



IP Office™ Platform 10.1

Installing and Maintaining the Avaya IP
Office™ Platform Application Server

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

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

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

1. Overview

1.1 What's New in Release 10.1.....	10
1.2 Avaya Pre-Built Servers.....	11
1.3 Non-Avaya Server Requirements.....	12
1.4 Using Linux.....	13
1.5 Additional Documentation.....	13
1.6 Small Community Networks.....	14
1.7 Licenses.....	15
1.8 Voicemail Pro Features.....	15
1.9 Supported Web Browsers.....	15
1.10 Password Authentication (Referred Authentication).....	16

2. Application Server Software Installation

2.1 Downloading Software.....	18
2.2 Changing the IP Office Security Settings.....	19
2.3 Information Requirements.....	20
2.4 Checking the Boot Order.....	21
2.5 Preparing the Bootable Software Installer.....	21
2.5.1 Preparing a DVD.....	21
2.5.2 Preparing a USB2 Installation Key.....	22
2.6 Adding an Additional Hard Disk.....	23
2.6.1 HP DL360G7.....	24
2.6.2 HPDL120G7.....	25
2.6.3 Dell R210.....	25
2.6.4 Dell R620.....	26
2.6.5 Dell R630.....	27
2.7 Server Software Installation.....	28
2.8 Server Ignition.....	30
2.9 Adding a Certificate to the Browser.....	34
2.10 Server Initial Configuration.....	36
2.11 Checking the Services.....	37
2.12 Application Configuration.....	38

3. Voicemail Pro Configuration

3.1 Adding Voicemail Licenses.....	41
3.2 IP Office Configuration.....	42
3.3 Installing the Voicemail Pro Client.....	43
3.4 Logging in to the Voicemail Server.....	44
3.5 Changing the Voicemail Server Password.....	45
3.6 Transferring Voicemail Server Settings.....	46
3.6.1 Transferring Custom Folders.....	48

4. one-X Portal for IP Office Configuration

4.1 Adding Licenses.....	50
4.2 Enabling one-X Portal for IP Office Users.....	51
4.3 one-X Portal for IP Office Configuration.....	52
4.4 Primary/Secondary Server Configuration.....	56
4.5 Initial AFA Login.....	57
4.6 If the Portal Service Status Remains Yellow.....	58
4.7 Transferring one-X Portal for IP Office Settings.....	59

5. WebRTC Configuration

5.1 Equinox Select Overview.....	63
5.2 Enable the Optional Services.....	64

5.3 Enabling SIP Extension Support.....	65
5.4 Configuring the WebRTC Gateway.....	67
5.5 Testing Operation.....	70
5.5.1 Adding the Server Certificate.....	70
5.5.2 Logging In.....	71
5.5.3 Downloading the Client Application.....	72
5.6 Logging and Debugging.....	73
5.7 External Client Access.....	74

6. Server Maintenance

6.1 Logging In.....	77
6.2 Logging Into Web Control Directly.....	79
6.3 Changing the IP Address Settings.....	80
6.4 Starting/Stopping Application Services.....	82
6.4.1 Starting a Service.....	82
6.4.2 Stopping a Service.....	82
6.4.3 Setting a Service to Auto Start.....	82
6.5 Changing the Linux Passwords.....	82
6.6 Shutting Down the Server.....	83
6.7 Rebooting the Server.....	83
6.8 Date and Time Settings.....	84
6.9 Creating Administrator Accounts.....	85
6.10 Setting the Menu Inactivity Timeout.....	85
6.11 Upgrading Applications.....	86
6.11.1 Loading Application Files onto the Server.....	86
6.11.2 Upgrading Application Files.....	87
6.11.3 Upgrading Using USB.....	88
6.12 Uninstalling an Application.....	91
6.13 Setting Up File Repositories.....	92
6.13.1 Source Files.....	92
6.13.2 Setting the Repository Locations.....	92
6.13.3 Uploading Local Files.....	93
6.13.4 Creating Remote Software Repositories.....	94
6.14 Downloading Log Files.....	95

7. Web Manager

7.1 Logging In to Web Manager.....	99
------------------------------------	----

8. Web Control/Platform View Menus

8.1 System.....	103
8.2 Logs.....	106
8.2.1 Debug Logs.....	107
8.2.2 Syslog Event Viewer.....	108
8.2.3 Download.....	108
8.3 Updates.....	109
8.3.1 Services.....	110
8.3.2 System.....	111
8.4 Settings: General.....	112
8.4.1 Software Repositories.....	112
8.4.2 Syslog.....	112
8.4.3 Certificates.....	113
8.4.4 Web Control.....	113
8.4.5 Backup and Restore.....	114
8.4.6 Voicemail Settings.....	114
8.4.7 Contact Recorder Settings.....	114
8.4.8 Integrated Reporting Settings.....	114
8.4.9 EASG Settings.....	114
8.4.10 Packet Capture Settings.....	115
8.4.11 Watchdog.....	115

8.4.12 Set Login Banner.....	116
8.5 Settings: System.....	117
8.5.1 Network.....	118
8.5.2 Avaya IP Office LAN Settings.....	119
8.5.3 Date and Time.....	119
8.5.4 Authentication.....	120
8.5.5 Increase Root Partition.....	120
8.5.6 HTTP Server.....	120
8.5.7 Change Root Password.....	120
8.5.8 Change Local Linux Account Password.....	121
8.5.9 Password Rules Settings.....	121
8.5.10 Firewall Settings.....	121
8.5.11 Additional Hard Drive Settings.....	122
8.6 VNC.....	123
8.7 App Center.....	124

9. Additional Processes

9.1 Initial Configuration Using IP Office Manager.....	126
--	-----

10.Document History

Index	129
-------------	-----

Chapter 1.

Overview

1. Overview

The IP Office Application Server is a single installation of selected IP Office™ Platform 10.1 applications running on Linux. The Linux operating system is included as part of the installation. However, installation requires minimal Linux knowledge due to the inclusion of a web based management interface to allow the server to be managed remotely via web browser.

The IP Office Application Server hosts the following applications:

- **Linux**
This is the base operating system used. However, no specific Linux knowledge is required for installation and maintenance.
- **Management Services**
This is a shell version of IP Office that allows basic configuration of services such as remote SSL VPN connections for server support. It also controls security settings for access to the server's menus. It does not support call features such as users, extensions or trunks.
- **one-X Portal for IP Office**
This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely via web browser.
- **Voicemail Pro**
This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail.
- **Integrated Contact Reporter**
This new service is a small contact centre reporting tool. Refer to the separate Integrated Contact Reporter documentation for full details of configuration and use.
- **Web License Manager**
This service allows the server to act as a WebLM server. IP Office systems using PLDS licenses can then use the address of the server for license validation.
- **Web Manager**
You can configure and manage the server via browser access to the Web Manager menus. The menus also allow the launching of other clients used to configure and monitor the services run by the server.
- **Optional Services**
The server can include a number of additional services. Click **Show optional services** to display those services.
 - **Equinox Select**
This is an WebRTC softphone that works with one-X Portal for IP Office and the WebRTC gateway services. Users can access it through their browser (currently Windows Chrome).
 - **Web Collaboration**
This service works with one-X Portal for IP Office. It provides users with web collaboration services usable in parallel with audio conference hosted by the telephone system. In the parallel web collaboration session, users can share views of their desktop, documents, etc.
 - **WebRTC Gateway**
This is a VoIP gateway service that allows the server to support user's making calls using WebRTC clients. Currently this is supported for Avaya Communicator for Web and for internal licensed web collaboration users.
 - **Media Manager**
This application is an alternative to Contact Recorder for IP Office for the long term storage and retrieval of call recordings. The recordings are made by Voicemail Pro. Those recordings are then collected by Media Manager and stored by it.
 - **Contact Recorder for IP Office**
Contact Recorder for IP Office is used in conjunction with Voicemail Pro for long term storage and retrieval of call recordings. The recordings are made by Voicemail Pro. Those recordings are then collected by Contact Recorder for IP Office and stored by it. For details on installation and support, refer to the Contact Recorder for IP Office Installation Manual. This service has been superseded by Media Manager but is still available for existing users.

Installation Options

The IP Office Application Server is either pre-installed onto a suitable server or as a DVD for installation onto a customer supplied server. Both options are covered by this manual.

1.1 What's New in Release 10.1

For those familiar with IP Office Application Server installation, the following is a summary of the changes in IP Office Release 10.1:

- **Media Manager**
This new service is a voice recordings archiving tool, including search and playback facilities. It is similar to Contact Recorder for IP Office but uses different licenses.
- **Integrated Contact Reporter**
This new service is a small contact centre reporting tool. Refer to the separate Integrated Contact Reporter documentation for full details of configuration and use.
- **[Enhanced Access Security Gateway Support](#)**^[114]
Support for ASG (Access Security Gateway) has been replaced with EASG (Enhanced Access Security Gateway).
- **Voicemail Pro Database Interaction**
For IP Office Application Server and Server Edition servers, the Voicemail Pro service now supports database interoperating with external MySQL and Postgres databases.
- **Voice Recording Library Operation**
The folder now used for store recordings waiting for collection by applications such as Integrated Contact Reporter or Media Manager has changed from `/opt/vmpro/VRL` to `/opt/vmpro/MM/VRL`.
- **Mount Path Display**
For servers with an additional hard drive added, the full path to the additional drive partitions is now displayed.

1.2 Avaya Pre-Built Servers

The IP Office Application Server is available pre-installed onto a suitable server. The general specification of the servers used is:

- **Form:** Rack mounted server PC.
- **RAM:** 12GB.
- **Hard Disk:** 250GB.
- **Ethernet Port:** Only a single port (eth0) is supported. This port is labeled as port 1 on the physical server.

Default Settings

The following are the default settings applied to the server applied shipment from Avaya:

- **DHCP Mode:** Off
- **IP Address:** 192.168.42.1
- **NetMask:** 255.255.255.0
- **Gateway:** Blank
- **Hostname:** The server MAC address.
- **DNS1:** Blank
- **DNS2:** Blank
- **Time Zone:** EST - Eastern Standard Time.

Applications Installed

- **Voicemail Pro**
 - **English and French Language TTS for Voicemail Pro**
- **one-X Portal for IP Office**

1.3 Non-Avaya Server Requirements

The following are the minimum server PC requirements.

- **IMPORTANT: Compatible Servers**

Avaya cannot guarantee the compatibility of any particular server PC for the operating system. It is the installer's responsibility to ensure that the server platform is compatible. A list of tested servers is available at <https://hardware.redhat.com/>.

	Minimum Specification	Recommended Specification
Processor	Intel 64-bit Dual Core 2.4GHz	Intel Pentium 64-bit Quad Core 2.4GHz or AMD Athlon 64 4000 + or equivalent.
RAM Memory	4GB	4GB
Hard Disk Space	30GB	30GB.

- **Operating System**

The IP Office Application Server installs a Linux operating system, replacing any existing operating system on the PC.

- **Drives**

DVD Drive for software installation. For Contact Recorder for IP Office, a DVD+RW or Blu Ray -R disc drive is recommended. For IP Office Release 9.0 Feature Pack 1, Contact Recorder for IP Office is supported on the same server as Voicemail Pro if an addition hard disk is installed. Refer to *"Installing Contact Recorder for IP Office"* for details.

- **Other Requirements:**

- The server PC must be configurable to boot from DVD or USB in order to overwrite any existing OS. This may require access to the BIOS in order to change the boot order of the PC.
- The IP Office Application Server operates as a headless server, i.e without requiring any keyboard, video and mouse (KVM) connections after initial installation. Users and maintainers access the server remotely from other PCs.

1.4 Using Linux

Though the server uses a Linux based operating system, no knowledge or experience of Linux is required. The IP Office Application Server is designed to be configured and maintained remotely using its web browser interface. Other services running on the server are administered using separate client applications.

No access to the Linux command line is expected. Avaya does not support use of the Linux desktop or command line to perform actions on the server except where specifically instructed by Avaya.

1.5 Additional Documentation

In addition to reading this manual, you should also have, have read and are familiar with the following manuals before attempting to install a system.

Related Documents

- **Deploying IP Office™ Platform Servers as Virtual Machines**
Covers deployment of the Server Edition and Application servers as virtual machines.
- **Administering Avaya one-X Portal for IP Office™ Platform**
This manual covers the installation and administration menus used for the one-X Portal for IP Office application. This manual is essential if the one-X Portal for IP Office needs configuring to support multiple IP Office servers in a Small Community Network.
- **Installing Avaya one-X® Portal for IP Office™ Platform**
This manual covers the Windows installation of one-X Portal for IP Office. However, notes within it for various scenarios are also applicable to one-X Portal for IP Office installed on a IP Office Application Server.
- **Deploying Avaya IP Office™ Platform Voicemail Pro (Windows)**
This manual covers voicemail server configuration and scenarios including multiple servers within a Small Community Network. Those scenarios can include a mix of Windows based and Linux based servers.
- **Administering Avaya IP Office™ Platform Voicemail Pro**
By default the voicemail server provides mailbox services to all users and hunt groups without any configuration. This manual covers the administration of the voicemail server using the Voicemail Pro client in order to enable additional features.
- **Administering Avaya IP Office™ Platform with Manager**
IP Office Manager is the application used to configure IP Office systems and the Management Services service. This manual details how to use IP Office Manager and the full range of IP Office configuration settings.
- **Administering Avaya IP Office™ Platform with Web Manager**
This covers the configuration of IP Office systems using the Web Manager menus.
- **Installing Avaya IP Office™ Platform Contact Recorder for IP Office**
Covers the additional steps required for installation and basic operation of the Contact Recorder for IP Office application.
- **Administering Contact Recorder for IP Office**
Administration and operation of the optional Contact Recorder for IP Office service.
- **Using Contact Recorder for IP Office**
Covers the use of Contact Recorder for IP Office.
- **Administering Avaya IP Office Platform Media Manager**
Administration and operation of the optional Media Manager service.
- **Using Avaya IP Office Platform Media Manager**
Covers the use of Media Manager.
- **Deploying IP Office™ Platform Server Edition Solution**
This manual covers the installation of Server Edition systems.

Technical Bulletins

Avaya provide a technical bulletin for each releases of IP Office software. The bulletin details changes that may have occurred too late to be included in this documentation. The bulletins also detail the changes in the software release compared to previous releases and any specific actions required or restrictions that apply if upgrading from a previous release.

Other Documentation and Documentation Sources

All the documentation for IP Office systems is available from the following web sites:

- **Avaya Support Web Site** - <http://support.avaya.com>
- **Avaya IP Office Knowledge Base** - <http://marketingtools.avaya.com/knowledgebase>

1.6 Small Community Networks

Up to 32 IP Office systems can connect using H323 SCN trunks to form a Small Community Network, supporting up to 1000 users.

When installing a server within a Small Community Network, it is important to be aware of the following factors affecting the different server applications:

- **one-X Portal for IP Office**

A Small Community Network only supports a single one-X Portal for IP Office server. The application can support up to 500 simultaneous one-X Portal for IP Office users.

- **Voicemail Pro**

In an Small Community Network, one Voicemail Pro server stores all mailboxes and their related messages, greeting and announcements. Additional Voicemail Pro servers installed in the network perform other specific roles. For full details, refer to the Voicemail Pro manuals.

- **Centralized Voicemail Server**

In the network, one Voicemail Pro server acts as the centralized voicemail server for all IP Office systems. This server stores all mailboxes and their related messages, greeting and announcements. This is mandatory regardless of the presence of any additional options below. The IP Office associated with the centralized server holds the licenses for voicemail server support. The other servers in the network do not require any voicemail licenses in order to use this server as their voicemail server.

- **Fallback IP Office**

Without needing to install another Voicemail Pro server, you can configure the IP Office hosting the centralized voicemail server such that, if for any reason it is stopped or disabled, the centralized voicemail server accepts control from another IP Office in the network.

- **Distributed Voicemail Servers**

You can install additional Voicemail Pro servers and associated these with other IP Office systems to provide call services for those systems. For example to record messages, play announcements, etc. However, any messages they record are automatically transferred to and stored on the centralized server. The IP Office associated with the distributed server requires the appropriate licenses for voicemail server support.

- **Backup Voicemail Server**

You can specify an additional voicemail sever as the backup server for the centralized server. If for any reason the voicemail application on the centralized server is stopped or disabled, the centralized IP Office will switch to using the backup voicemail server for its voicemail functions. During normal operation the centralized and backup voicemail servers automatically exchange information about mailboxes and voicemail service configuration. The backup voicemail server uses the licenses provided by the centralized IP Office. A distributed server cannot also be used as a backup server and vice versa.

1.7 Licenses

The use of various features is licensed, for example which users are able to use the one-X Portal for IP Office application. For the IP Office Application Server it is important to understand the role of the following system licenses:

- **Essential Edition**
This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
This license is required for use of the Voicemail Pro application. It also enables 4 voicemail ports. It is also required as a pre-requisite for the user profile licenses required for one-X Portal for IP Office users.
- **Preferred Edition Additional Voicemail Ports**
These licenses add additional voicemail ports in addition to the 4 enabled by the **Preferred Edition (Voicemail Pro)** license above.
- **Messaging TTS Pro**
This license enables the use of text-to-speech facilities using the optional Linux TTS software and user email reading. One license per simultaneous instance of TTS usage.
- **User Profile Licenses**
For a user to use the one-X Portal for IP Office application, you must license and configure the user to one of the following user profiles in the IP Office configuration: **Office Worker**, **Teleworker** or **Power User**. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

1.8 Voicemail Pro Features

Voicemail Pro runs on both Windows and Linux servers. Voicemail Pro running on Linux, such as with the IP Office Application Server, does not support the following Voicemail Pro features:

- **VB Scripting**
- **UMS Web Voicemail**
- **VPNM**

1.9 Supported Web Browsers

Avaya supports the following browsers for web access to the server menus:

- **Microsoft Internet Explorer 10 and 11.**
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

1.10 Password Authentication (Referred Authentication)

The password authentication for access to the services hosted by the server can use either each services' own security settings or use the security user accounts configured for the Management Services service running on the IP Office Application Server. The [Enable referred authentication](#) ^[120] setting controls the method used.

- These settings are only accessible if logged in via referred authentication or as the local Linux root.
- **Enabled**
With referred authentication enabled, the security settings of the Management Services service running on the IP Office Application Server control access to the following other services:
 - **Web control menus**
 - **Voicemail Pro admin**
 - **one-X Portal for IP Office admin**
 - **IP Office Web Manager**
- **Disabled**
With referred authentication disabled, each service controls access to itself using its own local account settings.

For Server Edition and IP Office Application Server servers, referred authentication is supported from IP Office Release 9.0 onwards and is the default on new installations. For the Unified Communications Module it is supported from IP Office Release 9.1 onwards.

Upgrading

For servers upgraded from pre-IP Office Release 9.0, the default authentication used depends on the status of the web control **Administrator** password:

- If the **Administrator** password is still default, the server defaults to **Enable referred authentication**.
- If the **Administrator** password is not default, the server does not default to **Enable referred authentication**.

Chapter 2.

Application Server Software Installation

2. Application Server Software Installation

This section covers the installation of the IP Office Application Server software onto a customer supplied server PC. This process uses various software packages downloaded from Avaya to create an installation DVD or bootable USB memory key.

2.1 Downloading Software

Avaya makes IP Office Application Server software for each IP Office release available from the Avaya support website (<http://support.avaya.com>) in a number of formats.

- **ISO Image**
You can use this type of file to reinstall the full set of software including the operating system. Before using an ISO image, you must backup all applications data.
- **Source ISO Image**
Some components of the software are open source. To comply with the license conditions of that software, Avaya is required to make the source software available. However, this file is not required for installation.
- **Avaya USB Creator Tool**
This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade.

To download Avaya software:




1. Browse to **<http://support.avaya.com>** and log in.
2. Select **Support by Product** and click **Downloads**.
3. Enter **IP Office** in the **Enter Product Name** box and select the matching option from the displayed list.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. The page lists the different sets of downloadable software for that release. Select the software for the IP Office Application Server.
6. The page displayed in a new tab or windows details the software available and provides links for downloading the files.
7. Also download the documents listed under the **RELATED DOCUMENTS** heading if shown.

2.2 Changing the IP Office Security Settings

The following elements of the IP Office security settings affect installation:

- The one-X Portal for IP Office application uses the **Enhanced TSPI** service and **EnhTcpaService** user for its connection to the IP Office. The installation assumes that the **EnhTcpaService** user is enabled and has the default password of **EnhTcpaPwd1**.
 - If the password is not at default during the IP Office Application Server installation, the one-X Portal for IP Office service will not start correctly and the service user account becomes locked. To resolve that, follow the steps below and then restart the one-X Portal for IP Office service.
 - Once the one-X Portal for IP Office service is operating correctly, you can change the **EnhTcpaPwd1** password.
- Voicemail Pro connects to the IP Office using the **Voicemail Password**. This is set in the IP Office system's security settings (System | Unsecured Interfaces) and must be matched by the password set in the [voicemail servers preferences](#)^[45] after installation.

To change the security settings:

1. Using IP Office Manager select **File | Advanced | Security**.
2. Enter the name and password for access to the IP Office security settings.
3. Click  **System** and then select the **Unsecured Interfaces** tab.
 - a. Click on the **Change** button next to the **Voicemail Password** field and set a new password. The default is blank.
 - b. Click **OK**.
4. Click  **Service Users** and select **EnhTcpaService**.
 - a. Check that the account status is set to **Enabled**.
 - b. Click on the Change button next to the **Password** field and set the password to **EnhTcpaPwd1**.
 - c. Click **OK**.
5. Click the  save icon.

2.3 Information Requirements

The following information is required during the installation process:

- **Server Applications**

During the installation process, you can select which IP Office Application Server applications are installed. Note that for each application selected, the normal license requirements still apply. Refer to the separate installation manual for each application for details.

- ☐ **Voicemail Pro**

If selected for installation, refer to the Voicemail Pro Linux Installation Manual for details of setup and configuration of the Voicemail Pro application.

- ☐ **Voicemail Text to Speech Prompts**

During installation, you can select whether you want TTS prompt installed. If selected, you will be prompted to select the languages that you want installed. These are installed from a separate sets of DVDs or downloadable ISO images.

- ☐ **one-X Portal for IP Office**

If selected, the same information is required as for a Windows based installation of the one-X Portal for IP Office application. For example, IP address of IP Office Application Server system, LDAP server information and voicemail server address (if other than the IP Office Application Server address). Refer to the one-X Portal for IP Office Installation manual.

- **Server IP Address Settings**

The IP Office Application Server supports IPv4 addressing obtain through either DHCP or static addressing.

	IPv4 Support
Use DHCP	<input type="checkbox"/>
IP Address	<input type="checkbox"/> _____
Prefix (Netmask)	<input type="checkbox"/> _____
Gateway	<input type="checkbox"/> _____
Primary DNS	<input type="checkbox"/> _____
Secondary DNS	<input type="checkbox"/> _____

- ☐ **Hostname**

A hostname helps simplify access to the server and the applications it provides rather than requiring users to use the IP address.

- ☐ **Timezone**

The timezone in which the server is located and whether the server should use UTC or local time.

- ☐ **Root Password**

- ☐ **Client PC**

The IP Office Application Server is designed and intended for remote configuration and management. It is not managed directly from the server. Therefore a client PC with a web browser on the same network as the server PC is required for configuration.

- If Voicemail Pro server is one of the selected server applications, then the client PC must be a Windows based PC onto which you can install the Voicemail Pro client.

2.4 Checking the Boot Order

You install the software by placing it onto a DVD or USB memory key from which the server PC then boots. The normal default for servers is to boot from CD/DVD drive and, if unsuccessful, then boot from the first hard disk. This boot order is set in the BIOS settings of the server PC.

In order to add other devices to the list of those from which the server can boot or to change the order of usage, you need to change the server's BIOS settings. The method of accessing the BIOS varies between servers. Refer to the PC manufacturer's documentation.

- Typically, an option to access the BIOS settings of a server appears briefly when the server PC is started. For example "Press Del for setup" indicates that the server BIOS is accessed by press the Delete key while the message appears. This option is only available for a few seconds whilst the existing BIOS settings are loaded, after which the server looks for and begins to load boot software if it finds a boot source, for example existing boot software on its hard disk.
- Once the PC displays its BIOS settings, the normal boot up process stops. The BIOS settings typically consist of several pages. The settings for the order in which the server looks at different devices for a boot software source are normally set on the **Advanced BIOS Features** page.
- To boot from a DVD, ensure that the server's DVD drive is set as the boot device used before the server's hard disk.
- To boot from a USB memory key, set a USB option as the boot device used before the server's hard disk. Depending on the BIOS, there may be multiple USB options. Select **USB-FDD**.
- The server's hard disk must remain in the list of boot devices. The server boots from the hard disk after the software installation.

2.5 Preparing the Bootable Software Installer

You can install the server software from either a DVD or a USB memory key. If not installing from an Avaya supplied DVD, you must download an ISO image from Avaya and use that to create the bootable DVD or USB memory key.

2.5.1 Preparing a DVD

To install from a DVD, you need to burn the .iso image file of the installation software onto a bootable DVD. The exact process for that depends on which software you use for the burning process. However, the following general recommendations apply:

- Do not use reusable DVDs.
- Burn the DVD at a slow speed such as 4x.

2.5.2 Preparing a USB2 Installation Key

This process extracts a downloaded ISO image onto a USB memory key and then turns that memory key into a bootable device for software installation or upgrading.

Prerequisites

- **4GB USB Memory Key**

Note that this process reformats the memory key and erases all files.

- **Avaya USB Creator Tool**

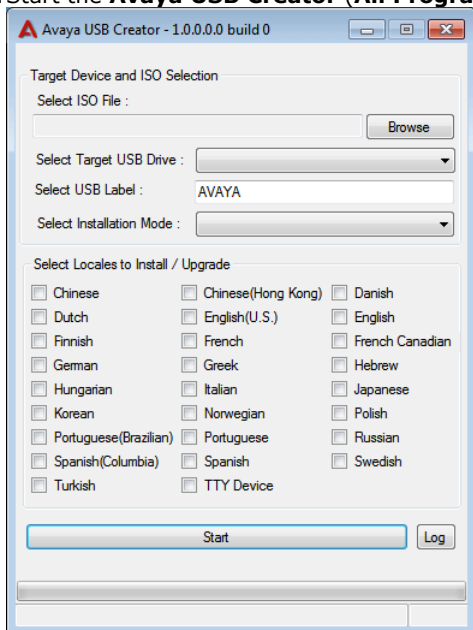
This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade.

- **Server Edition ISO Image**

You can download this file from the Avaya support website, see Downloading Module Software.

