



IP Office 7.0

one-X Portal for IP Office Installation

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation Disclaimer

Avaya Inc. is not 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.

Link Disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

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 Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s): 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, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use 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 identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at: <http://support.avaya.com/ThirdPartyLicense/>

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. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com. For additional support telephone numbers, see the Avaya Support web site (<http://www.avaya.com/support>).

Trademarks

Avaya and the Avaya logo are registered trademarks of Avaya Inc. in the United States of America and other jurisdictions.

Unless otherwise provided in this document, marks identified by "®," "™" and "SM" are registered marks, trademarks and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Documentation information

For the most current versions of documentation, go to the Avaya Support web site (<http://www.avaya.com/support>) or the IP Office Knowledge Base (<http://marketingtools.avaya.com/knowledgebase/>).

Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1 800 628 2888 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

1.1 Providers	8
1.2 one-X Portal for IP Office Settings	9
1.3 Telephony Notes	11
1.4 Small Community Network Support	12

2. Installation

2.1 Installation Requirements	15
2.2 Check the IP Office Security Settings	18
2.3 Add one-X Portal for IP Office Licenses	20
2.4 Configure Users for one-X Portal for IP Office	21
2.5 Checking Available Server Ports	22
2.6 Install the one-X Portal for IP Office Software	23
2.7 Initial Server Configuration	26
2.8 Test User Connection	30
2.9 Disable Java Updates	31
2.10 Advanced Configuration Options	32

3. Maintenance

3.1 Manually Starting the Service	37
3.2 Adding an Additional IP Office	38
3.3 Changing IP Office Details	41
3.4 Adding an LDAP External Directory Source	43
3.5 Adding/Deleting Users	44
3.6 Editing User Settings	44
3.7 Backing Up the Database	47
3.8 Restoring a Previous Backup	48
3.9 Checking and Updating the System Directory	49
3.10 Checking the External LDAP Directory	50
3.11 Upgrading one-X Portal for IP Office	51
3.12 Downgrading one-X Portal for IP Office	52
3.13 Removing one-X Portal for IP Office	53
3.14 Remote Logging	55
3.15 Troubleshooting	59
3.16 Agent Gadget Control	60

4. Administration

4.1 Login	63
4.2 Logout	63
4.3 Health	64
4.3.1 Component Status	64
4.3.2 Key Recent Events	64
4.3.3 Active Sessions	65
4.3.4 Environment	65
4.4 Configuration	66
4.4.1 Providers	66
4.4.2 Users	70
4.4.3 Backups	72
4.4.4 CSV	72
4.4.5 Branding	73
4.5 Diagnostics	74
4.5.1 Logging Configuration	74
4.5.2 Logging Viewer	75
4.5.3 Network Routes	75
4.5.4 IP Office Connections	76
4.5.5 Database Integrity	76

4.6 Directory Integration	77
4.6.1 Directory Synchronisation	77
4.6.2 System Directory	78
4.6.3 LDAP Directory Search	79
4.7 Help & Support	80

5. Backup/Restore

5.1 Superuser Login	82
5.2 System Status	83
5.3 Configuration	83
5.4 DB Operations	84
5.4.1 Backup	84
5.4.2 Restore	85

6. Glossary

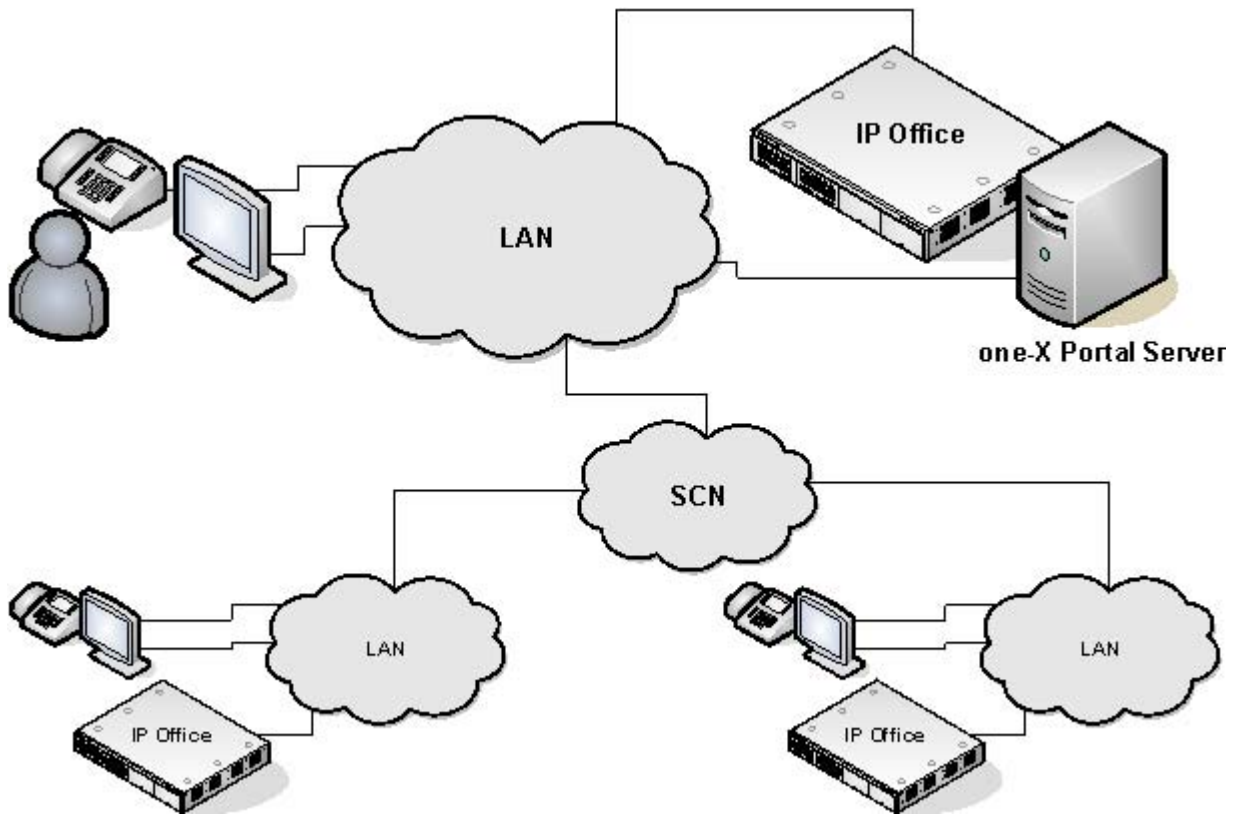
Index	89
-------------	----

Chapter 1.

one-X Portal for IP Office

1. one-X Portal for IP Office

This documentation covers the installation of one-X Portal for IP Office supported by IP Office Release <%BOMBAY%>. 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](#)^[12] (SCN). one-X Portal for IP Office supports up to 500 simultaneous sessions.



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.

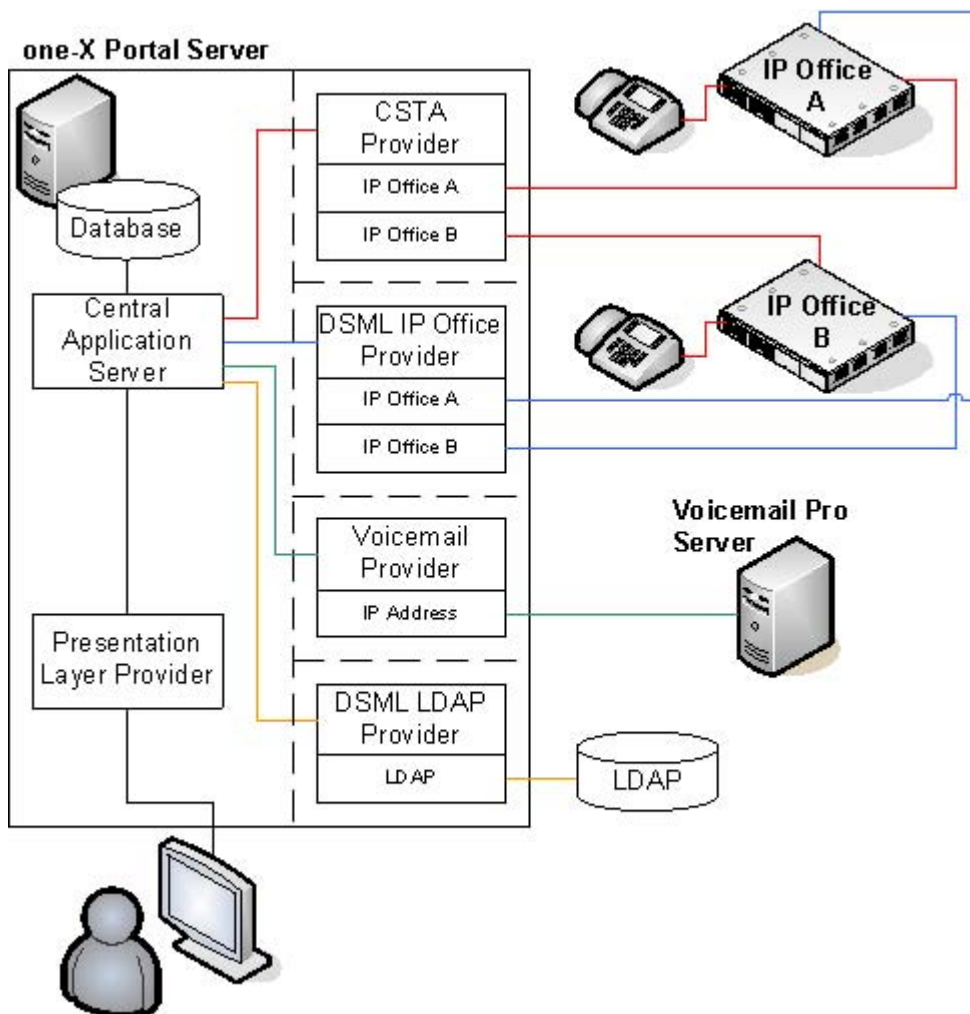
The one-X Portal for IP Office service communicates with the IP Office system using the IP Office's TSPI (Telephony Service Provider Interface) service. This service is configured through the security settings of the IP Office control units.

one-X Portal for IP Office is a licensed application, with each IP Office requiring a one-X Portal for IP Office license for those [users configured to use](#)^[21] one-X Portal for IP Office.

1.1 Providers

A key idea to understand for 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](#) ^[38] 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.

1.2 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 IP Office 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.
 - For users with a 1608, 1616, 9400, 9500 or 9600 phones, they 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](#)^[78] 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](#)^[43] 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	✓	✓	<p>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.</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> IP500/IP500v2: 10800 total personal directory records. For users with a 1608, 1616, 9400, 9500 or 9600 phones, they can edit or delete contacts through the phone's menus (primary phone number only).
Call Log	—	✓	A user's call log is stored in the configuration of their IP Office.
Voicemail Messages	—	✓	Details of the user's voicemail messages are taken from the voicemail server via the IP Office.
Profiles	✓	—	A user's profiles are stored by the one-X Portal for IP Office server. When a profile is made active it 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](#) ^[53] rather than [upgraded](#) ^[51].

1.3 Telephony Notes

Incoming Calls

The calls that reach the one-X Portal for IP Office user still fully controlled by the IP Office system settings. For example the user's call waiting settings, number of 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 phones, the call log shown by the phone and the redial function use information stored by the phone. Typically this will not include calls made using 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 call 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 system and to SIP extensions.
- Avaya 1400, 1600, 9400, 9500 and 9600 Series phones can be optionally set to use en-bloc dialing.

1.4 Small Community Network Support

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

- 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 temporarily hot desk. This means that all systems in the SCN must be the same IP Office software release.
- one-X Portal for IP Office does not provide additional SCN features. It only supports SCN features that are supported by the IP Office systems. For example, the park buttons provided by one-X Portal for IP Office are not supported between different systems in an SCN. This means that one-X Portal for IP Office users can only park and unpark calls on the IP Office on which they are registered.
- one-X Portal for IP Office 6.0 and higher supports up to 500 simultaneous sessions.

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 one-X Portal for IP Office Licenses](#) ²⁰
4. [Configure IP Office Users for one-X Portal for IP Office](#) 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
The IP Office Applications DVD for IP Office Release <%THISVERSION%> 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 System Requirements

- IP Office System
If the system running pre-IP Office Release <%THISVERSION%> software, it must be upgraded as per the relevant IP Office Technical Bulletins before proceeding.
 - IP Office Small Community Network Support
Operation with multiple IP Office's is only supported within a single IP Office Small Community Network (SCN).
 - Each IP Office must be running IP Office Release <%THISVERSION%> or higher software.
 - Each user and group name must be unique.
 - Each user and group extension number must be unique. The IP Office System Status Application (SSA) should be used to check for name and extension conflicts before installation of one-X Portal for IP Office.
- IP Office Release 6+ Licensing
This release of IP Office uses user profiles licenses. 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).
- RAM Memory: 2GB.
- 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 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>/local/start.asp* into a browser. If the IIS server does not respond 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.
 - one-X Portal for IP Office Licenses.
 - 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 enable the External tab in the one-X Portal for IP Office Directory gadget, details of the customer's LDAP server and search configuration details are required.

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

one-X Portal for IP Office 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 be 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 can be used with most phones supported by the Avaya IP Office telephone system but not with Phone Manager PC Softphone.


- 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.

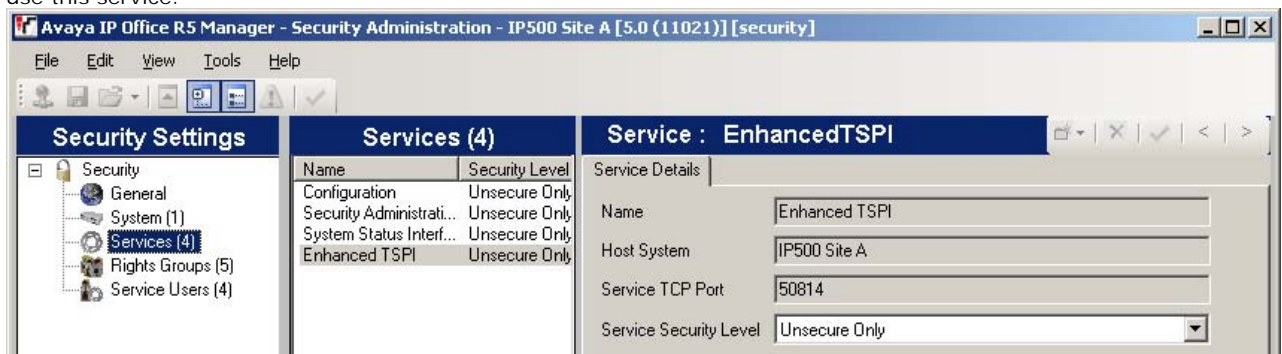
2.2 Check the IP Office Security Settings

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.

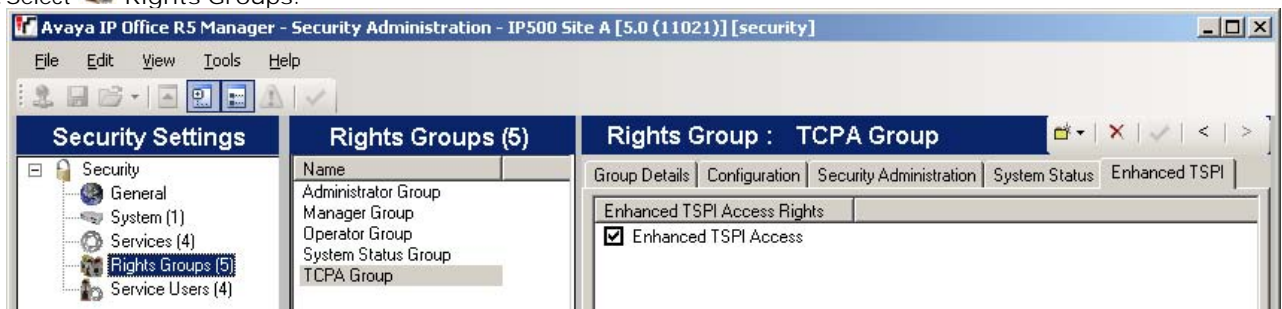
- Important: Perform this Process from the one-X Portal for IP Office Server PC
It is strongly recommended that this and other IP Office configuration actions are performed using IP Office Manager installed on the server PC. That then also tests the network routing between the server PC and the IP Office system. These can be installed from the IP Office Applications DVD.
- 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. If not already done, install IP Office Manager from the IP Office Applications DVD.
2. Start IP Office Manager and select File | Advanced | Security Settings.
3. Select the IP Office system and click OK.
4. Enter the user name and password for access to the IP Office's security settings.


