



IP Office™ Platform 9.1

Using the Avaya IP Office™ Platform
Server Edition Web Control Menus

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.

For full support, please see the complete document, Avaya Support Notices for Hardware Documentation, document number 03-600759.

For full support, please see the complete document, Avaya Support Notices for Software Documentation, document number 03-600758.

To locate this document on our website, simply go to <http://www.avaya.com/support> and search for the document number in the search box.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. 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 its hardware and Software ("Product(s)"). 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: <http://support.avaya.com>. 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. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://SUPPORT.AVAYA.COM/LICENSEINFO) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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. "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.

License type(s)

Designated System(s) License (DS). End User may install and use each copy 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, 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.

Database License (DL). End User may install and use each copy 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 a single instance of the same database.

CPU License (CP). End User may install and use each copy 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 reinstall 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 the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. "Instance" means one unique copy of the Software. 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 that 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"). 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 Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

1. Overview

- 1.1 Using Linux 11
- 1.2 Additional Documentation..... 11
- 1.3 Network Configuration Limitations..... 12
- 1.4 Voicemail Pro Features..... 12
- 1.5 Supported Web Browsers..... 12
- 1.6 Password Authentication (Referred Authentication).... 12

2. Voicemail Pro Configuration

- 2.1 Windows to Linux Voicemail Transfer..... 16

3. Server Maintenance

- 3.1 Logging In..... 19
- 3.2 Logging Into Web Control Directly..... 21
- 3.3 Changing the IP Address Settings..... 22
- 3.4 Starting/Stopping Application Services..... 23
 - 3.4.1 Starting a Service..... 23
 - 3.4.2 Stopping a Service..... 23
 - 3.4.3 Setting a Service to Auto Start..... 23
- 3.5 Changing the Linux Passwords..... 23
- 3.6 Shutting Down the Server..... 24
- 3.7 Rebooting the Server..... 24
- 3.8 Date and Time Settings..... 25
- 3.9 Creating Administrator Accounts..... 26
- 3.10 Setting the Menu Inactivity Timeout..... 26
- 3.11 Upgrading Applications..... 27
 - 3.11.1 Loading Application Files onto the Server..... 27
 - 3.11.2 Upgrading Application Files..... 28
 - 3.11.3 Upgrading Using USB..... 29
- 3.12 Uninstalling an Application..... 32
- 3.13 Setting Up File Repositories..... 33
 - 3.13.1 Source Files..... 33
 - 3.13.2 Setting the Repository Locations..... 33
 - 3.13.3 Uploading Local Files..... 34
 - 3.13.4 Creating Remote Software Repositories..... 35
- 3.14 Using VNC..... 36
 - 3.14.1 Starting the VNC Service..... 36
 - 3.14.2 Viewing the Desktop Via VNC..... 36
 - 3.14.3 Stopping the VNC Service..... 36
- 3.15 Downloading Log Files..... 37

4. Web Manager

- 4.1 Logging In to Web Manager..... 41

5. Web Control/Platform View Menus

- 5.1 System 45
- 5.2 Logs 47
 - 5.2.1 Debug Logs..... 48
 - 5.2.2 Syslog Event Viewer..... 49
 - 5.2.3 Download..... 49
- 5.3 Updates 50
 - 5.3.1 Services..... 51
 - 5.3.2 System..... 52
- 5.4 Settings: General..... 53
 - 5.4.1 Software Repositories..... 54
 - 5.4.2 Syslog..... 54

- 5.4.3 Certificates..... 55
- 5.4.4 Web Control..... 55
- 5.4.5 Backup and Restore..... 55
- 5.4.6 Voicemail Settings..... 56
- 5.4.7 Contact Recorder Settings..... 56
- 5.4.8 ASG Settings..... 56
- 5.4.9 Watchdog..... 57
- 5.4.10 one-X Portal Settings..... 57
- 5.4.11 Set Login Banner..... 57
- 5.5 Settings: System..... 58
 - 5.5.1 Network..... 58
 - 5.5.2 Avaya IP Office LAN Settings..... 59
 - 5.5.3 Date and Time..... 60
 - 5.5.4 Authentication..... 60
 - 5.5.5 Increase Root Partition..... 60
 - 5.5.6 HTTP Server..... 61
 - 5.5.7 Change Root Password..... 61
 - 5.5.8 Change Local Linux Account Password..... 61
 - 5.5.9 Password Rules Settings..... 61
 - 5.5.10 System Identification..... 61
 - 5.5.11 Firewall..... 62
 - 5.5.12 Additional Hardware..... 62
- 5.6 VNC 63
- 5.7 App Center..... 65

6. Document History

- Index71

Chapter 1.

