



IP Office

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

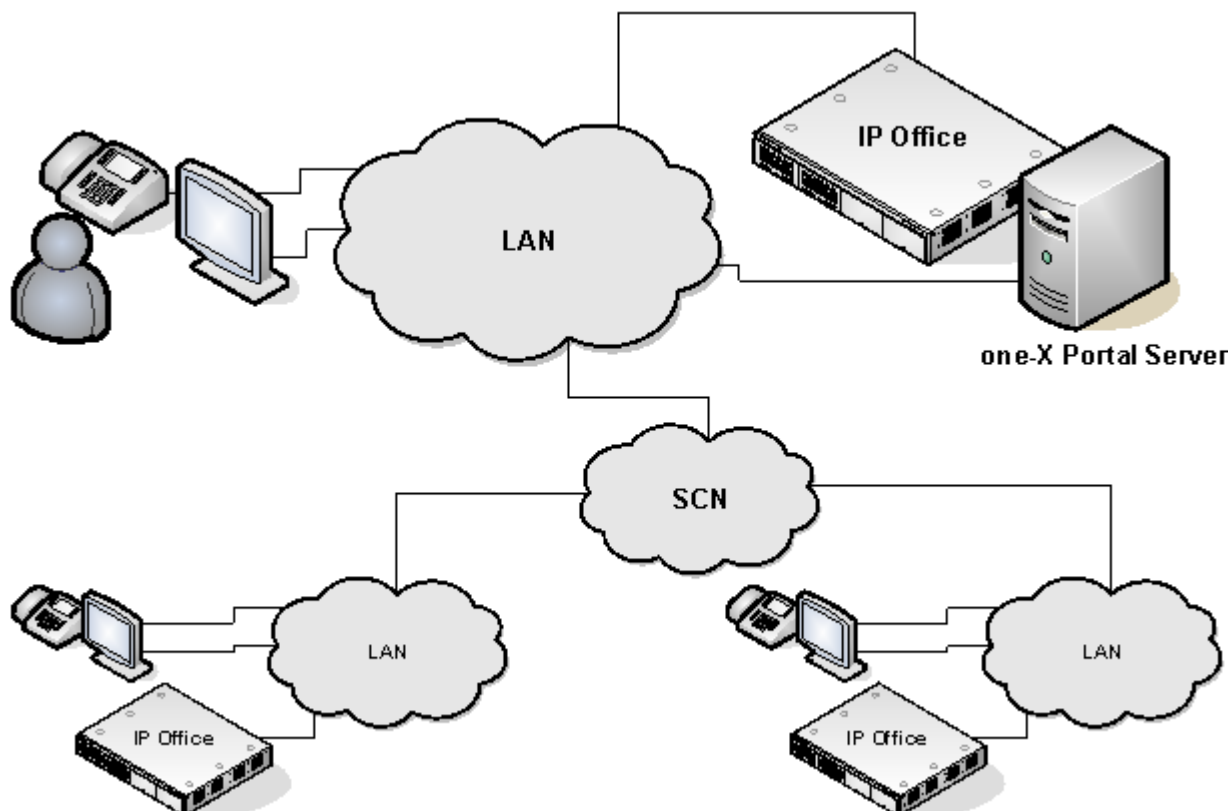
	4.6.2 System Directory.....	74
	4.6.3 LDAP Directory Search.....	75
	4.7 Help & Support.....	76
1. one-X Portal		
1.1 Providers	8	
1.2 one-X Portal Settings.....	9	
1.3 Telephony Notes.....	11	
1.4 Small Community Network Support.....	12	
2. Installation		
2.1 Installation Requirements.....	15	
2.2 Check the IP Office Security Settings.....	17	
2.3 Add one-X Portal Licenses.....	19	
2.4 Configure Users for one-X Portal.....	20	
2.5 Checking Available Server Ports.....	22	
2.6 Install the one-X Portal Software.....	23	
2.7 Initial Server Configuration.....	25	
2.8 Test User Connection.....	29	
2.9 Disable Java Updates.....	30	
2.10 Advanced Configuration Options.....	31	
3. Maintenance		
3.1 Manually Starting the Service.....	35	
3.2 Adding an Additional IP Office.....	36	
3.3 Changing IP Office Details.....	39	
3.4 Adding an LDAP External Directory Source.....	41	
3.5 Adding/Deleting Users.....	42	
3.6 Editing User Settings.....	42	
3.7 Backing Up the Database.....	45	
3.8 Restoring a Previous Backup.....	46	
3.9 Checking and Updating the System Directory.....	47	
3.10 Checking the External LDAP Directory.....	48	
3.11 Upgrading one-X Portal.....	49	
3.12 Downgrading one-X Portal.....	50	
3.13 Removing one-X Portal.....	51	
3.14 Remote Logging.....	53	
3.15 Troubleshooting.....	57	
4. Administration		
4.1 Login	61	
4.2 Logout	61	
4.3 Health	62	
4.3.1 Component Status.....	62	
4.3.2 Key Recent Events.....	62	
4.3.3 Active Sessions.....	63	
4.3.4 Environment.....	63	
4.4 Configuration.....	64	
4.4.1 Providers.....	64	
4.4.2 Users.....	68	
4.4.3 Backups.....	69	
4.4.4 CSV.....	69	
4.5 Diagnostics.....	70	
4.5.1 Logging Configuration.....	70	
4.5.2 Logging Viewer.....	71	
4.5.3 Network Routes.....	71	
4.5.4 IP Office Connections.....	72	
4.5.5 Database Integrity.....	72	
4.6 Directory Integration.....	73	
4.6.1 Directory Synchronisation.....	73	
	5. Glossary	
	Index	79

Chapter 1.

one-X Portal

1. one-X Portal

This documentation covers the installation of one-X Portal for IP Office (henceforth just one-X Portal). one-X Portal 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 server can support multiple IP Offices when they are connected in a single [IP Office Small Community Network](#) (SCN). one-X Portal 6 supports up to 500 simultaneous sessions.



one-X Portal installs as a service with an integral web server. Both user and administrator access to one-X Portal is via web browser to the one-X Portal server.

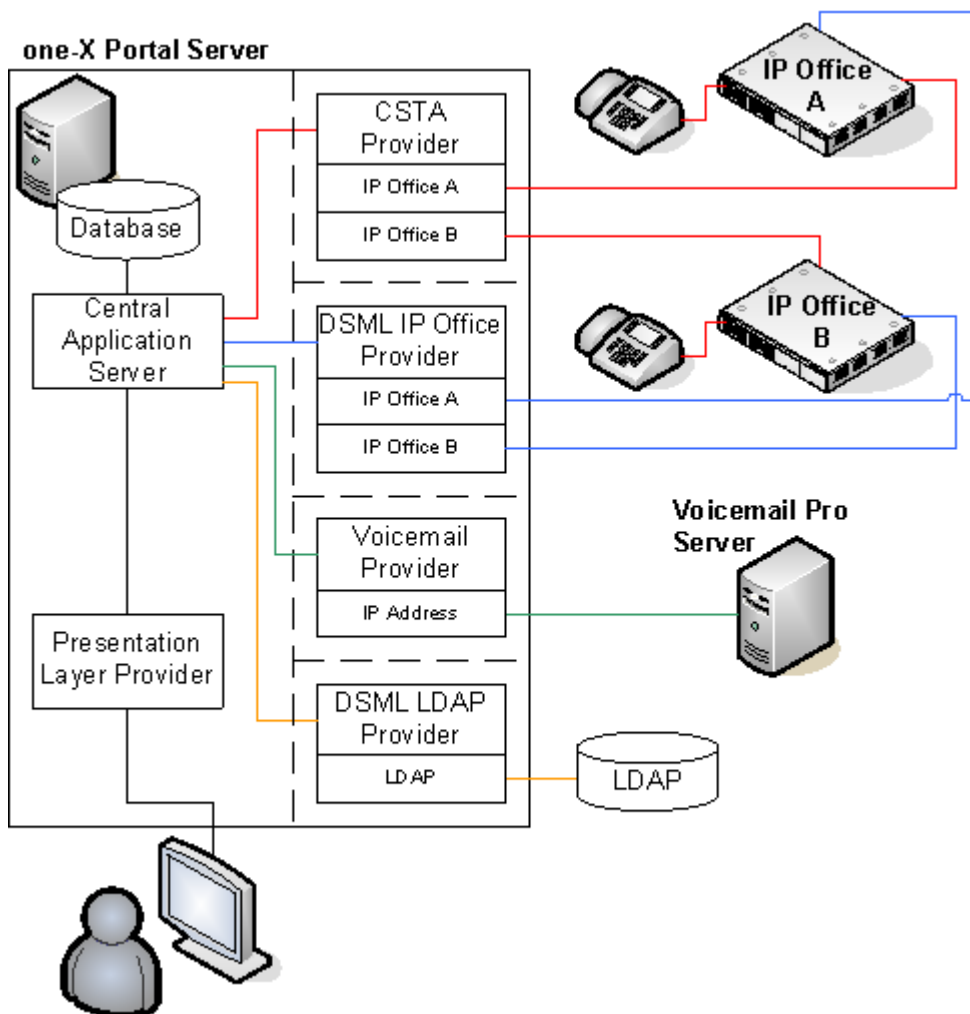
The one-X Portal service communicates with the IP Office system using the IP Office's TSPI (Telephony Service Provider Interface) service. This is a service supported by IP Office 5.0+ systems and configured through the security settings of the IP Office control units.

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

1.1 Providers

A key idea to understand for one-X Portal is providers. Providers are components of one-X Portal, 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 server.
- **Telephony CSTA Provider**
This type of provider handles telephony communications to and from the IP Office systems assigned to it.
- **Directory DSML IP Office Provider**
This type of provider handles obtaining directory information from the IP Office phone systems assigned to it.
- **Directory DSML LDAP Provider**
Handles obtaining LDAP directory information from an LDAP source. LDAP sources are assigned to the provider during installation.
- **VoiceMail Provider**
Handles direct interaction with the voicemail server for features such as message playback via the browser.



During installation:

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

1.2 one-X Portal Settings

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

Directories

The various directories available to a one-X Portal 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 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 only.

- Personal directory records stored by one-X Portal 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 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 only.
 - **IP500/IP500 V2:** 10800 total personal directory records.
 - **IP412:** 3600 total personal directory records.
 - **IP406 V2:** 1900 total personal directory records.
- For users with a 1608 or 1616 phone, they can edit or delete the contact 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 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.
- If multiple IP Office systems are configured to operate with one-X Portal, the system directories of each are combined by one-X Portal into a single system directory for use by one-X Portal 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 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 users, the number must be dialable by all one-X Portal users. Alternatively, short codes should be used to ensure that numbers selected from the one-X Portal system directory are interpreted correctly by the user's own IP Office
- The one-X Portal administrator can [add System Directory contacts](#)^[74] that are stored as part of the one-X Portal 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 users.

- **External Directory**

The external directory is not stored by one-X Portal. Instead one-X Portal performs a live search of the external directory source [configured](#)^[47] for one-X Portal 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 server.

Setting	one-X Portal	IP Office	Source/Storage
Personal Directory	✓	✓	<p>A user's personal directory is stored in the configuration of both one-X Portal 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 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 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 only. <ul style="list-style-type: none"> IP500/IP500 V2: 10800 total personal directory records. IP412: 3600 total personal directory records. IP406 V2: 1900 total personal directory records. For users with a 1608 or 1616 phone, they can edit or delete the contact 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 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.
Sound Configuration	✓	–	A user's one-X Portal sound preference is stored by one-X Portal.
Park Slots	✓	–	The park slot numbers used for a user's one-X Portal park buttons are stored by one-X Portal.

Note that those settings stored by one-X Portal are lost if one-X Portal is [reinstalled](#) ⁵¹ rather than [upgraded](#) ⁴⁹.

1.3 Telephony Notes

Incoming Calls

The calls that reach the one-X Portal 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 user will be down to IP Office system configuration settings.

Outgoing Calls

The outgoing calls that the one-X Portal 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 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 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.

Call Gadget Buttons

Within the sub-tab shown for each call being handled by the one-X Portal 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 useful to understand that it is not the one-X Portal application that controls which buttons are displayed. The actions currently performable on each call are indicated to one-X Portal as part of the CSTA 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 will not present the user with an **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 while 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.

1.4 Small Community Network Support

one-X Portal is supported within an IP Office Small Community Network (SCN). Each IP Office on which one-X Portal users use must meet the requirements for one-X Portal.

- one-X Portal 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 are not supported between different systems in an SCN. This means that one-X Portal users can only park and unpark calls on the IP Office on which they are registered.
- one-X Portal 6 supports up to 500 simultaneous sessions.

Chapter 2.

Installation

2. Installation

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

- **Important**

Installation of one-X Portal is greatly simplified if each IP Office contains at least one user already licensed and configured for one-X Portal 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](#) ^[17]
3. [Add one-X Portal Licenses](#) ^[19]
4. [Configure IP Office Users for one-X Portal](#) ^[20]
5. [Checking Available Ports](#) ^[22]
6. [Install the one-X Portal Software](#) ^[23]
7. [Initial Server Configuration](#) ^[25]
8. [Test User Connection](#) ^[29]

2.1 Installation Requirements

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

IP Office Software

- **IP Office Applications DVD**

The IP Office Applications DVD for IP Office 5.0 and higher includes the software for installation of one-X Portal. It also includes software for installation of IP Office Manager and the IP Office System Status Application which are required during one-X Portal installation.

IP Office System Requirements

- **IP Office Release 5 or higher**

If the system running pre-5.0 IP Office software, it must be upgraded as per the relevant IP Office Technical Bulletins for IP Office Release 5 or IP Office Release 6 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 5 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.

- **IP Office Release 5 Licensing**

This release of IP Office uses **one-X Portal for IP Office** licenses added to the IP Office configuration.

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

- For systems being upgraded from IP Office Release 5 to IP Office Release 6, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for users set to the **Basic User** profile.

Server PC Requirements

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

- **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 port is 8080. This can be changed if required during installation of the server software if necessary. See [Checking Available Ports](#) ²²⁷.
- **Firewall Exceptions**
Exceptions should be added to the server firewall for incoming access on the TCP port 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

Voicemail playback through the one-X Portal user's browser and personalized greeting playback require a Voicemail Pro 6.0 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 server.

-
- Check that the IIS on the voicemail server can be browsed by server name from the one-X Portal server PC. Enter **http://<voicemail_server_name>/localstart.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 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 each IP Office system:
 - IP Address.
 - Name and password for security settings access.
 - Name and password for configuration settings access.
 - one-X Portal Licenses.
 - Users who will be using one-X Portal 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 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 User Requirements

- **Browser**

Web browser with LAN access to the one-X Portal server. one-X Portal is tested using the current versions of the 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 currently supports **English, French, German, Italian, Dutch, Brazilian Portuguese** and **Russian**. 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 server you must check the IP Office security settings. one-X Portal uses a specific service and security service user account for the connection. This service is not necessarily present by default.