5. 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.

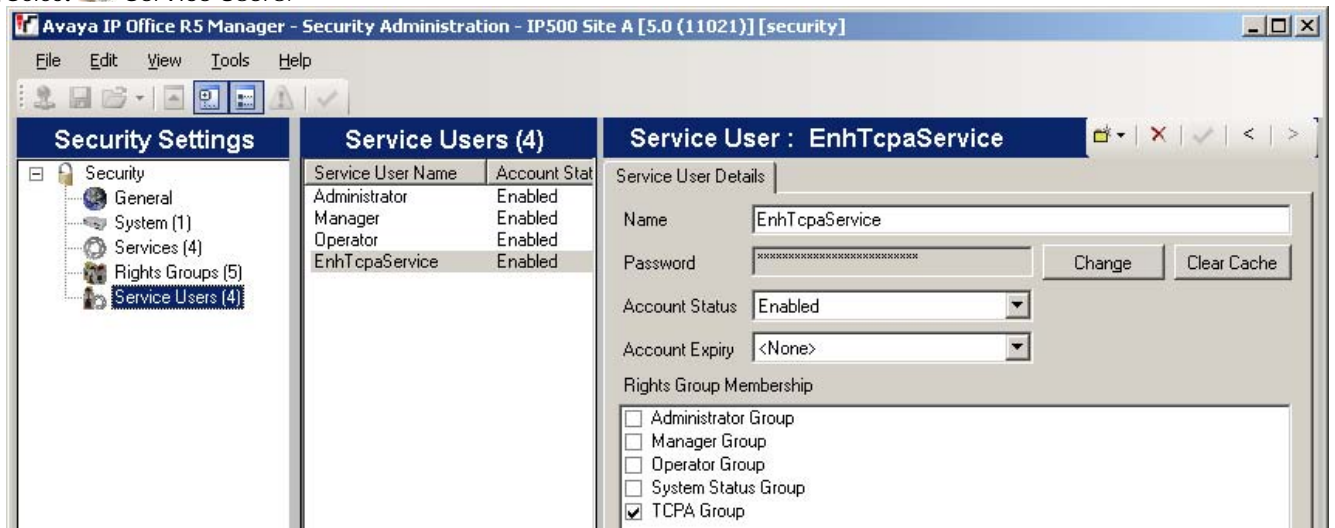


6. Select  Rights Groups.




7. 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.

8. Select  Service Users.



9. 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*.






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

2.3 Add one-X Portal for IP Office Licenses

Each user for one-X Portal for IP Office requires a one-X Portal for IP Office license. It is strongly recommended that the licenses are added to the IP Office configuration and validated before one-X Portal for IP Office is installed.

Each one-X Portal for IP Office 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.



- IP Office Release 6+ Licensing
This release of IP Office uses user profiles licenses. 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.
- For one-X Portal for IP Office 6.0 and higher, a user can refresh their browser without being logged out. All data will be retrieved from the server again 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 to ask whether they wish to logout, if they do not, the browser will be refreshed. With some browsers, for example Firefox, a user can close their browser without logging out and when they reopen te 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 for up to 6 hours.

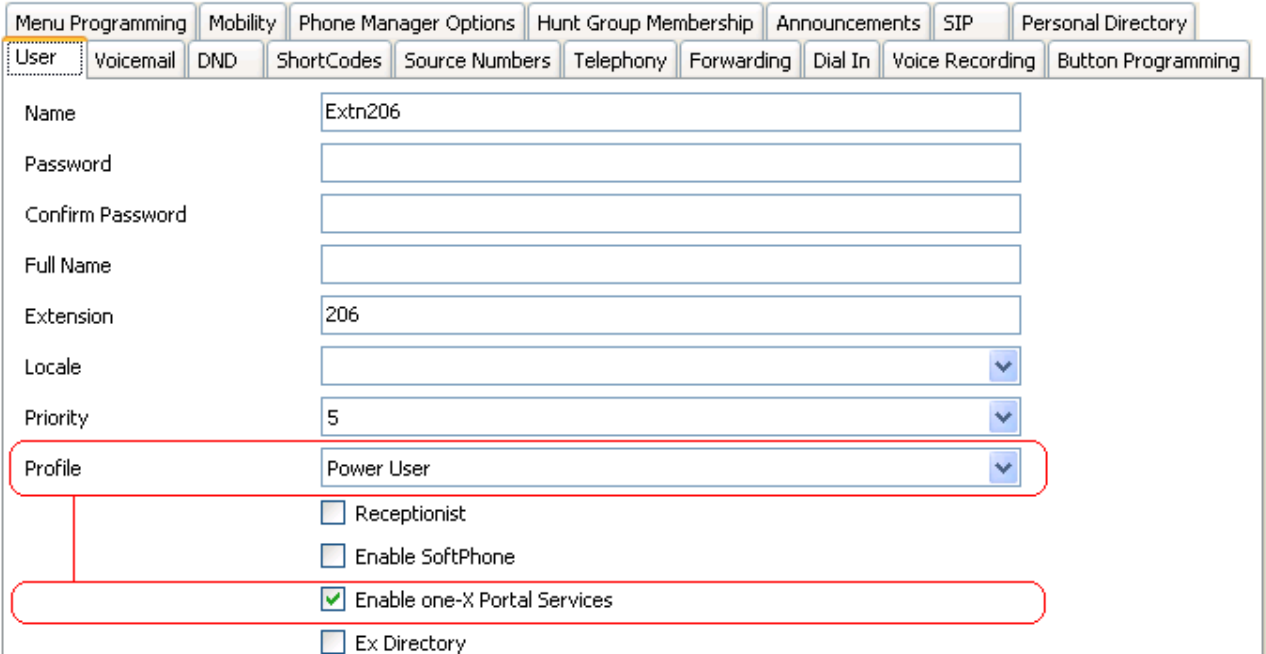
1. Start IP Office Manager and click on the  icon.
2. Select the IP Office and click OK.
3. Enter the user name and password for access to the IP Office's configuration settings.
4. Click on  License.
5. Click on  to enter a new license.
6. Enter the license or licenses provided for one-X Portal for IP Office operation on that system.
7. If the license has been entered correctly, the License Type will show *one-X Portal for IP Office*. 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 for one-X Portal for IP Office


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.

- IP Office Release 6+ Licensing
This release of IP Office uses user profiles licenses. 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.



The screenshot shows the 'User' configuration window in IP Office Manager. The 'User' tab is active. The 'Name' field is 'Extn206', 'Extension' is '206', and 'Profile' is 'Power User'. The 'Enable one-X Portal Services' checkbox is checked. Other options like 'Receptionist', 'Enable SoftPhone', and 'Ex Directory' are unchecked.

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](#)^[82] 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](#)^[53].

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

- Important

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 to 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.

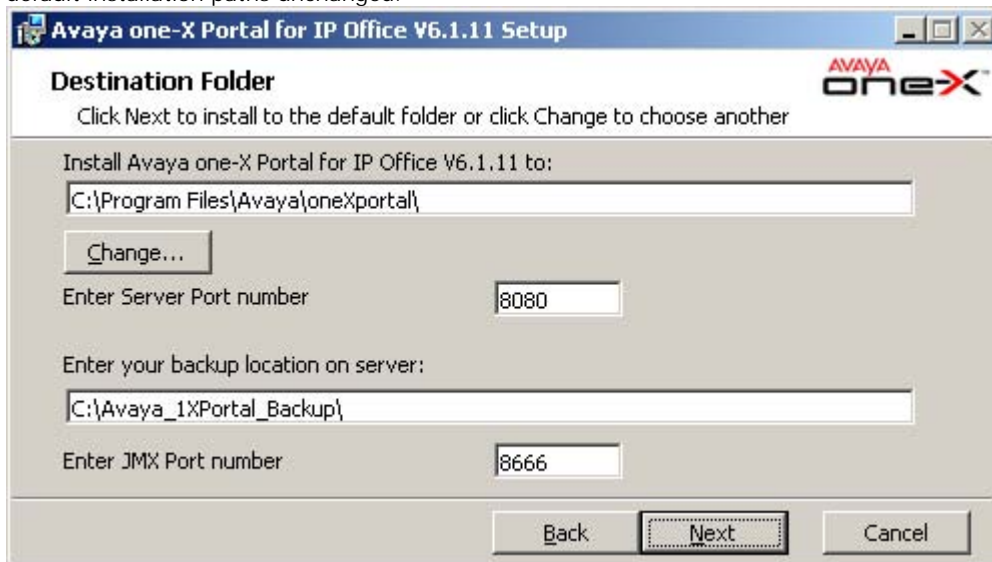
2. On the IP Office Application DVD, locate and double-click on the file one-Xportal.msi file to start the server software installation process.



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

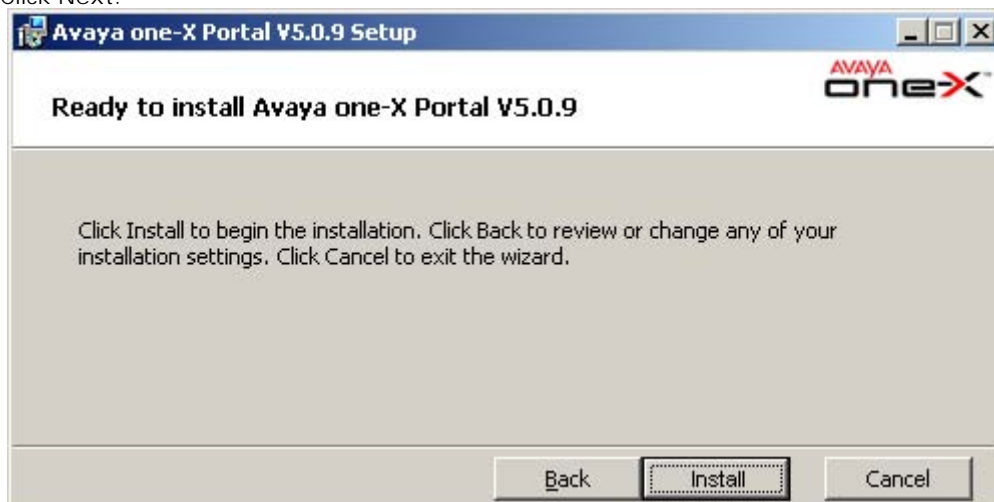


4. Select I install Java and click Next. Unless there is a reason to do otherwise, we recommend that you leave the default installation paths unchanged.

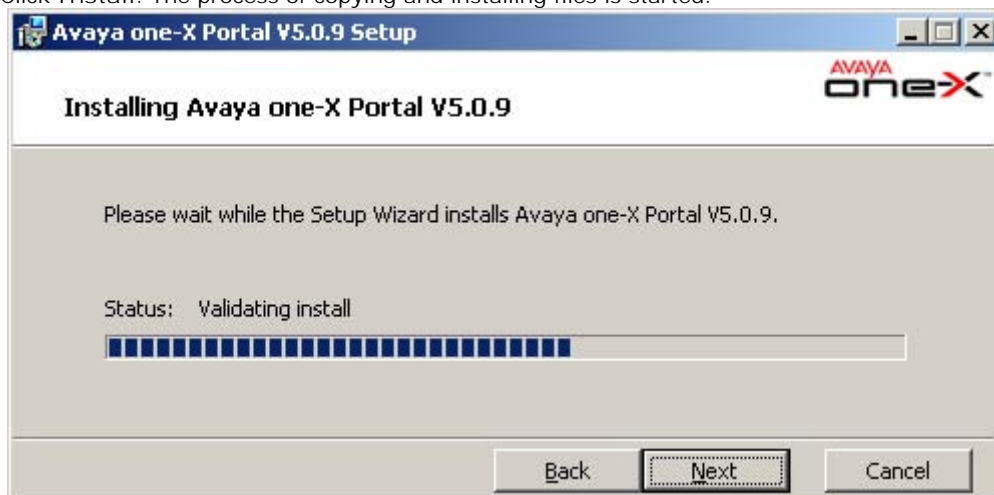


- Enter Server Port number: *Default = 8080*
If the server PC already has services using port 8080 (see [Checking Available Ports](#)^[22]), enter a new unused port number here. Note that once one-X Portal for IP Office is installed, the port number can only be changed by removing and then reinstalling 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](#)^[82] services.

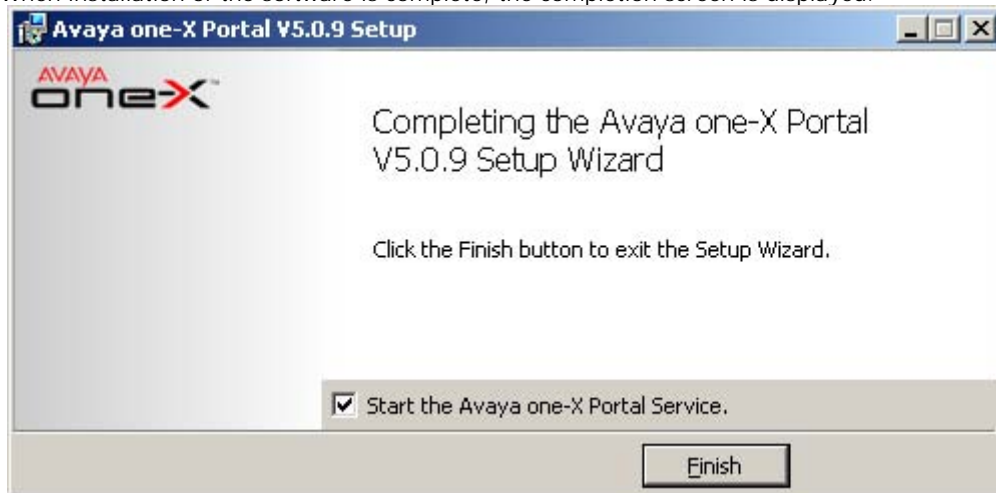
5. Click Next.



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



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



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](#)³⁷ before it can be configured.

9. Click on Finish.

10. Proceed to [Initial Server Configuration](#)²⁸.

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. If you did not select Start the Avaya one-X Portal Service during the software installation, [start the service manually](#)^[37].
2. On the one-X Portal for IP Office server, open a web browser and enter `http://127.0.0.1:8080`. If the software was installed using a different port number, replace the 8080 with that port number.
3. If the service has only just been started, you will have to wait a while whilst the services are started. This can take up to 15 minutes before one-X Portal for IP Office responds. 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. Once it reaches approximately 2.3GB, one-X Portal for IP Office has started.
4. The web server installed by the one-X Portal for IP Office installer should respond with its default web page.



5. 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.



6. The message *System is currently unavailable - please wait* may be displayed with the one-X Portal for IP Office application starts. When the message disappears approximately 15 minutes after the one-X Portal for IP Office service was started, you can login.
7. Check that the version reported matches the version expected. If not refer to the [Troubleshooting](#)^[59] section.
8. Enter the default administrator name (*Administrator*) and password (*Administrator*) and click Login.

9. 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

Next-> **Cancel**

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

11. 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

▶ Status

Check IP Office(s)-> **Configure for IP Office(s)->** **Next->** **Cancel & Restart**

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

12. 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 if 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

▶ Status

Check IP Office(s)-> Configure for IP Office(s)-> Next-> Cancel & Restart

13. 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.

Mid-Layer Telephony (CSTA) Directory (IP-Office) Directory (LDAP) **VoiceMail-Provider**

Provider's Mid-Layer Username izwi_user

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

Provider runs on Port 8080

Assign New Voicemail Server Unit

ID	VoiceMailServer IP Address	
0	EnterValidIPAddress	Delete

14. 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.

