38,828

Connection received from localhost:4560 | 147 | 171:171 | 0.0/s

3.15 Troubleshooting

Version Mismatch Problem

Symptoms	• Database integrity 74 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 51. 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 22. 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 51. 4. Install one-X Portal for IP Office 23.

3.16 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, 9400, 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.

Chapter 4. Administration

4. 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 62	**Component Status** 62	List the last status change of the server components.
	Key Recent Events 62	View the last 20 events on the server.
	Active Sessions 63	Show how many sessions are cached by one-X Portal for IP Office.
	Environment 63	Show a summary of the one-X Portal for IP Office server PC.
Configuration 64	**Providers** 64	View and edit the providers.
	Users 68	View and edit user one-X Portal for IP Office settings.
	Backups 70	Backup the one-X Portal for IP Office configuration database. Also restore a previous backup.
	CSV 70	Export the user directory and system directory.
Diagnostics	**Logging Configuration** 72	Configure the level and method of logging supported.
	Logging Viewer 73	Install and launch Chainsaw for log viewing.
	Network Routes 73	Test the IP connection path to an IP address.
	IP Office Connections 74	Test the IP connection path to an IP Office.
	Database Integrity 74	Test the structure of the database.
Directory Integration 75	**Directory Synchronization** 75	Force a system directory update by the server.
	System Directory 76	View the one-X Portal for IP Office system directory.
	LDAP Directory Search 77	View the external directory for which the one-X Portal for IP Office server has been configured.
Help & Support 78	**Help** 78	Access one-X Portal for IP Office help installed on the server.
	Avaya Support 78	Access the Avaya support web site for Avaya applications.
	About 78	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).

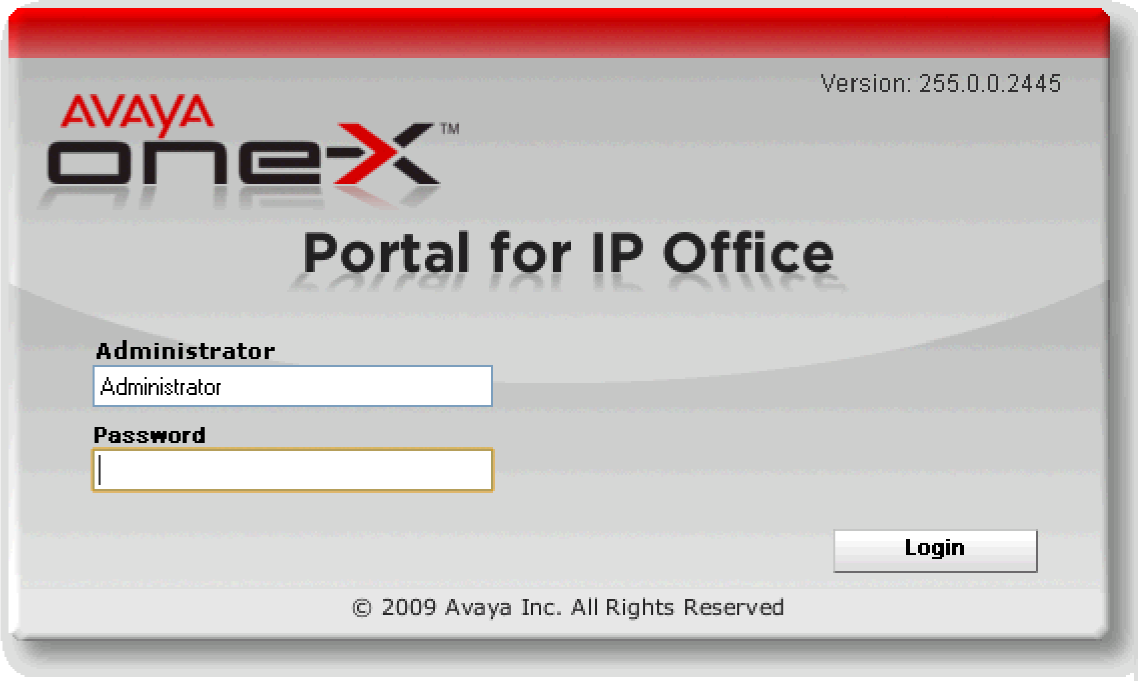
Within each menu, the clicking on the ▶ ▼ icon next to Description can be used to show/hide a short description of the menus function and content.

4.1 Login

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>/inyama/inyama.html?admin=true***. Replacing *<server_name>* with the server PC name and *<server_port>* with the port number selected during one-X Portal for IP Office software installation (the default is 8080).

2. The one-X Portal for IP Office login menu should be displayed.

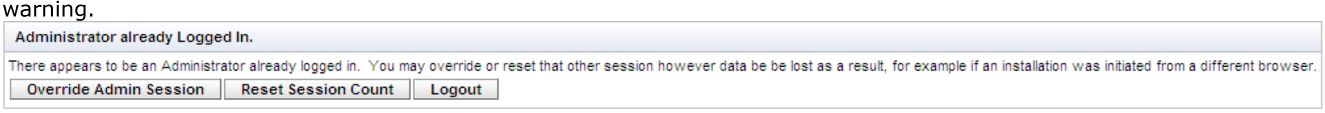


Administrator: Administrator

Password:

3. Enter the one-X Portal for IP Office administrator name and password as configured during installation.

4. If there is already a session connected as an administrator, the one-X Portal for IP Office server will display a warning.



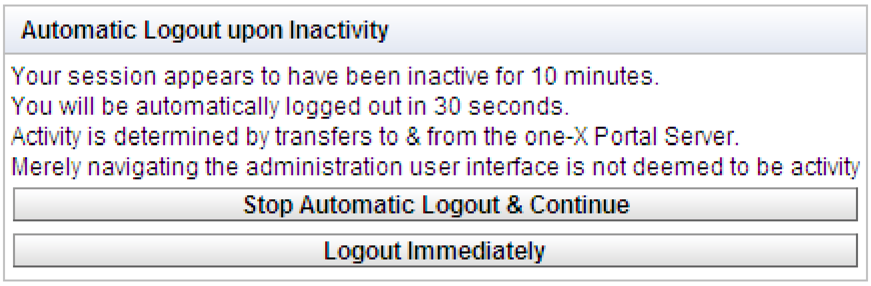
Administrator already Logged In.

There appears to be an Administrator already logged in. You may override or reset that other session however data be be lost as a result, for example if an installation was initiated from a different browser.

4.2 Logout

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

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



Automatic Logout upon Inactivity

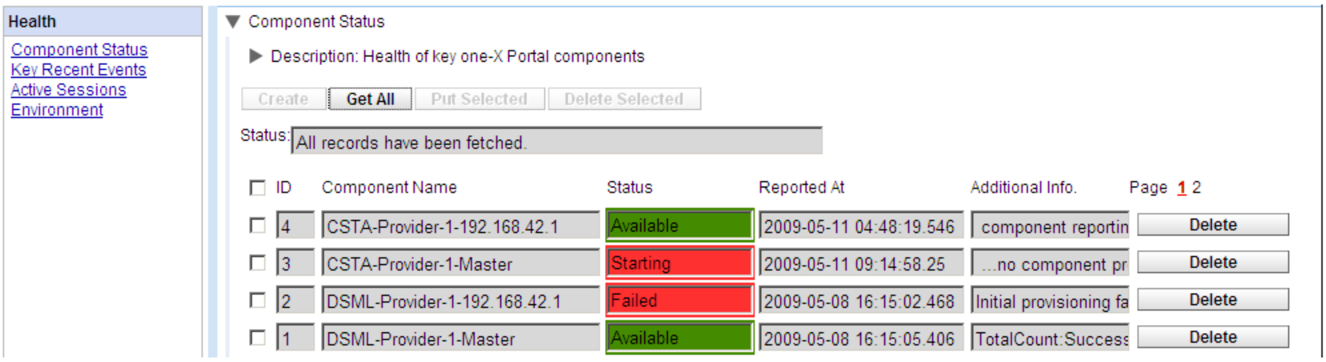
Your session appears to have been inactive for 10 minutes.
You will be automatically logged out in 30 seconds.
Activity is determined by transfers to & from the one-X Portal Server.
Merely navigating the administration user interface is not deemed to be activity

4.3 Health

4.3.1 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.



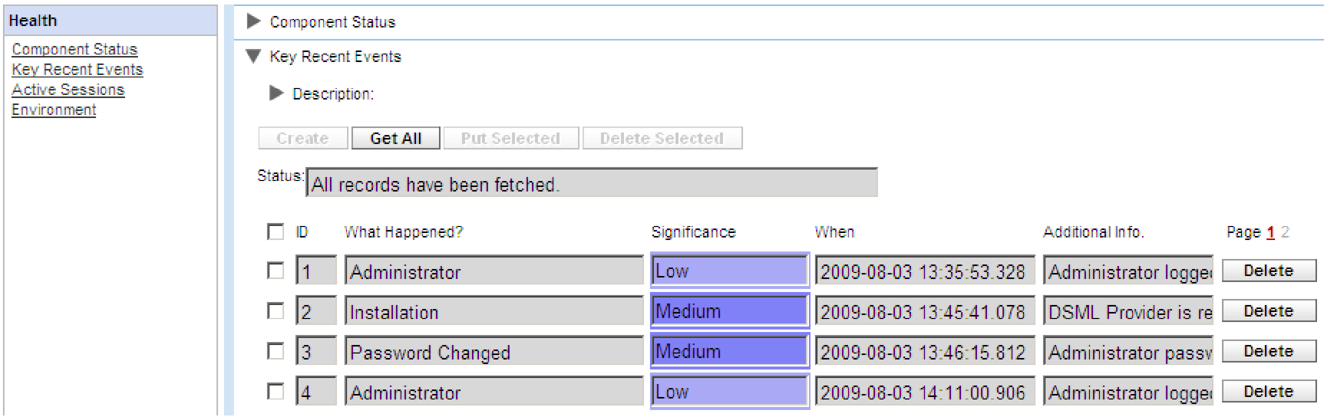
Status: All records have been fetched.