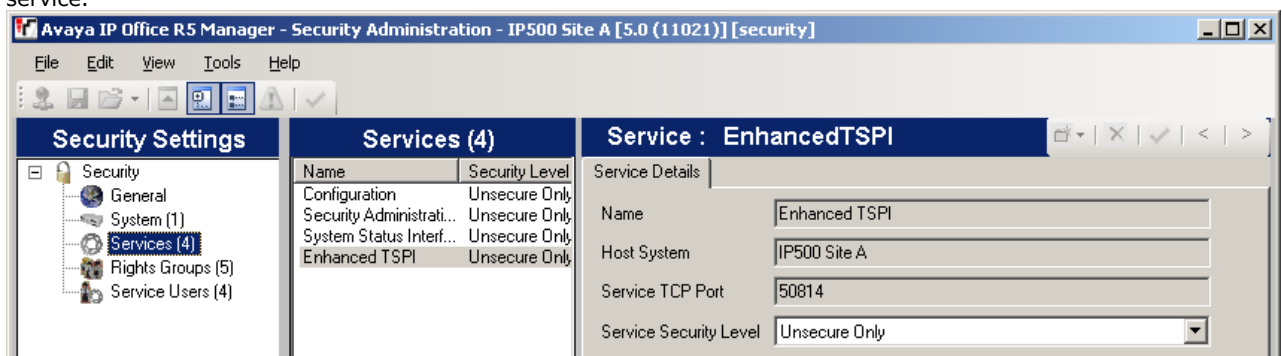
- **Important: Perform this Process from the one-X Portal Server PC**

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.

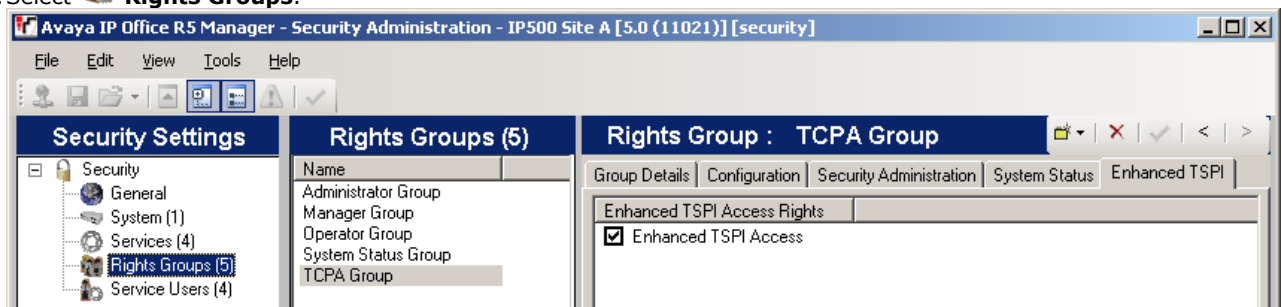
- **Important: Security Name and Password**

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

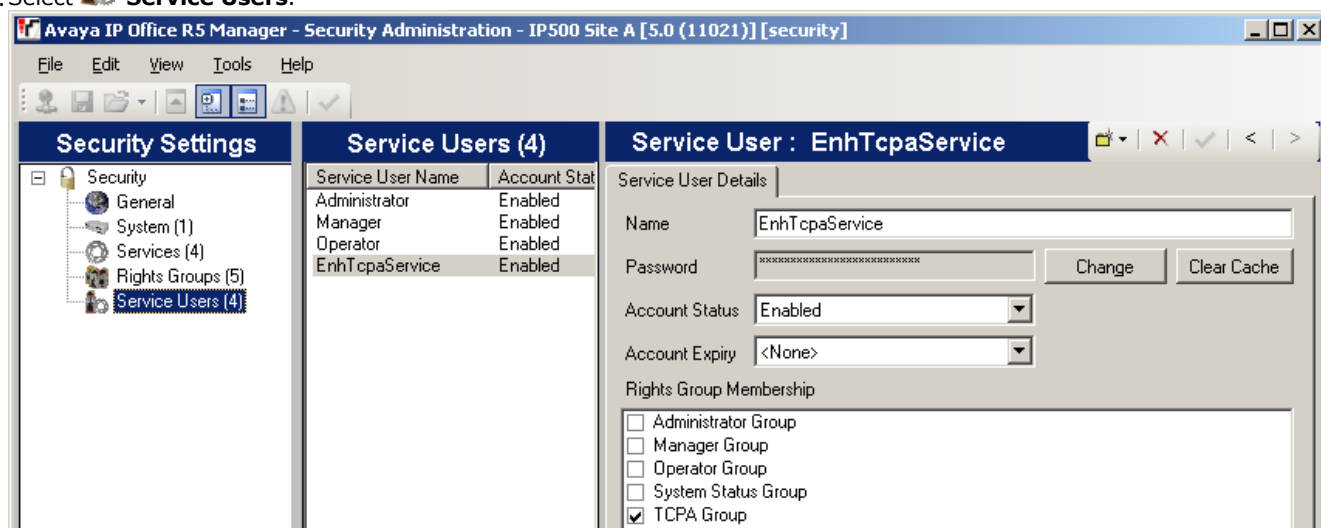


6. Select  **Rights Groups**.




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 Licenses

Each user for one-X Portal 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 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 5 Licensing**

This release of IP Office uses **one-X Portal for IP Office** licenses added to the IP Office configuration.

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

- For systems being upgraded from IP Office Release 5 to IP Office Release 6, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for users set to the **Basic User** profile.
- For one-X Portal 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 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 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 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 server.

2.4 Configure Users for one-X Portal

It is strongly recommended that at least one user on each IP Office system to be supported is configured as a one-X Portal user before the one-X Portal server is installed.

- **IP Office Release 5 Licensing**



This release of IP Office uses **one-X Portal for IP Office** licenses added to the IP Office configuration.

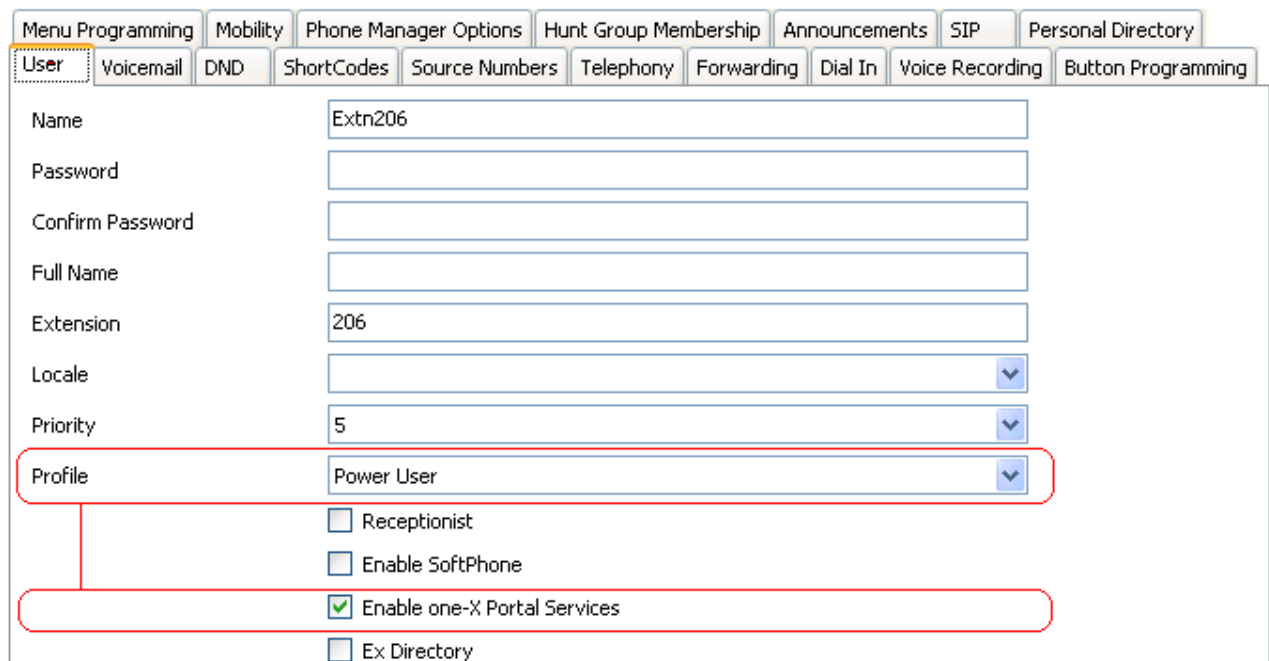
- **IP Office Release 6 Licensing**

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


- For systems being upgraded from IP Office Release 5 to IP Office Release 6, existing **one-X Portal for IP Office** licenses remain valid and can be used to enable one-X Portal for users set to the **Basic User** profile.

IP Office Release 6



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 operation.
6. Select the **User** tab.

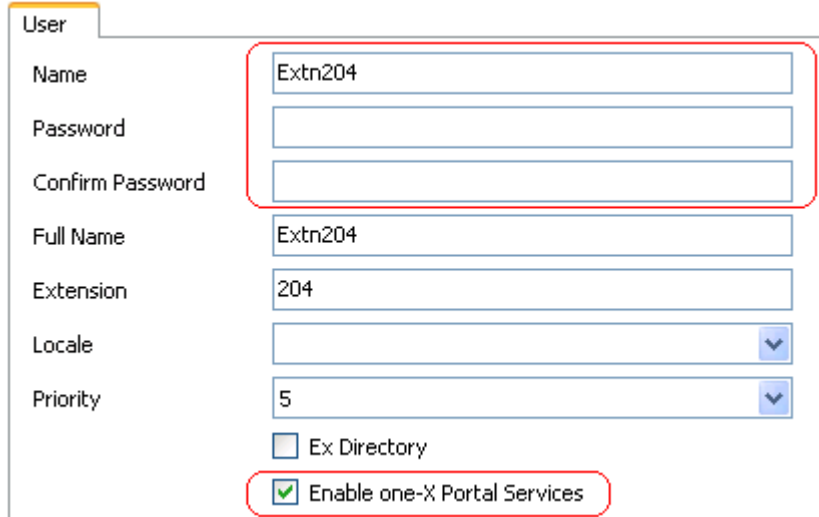


Menu Programming	Mobility	Phone Manager Options	Hunt Group Membership	Announcements	SIP	Personal Directory			
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	Extn206								
Password									
Confirm Password									
Full Name									
Extension	206								
Locale									
Priority	5								
Profile	Power User								
	<input type="checkbox"/> Receptionist								
	<input type="checkbox"/> Enable SoftPhone								
	<input checked="" type="checkbox"/> Enable one-X Portal Services								
	<input type="checkbox"/> Ex Directory								


7. Select the **Profile** which you want the user to use and for which the IP Office system has licenses. For one-X Portal the supported profiles are **Office User**, **Teleworker User** or **Power User**. The later two are also able to support the one-X Portal 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 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 services.
11. Click on  to save the updated configuration back to the IP Office system.

IP Office Release 5

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 operation.
6. Select the **User** tab.



User	
Name	<input type="text" value="Extn204"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Full Name	<input type="text" value="Extn204"/>
Extension	<input type="text" value="204"/>
Locale	<input type="text" value=""/> ▼
Priority	<input type="text" value="5"/> ▼
	<input type="checkbox"/> Ex Directory
	<input checked="" type="checkbox"/> Enable one-X Portal Services

7. Select **Enable one-X Portal Services**.
8. Note the user **Name** and **Password**. These are used by the user to login to one-X Portal.
 - 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.
1. Repeat the process for any other users who will be using one-X Portal services.
2. Click on  to save the updated configuration back to the IP Office system.

2.5 Checking Available Server Ports

The one-X Portal application installs as a service (*Avaya one-X Portal*) listening on a server's port. By default it uses port 8080.

It is important to check that port 8080 is not already in use by another application. If it is, a different unused port number should be specified during the one-X Portal software installation. The only way to change the port following installation is to [remove and then reinstall the software](#)^[5].

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

- **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. Those ports should not be used for one-X Portal.

- **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.

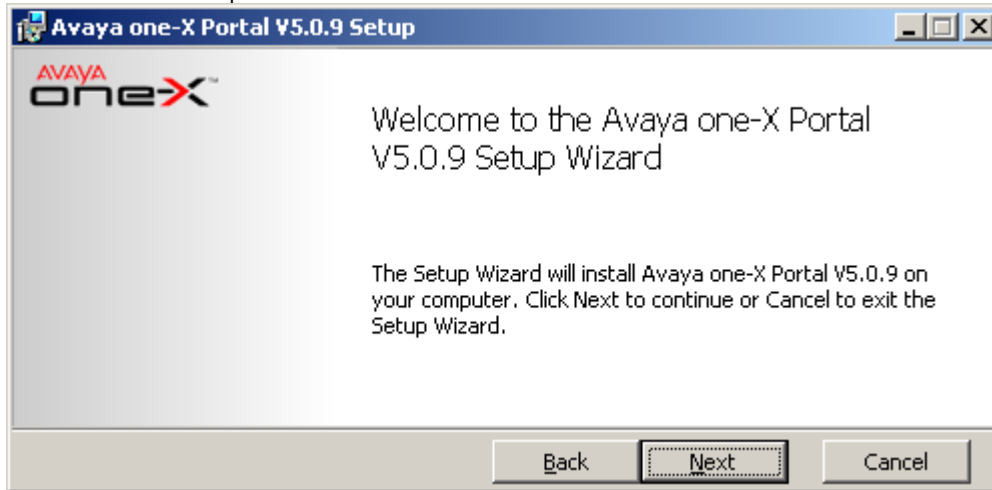
- **8081** - Default port used by IIS for Sharepoint Administration access.

2.6 Install the one-X Portal Software

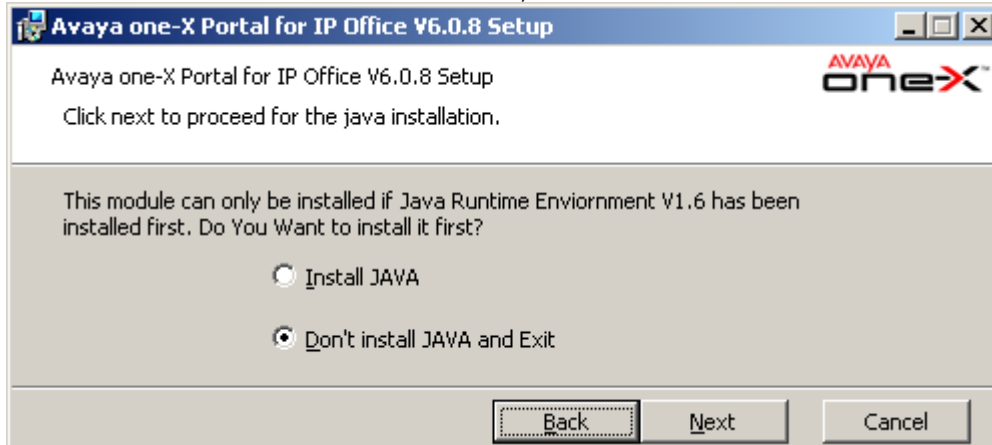
- **Important**

It is strongly recommended that you do not start software installation until the previous installation steps ([IP Office security settings](#) ^[17], [one-X Portal licenses](#) ^[19], [user configuration](#) ^[20]) have been completed.