Overview

1. Overview

This document provides details on the web control menus for the IP Office Server Edition application. These menus are accessed using a web browser.

IP Office Server Edition is a networked telephony solution that can consist of multiple servers. Each server can host a number of different applications depending on the server's role; Server Edition Primary Server, Server Edition Secondary Server and Server Edition Expansion System (L).

For IP Office Release 9.0, the web control menus are accessible as part of the Web Manager menus. Refer to the [IP Office Web Manager and IP Office Server Edition documentation](#) ^[17].

The IP Office Server Edition hosts the following applications:

- **Linux**
This is the base operating system used. However, no specific Linux knowledge is required for installation and maintenance.
- **IP Office**
This is a media gateway for voice and video calls using IP (H323 and SIP) trunks and telephones. The application is configured and managed remotely using the IP Office Server Edition Administrator Applications suite (IP Office Manager, System Status Application, System Monitor).
- **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 using web browser access. Each user who wants to use one-X Portal for IP Office needs to be licensed.
- **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. The number of simultaneous connections to voicemail is licensed.
- **IP Office 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. For servers that are part of a Server Edition network, the browseable menus for all the servers in the network are aggregated into one set of menus.
- **Optional Services**
The server can include a number of additional services. Click **Show optional services** to display those services.
 - **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.
 - **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.



1.1 Using Linux

Though the server uses a Linux based operating system, no knowledge or experience of Linux is required. The IP Office Server Edition 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.

1.2 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.
- **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 IP Office 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.
- **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>

1.3 Network Configuration Limitations

The IP Office control unit has two physical LAN interfaces: LAN1 and LAN2. The ports labeled LAN and WAN respectively. Scenarios where users of the one-X Portal for IP Office application are accessing it from the IP Office's other LAN should be avoided for more than 30 users.

They should also be avoided when using NAT on traffic between LAN1 and LAN2. These restrictions apply even for IP Office system is in a Small Community Network.

1.4 Voicemail Pro Features

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

- **VB Scripting**
- **UMS Web Voicemail**
- **3rd Party Database Integration**
- **VPN**

1.5 Supported Web Browsers

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

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

1.6 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 IP Office service running on the IP Office Server Edition. The [Enable referred authentication](#) ⁽⁶⁰⁾ setting controls the method used.

- **Enabled**
With referred authentication enabled, the security settings of the IP Office service running on the IP Office Server Edition 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.

Voicemail Pro Configuration

2. 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](#)^[11]. 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

b. Voicemail Pro Configuration

i. Install the Voicemail Pro client

ii. Log in to the Voicemail Pro server

iii. Change the voicemail server password

2.1 Windows to Linux Voicemail Transfer

You can transfer a set of Voicemail Pro backup files from a Windows based voicemail server to a Linux based voicemail server.

1. On the Windows voicemail server:
 - a. Using the Voicemail Pro client, perform an immediate backup on the Windows voicemail server, selecting to backup all types of file.
 - b. This will create a backup folder, the name of which includes the date and time of the backup and Immediate. For example **VMPro_Backup_26012011124108_Immediate**. The default path for such folders is **C:\Program Files\Avaya\IP Office\Voicemail Pro\Backup\Scheduled**.
 - c. Within Windows, locate the folder just created by the backup and copy the folder to the PC with your SSH file transfer tool.
2. Connect to the server using a SSH File transfer tool.
3. Copy the Windows backup folder into the folder **/opt/vmpro/Backup/Scheduled/OtherBackups**.
4. Using a web browser, [login](#) to the IP Office Server Edition.
5. Select **Settings**.
6. 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.
7. Click **OK**.

If you do not allow remote SSH access to the server, you can transfer files from the CD/DVD drive. This requires mounting the contents of the CD or DVD as part of the folder structure.

1. Create a CD or DVD with the Windows backup folder on it.
2. Login on the server as the root user.
3. Enter **eject -n**.
4. The response will be something like **eject: device is '/dev/hda'**.
5. Enter mount **/dev/hda/mnt/cdrom**.
6. The contents of the drive are now accessible as part of the file structure in the folder **/mnt/cdrom**.
7. Copy the backup folder from **/mnt/cdrom** to **/opt/vmpro/Backup/Scheduled/OtherBackups**. For example:
 - `cp -a -f /mnt/cdrom/VMPro_Backup_26012011124108_Immediate /opt/vmpro/Backup/Scheduled/OtherBackups`
8. The backup can now be restored using the web client.