☐	ID	Component Name	Status	Reported At	Additional Info.	Page 1 2
☐	4	CSTA-Provider-1-192.168.42.1	Available	2009-05-11 04:48:19.546	component reportin	Delete
☐	3	CSTA-Provider-1-Master	Starting	2009-05-11 09:14:58.25	...no component pr	Delete
☐	2	DSML-Provider-1-192.168.42.1	Failed	2009-05-08 16:15:02.468	Initial provisioning fa	Delete
☐	1	DSML-Provider-1-Master	Available	2009-05-08 16:15:05.406	TotalCount:Success	Delete

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.

4.3.2 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.



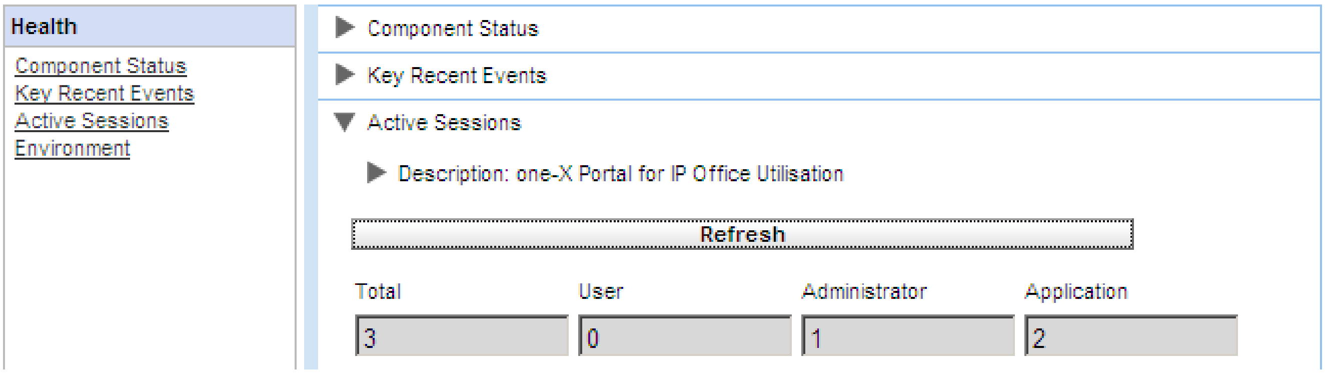
Status: All records have been fetched.

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

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

4.3.3 Active Sessions

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

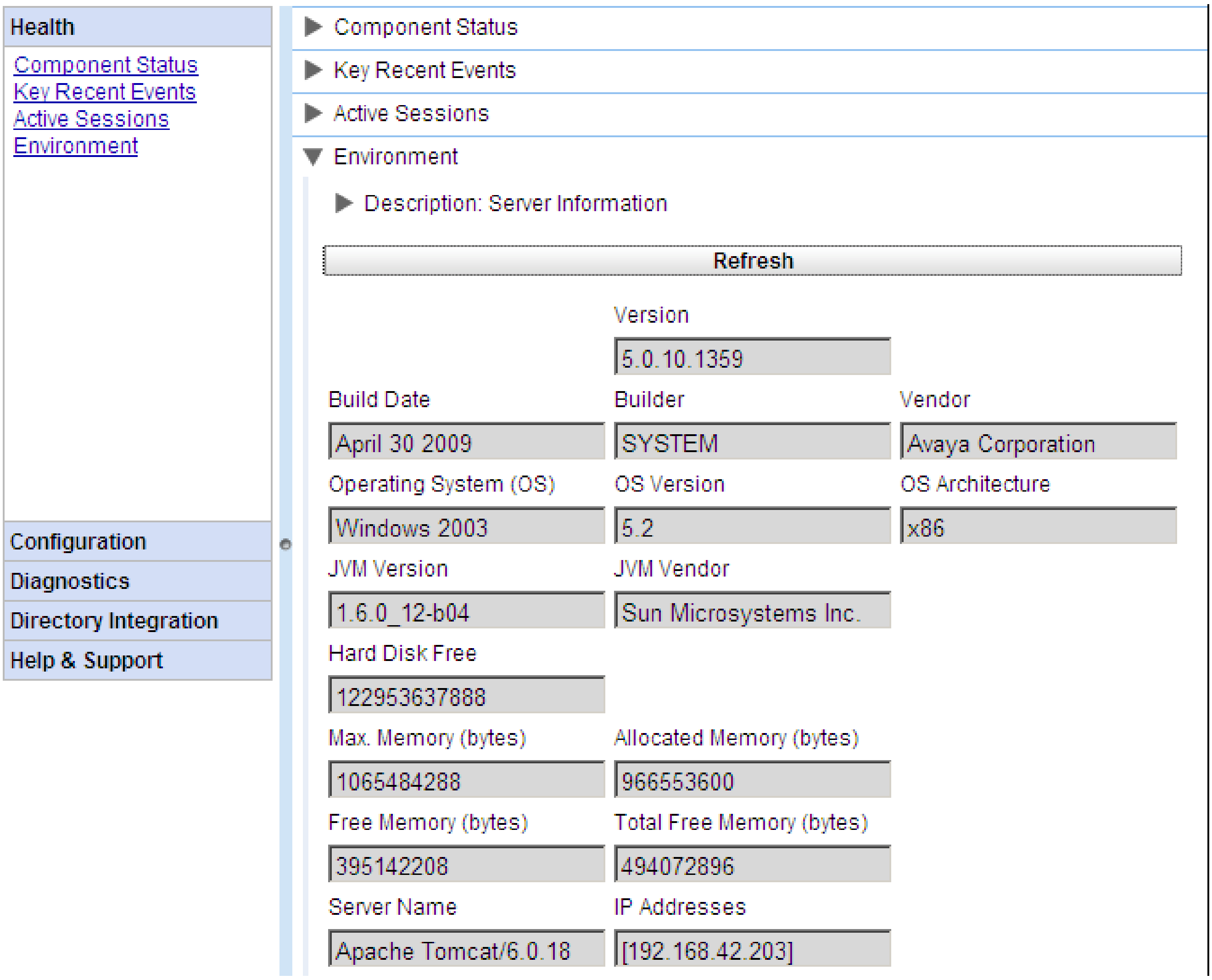


Total: 3
User: 0
Administrator: 1
Application: 2

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

4.3.4 Environment

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



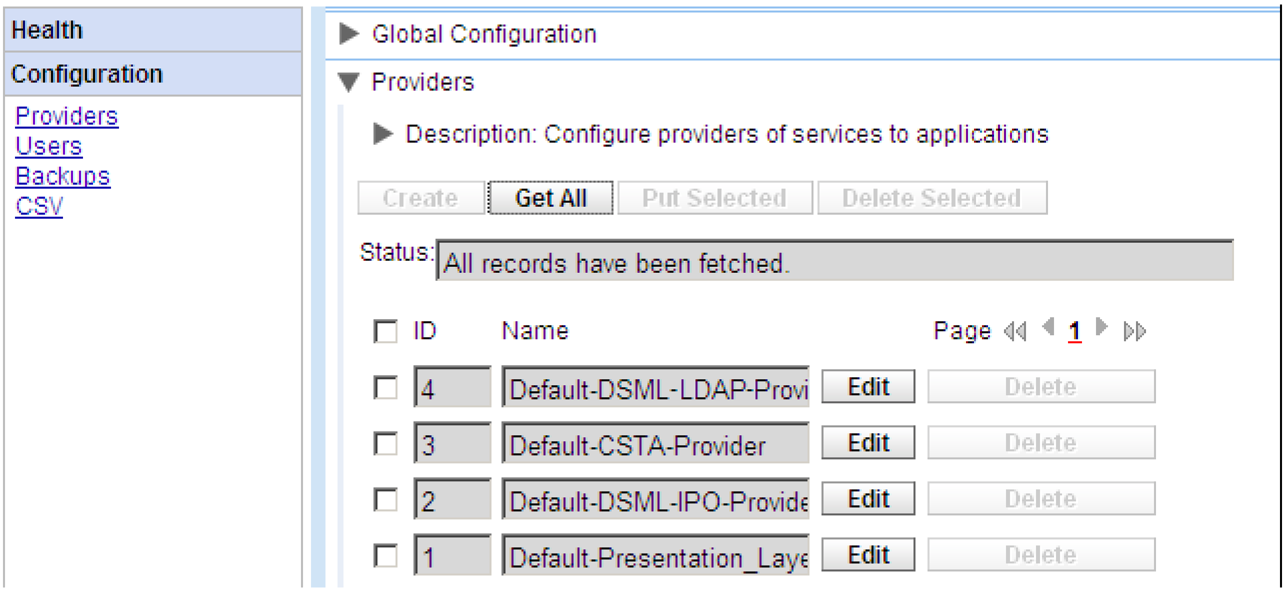
Version: 5.0.10.1359
Build Date: April 30 2009
Builder: SYSTEM
Vendor: Avaya Corporation
Operating System (OS): Windows 2003
OS Version: 5.2
OS Architecture: x86
JVM Version: 1.6.0_12-b04
JVM Vendor: Sun Microsystems Inc.
Hard Disk Free: 122953637888
Max. Memory (bytes): 1065484288
Allocated Memory (bytes): 966553600
Free Memory (bytes): 395142208
Total Free Memory (bytes): 494072896
Server Name: Apache Tomcat/6.0.18
IP Addresses: [192.168.42.203]

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

4.4 Configuration

4.4.1 Providers

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



▶ Description: Configure providers of services to applications

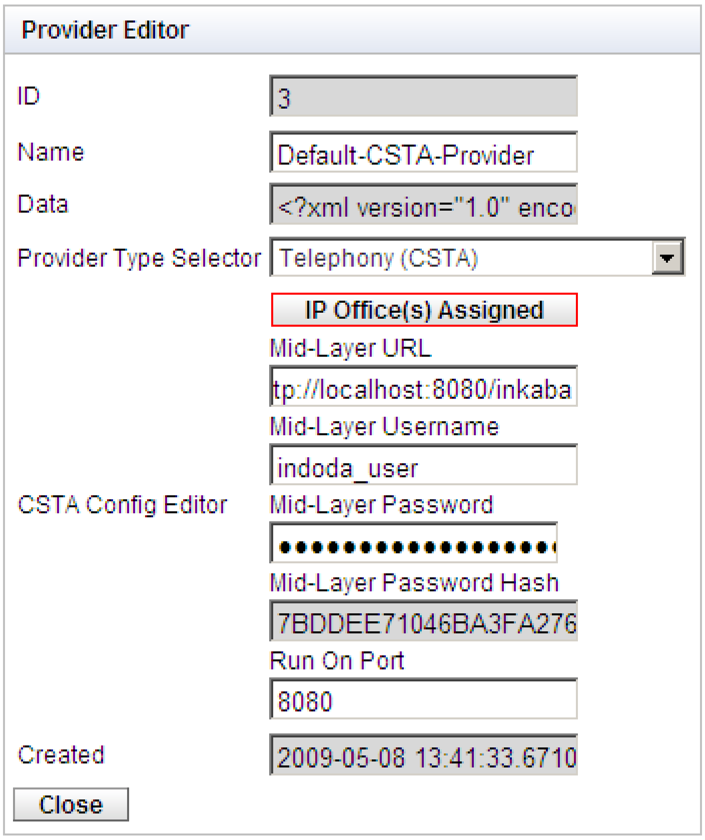
Status: All records have been fetched.