To create a bootable USB memory key:

1. Insert the USB memory key into a USB port on the PC.
2. Start the **Avaya USB Creator (All Programs | IP Office | Avaya USB Creator)**.



3. Click the **Browse** button and select the ISO file.
4. Use the **Select Target USB Drive** drop-down to select the USB memory key. Make sure that you select the correct USB device as this process overwrites all existing contents on the device.
5. In the **Select USB Label** field enter a name to help identify the key and its usage in future.
6. Use the **Select Installation Mode** options to select whether the USB memory key should be configured for an automatic software install (**Server Edition - Auto Install**), automatic software upgrade (**Server Edition - Auto Upgrade**) or a user menu driven install/upgrade (**Server Edition - Attended Mode**).
 - Note: The installation mode options available changed automatically based on the type of ISO file selected. If you do not see the correct options, check that you have selected a IP Office Application Server ISO file.
7. Use the **Select Locales to Install / Upgrades** check boxes to select which sets of Voicemail Pro prompts you want installed or upgraded. Only selecting the languages that you require significantly reduces the time required for the installation or upgrade.
8. Check that you have set the options correctly. Click **Start**.
9. Confirm that you want to continue.
10. The status bar at the bottom of the tool shows the progress of preparing the USB memory key. The process takes approximately 15 minutes though that can vary depending on the USB2 memory key and PC.

2.6 Adding an Additional Hard Disk

If Contact Recorder for IP Office or Media Manager is installed and enabled on the same server as Voicemail Pro, it must be configured to use a separate hard disk from Voicemail Pro. That requires the addition of an additional hard disk to the server (or a pair of hard disks if implementing RAID support).

The process for adding an additional hard disk depends on the type of server. This section only provides outline summaries. In all cases, for full details refer to the original equipment manufacturer's documentation.

Avaya supply the following servers:

- [HP ProLiant DL360G7 Server](#)^[24]
Avaya supplies and supports additional 300GB hard disks (DL360G7 SRVR 300GB 10K SAS 2.5" HDD). You can fit either a single disk or, for RAID1 support, two additional disks.
- [HP ProLiant DL120G7 Server](#)^[25]
Avaya supplies and supports an additional 250GB hard disk (Order code 700506869).
- [Dell PowerEdge R210 Server](#)^[25]
Avaya supplies and supports an additional 500GB hard disk (R210 II XL 500GB 7200 HDD).
- [Dell PowerEdge R620 Server](#)^[26]
Avaya supplies and supports additional 600GB hard disks (Order code 700506757). You can fit either a single disk or, for RAID1 support, two additional disks.
- [Dell PowerEdge R630 Server](#)^[27]
Avaya supplies and supports additional 600GB hard disks (Order code 700506757). You can fit either a single disk or, for RAID1 support, two additional disks.

2.6.1 HP DL360G7

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Decide if you will be adding a single HDD or a RAID set as the second drive:
 - A single drive requires 1 hard disk in slot 3.
 - A RAID pair requires 2 hard disks, in slots 3 and 4 respectively, which then act as mirrored images of each other.
2. Go the HP support page for the DL360G7 and download the Server Guide:
http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/action.process/public/psi/manualsDisplay/?sp4ts.oid=4091408&javax.portlet.action=true&spf_p.tpst=psiContentDisplay&javax.portlet.begCacheTok=com.vignette.cachetoken&spf_p.prp_psiContentDisplay=wsrp-interactionState%3DdocId%253Demr_na-c02065265%257CdocLocale%253Den_US&javax.portlet.endCacheTok=com.vignette.cachetoken

To install the additional hard disk(s):

1. Power down the server.
2. Remove the blank from slot 3. Also from slot 4 if installing a pair of drives for RAID. Refer to the server guide section "*Removing hard drive blanks*".
3. Insert the new hard disk into slot 3. Also into slot 4 if installing a pair of drives for RAID. Refer to the server guide section "*Installing a SAS hard drive*".
4. Power on the server.
5. When the "Press any Key to view Option ROM Messages" option appears, press any key.
6. Wait for the message "Slot 0 HP Smart Array P4101 Controller Initializing" to appear, then press **F8**.
7. From the **Main Menu** select **Create Logical Drive**. Select the following options:

Setting	Single Drive	RAID Pair
Available physical drive	Bay 3	Bay 3 and Bay 4
Raid Configurations	RAID 0	Raid 1+0
Parity Group Count	Leave blank	Leave blank
Spare	Leave blank	Leave blank
Maximum Boot partition	Disable	Disable

8. After the options have been selected, press **Enter** to save the configuration.
9. Press **F8** to confirm.
10. Select **Select View Logical Drive**. Ensure there are 2 drives listed, if not go back to step 7.
11. Press **Esc**.

2.6.2 HPDL120G7

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Go the HP support page for the DL360G7 and download the Server Guide:
http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/action.process/public/psi/manualsDisplay/?sp4ts.oid=5075933&javax.portlet.action=true&spf_p.tpst=psiContentDisplay&javax.portlet.begCacheTok=com.vignette.cachetoken&spf_p.prp_psiContentDisplay=wsrp-interactionState%3DdocId%253Demr_na-c02790682%257CdocLocal%253Den_US&javax.portlet.endCacheTok=com.vignette.cachetoken

To install the additional hard disk:

1. Power down the server.
2. Remove the blank from slot 3. Refer to the server guide section *"Removing a blank drive"*.
3. Insert the new hard disk into slot 3. Refer to the server guide section *"Installing a hot-plug drive"*.
4. Power on the server.
5. When the *"Press any Key to view Option ROM Messages"* option appears, press any key.
6. Wait for the message *"Slot 1 HP Smart Array P212 Controller Initializing"* to appear, then press **F8**.
7. From the **Main Menu** select **Create Logical Drive**. Select the following options:

Setting	Single Drive
Available physical drive	Bay 3
Raid Configurations	RAID 0
Parity Group Count	<i>Leave blank</i>
Spare	<i>Leave blank</i>
Maximum Boot partition	<i>Disable</i>

8. After the options have been selected, press **Enter** to save the configuration.
9. Press **F8** to confirm.
10. Select **Select View Logical Drive**. Ensure there are 2 drives listed, if not go back to step 7.
11. Press **Esc**.

2.6.3 Dell R210

The following is an outline of the process for adding additional drives to an Dell R210 server. For full details refer to the manufacturers documentation.

To install an addition hard disk:

1. Go the Dell support page for the R210 and download the User Manual:
ftp://ftp.dell.com/Manuals/all-products/esuprt_ser_stor_net/esuprt_poweredge/poweredge-r210_owner%27s%20manual_en-us.pdf
2. Power down the server.
3. Open the system. Refer to the server guide section *"Opening the system"*.
4. Install the 2nd hard drive under the optical drive. Refer to the server guide section *"Installing a Hard Drive"*.
5. Power on the server.
6. Press **F2** to get into the BIOS.
7. Scroll down to **SATA Settings** and press enter
8. Scroll down to **Port B** and change the setting from **Off** to **Auto**.
9. Press **Esc**.
10. Select **Save Changes and Exit**.

2.6.4 Dell R620

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Decide if you will be adding a single HDD or a RAID set as the second drive:
 - A single drive requires 1 hard disk in slot 2.
 - A RAID pair requires 2 hard disks, in slots 2 and 3 respectively, which then act as mirrored images of each other.
2. Go the Dell support page for the R620 and download the Owner's Manual:
http://topics-cdn.dell.com/pdf/powerededge-r620_Owner's%20Manual_en-us.pdf

To install the additional hard disk(s):

After adding the new physical drives, this process defines a new virtual drive by setting its Raid type and which physical drives it uses.

1. Power down the server.
2. Remove the blank from slot 2. Also from slot 3 if installing a pair of drives for RAID. Refer to server guide section on *"Removing A 2.5 Inch Hard-Drive Blank"*.
3. Insert the new hard disk into slot 2. Also into slot 3 if installing a pair of drives for RAID. Refer to server guide section on *"Installing A Hot-Swap Hard Drive"*.
4. Power on the server.
5. When the RAID controller BIOS details appears, shown by **"PowerEdge Expandable RAID Controller BIOS"**, press **Ctrl+R** to enter into the utility.
6. On the **VD Mgmt** tab, highlight the top line **PERC H710 Mini**.
7. Press **F2** and select **Create New VD**.
8. Select the following options:

Setting	Single Drive	RAID Pair
RAID Level	RAID-0	RAID-1
Select Disks	00:01:02	00:01:02 and 00:01:03
VD Size	<i>Leave as default</i>	<i>Leave blank</i>
Advanced settings	<i>Do not select</i>	<i>Leave blank</i>

9. Press **OK** if prompted.
10. Press **Esc** to leave the utility.
11. Reboot the system.

2.6.5 Dell R630

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Decide if you will be adding a single HDD or a RAID set as the second drive:
 - A single drive requires 1 hard disk in slot 2.
 - A RAID pair requires 2 hard disks, in slots 2 and 3 respectively, which then act as mirrored images of each other.
2. Go the Dell support page for the R630 and download the Owner's Manual:
http://topics-cdn.dell.com/pdf/poweredge-r630_Owner's%20Manual_en-us.pdf

To install the additional hard disk(s):

After adding the new physical drives, this process defines a new virtual drive by setting its Raid type and which physical drives it uses.

1. Power down the server.
2. Remove the blank from slot 2. Also from slot 3 if installing a pair of drives for RAID. Refer to server guide section on *"Removing A 2.5 Inch Hard-Drive Blank"*.
3. Insert the new hard disk into slot 2. Also into slot 3 if installing a pair of drives for RAID. Refer to server guide section on *"Installing A Hot-Swap Hard Drive"*.
4. Power on the server.
5. When the RAID controller BIOS details appears, shown by **"PowerEdge Expandable RAID Controller BIOS"**, press **Ctrl+R** to enter into the utility.
6. On the **VD Mgmt** tab, highlight the top line **PERC H730 Mini**.
7. Press **F2** and select **Create New VD**.
8. Select the following options:

Setting	Single Drive	RAID Pair
RAID Level	RAID-0	RAID-1
Select Disks	00:01:02	00:01:02 and 00:01:03
VD Size	<i>Leave as default</i>	<i>Leave blank</i>
Advanced settings	<i>Do not select</i>	<i>Leave blank</i>

9. Press **OK** if prompted.
10. Press **Esc** to leave the utility.
11. Reboot the system.

2.7 Server Software Installation

This process installs the Linux operating system onto the server and the Linux based applications. This installation process requires approximately 1 hour.

To install the server software from a bootable device:

1. Depending on the chosen method of installation:

- If installing from a DVD, immediately after powering up the PC, insert the DVD into the DVD drive.
- If installing from a USB memory key, insert the USB memory key into the first USB port and apply power to the PC.

2. The PC should boot and display the first server installation screen.

- If installing from a DVD and the PC does not boot from the DVD, the boot order of the server PC may need to be changed. See [Checking the Boot Order](#) ^[21].
- If installing from a USB memory key and the PC does not boot from the USB memory key:
 - if the server has several USB ports, reboot with the USB memory key in another one of the ports.
 - the boot order of the server may need to be changed. See [Checking the Boot Order](#).

3. The installer prompts whether it should check the installation media. Checking a DVD takes approximately 10 minutes.

a. To skip the media check, select **Skip**.

b. To proceed with a media check, select **OK**. When the check has completed, the installer provides options to check any other media, for example the TTS language DVDs.

4. Select the language that you want used for the installation process. Click **Next**.

5. Select the keyboard that matches the one you are using. Click **Next**.

6. Read the license agreement. If you accept the license agreement, click **Yes** and then click **Next**.

7. An upgrade menu appears if a previous release is already installed on the server. It details the existing installed options and the new installable options. Select either **Install** or **Upgrade** and click **Next**.

- **Install**

This option overwrites the existing installation including any customer data.

- **Upgrade**

This option upgrades the existing application and retains the existing customer data.

8. If you selected **Install**, the installer asks you to confirm the process. Select the required option and click **Next**.

- **Yes**

If selected, the installation process continues, formatting the whole drive for its use.

- **No**

If selected, the install process offers to shutdown the server. Either remove the device from which you were booting to allow the server to restart normally or allow the installation process to start again.

- **Advanced**

If selected, during the installation process you can select adjust the hard disk partitioning. However, if used, the installer does not display the **Upgrade** option (see [Step 7](#)) when booting from an ISO in future.

9. If you selected **Install**, continue below. If you selected **Upgrade**, go to step 11.

a. Set the host name for the server to use.

b. Click **Configure Network**.

a. Select the wired Ethernet connection being used (this is likely to be **eth0**) and click **Edit**.

b. Select the **IPv4 Settings** tab.

c. To change the address shown, click on the address and change the settings.

d. When finished setting the IP address details for the server, click **Apply**. Click **Close**. Click **Next**.

c. Enter and confirm the password for the root administrator account. This is the root user password for access to the operating system. Ensure that you note the password set. This password is needed for the server ignition process.

d. Click **Next**. Click **Next** again.

e. A menu for partitioning the server appears if you selected **Advanced** during step 8 above. The menu allows various options for partitioning of the server hard disk. However, if used, the installer does not display the **Upgrade** option (see [Step 7](#)) when booting from an ISO in future.

10. The process for formatting the disk starts. This runs for a couple of minutes.

11. The installer prompts you that it is about start installation of the software. Click **Next** to start.
12. When installation is complete, click **Next**.
13. Remove the DVD or USB memory key and then select **Reboot**.
14. Following the reboot, the server displays "SELinux targetted policy relabel is required" and performs that process. When completed, the server reboots again.
15. After the second reboot, wait until the server displays the address details for further configuration of the server. Use the address to start the server ignition process. See [Server Ignition](#)^[30].

2.8 Server Ignition

Following installation, you must ignite the server. You do this by web browser access to the server.

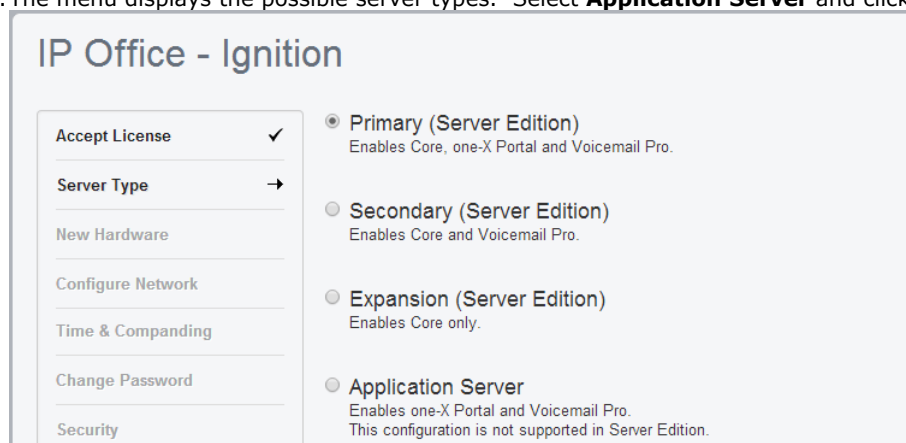
To start server ignition:

1. From a client PC, start the browser and enter **https://** followed by the IP address of the server and **:7071**. For example **https://192.168.42.1:7071**.
 - The browser may display a security warning. You must determine whether you want to continue.
2. The ignition login page appears. Note the various ID numbers shown, these are used for issuing licenses for the server.



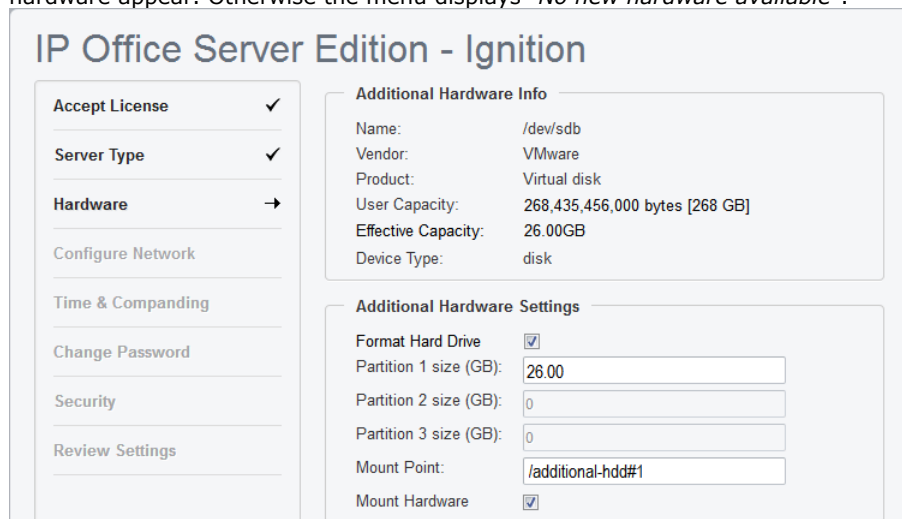
The screenshot shows the login page for IP Office Server Edition R10.1. It includes a login form with fields for User Name (root), Password, and Language (English). It also displays system information such as PLDS Host ID, System ID, and WebLM Host ID. A 'Login' button is at the bottom.

3. Enter the password set for the root account during the software installation. Click **Login**.
4. The license menu appears. If you accept the license, select **I Agree** and click **Next**.
5. The menu displays the possible server types. Select **Application Server** and click **Next**.



The screenshot shows the 'IP Office - Ignition' screen. On the left is a sidebar with options: Accept License (checked), Server Type (selected), New Hardware, Configure Network, Time & Companding, Change Password, and Security. The main area shows three server type options: Primary (Server Edition), Secondary (Server Edition), and Expansion (Server Edition), all of which are unselected. The 'Application Server' option is selected, with a note that this configuration is not supported in Server Edition.

6. If an additional hard disk for Contact Recorder for IP Office was added to the server, details of the additional hardware appear. Otherwise the menu displays "No new hardware available".



The screenshot shows the 'IP Office Server Edition - Ignition' screen. The sidebar on the left has 'Hardware' selected. The main area is divided into two sections: 'Additional Hardware Info' and 'Additional Hardware Settings'. The 'Additional Hardware Info' section displays details for a virtual disk, including Name, Vendor, Product, User Capacity, Effective Capacity, and Device Type. The 'Additional Hardware Settings' section includes checkboxes for 'Format Hard Drive' and 'Mount Hardware', and input fields for 'Partition 1 size (GB)', 'Partition 2 size (GB)', 'Partition 3 size (GB)', and 'Mount Point'.

For Contact Recorder for IP Office support it is recommended to accept the defaults. These are:

- a. Leave **Format Hard Drive** checked.
- b. Create a single partition for the whole disk. You can create up to 3 logical partitions on the physical disk.

c. Leave the **Mount Point** name as **/additional-hdd#1**. The full mount path name for each partition is automatically configured by the system adding **/partition1**, **/partition2**, etc. as a suffix. For example **/additional-hdd#1/partition1**. Note that it is this partition name, including **/partition1**, that should be used for Contact Recorder or Media Manager settings.

d. Select **Mount Hardware** to have the additional disk automatically mounted.

7. Click **Next**. Check and if necessary change the network settings for the server.

The screenshot shows the 'Avaya IP Office Application Server' configuration window. On the left is a sidebar with navigation links: 'Accept License' (checked), 'Server Type' (checked), 'New Hardware' (checked), 'Configure Network' (active, with a right arrow), 'Time & Companding', 'Change Password', 'Configure Services', 'Security', and 'Review Settings'. The main area is titled 'Network interface: eth0'. It contains three sections: 'Assign IP Address' with fields for 'Automatic (DHCP)' (unchecked), 'IP Address' (192.168.0.214), and 'Netmask' (255.255.255.0); 'Assign System Gateway' with a 'Gateway' field (192.168.0.1); and 'Assign System DNS Servers' with fields for 'Automatic (DHCP)' (unchecked), 'Primary DNS', and 'Secondary DNS'. At the bottom is a 'Hostname' field with the value 'localhost.localdomain'.

- **Hostname**

This value is used as the DNS host name of the server.

- **! IMPORTANT: DNS Routing**

For internal use, this value must be reachable by DNS within the customer network. If the server will also be supporting external applications, it needs to be reachable by external DNS. Consult with the customer's IT support to ensure the name is acceptable and that routing to it has been configured correctly.

8. Click **Next**. Set the time source for the server.

The screenshot shows the 'Avaya IP Office Application Server' configuration window with the 'Time & Companding' section active in the sidebar. The main area has a 'Use NTP' checkbox which is checked. Below it are fields for 'NTP Server' (0.pool.ntp.org), 'Date/Time' (2014-07-30 / 10 : 28), and 'Timezone' (Europe/London). At the bottom, a message states: 'Companding settings not available for the currently selected server type.'

9. Set the current time and date for the server or select to use the time provided by an NTP server.

10. Click **Next**. Enter and confirm the passwords. These are the passwords for various IP Office service accounts and also for the Linux accounts created on the server. Ensure that you note the passwords set.

The screenshot shows the 'Avaya IP Office Application Server' configuration interface. On the left is a sidebar with navigation links: 'Accept License' (checked), 'Server Type' (checked), 'New Hardware' (checked), 'Configure Network' (checked), 'Time & Companding' (checked), 'Change Password' (active, with a right arrow), 'Security', and 'Review Settings'. The main content area is titled 'Default account passwords are required to be changed.' and contains three sections for password entry:

- "root" and "security" password:** Fields for 'New Password:' and 'New Password (verify):', with a link to 'View password policy'.
- "Administrator" password:** Fields for 'New Password:' and 'New Password (verify):', with a link to 'View password policy'.
- "System" password:** Fields for 'New Password:' and 'New Password (verify):', with a link to 'View password policy'.

- The passwords must be 8 to 32 characters, containing at least two types of character (lower case, upper case, numeric and special characters) and no more the 3 consecutive characters.

- **root/security password**

This sets the password for both the Linux **root** user account and also the **security** account of the Management Services service.

- **Administrator password**

This sets the password for Linux **Administrator** account and also the **Administrator** account of the Management Services service run on the IP Office Application Server. With [Referred Authentication](#) ¹⁶ enabled (the default) this is also the default account used for Voicemail Pro and one-X Portal for IP Office administrator access.

- **System password**

This sets the **System** password for the Management Services.

11. For a server set to be an IP Office Application server, select which applications should start automatically. Unselected services are installed but not set running unless manually started.

The screenshot shows the 'Avaya IP Office Application Server' configuration interface. The sidebar on the left has 'Configure Services' as the active link, indicated by a right arrow. The main content area is titled 'Select which services will be configured to start automatically.' and contains two checked checkboxes:

- ☒ Voicemail Pro
- ☒ one-X Portal for IP Office

12. Click **Next**. The menu prompts which security certificate the server should use.

- If you select **Generate CA automatically**, you must download the certificate from the next screen.
- If you select **Import CA**, click **Browse** and locate the security certificate file that the server should use. Click **Upload**.

13. Check the displayed summary and use the **Previous** and **Next** options to readjust settings if necessary.

14. If **Generate New** was selected for the server's security certificate, download the security certificate files from the menu and store these safely. These certificates need to be used by the browser and other applications for future access to the server.

15. Follow the instructions for [adding a certificate to your browser](#)³⁴.

16. Click **Apply**. Click **OK** when displayed to access the server's Web Manager menus. Note that this can take up to 8 minutes.




2.9 Adding a Certificate to the Browser

For secure access to the server menus, the browser used requires the server certificate.

If using a certificate uploaded to the server, obtain a copy of the same certificate from the original source.

If using the server's own generated certificate, you can download from the ignition menu, or after ignition, from the [Certificates](#)^[113] section of the **Settings | General** menu. The server provides it certificate as a PEM or CRT file.


To add a server security certificate to Firefox:

1. Click the  icon and select  **Options**. Alternatively, click on the  **Settings** icon if shown on the browser home page.
2. Click **Advanced** and select **Certificates**.
3. Click **View Certificates**.
4. Click **Authorities**.
5. Click **Import**. Browse to the location of the CRT or PEM file downloaded from the server. Select the file and click **Open**.
6. Select all the check boxes to trust the certificate.
7. Click **OK** twice.

To add a server security certificate to Internet Explorer:

1. Click **Tools** and select **Internet Options**.
2. Select the **Content** tab and click **Certificates**.
3. Click **Import**.
4. Click **Next** and **Browse** to the location of the downloaded certificate. Select it and click **Open**.
5. Click **Next**. Click **Place all certificates in the following store**.
 - If using the server's own generated certificate, select the **Trusted Root Certification Authorities**.
 - If using a certificate from another source, select **Intermediate Certification Authorities**.
6. Click **Next** and then **Finish**.
7. Click **OK, Close**.
8. Click **OK**.

To add a server security certificate to Google Chrome:

1. Click the  icon and select **Settings**.
2. Click **Show advanced settings**. Scroll to **HTTP/SSL** and click **Manage certificates**.
8. Click **Import**.
9. Click **Next** and **Browse** to the location of the downloaded certificate. Select it and click **Open**.
10. Click **Next**. Click **Place all certificates in the following store**.
 - If using the server's own generated certificate, select the **Trusted Root Certification Authorities**.
 - If using a certificate from another source, select **Intermediate Certification Authorities**.
11. Click **Next** and then **Finish**.
12. Click **OK, Close**.

To add a server security certificate to Mac Safari:

1. From the browser, open the directory containing the certificate file.
2. Double-click the certificate.
3. You are prompted to store the certificate in the **login keychain** or the **system keychain**. To make the certificate available to all users of this system, select **system keychain**.

To add a server security certificate to Windows Safari:

1. From the browser, open the directory containing the certificate file.
2. Right-click the file and select **Install Certificate**. You may be prompted for admin credentials and/or a confirmation prompt.
3. On the first wizard screen, click **Next**.
4. On the **Certificate Store** screen select **Place all certificates in the following store**.
5. Click **Browse**.
6. Select the **Trusted Root Certification Authorities** option.
7. Click **OK**.
8. Click **Next**.
9. Click **Finish**. If another security warning dialog displays, click **Yes**.

2.10 Server Initial Configuration

The Management Services service which runs on the server requires some initial configuration. This is performed the first time you login into it using either IP Office Web Manager or IP Office Manager. This is especially important for servers centrally managed using Avaya System Manager.