Mid-Layer Telephony (CSTA) Directory (IP-Office) **Directory (LDAP)** VoiceMail-Provider

Provider's Mid-Layer Username indoda_user

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

Provider runs on Port 8080

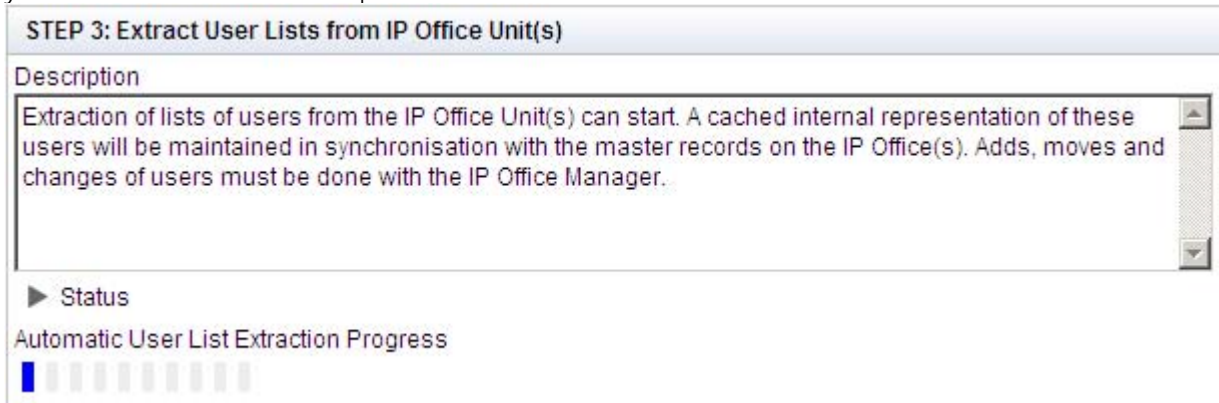
LDAP Server Address ldap://dap-server-ip-addre

LDAP Server Username global\your-username

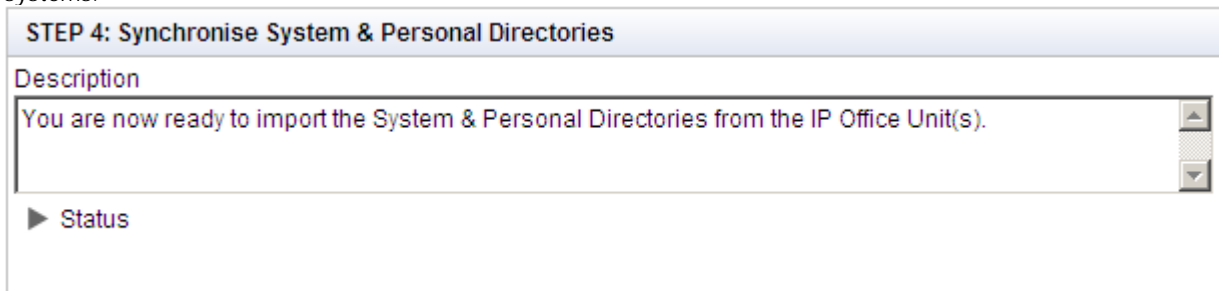
LDAP Server Password ●●●●●●●●

LDAP Server Base DN OU=myregion,OU=mybus

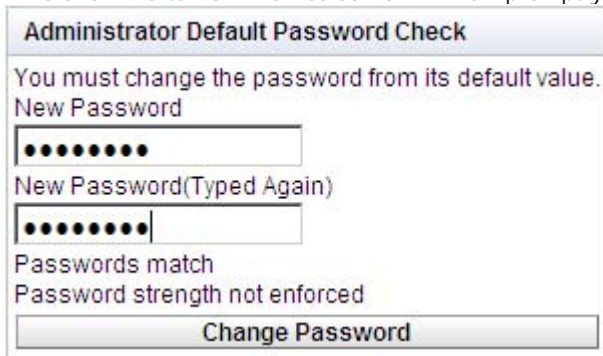
15. Click on Configure for IP Office(s). The one-X Portal for IP Office server will connect with each IP Office and automatically extract details of the IP Office users. If Simple Installation was selected, the installer will go through this and the following steps automatically. If Advanced Installation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



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



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



18. Enter a new password and click Change Password.

19. 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 Connection

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.

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.

2.10 Advanced Configuration Options

The options available through Advanced Installation should not currently be adjusted except for the settings on the Directory (LDAP) tab. That tab can be used to enter the details of the LDAP source to be used.

1. Select Advanced Installation.
2. Click on ► Advanced Provider Options.
3. The advanced options are shown as a set of 4 tabs.

- Mid-Layer

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider
Mid-Layer Host Name	<input type="text" value="localhost"/>			
Mid-Layer Port	<input type="text" value="8080"/>			
Mid-Layer Service Name	<input type="text" value="inkaba"/>			

- Telephony (CSTA)

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

- Directory (IP-Office)

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider
Provider's Mid-Layer Username	<input type="text" value="indoda_user"/>			
Provider's Mid-Layer Password	<input type="password" value="●●●●●●●●"/>			
Provider runs on Port	<input type="text" value="8080"/>			
Timeout	<input type="text" value="300"/>			

- Directory (LDAP)

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider
Provider's Mid-Layer Username	<input type="text" value="indoda_user"/>			
Provider's Mid-Layer Password	<input type="password" value="●●●●●●●●"/>			
Provider runs on Port	<input type="text" value="8080"/>			
LDAP Server Address	<input type="text" value="ldap://ldap-server-ip-addre"/>			
LDAP Server Username	<input type="text" value="global/your-username"/>			
LDAP Server Password	<input type="password" value="●●●●●●●●"/>			
LDAP Server Base DN	<input type="text" value="OU=myregion,OU=mybus"/>			

- Voicemail Provider

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider
-----------	------------------	-----------------------	------------------	---------------------------

Provider's Mid-Layer Username

Provider's Mid-Layer Password

Provider runs on Port

Assign New Voicemail Server Unit

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

4. Complete the details as required. Then continue as per normal [initial server configuration](#) ²⁸.

Chapter 3.

Maintenance

3. Maintenance

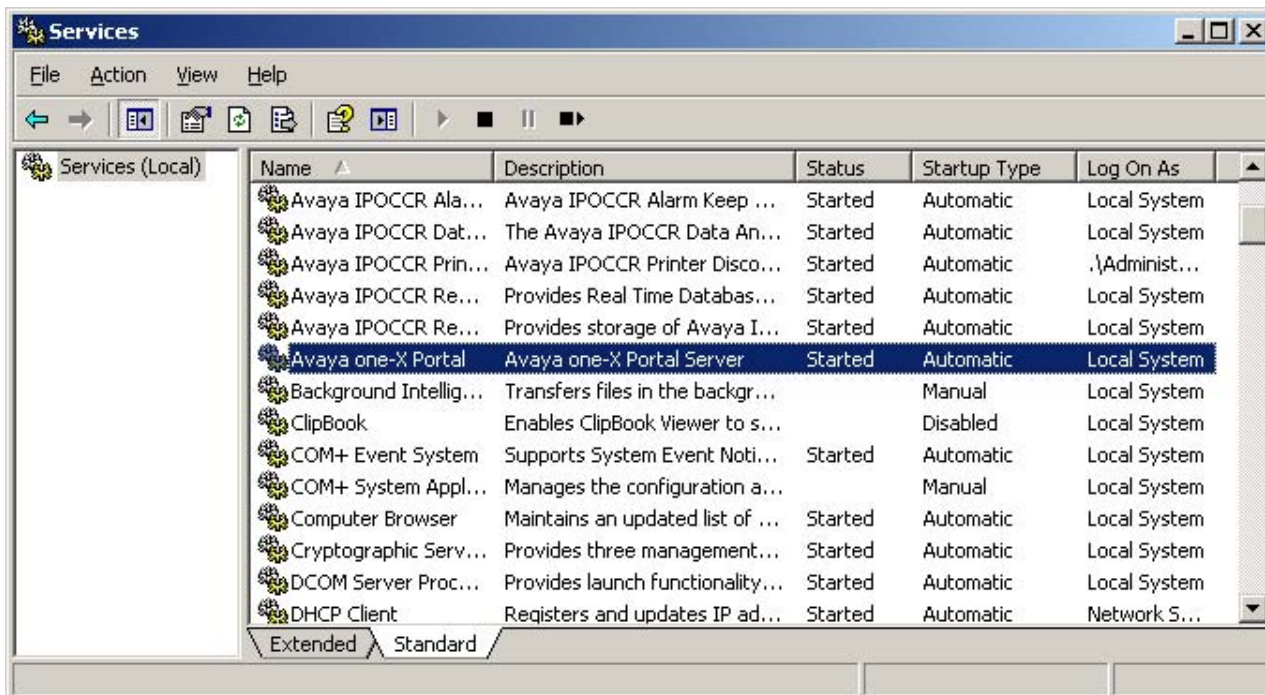
This section covers various post installation activities that may need to be performed.

- [Manually Starting the Service](#) ^[37]
- [Adding an Additional IP Office](#) ^[38]
- [Changing an IP Office Details](#) ^[41]
- [Adding/Deleting Users](#) ^[44]
- [Editing User Settings](#) ^[44]
- [Adding an LDAP Directory Source](#) ^[43]
- [Checking the External LDAP Directory](#) ^[50]
- [Backing Up the Database](#) ^[47]
- [Restoring a Previous Backup](#) ^[48]
- [Checking and Updating the System Directory](#) ^[49]
- [Upgrading one-X Portal for IP Office](#) ^[51]
- [Downgrading one-X Portal for IP Office](#) ^[52]
- [Removing one-X Portal for IP Office](#) ^[53]
- [Remote Logging](#) ^[55]
- [Agent Gadget Control](#) ^[60]

one-X Portal for IP Office 6.1 and higher supports an additional set of [backup and restore](#) ^[82] options.

3.1 Manually Starting the Service

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



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

- No Service !

If the service is not present, the most likely cause is a port conflict or Java problem. Refer to [Troubleshooting](#) ⁵⁹.

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.

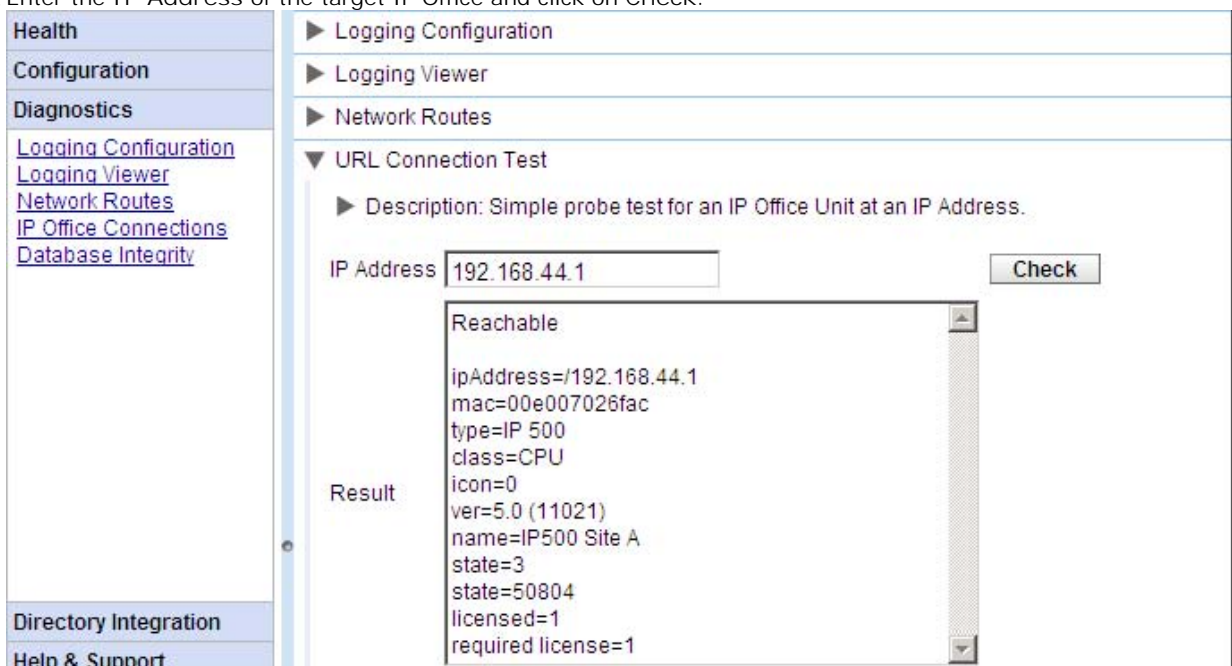
1. Before adding another IP Office to the one-X Portal for IP Office configuration:

- Check that the IP Office has been configured with the [security settings](#) for one-X Portal for IP Office operation.
- Check that the IP Office is [licensed](#) for one-X Portal for IP Office.
- Check that at least one user on the IP Office has been [enabled for one-X Portal for IP Office](#).

2. [Log in](#) to the administrator menus.

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

- a. Select Diagnostics and then IP Office Connections.
- b. Enter the IP Address of the target IP Office and click on Check.



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

4. Select Configuration and then Providers.

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

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

7. Click on IP Office(s) Assigned.

8. Click on Assign New IP Office Unit.

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			<input type="button" value="Delete"/>
1	192.168.44.1	EnhTcpaService	●●●●●●●●	<input type="button" value="Delete"/>

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

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

11. Click Close.

12. Click Close again.

13. Click 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](#) ³⁷.

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

17. Select Health and then Component Status.

18. Click on Get All. New CSTA and DSML components for the IP address of the newly added IP Office should be included. The status of these should be available.

Health

- [Component Status](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

▼ Component Status

► Description: Health of key one-X Portal components

Status: All records have been fetched.

ID	Component Name	Status	Reported At	Additional Info.	
<input type="checkbox"/> 5	CSTA-Provider-1-192.168.42.1	Available	2009-05-20 09:12:34.968	component reportin	<input type="button" value="Delete"/>
<input type="checkbox"/> 33	CSTA-Provider-1-192.168.44.1	Available	2009-05-20 09:10:53.656	component reportin	<input type="button" value="Delete"/>
<input type="checkbox"/> 4	CSTA-Provider-1-Master	Available	2009-05-20 09:12:35.156	... master is up	<input type="button" value="Delete"/>
<input type="checkbox"/> 3	DSML-Provider-1-192.168.42.1	Available	2009-05-20 09:13:40.234	Personal resynchron	<input type="button" value="Delete"/>

Page << 1 2 >>

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](#) 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.

The screenshot shows the 'Providers' configuration page in the one-X Portal. The left-hand navigation menu has 'Providers' selected under the 'Configuration' section. The main content area is titled 'Global Configuration' and 'Providers'. Below the title is a description: 'Description: Configure providers of services to applications'. There are four buttons: 'Create', 'Get All', 'Put Selected', and 'Delete Selected'. The 'Get All' button is highlighted. Below the buttons is a status bar that says 'Status: All records have been fetched.' Below the status bar is a table with columns for 'ID', 'Name', and 'Page'. The table contains four rows of provider records, each with an 'Edit' and 'Delete' button.

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

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

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

Mid-Layer Username: indoda_user

Mid-Layer Password: [REDACTED]

Mid-Layer Password Hash: 7BDDEE71046BA3FA276

Run On Port: 8080

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

Close

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

IP Office(s) assigned to Provider

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

ID	IP Address	User	Password	
0	192.168.42.1			Delete

Close Assign New IP Office Unit

7. Click Close.

8. Click Close again.

9. Click 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](#) ^[79] option in the administrator menus.

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

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

1. Login to the administrator menus.
2. Select Configuration and then Providers.
3. Click on Get All to retrieve the current provider records from the one-X Portal for IP Office database.
4. Click on the Edit button next to the LDAP provider.
5. Click on LDAP Server(s) Assigned. This will list the LDAP source already assigned.

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

- LDAP Server URL
The URL of the LDAP directory source, for example *ldap://ldap.example.com*.
- User/Password
The user name and password for access to the LDAP server.
- Base DN
This is also called the Search Base. It defines which set of records in the LDAP source should be used for searches. The LDAP sever administrator will provide a suitable string, for example *ou=Users,dc=global,dc=example,dc=com*.

7. Click on Edit Field Mapping. The field names (on the left) are the fields shown in the one-X Portal for IP Office directory. Enter the names of the matching field for each in the LDAP sources records.

8. Click Close.
9. Select the check box next to the new entry and click on Put Selected.
10. [Restart the Avaya one-X Portal service](#) ^[37].

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	✓	✓	<p>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.</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> IP500/IP500v2: 10800 total personal directory records. For users with a 1608, 1616, 9400, 9500 or 9600 phones, they can edit or delete contacts through the phone's menus (primary phone number only).
Call Log	-	✓	A user's call log is stored in the configuration of their IP Office.
Voicemail Messages	-	✓	Details of the user's voicemail messages are taken from the voicemail server via the IP Office.
Profiles	✓	-	A user's profiles are stored by the one-X Portal for IP Office server. When a profile is made active it 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:

Name:

Unique Identifier:

Display Name:

Password:

Password Hash:

User Configuration Type Selector:

My Status:

User Configuration Type Specific Editor:

Name	Type	Number
+ Add a new presence definition		

[Do Not Disturb Exceptions](#)

Created:

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

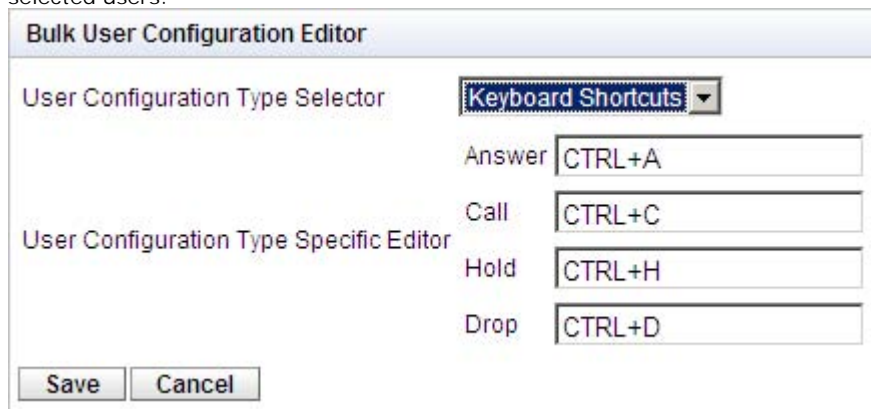
Bulk Editing

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



The dialog box is titled "Bulk User Configuration Editor". It contains two dropdown menus. The first is labeled "User Configuration Type Selector" and has "Select" chosen. The second is labeled "User Configuration Type Specific Editor" and has "Some User Configuration" chosen. At the bottom are "Save" and "Cancel" buttons.