	ID	Name		
□	4	Default-DSML-LDAP-Provi	Edit	Delete
□	3	Default-CSTA-Provider	Edit	Delete
□	2	Default-DSML-IPO-Provide	Edit	Delete
□	1	Default-Presentation_Laye	Edit	Delete

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

4.4.1.1 Telephony (CSTA) Provider

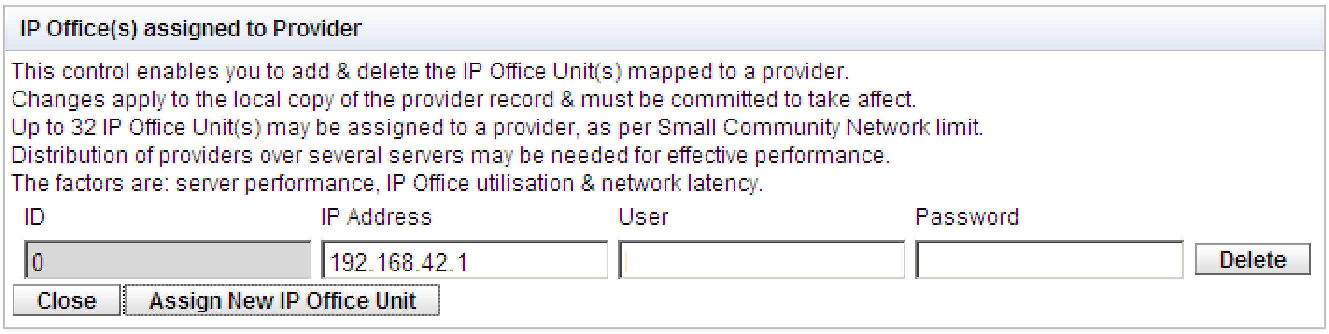
The settings below are shown for a Telephony (CSTA) provider. These should only be changed if you are experienced with the installation and operation of one-X Portal for IP Office.



Provider Editor

ID	3
Name	Default-CSTA-Provider
Data	<?xml version="1.0" enco
Provider Type Selector	Telephony (CSTA)
	IP Office(s) Assigned
CSTA Config Editor	Mid-Layer URL tp://localhost:8080/inkaba Mid-Layer Username indoda_user Mid-Layer Password ●●●●●●●●●●●●●●●●●● Mid-Layer Password Hash 7BDDEE71046BA3FA276 Run On Port 8080
Created	2009-05-08 13:41:33.6710

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



IP Office(s) assigned to Provider

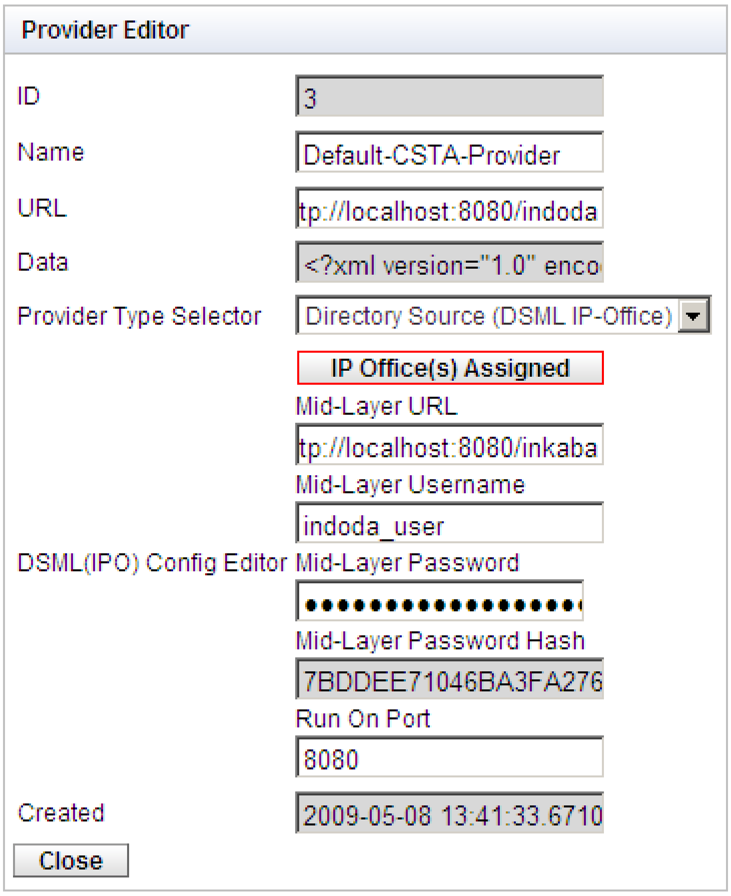
This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
Distribution of providers over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

ID	IP Address	User	Password	
0	192.168.42.1			Delete

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

4.4.1.2 DSML (IP Office) Provider

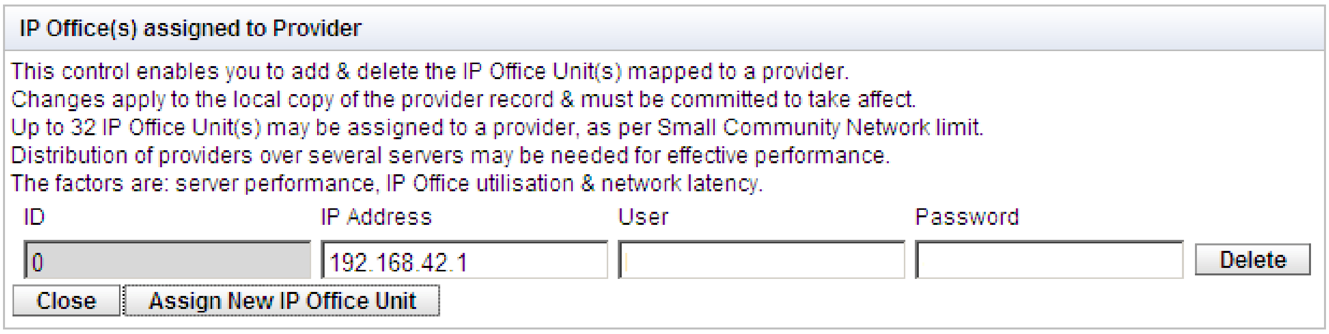
The settings below are shown for a Directory (DSML IP-Office) provider. These should only be changed if you are experienced with the installation and operation of one-X Portal for IP Office.



Provider Editor

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

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



IP Office(s) assigned to Provider

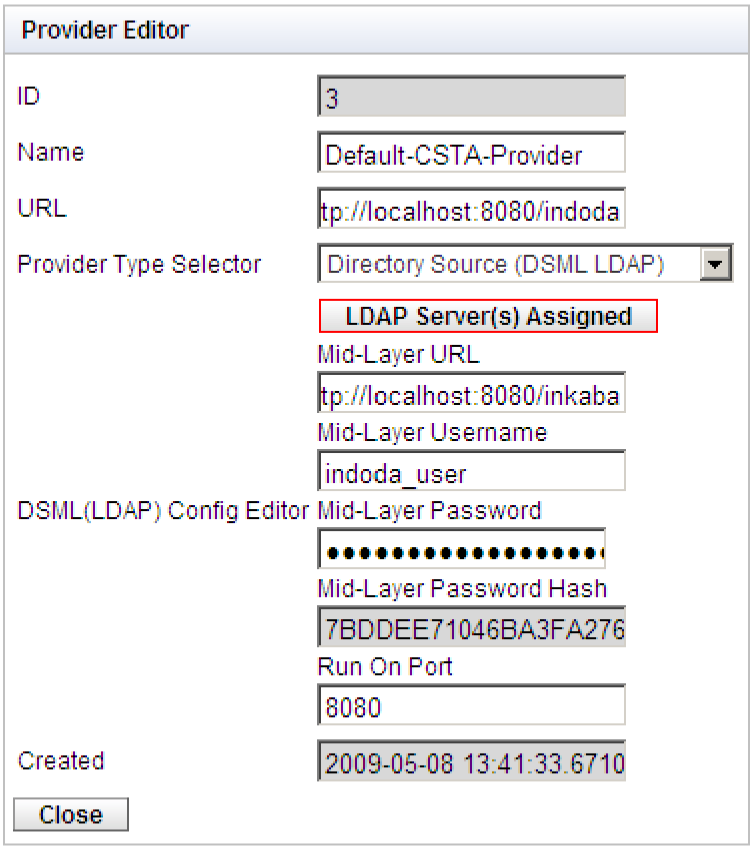
This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
Distribution of providers over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

ID	IP Address	User	Password	
0	192.168.42.1			Delete

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

4.4.1.3 DSML (LDAP) Provider

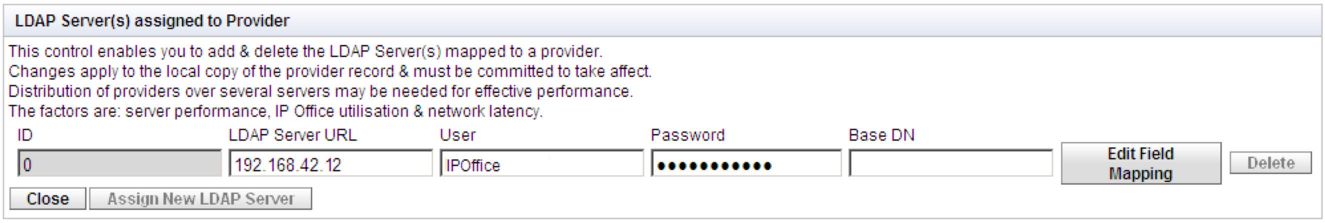
The settings below are shown for a **Directory (DSML LDAP)** provider.