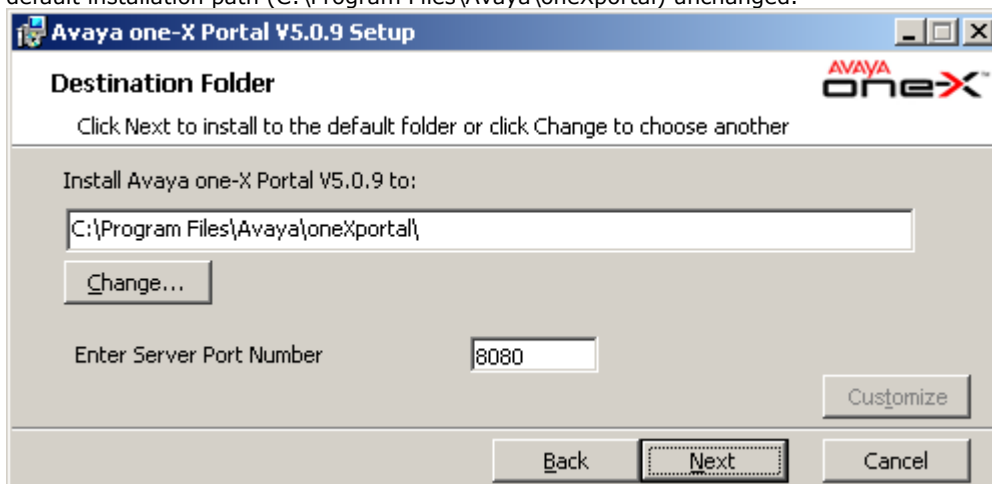
1. Check that you have logged in to the server using an account with full administrator rights.
2. On the IP Office Application DVD, locate and double-click on the file **one-Xportal.msi** file to start the server software installation process.



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



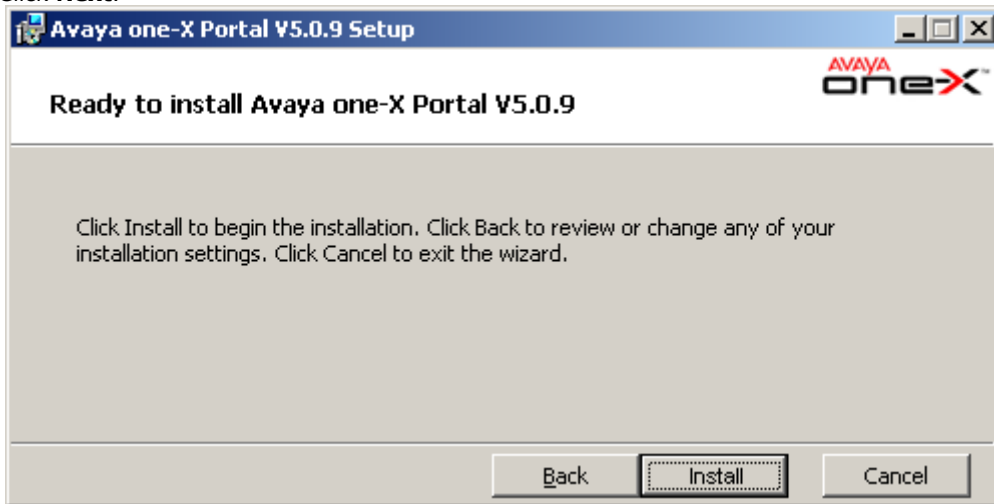
4. Select **Install Java** and click **Next**. Unless there is a reason to do otherwise we recommend that you leave the default installation path (C:\Program Files\Avaya\oneXportal) unchanged.



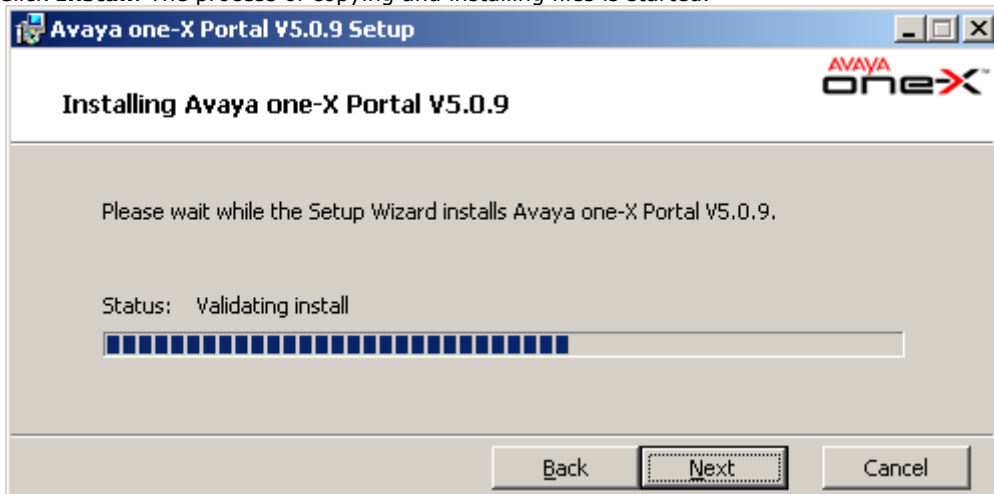
- **Enter Server Port number:** Default = 8080

If the server PC already has services using port 8080 (see Checking Available Ports), enter a new unused port number here. Note that once one-X Portal is installed, the port number can only be changed by removing and then reinstalling the one-X Portal software.

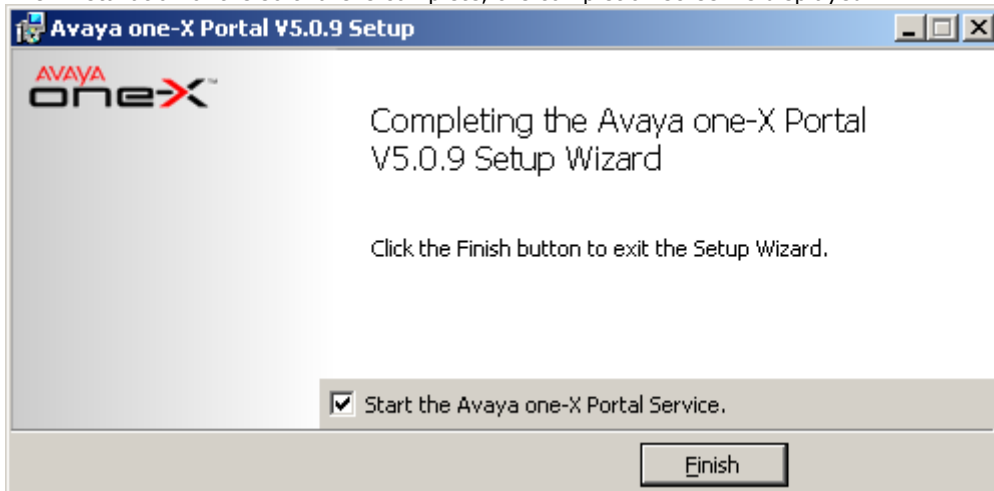
5. Click **Next**.



6. Click **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](#) ^[38] before it can be configured.

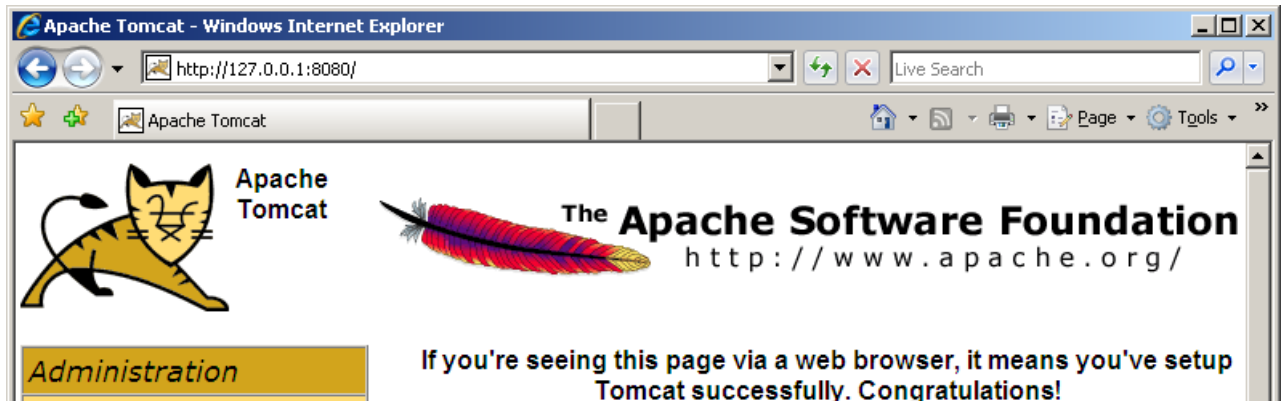
9. Click on **Finish**.

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

2.7 Initial Server Configuration

At this stage, the one-X Portal server software has been [installed](#) and the service started. However the one-X Portal 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](#).
2. On the one-X Portal 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 responds. One way to monitor progress is to use Windows Task Manager. Typically as one-X Portal is starting, the **PF Usage** will gradually increase. Once it reaches approximately 2.3GB, one-X Portal has started.
4. The web server installed by the one-X Portal 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 application.



6. The message **System is currently unavailable - please wait** may be displayed with the one-X Portal application starts. When the message disappears approximately 15 minutes after the one-X Portal service was started, you can login.
7. Check that the version reported matches the version expected. If not refer to the [Troubleshooting](#) 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 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 separated 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 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

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).

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"/>

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.

Provider's Mid-Layer Username:
 Provider's Mid-Layer Password:
 Provider runs on Port:
 LDAP Server Address:
 LDAP Server Username:
 LDAP Server Password:
 LDAP Server Base DN:

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

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

Description

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

► Status

Automatic User List Extraction Progress

■ | | | | | | | | | |

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

STEP 4: Synchronise System & Personal Directories

Description

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

► Status

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

Administrator Default Password Check

You must change the password from its default value.

New Password

●●●●●●●●

New Password (Typed Again)

●●●●●●●●

Passwords match

Password strength not enforced

Change Password

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 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 and use it to make and answer calls.

1. From a user PC, uses a web browser to browse to the one-X Portal 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 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 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](#) ^[27].

Chapter 3.

Maintenance

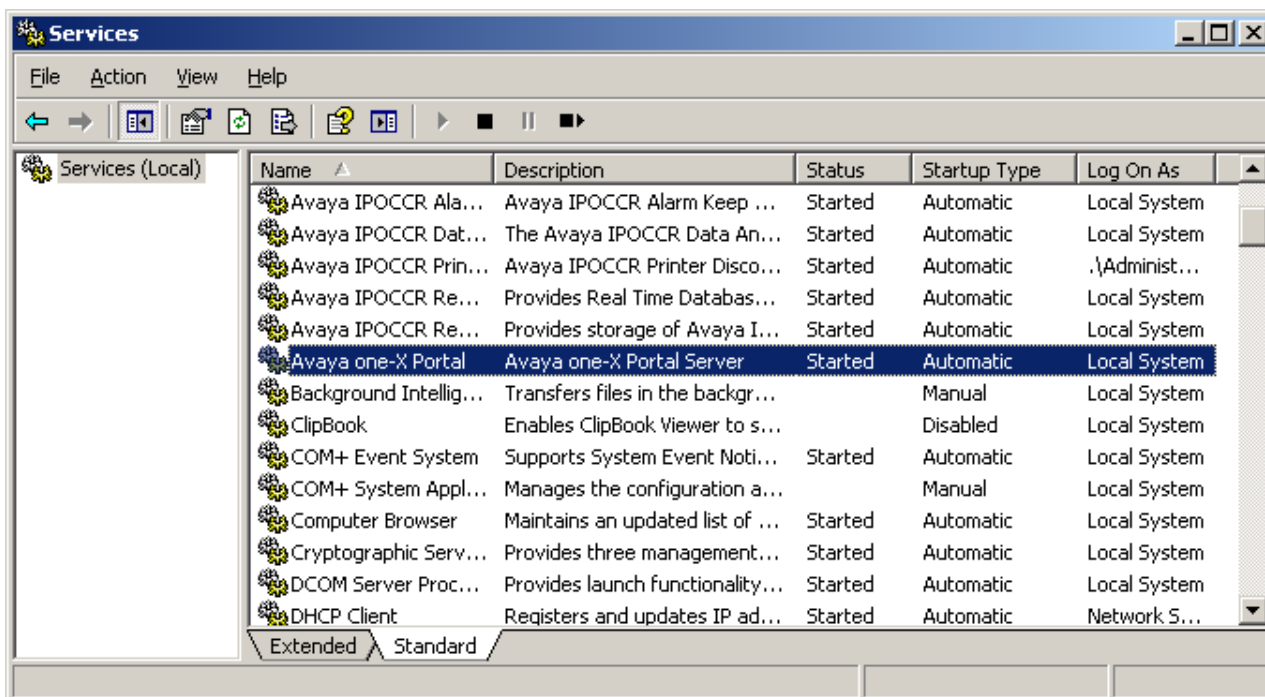
3. Maintenance

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

- [Manually Starting the Service](#) ^[35]
- [Adding an Additional IP Office](#) ^[36]
- [Changing an IP Office Details](#) ^[39]
- [Adding/Deleting Users](#) ^[42]
- [Editing User Settings](#) ^[42]
- [Adding an LDAP Directory Source](#) ^[41]
- [Checking the External LDAP Directory](#) ^[48]
- [Backing Up the Database](#) ^[45]
- [Restoring a Previous Backup](#) ^[46]
- [Checking and Updating the System Directory](#) ^[47]
- [Upgrading one-X Portal](#) ^[49]
- [Downgrading one-X Portal](#) ^[50]
- [Removing one-X Portal](#) ^[51]
- [Remote Logging](#) ^[53]

3.1 Manually Starting the Service

The one-X Portal 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 is starting, the **PF Usage** will gradually increase to approximately 2.3GB before one-X Portal has started.

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 will not be available to all users for up to 15 minutes.

1. Before adding another IP Office to the one-X Portal configuration:
 - Check that the IP Office has been configured with the [security settings](#) for one-X Portal operation.
 - Check that the IP Office is [licensed](#) for one-X Portal.
 - Check that at least one user on the IP Office has been [enabled for one-X Portal](#).
2. [Log in](#) to the administrator menus.
3. Check that the IP Office can be seen from the one-X Portal 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 database.

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

Provider Editor

ID

Name

Data

Provider Type Selector

IP Office(s) Assigned

Mid-Layer URL

Mid-Layer Username

CSTA Config Editor Mid-Layer Password

Mid-Layer Password Hash

Run On Port

Created

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

IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 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="password"/>	<input type="button" value="Delete"/>

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	
<input type="text" value="0"/>	<input type="text" value="192.168.42.1"/>	<input type="text"/>	<input type="password"/>	<input type="button" value="Delete"/>
<input type="text" value="1"/>	<input type="text" value="192.168.44.1"/>	<input type="text" value="EnhTcpcService"/>	<input type="password" value="....."/>	<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 TCPA security user configured in the IP Office system.

11. Click **Close**.

12. Click **Close** again.

13. Click on **Put Selected**. This writes the new settings of the CSTA provider back to the one-X Portal database.

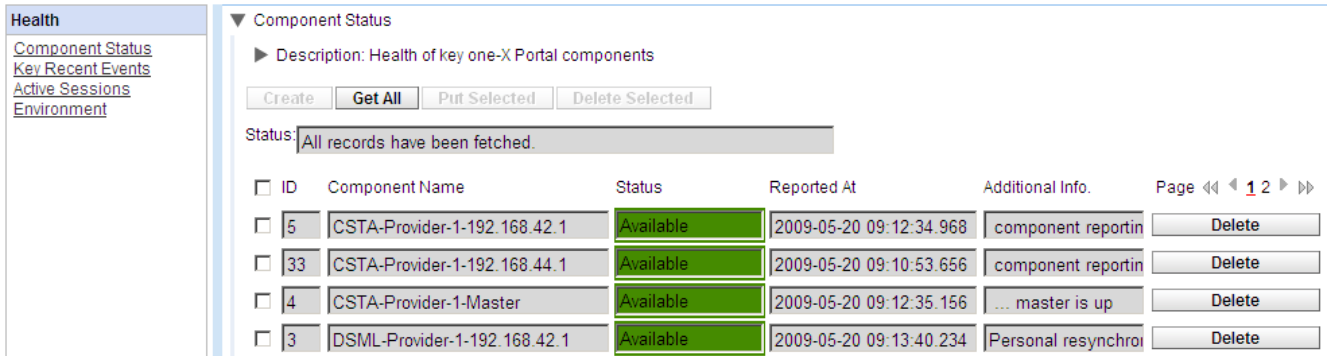
14. Repeat the process but this time adding the new IP Office to the IP Offices assigned to the **Default- DSML-IPO-Provider**. Again end with **Put Selected**.