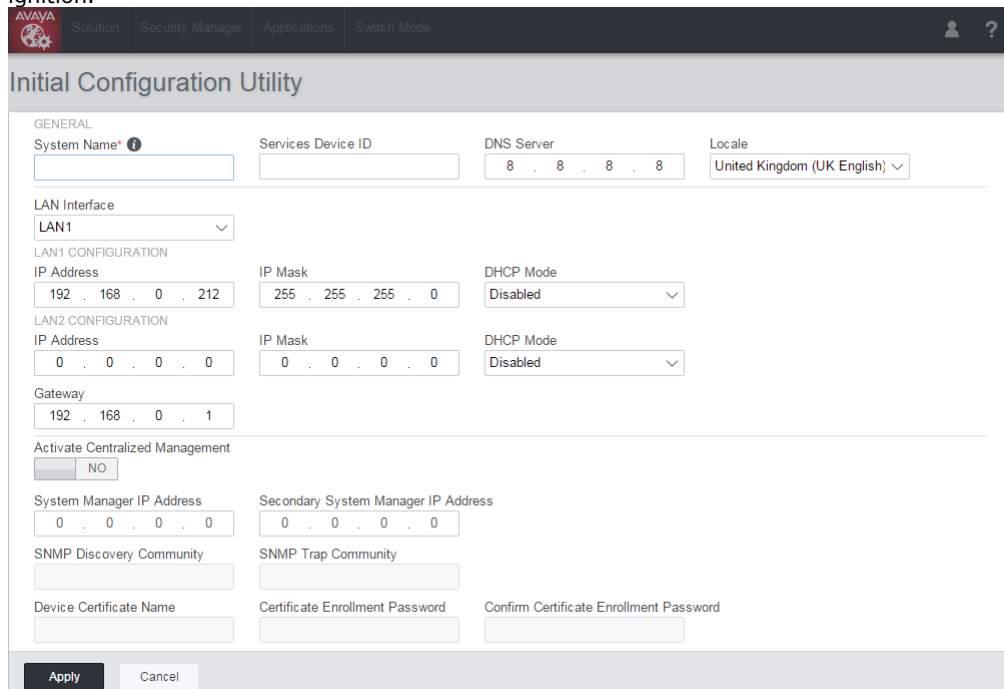
The following method does the initial configuration as part of the first login to IP Office Web Manager.

To perform initial configuration through IP Office Web Manager:

1. Log in to IP Office Web Manager.
 - a. Enter **https://** followed by the server address. Click on the **IP Office Web Manager** link.

The image shows the login page for Avaya IP Office Web Manager. On the left is a red vertical banner with the 'AVAYA' logo. To the right, the title 'Avaya IP Office Web Manager' is at the top. Below it are input fields for 'User Name' (containing 'Administrator'), 'Password' (masked with dots), and a 'Select Language' dropdown menu (set to 'English'). There is an unchecked checkbox for 'Offline management' and a 'Login' button at the bottom. A copyright notice '© 2015 Avaya Inc. All Rights Reserved.' is at the very bottom.

- b. Enter the user name **Administrator** and the password that was created for that user during ignition.
2. Web manager displays the initial configuration menu for the Management Services service. If this does not appear, click **Solution**. Most of the settings are automatically completed using the values you entered during module ignition.

The image shows the 'Initial Configuration Utility' web interface. At the top is a navigation bar with 'AVAYA', 'Solution', 'Security Manager', 'Applications', and 'Switch Mode'. The main title is 'Initial Configuration Utility'. Below this is a 'GENERAL' section with various configuration fields. 'System Name' is a text box. 'Services Device ID' is a text box. 'DNS Server' is a text box with '8 . 8 . 8 . 8'. 'Locale' is a dropdown menu set to 'United Kingdom (UK English)'. 'LAN Interface' is a dropdown menu set to 'LAN1'. Under 'LAN1 CONFIGURATION', 'IP Address' is '192 . 168 . 0 . 212', 'IP Mask' is '255 . 255 . 255 . 0', and 'DHCP Mode' is 'Disabled'. Under 'LAN2 CONFIGURATION', 'IP Address' is '0 . 0 . 0 . 0', 'IP Mask' is '0 . 0 . 0 . 0', and 'DHCP Mode' is 'Disabled'. 'Gateway' is '192 . 168 . 0 . 1'. There is a section for 'Activate Centralized Management' with a 'NO' button. Below that are fields for 'System Manager IP Address' (0 . 0 . 0 . 0), 'Secondary System Manager IP Address' (0 . 0 . 0 . 0), 'SNMP Discovery Community', 'SNMP Trap Community', 'Device Certificate Name', 'Certificate Enrollment Password', and 'Confirm Certificate Enrollment Password'. At the bottom are 'Apply' and 'Cancel' buttons.

3. Check the values are as expected:
 - If the module will be under centralized management from Avaya System Manager, select the **Centralized Management** checkbox. Enter the details required for Avaya System Manager.
4. Click **Apply**. The service is restarted using the values set in the menu. After the restart the browser is redirected to the normal web management menus.

2.11 Checking the Services

After logging in to the IP Office Application Server, the **System** page provides a summary of the services that the server can provide and the status (started or stopped) of those services. By default all the application services are set to automatically start. However, they may still require individual configuration and the addition of licenses to the IP Office configuration.

- **Management Services**

This is a shell version of IP Office that allows basic configuration of services such as remote SSL VPN connections for server support. It also controls security settings for access to the server's menus. It does not support call features such as users, extensions or trunks.

- **one-X Portal for IP Office**

This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely via web browser.

- **Voicemail Pro**

This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail.

- **Integrated Contact Reporter**

This new service is a small contact centre reporting tool. Refer to the separate Integrated Contact Reporter documentation for full details of configuration and use.

- **Web License Manager**

This service allows the server to act as a WebLM server. IP Office systems using PLDS licenses can then use the address of the server for license validation.

- **Web Manager**

You can configure and manage the server via browser access to the Web Manager menus. The menus also allow the launching of other clients used to configure and monitor the services run by the server.

- **Optional Services**

The server can include a number of additional services. Click **Show optional services** to display those services.

- **Equinox Select**

This is an WebRTC softphone that works with one-X Portal for IP Office and the WebRTC gateway services. Users can access it through their browser (currently Windows Chrome).

- **Web Collaboration**

This service works with one-X Portal for IP Office. It provides users with web collaboration services usable in parallel with audio conference hosted by the telephone system. In the parallel web collaboration session, users can share views of their desktop, documents, etc.

- **WebRTC Gateway**

This is a VoIP gateway service that allows the server to support user's making calls using WebRTC clients. Currently this is supported for Avaya Communicator for Web and for internal licensed web collaboration users.

- **Media Manager**

This application is an alternative to Contact Recorder for IP Office for the long term storage and retrieval of call recordings. The recordings are made by Voicemail Pro. Those recordings are then collected by Media Manager and stored by it.

- **Contact Recorder for IP Office**

Contact Recorder for IP Office is used in conjunction with Voicemail Pro for long term storage and retrieval of call recordings. The recordings are made by Voicemail Pro. Those recordings are then collected by Contact Recorder for IP Office and stored by it. For details on installation and support, refer to the Contact Recorder for IP Office Installation Manual. This service has been superseded by Media Manager but is still available for existing users.

To check the services:

1. Login and select the **System** menu.

Services		Start All	Stop All	
↓ Select which services will be configured to start automatically.				
<input checked="" type="checkbox"/>	Management Services 9.1.0.0 build 267	UpTime 49:00	Mem/CPU usage 146304K / 1%	Stop
<input checked="" type="checkbox"/>	Voicemail 9.1.0.0 build 68	UpTime 48:52	Mem/CPU usage 9912K / 0%	Stop
<input checked="" type="checkbox"/>	one-X Portal 9.1.0.0 build 107	UpTime 49:16	Mem/CPU usage 763316K / 0%	Force Stop
<input checked="" type="checkbox"/>	Web Manager 9.1.0.0 build 207	UpTime 50:37	Mem/CPU usage 348312K / 3.1%	Stop
> Show optional services				

2. Check that the expected services have been started. If not, start the required services using the **Start** buttons on the right. Select **Show optional services** to show all services.
 - The one-X Portal for IP Office service remains yellow until its configuration is completed.
 - Note that The **Voicemail** service shows green even if it is not connected to the IP Office due to a password mismatch.
3. Check the **Notifications** panel is not listing any errors that would indicate a problem with the installation.
4. If all the services are started as expected, you can now configure each service.

2.12 Application Configuration

The individual applications that the server is running for the IP Office systems now need to be configured. This requires entry of the appropriate licenses, user configuration and application configuration. This is covered in the following chapters. Key steps are:

1. For Voicemail Pro, the voicemail password set in the IP Office system's security settings must also be set in the voicemail server's preferences.
2. For one-X Portal for IP Office, the applications configuration menu needs to be run during which is it given details of the IP Office system it is supporting.

Chapter 3.

Voicemail Pro Configuration

3. Voicemail Pro Configuration

By default the Voicemail Pro application automatically provides basic mailbox services for all users and hunt groups in the IP Office configuration. For installations with just a single IP Office and Voicemail Pro server this normally occurs without any further configuration.

Details of IP Office and Voicemail Pro configuration are covered by the [Voicemail Pro Installation manual and Voicemail Pro Administration manuals](#)^[13]. This section of this manual covers only the minimum steps recommended to ensure that the voicemail server is operating.

Initial Configuration Summary

a. IP Office Configuration

- i. [Adding voicemail licenses](#)^[41]
- ii. [Check the Voicemail Type Setting](#)^[42]

b. Voicemail Pro Configuration

- i. [Install the Voicemail Pro client](#)^[43]
- ii. [Log in to the Voicemail Pro server](#)^[44]
- iii. [Change the voicemail server password](#)^[45]

Transferring Settings from a Previous Server

For an IP Office system already configured to operate with an external Voicemail Pro server; you can transfer the settings, prompts and messages on the old server to the new server. See [Transferring Voicemail Server Settings](#)^[46].

3.1 Adding Voicemail Licenses

The Voicemail Pro application will operate for up to 2 hours without a license. This allows a level of basic installation testing and configuration. However, for full operation the application must be licensed using licenses entered into the IP Office configuration.

For Voicemail Pro operation on IP Office Application Server, the following licenses are used:

- **Essential Edition**
This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
This license is required for use of the Voicemail Pro application. It also enables 4 voicemail ports. It is also required as a pre-requisite for the user profile licenses required for one-X Portal for IP Office users.
- **Preferred Edition Additional Voicemail Ports**
These licenses add additional voicemail ports in addition to the 4 enabled by the **Preferred Edition (Voicemail Pro)** license above.
- **Messaging TTS Pro**
This license enables the use of text-to-speech facilities using the optional Linux TTS software and user email reading. One license per simultaneous instance of TTS usage.

3.2 IP Office Configuration

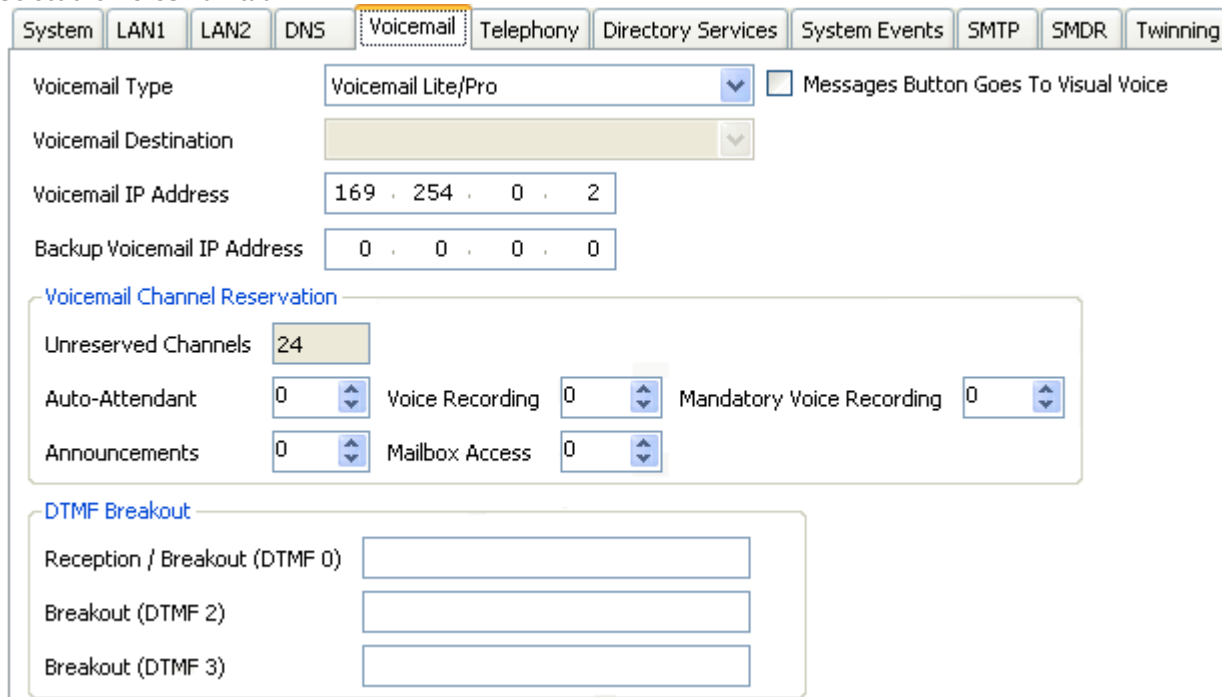
When a IP Office Application Server running Voicemail Pro is added, the IP Office system configuration needs to be adjusted to use the voicemail server. If a different role is intended for the voicemail server (see [Small Community Networks](#)^[14]), refer to the Voicemail Pro Installation Manual.

To set the voicemail server address:

1. Start IP Office Manager and receive the configuration from the IP Office system.

2. Select  **System**.

3. Select the **Voicemail** tab.



System LAN1 LAN2 DNS **Voicemail** Telephony Directory Services System Events SMTP SMDR Twinning

Voicemail Type Voicemail Lite/Pro ☐ Messages Button Goes To Visual Voice

Voicemail Destination

Voicemail IP Address 169 . 254 . 0 . 2

Backup Voicemail IP Address 0 . 0 . 0 . 0

Voicemail Channel Reservation

Unreserved Channels 24

Auto-Attendant 0 Voice Recording 0 Mandatory Voice Recording 0

Announcements 0 Mailbox Access 0

DTMF Breakout

Reception / Breakout (DTMF 0)

Breakout (DTMF 2)

Breakout (DTMF 3)

- Check that the **Voicemail Type** is set to **Voicemail Lite/Pro**.
- The **Voicemail IP Address** should be set to match the IP address given to the server hosting Voicemail Pro. For simplicity, if you only have the one voicemail server, an address of 0.0.0.0 tells the IP Office to broadcast a request for the voicemail server and to use the server that replies.
- In the **Voicemail Channel Reservation** section, the number of channels will be 4 plus any additional channels licensed.


4. Save any changes back to the IP Office system.

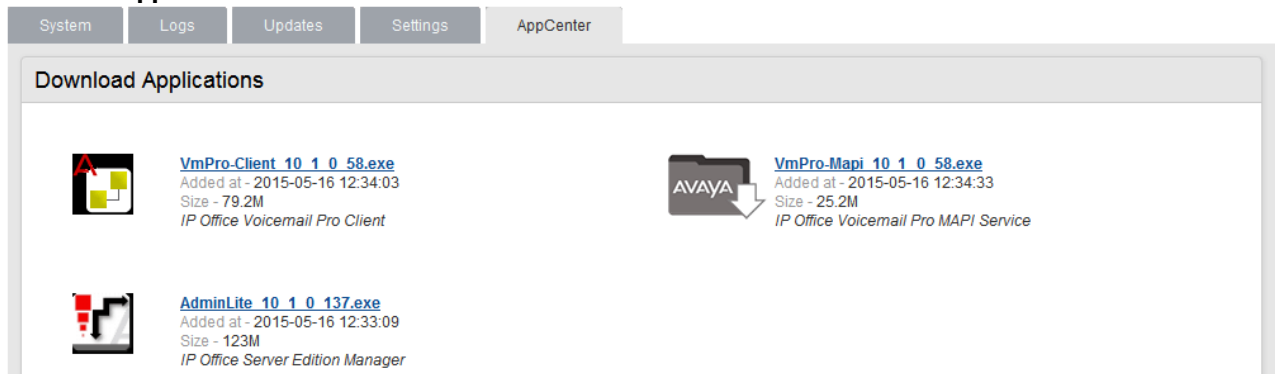
3.3 Installing the Voicemail Pro Client

You can install the Voicemail Pro client onto a Windows PC. You can then use it to remotely administer the voicemail server.

Using the following process you can download the software for installing the client from the server.

To download and install the Voicemail Pro client:

1. Log in to [wIP Office Web Manager](#)⁹⁹. In the displayed list of systems, click on the  icon next to the server and select **Platform View**.
2. Select the **AppCenter** tab.

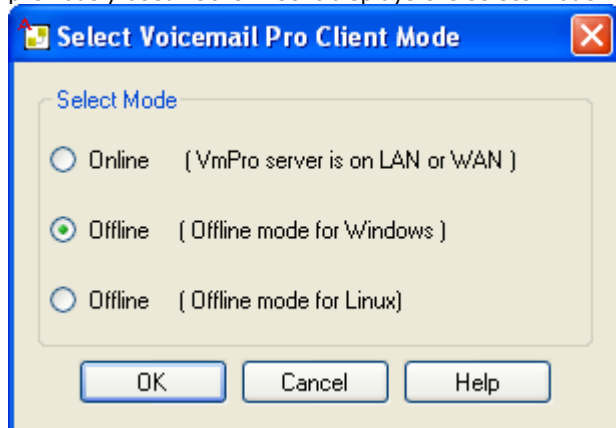


3. Click on the link for the Voicemail Pro client file in order to download the software package for installing the client.
4. Run the software package to install the Voicemail Pro client.

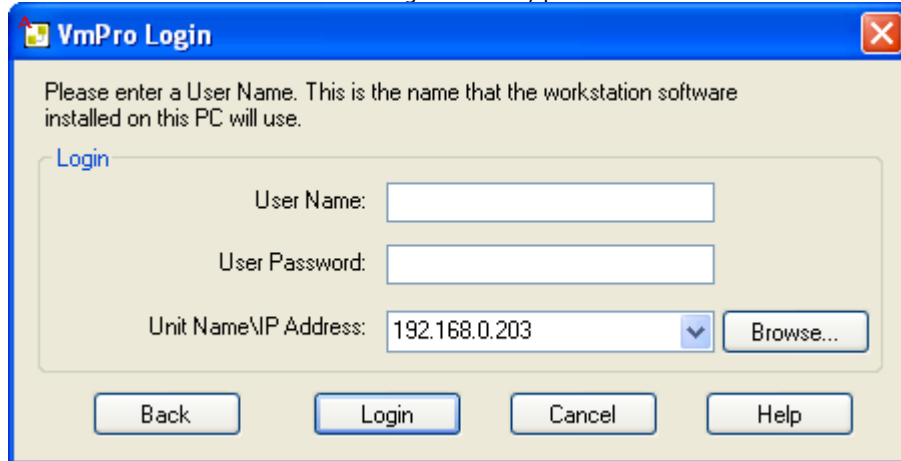
3.4 Logging in to the Voicemail Server

To login with the Voicemail Pro client:

1. From the **Start** menu, select **Programs | IP Office | Voicemail Pro Client**.
2. The Voicemail Pro Client window opens. If the client has run before, it attempts to start in the same mode as it previously used. Otherwise it displays the select mode menu.



3. Select **Online**. The menu for entering the name, password and details of the server appears.



4. Enter the **User Name** and **User Password** for an administrator account on the IP Office system.
5. In the **Unit Name\IP Address** field enter the DNS name or IP address of the voicemail server. Alternatively click on **Browse** to search the local network for a server and select a server from the results.
6. Click **Login**. If requested to download the call flows, select **Download**.

3.5 Changing the Voicemail Server Password


The connection between the IP Office and the Voicemail Pro services uses a password set in the IP Office security settings. When you change the password in the IP Office system's security settings, you must also change the password set in the voicemail server's preferences.

You can set the voicemail server preferences through IP Office Web Manager or using the Voicemail Pro client. Note that after changing the password, you do not need to restart the voicemail service. However, it may take a couple of minutes for the two systems to connect.

To change the voicemail server password using IP Office Web Manager:

1. Login to the IP Office Application Server server's IP Office Web Manager menus.
2. Click on **Applications** and select **Voicemail Pro - System Preferences**.
3. In the **Voicemail Password** box, enter the same password as set in the IP Office system's security settings.
4. Click **Update**.
5. When prompted to confirm the changes, click **Yes**.

To change the voicemail server password using the Voicemail Pro client:

1. Start the Voicemail Pro client and login to the server.
2. Click the  icon. Alternatively, from the **Administration** menu select **Preferences**.
3. Select the **General** tab.
4. In the **Voicemail Password** field, enter the same password that has been set in the IP Office system's security settings.
5. Click **Save & Make Live**.

3.6 Transferring Voicemail Server Settings

If the IP Office Application Server is replacing an existing voicemail server, you can transfer a backup of all the settings, prompts and messages to the new server. If the existing server is a Linux based server, use SSH file transfer to retrieve the backup files from the server. Otherwise, if Windows based, copy the folder from the server.

Then use SSH File transfer to transfer the backup file set onto the new server.

- **Backing Up/Restoring Custom Folders**

If the existing voicemail server uses folders outside its default folders those folders are not included in the backup/restore processes. To transfer additional folders see [Transferring Custom Folders](#)^[48].

To back up the old voicemail server:

Refer to the appropriate Voicemail Pro documentation for the release of Voicemail Pro server software.

To transfer the backup to a USB memory key:

The location of the backup files on the old server depends on whether it was a Windows based or Linux based server:

- **Windows Server**

You can select the backup location before starting the backup. The default location for backup files is **C:\Program Files\Avaya\IP Office\Voicemail Pro\Backup\Scheduled**.

1. Using **My Computer**, locate the previous manual backup. The date and time is part of the folder name for the backup.
2. Right-click on the folder and select **Properties**. Check that the Size on disk is within the capacity of the USB memory key.
 - If not, copy the backup folder and all its contents onto a PC from which you can eventually load it onto the new server using an SSH file transfer.
 - If with the USB memory key capacity, Copy the backup folder and all its content onto a USB memory key. Do not put the folder into another folder or change the folder name.

- **Linux Server**

The default location for backup files on a Linux server is **/opt/vmpro/Backup/Scheduled**.

1. Using an SSH file transfer tool, connect to the old server and browse to **/opt/vmpro/Backup/Scheduled/Immediate**.
2. Locate the manual backup taken above. The date and time is part of the folder name for the backup.
3. Copy the folder and all its contents onto the PC running SSH.
4. Right-click on the folder and select **Properties**. Check that the Size on disk is within the capacity of the USB memory key.
 - If not, copy the backup folder and all its contents onto a PC from which you can eventually load it onto the new server using an SSH file transfer.
 - If within the USB memory key capacity, copy the backup folder and all its content onto a USB memory key. Do not put the folder into another folder or change the folder name.

To shut down the old voicemail server:

Once you have backed up the server you can shut it down. This releases all the licenses it obtained from the IP Office system.

1. Once the backup above has been completed, select **File | Voicemail Shutdown | Shutdown**.
2. Select **Shut Down Immediately**. This will start a forced shutdown of the server, ending any currently active voicemail sessions.

To load the backup onto the new server from a USB memory key:

If you were able to load the voicemail backup onto a USB memory key, you can load it onto the Unified Communications Module server directly from the USB memory key.

1. Insert the USB memory key into one of the module's USB sockets.
2. Using a web browser, login to the server's web control menus.
3. Select **Settings**. On the **General** tab, select the **Restore** button for the Voicemail service. The list of available backups will include the one on the USB memory key.
6. Select the backup on the USB memory key and click **OK**.
7. Do not remove the USB memory key until all USB memory key activity has ceased.
8. After completing the restore, use the **System** menu to **Stop** and then **Start** the voicemail service.

To load the backup onto the new server using SSH:

Use the following method to transfer and then restore the backup.

1. Connect to the IP Office Application Server using an SSH File transfer tool.
2. Copy the backup folder into the folder **/opt/vmpro/Backup/Scheduled/OtherBackups**.
3. Using a web browser, [login](#) ⁷⁹ to the server.
4. Select **Settings**. On the **General** tab, select the **Restore** button for the Voicemail service. From the list of available backups, select the one just copied onto the server.
5. Click **OK**.
6. After completing the restore, use the **System** menu to **Stop** and then **Start** the voicemail service.

3.6.1 Transferring Custom Folders

Linux based servers do not include manually created folders in the backup or restore processes. Instead you need to copy the additional folders manually.

For example, if a folder containing custom prompts for use in call flows was created separate from the default language folders, that server does not automatically backup or restore that folder. To resolve this, you must backup and restore the additional folder manually. The following example copies a folder called **Custom** from an existing server to create a backup.

To manually backup a custom folder:

1. Using an SSH file transfer tool, copy the folder **Custom** from **/opt/vmpro** to your PC to create a backup of the folder.

To manually restore a custom folder:

1. To restore the folder, again using an SSH file transfer tool, copy the folder to the **/home/Administrator** folder on the server.
2. Using the SSH command line, you now need to copy the **Custom** folder from **/home/Administrator** to the **/opt/vmpro** folder.
 - a. Login to the system's command line interface using the existing root user password. You can do this either on the server or remotely using an SSH client shell application.
 - **If logging in on the server:**
 - a. At the **Command:** prompt, enter **login**.
 - b. At the **login:** prompt enter **Administrator**.
 - c. At the **Password:** prompt, enter the password for the user entered above.
 - d. To launch the Avaya command line interface, enter **/opt/Avaya/clish**.
 - **If logging in remotely:**
 - a. Start your SSH shell application and connect to the IP Office Application Server PC. The exact method will depend on the application used.
 - The **Host Name** is the IP address of the IP Office Application Server.
 - The **User Name** is **Administrator**.
 - The **Protocol** is **SFTP/SSH**.
 - The **Port** is **22**.
 - b. If this is the first time the application has connected to the IP Office Application Server, accept the trusted key.
 - c. When prompted, enter the Linux Administrator account password.
 - b. Enter **admin**. At the password prompt enter the admin password. The prompt should change to **Admin>**.
 - c. Enter **root**. At the password prompt, enter the current root user password.
 - d. When logged in, the prompt changes to something similar to **root@APPSDVD~]#**.
 - e. Change directory by entering **cd /home/Administrator**.
 - f. Move the **Custom** sub-folder to **/opt/vmpro** by entering **mv Custom /opt/vmpro**.
3. Using the SSH file transfer tool again, verify that the **Custom** folder has been copied to **/opt/vmpro** as required.

Chapter 4.

one-X Portal for IP Office Configuration

4. one-X Portal for IP Office Configuration

At this stage, whilst installed and started, the one-X Portal for IP Office server and IP Office still require some configuration. The following sections are a summary only. For full details, refer to the [one-X Portal for IP Office Installation manual](#)^[13].