Provider Editor

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

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

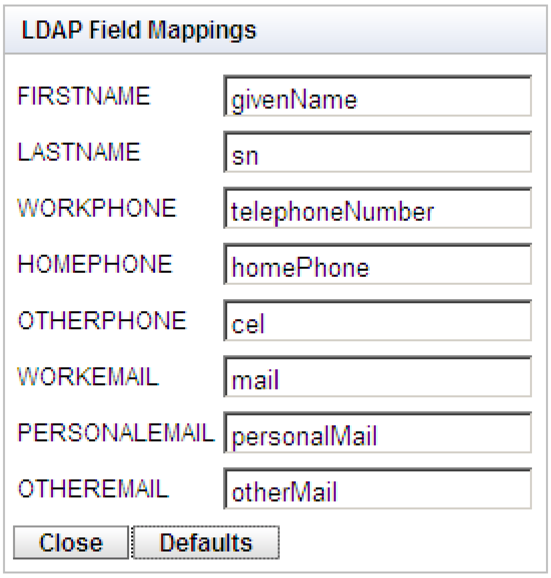


LDAP Server(s) assigned to Provider

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

ID	LDAP Server URL	User	Password	Base DN
0	192.168.42.12	IPOffice	●●●●●●●●●●●	

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



LDAP Field Mappings

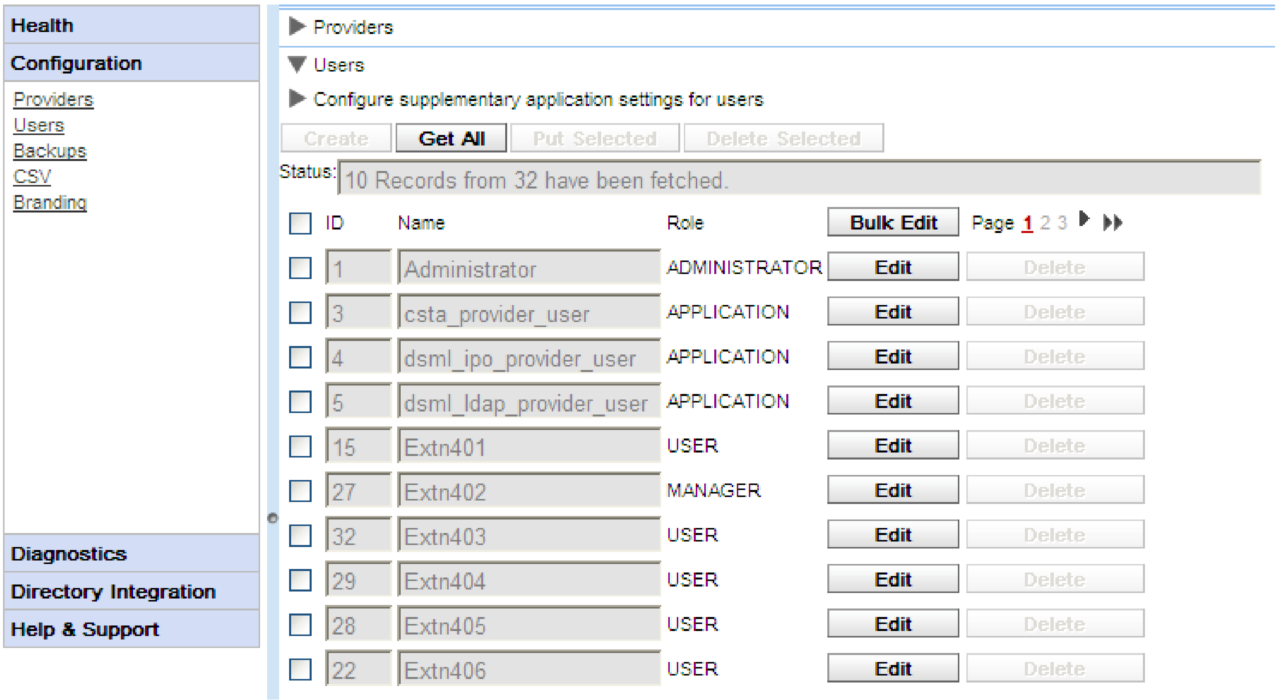
FIRSTNAME	givenName
LASTNAME	sn
WORKPHONE	telephoneNumber
HOMEPHONE	homePhone
OTHERPHONE	cel
WORKEMAIL	mail
PERSONALEMAIL	personalMail
OTHEREMAIL	otherMail

4.4.2 Users

The **Users** menu allows you to view the IP Office users. This includes all IP Office users, not just those enabled for one-X Portal for IP Office operation. The menu can be used to edit some user settings stored by the one-X Portal for IP Office. It cannot be used to edit user settings stored by the IP Office.

1. Select **Configuration** and then **Users**.

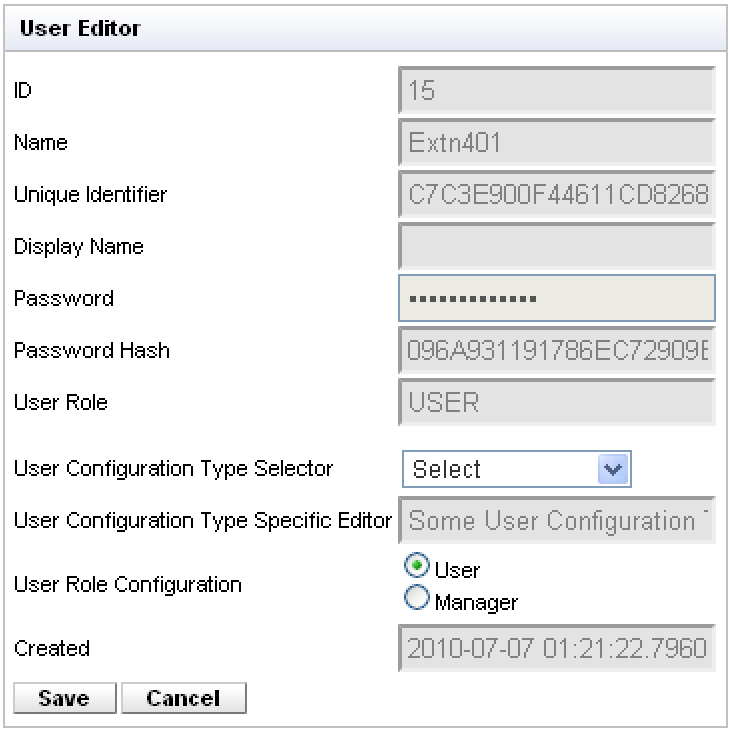
2. Click on **Get All**.



Status: 10 Records from 32 have been fetched.

□	ID	Name	Role	Bulk Edit	Page 1 2 3 ▶ ▶▶
□	1	Administrator	ADMINISTRATOR	Edit	Delete
□	3	csta_provider_user	APPLICATION	Edit	Delete
□	4	dsml_ipo_provider_user	APPLICATION	Edit	Delete
□	5	dsml_ldap_provider_user	APPLICATION	Edit	Delete
□	15	Extn401	USER	Edit	Delete
□	27	Extn402	MANAGER	Edit	Delete
□	32	Extn403	USER	Edit	Delete
□	29	Extn404	USER	Edit	Delete
□	28	Extn405	USER	Edit	Delete
□	22	Extn406	USER	Edit	Delete

3. Browse through the users. When the required used is located, click on **Edit**. You can also select multiple users and then click **Bulk Edit** in order to edit several users at the same time.



User Editor

ID	15
Name	Extn401
Unique Identifier	C7C3E900F44611CD8268
Display Name	
Password	•••••••••••••
Password Hash	096A931191786EC72909E
User Role	USER
User Configuration Type Selector	Select
User Configuration Type Specific Editor	Some User Configuration `
User Role Configuration	● User ○ Manager
Created	2010-07-07 01:21:22.7960

4. Use the **User Configuration Type Selector** to select the user settings to edit. The options are **Screen Popping**, **Park Slots** and **Bridge Number**.

5. The **User Role Configuration** is currently used in conjunction with Customer Call Reporter. The name and password of a user set as ***Manager*** can be entered into the Customer Call Reporter application's configuration. Those details enable the Customer Call Reporter feature for forcing agent states.

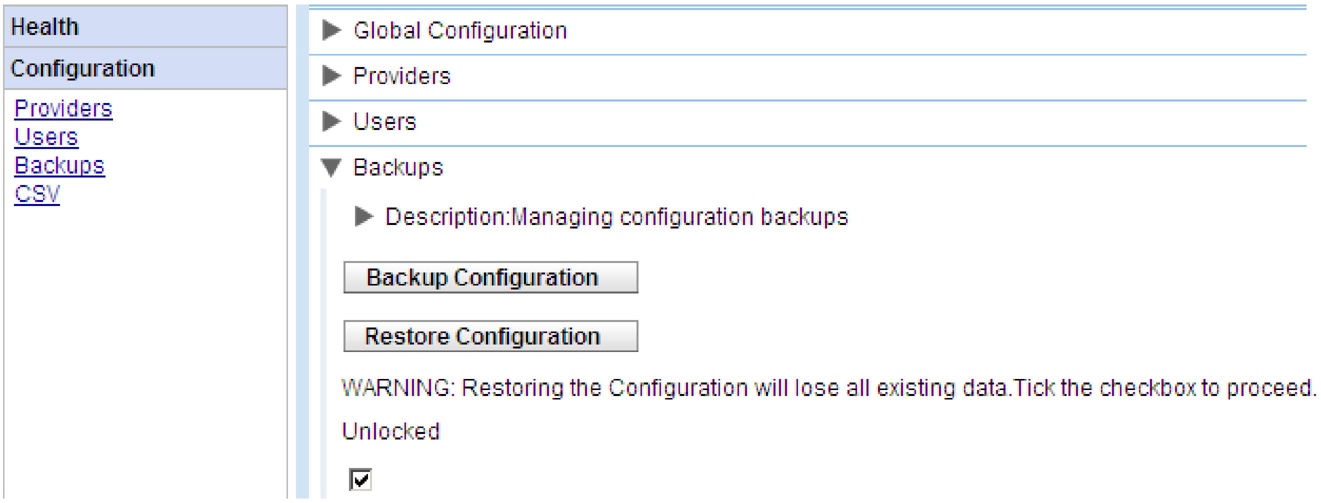
6. When the changes required have been made click **Save**.