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

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

Create **Get All** Put Selected Delete Selected

Status: All records have been fetched.

<input type="checkbox"/>	ID	Component Name	Status	Reported At	Additional Info.	Page << 1 2 >>
<input type="checkbox"/>	5	CSTA-Provider-1-192.168.42.1	Available	2009-05-20 09:12:34.968	component reportin	Delete
<input type="checkbox"/>	33	CSTA-Provider-1-192.168.44.1	Available	2009-05-20 09:10:53.656	component reportin	Delete
<input type="checkbox"/>	4	CSTA-Provider-1-Master	Available	2009-05-20 09:12:35.156	... master is up	Delete
<input type="checkbox"/>	3	DSML-Provider-1-192.168.42.1	Available	2009-05-20 09:13:40.234	Personal resynchro	Delete

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

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

3.3 Changing IP Office Details

If the details (IP address, TCPA service user name or password) of an assigned IP Office are changed, the IP Office settings within the one-X Portal 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 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 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 database.

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

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

Provider Editor

ID:

Name:

Data:

Provider Type Selector:

IP Office(s) Assigned

Mid-Layer URL:

Mid-Layer Username:

Mid-Layer Password:

Mid-Layer Password Hash:

Run On Port:

Created:

- 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
<input type="text" value="0"/>	<input type="text" value="192.168.42.1"/>	<input type="text"/>	<input type="password"/>

- Click **Close**.
- Click **Close** again.
- Click on **Put Selected**. This writes the new settings of the CSTA provider back to the one-X Portal database.
- 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**.
- 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](#)  option in the administrator menus.

Unlike the LDAP support in the IP Office, the one-X Portal sever does not import records from the LDAP source and then use those records as a directory. Instead, when a one-X Portal user enters characters in the External Directory tab of the Directory gadget, the one-X Portal server uses the LDAP source settings to do a live search of the LDAP source records. The one-X Portal 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 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 database.
4. Click on the **Edit** button next to the LDAP provider.
5. Click on **LDAP Server(s) Assigned**. This will list the LDAP source already assigned.

LDAP Server(s) assigned to Provider				
This control enables you to add & delete the LDAP Server(s) mapped to a provider. Changes apply to the local copy of the provider record & must be committed to take affect. Distribution of providers over several servers may be needed for effective performance. The factors are: server performance, IP Office utilisation & network latency.				
ID	LDAP Server URL	User	Password	Base DN
0	192.168.42.12	IPOffice	*****	
<input type="button" value="Edit Field Mapping"/> <input type="button" value="Delete"/>				
<input type="button" value="Close"/> <input type="button" value="Assign New LDAP Server"/>				

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

- **LDAP Server URL**

The URL of the LDAP directory source, for example *ldap://ldap.example.com*.

- **User/Password**


The user name and password for access to the LDAP server.

- **Base DN**

This is also called the **Search Base**. It defines which set of records in the LDAP source should be used for searches. The LDAP sever administrator will provide a suitable string, for example *ou=Users,dc=global,dc=example,ddc=com*.

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

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"/>
<input type="button" value="Close"/> <input type="button" value="Defaults"/>	

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](#) .

3.5 Adding/Deleting Users

The one-X Portal 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 after approximately 5 minutes.

3.6 Editing User Settings

Most of the settings set by one-X Portal users through their **Configuration** tab, for example **Profile** definitions, are stored as part of the one-X Portal database. As the one-X Portal 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	IP Office	Source/Storage
Personal Directory	✓	✓	<p>A user's personal directory is stored in the configuration of both one-X Portal 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 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 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 only. <ul style="list-style-type: none"> IP500/IP500 V2: 10800 total personal directory records. IP412: 3600 total personal directory records. IP406 V2: 1900 total personal directory records. For users with a 1608 or 1616 phone, they can edit or delete the contact 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 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.
Sound Configuration	✓	-	A user's one-X Portal sound preference is stored by one-X Portal.
Park Slots	✓	-	The park slot numbers used for a user's one-X Portal park buttons are stored by one-X Portal.

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.

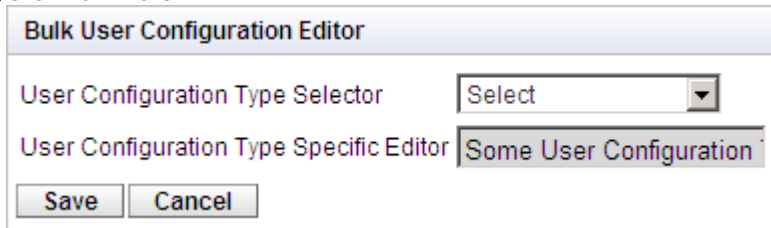
User Editor

ID	<input type="text" value="31"/>						
Name	<input type="text" value="Agent A"/>						
Unique Identifier	<input type="text" value="E115E100BA5E11D6A70"/>						
Display Name	<input type="text"/>						
Password	<input type="password" value="••••••••••"/>						
Password Hash	<input type="text" value="096A931191786EC72909f"/>						
User Configuration Type Selector	<input type="text" value="Presence"/> ▼						
My Status	<input type="text" value="Available"/> ▼						
User Configuration Type Specific Editor	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Name</th> <th style="width: 30%;">Type</th> <th style="width: 20%;">Number</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="text-align: center;">+ Add a new presence definition</td> </tr> </tbody> </table> <p>Do Not Disturb Exceptions</p>	Name	Type	Number	+ Add a new presence definition		
Name	Type	Number					
+ Add a new presence definition							
Created	<input type="text" value="2009-06-11 07:43:28.7180"/>						

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 database, select the check box next to the user and click on **Put Selected**.

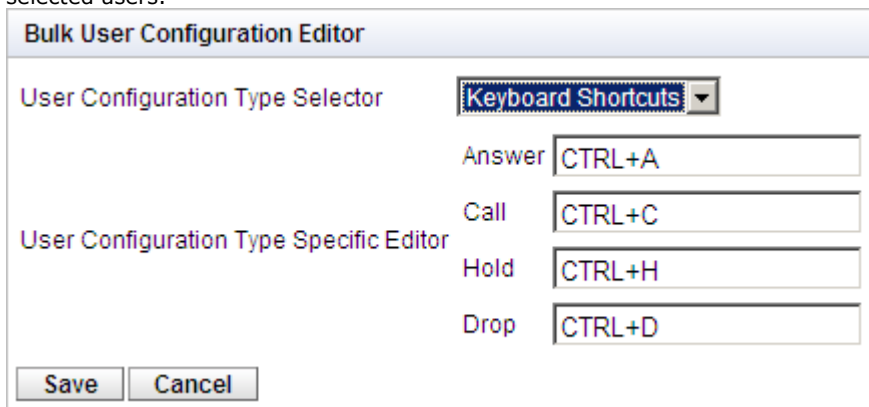
Bulk Editing

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" as its current value. The second is labeled "User Configuration Type Specific Editor" and has "Some User Configuration" as its current value. At the bottom of the dialog are two buttons: "Save" and "Cancel".

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



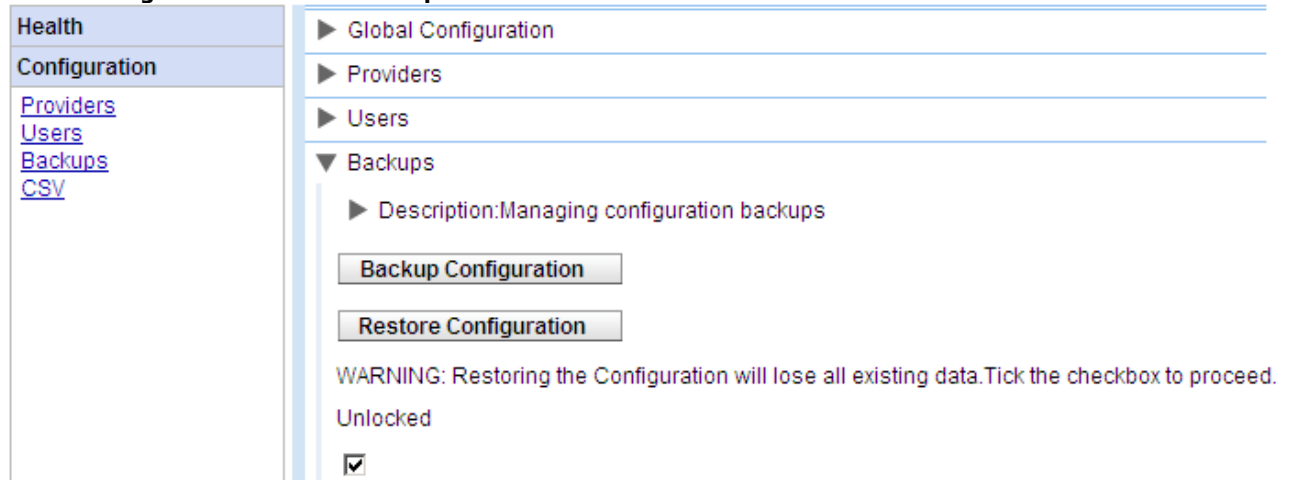
The dialog box is titled "Bulk User Configuration Editor". The "User Configuration Type Selector" dropdown is now set to "Keyboard Shortcuts". Underneath, the "User Configuration Type Specific Editor" section has four sub-sections, each with a text input field: "Answer" with "CTRL+A", "Call" with "CTRL+C",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

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

3.7 Backing Up the Database

You can backup the one-X Portal database of settings. The resulting file can be [restored](#) if necessary.

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

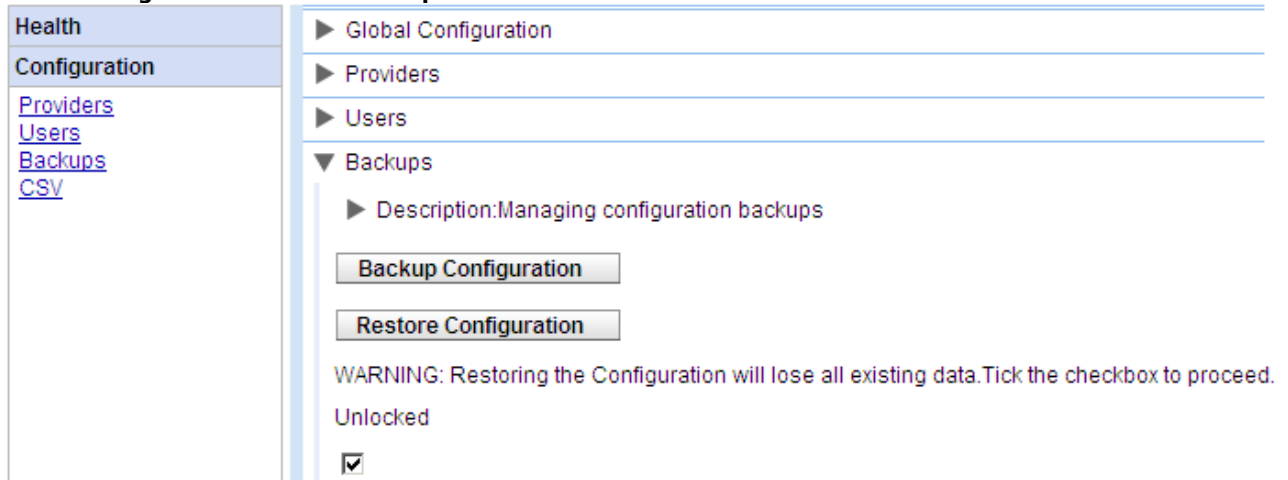


2. Click on **Backup Configuration**.
3. The configuration is backed up as **backup.sql** in the bin folder of the one-X Portal application (default C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\bin\backup.sql).

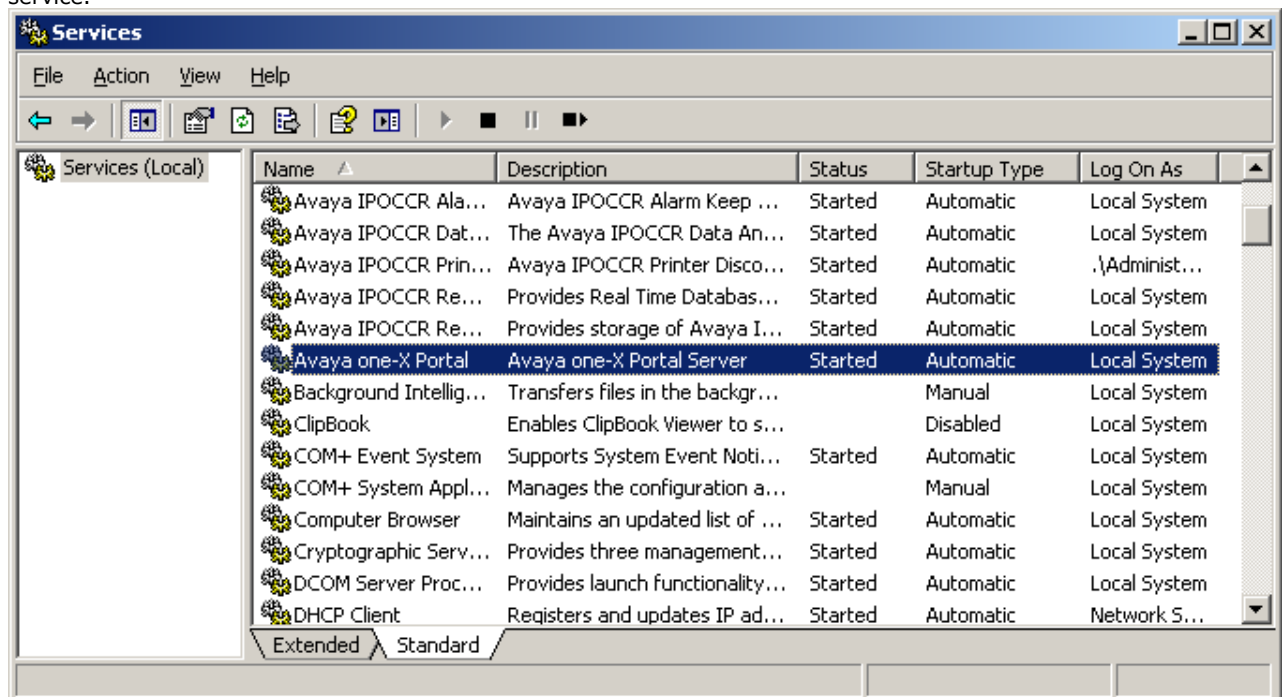
3.8 Restoring a Previous Backup

This process will override the current one-X Portal configuration. It needs to be followed by a restart of the one-X Portal service. It requires the one-X Portal 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 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 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 server service.



3.9 Checking and Updating the System Directory

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

By default, the one-X Portal application updates the system directory records every 300 seconds approximately. Through the one-X Portal 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 users.

1. Select **Directory Integration**.
2. Select **System Directory**. The current system directory is shown. Check that the entries are as expected.