Initial Configuration Summary

- a. [Add licenses](#)^[50]
Those IP Office users who want to use the one-X Portal for IP Office application need to have their **Profile** set to **Office Worker**, **Teleworker** or **Power User** and the **Enable one-X Portal Services** option selected. To do this requires the addition of licenses for those roles.
- b. [Enable one-X Portal for IP Office users](#)^[51]
When licenses are available, the number of licenses allows the configuration of the equivalent number of users for those roles and then for one-X Portal for IP Office usage.
- c. [one-X Portal for IP Office configuration](#)^[52]
Having licensed and configured some users for one-X Portal for IP Office, you need to login as the one-X Portal for IP Office administrator in order to perform initial one-X Portal for IP Office configuration.
- d. [Server Edition Server Configuration](#)^[56]
If using the server to support a Server Edition Primary Server or Server Edition Secondary Server, some configuration of the Server Edition server is required.



4.1 Adding Licenses

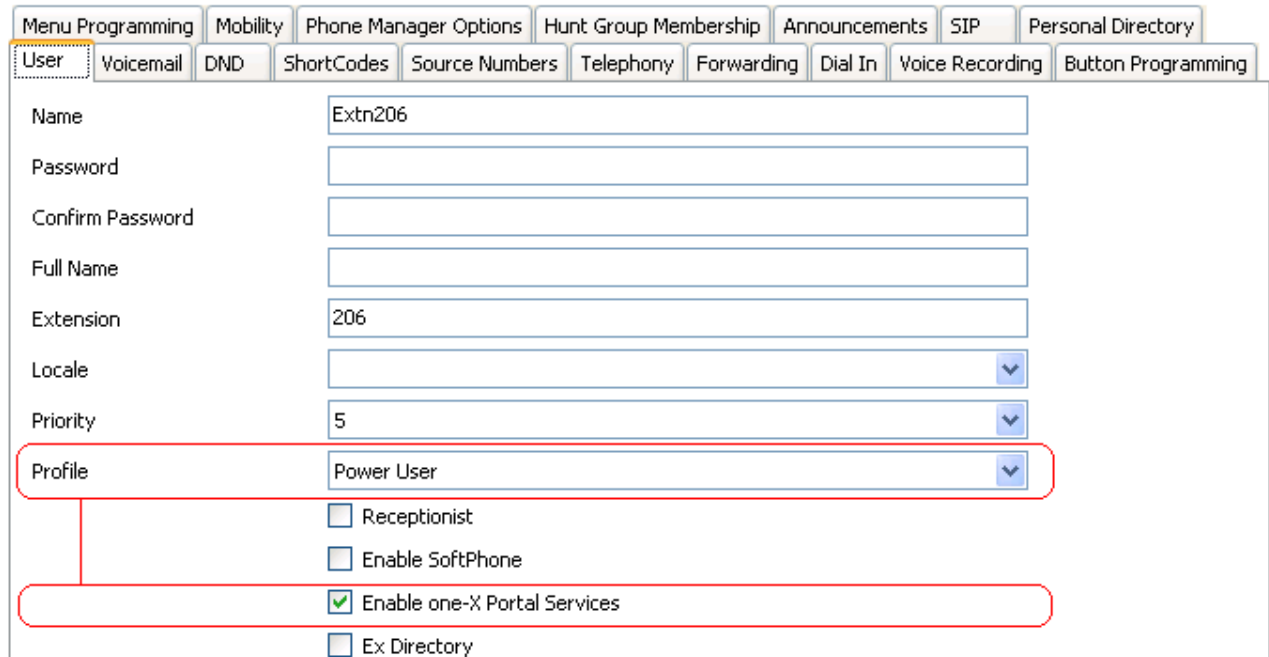
In order to log into and use the one-X Portal for IP Office application, a user must have their **Profile** setting in the IP Office configuration set to one of the following user profile roles: **Office Worker**, **Teleworker** or **Power User**. To do that requires matching **Office Worker**, **Teleworker** or **Power User** licenses in the system configuration.

4.2 Enabling one-X Portal for IP Office Users




Those users who want to use the one-X Portal for IP Office application need to have their **Profile** set to **Office Worker**, **Teleworker** or **Power User** and the **Enable one-X Portal Services** option selected. This requires [available licenses](#) for those roles.


To enable one-X Portal for IP Office users:

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 configuration settings.
4. Click on  **User**.
5. Select the user who you want to enable for one-X Portal for IP Office operation. 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 
☐ Receptionist
☐ Enable SoftPhone
☒ Enable one-X Portal Services
☐ Ex Directory

6. Change the user's **Profile** to **Office Worker**, **Teleworker** or **Power User**.
7. Select the **Enable one-X Portal Services** check box.
8. Note the user **Name** and **Password**. The user uses these to login to one-X Portal for IP Office.
10. Repeat the process for any other users who will use one-X Portal for IP Office.
11. Click on  to save the updated configuration back to the IP Office system.

4.3 one-X Portal for IP Office Configuration

The initial one-X Portal for IP Office configuration is done using web browser access to the administrator address.

To login to one-X Portal for IP Office:

1. Open a web browser and enter **https://** followed by the IP address of the IP Office Application Server and then **:9443/onexportal-admin.html**.
2. The login menu appears. If the message **System is currently unavailable - please wait** appears, the one-X Portal for IP Office application is still starting. When the message disappears, you can login.
3. Enter the default administrator name (**Administrator**) and password (**Administrator**) and click **Login**.
4. The **License Agreement** page appears. When you have read the license, select **Have Read & Agree** and then click on **Next**.
5. The menu now allows entry of the IP address of the IP Office system to which you want the one-X Portal for IP Office server to connect.

STEP 2: Setting the IP Office IP Addresses

Description

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

For example enter: 192.168.42.1,192.168.42.2

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

IP Office Unit IP Address(es)

192.168.42.1

IP Office(s) not yet checked.

☒ Simple Installation ☐ Advanced Installation

► Status

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

- In the following menus, the ► **Status** icon is used to show/hide status messages about the installation process.
 - You can enter the addresses of multiple IP Office systems in your network. For IP Office Release 10 and higher, you can enter just one address. The one-X Portal for IP Office is informed by that system about the others systems in the network and about the voicemail server. However takes a while to occur after initial installation and assumes that the security settings of all the systems are the same. If you want to configure portal resiliency at this stage, enter the address of both the primary and secondary IP Office systems.
6. Enter the addresses in the form and select **Check IP Office(s)**. The one-X Portal for IP Office server will attempt to connect to each of the indicated systems. The amber background will change to green if this is successful.

IP Office Unit IP Address(es)

192.168.42.1

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

☒ Simple Installation ☐ Advanced Installation

► Status

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

7. Click on **Advanced Installation** and expand the **Advanced Provider Options** section.

☐ Simple Installation ☒ Advanced Installation

▼ Advanced Provider Options

► Description:

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

Mid-Layer Host Name localhost

Mid-Layer Port 8080

Mid-Layer Service Name inkaba

- a. Select **Telephony (CSTA)**. If you changed the password used for the IP Office system's **EnhTcpsaService** user (see [Changing the IP Office Security Settings](#)^{19h}), set the same password here.

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider	IM/Presence
Provider's Mid-Layer Username	indoda_user				
Provider's Mid-Layer Password	●●●●●●●●				
Provider runs on Port	8080				
Common SAP Username	EnhTcpsaService				
Common SAP Password	●●●●●●●●				

- b. Select **Directory (IP Office)**. Check that the provider address and port match those expected.

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider	IM/Presence
Provider's Mid-Layer Username	indoda_user				
Provider's Mid-Layer Password	●●●●●●●●				
Provider runs on Port	8080				
Timeout	300				
DSML Provider IP Address	DSML Provider Port	Secure Connection			
192.168.0.214	443	<input checked="" type="checkbox"/>			
Delete					

- c. If the customer has an LDAP directory source that they want used for the external directory, select **Directory (LDAP)**. Enter the details for the LDAP connection.

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider	IM/Presence
Provider's Mid-Layer Username	indoda_user				
Provider's Mid-Layer Password	●●●●●●●●				
Provider runs on Port	8080				
LDAP Server Address	ldap://ldap-server-ip-a				
LDAP Server Username	globallyour-username				
LDAP Server Password					
LDAP Server Base DN	OU=myregion,OU=myt				

- d. Select **VoiceMail-Provider**. Enter the IP address of the voicemail server. If the application server is running the voicemail service, set this to the IP address of the application server.

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider	IM/Presence
Provider's Mid-Layer Username	izwi_user				
Provider's Mid-Layer Password	●●●●●●●●				
Provider runs on Port	8080				
Assign New Voicemail Server Unit					
ID	VoiceMailServer IP Address				
0	Enter valid ip address Delete				

- e. Select **IM/Presence**. Enter the DNS domain name that the server should use for IM/presence service.

Mid-Layer	Telephony (CSTA)	Directory (IP-Office)	Directory (LDAP)	VoiceMail-Provider	IM/Presence
XMPP Domain Name	localhost.localdomain				

8. Note: This step is only possible if the addresses of both the primary and secondary IP Offices were entered at the start. If the application server is going to be used to support a Server Edition network, expand the **Resiliency Configuration** option. In a Server Edition network, separate portal services can be associated with the network's primary server and its secondary server. While normally only the primary portal server is active, the secondary can become active if the primary is unavailable for some reason. For further details of portal resiliency, refer to the Administering Avaya one-X Portal for IP Office manual.

☐ Simple Installation ☒ Advanced Installation

► Advanced Provider Options

▼ Resiliency

Resiliency Configuration

☒ Enable Resiliency
 This one-X Portal is: Secondary ▼

	FQDN/IP Address
Primary one-X Portal	135.64.43.157
Primary IP Office	135.124.57.122
Secondary one-X Portal	135.64.43.24
Secondary IP Office	135.124.57.94

Note: Resiliency is a feature provided only for IP Office Server Edition platform.

► Status

- If the application server is supporting the primary server in a Server Edition network and portal resiliency is required, select **Primary**.
- If the application server is supporting the secondary server in a Server Edition network and portal resiliency is required, select **Secondary**.
- Complete the table of addresses for the primary and secondary portal and IP Office services.

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

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

Description

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

► Status

Automatic User List Extraction Progress

10. Having extracted user details, the one-X Portal for IP Office server extracts 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

11. The one-X Portal for IP Office server now prompts you to change the password used for administrator access.

Change Local Account Password

Password Complexity Requirements:

1. Minimum Password length supported is 8 characters
2. Used password characters must include characters from at least 2 of the 'code point sets' listed below.
For example a mix of lower case and upper case. In addition, there should not be any adjacent repeated characters of any type.
 - a. Lower-case alphabetic characters.
 - b. Upper-case alphabetic character.
 - c. Numeric characters.
 - d. Non-alphanumeric characters (for example # or *).

Account Name:

New Password:

Confirm New Password:

Administrator password cannot be blank.

- a. Enter a new password and click **Change Password**. The initial configuration is complete. Note that it will still be at least another 5 minutes before the one-X Portal for IP Office is usable by end users.
 - b. You now have access to the one-X Portal for IP Office administration menus. For full details refer to the [Administering one-X Portal for IP Office](#) ¹³ manual.
12. Click on **Log Out**.
13. Click on **User Login** shown top-right.
14. The login window will display **System in currently unavailable**. When this message is no longer displayed, attempt to login as a user.

4.4 Primary/Secondary Server Configuration


If the IP Office Application Server is to provide portal services for a Server Edition network, it requires additional configuration. This is done through the Web Manager menus of the Server Edition Primary Server.

For IP Office Release 10 and higher, the Server Edition Secondary Server also runs a portal service for use in portal resilience (for further details of portal resiliency, refer to the Administering Avaya one-X Portal for IP Office manual). This portal service can also be replaced by a separate application server.

Summary:

1. Disable the one-X Portal for IP Office service on the Server Edition Primary Server.
2. Add the application server to the primary server's IP Office Web Manager menus.
3. Add the address of the application server to the primary server's web control menus.


To disable the primary server's port service:

1. [Login](#)  to the primary or secondary server and access its platform view.
2. Stop the **one-X Portal** service if running and ensure that the auto-start box is unchecked.
 - In addition on the **Updates** tab you can select to **Uninstall** the **one-X Portal** service.

To add the application server:

1. Login to the primary or secondary server and select the **Solution** view.
2. Click on **Solution Settings** and select **Application Server**.
3. Enter the address of the application server and click **Add**.

To enter the address of the remote one-X Portal:

1. [Login](#)  to the primary or secondary server and access its platform view.
2. Select **Settings** and then **General**.
3. In the **one-X Portal Settings** section, untick **Use Local IP**.
4. In the **Remote IP** field enter the address of the application server that is running the alternate portal service.
5. Click **Save**.

4.5 Initial AFA Login

This process is only necessary if not using [Referred Authentication](#) ⁽¹⁶⁾ for administrator security. You can use the AFA menus to perform backup and restoration operations. Even if not used, you should login in order to change the menu's default password.

To login to the one-X Portal for IP Office AFA service:

1. Open a web browser and enter **https://** followed by the IP address of the IP Office Application Server and then **:9443/onexportal-afa.html**.
2. At the login menu, enter the name **Superuser** and the associated password. The default password is **MyFirstLogin1_0**. After logging with the default password you are prompted to change that password:

Change Local Account Password

Password Complexity Requirements:

1. Minimum Password length supported is 8
2. The password characters must include characters from at least 2 of the 'complexity rules' listed below.
For example a mix of lower case and upper case. In addition, three or more repeated characters of the same case are not allowed.

- a. Lower-case alphabetic characters.
- b. Upper-case alphabetic characters.
- c. Numeric characters.
- d. Non-alphanumeric characters (for example # or *).

Display Name

Password

Confirm Password




- **Display Name**
Enter a name for display in the one-X Portal for IP Office menus.
- **Password/Confirm Password**
Enter a password that will be used for future access.

4.6 If the Portal Service Status Remains Yellow

The most likely cause for the one-X Portal for IP Office service not working and remaining yellow in the platform view of the services is a password mismatch.

The mismatch is between the **EnhTcpsaService** service user in the IP Office system's security settings and two of the providers within the portal configuration (the **Default-CSTA-Provider** and the **Default-DSML-IPO-Provider**). This password mismatch causes the IP Office to automatically lock the **EnhTcpsaService** user account.

To reset the portal and IP Office passwords:

1. Change the portal provider passwords to the new, strong password:
 - a. Login to the portal services administrator menus. You can do this by logging in to the portal server's Web Manager menus, clicking on Applications and selecting one-X Portal.
 - b. Click **Configuration** and select **Providers**.
 - c. Set the **Provider Name** field to **Telephony (CSTA)**.
 - d. Click on the  edit icon next to the listed provider.
 - e. Set the **Password** and click **Save**.
 - f. Set the **Provider Name** field to **Directory (IP-Office)** and repeat the process.
2. Stop the one-X Portal for IP Office service:
 - a. Login to the server's web manager menus.
 - b. From the Solution page, click on the  icon next to the portal server and select **Platform View**.
 - c. Stop the **one-X Portal** service. Wait until the status icon changes to red.
3. Change the password of the IP Office EnhTcpsaService service user:
 - a. Click on **Security Manager** and select **Service Users**.
 - b. Click on the  edit icon for the **EnhTcpsaService** user.
 - c. Set the **Password** to the same as was set for the portal providers above and click **Save**.
 - d. Change the **Account Status** back to **Enabled**.
 - e. Click **Update**.
4. Restart the one-X Portal for IP Office service:
 - a. Select the platform view for the portal server again.
 - b. Start the **one-X Portal** service. Wait for the status icon to change to green. This can take up to 5 minutes.

4.7 Transferring one-X Portal for IP Office Settings

If the IP Office Application Server is replacing an existing one-X Portal for IP Office server, you can transfer a backup of all the previous settings to the new server. The backup and restore process can use either an intermediate FTP file server or can use files downloaded and restored to and from the browsing PC.

To back up the one-X Portal for IP Office:

The backup process creates a zip file with the date and time added to the file name of the zip file.

1. Browse to the old server using the address ***http://<server>:8080/onexportal-afa.html*** where *<server>* is the name or the IP address of the server.
2. At the login menu, enter the name **Superuser** and enter the associated password.
3. Select **DB Operations**.
4. Select **Backup**.
5. For **Backup To** select either **FTP** (an FTP server) or **Local Drive** (the PC from which you are browsing). If you select FTP, you will also need to complete address, name and password settings for uploading files to the FTP server.
6. Click **Backup**.

To restore the one-X Portal for IP Office settings:

1. Browse to the new server using the address ***http://<server>:8080/onexportal-afa.html*** where *<server>* is the name or the IP address of the server.
2. At the login menu, enter the name **Superuser** and enter the associated password.
3. Select **DB Operations**.
4. Select **Restore**.
5. For **Restore From** select either **FTP** (an FTP server) or **Local Drive** (the PC from which you are browsing). If you select FTP, you will also need to complete address, name and password settings uploading files to the FTP server.
 - If you select **FTP**:
 - a. Click **Show Available Backups**.
 - b. Select the backup to restore and click **Restore**.
 - If you select **Local Drive**:
 - a. Use the **Browse** option to select the backup file.
 - b. Click **Restore**.

Chapter 5.

WebRTC Configuration

5. WebRTC Configuration

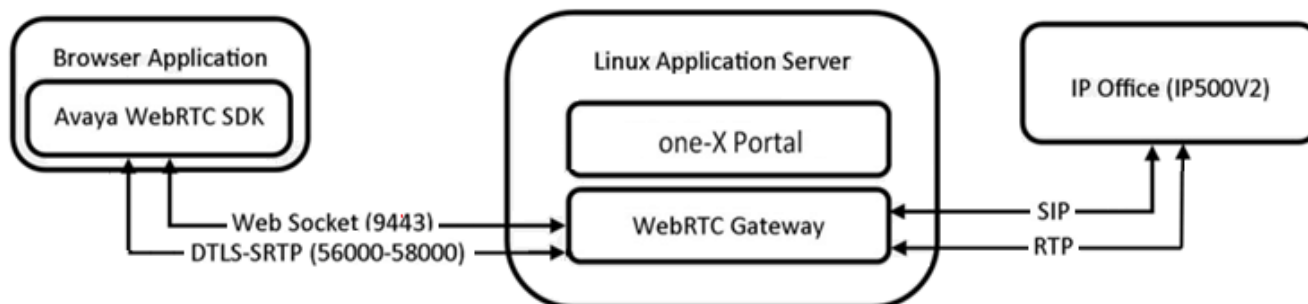
WebRTC (Web Real-Time Communication) is a set of communications protocols that allows web browsers to communicate with servers to share information in realtime including audio and video. Linux-based servers support a WebRTC Gateway service that can be used for a number of roles.

Support for:

- **Aura Call Center Elite Agent App**
- **IPOCC Chrome Client**
- **Avaya Communicator for Web**
- **Web Collaboration**
- **WebRTC SDK**

The IP Office WebRTC SDK is available through the Avaya DevConnect program and allows developers to create their own WebRTC applications.

This document covers the configuration for supporting the WebRTC with an IP500 V2 and application server.



5.1 Equinox Select Overview

When being used to provide portal services to an IP500 V2, the application server can be used to also support the Equinox Select client.

- The Equinox Select is a softphone useable through a web browser interface.
- It is currently supported with Windows Chrome only.
- It supports audio calls. For calls to another Equinox Select user it also supports video.

System Requirements

- IP Office Release 10.1.
- System licenses to support one-X Portal for IP Office.
- The application server can act as the WebRTC proxy for a single IP500 V2 system. Only users registered on that system, even if it is in an SCN, can use the client. However, client users can make and receive calls from other users within the SCN.

User Requirements

- The user must be configured on the IP500 V2 system associated with the one-X Portal for IP Office.
- The user does not have to be configured with or associated with a SIP extension.
- Licensed and configured as one-X Portal for IP Office user.
- PC with speaker and microphone. Option camera for video calls.
- Windows Chrome.
- The user browser needs to be configured with the server certificate.


Process Summary

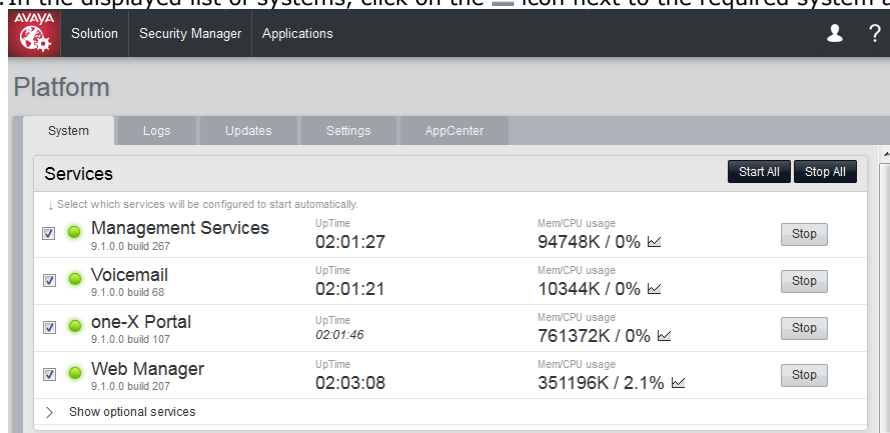
1. [Configure and test one-X Portal for IP Office operation](#) ⁵⁰
2. [Enable the IP Office for SIP extension operation](#) ⁶⁵
Note that this will require the IP Office system to be restarted, stopping any current calls in progress.
3. [Enable the optional WebRTC Gateway and Equinox Select services](#) ⁶⁵
4. [Configure the WebRTC Gateway service](#) ⁶⁷
5. [Testing operation](#) ⁷⁰
 - a. [Adding the security certificate](#) ⁷⁰
 - b. [Logging in](#) ⁷¹
 - c. [Downloading the client application](#) ⁷²

5.2 Enable the Optional Services

In addition to the portal service, the Equinox Select client uses two additional services on the application server.

To enable the optional services:

1. [Login](#) to the server's web configuration menus.
2. Click **Solutions**.
3. In the displayed list of systems, click on the  icon next to the required system and select **Platform View**.



4. Click on **Show optional services**.
5. Check that both the **Equinox Select** and **WebRTC Gateway** services are ticked to automatically start.
6. Check that both services have started. If necessary click the **Start** button next to the service if not already started.

5.3 Enabling SIP Extension Support

To allow the use of the WebRTC clients, the IP Office system needs to be configured as a SIP registrar to support SIP extensions.

- **Reboot Required**

Note that changing the SIP registrar settings of an IP Office system requires the IP Office system to be rebooted.

To enable SIP extension support:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** or **System Settings | System**.
3. Select **LAN1** or **LAN2** as required and then select the **VoIP** tab.

The screenshot shows the IP Office configuration interface. On the left is a sidebar with a tree view containing: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (selected), LAN2, VoIP, VoIP Security, Voice Compression Module (VCM), Directory Services, Telephony, and Contact Center. The main area has tabs for LAN Settings, VoIP, and Network Topology. The VoIP tab is active, showing configuration for H.323 GATEKEEPER and SIP REGISTRAR. The H.323 GATEKEEPER section includes 'H.323 Gatekeeper Enable' (YES), 'H.323 Signaling Over TLS' (Preferred), 'Auto-create Extension' (NO), 'H.323 Remote Extension Enable' (YES), and 'Remote Call Signaling Port' (1720). The SIP REGISTRAR section includes 'SIP Trunks Enable' (YES), 'SIP Remote Extension Enable' (NO), 'Challenge Expiry Time (sec)' (10), 'SIP Registrar Enable' (YES), 'Auto-create Extension/User' (NO), 'SIP Domain Name' (example.com), and 'SIP Registrar FQDN' (ip500.example.com). The LAYER 4 PROTOCOL section includes 'UDP' (YES), 'TCP' (YES), 'TLS' (NO), 'UDP Port' (5060), 'TCP Port' (5060), and 'TLS Port' (5061). Red boxes highlight the SIP REGISTRAR and LAYER 4 PROTOCOL sections.

- **SIP Registrar Enable**
Check that **SIP Registrar Enable** is selected.
- **Auto-create Extn/User: Default = Off**
When this option is selected, the IP Office automatically creates user and SIP extension entries in its configuration based on SIP extension registration.
- **! WARNING**
Leaving this settings enabled is strongly deprecated. For Release 9.1 and higher, the system automatically disables the settings 24-hours after it is enabled.
- **SIP Remote Extn Enable: Default = Off**
Currently remote SIP extension options are only supported for Avaya SIP client applications. Remote connection is not supported for third-party SIP devices.
- **SIP Domain Name: Default = Blank**
This value is used by SIP endpoints for registration with the system. The entry should match the domain suffix part of the **SIP Registrar FQDN** below, for example *example.com*. If left blank, registration uses the LAN IP address which is only suitable for internal access.
 - Note: For Avaya SIP telephones supported for resilience, the **SIP Domain Name** must be common to all systems in the network.
 - This is the local SIP registrar domain name that needed by SIP devices in order to register with the IP Office. If you are using TLS, this value needs to be included in the security certificates applied to the IP Office and, if used, separate HTTP file server.

- **SIP Registrar FQDN:** *Default = Blank*

This is the fully-qualified domain name, for example *server.example.com*, to which the SIP endpoint should send its registration requests. This address must be resolvable by DNS to the IP address of the IP Office system. When using external SIP devices, this address must be resolvable both internally and externally using a method such as split DNS. This setting is not used for Equinox Select.

- **Layer 4 Protocol:** *Default = Both TCP & UDP*

These fields set the transport protocol for SIP traffic between the IP Office and SIP extension devices. This should match the **Transport Type (TCP or TLS)** selected in the [WebRTC Gateway's settings](#)^[67].

- Do not enable a protocol unless it is intended to be used. Clients only use the first enabled protocol that they support in the order TLS, TCP, UDP. They will not fallback to another enabled protocol if problems are encountered in the highest protocol. For example, if TLS is enabled the phone will attempt to use TLS (for example requesting certificates etc) and will not fallback to TCP or UDP if TLS operation is not correctly configured.

- **UDP Port:** *Default = Enabled/5060*

The SIP port used if using UDP. The default is 5060.

- **TCP Port:** *Default = Enabled/5060*

The SIP port used if using TCP. The default is 5060.

- **TLS Port:** *Default = Disabled/5061*

The SIP port used if using TLS. The default is 5061. This option requires server certification to be applied to the IP Office system and to any phone file server. Do not enable TLS and connect phones until the correct server certification has been complete.

- **Challenge Expiry Time (sec):** *Default = 10*

The challenge expiry time is used during SIP extension registration. When a device registers, the system sends back a challenge and waits for a response. If the response is not received within this timeout the registration fails.

- **Port Number Range (Min-Max)**

These fields set the port range used by the IP Office service. Ensure that these do not overlap with the public port range configured for the WebRTC Gateway.

5. If you have made any changes, save the configuration back to the IP Office.

5.4 Configuring the WebRTC Gateway

The following settings are for the WebRTC gateway service being run by the application server.