7. If changes have been made to any user records, use the **Put Selected** button to write those changes into the one-X Portal for IP Office database.

If you think that the user records do not match the users configured on the IP Office systems, the **Directory Integration | Directory Synchronization** 75 menu can be used to force an update from the IP Office systems.

4.4.3 Backups

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



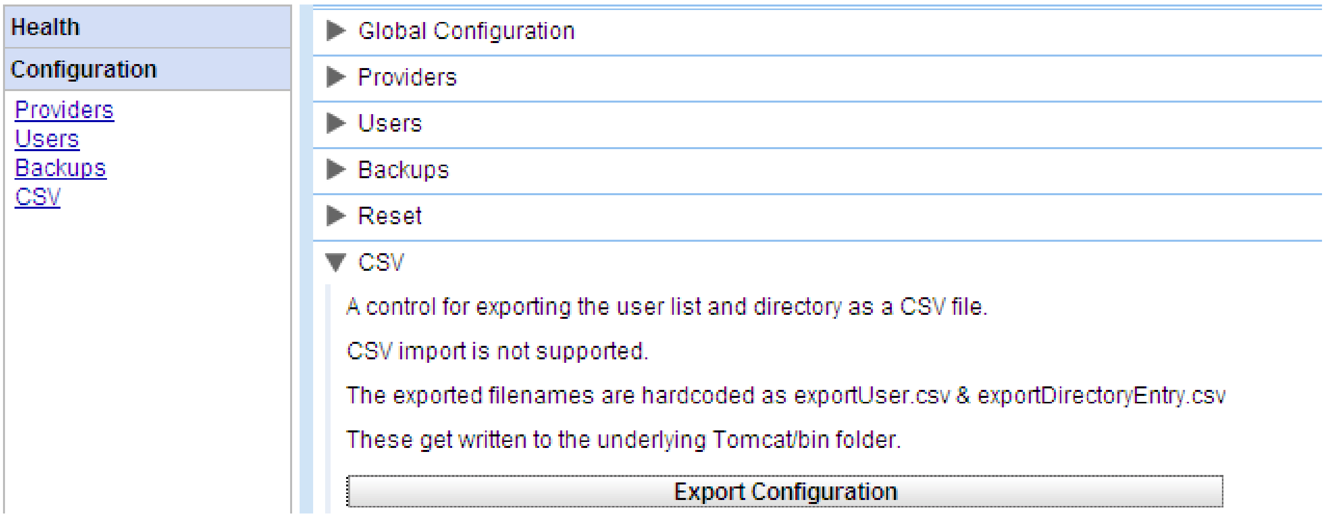
Description:Managing configuration backups

WARNING: Restoring the Configuration will lose all existing data.Tick the checkbox to proceed.

Note that this is only intended as a simply backup and restore to allow rollback of server changes while making and testing administration changes. A more sophisticated set of backup and restore 80 options are available.

4.4.4 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.



A control for exporting the user list and directory as a CSV file.

CSV import is not supported.

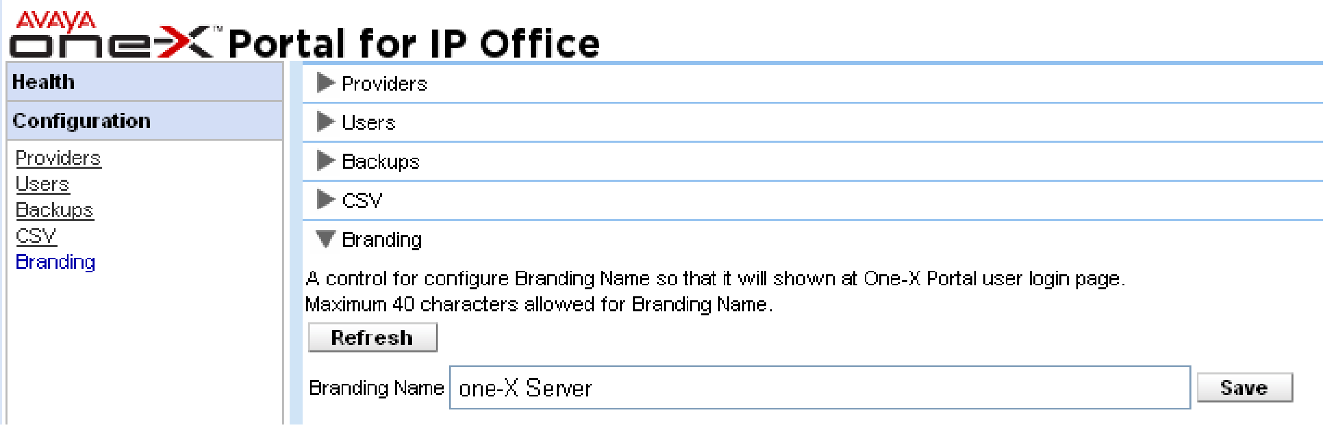
The exported filenames are hardcoded as exportUser.csv & exportDirectoryEntry.csv

These get written to the underlying Tomcat/bin folder.

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***

4.4.5 Branding

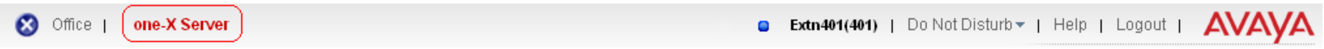
This menu allows you to specify some text that is then displayed on the one-X Portal for IP Office pages after a user has logged in.



A control for configure Branding Name so that it will shown at One-X Portal user login page.
Maximum 40 characters allowed for Branding Name.

Branding Name: one-X Server

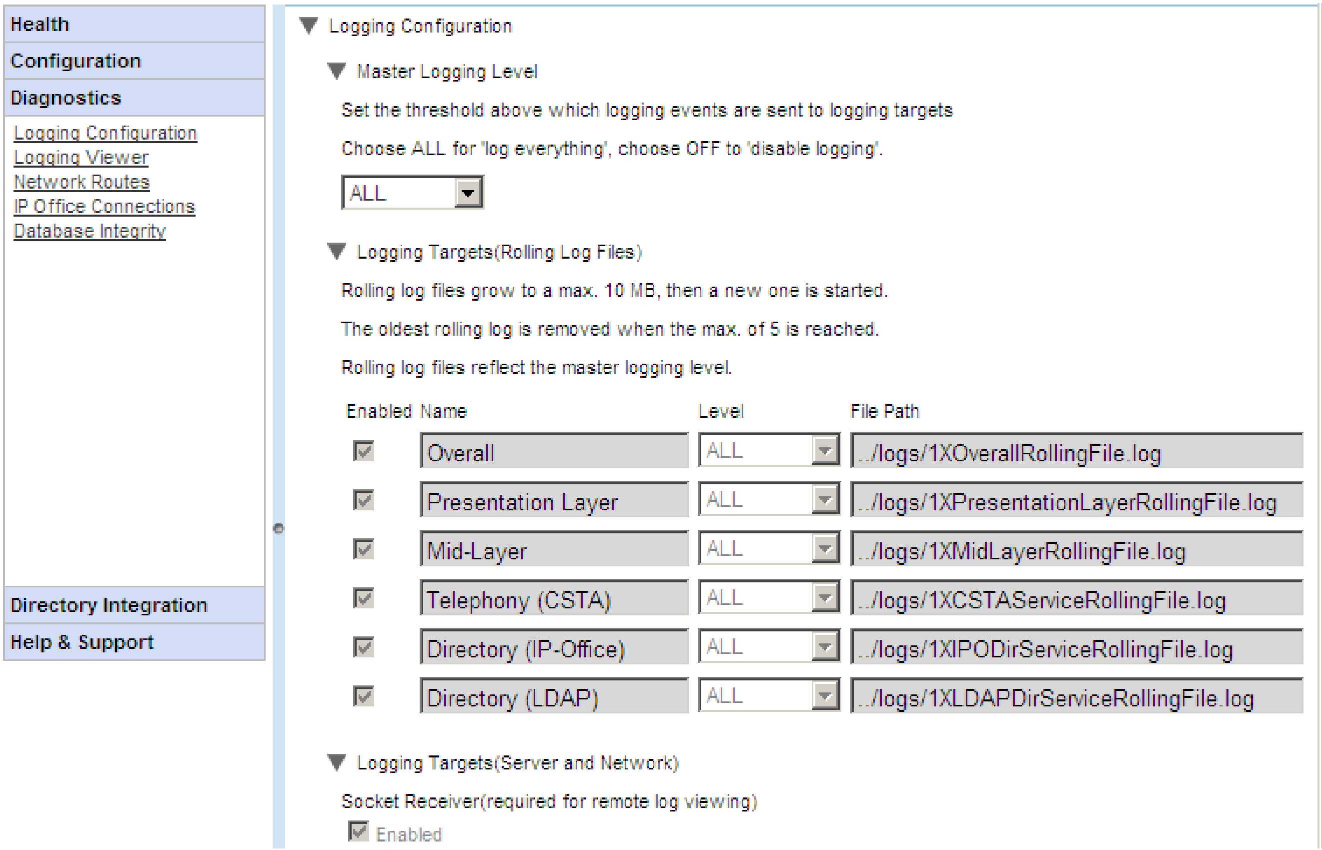
The text is displayed in the one-X Portal for IP Office title bar as shown below.



4.5 Diagnostics

4.5.1 Logging Configuration

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



▼ Logging Configuration

▼ Master Logging Level

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

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

ALL

▼ Logging Targets(Rolling Log Files)

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

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

Rolling log files reflect the master logging level.

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

▼ Logging Targets(Server and Network)

Socket Receiver(required for remote log viewing)

☑ Enabled

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.