The screenshot shows the 'System Directory' view. On the left, a navigation menu includes 'Health', 'Configuration', 'Diagnostics', 'Directory Integration', 'Directory Synchronisation', 'System Directory', and 'LDAP Directory Search'. The 'System Directory' is selected. The main content area is titled 'Directory Synchronisation' and contains a section for 'System Directory'. This section displays a list of users in two columns: Alec Creed, Andy Ertle Sip, Ashley Walton, AWaltonIP, BradSIP, BradT, Bract, Dave H V5, Emma Potter, Ernesto 8579, Extn1234, Extn1860, Extn3205, Geoff Froud, Graham Richards, and Imerio IP. Below the list is a search bar with the text 'Enter a name' and a plus icon. At the bottom right of the search area are navigation arrows and the number '12'.


3. If you feel that an update is required, select **Directory Synchronization**.

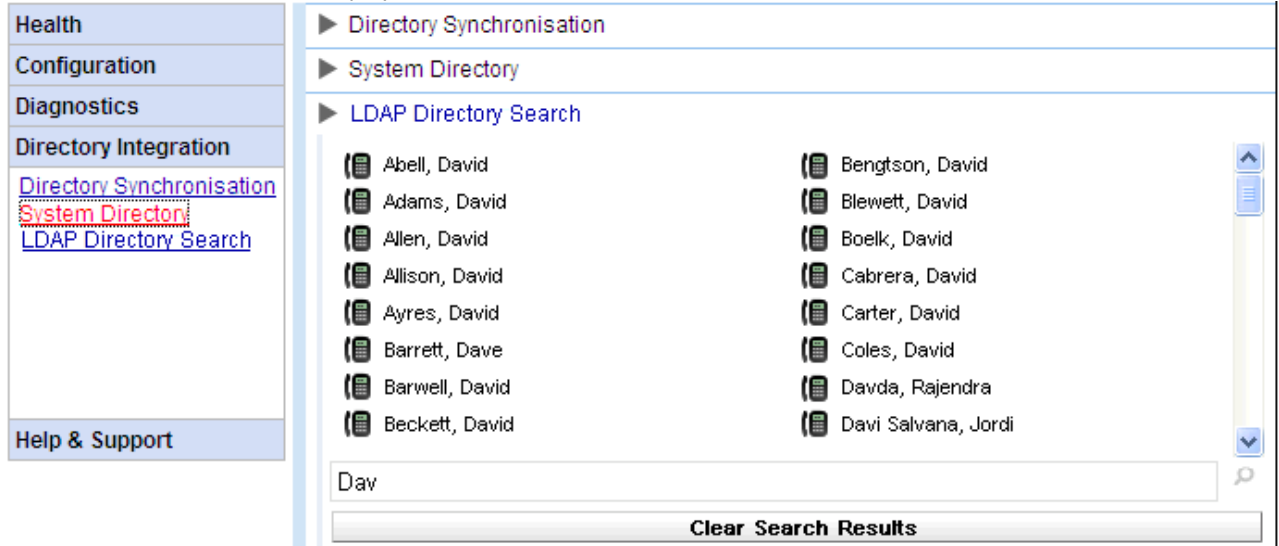
The screenshot shows the 'Directory Synchronization' view. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Directory Synchronisation' and contains a section for 'Description: Forcing Directory Cache Update'. Below the description are two buttons: 'Force a Resynchronisation with IP Office User Lists' and 'Force a Resynchronisation with IP Office Directories'.

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

3.10 Checking the External LDAP Directory

If you have configured an LDAP external directory source, access to it by one-X Portal 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.



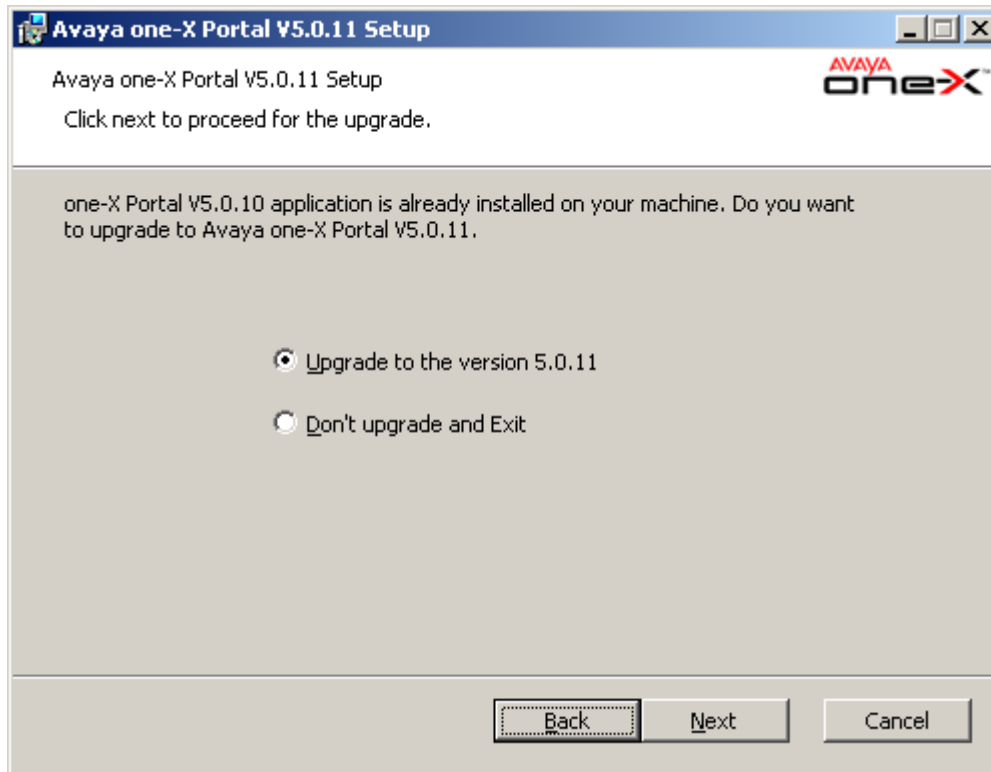
3.11 Upgrading one-X Portal

Before upgrading one-X Portal ensure that you have read the Avaya IP Office Technical Bulletin for the release of one-X Portal 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.

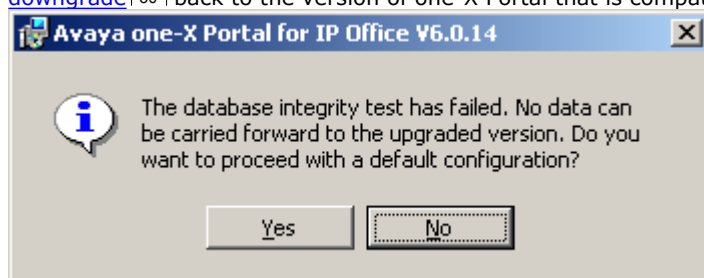
If one-X Portal is already installed on a server PC and the installation file for a later version is run, the existing version will be detected and you will be prompted whether to upgrade or not. If you select to upgrade, the process is similar to normal software installation, however some installation 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 will not be available to all users for up to 15 minutes.



- If the existing one-X Portal database cannot be upgraded a warning will be displayed. If you select Yes, the existing database is replaced with a defaulted database. If you select No you will need to rerun the installer in order to [downgrade](#) back to the version of one-X Portal 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 system and should not be used for restoration of setting. Refer to [Backing Up the Database](#) for details of creating a full backup.

3.12 Downgrading one-X Portal

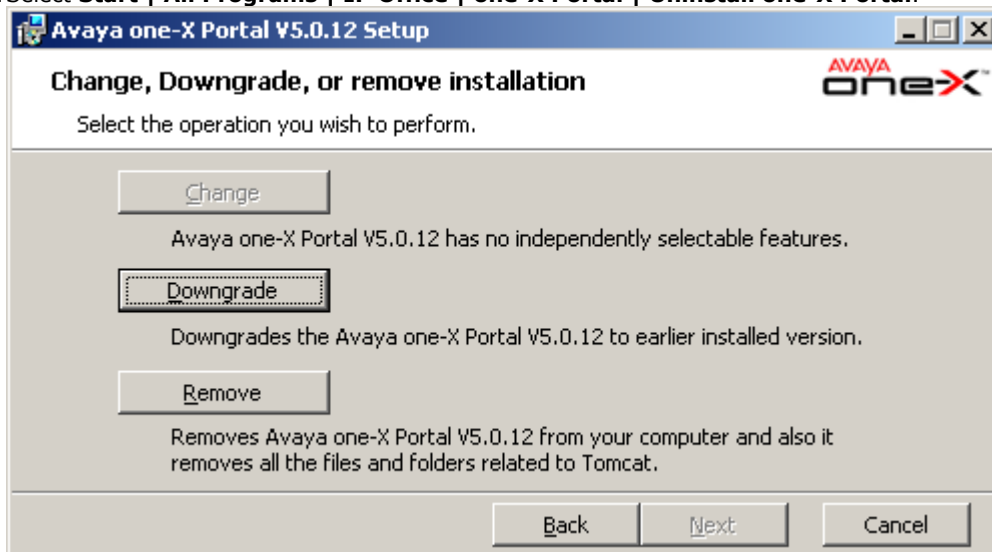
If the one-X Portal application software has been upgraded using the [upgrade process](#)^[49], it is also possible to downgrade back to the [original installed](#) version.

- **Note:** The installation of one-X Portal and the last upgrade to one-X Portal 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.

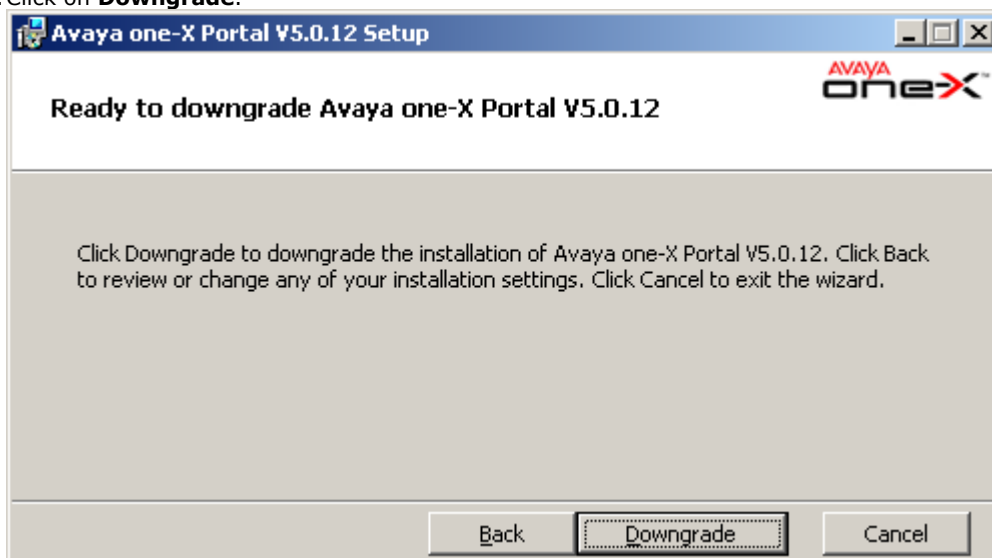
Before downgrading one-X Portal ensure that you have read the Avaya IP Office Technical Bulletin for the one-X Portal software releases. The Technical Bulletin will include details of any special requirements and additional steps that may not be in this documentation.

- **Warning**
This process requires the Avaya one-X Portal service to be restarted. During the restart one-X Portal 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](#)^[35].

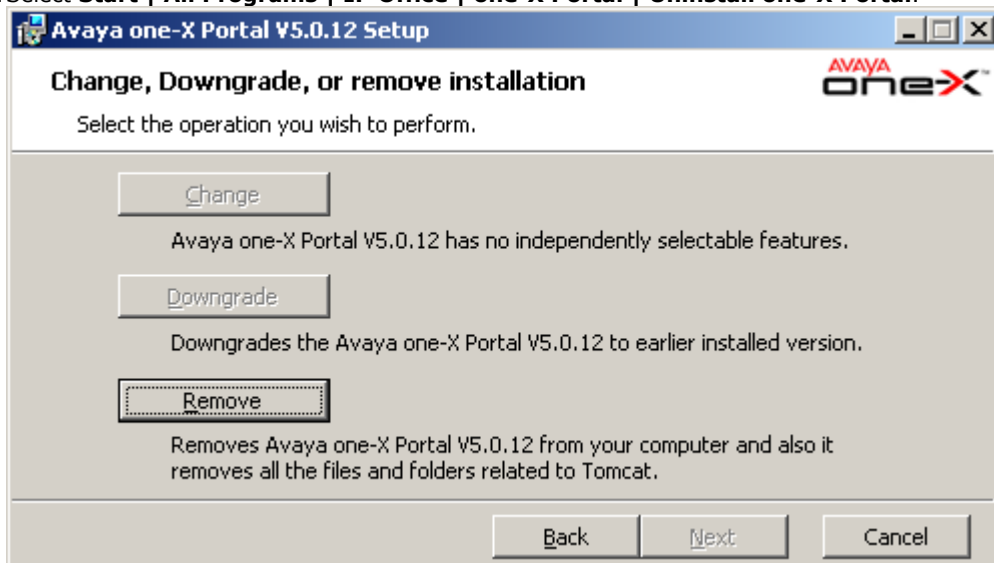
3.13 Removing one-X Portal

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

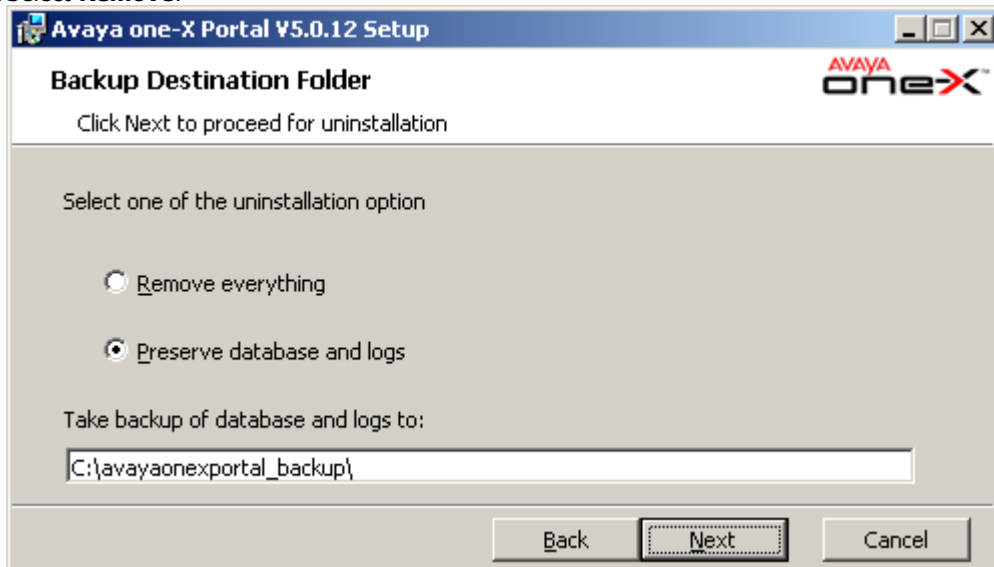
Uninstalling one-X Portal

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

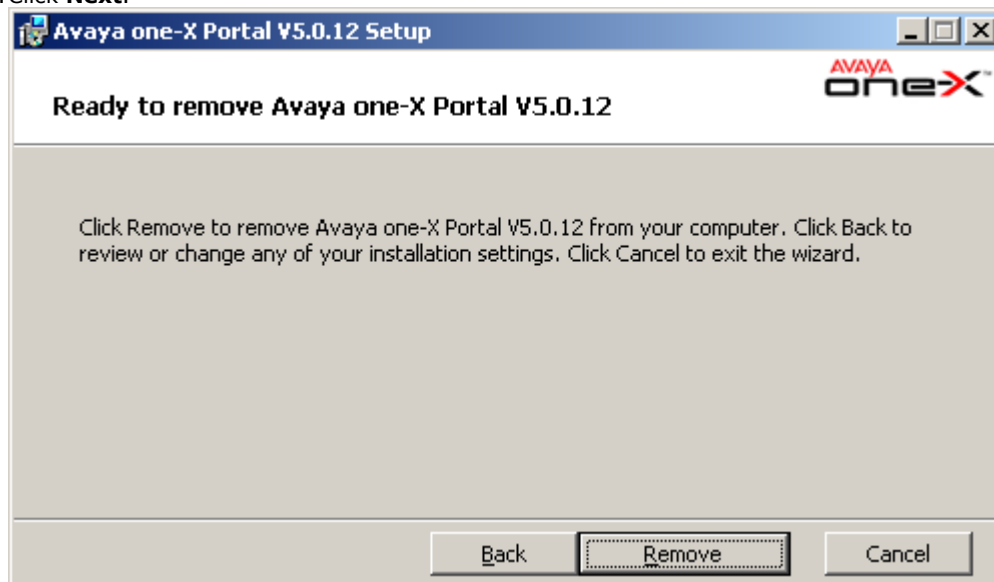
1. Select **Start | All Programs | IP Office | one-X Portal | Uninstall one-X Portal**.