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



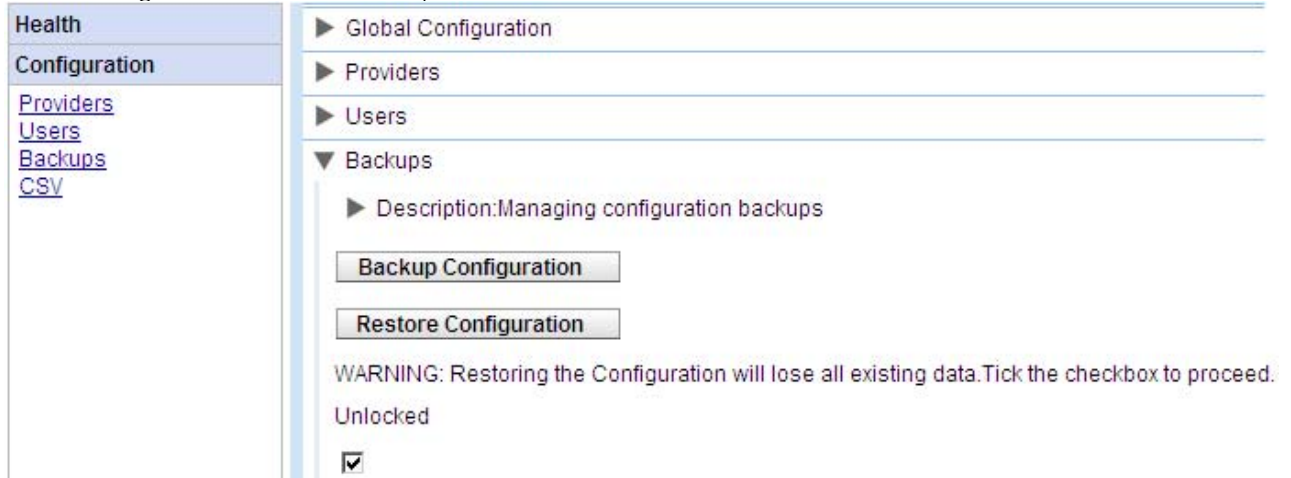
The dialog box is titled "Bulk User Configuration Editor". The "User Configuration Type Selector" dropdown is now set to "Keyboard Shortcuts". Underneath, the "User Configuration Type Specific Editor" section has four sub-sections: "Answer" with "CTRL+A", "Call" with "CTRL+C", "Hold" with "CTRL+H", and "Drop" with "CTRL+D". "Save" and "Cancel" buttons are at the bottom.

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](#)⁴⁸ if necessary.

1. Select Configuration and then Backups.

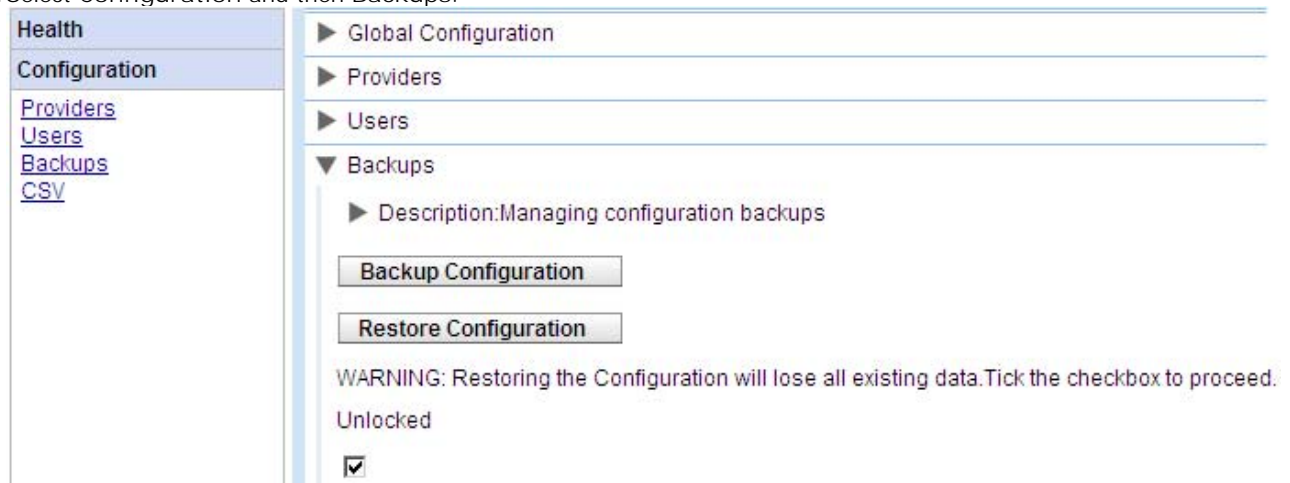


2. Click on Backup Configuration.
3. The configuration is backed up as *backup.sql* in the bin folder of the one-X Portal for IP Office application (default C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\bin\backup.sql).

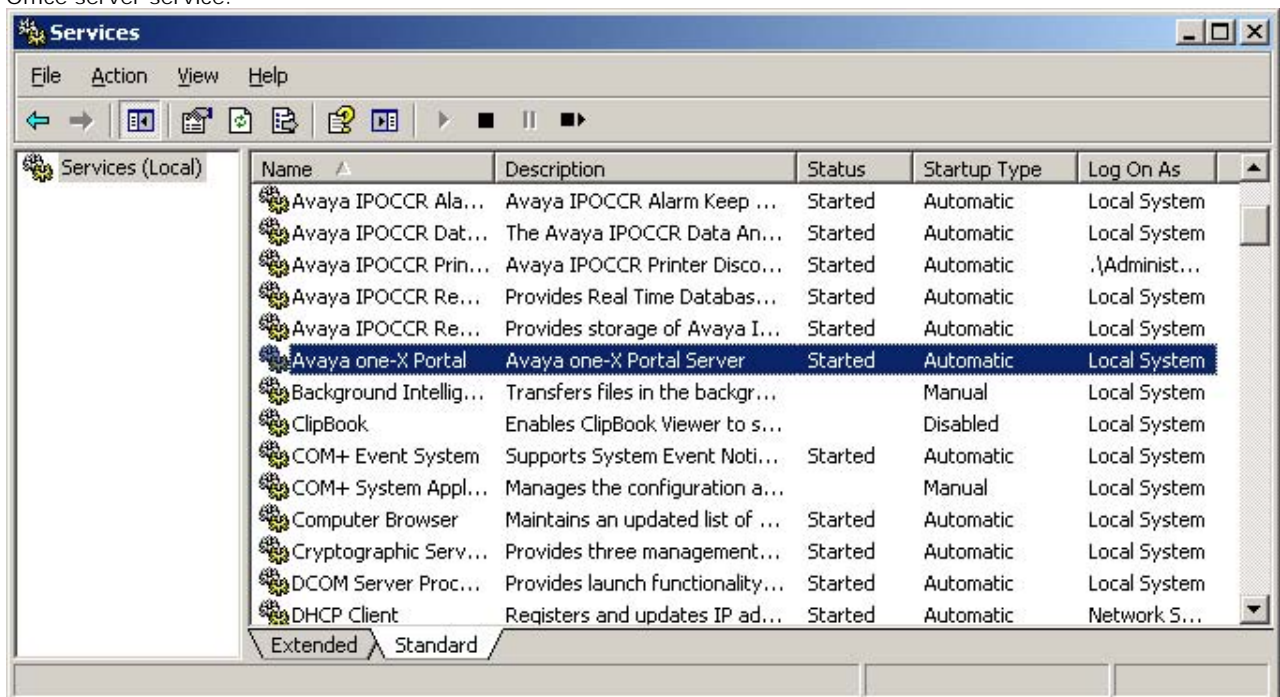
3.8 Restoring a Previous Backup

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\apache-tomcat-6.0.18\bin\backup.sql) for restoration.

1. Select Configuration and then Backups.



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



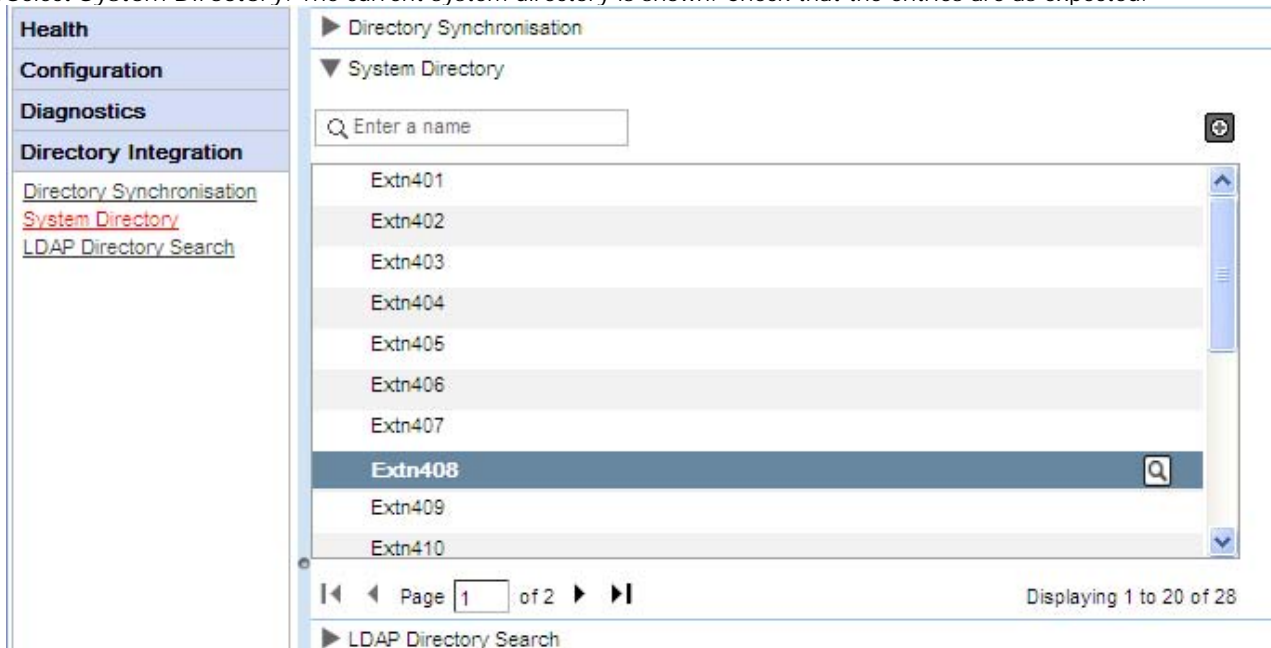
3.9 Checking and Updating the System Directory

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.

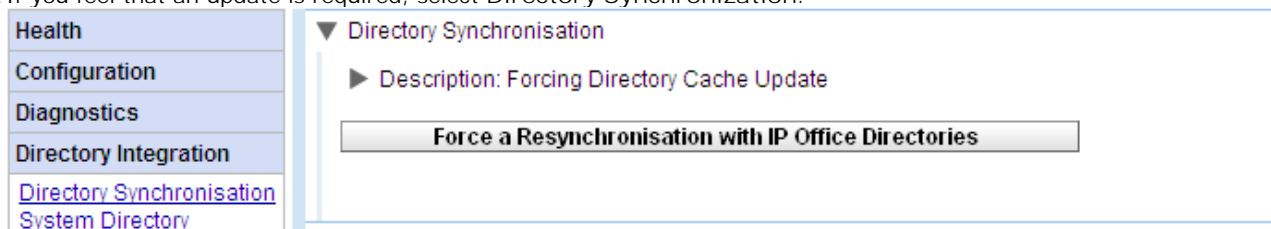
By default, the one-X Portal for IP Office application updates the system directory records every 300 seconds approximately. Through the one-X Portal for IP Office administrator menus you can view the system directory and, if necessary, force an update.

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.

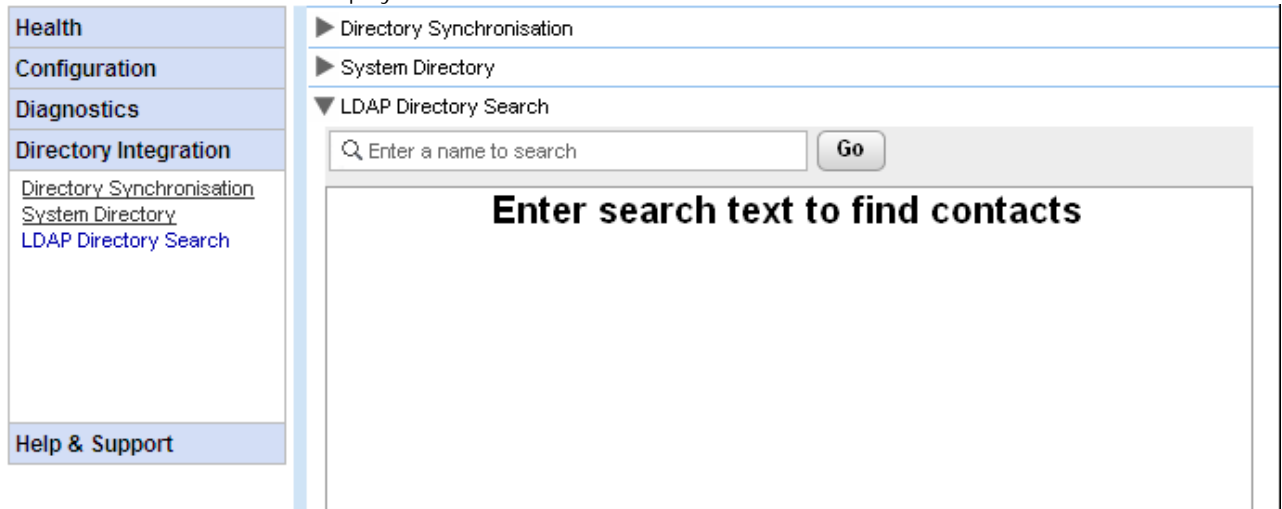


4. Click on Force a Resynchronization to all IP Office Directories.

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.

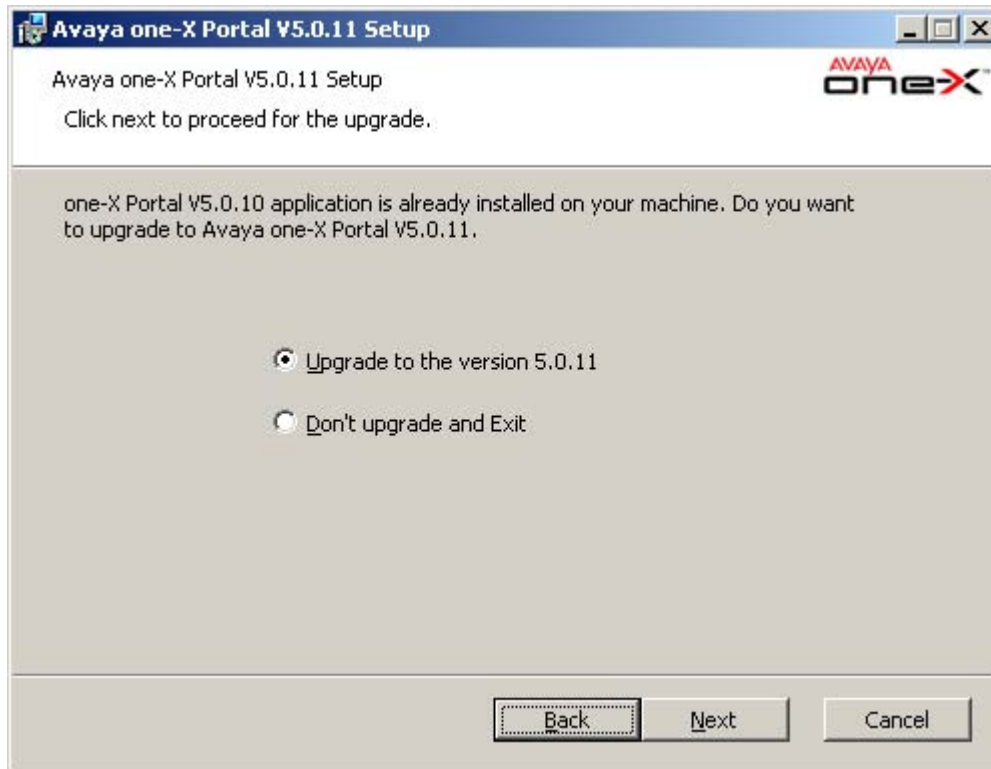


3.11 Upgrading one-X Portal for IP Office

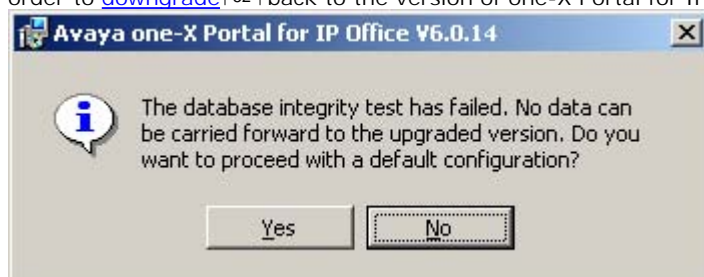
Before upgrading one-X Portal for IP Office ensure that you have read the Avaya IP Office Technical Bulletin for the release of one-X Portal for IP Office software to which you want to install or the IP Office software release in which it was included. The Technical Bulletin will include details of any 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.