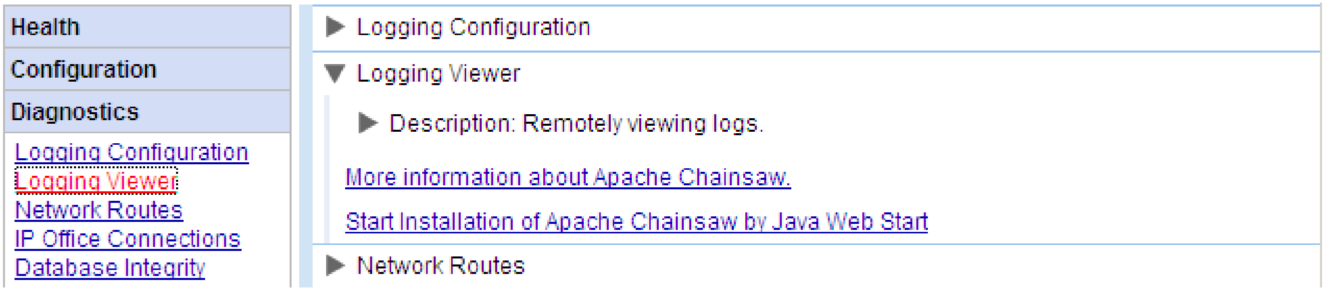
        - **Directory (IP Office):** *1XIPODirServiceRollingFile.log*
          This log captures IP Office directory information.

        - **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.

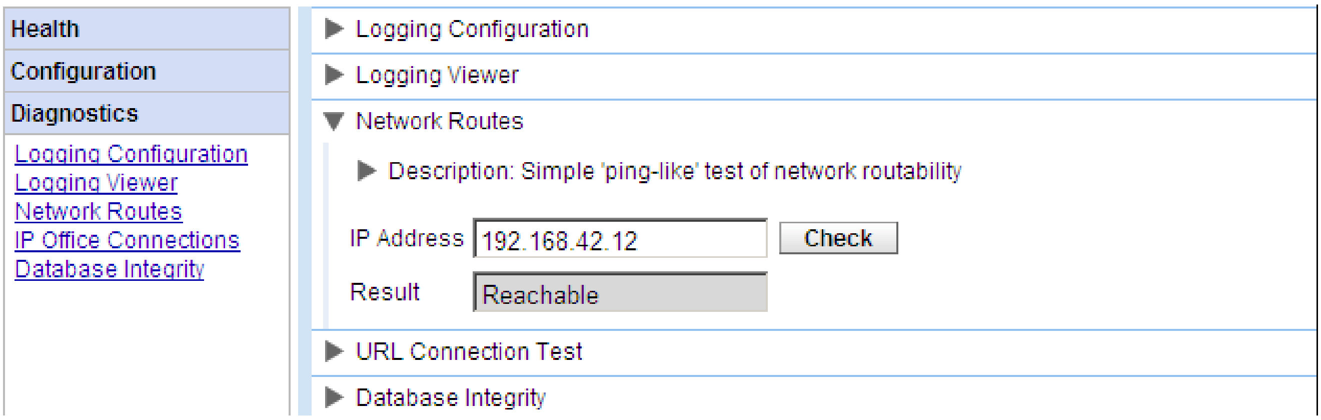
4.5.2 Logging Viewer

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 installing Apache Chainsaw.



4.5.3 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 74 should be used instead.



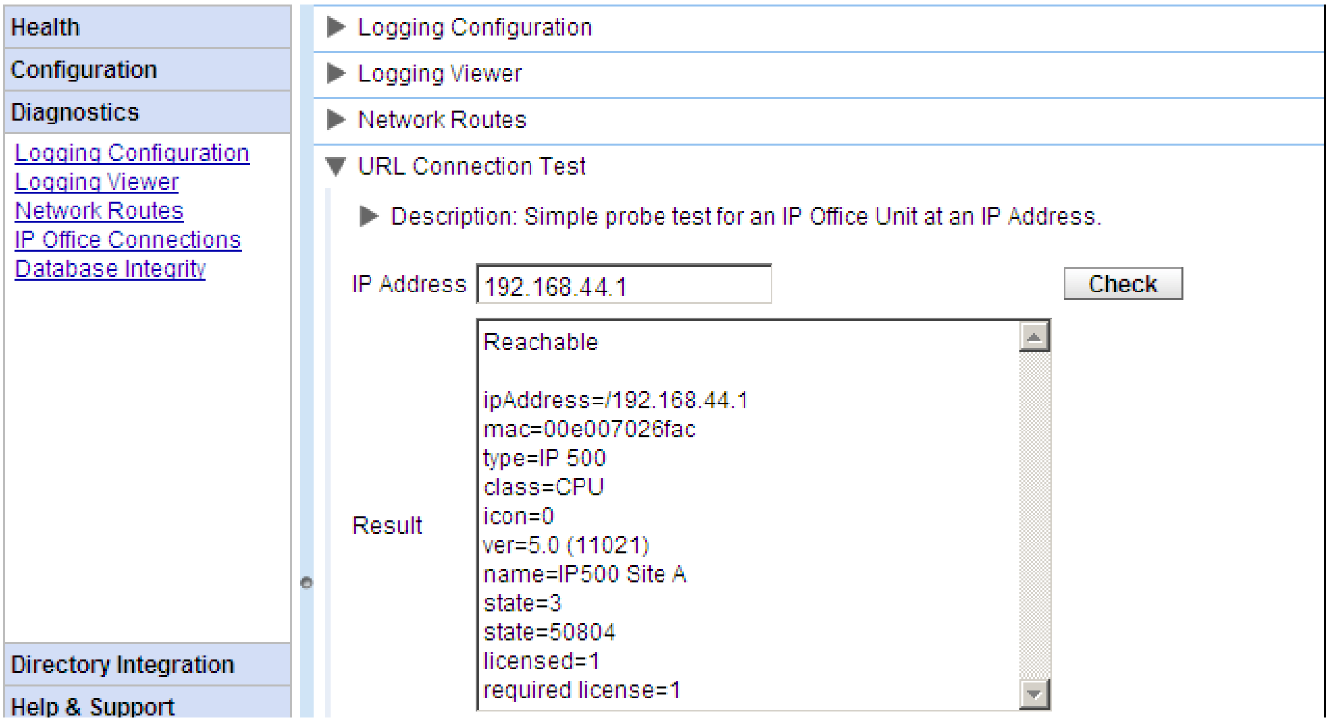
IP Address 192.168.42.12

Result Reachable

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***.

4.5.4 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).



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

IP Address: 192.168.44.1

Result:

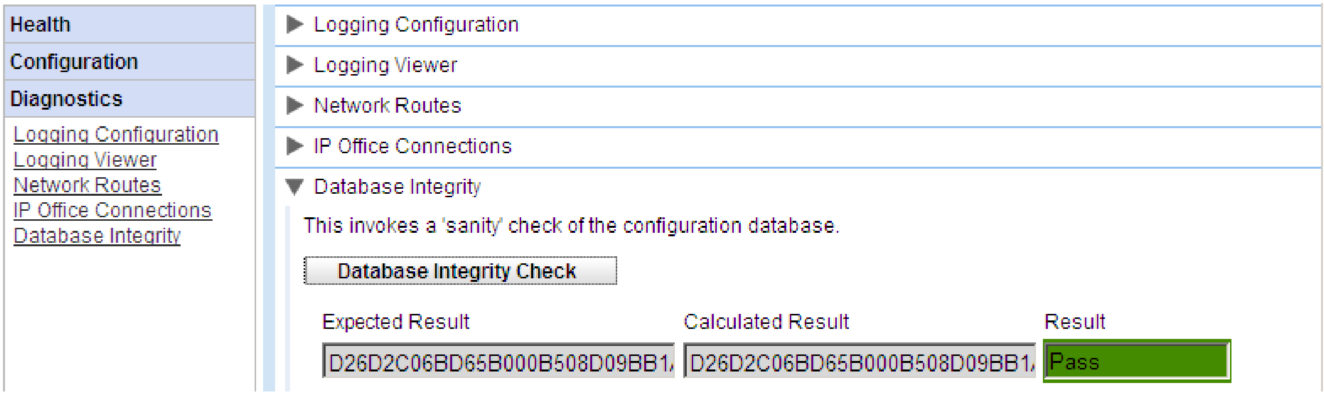
```
Reachable

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

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.

4.5.5 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.



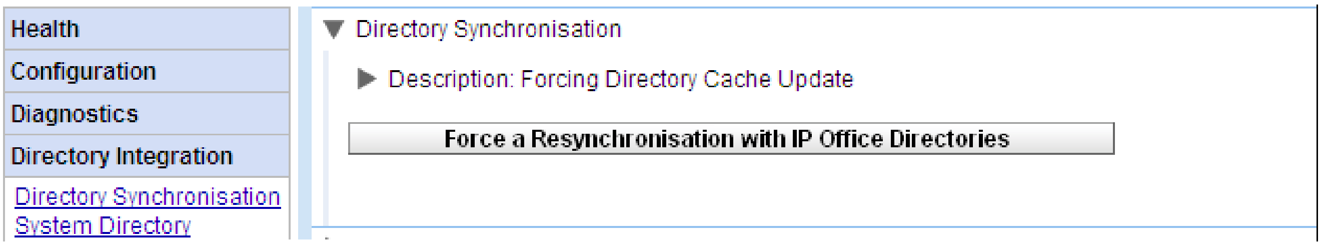
This invokes a 'sanity' check of the configuration database.

Expected Result	Calculated Result	Result
D26D2C06BD65B000B508D09BB1/	D26D2C06BD65B000B508D09BB1/	Pass

4.6 Directory Integration

4.6.1 Directory Synchronisation

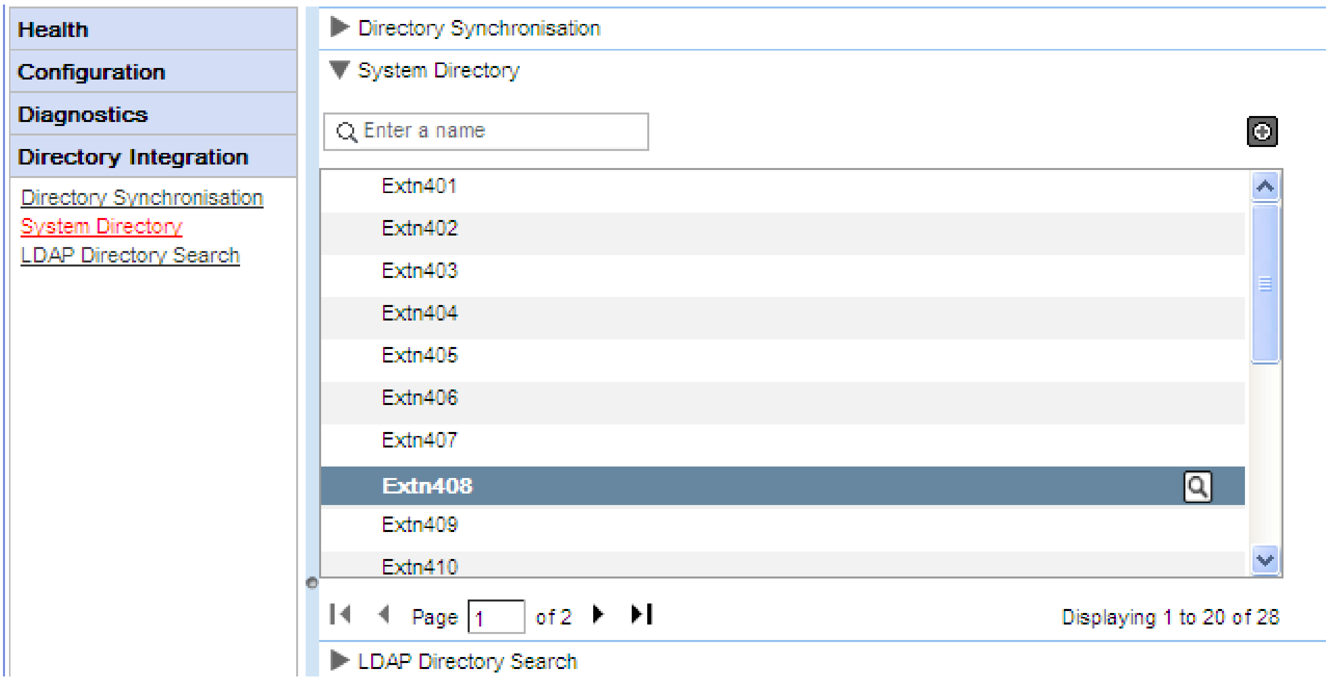
During normal operation, the one-X Portal for IP Office server updates the records every 300 seconds approximately. However, if necessary this menu can be used to force an update of the system directory and IP Office users.


Health
Configuration
Diagnostics
Directory Integration
Directory Synchronisation
System Directory
▼ Directory Synchronisation
▶ Description: Forcing Directory Cache Update
Force a Resynchronisation with IP Office Directories

- **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** 76 option.

4.6.2 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.



Extn401
Extn402
Extn403
Extn404
Extn405
Extn406
Extn407
Extn408
Extn409
Extn410

Displaying 1 to 20 of 28

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. If necessary you can force an update using the **Directory Synchronization** 75 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.

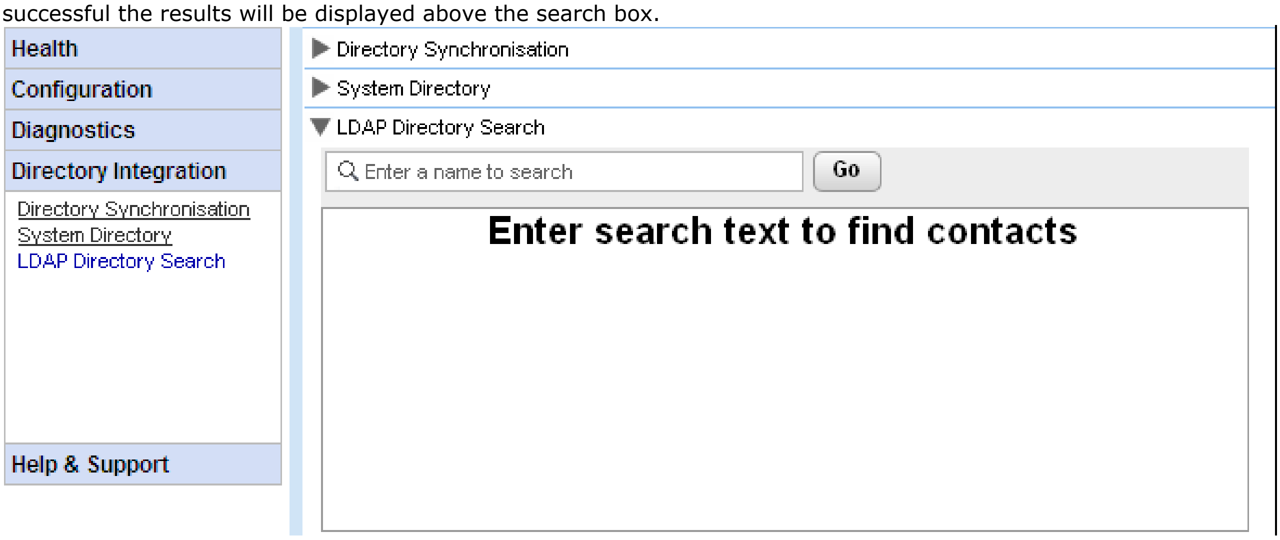
4.6.3 LDAP Directory Search

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.

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.



4.7 Help & Support

Help | Help

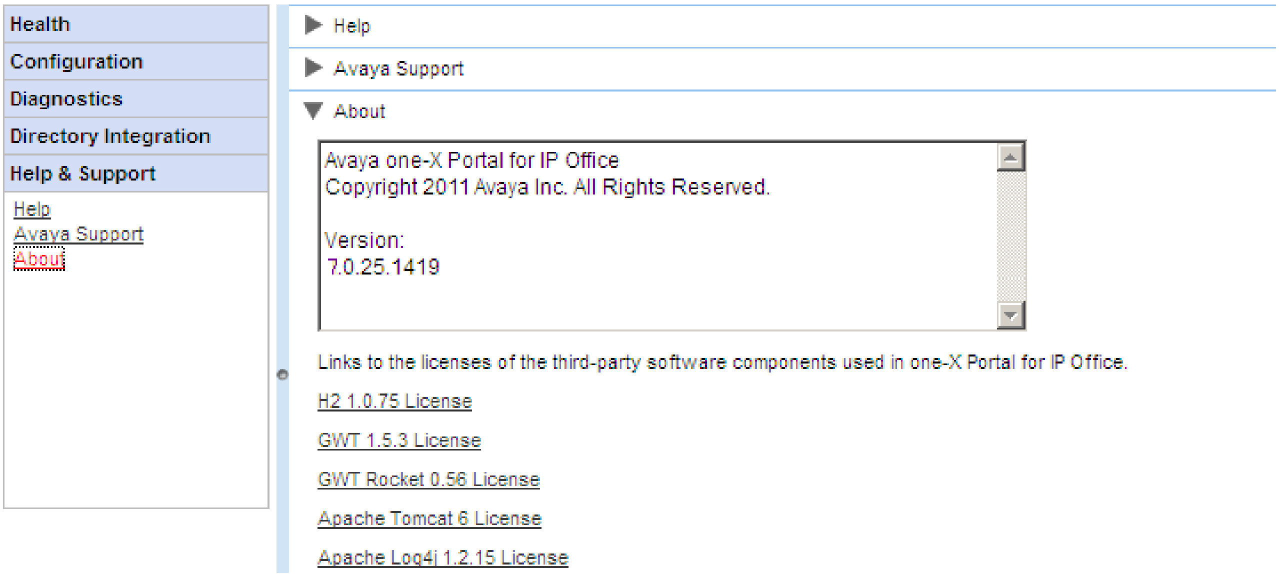
Provides links to both the one-X Portal for IP Office user help and to this document as help.

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.



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

Version:
7.0.25.1419

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

H2 1.0.75 License

GWT 1.5.3 License

GWT Rocket 0.56 License

Apache Tomcat 6 License

Apache Log4j 1.2.15 License

Chapter 5. Backup/Restore

5. Backup/Restore

The one-X Portal for IP Office supports a set of menus for the backup and, if necessary, 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.

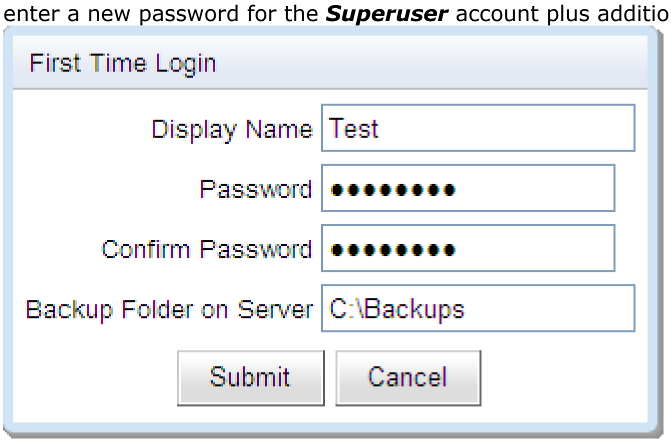
The menus are also intended to allow backup and restoration between an old and a new installation of one-X Portal for IP Office on a new server. However it is not supported for backup and restoration between different versions of one-X Portal for IP Office, for example from 6.1 to 7.0.

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

5.1 Superuser Login

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

1. Enter the browser address ***http://<server>:8080/induna/induna.html***.
2. At the login menu, enter the name ***Superuser*** and enter the associated password.
    - If this is the first login, 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.



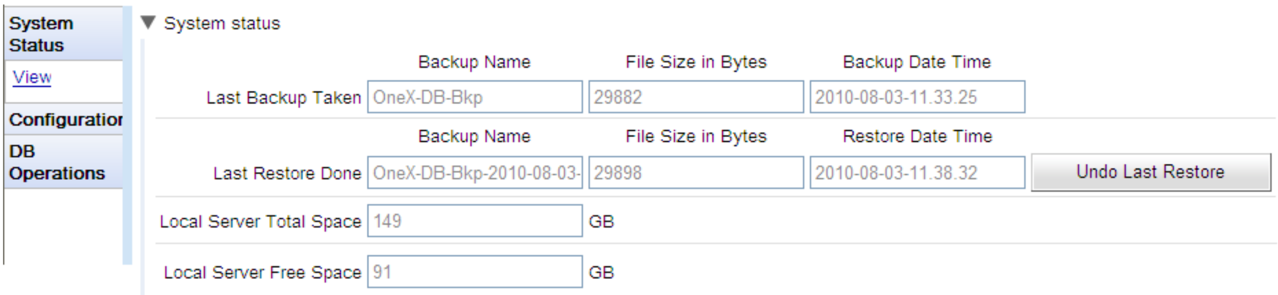