2. Select **Remove**.



3. Click **Next**.



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

Removing one-X Portal via the Control Panel

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

1. Start the standard Windows Control Panel.
2. Select **Add or Remove Programs**.
3. Select **one-X Portal** and then click **Remove**.
 - If the one-X Portal has been upgraded at some stage, there will be a program entry for both the original one-X Portal 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 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 server administrator interface includes links to install Apache Chainsaw.

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

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

Logging Configuration

▼ Master Logging Level

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

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

ALL

▼ Logging Targets(Rolling Log Files)

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

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

Rolling log files reflect the master logging level.

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

▼ Logging Targets(Server and Network)

Socket Receiver(required for remote log viewing)

Enabled

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

3. Select **Logging Viewer**.

► Logging Configuration

▼ Logging Viewer

► Description: Remotely viewing logs.

[More information about Apache Chainsaw.](#)

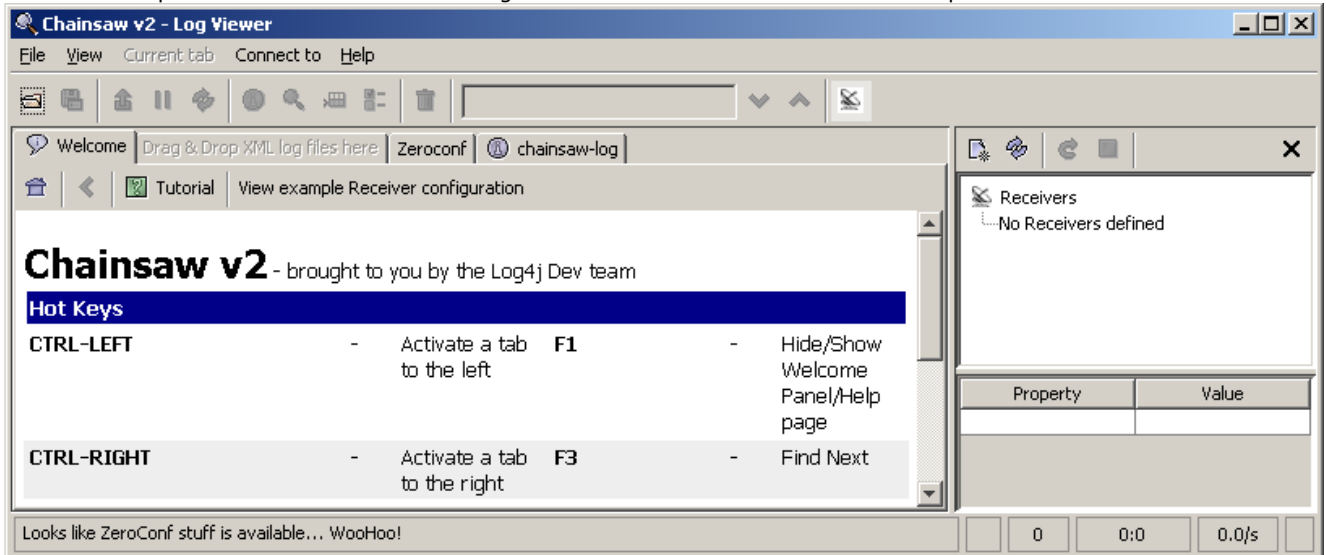
[Start Installation of Apache Chainsaw by Java Web Start](#)

► Network Routes

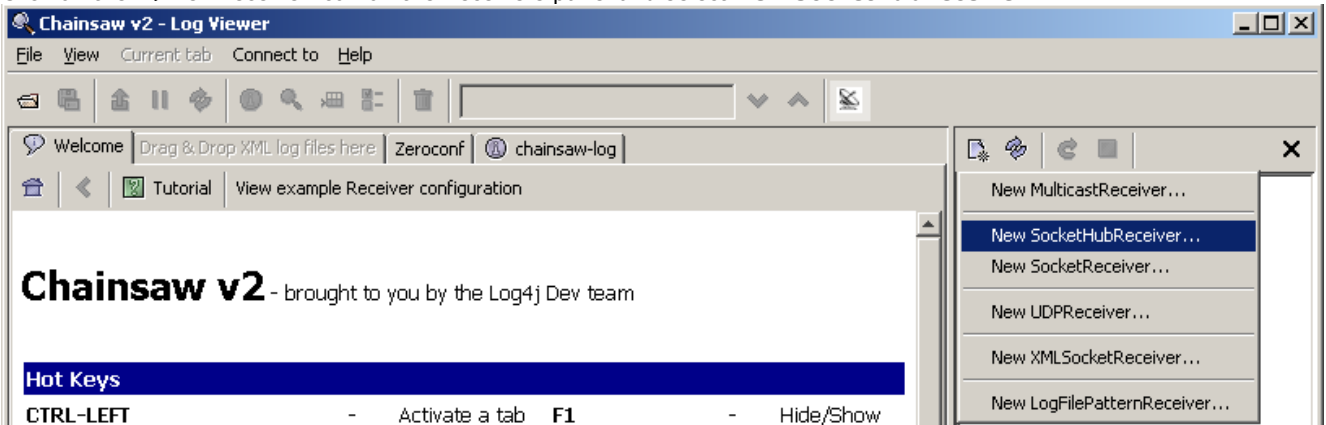
4. Click on **Start Installation of Apache Chainsaw by Java Web Start**.

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

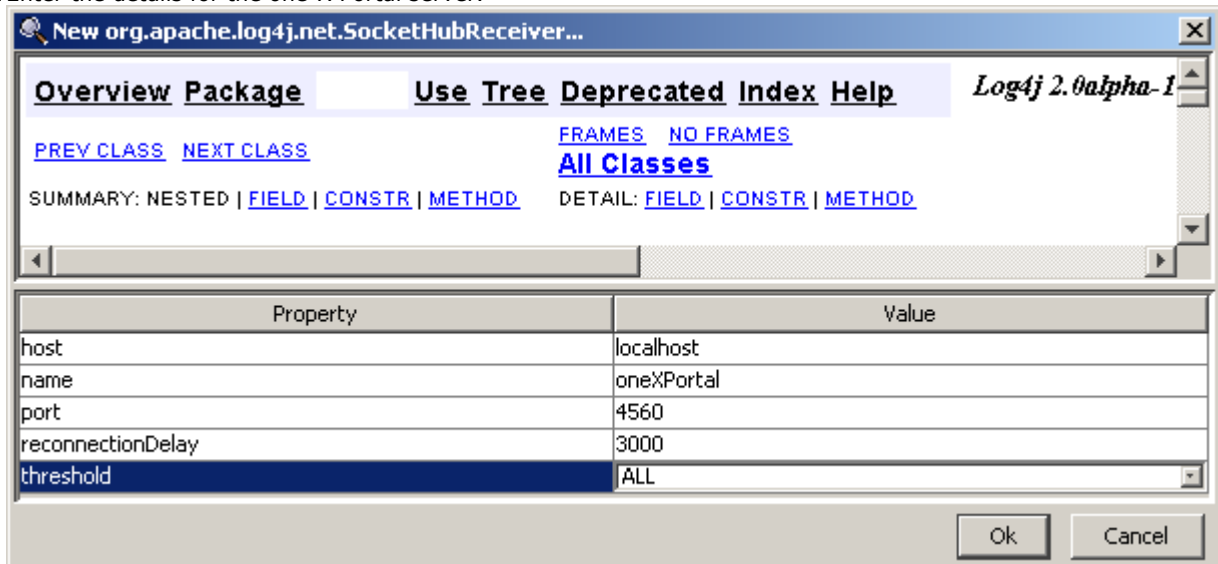
6. The Receivers panel should be visible on the right. If not click on the  button in the top toolbar.



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

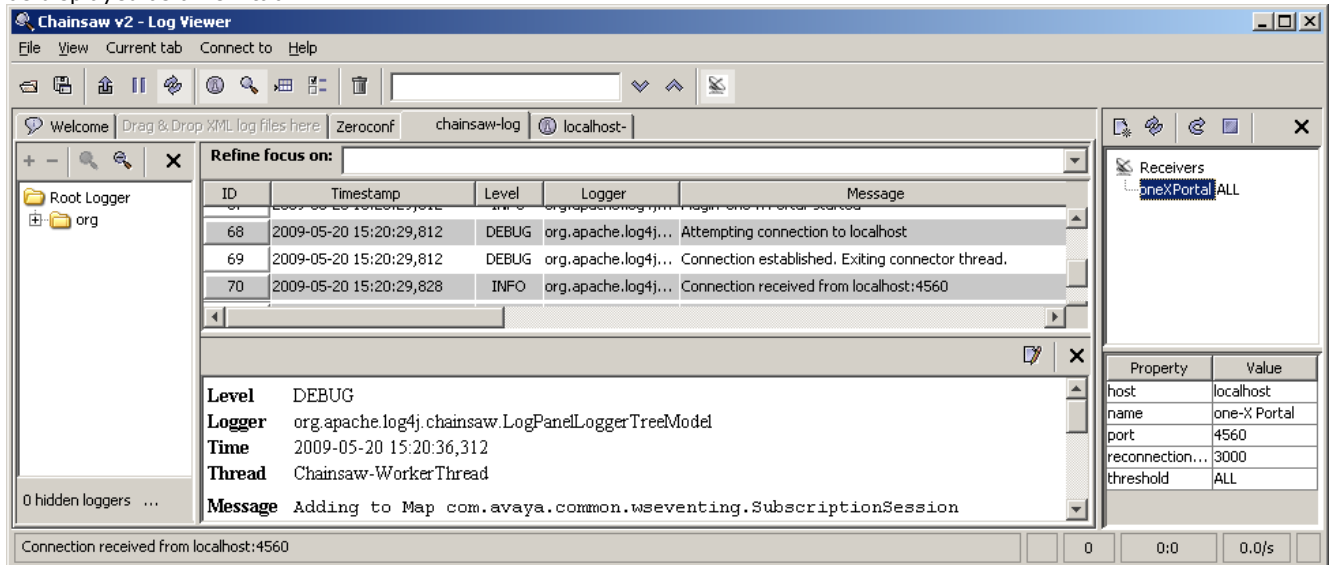


8. Enter the details for the one-X Portal server.

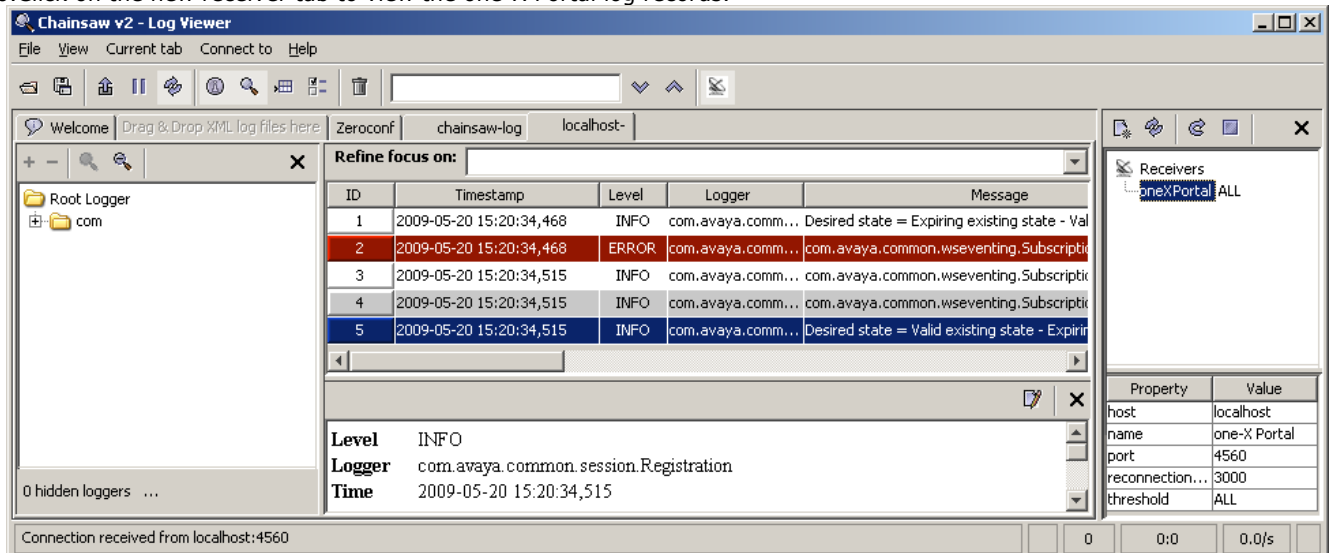


host	This field sets the address of the one-X Portal server. In the example above chainsaw is being run on the one-X Portal server PC.
name	This field is for display only. Enter a name for the receiver entry in Chainsaw.
port	Set this to 4560. This is the port to which one-X Portal outputs log records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

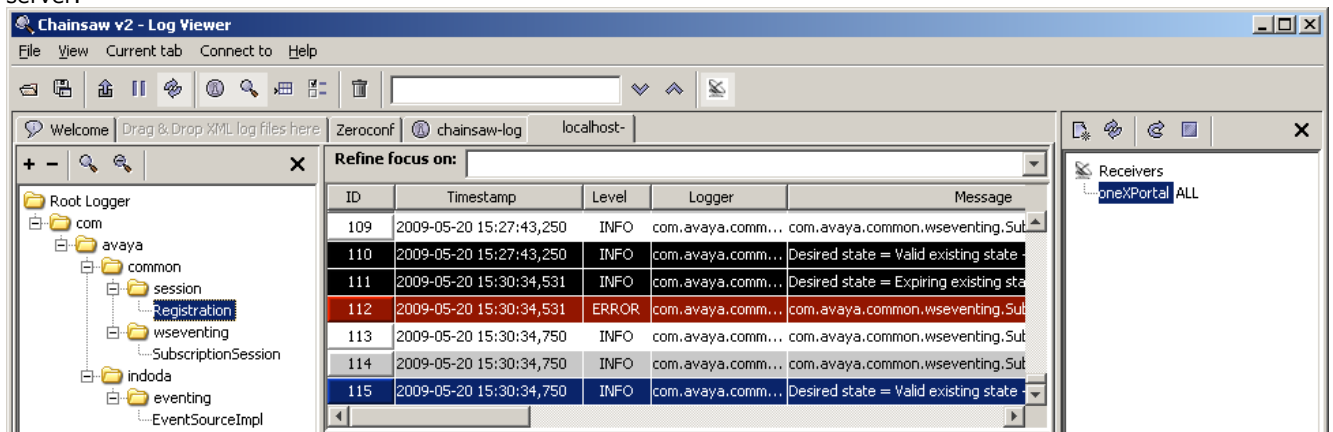
9. When you have completed the fields, click OK. After a few seconds the receiver should start and connect to the one-X Portal server. The process will appear as log events on the chainsaw-log tab and when completed the receiver will be displayed as a new tab.