To enable the WebRTC gateway:

1. [Login](#) ⁷⁷ to the server's web configuration menus.

2. Click **Solutions**.

3. Click **Applications** and select **WebRTC Configuration**.

- **! Important**

To access the WebRTC Gateway configuration settings in IP Office Web Manager, you must log account must belong to a security rights group that has WebRTC Gateway Administrator rights enabled. That is configured through the servers security setting using IP Office Manager.

4. On the **System Settings** menu, check the settings:

WebRTC Gateway

System Settings	SYSTEM SETTINGS		
SIP Server Settings	Network Interface	Local IP Address	
Media Gateway Settings	eth0	192 . 168 . 0 . 213	
	Gateway Listen Port	SIP Trunk Listen Port	Logging Level
	42004	42008	Info

- **Network Interface**

For information only. This is the server interface used by the gateway service.

- **Local IP Address**

For information only. This is the current IP address associated with the selected **Network Interface**.

- **Gateway Listen Port**

This is the port on which the gateway listens for any incoming calls from the IP Office system. This setting is used when configuring an application server for operation with an IP500 V2.

- **SIP Trunk Listen Port**

This is the port on which the gateway listens for SIP trunk connections from the IP Office system. Not currently used.

- **Logging Level**

This sets the level of logging used by the gateway. The log files, prefixed **WebRTCGateway**, can be downloaded through the server's web control/platform view menus (**Logs | Download**). The default setting is **Info**.

5. Click **Save** to save any changes.

6. On the **SIP Server Settings** menu, adjust the settings to match the SIP extension configuration of the IP Office system:

WebRTC Gateway

System Settings	SIP SERVER SETTINGS		
SIP Server Settings	Configuration Mode	Domain Name	Private IP Address
Media Gateway Settings	Manual	example.com	192 . 168 . 0 . 200
	Private TCP Port	Private UDP Port	Private TLS Port
	5060	5060	5061
	Public IP Address	Public TCP Port	Public UDP Port
	0 . 0 . 0 . 0	5060	5060
	Public TLS Port	Transport Type	
	5061	TCP	

- **Configuration Mode**

For Server Edition servers the **Automatic** setting can be used. That automatically configures the gateway to match other IP Office service settings. For an application server, select **Manual**.

- **Domain Name**

Set this field to match the domain name configured in the [SIP Registrar settings](#) ⁶⁵ of the IP Office system.

- **Private IP Address**

Set this to the address of the IP Office system configured as the SIP registrar for WebRTC client users.

- **Private TCP Port/Private UDP Port/Private TLS Port**

Set these fields to match the protocol ports configured for the SIP registrar on the IP Office.

- **Public IP Address**

Leave this set to 0.0.0.0 to use the application server's IP address.

- **Public TCP Port/Public UDP Port/Public TLS Port**

Use these fields to set the ports that should be used for each protocol by client applications.

- **Transport Type**

Select the protocol that the gateway and clients should use. TCP or TLS are supported for Equinox Select. This must match the **Layer 4 Protocol** settings of the [IP Office SIP Registrar](#)⁶⁵.

- Do not enable a protocol unless it is intended to be used. Clients only use the first enabled protocol that they support in the order TLS, TCP, UDP. They will not fallback to another enabled protocol if problems are encountered in the highest protocol. For example, if TLS is enabled the phone will attempt to use TLS (for example requesting certificates etc) and will not fallback to TCP or UDP if TLS operation is not correctly configured.

7. Click **Save** to save any changes.

8. Select the **Media Gateway Settings** menu and adjust the settings if required:

- **RTP Port Range (Private)**

These fields set the minimum and maximum RTP ports for connections between the gateway services and the IP Office system.

- **RTP Port Range (Public)**

These fields set the minimum and maximum RTP ports for connections from the WebRTC clients. If supporting external clients, these ports should be allowed for routing to the gateway server in the customer's external firewalls. Ensure that these do not overlap with the RTP port range configured for the IP Office SIP registrar.

- **Codecs - Audio**

Use this list to adjust the order of codec preference. It is recommended that both the PCM codec choices are kept at the top of the list.

- **Codecs - Video**

Currently **VP8** is the only supported video codec.

- **DTMF Payload Type: Default = 101**

This field set the default value for RFC2833 payload negotiation. This value is used with clients and services that do not support dynamic payload negotiation.

- **STUN/TURN Settings**

The following setting allow the media gateway to be used with external clients via STUN and TURN servers. If enabled, the settings need to match the STUN/TURN server. For details of doing this with an Avaya Session Border Controller for Enterprise, refer to the "IP Office SIP Phones with ASBCE" manual.

- **STUN Server Address: Default = 0.0.0.0 (Disabled)**

The gateway service can use STUN to attempt to resolve issues caused by network address translation (NAT) being applied to traffic between it and external clients. The gateway attempts to use STUN if a STUN server address is set.

- **STUN Server Port:**

Sets the port used for connection to the STUN server. The default is 3478.

- **TURN Server Address:** *Default = 0.0.0.0 (Disabled)*
The gateway service can use TURN to attempt to resolve issues caused by network address translation (NAT) being applied to traffic between it and external clients. Unlike STUN, all traffic is routed via a TURN server. The gateway attempts to use TURN if a TURN server address is set.
- **TURN Server Port:**
Sets the port used for connection
- **TURN User Name/TURN Password:**
Enter the name and password of the account on the TURN server if authentication is being used.

9. Click **Save** to save any changes.

5.5 Testing Operation

1. Add the Server Security Certificate:

Download a copy of the CA certificate used to sign the server's own identity certificate. Install the CA certificate in the browser's certificate store.

2. Login to Equinox Select using the browser:

Login to https://<gateway_address>:9443/equinox.

3. Install the Client Application


If required, an application to provide Equinox Select is a minimal window can be installed and used to access the application.

5.5.1 Adding the Server Certificate

Initial Equinox Select access to the server uses secure access. The browser used therefore needs to have a copy of the same CA certificate as used to sign the application server's own identity certificate.

- If the server is using its own auto-generated certificate, you can download the certificate from the **Certificates** section of the **Settings | General** menu. Download the DER-encoded certificate (a CRT file).
- If the server is using an identity certificate generated elsewhere and then uploaded to the server, obtain a copy of the CA certificate from the same source.

To add a server security certificate to Google Chrome:

1. Click the  icon and select **Settings**.
2. Click **Show advanced settings**. Scroll to **HTTP/SSL** and click **Manage certificates**.
3. Click **Import**.
4. Click **Next** and **Browse** to the location of the downloaded certificate. Select it and click **Open**.
5. Click **Next**. Click **Place all certificates in the following store**.
 - If using the server's own generated certificate, select the **Trusted Root Certification Authorities**.
 - If using a certificate from another source, select **Intermediate Certification Authorities**.
6. Click **Next** and then **Finish**.
7. Click **OK, Close**.

5.5.2 Logging In

To login to Equinox Select using Chrome:

1. Check that the PC has microphone and speaker facilities connected and enabled.
2. Start Windows Chrome.
3. Browse to https://<application_server>:9443/equinox where *<application_server>* is the IP address or fully-qualified domain name of the application server.
4. The browser prompts you that the site want to **Show notifications**. Select **Allow**. This is essential for functions such as answering incoming calls.
5. When prompted, enter the user name and password.
6. Click **Login**.
7. If prompted, allow the application to use your microphone and or camera.
8. Make a test call to another extension.

There is a Windows client application that can be used to provide access to the client. See [Downloading the Client Application](#).

To start the Windows application:


1. Click on the Avaya Equinox Select icon on the desktop or select it from the programs list.
2. Enter the server IP address or name. You do not need to add the **https:** or **:9443** details.
3. When prompted to **Show Notifications**, select **Allow**.
4. Enter your user name and password and click **Login**.
5. If prompted, allow the application to use your microphone and or camera.

5.5.3 Downloading the Client Application

Whilst users can access the client through [their browser](#)^[71], it may be more convenient to access it in a window that has the minimum of other menus, maximising space for the client. This can be done in a number of ways:


To add the client as a Chrome desktop application:

This creates a desktop shortcut that will launch the client in a basic browser window (ie. title bar only, no other Chrome menus visible).

1. [Login using Chrome](#)^[71] as normal.
2. Click on the browser's  options icon (not the one for Equinox Select).
3. Select **More Tools | Add to desktop**.
4. Select **Open as window**.
5. Click **Add**.

To install the Windows application:

This installs a Windows application that creates a menu-less window for the client to run in.

1. Download the client application installer. This can be done in a number of ways:
 - From within Equinox Select: Click the  icon and select **Downloads | Avaya Equinox Select client for Windows**.
 - From within one-X Portal for IP Office: Click on **Configure** and select the **Desktop Integration** tab. Select **Download installer for Equinox Select client**.
2. Locate the downloaded file (*AvayaEquinoxSelect.exe*).
3. Right-click on the file and select **Run as administrator**.
4. Select the language for installation. This does not affect the language in which the client will run. Click **OK**.
5. When displayed, click **Next**.
6. Accept the license terms and click **Next**.
7. Unless there is a specific reason to do otherwise, accept the default directory selection and click **Next**.
8. Click **Install**.
9. Click **Finish**.

To start the Windows application:

1. Click on the Avaya Equinox Select icon on the desktop or select it from the programs list.
2. Enter the server IP address or name. You do not need to add the **https:** or **:9443** details.
3. When prompted to **Show Notifications**, select **Allow**.
4. Enter your user name and password and click **Login**.
5. If prompted, allow the application to use your microphone and or camera.

5.6 Logging and Debugging


You can obtain log messages from both the Equinox Select application and the WebRTC Gateway service.

To run the PhoneService test application:


To check basic WebRTC client connection, the WebRTC Gateway service includes a simple test application.

1. Browse to `http://<server_address>:9443/PhoneService`.
2. Login using the user details of a user configured for portal use.


To view the client debug messages:

1. Within Equinox Select, click  and select **Help**.
2. Click **Debug Window**.
3. Use the **Filters** to select the type of debug messages that you want displayed.
4. You can use the **Clear** button to remove all previous messages from the display.



To download the clients log files:

1. Within Equinox Select, click  and select **Help**.
2. Click **Grab Logs**.
3. The browser will download the logs files to its default download folder.

To set the level of server logging:

1. [Login](#)  to the server's web configuration menus.
2. Click **Solutions**.
3. Click **Applications** and select **WebRTC Configuration**.
4. On the **System Settings** menu, set the **Logging Level** required. Info is the normal level for an operating system. Select Debug when necessary to resolve existing issues. Trace provides maximum detail if Debug proves not sufficient to resolve the issue.
5. Click **Save** to save any changes.

To download the server log files:

2. [Login](#)  to the server's web configuration menus.
3. Click **Solutions**.
3. In the displayed list of systems, click on the  icon next to the required system and select **Platform View**.
4. Click on **Logs** and select the **Download** sub tab.
5. Click on the **Create Archive** button.
6. Download the WebRTC Gateway log file from the list.

To measure client/server communication:

The WebRTC Gateway server includes a packet monitoring service.

1. Browse to `http://<server_address>:9443/netz`.
2. For **Live Monitoring**, login with the user name/password details of a WebRTC client user. The **Offline Analyzer** option can be used to display packet information previously downloaded in RTCmon log files.
3. Click Start to collect and display data on the clients WebRTC calls.

5.7 External Client Access

External client access uses the following ports. These ports need to be enabled, and if necessary correctly routed, to the WebRTC Gateway:

- TCP/HTTPS/Web Socket access on port 9443. Not adjustable.
- TCP or TLS on the public ports range set in the WebRTC Gateway service configuration. The defaults are 56000 to 58000.
- To handle address translation between the external and internal networks, the WebRTC Gateway supports STUN and TURN.
- The devices used must also support the security certificate CA chain as the WebRTC Gateway.

Using an Avaya Session Border Controller for Enterprise

All the above requirements can be configured on an Avaya Session Border Controller for Enterprise. Refer to the the "IP Office SIP Phones with ASBCE" manual.

The basic steps required are:

- Add security certificates that use the same CA source to the ASBCE and create a TLS profile that uses those certificates.
- Create a reverse proxy policy for HTTPS connections to the server hosting the WebRTC Gateway service.
- Enable STUN and TURN operation on the Avaya Session Border Controller for Enterprise and in the WebRTC Gateway settings.

Chapter 6.

Server Maintenance

6. Server Maintenance

This section covers basic maintenance tasks for Linux based IP Office server platforms that can be done using the server's web control menus.

- [Logging in Directly](#) ⁷⁹
- [Starting/Stopping Application Services](#) ⁸²
- [Changing the Linux Passwords](#) ⁸²
- [Changing the IP Address Settings](#) ⁸⁰
- [Server Shutdown](#) ⁸³
- [Rebooting the Server](#) ⁸³
- [Date and Time Settings](#) ⁸⁴
- [Creating Administrator Accounts](#) ⁸⁵
- [Setting the Menu Inactivity Timeout](#) ⁸⁵
- [Upgrading an Application](#) ⁸⁶
- [Uninstalling an Application](#) ⁹¹
- [Setting Up File Repositories](#) ⁹²
- [Downloading Log Files](#) ⁹⁵

6.1 Logging In

You can access the web control/platform view menus for each server platform in a network via IP Office Web Manager.

Avaya supports the following browsers for web access to the server menus:

- **Microsoft Internet Explorer 10 and 11.**
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

To access Web Manager:

1. Log in to IP Office Web Manager.

a. Enter **https://** followed by the server address. Click on the **IP Office Web Manager** link.



The screenshot shows the Avaya IP Office Web Manager login interface. On the left is a red vertical bar with the AVAYA logo. The main area has a white background with the title 'Avaya IP Office Web Manager'. Below the title are three input fields: 'User Name' with 'Administrator' entered, 'Password' with masked characters, and 'Select Language' with 'English' selected. There is a checkbox for 'Offline management' and a 'Login' button. At the bottom, it says '© 2015 Avaya Inc. All Rights Reserved.'

b. Enter the user name and password.

c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. However, an upgraded server can also use the Management Services and so needs to change its default security passwords. Note that this does not change the Linux **root** and **Administrator** account passwords.



The screenshot shows the Avaya IP Office Web Manager password change interface. On the left is a red vertical bar with the AVAYA logo. The main area has a white background with the title 'Avaya IP Office Web Manager'. Below the title are three sections for password changes: 'Change Password' (with Password and Confirm Password fields), 'Change Security Administrator Password' (with Password and Confirm Password fields), and 'Change System Password' (with Password and Confirm Password fields). There is a 'Save' button at the bottom. At the bottom, it says '© 2014 Avaya Inc. All Rights Reserved.'

- **Change Password**

This sets the password for the **Administrator** account of the Management Services service run on the IP Office Application Server. With [Referred Authentication](#) ^{16h} enabled (the default) this is also the default account used for Voicemail Pro, one-X Portal for IP Office and Web Manager administrator access.


- **Change Security Administrator Password**

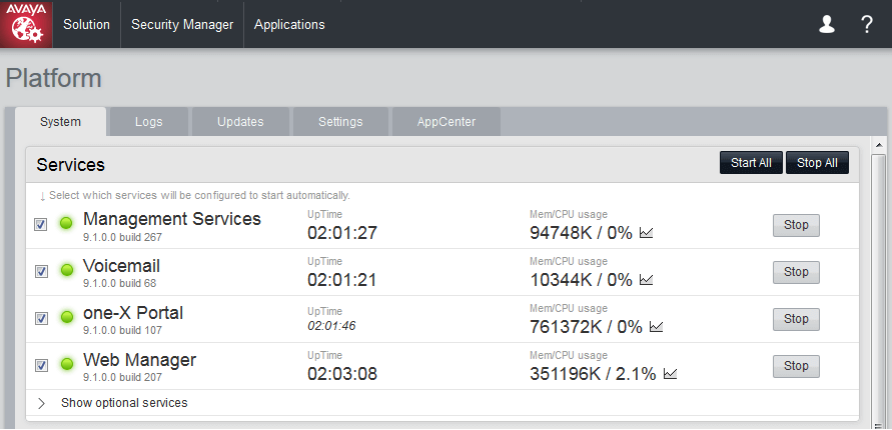
This sets the password for the Management Services security administrator account.

- **Change System Password**

This sets the **System** password for the Management Services.

2. Click on **Solution**.

3. In the displayed list of systems, click on the  icon next to the required system and select **Platform View**.



The screenshot shows the Avaya Platform View interface. At the top, there is a navigation bar with the Avaya logo and tabs for 'Solution', 'Security Manager', and 'Applications'. Below this, the 'Platform' section is visible, with sub-tabs for 'System', 'Logs', 'Updates', 'Settings', and 'AppCenter'. The 'System' tab is active, displaying a list of services. The services are listed in a table with columns for service name, version, uptime, memory/CPU usage, and a 'Stop' button. The services shown are Management Services, Voicemail, one-X Portal, and Web Manager. A 'Start All' button is located at the top right of the services list.

Service	Version	UpTime	Mem/CPU usage	Stop
Management Services	9.1.0.0 build 267	02:01:27	94748K / 0%	Stop
Voicemail	9.1.0.0 build 68	02:01:21	10344K / 0%	Stop
one-X Portal	9.1.0.0 build 107	02:01:46	761372K / 0%	Stop
Web Manager	9.1.0.0 build 207	02:03:08	351196K / 2.1%	Stop

> Show optional services

6.2 Logging Into Web Control Directly

Use the following method to login directly to the server's web control menus rather than via the server [Web Manager](#)^[77] menus. This method of logging may be necessary if the **Web Manager** service is not running on the server for some reason.

Avaya supports the following browsers for web access to the server menus:

- **Microsoft Internet Explorer 10 and 11.**
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

To login to the server web control menus:

1. From a client PC, start the browser. Enter **https://** followed by the address of the server and **:7071**. If the IP address is unknown, see Viewing the Module IP Address.
 - If the browser displays a security warning, you may need to load the server's security certificate. See [Adding a Certificate to the Browser](#)^[34].
2. Select the **Language** required.

3. Enter the name and password for server administration.
4. If the login is successful, the server's [System](#)^[103] page appears.

6.3 Changing the IP Address Settings

Using the server's web control menus (also call "platform view"), you can change the server's network settings.

- **Warning**

Changing IP address and other network settings will require you to login again. If the server is using DHCP or is switched to DHCP, the address obtained for the server appears on the server's command line display.

To change the IP address:

1. [Login](#) ⁽⁷⁷⁾ to the server's web configuration menus.

2. Select **Settings**.

3. Select **System**.

4. Set the **Network** section as required.

- **Network Interface**

This drop down allows selection of network interfaces for which the settings are shown. Within the IP Office configuration, **Eth0** matches LAN1, **Eth1** matches LAN2. A pre-built server only uses **Eth0**. This port is labeled as port 1 on the physical server.

- **Host Name**

Sets the host name that the IP Office Application Server should use. This setting requires the local network to support a DNS server. Do not use **localhost**.

- **! IMPORTANT: DNS Routing**

For internal use, this value must be reachable by DNS within the customer network. If the server will also be supporting external applications, it needs to be reachable by external DNS. Consult with the customer's IT support to ensure the name is acceptable and that routing to it has been configured correctly.

- **! IMPORTANT: Security Certificate Field**

This value is used as part of the default security certificate generated by the server. If changed, the server generates a new default certificate, during which time access to the server is disrupted for several minutes. In addition, any applications using the default certificate need to be updated with the new certificate.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual *"Deploying Avaya IP Office Servers as Virtual Machines"* for further details.

- **Use DHCP**

If selected, the IP address, subnet mask and default gateway information is obtained by the server making DHCP requests. The related fields are greyed out and cannot be set manually, instead they show the values obtained in response to the DHCP request.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual *"Deploying Avaya IP Office Servers as Virtual Machines"* for further details.

- **IP Address**

Displays the IP address set for the server. If not using DHCP, you can edit the field to change the setting.

- **! IMPORTANT: Security Certificate Field**

This value is used as part of the default security certificate generated by the server. If changed, the server generates a new default certificate, during which time access to the server is disrupted for several minutes. In addition, any applications using the default certificate need to be updated with the new certificate.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual *"Deploying Avaya IP Office Servers as Virtual Machines"* for further details.

- **Subnet Mask**

Displays the subnet mask applied to the IP address. If not using DHCP, you can edit the field to change the setting.

- **Default Gateway**

Displays the default gateway settings for routing. If not using DHCP, you can edit the field to change the setting.

- **System DNS**

Enter the address of the primary DNS server. This option is greyed out if the address of the DNS server is set to be obtained from the DHCP server (see below).

- **Automatically obtain DNS from provider**

This setting is only used if **Use DHCP** is also selected. If selected, the server attempts to obtain DNS server details from the DHCP server.

5. Click **Save**. The server restarts.

6.4 Starting/Stopping Application Services

You can start and stop each of the application services installed on the server. You can set the services to automatically restart after a server reboot.

6.4.1 Starting a Service

Note that some services are linked and so cannot be started or auto-started if the other related service is not also started or set to auto-start. For example, the **WebRTC Gateway**, **Web Collaboration** and **Equinox Select** services require the **one-X Portal** service to be started and running.

To start a service:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select **System**. The menu lists the services and their status.
3. To start a particular service click on the **Start** button next to the service. To start all the services that are not currently running, click on the **Start All** button.

6.4.2 Stopping a Service

Note that some services are linked and so cannot be started or auto-started if the other related service is not also started or set to auto-start. For example, the **WebRTC Gateway**, **Web Collaboration** and **Equinox Select** services require the **one-X Portal** service to be started and running.

To stop a service:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select **System**. The menu lists the services and their status.
3. To stop a particular service click on the **Stop** button next to the service. To stop all the services that are currently running, click on the **Stop All** button.
4. The service's status changes to **Stopping**. If it remains in this state too long, you can force the service to stop by clicking on **Force Stop**.

6.4.3 Setting a Service to Auto Start

Note that some services are linked and so cannot be started or auto-started if the other related service is not also started or set to auto-start. For example, the **WebRTC Gateway**, **Web Collaboration** and **Equinox Select** services require the **one-X Portal** service to be started and running.

To set a service to auto start:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select **System**. The menu lists the services and their status.
3. Use the **Auto Start** check box to indicate whether a service should automatically start when the server starts.

6.5 Changing the Linux Passwords

Server installation creates two Linux user accounts; **root** and **Administrator**. You set their initial passwords during the server ignition.

- These settings are only accessible if logged in via referred authentication or as the local Linux root.

To change the server's Linux account passwords:

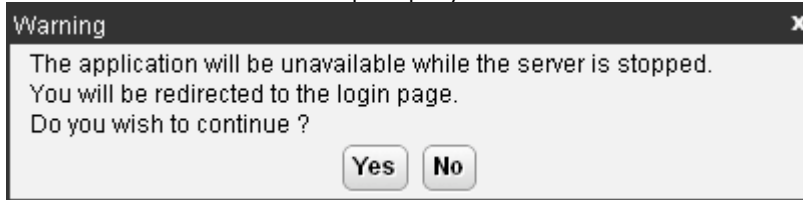
1. [Login](#)^[77] to the server's web configuration menus.
2. Select **Settings** and click on the **System** tab.
3. Use the **Change root Password** section to set the new password for the root account. The new password must conform to the [password rules settings](#)^[127].
4. Use the **Change Local Linux Account Password** to set the new password for the **Administrator** account. Note that this is different from the **Administrator** account used for access to IP Office services. The new password must conform to the [password rules settings](#)^[127].
5. Click **Save**.

6.6 Shutting Down the Server

Use this process when it is necessary to switch off the IP Office Application Server for any period. Once the process has been completed, you can switch off power to the server. To restart the server, switch the server power back on.

To shutdown the server:

1. [Login](#)^[77] to the server's web configuration menus.
2. After logging in, select the [System](#)^[103] page.
3. Click on **Shutdown**. The menu prompts you to confirm the action.



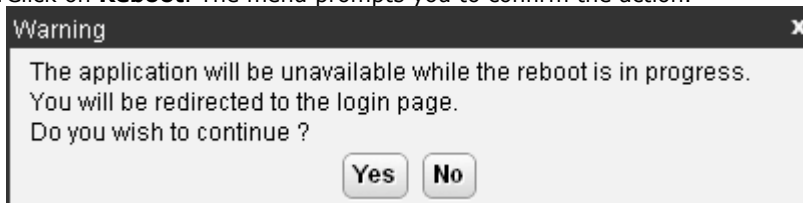
4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 2 minutes, the server shuts down.
7. Switch off power to the server.

6.7 Rebooting the Server

Rebooting the server stops all currently running services and then stops and restarts the server. Only those application services set to [Auto Start](#)^[82] automatically restart after the reboot.

To reboot the server:

1. [Login](#)^[77] to the server's web configuration menus.
2. After logging in, select the [System](#)^[103] page.
3. Click on **Reboot**. The menu prompts you to confirm the action.



4. Click **Yes** to confirm that you want to proceed with the reboot.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 5 minutes, you should be able to login again.
7. Once logged in, you can manually restart any services required if not set to **Auto Start**.

6.8 Date and Time Settings

You can change the date and time settings used by the server through the server's web configuration pages. The [System](#) menu shows the server's current date and time.

To change the server date and time settings:

1. [Login](#) to the server's web configuration menus.

2. Select **Settings**.

3. Select **System**.

4. Select the **Date Time** section.

- **Date**

For a server not using NTP, this field shows the server's current date and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.

- **Time**

For a server not using NTP, this field shows the server's current UTC time and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.

- **Timezone**

In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field determines the appropriate offset applied to the UTC time above. Note that changing the timezone can cause a "Session expired" message to appear in the browser in which case you need to login again.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual "Deploying Avaya IP Office Servers as Virtual Machines" for further details.

- **Enable Network Time Protocol**

When selected, the server obtains the current date and time from the NTP servers listed in the **NTP Servers** list below. It then uses that date and time and makes regular NTP requests for updates.

- **NTP Servers**

With **Enable Network Time Protocol** selected, use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at <http://support.ntp.org/bin/view/Servers/WebHome>. However, it is your responsibility to comply with the usage policy of the chosen server. Choose several unrelated NTP servers in case one of the servers becomes unreachable or its clock unreliable. The server uses the responses it receives from each NTP server to determine reliability.

- The IP Office system can also use NTP to obtain its system time.

- **Synchronize system clock before starting service**

Use this option to synchronize the system clock to an NTP time server before starting other services. Do not use this option if the time server cannot be reliably reached. Waiting for synchronization to occur may block use of the system until a timeout has passed.

- **Use local time source**

When not selected, external NTP takes priority over the internal system clock. If selected, the local system clock is used as the time source. Only use this option if system clock is synchronized with another reliable source, for example a radio controlled clock device.

5. Click **Save**.



6.9 Creating Administrator Accounts

The IP Office system's security configuration controls access to the web control menus.