- 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](#)^[52] back to the version of one-X Portal for IP Office that is compatible with the database.



During the upgrade process a backup file is created (backup.sql). This is not a full backup of the one-X Portal for IP Office system and should not be used for restoration of setting. Refer to [Backing Up the Database](#)^[47] 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](#)^[54], 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.

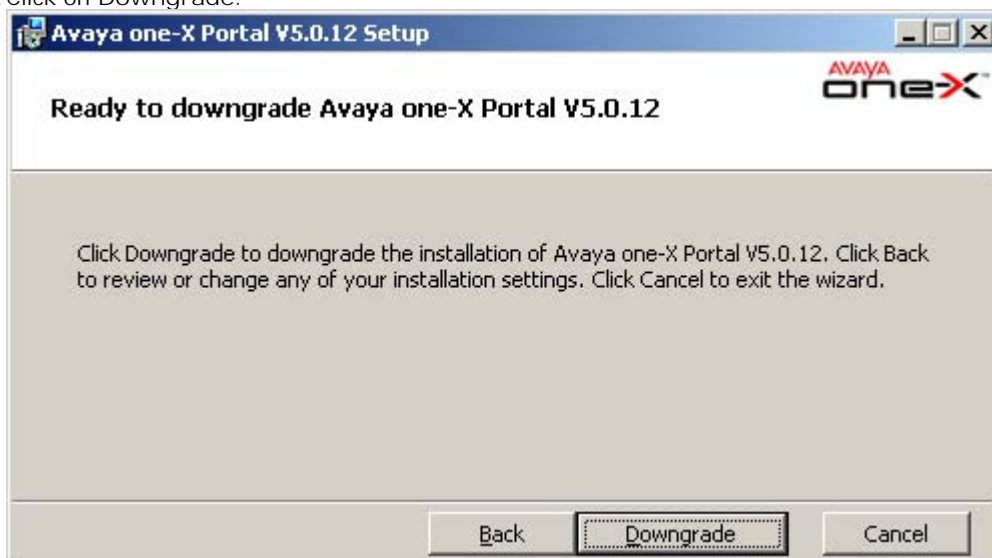
Before downgrading one-X Portal for IP Office ensure that you have read the Avaya IP Office Technical Bulletin for the one-X Portal for IP Office software releases. The Technical Bulletin will include details of any special requirements and additional steps that may not be in this documentation.

- 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.



2. Click on Downgrade.



3. When the downgrade has been completed, the Avaya one-X Portal needs to be [restarted manually](#)^[37].

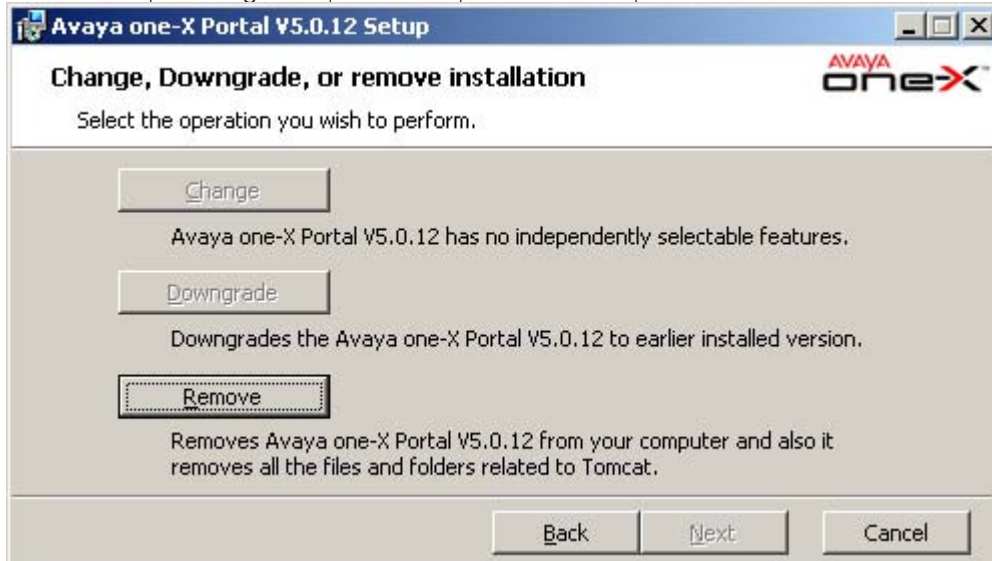
3.13 Removing one-X Portal for IP Office

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

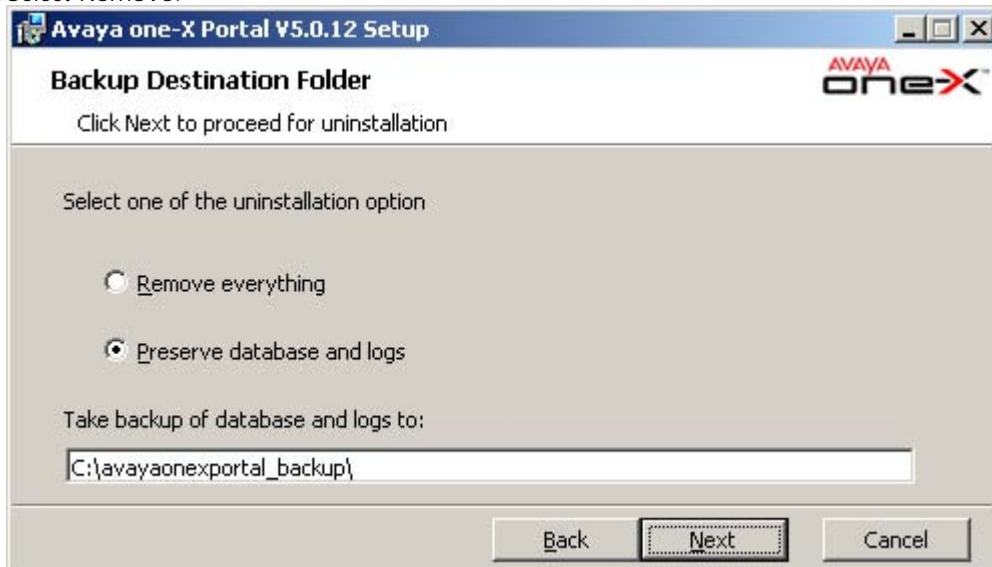
Uninstalling one-X Portal for IP Office

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

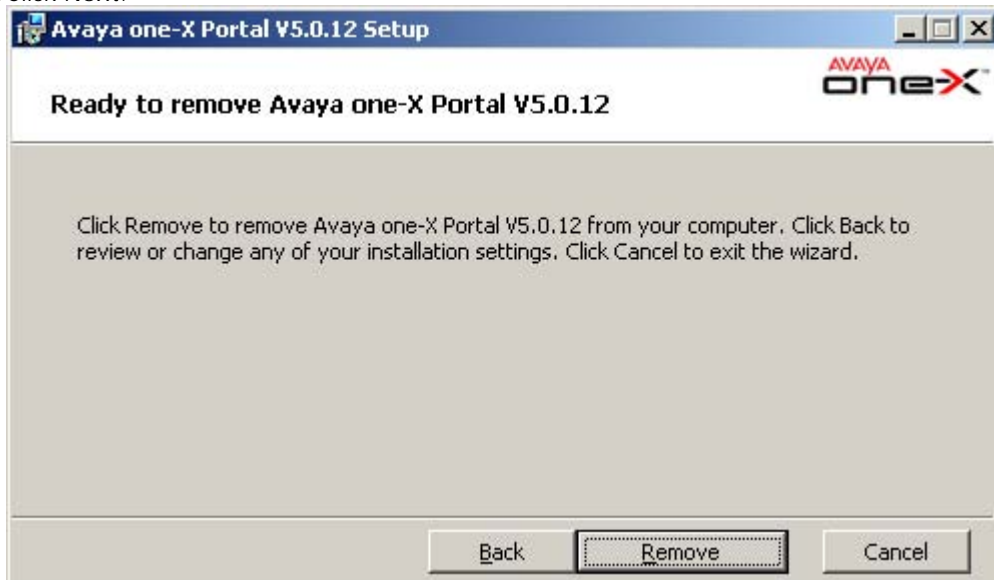
1. Select Start | All Programs | IP Office | one-X Portal | Uninstall one-X Portal.



2. Select Remove.



3. Click Next.



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

Removing one-X Portal for IP Office via the Control Panel

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

1. Start the standard Windows Control Panel.

2. Select Add or Remove Programs.

3. Select one-X Portal and then click Remove.

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

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.

The screenshot shows the Apache Chainsaw configuration interface. On the left is a navigation menu with categories: Health, Configuration, Diagnostics, Directory Integration, and Help & Support. Under Diagnostics, there are links for Logging Configuration, Logging Viewer, Network Routes, IP Office Connections, and Database Integrity. The main content area is titled 'Logging Configuration' and contains several sections:

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

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


- Logging Targets(Server and Network):** A checkbox for 'Socket Receiver(required for remote log viewing)' is checked and labeled 'Enabled'.

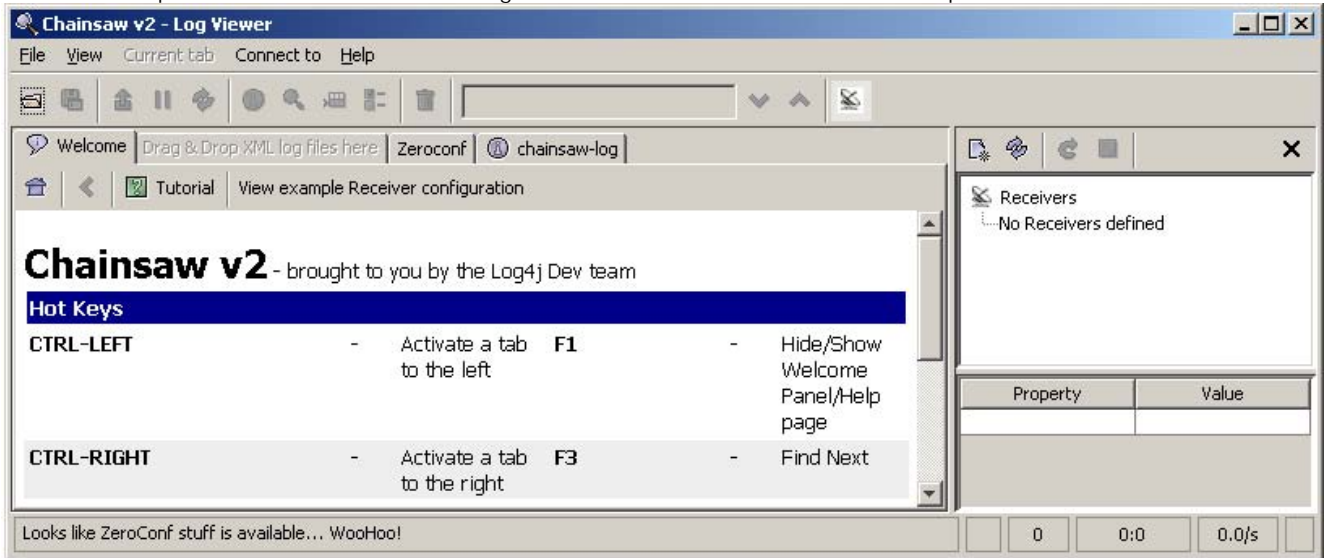
2. Check that Socket Receiver is enabled.
3. Select Logging Viewer.

The screenshot shows the Apache Chainsaw configuration interface with the 'Logging Viewer' section selected. The navigation menu on the left is the same as in the previous screenshot, but 'Logging Viewer' is now highlighted. The main content area shows:

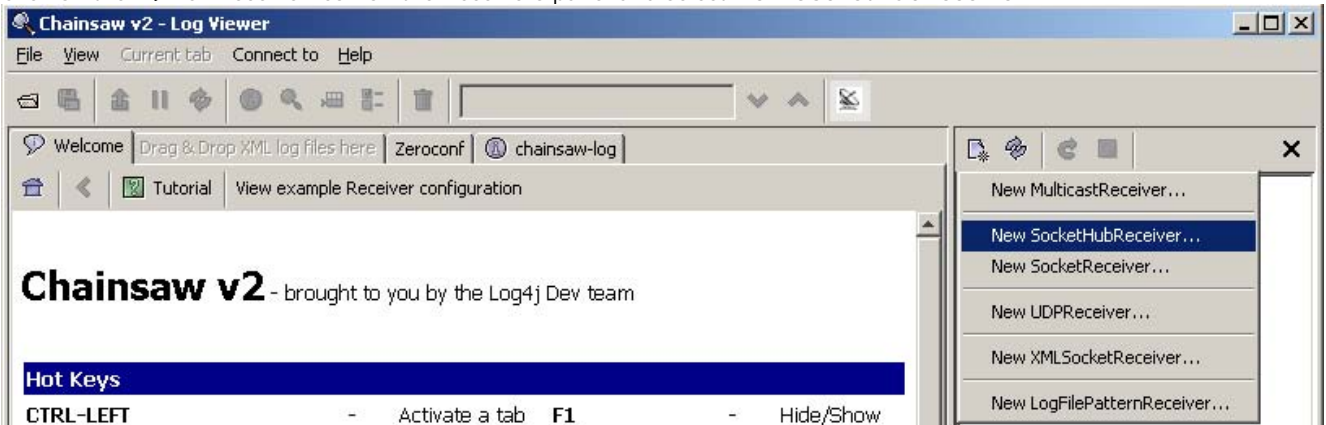
- Logging Configuration:** A collapsed section.
- Logging Viewer:** A section with a description: 'Remotely viewing logs.' Below the description are two links: 'More information about Apache Chainsaw' and 'Start Installation of Apache Chainsaw by Java Web Start'.
- Network Routes:** A collapsed section.

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

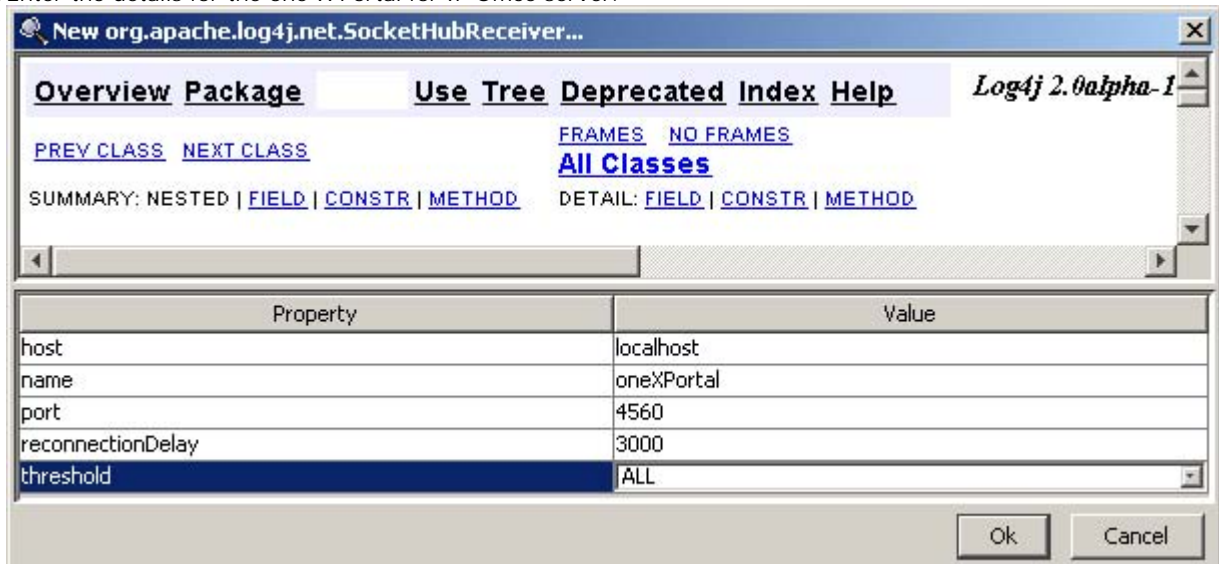
6. The Receivers panel should be visible on the right. If not click on the  button in the top toolbar.