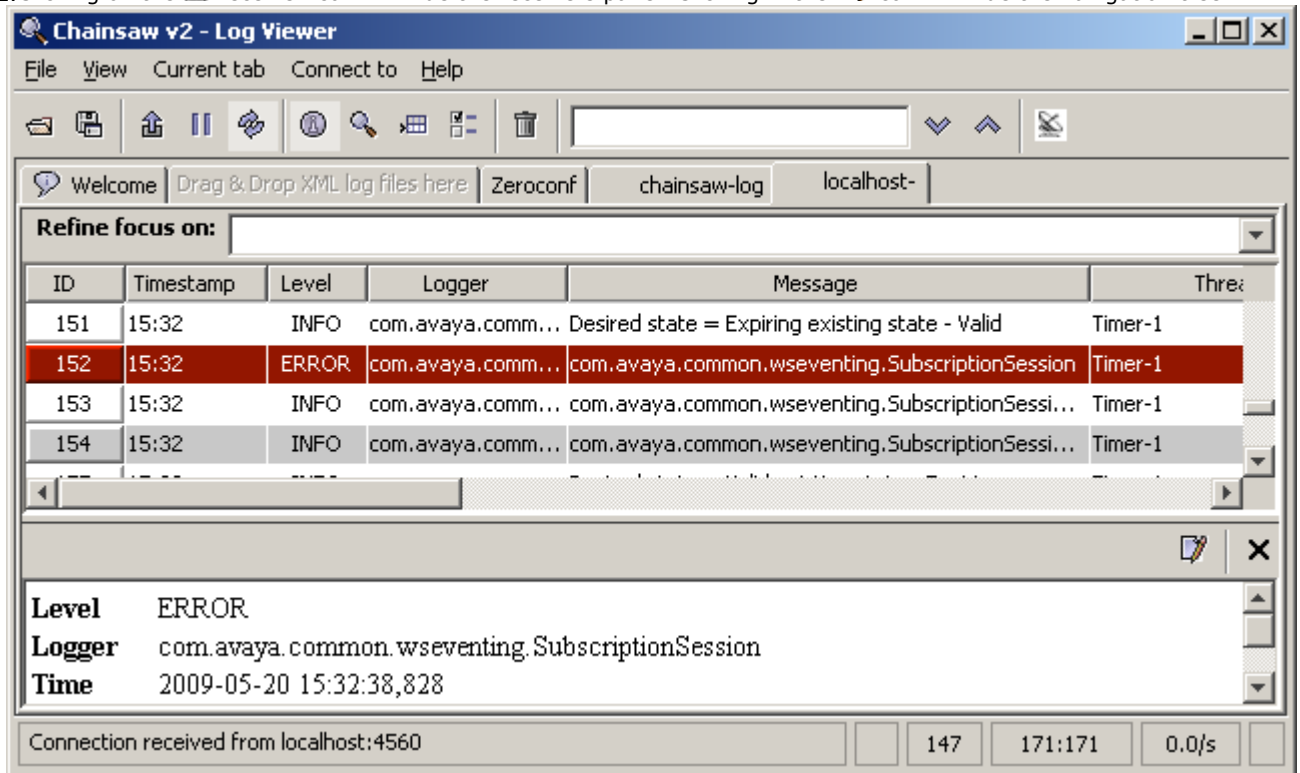
10. Click on the new receiver tab to view the one-X Portal log records.



11. The navigation tree on the left can be used to focus the log view onto a particular component of one-X Portal 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 has a "Refine focus on:" search bar and a table of log entries. The table has columns for ID, Timestamp, Level, Logger, Message, and Thread. Row 152 is highlighted in red, indicating an error. Below the table, a detailed view of the selected log entry is shown, including its Level (ERROR), Logger (com.avaya.common.wseventing.SubscriptionSession), and Time (2009-05-20 15:32:38,828). At the bottom, a status bar shows "Connection received from localhost:4560" and some statistics.

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

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

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

3.15 Troubleshooting

Version Mismatch Problem

Symptoms	<ul style="list-style-type: none"> • Database integrity check fails. • When starting one-X Portal, the version shown on the login page is the previous version and differs from that reported by Windows (Start Programs IP Office Avaya one-X Portal for IP Office Uninstall Vx.XX) menu.
Cause	Normally the one-X Portal installer will automatically stop any Tomcat web server associated with a previous installation of one-X Portal. However it has been found that it in some cases it fails to stop the Tomcat server but will still report successful completion of the installation process. This leads to a version mismatch between components.
Resolution	<ol style="list-style-type: none"> 1. Remove one-X Portal. 2. Manually delete the one-X Portal 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.

one-X Portal Does Not Start

Symptoms	<ul style="list-style-type: none"> • one-X Portal 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. Using the Windows Add or Remove Programs applet, remove Java. 2. Remove one-X Portal. 3. Install one-X Portal.

Chapter 4.

Administration

4. Administration

The one-X Portal administration menu provides a range of options for monitoring and configuring the one-X Portal application.

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

It is important to understand that the one-X Portal 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.

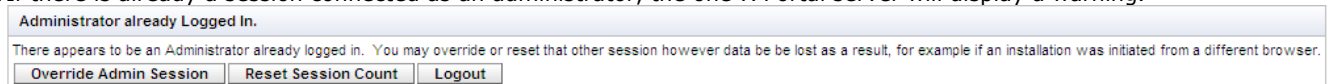
4.1 Login

Access to the administration menus for one-X Portal 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 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 software installation](#) (the default is 8080).
2. The one-X Portal login menu should be displayed.



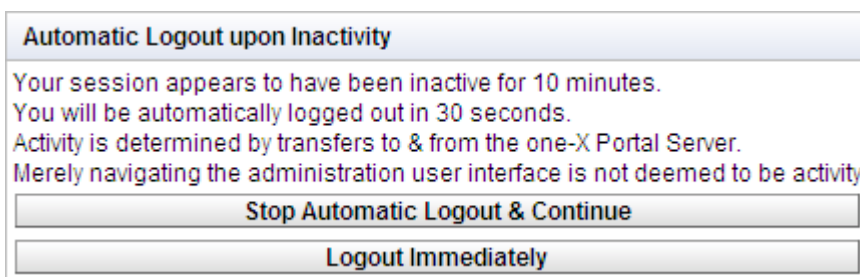
3. Enter the one-X Portal administrator name and password as configured during installation.
4. If there is already a session connected as an administrator, the one-X Portal server will display a warning.



4.2 Logout

The **Logout** option at the top right of the one-X Portal 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.

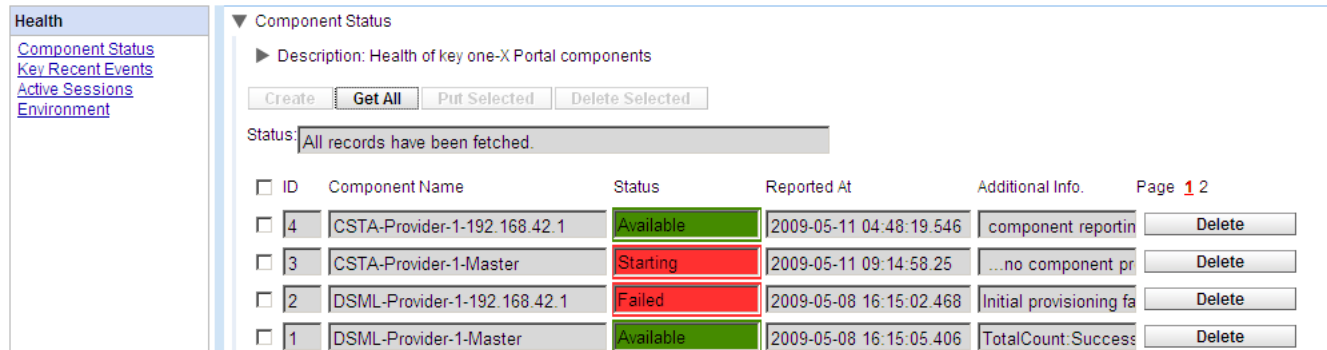


4.3 Health

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 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.

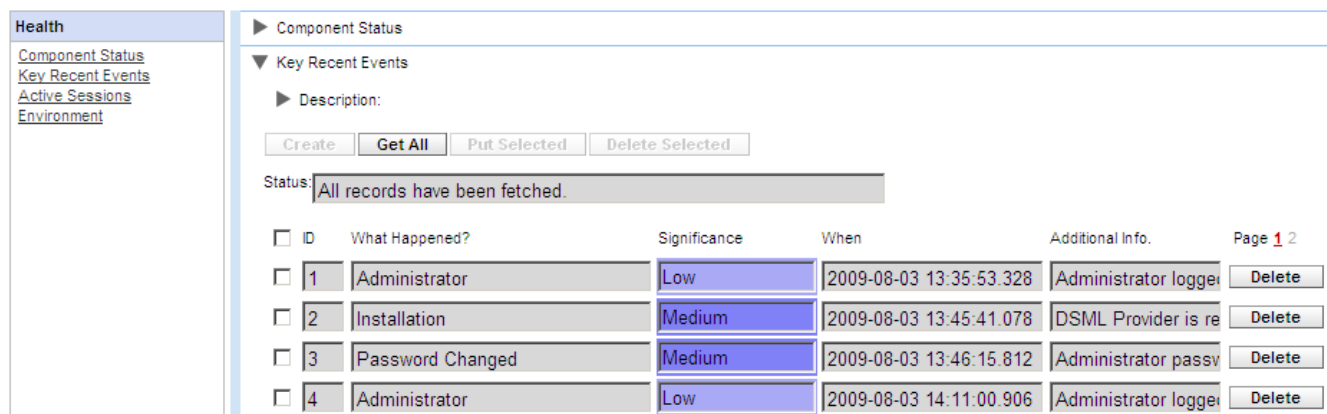


ID	Component Name	Status	Reported At	Additional Info.	Page 1 2
<input type="checkbox"/> 4	CSTA-Provider-1-192.168.42.1	Available	2009-05-11 04:48:19.546	component reportin	Delete
<input type="checkbox"/> 3	CSTA-Provider-1-Master	Starting	2009-05-11 09:14:58.25	...no component pr	Delete
<input type="checkbox"/> 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 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 application. These can be actions performed by the one-X Portal service and also administration actions such as administrator log in/log out, administrator password changes, provider changes, and configuration restorations.



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**.
2. Click **Get All** to retrieve the event records from the one-X Portal 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 server.

The screenshot shows the 'Health' menu on the left with 'Active Sessions' selected. The main content area shows 'Component Status', 'Key Recent Events', and 'Active Sessions'. Under 'Active Sessions', there is a description 'one-X Portal for IP Office Utilisation' and a 'Refresh' button. Below this is a table with four columns: Total, User, Administrator, and Application. The values are 3, 0, 1, and 2 respectively.

Total	User	Administrator	Application
3	0	1	2

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

4.3.4 Environment

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

The screenshot shows the 'Health' menu on the left with 'Environment' selected. The main content area shows 'Component Status', 'Key Recent Events', 'Active Sessions', and 'Environment'. Under 'Environment', there is a description 'Server Information' and a 'Refresh' button. Below this is a table with various server information fields and their values.

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 server.

The screenshot displays the 'Providers' configuration page. On the left, a navigation menu includes 'Health', 'Configuration', 'Providers', 'Users', 'Backups', and 'CSV'. The main content area is titled 'Global Configuration' and 'Providers'. It features 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 shows 'All records have been fetched.' Below this is a table of providers with checkboxes, ID, Name, Edit, and Delete buttons. The table is paginated to show page 1 of 1.

<input type="checkbox"/>	ID	Name		Page
<input type="checkbox"/>	4	Default-DSML-LDAP-Provi	Edit Delete	1
<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, one provider of each type is created. The Providers menu allows editing of which IP Offices and LDAP servers are assigned to the providers.

4.4.1.1 Telephony (CSTA) Provider

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

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

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

IP Office(s) assigned to Provider			
This control enables you to add & delete the IP Office Unit(s) mapped to a provider.			
Changes apply to the local copy of the provider record & must be committed to take affect.			
Up to 32 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.			
Distribution of providers over several servers may be needed for effective performance.			
The factors are: server performance, IP Office utilisation & network latency.			
ID	IP Address	User	Password
0	192.168.42.1		
			<input type="button" value="Delete"/>
<input type="button" value="Close"/>		<input type="button" value="Assign New IP Office Unit"/>	

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

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.

Provider Editor

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

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

IP Office(s) assigned to Provider

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

ID	IP Address	User	Password	
<input type="text" value="0"/>	<input type="text" value="192.168.42.1"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>
<input type="button" value="Close"/> <input type="button" value="Assign New IP Office Unit"/>				

The **User** and **Password** details used must match the TCPA service user configured in the IP Office system's [security configuration settings](#) ⁽¹⁷⁾.

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 directory display fields.

LDAP Server(s) assigned to Provider

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

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

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

LDAP Field Mappings

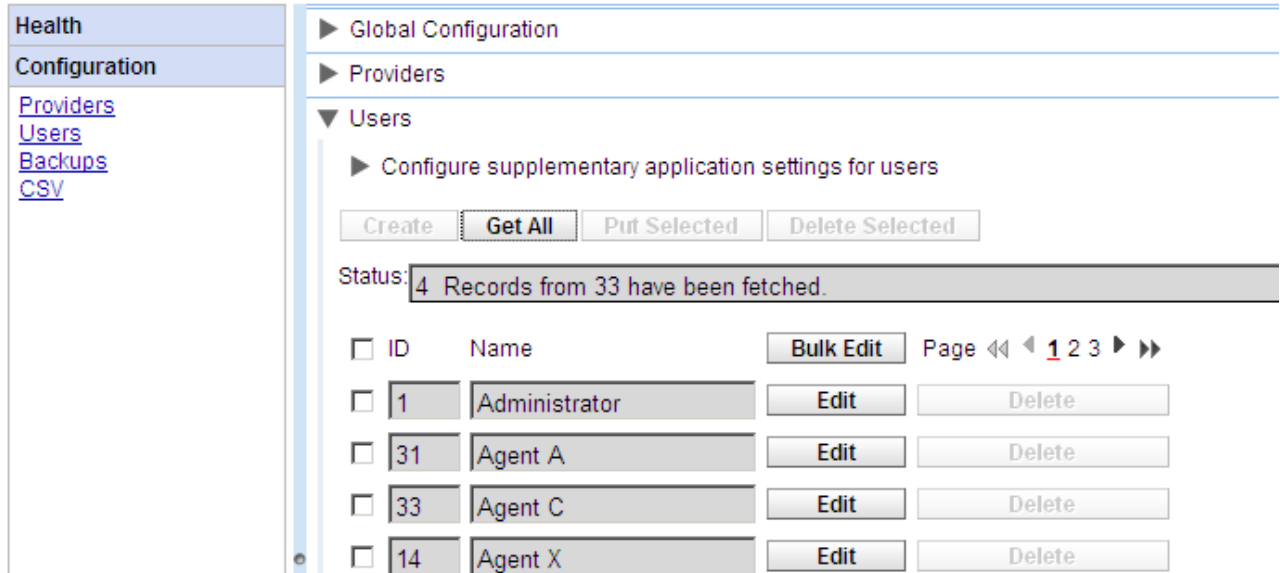
FIRSTNAME	<input type="text" value="givenName"/>
LASTNAME	<input type="text" value="sn"/>
WORKPHONE	<input type="text" value="telephoneNumber"/>
HOMEPHONE	<input type="text" value="homePhone"/>
OTHERPHONE	<input type="text" value="cel"/>
WORKEMAIL	<input type="text" value="mail"/>
PERSONALEMAIL	<input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

The menu can be used to edit users. The settings that can be edited are those available to a user through the **Configuration** tab when they access one-X Portal using a browser (except DND Exceptions). Other user settings and information (for example call logs) are stored by the IP Office system, not by the one-X Portal database.