Service users can have two levels of web control access. You can combine these to give a user full access:

- **Web Control Security**
Access to the Certificates settings, change root and local administrator password controls and set password rules settings.
- **Web Control Administrator**
Access to all other settings options.

To view and adjust rights group settings:

1. Using IP Office Manager, select **File | Advanced | Security Settings**.
2. Select the IP Office system and click **OK**.
3. Enter the name and password for access to the IP Office system's security settings.
4. Select  **Rights Groups**.
5. Select the **External** tab. This tab includes settings for level of web control access allowed to members of the rights group.
 - **Web Control Security**
Access to the Certificates settings, change root and local administrator password controls and set password rules settings.
 - **Web Control Administrator**
Access to all other settings options.
6. Select a particular rights group in the list to see what level of access the rights group has.
7. If you make any changes, click **OK**.
8. Click on the  icon to save the changes.

To change a service user's rights group memberships:


1. Using IP Office Manager, select **File | Advanced | Security Settings**.
2. Select the IP Office system and click **OK**.
3. Enter the name and password for access to the IP Office system's security settings.
4. Select  **Service Users**.
5. Select the service user. The details show the rights group of which that service user is a member.

6.10 Setting the Menu Inactivity Timeout

You can adjust the inactivity time applied to the web control menus.

- **! Note**
Changing this setting will require you to login again.

To change the menu inactivity timeout:

1. [Login](#)  to the server's web configuration menus.
2. Select **Settings**.
3. Select **General**.
4. Select the **Web Control** section.
 - **Inactivity Timeout**
Select the period of inactivity after which the server automatically logs out the web session. Changing this value requires you to login again. The options are **5 minutes**, **10 minutes**, **30 minutes** and **1 hour**.
5. Click **Save**. The server will advise you that it is restarting the web service and that you will need to login again.

6.11 Upgrading Applications

The preferred method for upgrading servers and server applications is to use the [Web Manager menus](#)^[98]. However, you can use the previous web control methods for legacy installations.

You can upgrade individual application services without having to reinstall or upgrade the whole server. This is done using either an .rpm file or a .zip file of multiple .rpm's uploaded to the server (local) or downloaded by the server from an HTTP folder (remote repository), see [File Repositories](#)^[92].

Once an .rpm file or files are available, the IP Office Application Server web configuration pages will list the available versions and allow switching between versions or simple upgrading to the latest version.

- **! Upgrade Warning**

Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.

- **! Password Change Required after Upgrading to 9.1+**

When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See [Logging Into Web Manager](#)^[99].

- **! Disable one-X Portal for IP Office Logging before upgrading**

You must disable one-X Portal for IP Office logging prior to upgrading. If you do not do this, one-X Portal for IP Office admin is very slow to respond after the upgrade. You can disable one-X Portal for IP Office logging through the one-X Portal for IP Office administrator menus by setting the **Master Logging Level (Diagnostics | Logging Configuration)** to **OFF**.

The options in this section cover the upgrading of individual components of the operating system and applications supported by the IP Office Application Server.

6.11.1 Loading Application Files onto the Server

This method uploads the RPM file for an application onto the server. You can then use the file to update the application. The alternative is to use files loaded into a [remote software repository](#)^[94].

- **Voicemail Pro**

Avaya splits each version of Voicemail Pro into separate RPM files for the server and for each supported prompt language. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

To upload application files onto the server:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Applications**.
4. Click on the **Browse** button and browse to the [location of the file](#)^[92] that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

6.11.2 Upgrading Application Files

Where multiple versions of a software component are available on the server, you can use the web menus to update or change the current version installed.

To upgrade application files:

1. [Login](#) to the server's web configuration menus.
2. Select the **Updates** page.

Services						Check Now	Clear Local Cache	Update All
Application	Description	Current Version	Latest Available	Status	Actions			
TTSEnglish	Avaya application.	7.0.0.25 build 4	7.0.0.25 build 4	up to date	Change Version	Update	Uninstall	
Management Services	Avaya application. Placeholder description for IP Office.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version	Update	Uninstall	
one-X Portal	Avaya application. Placeholder description for one-X Portal.	10.0.0.0 build 223	10.0.0.0 build 223	up to date	Change Version	Update	Uninstall	
Voicemail	Avaya application. Placeholder description for Voicemail.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version	Update	Uninstall	
Watchdog	Avaya application. Placeholder description for Watchdog.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version	Update	Uninstall	
Web Manager	Avaya application. Placeholder description for Web Manager.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version	Update	Uninstall	
webcontrol	Avaya application. Web page used to manage the local machine. Requires cli-commands of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version	Update	Uninstall	
webcontrol-plugin-appscard	Avaya application. Webcontrol plugin used in UCM systems. Requires webcontrol of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version	Update	Uninstall	
VMPProWebService	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version	Update	Uninstall	
VmPro-Mapi	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	out of date	Change Version	Update	Uninstall	

3. The **Services** section displays the current version and latest available version of each application service.

- Some applications may not support upgrading or downgrading whilst installed. For those applications, the **Change Version** and **Update** buttons remain greyed out even if there are updates available in the application file repository. You must first use the **Uninstall** button to uninstall the application before the **Change Version** and **Update** buttons become useable.

4. Select one of the following actions:

- To update an application to the latest version available, click on **Update**.
- To update all applications to the latest version available, click on **Update All**.
- To change the current version of an application, click **Change Version**. Select the version required and click **Apply**.

6.11.3 Upgrading Using USB

Upgrading the IP Office Application Server through the use of [RPM or ZIP files is recommended](#)^[88]. However, if necessary, you can use a USB memory key to perform an upgrade.

6.11.3.1 Preparing a USB Upgrade Key

This process uses a downloaded ISO image to create a bootable USB memory key for software upgrading. Using this device installs the software without, overwriting any existing software and data on the server.

- **! Upgrade Warning**

Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.

- **! Password Change Required after Upgrading to 9.1+**

When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See [Logging Into Web Manager](#)^[99].

Prerequisites

- **4GB USB Memory Key**

Note that this process reformats the memory key and erases all files.

- **Avaya USB Creator Tool**

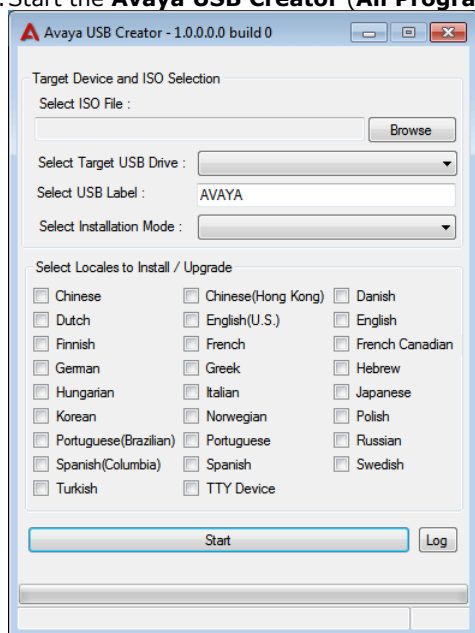
This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade.

- **Server Edition ISO Image**

You can download this file from the Avaya support website, see Downloading Module Software.

To create a bootable USB memory key:

1. Insert the USB memory key into a USB port on the PC.
2. Start the **Avaya USB Creator (All Programs | IP Office | Avaya USB Creator)**.



3. Click the **Browse** button and select the ISO file.
4. Use the **Select Target USB Drive** drop-down to select the USB memory key. Make sure that you select the correct USB device as this process overwrites all existing contents on the device.
5. In the **Select USB Label** field enter a name to help identify the key and its usage in future.
6. Use the **Select Installation Mode** options to select whether the USB memory key should be configured for an automatic software install (**Server Edition - Auto Install**), automatic software upgrade (**Server Edition - Auto Upgrade**) or a user menu driven install/upgrade (**Server Edition - Attended Mode**).
 - Note: The installation mode options available changed automatically based on the type of ISO file selected. If you do not see the correct options, check that you have selected a IP Office Application Server ISO file.

7. Use the **Select Locales to Install / Upgrades** check boxes to select which sets of Voicemail Pro prompts you want installed or upgraded. Only selecting the languages that you require significantly reduces the time required for the installation or upgrade.
8. Check that you have set the options correctly. Click **Start**.
9. Confirm that you want to continue.
10. The status bar at the bottom of the tool shows the progress of preparing the USB memory key. The process takes approximately 15 minutes though that can vary depending on the USB2 memory key and PC.

6.11.3.2 Upgrading Using a USB Upgrade Key

- **! Upgrade Warning**

Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.

- **! Password Change Required after Upgrading to 9.1+**

When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See [Logging Into Web Manager](#)^[99].

To upgrade from a USB memory key:

1. Prepare a bootable USB upgrade key. See [Preparing a USB Upgrade Key](#)^[88].
2. Insert the USB upgrade key into a USB socket and [reboot the server](#)^[83].
3. Follow the same process as for [Software Installation](#)^[28]. However, when the upgrade menu appears, select **Upgrade** rather than **Install**.

6.12 Uninstalling an Application

You can use the **Updates** menu to uninstall an application service. This removes the application from the list of service unless files for its reinstallation are present in the server's configured file repository.

- **! WARNING**

You should only uninstall an application if instructed by Avaya. Uninstalling an application can have affects on the operation of other applications.

To uninstall an application:

1. [Login](#) ⁷⁷ to the server's web configuration menus.
2. Select the **Updates** page.


Services						Check Now	Clear Local Cache	Update All
Application	Description	Current Version	Latest Available	Status	Actions			
TTSEnglish	Avaya application.	7.0.0.25 build 4	7.0.0.25 build 4	up to date	Change Version Update Uninstall			
Management Services	Avaya application. Placeholder description for IP Office.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
one-X Portal	Avaya application. Placeholder description for one-X Portal.	10.0.0.0 build 223	10.0.0.0 build 223	up to date	Change Version Update Uninstall			
Voicemail	Avaya application. Placeholder description for Voicemail.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version Update Uninstall			
Watchdog	Avaya application. Placeholder description for Watchdog.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
Web Manager	Avaya application. Placeholder description for Web Manager.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
webcontrol	Avaya application. Web page used to manage the local machine. Requires cli-commands of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
webcontrol-plugin-appscard	Avaya application. Webcontrol plugin used in UCM systems. Requires webcontrol of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
VMProWebService	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version Update Uninstall			
VmPro-Mapi	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	out of date	Change Version Update Uninstall			

3. The **Services** section displays the current version and latest available version of each application service.
4. To uninstall a service, click on **Uninstall**.

- If there are installation files for the application in the application [file repository](#) ⁹², the button becomes an **Install** button.
- If there are no installation files for the application in the file repository, the menu no longer list the application.

6.13 Setting Up File Repositories

The [Updates](#)^[109] and [Web Client](#)^[124] menus use files stored in the configured file repositories. A repository is a set of files uploaded to the server or the URL of a remote HTTP server folder.

You can add files to these repositories without affecting the existing operation of the server. However, when the application or operating system repositories contain later versions of the files than those currently installed, a  warning icon appears on the **Updates** menu.

6.13.1 Source Files

Avaya may make update files available individually in response to particular issues or to support new IP Office releases. The files are also included on the IP Office Application Server DVD. You can extract files from a DVD ISO image using an application such as WinZip.

- **! Upgrade Warning**

Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.

- **! Password Change Required after Upgrading to 9.1+**

When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See [Logging Into Web Manager](#)^[99].

		DVD/.ISO Folder	Description
Applications	Voicemail Pro	\avaya\vmpro	<ul style="list-style-type: none">• These are files used by the IP Office applications and services provided by the server.
	one-X Portal for IP Office	\avaya\oneX	
Downloads		\avaya\thick_clients	<ul style="list-style-type: none">• These are files used to provide the downloads from the App Center^[124] menu.
Operating System		\Packages	<ul style="list-style-type: none">• These are files used by the Linux operating system and its services.

- **Voicemail Pro**

Avaya splits each version of Voicemail Pro into separate RPM files for the server and for each supported prompt language. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

6.13.2 Setting the Repository Locations

The IP Office Application Server can use either remote or local software repositories to store software update files. The server has separate repositories for operating system updates, IP Office application installation files and Windows client files. The [Updates](#)^[109] and [AppCenter](#)^[124] menus use the files present in the appropriate repository.

- **Repository**

If not using the **Local** option, this field sets the URL of a [remote HTTP file repository](#)^[94]. Note that you cannot use the same URL for more than one repository.

- **Local**

This checkbox sets whether the file repository used is local (files stored on the IP Office Application Server) or remote (a folder on a HTTP web server specified in the Repository field).

- **File / Browse / Add**

With **Local** selected, you can use this field and adjacent buttons to browse for a specific update file. After selecting the file, click **Add** to upload the file to the server's file store.

6.13.3 Uploading Local Files

You can use the processes below to upload files to the server. The file types are:

- **Application**
These are files used by the IP Office applications and services provided by the server.
- **Downloads**
These are files used to provide the downloads from the [App Center](#)^[124] menu.
- **Operating System**
These are files used by the Linux operating system and its services.

6.13.3.1 Uploading Application Files

This method uploads the RPM file for an application onto the server. You can then use the file to update the application. The alternative is to use files loaded into a [remote software repository](#)^[94].

- **Voicemail Pro**
Avaya splits each version of Voicemail Pro into separate RPM files for the server and for each supported prompt language. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

To upload application files onto the server:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Applications**.
4. Click on the **Browse** button and browse to the [location of the file](#)^[92] that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

6.13.3.2 Uploading Operating System Files

This method uploads the .rpm file for an application onto the IP Office Application Server. You can then use the file to update the IP Office applications.

To upload operating system files:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Operating System**.
4. Click on the **Browse** button and browse to the [location of the file](#)^[92] that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

6.13.3.3 Uploading Windows Client Files

This method uploads the .rpm file for an application onto the IP Office Application Server.

To upload Windows client files:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Downloads**.
4. Click on the **Browse** button and browse to the [location of the file](#)^[92] that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

6.13.4 Creating Remote Software Repositories

Alternatively to using [local files uploaded to the server](#)^[86] for updates, the server can use files stored in folders on a remote HTTP server.

To create an application update repository:

1. Create a folder on the web server for the remote file repository. For example a folder called **Applications**.
2. The folder directory must be browseable. For example, on a Microsoft Internet Information Services server, right-click on the folder, select **Properties** and select the **Directory Browse** option.
3. Copy the .rpm files from their [source](#)^[92] into the folder.
4. From another PC, test that you can browse to the URL of the folder and that the list of files in the folder appears.
5. Login to the IP Office Application Server web configuration pages.
6. Select **Settings** and then **General**.
7. Uncheck the **Local** checkbox for **Applications**. Enter the URL of the HTTP server folder into the preceding field.
8. Click **Save**.
9. Select **Updates**.
10. If the server is able to access the HTTP folder, the details of the versions available will now reflect those available in that folder. The message **repository error** indicates that the IP Office Application Server was not able to connect to the folder or not able to list the files in the folder.

To create a Windows client repository:

The process is the similar to that shown above for application RPM files. However, you should use a separate folder on the HTTP server.

To create an operating system repository:

The repository for operating system updates is different from those used for application updates and downloads. It must be a YUM repository. Details of how to setup and configure a YUM repository depend on the version of Linux on the HTTP server. Each time you add, delete or change an RPM file, you must update the directory using a **createrepo <folder_path>** command.

6.14 Downloading Log Files

The server collects and store log events. These are viewable through the [Logs](#)^[106] sub-menus. The [Download](#)^[108] sub-menu allows the archiving and download of the log files.

For IP Office Release 10.0, you can configure the server to include packet capture logs for the server, see [Packet Capture Settings](#)^[115].

To create archive files:

1. [Login](#)^[77] to the server's web configuration menus.
2. Select **Logs**.
3. Select **Download**.
4. Click on the **Create Archive** button. The button remains greyed out while the archive creation is running:
 - For debug files, the archive contains any debug records since the last creation of a debug archive.
 - For log files, the server creates a separate archive file for each service. The archive file contains all log files available on the server.

To download archive files:

1. To download an archive file, click on the file name of the archive file.
2. The process for downloading then depends on the browser.

To delete archive files:

1. To delete an archive, select the **Delete** checkbox next to the archive file in the list. To select all the archive files click on **Select All**.
2. To delete the selected files, click on **Delete Selected**.

Chapter 7.

Web Manager

7. Web Manager

The primary method for server management is through its Web Manager menus. For details of using Web Manager refer to separate [IP Office Web Manager documentation](#)^[13].

Through Web Manager you can perform the following actions. Note that access to some functions depends on the security rights of the account used to [login to Web Manager](#)^[99].

- **Backup Applications**

You can configure backups of the server applications to a remote server. These backups can use a variety of protocols (HTTP, HTTPS, FTP, SFTP, SCP). In addition to selecting the application services included in a backup, you can schedule backups.

- **Restore Previous Backups**

You can use control the restoration of a previous backups.

- **Upgrade the Server**

You can use the menus to upload a new ISO image and then use that image file to upgrade the server.

- **Launch Other Applications**

You can launch the other administrator applications used by the server or the applications it runs:

- **IP Office Manager**

If installed on the user PC, Web Manager can launch IP Office Manager.

- **Voicemail Pro Client**

If installed on the user PC, Web Manager can launch the voicemail client to allow configuration of the voicemail server and editing of voicemail call flows.

- **one-X Portal for IP Office**

You can access the administration menus for the one-X Portal for IP Office service from within Web Manager.

- **System Status Application**

You can start System Status Application without needing to install it on the user PC.

- **Web Control**

You can access the server's web control menus through Web Manager.

- **Configure Voicemail Server Preferences**

For server's running the Voicemail Pro service, you can set the voicemail server preferences using Web Manager.

- **Security User**

Web Manager can configure the security privileges of IP Office service user accounts.

- **File Management**

Web Manager can upload files to the server. This includes the uploading of custom voicemail prompts.

7.1 Logging In to Web Manager


Avaya supports the following browsers for web access to the server menus:

- **Microsoft Internet Explorer 10 and 11.**
- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**
- **Safari**

To access Web Manager:

1. Log in to IP Office Web Manager.

a. Enter **https://** followed by the server address. Click on the **IP Office Web Manager** link.



b. Enter the user name and password.

c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. However, an upgraded server can also use the Management Services and so needs to change its default security passwords. Note that this does not change the Linux **root** and **Administrator** account passwords.



- **Change Password**

This sets the password for the **Administrator** account of the Management Services service run on the IP Office Application Server. With [Referred Authentication](#) enabled (the default) this is also the default account used for Voicemail Pro, one-X Portal for IP Office and Web Manager administrator access.


- **Change Security Administrator Password**

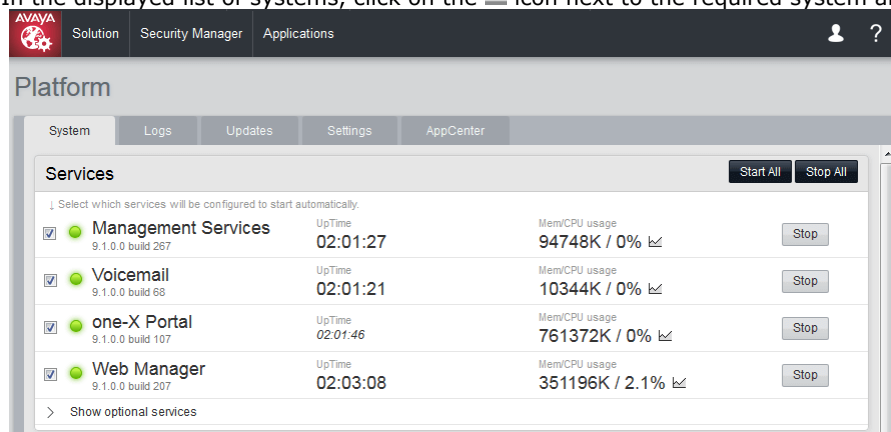
This sets the password for the Management Services security administrator account.

- **Change System Password**

This sets the **System** password for the Management Services.

2. Click on **Solution**.

3. In the displayed list of systems, click on the  icon next to the required system and select **Platform View**.



Chapter 8.

Web Control/Platform View Menus

8. Web Control/Platform View Menus

The IP Office Application Server web control menus are as follows. Note that these menus are common to all the Linux based servers supported by IP Office. However, the menus and menu option shown vary depending on the types of server and the server's role.

- **[System](#)**^[103]
This menu gives an overview of the status of the applications hosted on the server.
- **[Logs](#)**^[107]
This menu has sub-menus for viewing and managing log records and log files.
 - **[Debug Logs](#)**^[107]
View the current log files for the server and the application services hosted by the server.
 - **[Syslog Event Viewer](#)**^[108]
View Syslog log records received and or generated by the server.
 - **[Download](#)**^[108]
Create and download archive files of existing log records.
- **[Updates](#)**^[109]
Display the versions of applications and components installed and the alternate versions available.
- **Settings**
This menu has sub-menus for various areas of server configuration and operation.
 - **[General](#)**^[112]
General server settings such as the locations of software update repositories.
 - **[System](#)**^[117]
View and manage the server setting for date, time and IP address details.
- **[AppCenter](#)**^[124]
You can download the installation packages for applications such as the Voicemail Pro client application from this page.
- **[VNC](#)**^[123]
This menu only appears on Server Edition systems.

8.1 System

This menu provides an overview of the server status including the status of the application services running on the server.

System | Logs | Updates | Settings | AppCenter

Services [Start All] [Stop All]

↓ Select which services will be configured to start automatically.

Service	UpTime	Mem/CPU usage	Stop
<input checked="" type="checkbox"/> Management Services 10.1.0.0 build 137	03:12:43	57684K / 0%	[Stop]
<input checked="" type="checkbox"/> Contact Reporter 10.1.0.0 build 137	03:12:36	10376K / 0%	[Stop]
<input checked="" type="checkbox"/> Voicemail 10.1.0.0 build 58	03:12:36	10376K / 0%	[Stop]
<input checked="" type="checkbox"/> one-X Portal 10.1.0.0 build 223	03:13:02	759248K / 0%	[Stop]
<input checked="" type="checkbox"/> Web Manager 10.1.0.0 build 137	03:14:01	420556K / 1.4%	[Stop]
<input checked="" type="checkbox"/> Web License Manager 10.1.0.0 build 137	03:14:01	420556K / 1.4%	[Stop]

> Show optional services

Notifications

There are no notifications available

System [Shutdown] [Reboot]

No CPU history data available

Memory Usage

used (1764.21MB)
free (1435.94MB)

Disk Usage

used (16807.56MB)
free (131892.57MB)

OS: Linux release 6.8 (Final)
 Kernel Version: 2.6.32-504.8.1.el6.x86_64
 UpTime: 14 minutes
 Server Time: 10:32
 Average CPU Load: 0.73 (1min), 2.42 (5min), 1.88 (15min)
 Server Type:
 Processor: AMD Athlon(tm) 64 X2 Dual Core Processor 4200+
 Speed: 2.1GHz
 Cores: 2
 Hard Disk Size: 145.2G
 RAM: 3.1G
 Disk RAID Levels: -
 Disk Array Types: -
 Quota available for: None
 backup data:

• Services

This table lists the services supported by the server. In addition to showing the status of the service, it also contains buttons to start/stop each service. Clicking on the link for **Mem/CPU usage** will display a summary graph of CPU and memory usage by the application.

• Management Services

This is a shell version of IP Office that allows basic configuration of services such as remote SSL VPN connections for server support. It also controls security settings for access to the server's menus. It does not support call features such as users, extensions or trunks.

• one-X Portal for IP Office

This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely via web browser.

• Voicemail Pro

This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail.

• Integrated Contact Reporter

This new service is a small contact centre reporting tool. Refer to the separate Integrated Contact Reporter documentation for full details of configuration and use.

• Web License Manager

This service allows the server to act as a WebLM server. IP Office systems using PLDS licenses can then use the address of the server for license validation.

- **Web Manager**

You can configure and manage the server via browser access to the Web Manager menus. The menus also allow the launching of other clients used to configure and monitor the services run by the server.

- **Optional Services**

The server can include a number of additional services. Click **Show optional services** to display those services.

- **Equinox Select**

This is an WebRTC softphone that works with one-X Portal for IP Office and the WebRTC gateway services. Users can access it through their browser (currently Windows Chrome).

- **Web Collaboration**

This service works with one-X Portal for IP Office. It provides users with web collaboration services usable in parallel with audio conference hosted by the telephone system. In the parallel web collaboration session, users can share views of their desktop, documents, etc.

- **WebRTC Gateway**

This is a VoIP gateway service that allows the server to support user's making calls using WebRTC clients. Currently this is supported for Avaya Communicator for Web and for internal licensed web collaboration users.

- **Media Manager**

This application is an alternative to Contact Recorder for IP Office for the long term storage and retrieval of call recordings. The recordings are made by Voicemail Pro. Those recordings are then collected by Media Manager and stored by it.

- **Contact Recorder for IP Office**

Contact Recorder for IP Office is used in conjunction with Voicemail Pro for long term storage and retrieval of call recordings. The recordings are made by Voicemail Pro. Those recordings are then collected by Contact Recorder for IP Office and stored by it. For details on installation and support, refer to the Contact Recorder for IP Office Installation Manual. This service has been superseded by Media Manager but is still available for existing users.

- **Notifications**

This table shows important messages.

- **System**

This table gives a general overview of the sever status. This section also provides controls to shutdown or reboot the server. Note that it may take up to 10 minutes for CPU usage data to appear after a server reboot.

- **OS/Kernel:**

The overall version of the Linux operating system installed on the server and the version of the operating system kernel.

- **Up Time:**

This field shows the system running time since the last server start.

- **Server Time:**

This field shows the current time on the server.

- **Average CPU Load:**

This field shows the average CPU load (percentage use) for the preceding minute, 5 minute and 15 minute periods.

- **Speed:**

Indicates the processor speed.

- **Cores:**

Indicates the number of processor cores.

- **Hard Disk Size:**

Indicates the hard disk size.

- **RAM:**

Indicates the amount of RAM memory.

- **Disk RAID Levels:**

Indicates the RAID type, if any.

- **Disk Array Types:**

Indicates the type of disk array used for RAID.

- **Quota available for backup data:**

Displays the amount of space reserved for local backups if [Enable HTTP file store for backup/restore](#) is enabled.

- **Virtualized:**

Indicates whether the server is running as a virtualized session.

- **Last Successful Logon:**

This field shows the date and time of the last successful logon, including the current logon.

- **Unsuccessful Logon Attempts:**

This field shows a count of unsuccessful logon attempts.

- **Shutdown**

Selecting this button starts a process that stops all services and then shuts down the server.

- **Reboot**

Selecting this button starts a process that stops all services and then stops and restart the server.