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

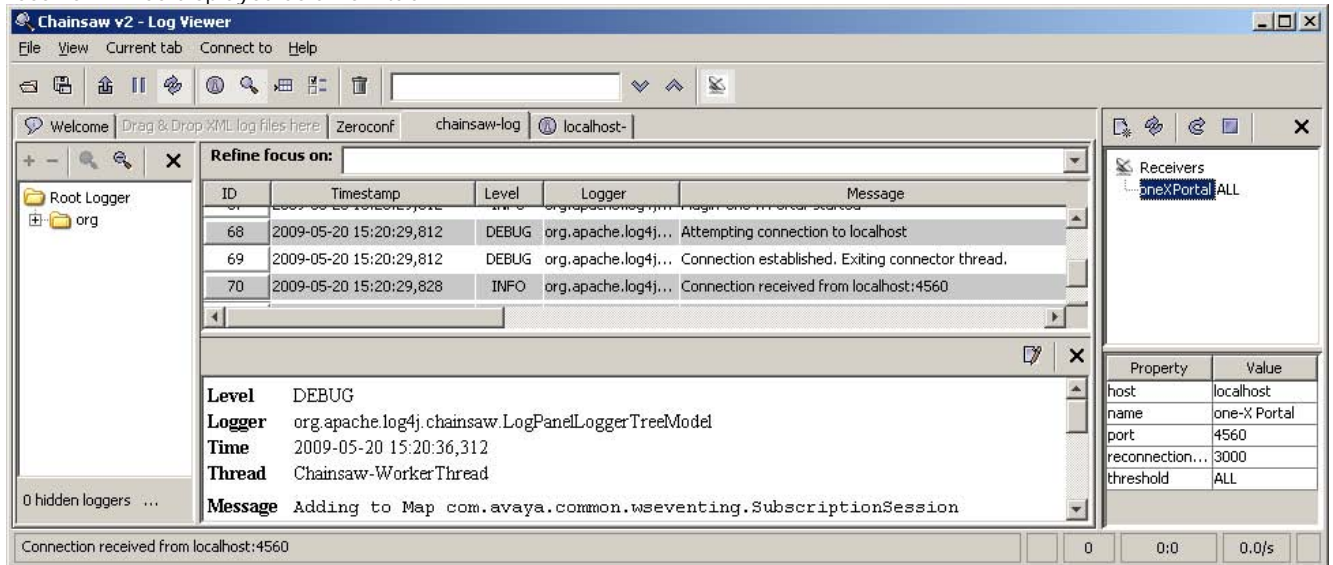


8. Enter the details for the one-X Portal for IP Office server.

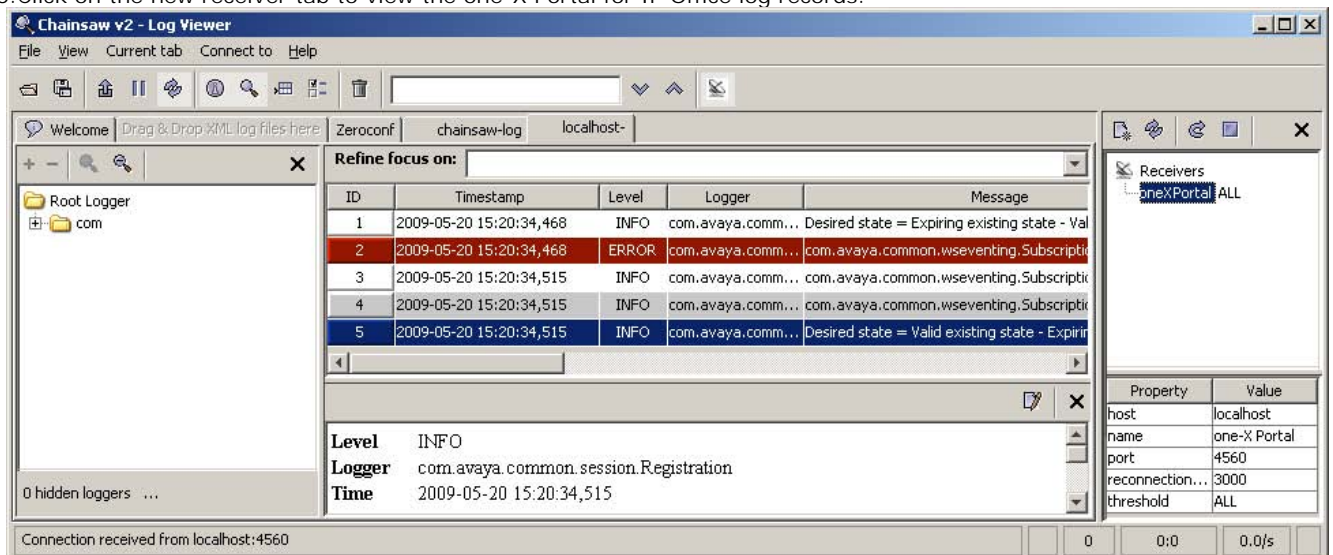


host	This field sets the address of the one-X Portal for IP Office server. In the example above chainsaw is being run on the one-X Portal for IP Office server PC.
name	This field is for display only. Enter a name for the receiver entry in Chainsaw.
port	Set this to 4560. This is the port to which one-X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

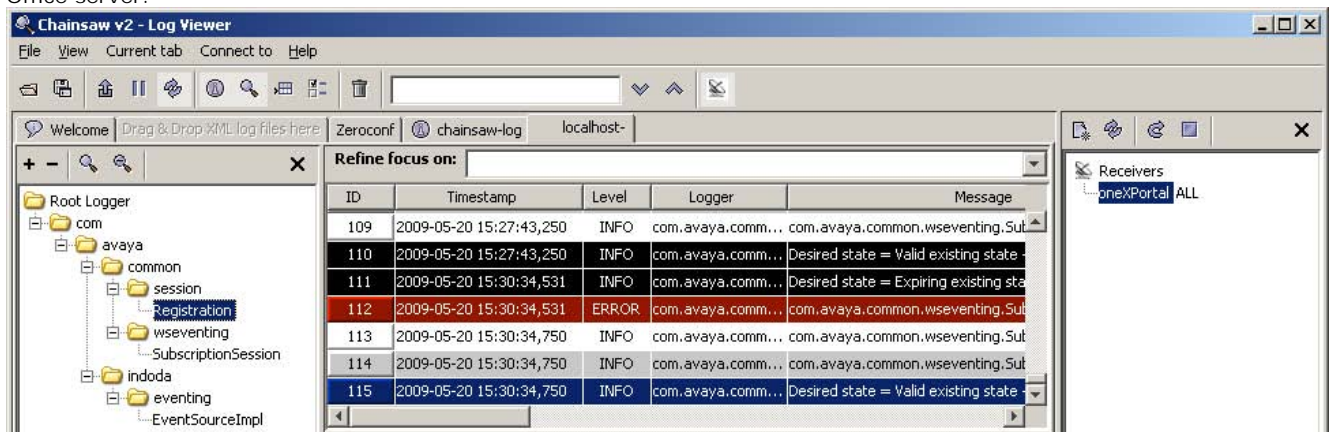
9. When you have completed the fields, click OK. After a few seconds the receiver should start and connect to the one-X Portal for IP Office server. The process will appear as log events on the chainsaw-log tab and when completed the receiver will be displayed as a new tab.





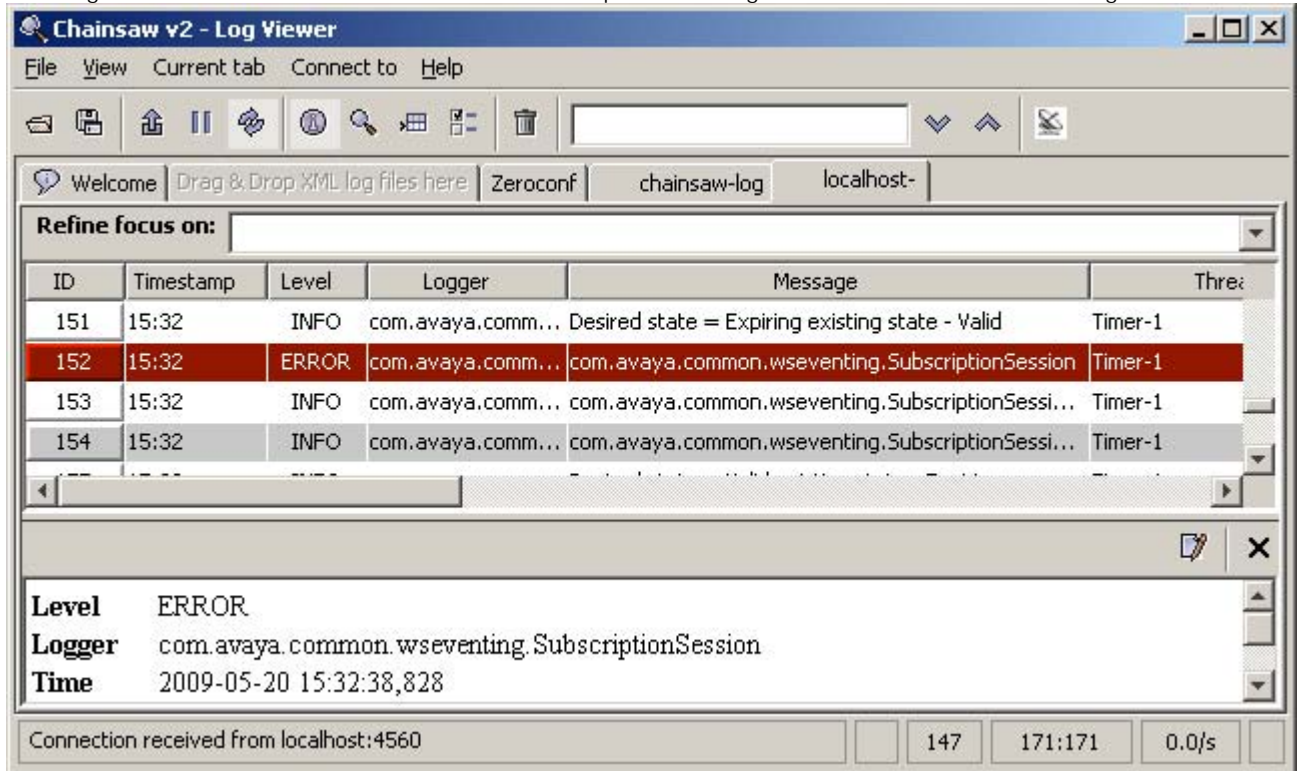
10. Click on the new receiver tab to view the one-X Portal for IP Office log records.



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



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



The screenshot shows the Chainsaw v2 - Log Viewer application window. The title bar reads "Chainsaw v2 - Log Viewer". The menu bar includes "File", "View", "Current tab", "Connect to", and "Help". The toolbar contains various icons for file operations and navigation. The main area displays a log table with the following data:

ID	Timestamp	Level	Logger	Message	Thread
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