1. Select **Configuration** and then **Users**.
2. Click on **Get All**.



<input type="checkbox"/>	ID	Name	Bulk Edit	Page	◀	1	2	3	▶	▶▶
<input type="checkbox"/>	1	Administrator	Edit							
<input type="checkbox"/>	31	Agent A	Edit							
<input type="checkbox"/>	33	Agent C	Edit							
<input type="checkbox"/>	14	Agent X	Edit							

3. Browse through the users.

If you think that the user records do not match the users configured on the IP Office systems, the [Directory Integration | Directory Synchronization](#) ⁷³ menu can be used to force an update from the IP Office systems.

4.4.3 Backups

This menu provided options to [backup](#)^[45] the one-X Portal configuration. It can also be used to [restore](#)^[46] a previous backed up configuration.

The screenshot shows the configuration interface with a left-hand navigation menu containing 'Health', 'Configuration', 'Providers', 'Users', 'Backups', and 'CSV'. The main content area is titled 'Global Configuration' and includes sub-sections for 'Providers', 'Users', and 'Backups'. Under 'Backups', there is a description: 'Description: Managing configuration backups'. Below this are two buttons: 'Backup Configuration' and 'Restore Configuration'. A warning message states: 'WARNING: Restoring the Configuration will lose all existing data. Tick the checkbox to proceed.' Below the warning, the text 'Unlocked' is displayed, followed by a checked checkbox.

4.4.4 CSV

This menu allows you to export the user information and system directories being used by the one-X Portal server to .csv format files. The files are exported to the **/bin** sub-folder of the application directory (by default **C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\bin**). Any existing file is overwritten.

The screenshot shows the configuration interface with the left-hand navigation menu. The main content area is titled 'Global Configuration' and includes sub-sections for 'Providers', 'Users', 'Backups', 'Reset', and 'CSV'. Under 'CSV', there is a description: 'A control for exporting the user list and directory as a CSV file. CSV import is not supported. The exported filenames are hardcoded as exportUser.csv & exportDirectoryEntry.csv. These get written to the underlying Tomcat/bin folder.' Below this text is a button labeled 'Export Configuration'.

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**

4.5 Diagnostics

4.5.1 Logging Configuration

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

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

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 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 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](#)^[53] 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 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](#)^[72] 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 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 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

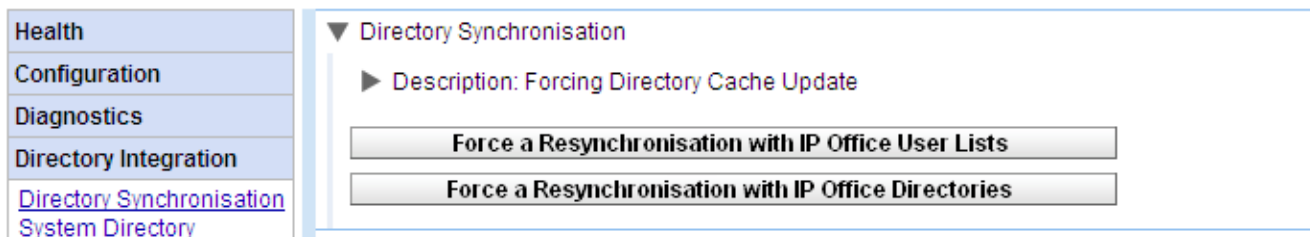
This menu can be used to check the database structure. It will return **Pass** if the tables and fields within the database are as expected for the particular version of one-X Portal. It does not check the data within the fields. If **Fail** is reported refer to the [Troubleshooting](#) section for known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

Expected Result	Calculated Result	Result
D26D2C06BD65B000B508D09BB1	D26D2C06BD65B000B508D09BB1	Pass

4.6 Directory Integration

4.6.1 Directory Synchronisation

During normal operation, the one-X Portal 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/or IP Office users.



- Force a Resynchronization with IP Office User Lists**
 Requests an update of the IP Office users configured on the IP Office systems. The user can be viewed through the [Providers | Users](#) option.
- 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 users. You can search the directory in the same way as if you were using the one-X Portal 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 server updates system and personal directory records every 300 seconds approximately. If necessary you can force an update using the [Directory Synchronization](#) ^[73] option.


- For some directory contacts, one-X Portal can indicate the contacts current status by using different icons. For contacts that have multiple telephone numbers, the status is based that of the work number.

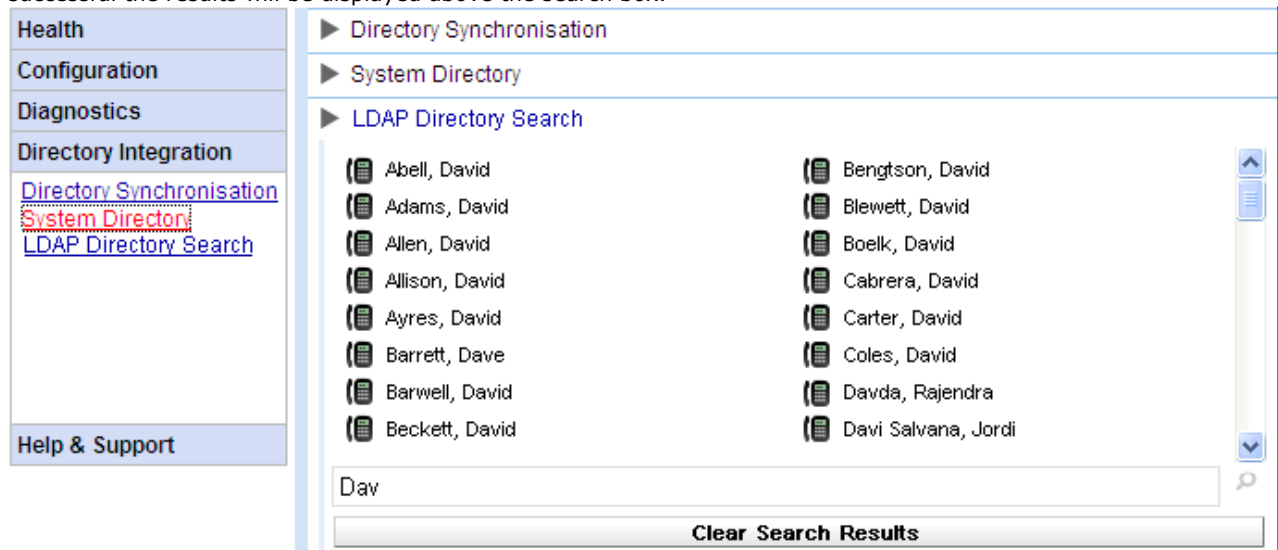
State	Icon	Description
Available		The normal state for a user showing that their work extension is not in use.
Busy		The normal state for a user showing that their work extension is currently on a call.
Do Not Disturb		The user has set Do Not Disturb . Calls to them will go to voicemail if enabled or 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.

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 only and are accessible by users through one-X Portal 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 users. This allows you to test the operation of the [LDAP Provider](#)^[41].

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 displays the LDAP Directory Search interface. On the left, a navigation menu includes 'Health', 'Configuration', 'Diagnostics', 'Directory Integration', and 'Help & Support'. Under 'Directory Integration', the following options are listed: 'Directory Synchronisation', 'System Director', and 'LDAP Directory Search'. The 'LDAP Directory Search' option is selected and expanded, showing a list of names in two columns:

Abell, David	Bengtson, David
Adams, David	Blewett, David
Allen, David	Boelk, David
Allison, David	Cabrera, David
Ayres, David	Carter, David
Barrett, Dave	Coles, David
Barwell, David	Davda, Rajendra
Beckett, David	Davi Salvana, Jordi

Below the list is a search box containing the text 'Dav' and a magnifying glass icon. A 'Clear Search Results' button is located at the bottom of the search area.

4.7 Help & Support

Help | Help

Provides links to both the one-X Portal 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 installation.



The screenshot displays 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 Help & Support, there are links for Help, Avaya Support, and About. The main content area shows a tree view with 'Help', 'Avaya Support', and 'About' expanded. The 'About' section contains a text box with the following text: 'Avaya one-X Portal for IP Office', 'Copyright 2009 Avaya Inc. All Rights Reserved.', and 'Version: 5.0.25.1419'. Below this text box, there is a link to the licenses of the third-party software components used in one-X Portal for IP Office, followed by a list of 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.

Glossary

5. Glossary

CSTA - Computer Supported Telecommunications Application.

Indoda - The Zulu word for 'man'.

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 53

8

8080 22

A

About 60

Active Sessions 60, 63

Add

IP Office 36

LDAP 41

Licenses 19

User 42

Administrator

Help 76

Login 25

Name 61

Advanced 31

Apache

Chainsaw 53, 71

Applications DVD 15

Assign

IP Office 36, 39

IP Office (CSTA) 65

IP Office (Directory) 66

LDAP Provider 67

Providers 64

Automatic logout 61

Avaya Support 60

B

Backup 45, 69

Restore 46

Backups 60

Base DN 41

browser 15

Bulk Edit 42, 68

User 42

C

Call Log 42

Chainsaw 53, 71

Component Status 60, 62

Computer Supported Telecommunications Application 78

Configuration 60

Backup 45

Backups 69

Bulk Edit 42

CSV 69

During installation 25

Export 69

Providers 64

Restore 46, 69

User 20

Users 68

Control Panel 51

Cookies 15

CSTA 65, 78

CSTA (IP Office) Provider 65

CSV 60, 69

D

Database

Backup 45, 69

Check 72

Restore 46, 69

Sanity Check 72

Database Integrity 60

Deinstall 51

Delete

IP Office 39

User 42

Diagnostics 60

Connections 72

Database Integrity 72

IP Office Connections 72

Logging Configuration 53, 70

Logging Viewer 53, 71

Network Routes 71

Directories 9

Directory

Export 69

Resynch 47, 73

Directory (DSML IP Office) 66

Directory (DSML LDAP) 67

Directory DSML IP Office Provider 8

Directory DSML LDAP Provider 8

Directory Integration 60

Directory Synchronization 47, 73

Directory Intergration

LDAP 48, 75

System Directory 47, 74

Directory Search

LDAP 48, 75

System Directory 47, 74

Directory Synchronization 60

DND Exceptions 42

Downgrading 50

DSML (IP Office) Provider 66

DSML (LDAP) Provider 67

DVD 15

E

Echo 71

Edit

Bulk Edit 42

IP Office Security Settings 17

IP Office settings 39

User settings 42, 68

Enable one-X Portal Services 20

Enhanced TSPI 17

Enhanced TSPI Access 17

Enhanced TSPI service 17

EnhTcpaService 17

Environment 60

Events 62

Exceptions 42

Explorer 15

Export Configuration 69

exportDirectoryEntry.csv 69

exportUser.csv 69

External Directory 9

Search 48, 75

F

Field Mapping 41, 67

Firefox 15

Firewall 15, 22

Force a Resynchronization 47, 73

H

Hard Disk 15

Health 60

Active Sessions 63

Health 60
 Component Status 62
 Environment 63
 Key Recent Events 62
Help 60
 About 76
 Avaya Support 76
 Help 76
I
Immediate logout 61
Initial configuration 25
Install
 Software 23
Installation
 Advanced 31
Internet Explorer 15
IP Office
 Applications DVD 15
 Check 25
 Connections 60
 CSTA Provider 65
 Directory Provider 66
 License 19
 Security Settings 17
 Select 25
 System Requirements 15
 User configuration 20

J
Java Web Start 53
JavaScript 15
K
Key Recent Events 60, 62
Keyboard Shortcuts 42

L
LDAP
 Assign 41
 Directory Search 48, 60, 75
 Provider 67
License
 Add 19
Listing Ports 22
Log Files 70
Log4j format 53
Logging 53
 Configuration 60
 Level 70
 Targets 70
 Viewer 53, 60
Logging Configuration 53
Login 29, 61
 Administrator 25
Logout 61

M
Maintenance 34
Master Logging Level 70
Messages 42
Mozilla Firefox 15

N
Name 20
Network Routes 60, 71
Not Reachable 71

O
Operating System 15
Override Admin Session 61

P
Park Slots 42
Password 20, 61
 Change 25
Personal Directory 9, 42
PING 71
Port 15
 4560 53
 7 71
 8080 23
 Set 23
Ports 22
Presence 42
Presentation Level Provider 8
Provider 8, 60
 Assign 64
 CSTA (IP Office) 65
 Directory (DSML IP Office) 66
 Directory (DSML LDAP) 67
 DSML (IP Office) 66
 DSML (LDAP) 67
 View 64

Q
Quick Time 15
R
RAM Memory 15
Reachable 71
Recent Events 62
Remember me on this computer 15
Remote Logging 53
Remove
 IP Office 39
 one-X Portal 51
 User 42
Reserved Ports 22
Reset Session Count 61
Restart Service 35
Restore 46, 69
 Backup 45
Resynchronization 47, 73
Rights Group 17
Rolling Log Files 70
Routes 71

S
Safari 15
Sanity 72
Search
 LDAP 48, 75
 System Directory 47, 74
Search Base 41
Security Settings 17
Server
 Information 63
 PC Requirements 15
 Version 63
Service
 Restart 35
Service User 17
Services 17
Sessions 63
Settings
 Backup 45
 Bulk Edit 42
 Restore 46
 User 20

Shortcuts 42
Socket Receiver 53, 70
Software
 Install 23
Start Service 35
Status 62
Synchronization 47, 73
System Directory 9, 60
 Directory Search 47, 74
 Export 69
 Resynch 47, 73

T

TCP Port 7 71
TCPA 78
TCPA Group 17
Telephony CSTA Provider 8
Telephony Service Provider Interface 78
Test
 External Directory 48, 75
 IP Office connection 72
 LDAP Directory 48, 75
 Network Route 71
 System Directory 47, 74
 User Login 29

Thin Client Productivity Application 78
TSPI 78

U

Uninstall 51
Upgrading 49
User
 Add 42
 Built Edit 42
 Configuration 20
 Delete 42
 Edit settings 42
 Export 69
 Help 76
 Login 29
 Name 20
 Password 20
 User name 20
Users 60
 Active 63
 Edit settings 68
 Resynch 47, 73
 View 68

V

Version 63
View
 Component Status 62
 Key Recent Events 62
 Providers 64
Voicemail Messages 42

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".

© 2010 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>