8.2 Logs

This menu contains the following sub-menus:

- [Debug Logs](#) ^[107]
View the current log files for the server and the application services hosted by the server.
- [Syslog Event Viewer](#) ^[108]
View Syslog log records received and or generated by the server.
- [Download](#) ^[108]
Create and download archive files of existing log records.

System

Logs

Updates

Settings

AppCenter

Debug Logs

Syslog Event Viewer

Download

Application Log

Application: All

Refresh

Application	Message
Voicemail	Maximum recording capacity: Unlimited, Maximum Recording Time: 120 seconds
Voicemail	Maximum Sessions: 40, Minimum PIN length: 0 digits
Voicemail	SMTP:-
Voicemail	Host address 0.0.0.0, port 25, Login method "none", email from "", login user ""
Voicemail	Memory statistics:-
Voicemail	System bytes: 5636KB, in use bytes: 5428KB
Voicemail	Number of threads: 48 (48)
Voicemail	Virtual memory size: 134MB, resident set size: 25MB
Voicemail	Resource usage statistics:-
Voicemail	User CPU time used: 1720.015517, system CPU time used: 1066.166917

Audit Log

Refresh

Timestamp	User	Action
2015-03-11 15:54:17	Administrator	logged in
2015-03-11 15:52:51	Administrator	logged out
2015-03-11 15:43:07	Administrator	logged in
2015-03-11 15:32:02	Administrator	logged out
2015-03-11 15:31:48	Administrator	set one-X Portal address to <148.147.170.168>
2015-03-11 15:31:11	Administrator	change autostart state for one-X Portal to off
2015-03-11 15:30:40	Administrator	install one-X Portal version 9.0.0.209
2015-03-11 15:29:44	Administrator	logged in
2015-03-11 15:27:29	Administrator	upload file to apps repository
2015-03-11 15:27:22	Administrator	upload file to apps repository

8.2.1 Debug Logs

You can access this menu by selecting **Logs** and then clicking **Debug Logs**. The menu shows the server application logs and audit log records.

Application Log Application: All Refresh

Application	Message
Voicemail	Maximum recording capacity: Unlimited, Maximum Recording Time: 120 seconds
Voicemail	Maximum Sessions: 40, Minimum PIN length: 0 digits
Voicemail	SMTP:-
Voicemail	Host address 0.0.0.0, port 25, Login method "none", email from "", login user ""
Voicemail	Memory statistics:-
Voicemail	System bytes: 5636KB, in use bytes: 5428KB
Voicemail	Number of threads: 48 (48)
Voicemail	Virtual memory size: 134MB, resident set size: 25MB
Voicemail	Resource usage statistics:-
Voicemail	User CPU time used: 1720.015517, system CPU time used: 1066.166917

Audit Log Refresh

Timestamp	User	Action
2015-03-11 15:54:17	Administrator	logged in
2015-03-11 15:52:51	Administrator	logged out
2015-03-11 15:43:07	Administrator	logged in
2015-03-11 15:32:02	Administrator	logged out
2015-03-11 15:31:48	Administrator	set one-X Portal address to <148.147.170.168>
2015-03-11 15:31:11	Administrator	change autostart state for one-X Portal to off
2015-03-11 15:30:40	Administrator	install one-X Portal version 9.0.0.209
2015-03-11 15:29:44	Administrator	logged in
2015-03-11 15:27:29	Administrator	upload file to apps repository
2015-03-11 15:27:22	Administrator	upload file to apps repository

- Application Log**

This table lists the last 1000 log records for a selected server application. The **Application** drop-down selects the records shown. Clicking on a column header sorts the records using that column. For Voicemail Pro the level of log information output is set through the **Debug** section of the [Settings | General](#) ^[114] menu. For one-X Portal for IP Office the level of log information output is set through the applications own administration menus, not through the IP Office Application Server menus.

- Audit Log**

This table lists the actions performed by users logged in through the IP Office Application Server's web browser interface. Clicking on a column header sorts the records using that column.

8.2.2 Syslog Event Viewer

This menu displays the server's Syslog records. These are combined records from the various applications (Voicemail Pro, one-X Portal for IP Office, etc) running on the server and the server operating system itself. It also shows Syslog records received by the server from other servers.

You can use the [Settings | General](#)^[112] menu to configure the sending and receiving of Syslog records to and from other servers. You can also configure how long the server keeps different types of records and how many records it keeps.

System

Logs

Updates

Settings

AppCenter

Debug Logs

Syslog Event Viewer

Download

Syslog Events

Host: AllEvent Type: AllView: AllTag: AllRefresh

Date	Host	Type	Tag	Message
2015-03-11 15:57:56	ServerEdition	SEC	Operating System	Administrator : TTY=unknown ; PWD=/opt/webcontrol ; USER=root ; COMMAND=/bin/chmod -R 777 /var/log/rsyslog/
2015-03-11 15:57:50	localhost	AUD	Operating System	type=USER_CMD msg=audit(1363017465.033:74205): user pid=18885 uid=0 auid=4294967295 ses=4294967295 msg=cwd="/opt/webcontrol" cmd=73657276696365207761746368646F6720737461747573 terminal=? res=success'
2015-03-11 15:57:50	localhost	AUD	Operating System	type=CRED_ACQ msg=audit(1363017465.034:74206): user pid=18886 uid=0 auid=4294967295 ses=4294967295 msg=op=PAM:setcred acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'
2015-03-11 15:57:50	localhost	AUD	Operating System	type=USER_START msg=audit(1363017465.034:74207): user pid=18886 uid=0 auid=4294967295 ses=4294967295 msg=op=PAM:session_open acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'
2015-03-11 15:57:50	localhost	AUD	Operating System	type=USER_START msg=audit(1363017465.087:74213): user pid=18913 uid=0 auid=4294967295 ses=4294967295 msg=op=PAM:session_open acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'

- The **Refresh** button is used to update the table of records shown using the options in the drop-down filters (**Host**, **Event Type**, **View** and **Tag**). Note however that the filter options are set when the menu is opened. To update the options, select another menu and then return to this menu. For example, if another host is added to the network and sends records to the server, the new server only appears in the **Hosts** drop-down after reloading the menu.

8.2.3 Download

You can access this menu by selecting **Logs** and then clicking **Download**. You can use the menu to [create and download archives files](#)^[95]. For support issues, Avaya will require the archive files downloaded from the server. The server compresses the log files into a **.tar.gz** format file. You can then download the file by clicking on the link.

For IP Office Release 10.0, you can configure the server to include packet capture logs for the server, see [Packet Capture Settings](#)^[115].

System

Logs

Updates

Settings

AppCenter

Debug Logs

Syslog Event Viewer

Download

Debug Files

Select AllCreate ArchiveDelete Selected

There is no data available

There are no core dump files available.

Logs

Select AllCreate ArchiveDelete Selected

Name	Last Modified	Size	Delete
webmanagement_logs_2015-03-11-16-01.tar.gz	2013-05-11 16:01:33	1019K	<input type="checkbox"/>
system_logs_2015-05-11-16-01.tar.gz	2013-05-11 16:01:32	54.3K	<input type="checkbox"/>
webcontrol_logs_2015-03-11-16-01.tar.gz	2013-05-11 16:01:25	287.3K	<input type="checkbox"/>
ipoffice_logs_2015-03-11-16-01.tar.gz	2013-05-11 16:01:25	104.4K	<input type="checkbox"/>
voicemail_logs_2015-03-11-16-01.tar.gz	2013-05-11 16:01:25	930K	<input type="checkbox"/>
install_logs_2015-03-11-16-01.tar.gz	2013-05-11 16:01:25	10.2K	<input type="checkbox"/>
onex_logs_2015-03-11-16-01.tar.gz	2013-05-11 16:01:25	1.1K	<input type="checkbox"/>

8.3 Updates

This menu displays the different versions of server operating system files and application files available in the file repositories. The file repository locations are configured through the [Settings | General](#) ^[112] page.

System
Logs
Updates
Settings
AppCenter

System
Check Now
Review Updates
Update All

OS	Version	Kernel Version	Last Update	Status
Linux	release 6.6 (Final)	3.11.4-1.appscard.el6.i686	-	up to date

Services
Check Now
Clear Local Cache
Update All

Application	Description	Current Version	Latest Available	Status	Actions
TTSEnglish	Avaya application.	7.0.0.25 build 4	7.0.0.25 build 4	up to date	Change Version Update Uninstall
Management Services	Avaya application. Placeholder description for IP Office.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall
one-X Portal	Avaya application. Placeholder description for one-X Portal.	10.0.0.0 build 223	10.0.0.0 build 223	up to date	Change Version Update Uninstall
Voicemail	Avaya application. Placeholder description for Voicemail.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version Update Uninstall
Watchdog	Avaya application. Placeholder description for Watchdog.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall
Web Manager	Avaya application. Placeholder description for Web Manager.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall
webcontrol	Avaya application. Web page used to manage the local machine. Requires cli-commands of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall
webcontrol-plugin-appscard	Avaya application. Webcontrol plugin used in UCM systems. Requires webcontrol of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall
VMProWebService	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version Update Uninstall
VmPro-Mapi	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	out of date	Change Version Update Uninstall

The menu consists of 2 sections:

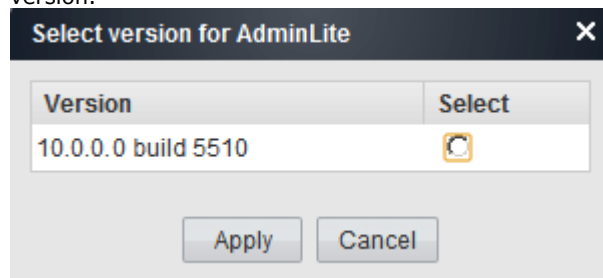
- [Services](#) ^[110]
This section displays the current version of application files. It also shows whether update files are available.
- [System](#) ^[111]
This section displays the current version of the operating system and whether update files are available.

8.3.1 Services

You can access this menu by selecting **Updates**. The **Services** section shows details of the current version of each application installed and the latest version available.

Services						Check Now	Clear Local Cache	Update All
Application	Description	Current Version	Latest Available	Status	Actions			
TTSEnglish	Avaya application.	7.0.0.25 build 4	7.0.0.25 build 4	up to date	Change Version Update Uninstall			
Management Services	Avaya application. Placeholder description for IP Office.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
one-X Portal	Avaya application. Placeholder description for one-X Portal.	10.0.0.0 build 223	10.0.0.0 build 223	up to date	Change Version Update Uninstall			
Voicemail	Avaya application. Placeholder description for Voicemail.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version Update Uninstall			
Watchdog	Avaya application. Placeholder description for Watchdog.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
Web Manager	Avaya application. Placeholder description for Web Manager.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
webcontrol	Avaya application. Web page used to manage the local machine. Requires cli-commands of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
webcontrol-plugin-appscard	Avaya application. Webcontrol plugin used in UCM systems. Requires webcontrol of equal or greater version.	10.0.0.0 build 137	10.0.0.0 build 137	up to date	Change Version Update Uninstall			
VMPProWebService	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	up to date	Change Version Update Uninstall			
VmPro-Mapi	OS application.	10.0.0.0 build 58	10.0.0.0 build 58	out of date	Change Version Update Uninstall			

- The **Change Version**, **Update** and **Update All** buttons in the panel are not useable unless appropriate update files are available in the applications [software repository](#)^[92]. This also affects the availability of the **Install** button option.
- **Change Version**
Clicking on this button shows the update files available for the application in the server's [file repository](#)^[92] with the current version selected. Selecting another version and clicking **Apply** upgrades or downgrades to that version.



- **Update**
Clicking on this button starts an update of the related application to the latest available version in the application [file repository](#)^[92].
- **Uninstall**
Clicking on this button uninstalls the selected application.
 - If there are installation files for the application in the application [file repository](#)^[92], the button becomes an **Install** button.
 - If there are no installation files for the application in the file repository, the menu no longer list the application.
- **Install**
This button appears for uninstalled applications if the server has files for the application the application file repository.
- **Check Now**
Clicking this button makes the IP Office Application Server recheck the version of update files available in the file repository. Normally it does this automatically when the **Updates** page is loaded.
- **Clear Local Cache**
Clicking this button removes older update installation files and other material that may accumulate on the server over time.
- **Update All**
Clicking this button upgrade those applications that support upgrading without being uninstalled (see above) to the latest versions available in the application file repository.

8.3.2 System

You can access this menu by selecting **Updates**. The **System** section shows details of the operating system.

System				
			Check Now	Review Updates
			Update All	
OS	Version	Kernel Version	Last Update	Status
Linux	release 6.6 (Final)	3.11.4-1.appscard.el6.i686	-	up to date

- **Check Now**

Clicking this button makes the IP Office Application Server recheck the version of update files available in the file repository. Normally it does this automatically when the **Updates** page is loaded.

- **Review updates**

Clicking this button will display a list of the available update files. This list allows selection of which updates you want to install.

System Updates		
Select	Name	Version
<input checked="" type="checkbox"/>	NetworkManager.i386	1:0.7.0-10.el5_5.1
<input checked="" type="checkbox"/>	NetworkManager-glib.i386	1:0.7.0-10.el5_5.1
<input checked="" type="checkbox"/>	apr.i386	1.2.7-11.el5_5.2
<input checked="" type="checkbox"/>	apr-util.i386	1.2.7-11.el5_5.1
<input checked="" type="checkbox"/>	autofs.i386	1:5.0.1-0.rc2.143.el5_5.4
<input checked="" type="checkbox"/>	bzip2.i386	1.0.3-6.el5_5
<input checked="" type="checkbox"/>	bzip2-libs.i386	1.0.3-6.el5_5
<input checked="" type="checkbox"/>	crash.i386	4.1.2-4.el5.centos.1
<input checked="" type="checkbox"/>	db4.i386	4.3.29-10.el5_5.2
<input checked="" type="checkbox"/>	dbus-glib.i386	0.73-10.el5_5
<input checked="" type="checkbox"/>	device-mapper.i386	1.02.39-1.el5_5.2
<input checked="" type="checkbox"/>	device-mapper-event.i386	1.02.39-1.el5_5.2
Select All Unselect All Apply Selected Updates Cancel		

- **Update All**

Clicking this button will install all the available updates without going through the process of selecting with updates to install.

8.4 Settings: General

You can access this menu by selecting **Settings** and clicking on the **General** tab.

8.4.1 Software Repositories

The IP Office Application Server can use either remote or local software repositories to store software update files. The server has separate repositories for operating system updates, IP Office application installation files and Windows client files. The [Updates](#)^[109] and [AppCenter](#)^[124] menus use the files present in the appropriate repository.

- **Repository**

If not using the **Local** option, this field sets the URL of a [remote HTTP file repository](#)^[94]. Note that you cannot use the same URL for more than one repository.

- **Local**

This checkbox sets whether the file repository used is local (files stored on the IP Office Application Server) or remote (a folder on a HTTP web server specified in the Repository field).

- **File / Browse / Add**

With **Local** selected, you can use this field and adjacent buttons to browse for a specific update file. After selecting the file, click **Add** to upload the file to the server's file store.

8.4.2 Syslog

These settings control the receiving and the forwarding of Syslog records by the server. For details of system monitor Syslog records, refer to the "Using IP Office System Monitor" manual.

- **Log files age (days)**

Set the number of days the server retains each type of record before automatically deleting it. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. These settings are not applied to the server's own Syslog monitor records which are retained for 3 days.

- **Apply general settings to all file types**

If selected, the setting for General log files is applied to all file types.

- **Max log size (MB)**

Set the maximum total size of each type of records the server retains before automatically deleting the oldest records. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. These settings are not applied to the server's own Syslog monitor records.

- **Apply general settings to all file types**

If selected, the setting for **General log files** is applied to all file types.

- **Receiver Settings**

These settings control if and how the server can receive Syslog records.

- **Enable**

If selected, the server can receive Syslog records using the port configured below.

- **TCP Port**

Sets the port number used for receiving Syslog records using **TCP**.

- **TLS Port**

Sets the port number used for receiving Syslog records using **TLS**.

- **UDP Port**

Sets the port number used for receiving Syslog records using **UDP**.

- **Forward Destination 1**

These settings control whether the server forwards copies of Syslog records it receives to another server.

- **Enable**

If selected, the server will forward copies of the Syslog records it receives.

- **IP Address: Port**

Sets the address of the destination server and the destination port for the forwarded records.

- **Protocol**

Set the protocol, **UDP**, **TLS** or **TCP**, for the forwarding.

- **Forward Destination 2**

These settings control whether the server forwards copies of the Syslog records it receives to a second server. The settings are the same as for the first forwarding destination.

- **Select Log Sources**

These options allow selection of which server reporting to include in the Syslog reports. The available options are:

- **Authentication and authorization privileges**

- **Information stored by the Linux audit daemon (auditd)**

- **NNTP(News)/UUCP(Usenet) protocols**
- **Apache web server access_log and error_log**

8.4.3 Certificates

This menu allows the generation or downloading of the security certificate that can then be used by the IP Office applications hosted by the server.

CA Certificate

- **Create new**
If selected, the server generates a new own security certificate when **Regenerate** is clicked.
- **Renew existing**
If selected, the server's current self-generated security certificate is renewed when **Regenerate** is clicked.
- **Import**
If select, the fields for browsing to and selecting a certificate file to upload to the server appear. Select the file and click **Upload**.
- **Export**
The server's current security certificate is not included in any application backup and restore operations. The **Export** option allow you to export the server's current certificate as an encrypted file. You can then later restore the certificate back to the same server using the **Import** option.
 - **Password/Confirm Password**
Enter a password that the server then applies to the encrypted certificate file when using **Encrypt and Download**.
 - **Encrypt and Download**
When pressed, the server displays a pop-up link from which you can download an encrypted file containing the server's current certificate. Once you have downloaded the file it is deleted from the server.
- **Regenerate**
Create a certificate or renew the existing certificate.
- **Download (PEM-Encoded)**
Download the certificate as a PEM file. You can then apply the certificate to any remote device that needs to establish secure encrypted connection with the server.
- **Download (DER-Encoded)**
Download the certificate as a CRT file. You can then the certificate to any remote device that needs to establish secure encrypted connection with the server.

Identity Certificates

- **Renew automatically**
If selected, the server automatically generates a new security certificate following any major change such as changes to its LAN settings. The server automatically applies the new certificate to the application services run on the server.
- **Create certificate for a different machine**
If selected, the server can generate a new security certificate for another server. Note however that this requires a settings to exactly match those of the other server in order for the certificate to be regarded as valid for one offered by that other server.
- **Regenerate and Apply**
When clicked, the server generates a new security certificate using the identity settings specified. The server then applies the security certificate to the IP Office application services run by the server. Note that this process requires the services to all be automatically stopped and restarted which will end any current connections.
- **Download (PEM-encoded)**
Download the certificate using the identity settings specified as a PEM file. You can then apply the certificate to any remote device that needs to establish secure encrypted connection with the server.
- **Download (DER-encoded)**
Download the certificate using the identity settings specified as a CRT file. You can then the certificate to any remote device that needs to establish secure encrypted connection with the server.

8.4.4 Web Control

Note that changing any of these settings will require you to login again.

- **Inactivity Timeout**
Select the period of inactivity after which the server automatically logs out the web session. Changing this value requires you to login again. The options are **5 minutes**, **10 minutes**, **30 minutes** and **1 hour**.

8.4.5 Backup and Restore

These controls allow you to backup and restore the application settings of selected IP Office applications. This is a local backup onto the server. For more advanced backup functions use the Web Manager menus.

Note that these options are not shown if the web control menus are accessed as within an embedded window within web management.

- **Management Services**

These control provides options to backup/restore the configuration settings of the Management Services application running on the server.

- **Voicemail Pro Server**

For the Voicemail Pro server, these controls can only be used to restore an existing backup. Using the Voicemail Pro client, you can configure the voicemail server to perform regular (daily, weekly and or monthly) automatic backups of selected options including messages and prompts. You can also use the Voicemail Pro client to perform an immediate backup.

- Selecting the **Restore** button displays the backups available in the backup folder (*/opt/vmpro/Backup/Scheduled*). The backup name includes the date and time and whether the backup was a manual or scheduled backup. Selecting a backup and clicking **OK** starts the restoration process. For details, refer to the Voicemail Pro client help.

- **Warning: Close any Voicemail Pro client before restoring**

The restoration process requires the voicemail service to shutdown and restart. This does not occur if any Voicemail Pro client is connected to the service during the restore and leads to an incorrect restoration of files.


- **one-X Portal for IP Office**

one-X Portal for IP Office has its own method of backup and restore. You can access this through the one-X Portal for IP Office web client administration menus.

- **WebRTC**

Allow backup and restoration of the WebRTC settings.

8.4.6 Voicemail Settings

This setting sets the debug logging level used by the Voicemail Pro application if running. For the one-X Portal for IP Office application, the logging level is set through the applications own web administration menus. Log files are retrievable through the [Logs | Download](#)  menu.

- **Debug Level**

This control sets the level of information that the service includes in its log files. The options are **None**, **Critical**, **Error**, **Warning**, **Information** and **Verbose**. The default level is **Information**.

8.4.7 Contact Recorder Settings

This settings sets the debug logging level used by the Contact Recorder for IP Office application if installed on the server.

- **Debug Level**

This control sets the level of information that the service includes in its log files. The options are **None**, **Critical**, **Error**, **Warning**, **Information** and **Verbose**. The default level is **Information**.

8.4.8 Integrated Reporting Settings

This settings sets the debug logging level used by the Integrated Contact Reporter application if installed on the server.

- **Debug Level**

This control sets the level of information that the service includes in its log files. The options are **None**, **Critical**, **Error**, **Warning**, **Information** and **Verbose**. The default level is **Information**.

8.4.9 EASG Settings

The server uses these settings for connections from an Avaya Enhanced Access Security Gateway (EASG) server. EASG is used by systems' being supported directly by Avaya. It allows Avaya technician access to the server for server maintenance.

Note that only users with Web Services Security rights are able to change the EASG settings.

- **Status**

This field sets whether the EASG service is enabled on the server. In order to use EASG the server's product ID must be registered through the Avaya Global Registration Tool (GRT) website.

- **Port**

This field sets the port on which the service listens for connections. The default port is **2222**.

- **Service Listening**
Select whether the server listens on any connection (**Any**) or just on SSL VPN tunnels (**Any Tunnel**).
 - **Any**
If selected, the server listens on any connection. This setting is deprecated as it is less secure than **Any Tunnel**.
 - **Any Tunnel**
If selected, the server only listens on SSL VPN connections. This requires the IP Office configuration to include an SSL VPN tunnel.
- **EASG Users**
This drop down lists the different types of user logins (**craft**, **init**, **inads**, **rasaccess** and **sroot**) that may be used by the EASG service and technicians.
- **EASG User Enabled**
Sets whether access by the EASG users currently selected above is enabled or disabled.
- **EASG Technician Certificates**
Lists the current technician certificates present on the server.
 - **Delete Selected Certificate**
Delete the certificate currently selected in the **EASG Technician Certificates** selector above.
 - View Selected Certificate
View the certificate currently selected in the **EASG Technician Certificates** selector above.
- **Upload Technician Certificate**
Certificates are used to control technician access to the server for maintenance actions. If a technician requires access to the server for maintenance, they will provide a certificate that must first be uploaded to the server using this menu. Typically these are short-lived certificates valid for the period of potential maintenance access needed, for example 14 days.
 - **Browse**
Browse for the certificate file to upload.
 - **Password**
Enter the password for the certificate.
 - **Upload**
Click to upload the selected certificate file.
- **Product Id**
The product ID. This is the ID registered with the EASG server from which the server is maintained.
- **Change Product Id**
If clicked a new ID is generated for the server. This will require the server to be re-registered with the Avaya GRT website.

8.4.10 Packet Capture Settings

Supported for IP Office Release 10.0 and higher. This menu allows the configuration of packet capture on one or all of the server's LAN interfaces. When enabled, traffic is logged to tcpdump log files that can be downloaded from the [Logs | Download](#)^[108] menu along with other log files.

- **Interface:** *Default = All*
This field allows selection of the server LAN interface to which packet capture is applied when run.
- **Maximum File Size (MB):** *Default = 100MB, Range = 1MB to 2000MB*
This field sets the maximum size of each individual log file size. When the current file reaches this size a new log file is started.
- **Maximum File Number:** *Default = 10, Minimum = 1*
This field sets the maximum number of packet capture log files. On reaching this limit, when the server starts a new log file it also automatically deletes the oldest log file.
- **Maximum Total Size (MB):** *Default = 5120MB*
This field shows the total allowed file space for packet capture log files. The combined values of the fields above cannot exceed this value.
- **Start/Stop:** *Default = Stopped*
These buttons control whether packet capture logging is running or not.

8.4.11 Watchdog

- **Log files age (days)**
Sets the number of days that log file records are retained. This does not affect log file [archives](#)^[108]. Not applied to one-X Portal for IP Office.

8.4.12 Set Login Banner

- **Login Banner Text**

You can use this field to set the additional text displayed on the login menu. After changing the text click **Save**. By default the field is blank.

8.5 Settings: System

You can access this menu by selecting **Settings** and clicking on the **System** tab.

8.5.1 Network

- **Network Interface**

This drop down allows selection of network interfaces for which the settings are shown. Within the IP Office configuration, **Eth0** matches LAN1, **Eth1** matches LAN2. A pre-built server only uses **Eth0**. This port is labeled as port 1 on the physical server.

- **Host Name**

Sets the host name that the IP Office Application Server should use. This setting requires the local network to support a DNS server. Do not use **localhost**.

- **! IMPORTANT: DNS Routing**

For internal use, this value must be reachable by DNS within the customer network. If the server will also be supporting external applications, it needs to be reachable by external DNS. Consult with the customer's IT support to ensure the name is acceptable and that routing to it has been configured correctly.

- **! IMPORTANT: Security Certificate Field**

This value is used as part of the default security certificate generated by the server. If changed, the server generates a new default certificate, during which time access to the server is disrupted for several minutes. In addition, any applications using the default certificate need to be updated with the new certificate.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual *"Deploying Avaya IP Office Servers as Virtual Machines"* for further details.

- **Use DHCP**

If selected, the IP address, subnet mask and default gateway information is obtained by the server making DHCP requests. The related fields are greyed out and cannot be set manually, instead they show the values obtained in response to the DHCP request.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual *"Deploying Avaya IP Office Servers as Virtual Machines"* for further details.

- **IP Address**

Displays the IP address set for the server. If not using DHCP, you can edit the field to change the setting.

- **! IMPORTANT: Security Certificate Field**

This value is used as part of the default security certificate generated by the server. If changed, the server generates a new default certificate, during which time access to the server is disrupted for several minutes. In addition, any applications using the default certificate need to be updated with the new certificate.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual *"Deploying Avaya IP Office Servers as Virtual Machines"* for further details.