Below the table, a detailed view of the selected error entry is shown:

```

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

At the bottom of the window, a status bar displays "Connection received from localhost:4560" and several numerical indicators: 147, 171:171, and 0.0/s.

3.15 Troubleshooting

Version Mismatch Problem

Symptoms	<ul style="list-style-type: none"> • Database integrity ^[76] check fails. • When starting one-X Portal for IP Office, the version shown on the login page is the previous version and differs from that reported by Windows (Start Programs IP Office Avaya one-X Portal for IP Office Uninstall 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 in some cases it fails to stop the Tomcat server but will still report successful completion of the installation process. This leads to a version mismatch between components.
Resolution	<ol style="list-style-type: none"> 1. Remove one-X Portal for IP Office ^[53]. 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	<ul style="list-style-type: none"> • one-X Portal for IP Office fails to start. • Prorun Error appears in the Tomcat server log files. • Other Java applications fail to run on the server (for example the IP Office System Status Application).
Resolution	<ol style="list-style-type: none"> 1. Check for a port conflict ^[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 ^[53]. 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 ⁶⁴	Component Status ⁶⁴	List the last status change of the server components.
	Key Recent Events ⁶⁴	View the last 20 events on the server.
	Active Sessions ⁶⁵	Show how many sessions are cached by one-X Portal for IP Office.
	Environment ⁶⁵	Show a summary of the one-X Portal for IP Office server PC.
Configuration ⁶⁶	Providers ⁶⁶	View and edit the providers.
	Users ⁷⁰	View and edit user one-X Portal for IP Office settings.
	Backups ⁷²	Backup the one-X Portal for IP Office configuration database. Also restore a previous backup.
	CSV ⁷²	Export the user directory and system directory.
Diagnostics	Logging Configuration ⁷⁴	Configure the level and method of logging supported.
	Logging Viewer ⁷⁵	Install and launch Chainsaw for log viewing.
	Network Routes ⁷⁵	Test the IP connection path to an IP address.
	IP Office Connections ⁷⁶	Test the IP connection path to an IP Office.
	Database Integrity ⁷⁶	Test the structure of the database.
Directory Integration ⁷⁷	Directory Synchronization ⁷⁷	Force a system directory update by the server.
	System Directory ⁷⁸	View the one-X Portal for IP Office system directory.
	LDAP Directory Search ⁷⁹	View the external directory for which the one-X Portal for IP Office server has been configured.
Help & Support ⁸⁰	Help ⁸⁰	Access one-X Portal for IP Office help installed on the server.
	Avaya Support ⁸⁰	Access the Avaya support web site for Avaya applications.
	About ⁸⁰	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.

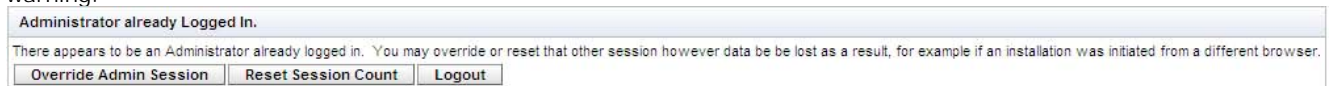
4.1 Login

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.



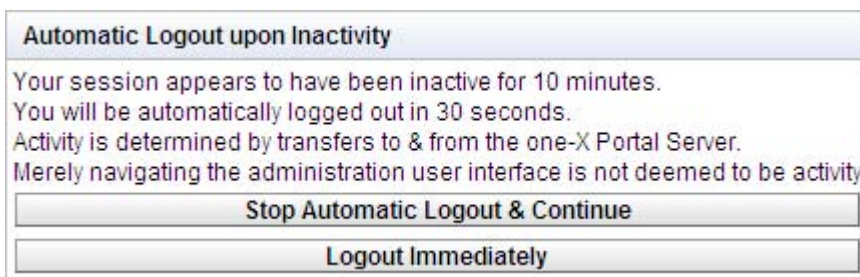
3. Enter the one-X Portal for IP Office administrator name and password as configured during installation.
4. If there is already a session connected as an administrator, the one-X Portal for IP Office server will display a warning.



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.



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.

Health

- [Component Status](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

Component Status

Description: Health of key one-X Portal components

Create Get All Put Selected Delete Selected

Status: All records have been fetched.

ID	Component Name	Status	Reported At	Additional Info.	Page 1 2
<input type="checkbox"/> 4	CSTA-Provider-1-192.168.42.1	Available	2009-05-11 04:48:19.546	component reportin	Delete
<input type="checkbox"/> 3	CSTA-Provider-1-Master	Starting	2009-05-11 09:14:58.25	...no component pr	Delete
<input type="checkbox"/> 2	DSML-Provider-1-192.168.42.1	Failed	2009-05-08 16:15:02.468	Initial provisioning fa	Delete
<input type="checkbox"/> 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.

Health

- [Component Status](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

Component Status

Key Recent Events

Description:

Create Get All Put Selected Delete Selected

Status: All records have been fetched.

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

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

Total	User	Administrator	Application
3	0	1	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.

The screenshot shows the 'Health' menu on the left with 'Environment' selected. The main content area displays 'Component Status', 'Key Recent Events', 'Active Sessions', and 'Environment'. Under 'Environment', there is a description 'Description: Server Information' and a 'Refresh' button. Below the button is a table with the following data:

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

The screenshot shows the 'Providers' configuration page. On the left is a navigation menu with 'Health' and 'Configuration' sections. Under 'Configuration', there are links for 'Providers', 'Users', 'Backups', and 'CSV'. The main content area is titled 'Global Configuration' and 'Providers'. It includes a description: 'Configure providers of services to applications'. Below the description are buttons for 'Create', 'Get All', 'Put Selected', and 'Delete Selected'. A status bar indicates 'All records have been fetched.' Below this is a table of providers with columns for 'ID', 'Name', and actions 'Edit' and 'Delete'. The table is paginated to show page 1 of 1.

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

4.4.1.2 DSML (IP Office) Provider

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

Provider Editor

ID:

Name:

URL:

Data:

Provider Type Selector: ▼

IP Office(s) Assigned

Mid-Layer URL:

Mid-Layer Username:

DSML(IPO) Config Editor Mid-Layer Password:

Mid-Layer Password Hash:

Run On Port:

Created:

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

IP Office(s) assigned to Provider

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

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

The User and Password details used must match the TCPA service user configured in the IP Office system's [security configuration settings](#)^[18].

4.4.1.3 DSML (LDAP) Provider

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

Provider Editor

ID:

Name:

URL:

Provider Type Selector:

LDAP Server(s) Assigned

Mid-Layer URL:

Mid-Layer Username:

DSML(LDAP) Config Editor Mid-Layer Password:

Mid-Layer Password Hash:

Run On Port:

Created:

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

LDAP Server(s) assigned to Provider

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

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

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	<input type="text" value="givenName"/>
LASTNAME	<input type="text" value="sn"/>
WORKPHONE	<input type="text" value="telephoneNumber"/>
HOMEPHONE	<input type="text" value="homePhone"/>
OTHERPHONE	<input type="text" value="cel"/>
WORKEMAIL	<input type="text" value="mail"/>
PERSONALEMAIL	<input type="text" value="personalMail"/>
OTHEREMAIL	<input type="text" value="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.

The screenshot shows the 'Users' management interface. On the left is a navigation menu with 'Configuration' selected and 'Users' highlighted. The main content area has a 'Providers' section and a 'Users' section. Under 'Users', there are buttons for 'Create', 'Get All', 'Put Selected', and 'Delete Selected'. Below these is a status bar indicating '10 Records from 32 have been fetched.' A table lists users with columns for ID, Name, Role, Bulk Edit, and Edit/Delete buttons. The 'Get All' button is highlighted in the screenshot.

ID	Name	Role	Bulk Edit	Page 1 2 3 >>
<input type="checkbox"/>	1	Administrator	ADMINISTRATOR	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	3	csta_provider_user	APPLICATION	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	4	dsml_ipo_provider_user	APPLICATION	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	5	dsml_ldap_provider_user	APPLICATION	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	15	Extn401	USER	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	27	Extn402	MANAGER	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	32	Extn403	USER	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	29	Extn404	USER	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	28	Extn405	USER	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	22	Extn406	USER	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

3. Browse through the users. When the required user 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.

The 'User Editor' dialog box is shown. It contains the following fields and values:

- ID: 15
- Name: Extn401
- Unique Identifier: C7C3E900F44611CD8268
- Display Name: (empty)
- Password: (masked with dots)
- Password Hash: 096A931191786EC72909E
- User Role: USER
- User Configuration Type Selector: Select (dropdown menu)
- User Configuration Type Specific Editor: Some User Configuration (text field)
- User Role Configuration: User, Manager (radio buttons)
- Created: 2010-07-07 01:21:22.7960

Buttons for 'Save' and 'Cancel' are at the bottom.

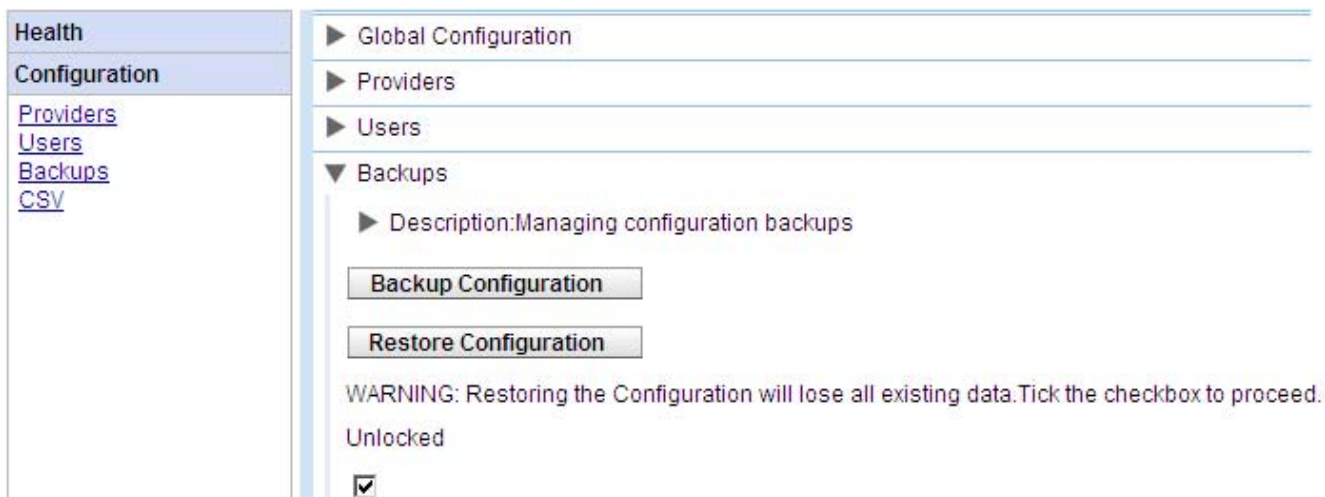
4. Use the User Configuration Type Selector to select the user settings to edit. The options are Screen Popping, Park Slots and Bridge Number.
5. The User Role Configuration is currently used in conjunction with Customer Call Reporter. The name and password of a user set as *Manager* can be entered into 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](#) ^[77] menu can be used to force an update from the IP Office systems.

4.4.3 Backups

This menu provided options to [backup](#)^[47] the one-X Portal for IP Office configuration. It can also be used to [restore](#)^[48] a previous backed up configuration.



Note that this is only intended as a simply backup and restore to allow rollback of server changes while making and testing administration changes. For one-X Portal for IP Office 6.1 a more sophisticated set of [backup and restore](#)^[82] 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\apache-tomcat-6.0.18\bin*). Any existing file is overwritten.



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

The screenshot shows the configuration interface for the AVAYA one-X Portal for IP Office. On the left is a navigation menu with 'Configuration' selected. The main area shows a tree view with 'Branding' expanded. Below this, there is a description: 'A control for configure Branding Name so that it will shown at One-X Portal user login page. Maximum 40 characters allowed for Branding Name.' There is a 'Refresh' button and a text input field containing 'one-X Server', followed by a 'Save' button.

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

The screenshot shows the title bar of the one-X Portal for IP Office. On the left, it displays 'Office | one-X Server'. On the right, it shows 'Extn401(401) | Do Not Disturb | Help | Logout | AVAYA'.

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.

The screenshot displays the 'Logging Configuration' interface. On the left is a navigation menu with 'Diagnostics' selected, containing links for 'Logging Configuration', 'Logging Viewer', 'Network Routes', 'IP Office Connections', and 'Database Integrity'. The main content area is titled 'Logging Configuration' and contains several sections:

- Master Logging Level:** A dropdown menu is set to 'ALL'. Text below reads: 'Set the threshold above which logging events are sent to logging targets. Choose ALL for 'log everything', choose OFF to 'disable logging'.'
- Logging Targets (Rolling Log Files):** Text explains: '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.'
- Logging Targets Table:** A table with columns 'Enabled', 'Name', 'Level', and 'File Path'. All 'Enabled' checkboxes are checked, and all 'Level' dropdowns are set to 'ALL'.

Enabled	Name	Level	File Path
<input checked="" type="checkbox"/>	Overall	ALL	../logs/1XOverallRollingFile.log
<input checked="" type="checkbox"/>	Presentation Layer	ALL	../logs/1XPresentationLayerRollingFile.log
<input checked="" type="checkbox"/>	Mid-Layer	ALL	../logs/1XMidLayerRollingFile.log
<input checked="" type="checkbox"/>	Telephony (CSTA)	ALL	../logs/1XCSTAServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (IP-Office)	ALL	../logs/1XIPODirServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (LDAP)	ALL	../logs/1XLDAPDirServiceRollingFile.log
- Logging Targets (Server and Network):** A 'Socket Receiver (required for remote log viewing)' checkbox is checked and labeled '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\apache-tomcat-6.0.18\logs*). Each log file can grow to approximately 10MB before a new file is started. When there are 5 files of a particular type, the oldest file is deleted when a new file is started.