First Time Login

Display Name	Test
Password	●●●●●●●●
Confirm Password	●●●●●●●●
Backup Folder on Server	C:\Backups

- **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.

5.2 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.



	Backup Name	File Size in Bytes	Backup Date Time
Last Backup Taken	OneX-DB-Bkp	29882	2010-08-03-11.33.25

	Backup Name	File Size in Bytes	Restore Date Time
Last Restore Done	OneX-DB-Bkp-2010-08-03-	29898	2010-08-03-11.38.32

Local Server Total Space 149 GB

Local Server Free Space 91 GB

- **Last Backup Taken**
  This section gives details of the last backup taken using the Backup menu. The backup file name will have been a zip file named with the the **Backup Name** plus the **Backup Date Time**. For example, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.

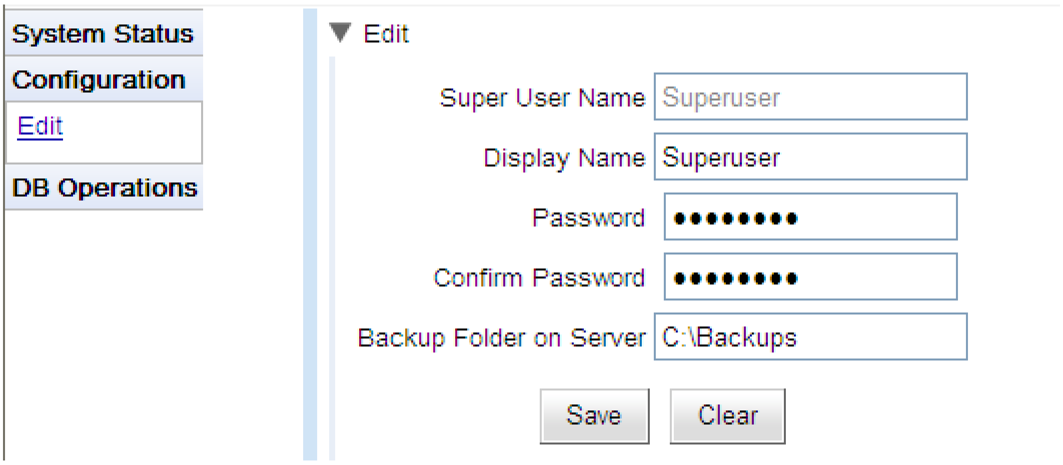
- **Last Restore Done**
  This section gives details of the last restore operation. The time and date of the restore are shown and the name of the file used for that operation. The Undo Last Restore control can be used to rollback the restore action.

- **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.

5.3 Configuration

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



Super User Name: Superuser

Display Name: Superuser

Password: ••••••••

Confirm Password: ••••••••

Backup Folder on Server: C:\Backups

- **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.

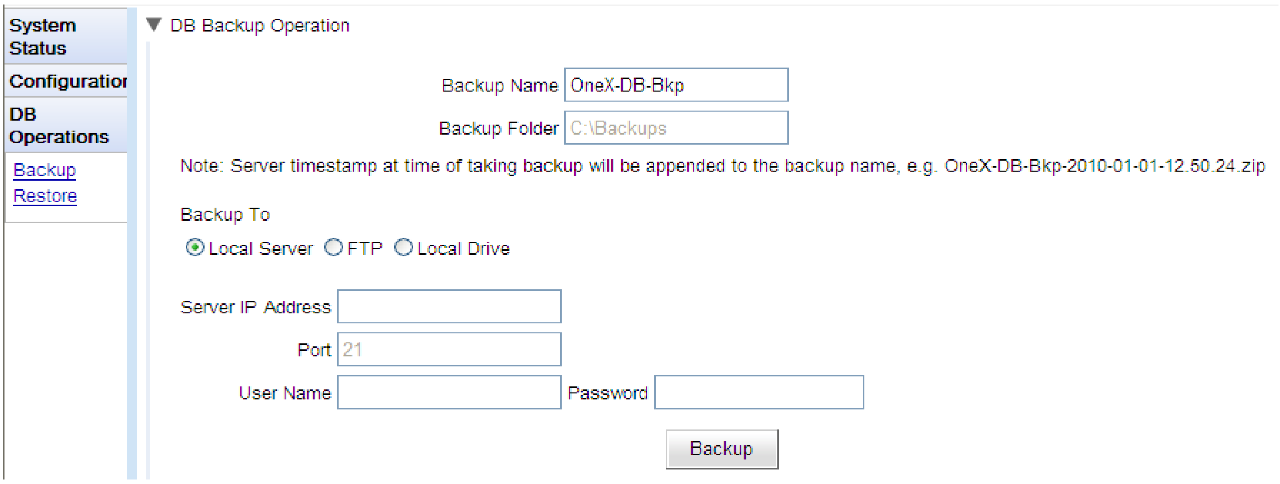
- **Backup Folder**
  This is the path to be used for backup and restore operations on the one-X Portal for IP Office server. Note that even if backing up and restoring to and from an FTP or local PC folder, this server folder is still used for temporary file storage.

5.4 DB Operations

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

5.4.1 Backup

This menu is used to create backup files.



▼ DB Backup Operation

Backup Name: OneX-DB-Bkp

Backup Folder: C:\Backups

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

Backup To

● Local Server ○ FTP ○ Local Drive

Server IP Address:

Port: 21

User Name: Password:

- **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.

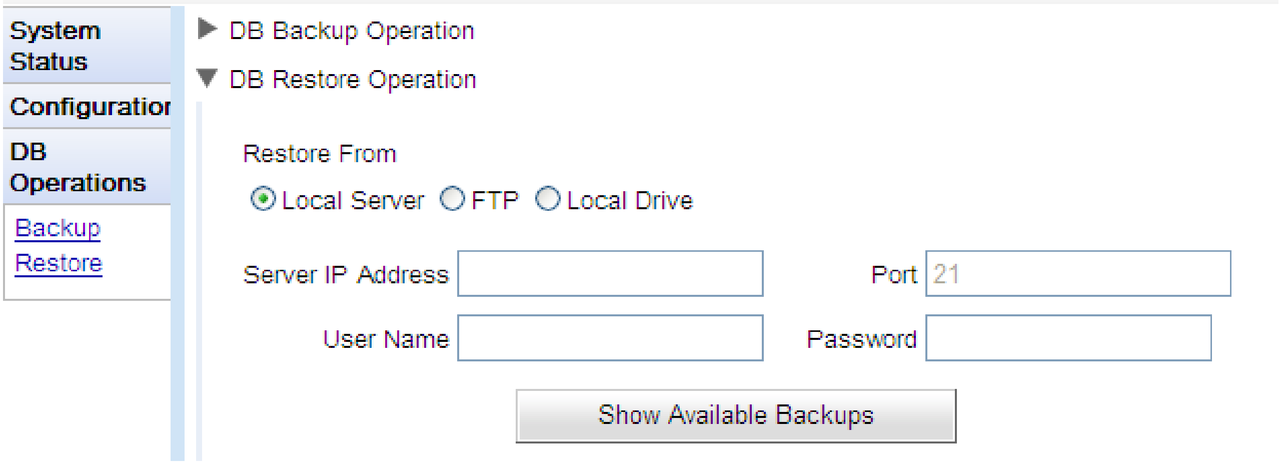
  - **Port**
    The FTP port on the server. The normal default is port 21.

  - **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.

5.4.2 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** 81 control. Restoration is only supported from a backup of the same one-X Portal for IP Office version.



Restore From

● Local Server ○ FTP ○ Local Drive

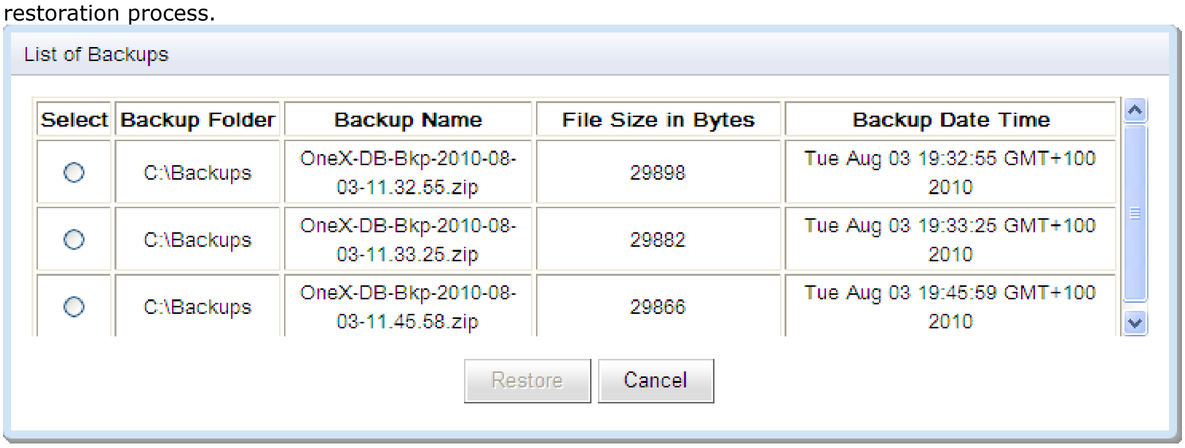
Server IP Address:

Port: 21

User Name:

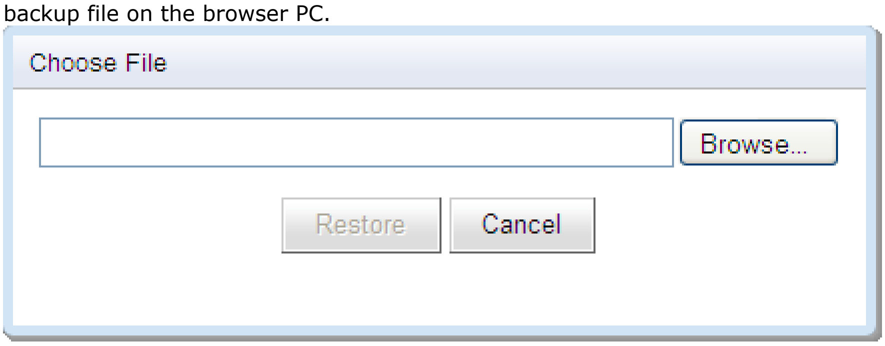
Password:

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



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

- **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 6. Glossary

6. 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.

Index

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.