- **Subnet Mask**

Displays the subnet mask applied to the IP address. If not using DHCP, you can edit the field to change the setting.

- **Default Gateway**

Displays the default gateway settings for routing. If not using DHCP, you can edit the field to change the setting.

- **System DNS**

Enter the address of the primary DNS server. This option is greyed out if the address of the DNS server is set to be obtained from the DHCP server (see below).

- **Automatically obtain DNS from provider**

This setting is only used if **Use DHCP** is also selected. If selected, the server attempts to obtain DNS server details from the DHCP server.

- **Create Subinterface**

You can use this control to create an additional VLAN subnet on the same port. Clicking the button displays the menu for the subinterface network settings.

- **Delete Subinterface**

Delete the subinterface.

8.5.2 Avaya IP Office LAN Settings

- **Avaya Office LAN1**

These settings are used for the LAN1 interface of the IP Office application run by the server. LAN1 is also referred to as LAN.

- **Enable Traffic Control**

When enabled, the server throttles the rate at which it sends UDP packets from the IP Office service to IP Office System Monitor. This may be necessary if the IP Office System Monitor traces indicate a high number of lost packets.

- **Network Interface**

Use the drop-down to select which port on the server should be used for LAN1.

- **Avaya Office LAN2**

These settings are used for the LAN2 interface of the Management Services application run by the server. LAN2 is also referred to as WAN.

8.5.3 Date and Time

The server uses these settings to set or obtain a UTC date and time. The server uses those values for its services.

- **Date**

For a server not using NTP, this field shows the server's current date and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.

- **Time**

For a server not using NTP, this field shows the server's current UTC time and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.

- **Timezone**

In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field determines the appropriate offset applied to the UTC time above. Note that changing the timezone can cause a "Session expired" message to appear in the browser in which case you need to login again.

- **! WARNING**

For a virtualized server this field is used to generate the server's **Host PLDS ID**. Changing this value changes that ID. If that ID has been used to generate a local (nodal) PLDS license file for the server, those licenses will become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual "Deploying Avaya IP Office Servers as Virtual Machines" for further details.

- **Enable Network Time Protocol**

When selected, the server obtains the current date and time from the NTP servers listed in the **NTP Servers** list below. It then uses that date and time and makes regular NTP requests for updates.

- **NTP Servers**

With **Enable Network Time Protocol** selected, use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at <http://support.ntp.org/bin/view/Servers/WebHome>. However, it is your responsibility to comply with the usage policy of the chosen server. Choose several unrelated NTP servers in case one of the servers becomes unreachable or its clock unreliable. The server uses the responses it receives from each NTP server to determine reliability.

-
- The IP Office system can also use NTP to obtain its system time.
 - **Synchronize system clock before starting service**
Use this option to synchronize the system clock to an NTP time server before starting other services. Do not use this option if the time server cannot be reliably reached. Waiting for synchronization to occur may block use of the system until a timeout has passed.
 - **Use local time source**
When not selected, external NTP takes priority over the internal system clock. If selected, the local system clock is used as the time source. Only use this option if system clock is synchronized with another reliable source, for example a radio controlled clock device.

8.5.4 Authentication

This menu controls the method of password storage and authentication used by server applications.

- These settings are only accessible if logged in via referred authentication or as the local Linux root.
- **Enable referred authentication**
The password authentication used for access to the some services hosted by the server use either each services' own security settings or the security user accounts configured in the Management Services service running on the IP Office Application Server. See [Password Authentication](#)^[16]. This setting controls which method is used.
 - **Enabled**
With referred authentication enabled, the security settings of the Management Services service running on the IP Office Application Server control access to the following other services:
 - **Web control menus**
 - **Voicemail Pro admin**
 - **one-X Portal for IP Office admin**
 - **IP Office Web Manager**
 - **Disabled**
With referred authentication disabled, each service controls access to itself using its own local account settings.

8.5.5 Increase Root Partition

This menu option is supported for VMware virtualized servers. If through the menus of the virtual machine's host platform, the size of the root disk is increased, this menu then needs to be used to instruct the virtual server to use that additional space.

- **Increase Partition Size**
If additional disk space is available it is indicated by the menu. Clicking the button instructs the server to adjust its root partition to include that additional space and to format the additional space appropriately. After clicking **Save** the server must be restarted.

8.5.6 HTTP Server

This setting controls where the server allows storage for HTTP/HTTPS backup.

- **Enable HTTP file store for backup/restore**
If selected, the server can act as the 'remote server' destination for HTTP/HTTPS backups configured through the Web Manager menus. When enabled, the [System](#)^[103] menu displays the quota available for backups. Servers with Voicemail Pro only support this option on disks larger than 155GB. Servers without Voicemail Pro only support this option on disks larger than 95GB.

8.5.7 Change Root Password

Server installation creates two Linux user accounts; **root** and **Administrator**. You can use these fields to change the **root** account password. The new password must conform to the [password rules](#)^[12].

- These settings are only accessible if logged in via referred authentication or as the local Linux root.
- **New Password**
Enter the new password.
- **Confirm New Password**
Confirm the new password.

8.5.8 Change Local Linux Account Password

Server installation creates two Linux user accounts; **root** and **Administrator**. You can use these fields to change the **Administrator** account password.

- These settings are only accessible if logged in via referred authentication or as the local Linux root.

Note that this is different from the **Administrator** account used for access to Web Manager and the Management Services configuration. Whilst both **Administrator** accounts are given the same password during the server ignition, this menu allows the Linux password to be changed separately.

The password for the **Administrator** account used by Web Manager and Management Services configuration is changed using those applications.

The new password must conform to the [password rules](#)^[12].

- **New Password**
Enter the new password.
- **Confirm New Password**
Confirm the new password.

8.5.9 Password Rules Settings

These settings set the password requirements used when changing passwords through using these menus.

- **Minimum password length**
This field set the minimum length of new passwords. Note that the combined requirements of the fields below for particular character types may create a requirement that exceed this value. Note also that the maximum password length is 31 characters.
- **Minimum number of uppercase characters**
This field sets the number of uppercase alphabetic characters that new passwords must contain.
- **Minimum number of lowercase characters**
This field sets the number of lowercase alphabetic characters that new passwords must contain.
- **Minimum number of numeric characters**
This field sets the number of numeric characters that new passwords must contain.
- **Minimum number of special characters**
This field sets the number of non-alphanumeric characters that new passwords must contain.
- **Allow character sequences**
When selected, the server allows character sequences such as **1234** or **1111** or **abcd** in new passwords. When not selected, the field below sets the maximum length of any sequence.
 - **Maximum allowed sequence length**
When **Allow character sequences** is not selected, this field sets the maximum allowed length of any character sequence .

8.5.10 Firewall Settings

The server can apply firewall controls to the incoming traffic it receives.

- **Activate**
Sets whether the firewall is active.
- **Enabled Filtering**
Sets whether the firewall should apply filtering to the traffic received by the server.
- **Enable TCP ports**
Select whether the server allows the following TCP ports when the firewall is active.
 - **21:** If selected, allow port TCP 21.
 - **25:** If selected, allow port TCP 25.
 - **80:** If selected, allow port TCP 80.
 - **8000:** If selected, allow port TCP 8000.
 - **! WARNING: Blocking Port 8000 Disables Solution Upgrades**
If filtering is enabled but with port 8000 disabled, then centralized upgrading from the primary server of associated secondary, application and expansion servers is blocked.
 - **8069:** If selected, allow port TCP 8069.
 - **8080:** If selected, allow port TCP 8080.
 - **9080:** If selected, allow port TCP 9080.

- **Enable UDP ports**

Select whether the server allows the following UDP ports when the firewall is active.

- **69:** If selected, allow port UDP 69.

8.5.11 Additional Hard Drive Settings

These additional settings appear on servers with an additional hard disk.

- **Additional Hardware Info**

The fields vary depending on the type and location of the additional hard disk.

- **Mount**

- **Activate**

Enabling this option automatically mounts the additional hard disk.

- **Mount Point Path**

This is the root name assigned for the additional hard disk and the disk partition. The full mount path name for each partition is automatically configured by the system adding **/partition1**, **/partition2**, etc. as a suffix. For Contact Recorder for IP Office set the name to **/additional-hdd#1**.

- **Current Partition Mount Points**

This field shows the full path for the partitions created on the disk. This is the path that should be used for other applications to use the partition. For example this is the value to use for the Contact Recorder for IP Office application's **Call Storage Path** setting.

- **Format Hard Drive**

These options are shown for an additional hard drive added after initial system installation.

- **Enable**

Is selected, format the additional drive using the partition settings below. This will erase any existing data on the additional drive.

- **Partition X size (GB)**

Set the size for the partitions, up to 3, to be created on the additional drive when formatted.

8.6 VNC

This menu allows you to configure VNC access to the server's graphical desktop. You can then use the VNC access either through these menus or using a separate third-party such as TigerVNC. See Using VNC. The VNC menu is not supported for virtualized servers.

- VNC access using the root user account is not supported. Some applications, for example Wireshark, require root user permissions and so cannot be used when accessing the server via VNC.
- For a server deployed as a VMware virtual machine, additional configuration may be necessary to allow the use of the VNC menu. For details refer to the manual "Deploying Avaya IP Office™ Platform Servers as Virtual Machines".

Settings

You can use this menu to start and stop the server's VNC service. The VNC client used to access the desktop must match the **Port** settings.

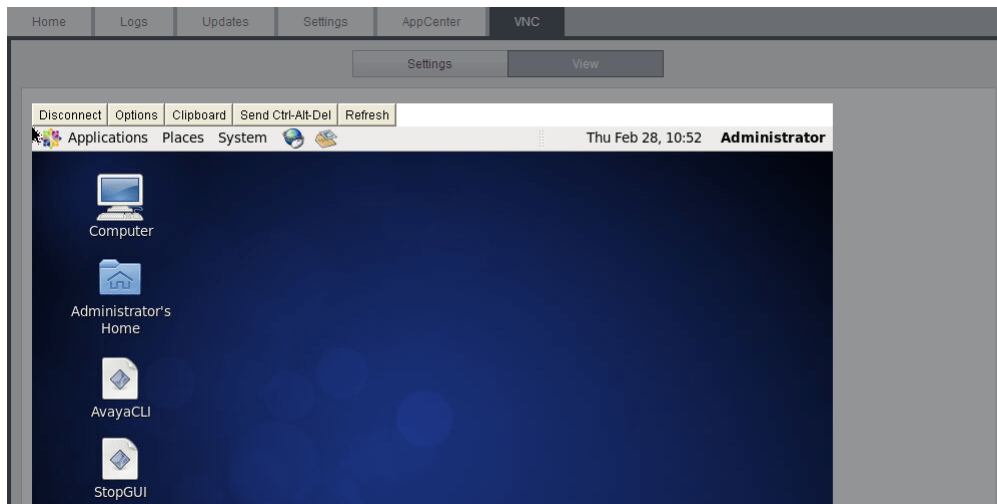
The screenshot shows the 'VNC Settings' dialog box within the 'Settings' tab of the Web Control interface. The dialog has a 'Password' field and a 'Port' field with the value '5807'. There are 'Start VNC', 'Stop VNC', and 'Apply' buttons. The background shows the 'Settings' tab with 'System', 'Logs', 'Updates', 'Settings', 'AppCenter', 'Linux Downloads', and 'VNC' tabs at the top.

View

You can use this menu to connect and display the desktop using the browser as the VNC client.

The screenshot shows the 'VNC Authentication' dialog box. It has a 'Password' field and an 'OK' button. The background shows the 'VNC' tab of the Web Control interface with 'Home', 'Logs', 'Updates', 'Settings', 'AppCenter', and 'VNC' tabs at the top. Below the tabs are 'Settings' and 'View' buttons. A menu bar with 'Disconnect', 'Options', 'Clipboard', 'Send Ctrl-Alt-Del', and 'Refresh' is visible.

Once the password is accepted, the operating system desktop appears.



8.7 App Center

You can access this menu by selecting **AppCenter**. You can use the menu to download files for use on the local PC. For example, the Voicemail Pro client used to administer the Voicemail Pro server application.

The file repository location is configured through the [Settings | General](#) ⁽¹¹²⁾ page.

Application	Added at	Size	Description
Softconsole_10_1_0_0_0.exe	2015-05-16 05:54:25	53.9M	IP Office SoftConsole
AdminLite_10_1_0_137.exe	2015-05-16 05:54:13	123M	IP Office Server Edition Manager
VmPro-Client_10_1_0_58.exe	2015-05-16 05:54:21	79.2M	IP Office Voicemail Pro Client
TAPI_1_0_0_41.exe	2015-05-16 05:54:27	10.6M	IP Office TAPI Service Provider
VmPro-Mapi_10_1_0_58.exe	2015-05-16 05:54:21	25.2M	IP Office Voicemail Pro MAPI Service
Softphone_Mac_4.1.1.2_CE4112c_74851.dmg	2015-05-16 05:54:23	45.2M	IP Office Video Softphone (Mac)
DLink_1_0_0_5.exe	2015-05-16 05:54:28	3.5M	IP Office DevLink

The files included in the installation may vary. Note that some packages require the addition of licenses to the system and configuration changes. Refer to the specific installation manuals for those applications:

- **VmPro...ClientOnly.exe**
This is the installation package for the Voicemail Pro client application used to administer the Voicemail Pro server application.
- **VmPro...Mapi.exe**
This is the installation package for the MAPI proxy. This is installed on a Windows PC in the same network as the Windows Exchange server. It allows the Linux based Voicemail Pro server to access UMS services. Refer to the Voicemail Pro installation manual.
- **IPOAdminLite...**
This is the installation package for the IP Office Manager application. Note that this is an installer for IP Office Manager, System Monitor and System Status Application tools only. It is not the full IP Office Administration and User package used with other IP Office systems.
- **DLink...**
This is the installation package for the IP Office DevLink 3rd-party TAPI interface.
- **TAPI...**
This is the installation package for the IP Office 1st -party TAPI interface.
- **Softconsole...**
This is the installation package for the IP Office SoftConsole application. This is an application used by receptionist and operator type users to answer and distribute incoming calls.
- **...Softphone...**
This is a SIP softphone application for use by individual users. For IP Office Release 9.1 only the Mac version is provided and supported.

Chapter 9.


Additional Processes

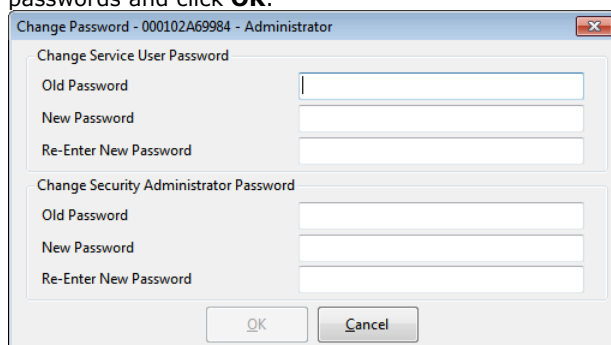
9. Additional Processes

9.1 Initial Configuration Using IP Office Manager

The Management Services service's initial configuration can be done using IP Office Manager rather than IP Office Web Manager if necessary. This is especially important for servers centrally managed using Avaya System Manager.

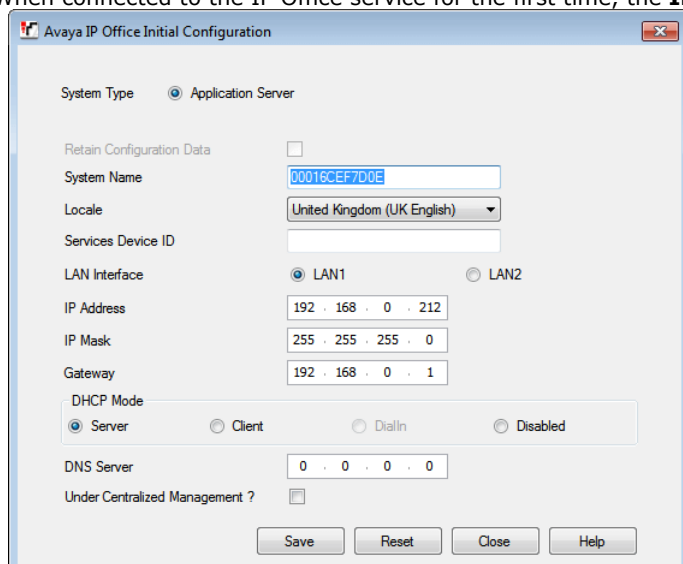
To perform IP Office initial configuration:

1. Start IP Office Manager. Click  and use the **Select IP Office** menu to discover the available IP Office systems.
2. Select the tick box next to the application server. Click **OK**.
 - If any Management Services passwords are at their default values, a menu to change the default passwords appears. These are the passwords for the Management Services and Web Manager menu **Administrator** (default password **Administrator**) and **security** (default password **securitypwd**) users. Enter the new passwords and click **OK**.



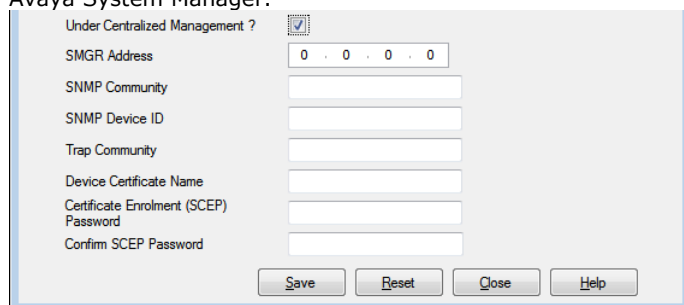
The image shows a 'Change Password' dialog box for the 'Administrator' user. It contains two sections: 'Change Service User Password' and 'Change Security Administrator Password'. Each section has fields for 'Old Password', 'New Password', and 'Re-Enter New Password'. The 'Old Password' field for the Administrator is empty, while the others contain placeholder text. At the bottom are 'OK' and 'Cancel' buttons.

3. When connected to the IP Office service for the first time, the **Initial Configuration** menu appears.



The image shows the 'Avaya IP Office Initial Configuration' dialog box. It has a 'System Type' section with 'Application Server' selected. Below are various configuration fields: 'Retain Configuration Data' (checkbox), 'System Name' (text field with '00016CEF7D0E'), 'Locale' (dropdown menu showing 'United Kingdom (UK English)'), 'Services Device ID' (text field), 'LAN Interface' (radio buttons for 'LAN1' and 'LAN2'), 'IP Address' (text field with '192 . 168 . 0 . 212'), 'IP Mask' (text field with '255 . 255 . 255 . 0'), 'Gateway' (text field with '192 . 168 . 0 . 1'), 'DHCP Mode' (radio buttons for 'Server', 'Client', 'DialIn', and 'Disabled'), 'DNS Server' (text field with '0 . 0 . 0 . 0'), and 'Under Centralized Management ?' (checkbox). At the bottom are 'Save', 'Reset', 'Close', and 'Help' buttons.

4. Check that the settings match those required for the server and the IP Office. For full details, refer to the IP Office Manager help.
5. If the server will be under centralized management from Avaya System Manager, select the **Centralized Management** checkbox. Enter the details required for the Avaya System Manager. Enter the details required for Avaya System Manager.



The image shows a dialog box for 'Under Centralized Management ?'. It has a checkbox that is checked. Below are several text fields: 'SMGR Address' (text field with '0 . 0 . 0 . 0'), 'SNMP Community', 'SNMP Device ID', 'Trap Community', 'Device Certificate Name', 'Certificate Enrolment (SCEP) Password', and 'Confirm SCEP Password'. At the bottom are 'Save', 'Reset', 'Close', and 'Help' buttons.

6. Click **Save**. When displayed, click **OK**.

Chapter 10.

Document History

10. Document History

Date	Issue	Changes
21st March 2017	12a	<ul style="list-style-type: none">• Updated for IP Office Release 10.1.
16th May 2017	12b	<ul style="list-style-type: none">• First issue for 10.1. GA.
5th June 2017	12c	<ul style="list-style-type: none">• WebRTC Configuration section hidden.
13th June 2017	12d	<ul style="list-style-type: none">• WebRTC Configuration section reinstated.
5th July 2017	12e	<ul style="list-style-type: none">• Minor corrections. [IPOFFICE-108272]
21st August 2017	12f	<ul style="list-style-type: none">• Minor typo correction.
11th September 2017	12g	<ul style="list-style-type: none">• Clarify the use of the Archive Solution setting for call recording.
6th November 2017	12h	<ul style="list-style-type: none">• Additional hard drive installation notes added to Application Server output.• Clarification on changing portal password to achieve synch with IP Office.• Remove incorrect mention of Edge support for Contact Recorder

Index

3

3rd Party database integration 15

A

Add

Sub-interface 118

Additional documentation 13

Address

DNS 80, 118

IP 80, 118

Administrator

Login 50

Application

Auto-start 82

Install 86

Repositories 92, 112

Start 82

Stop 82

Uninstall 91

Upgrade 86, 87

Application files

Upload files 86, 93

Application Logs 107

Archive 108

Audit Log 107

Auto-start 82

B

Backup 112

Custom folders 48

one-X Portal for IP Office 59

Voicemail 46

BIOS 21

Boot

BIOS order 21

Browser 15

Bulletins 13

C

CentOS 13

Compatibility 12

Challenge Expiry Time 65

Change

IP Address 80

Check

Software version 110, 111

Clients 124

Compatibility 12

Configuration

one-X Portal for IP Office 50

Voicemail Pro 40

ContactStore 15

CPU

Usage 103

Create

DVD 21

Create a USB device 22, 88

Create Archive 108

Custom folders

Backup/restore 48

D

Database integration 15

Date 84, 119

Default

Gateway 80, 118

Password 79

Delete

Sub-interface 118

DHCP 80, 118

Disk

Usage 103

Disk Space 12

DNS 80, 118

Domain Name 65

Download

Logs 108

Windows Clients 124

DVD 21

DVD Drive 12

E

Enable Traffic Control 80, 118

F

Forward

Syslog records 112

FQDN 65

Fully Qualified Domain Name 65

G

Gateway 80, 118

General 112

H

Hard Disk 12

Headless 12

Home 103

Host Name 80, 118

I

Ignite 30

Inactivity timeout 85, 113

Initial configuration 50

Install

Application 86

IP Office Application Server 28

Service 86

Interface 80, 118

IP Address 42, 80, 118

IP Office

Check 50

Select 50

J

Javascript 15

L

Layer 4 Protocol 65

Linux 12, 13

Installation 28

Local 112

Log Files Age 112

Logging In 36, 79

Login 44, 79

Administrator 50

Banner text 112

Logs 106

Application 107

Archive 108

Audit 107

Download 108

Log Files Age 112

M

Mask 80, 118

Memory 12

Usage 103

Menu

- Download 108
- General 112
- Home 103
- Logs 106
- Logs Download 108
- Logs View 107
- Services 110
- System 111, 117
- Updates 109
- Updates Services 110
- Updates System 111
- View 107
- Windows Clients 124

Menus

- Inactivity timeout 85, 113

Module

- Restart 83
- Shutdown 83

N

Network 80, 118

- Change IP address 80
- Sub-interface 118

Network Time Protocol 84, 119

no Remote 44

Notifications 103

NTP 84, 119

O

one-X Portal for IP Office

- Auto-start 82
- Backup/restore 59
- Configuration 50
- Start 82
- Stop 82

Operating system 12

- Repositories 92, 112
- Upload files 93

P

Password

- Change 50
- Default 79
- Root password 82
- Rules 121

PC Requirements 12

Port

- Web Control 112

Processor 12

Protocol 65

R

RAM 12

- Usage 103

Reboot 83, 103

Recieve

- Syslog 112

Registrar 65

Related documents 13

Remote

- Server desktop 123

Remote Extension

- Enable 65

Remote Software Repositories 94

Remove

- Sub-interface 118

Repositories 92, 94, 112

Repository 112

Requirements 12

Restart 83

Restore 112

- Custom folders 48
- one-X Portal for IP Office 59
- Voicemail 46

Role 30

Root password

- Change 82
- Rules 121
- Set 30

Rules 121

S

Send

- Syslog records 112

Server

- Ignite 30
- NTP 84, 119
- Reboot 83, 103
- Role 30
- Shutdown 83, 103
- Type 30

Server desktop

- Remote 123

Server Name 44

Service

- Auto-start 82
- Install 86
- Start 82
- Stop 82
- Uninstall 91
- Upgrade 86

Services 110

- Start 103
- Status 103
- Stop 103
- View 37

Set

- Login banner 112
- Root password 30

Shutdown 83, 103

SIP

- Domain Name 65
- FQDN 65
- Registrar 65

SNMP 112

SNMP Support 112

Software 44

- Repositories 92, 112
- Repositories 94
- Unetbootin 18, 22, 88
- USB 18, 22, 88

Software Repositories 112

Software version

- Check 110, 111

Specification 12

Start 83

- Auto-start 82
- Service 82

Start Services 103

Status 103

Stop

- Service 82

Stop Services 103

Sub-interface 118

Subnet Mask 80, 118

- Supported
 - Browsers 15
- syslinux.cfg 22, 88
- Syslog
 - Settings 112
 - View 108
- System 111, 117
- T**
- TCP
 - Port 65
- Technical bulletins 13
- Time
 - Timezone 84, 119
- Timeout 85, 113
- TLS
 - Port 65
- Traffic Control 80, 118
- Type 30
- U**
- UDP
 - Port 65
- UMS 15
- Uninstall
 - Application 91
 - Service 91
- Unit Name/IP Address 44
- Update
 - Check version 110, 111
 - Services 110
 - System 111
- Updates
 - Services 109
 - System 109
- Upgrade
 - Application files 87
- Upgrading Applications 86
- Upload
 - Application files 86, 93
 - Operating system 93
 - Windows client files 93
- Usage
 - CPU 103
 - Disk 103
 - Memory 103
- USB
 - Create a bootable... 22, 88
 - Software 18, 22, 88
- V**
- Version
 - Check 110, 111
- View
 - Services 37
 - Syslog records 108
- View Logs 107
- VNC 123
- Voicemail
 - Auto-start 82
 - Backup/restore 46
 - Start 82
 - Stop 82
- Voicemail IP Address 42
- Voicemail Pro
 - Configuration 40
 - Limitations 15
- Voicemail Pro Client
 - run 44
- Voicemail Pro Client window 44
- Voicemail Pro Login window 44
- Voicemail Pro Server
 - connect 44
- Voicemail Type 42
- VPNM 15
- W**
- WAN 44
- Watchdog 112
- Web browser 15
- Web Control Port 112
- Windows client
 - Repositories 92, 112
- Windows client files
 - Upload files 93
- Windows Clients 124
- Workstation 44