 - **Overall:** *1XOverallRollingFile.log*
This is an overall log file of all types of logged events.
 - **Presentation Layer:** *1XPresentationLayerRollingFile.log*
This log captures user browser activity information!
 - **Mid-Layer:** *1XMidLayerRollingFile.log*
This log captures interaction between the various one-X Portal for IP Office components including the IP Offices.
 - **Telephony (CSTA):** *1XCSTAServiceRollingFile.log*
This log captures telephony information. That includes obtaining user and licensing information from the IP Offices.
 - **Directory (IP Office):** *1XIPODirServiceRollingFile.log*
This log captures IP Office directory information.
 - **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 and [installing Apache Chainsaw](#)^[55] which is a suitable logging application .

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

4.5.3 Network Routes

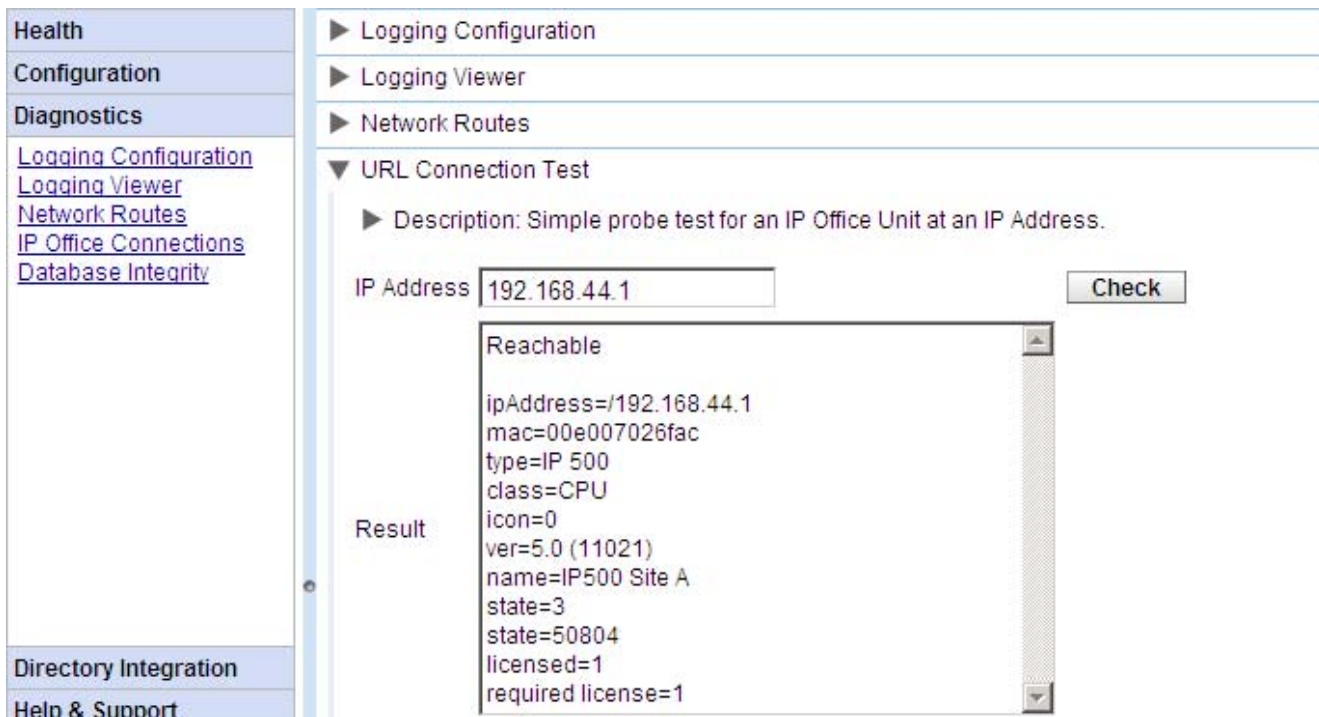
This menu can be used to test routing from the one-X Portal for IP Office server to an IP Office address. It uses TCP to port 7 (Echo service) on the target IP address. Note that this does not work with IP Office control units, for which the [IP Office Connections](#)^[76] should be used instead.

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

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

4.5.4 IP Office Connections

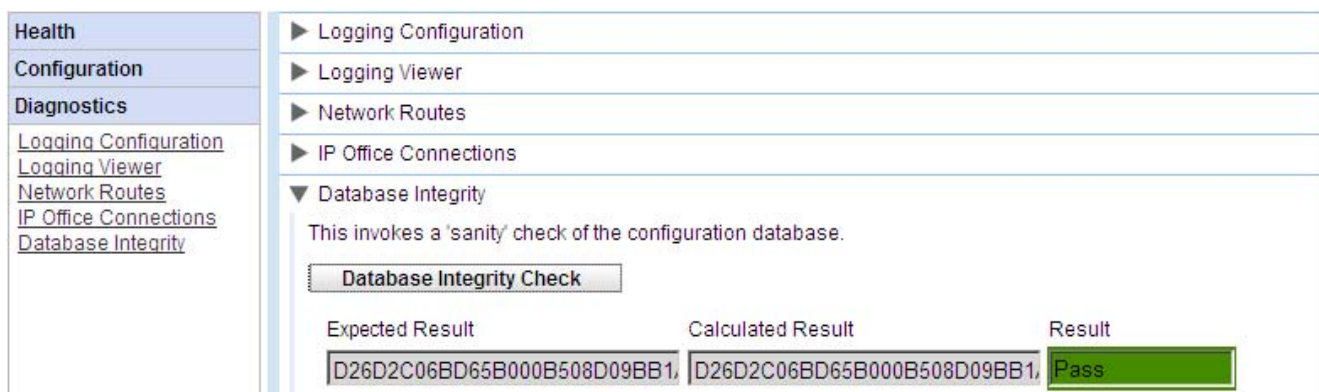
This menu can be used to check the connection between the one-X Portal for IP Office server and a particular IP Office. The connection check uses the standard discovery method used by IP Office applications such as IP Office Manager (connection to port 50804 of the IP Office control unit).



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

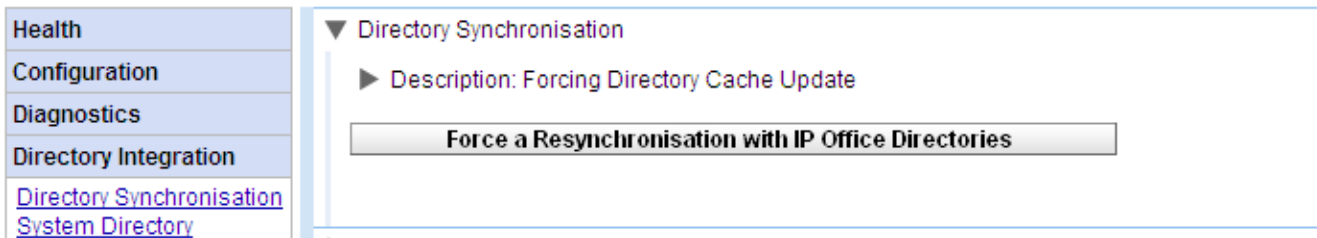
This menu can be used to check the database structure. It will return Pass if the tables and fields within the database are as expected for the particular version of one-X Portal for IP Office. It does not check the data within the fields. If Fail is reported refer to the [Troubleshooting](#) section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



4.6 Directory Integration

4.6.1 Directory Synchronisation

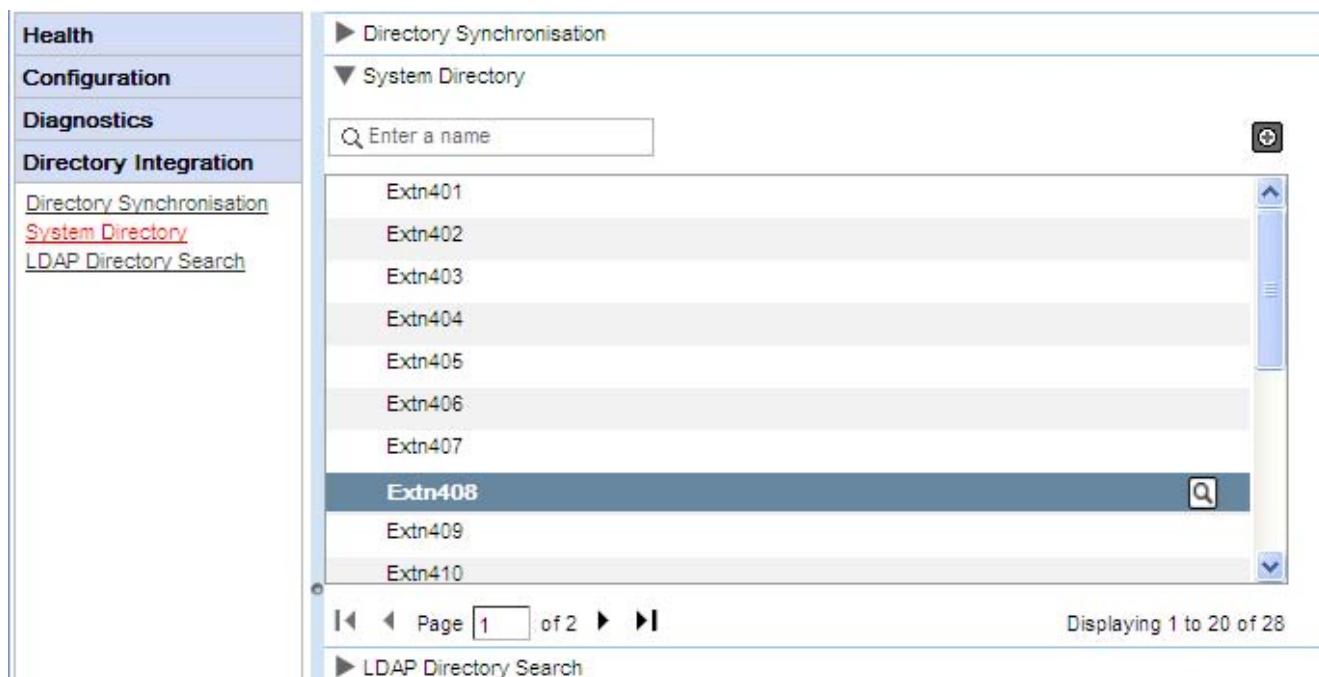
During normal operation, the one-X Portal for IP Office server updates the records every 300 seconds approximately. However, if necessary this menu can be used to force an update of the system directory and IP Office users.




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







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 way as if you were using the one-X Portal for IP Office client.



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

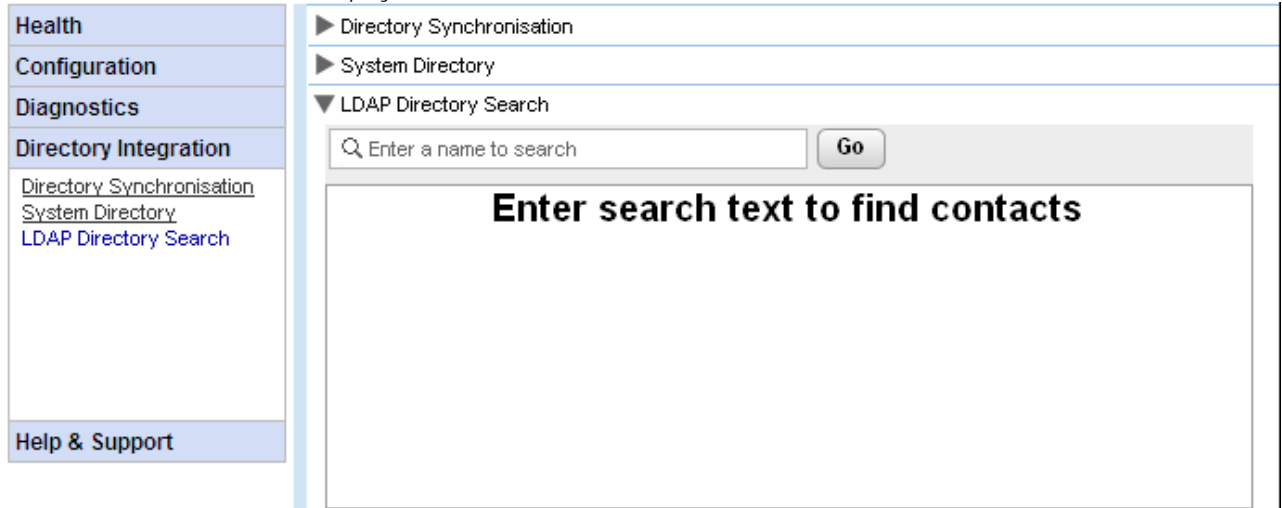
State	Icon	Description
Available		The normal state for a user showing that their work extension is not in use.
Busy		The normal state for a user showing that their work extension is currently on a call.
Do Not Disturb		The user has set Do Not Disturb. Calls to them will go to voicemail if enabled or 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 and are accessible by users through one-X Portal for IP Office only. These contacts can have multiple phone numbers and email addresses configured if required. To delete contacts that have been added in this way, click on the contact and select Delete in the contact details.

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](#) ^[43].

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



The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes sections for Health, Configuration, Diagnostics, Directory Integration, and Help & Support. Under Directory Integration, there are links for Directory Synchronisation, System Directory, and LDAP Directory Search. The main content area is titled 'LDAP Directory Search' and contains a search input field with the placeholder text 'Enter a name to search', a 'Go' button, and a large text box below it that says 'Enter search text to find contacts'.

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.

The screenshot displays the user interface of the one-X Portal for IP Office. On the left, a vertical navigation menu lists several categories: Health, Configuration, Diagnostics, Directory Integration, and Help & Support. The 'Help & Support' category is expanded, showing sub-links for 'Help', 'Avaya Support', and 'About'. The 'About' link is selected, leading to the main content area. This area features a tree view with 'About' expanded, showing the following text: 'Avaya one-X Portal for IP Office', 'Copyright 2011 Avaya Inc. All Rights Reserved.', and 'Version: 7.0.25.1419'. Below this, there is a section titled 'Links to the licenses of the third-party software components used in one-X Portal for IP Office.' which lists several licenses: 'H2 1.0.75 License', 'GWT 1.5.3 License', 'GWT Rocket 0.56 License', 'Apache Tomcat 6 License', and 'Apache Log4j 1.2.15 License'.

Chapter 5.

Backup/Restore

5. Backup/Restore

one-X Portal for IP Office 6.1 supports a new 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.

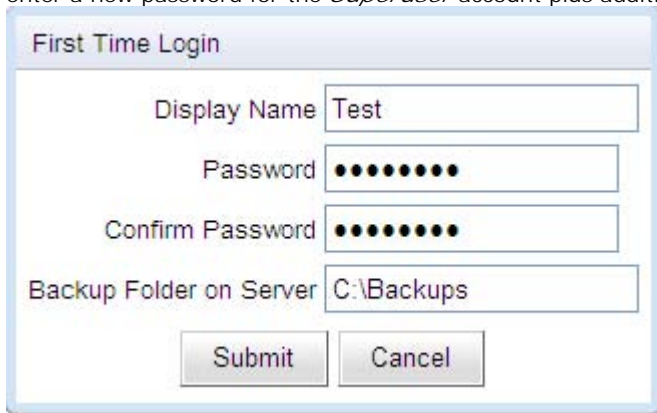
The menus are also intended to allow backup and restoration between an old and a new installation of one-X Portal for IP Office on a new server. However it is not supported for backup and restoration between different versions of one-X Portal for IP Office, for example from 6.1 to 7.0.

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.



- 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.

System status			
	Backup Name	File Size in Bytes	Backup Date Time
Last Backup Taken	OneX-DB-Bkp	29882	2010-08-03-11.33.25
	Backup Name	File Size in Bytes	Restore Date Time
Last Restore Done	OneX-DB-Bkp-2010-08-03-	29898	2010-08-03-11.38.32
Undo Last Restore			
Local Server Total Space	149	GB	
Local Server Free Space	91	GB	

- Last Backup Taken**
 This section gives details of the last backup taken using the Backup menu. The backup file name will have been a zip file named with the 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.

Edit	
Super User Name	Superuser
Display Name	Superuser
Password	●●●●●●●●
Confirm Password	●●●●●●●●
Backup Folder on Server	C:\Backups
<input type="button" value="Save"/> <input type="button" value="Clear"/>	

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

System Status

Configurator

DB Operations

Backup

Restore

DB Backup Operation

Backup Name

Backup Folder

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

User Name Password

Backup

- **Backup Name**
This name is used for the backup zip files. The date and time of the backup is also added to the file name. For example, *OneX-DB-Bkp-2010-08-03-11.33.25.zip*.
- **Backup 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 option 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.

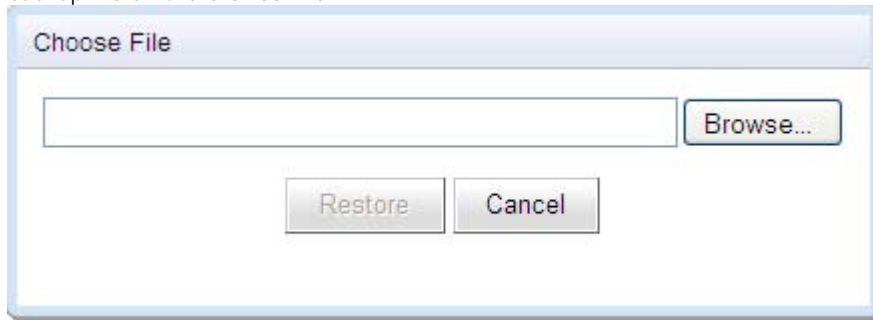
5.4.2 Restore

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](#) control. Restoration is only supported from a backup of the same one-X Portal for IP Office version.

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

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

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



Chapter 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

4

4560 55

8

8080 22

A

About 62

Active Sessions 62, 65

Add

IP Office 38

LDAP 43

Licenses 20

User 44

Administrator

Help 80

Login 26

Name 63

Advanced 32

Agent 60

Apache

Chainsaw 55, 75

Applications DVD 15

Assign

IP Office 38, 41

IP Office (CSTA) 67

IP Office (Directory) 68

LDAP Provider 69

Providers 66

Automatic logout 63

Avaya Support 62

B

Backup 47, 72

Restore 48

Backups 62

Base DN 43

browser 15

Bulk Edit 44, 70

User 44

C

Call Log 44

Chainsaw 55, 75

Component Status 62, 64

Computer Supported Telecommunications Application 88

Configuration 62

Backup 47

Backups 72

Bulk Edit 44

CSV 72

During installation 26

Export 72

Providers 66

Restore 48, 72

User 21

Users 70

Control Panel 53

Cookies 15

CSTA 67, 88

CSTA (IP Office) Provider 67

CSV 62, 72

D

Database

Backup 47, 72

Check 76

Restore 48, 72

Sanity Check 76

Database Integrity 62

Deinstall 53

Delete

IP Office 41

User 44

Diagnostics 62

Connections 76

Database Integrity 76

IP Office Connections 76

Logging Configuration 55, 74

Logging Viewer 55, 75

Network Routes 75

Directories 9

Directory

Export 72

Resynch 49, 77

Directory (DSML IP Office) 68

Directory (DSML LDAP) 69

Directory DSML IP Office Provider 8

Directory DSML LDAP Provider 8

Directory Integration 62

Directory Synchronization 49, 77

Directory Intergration

LDAP 50, 79

System Directory 49, 78

Directory Search

LDAP 50, 79

System Directory 49, 78

Directory Synchronization 62

DND Exceptions 44

Downgrading 52

DSML (IP Office) Provider 68

DSML (LDAP) Provider 69

DVD 15

E

Echo 75

Edit

Bulk Edit 44

IP Office Security Settings 18

IP Office settings 41

User settings 44, 70

Enable one-X Portal Services 21

Enhanced TSPI 18

Enhanced TSPI Access 18

Enhanced TSPI service 18

EnhTcpaService 18

Environment 62

Events 64

Exceptions 44

Explorer 15

Export Configuration 72

exportDirectoryEntry.csv 72

exportUser.csv 72

External Directory 9

Search 50, 79

F

Field Mapping 43, 69

Firefox 15

Firewall 15, 22

Force a Resynchronization 49, 77

G

Group 60

H

Hard Disk 15
Health 62

- Active Sessions 65
- Component Status 64
- Environment 65
- Key Recent Events 64

Help 62

- About 80
- Avaya Support 80
- Help 80

Hunt Group 60

I

Immediate logout 63
Initial configuration 26
Install

- Software 23

Installation

- Advanced 32

Internet Explorer 15
IP Office

- Applications DVD 15
- Check 26
- Connections 62
- CSTA Provider 67
- Directory Provider 68
- License 20
- Security Settings 18
- Select 26
- System Requirements 15
- User configuration 21

J

Java Web Start 55
JavaScript 15

K

Key Recent Events 62, 64
Keyboard Shortcuts 44

L

LDAP

- Assign 43
- Directory Search 50, 62, 79
- Provider 69

License

- Add 20

Listing Ports 22
Log Files 74
Log4j format 55
Logging 55

- Configuration 62
- Level 74
- Targets 74
- Viewer 55, 62

Logging Configuration 55
Login 30, 63

- Administrator 26

Logout 63

M

Maintenance 36
Master Logging Level 74
Membership 60
Messages 44
Mozilla Firefox 15

N

Name 21

Network Routes 62, 75
Not Reachable 75

O

Operating System 15
Override Admin Session 63

P

Park Slots 44
Password 21, 63

- Change 26

Personal Directory 9, 44
PING 75
Port 15

- 4560 55
- 7 75
- 8080 23
- Set 23

Ports 22
Presence 44
Presentation Level Provider 8
Provider 8, 62

- Assign 66
- CSTA (IP Office) 67
- Directory (DSML IP Office) 68
- Directory (DSML LDAP) 69
- DSML (IP Office) 68
- DSML (LDAP) 69
- View 66

Q

Quick Time 15

R

RAM Memory 15
Reachable 75
Recent Events 64
Remember me on this computer 15
Remote Logging 55
Remove

- IP Office 41
- one-X Portal for IP Office 53
- User 44

Reserved Ports 22
Reset Session Count 63
Restart Service 37
Restore 48, 72

- Backup 47

Resynchronization 49, 77
Rights Group 18
Rolling Log Files 74
Routes 75

S

Safari 15
Sanity 76
Search

- LDAP 50, 79
- System Directory 49, 78

Search Base 43
Security Settings 18
Server

- Information 65
- PC Requirements 15
- Version 65

Service

- Restart 37

Service User 18
Services 18

Sessions 65
Settings
 Backup 47
 Bulk Edit 44
 Restore 48
 User 21
Shortcuts 44
Socket Receiver 55, 74
Software
 Install 23
Start Service 37
Status 64
Synchronization 49, 77
System Directory 9, 62
 Directory Search 49, 78
 Export 72
 Resynch 49, 77

T

TCP Port 7 75
TCPA 88
TCPA Group 18
Telephony CSTA Provider 8
Telephony Service Provider Interface 88
Test
 External Directory 50, 79
 IP Office connection 76
 LDAP Directory 50, 79
 Network Route 75
 System Directory 49, 78
 User Login 30
Thin Client Productivity Application 88
TSPI 88

U

Uninstall 53
Upgrading 51
User
 Add 44
 Bulk Edit 44
 Configuration 21
 Delete 44
 Edit settings 44
 Export 72
 Help 80
 Login 30
 Name 21
 Password 21
 User name 21
Users 62
 Active 65
 Edit settings 70
 Resynch 49, 77
 View 70

V

Version 65
View
 Component Status 64
 Key Recent Events 64
 Providers 66
Voicemail Messages 44

W

Windows Media Player 15

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.

Intellectual property related to this product (including trademarks) and registered to Lucent Technologies have been transferred or licensed to Avaya.

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

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

Any comments or suggestions regarding this document should be sent to "wgctechpubs@avaya.com".

© 2011 Avaya Inc. All rights reserved.

Avaya
Unit 1, Sterling Court
15 - 21 Mundells
Welwyn Garden City
Hertfordshire
AL7 1LZ
England.

Tel: +44 (0) 1707 392200
Fax: +44 (0) 1707 376933

Web: <http://marketingtools.avaya.com/knowledgebase>