Chapter 3.

Server Maintenance

3. 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.

For IP Office Release 9.1, the web control menus (also called "platform view" or "web control panel (WCP)") are a sub-component of the server's [Web Manager](#)^[40] menus through which they can be accessed.

- [Accessing the Web Control Menus](#)^[19]
- [Logging in Directly](#)^[21]
- [Starting/Stopping Application Services](#)^[23]
- [Changing the Linux Passwords](#)^[23]
- [Changing the IP Address Settings](#)^[22]
- [Server Shutdown](#)^[24]
- [Rebooting the Server](#)^[24]
- [Date and Time Settings](#)^[25]
- [Creating Administrator Accounts](#)^[26]
- [Setting the Menu Inactivity Timeout](#)^[26]
- [Upgrading an Application](#)^[27]
- [Uninstalling an Application](#)^[32]
- [Setting Up File Repositories](#)^[33]
- [Using VNC](#)^[36]
- [Downloading Log Files](#)^[37]

3.1 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.**
- **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 IP Office passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. 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 IP Office service run on the IP Office Server Edition. With [Referred Authentication](#) ⁽¹²⁾ 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**

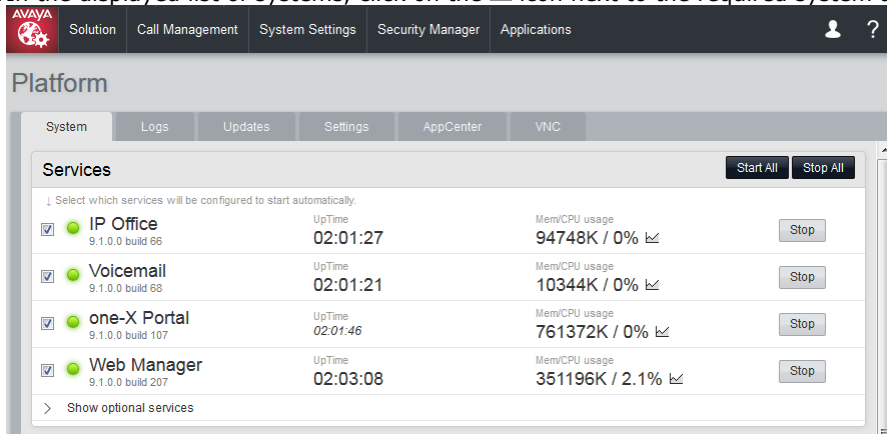
This sets the password for the IP Office security administrator account.

- **Change System Password**

This sets the **System** password for the IP Office.

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 displays the Avaya Platform Server Edition Web Control Menus interface. At the top, there is a navigation bar with the Avaya logo and several menu items: Solution, Call Management, System Settings, Security Manager, and Applications. Below the navigation bar, the main content area is titled "Platform" and contains a sub-menu with options: System, Logs, Updates, Settings, AppCenter, and VNC. The "Services" section is active, showing a list of services that can be configured to start automatically. Each service entry includes a checkbox, the service name, its version/build number, up-time, and memory/CPU usage. A "Stop" button is provided for each service. At the top right of the Services section, there are "Start All" and "Stop All" buttons. Below the list, there is a link to "Show optional services".

Service Name	Version/Build	UpTime	Mem/CPU usage	Action
<input checked="" type="checkbox"/> IP Office	9.1.0.0 build 66	02:01:27	94748K / 0%	Stop
<input checked="" type="checkbox"/> Voicemail	9.1.0.0 build 68	02:01:21	10344K / 0%	Stop
<input checked="" type="checkbox"/> one-X Portal	9.1.0.0 build 107	02:01:46	761372K / 0%	Stop
<input checked="" type="checkbox"/> Web Manager	9.1.0.0 build 207	02:03:08	351196K / 2.1%	Stop

3.2 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](#)^[19] 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.**
- **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.
2. Select the **Language** required.



IP Office Server Edition R9.1

Please log on.

Logon:

Password:

Language: English

© 2014 Avaya Inc. All rights reserved - [View EULA](#)

3. Enter the name and password for server administration.
4. If the login is successful, the server's [System](#)^[45] page appears.

3.3 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](#) ^[19] 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.

- **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.

- **Host Name**

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

- **! WARNING**

For a virtualized server, shown by the **Virtualized** value on the [System](#) ^[45] menu, this field is part of the **System Identification (SID)** used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

- **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.

- **IP Address**

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

- **! WARNING**

For a virtualized server, shown by the **Virtualized** value on the [System](#) ^[45] menu, this field is part of the **System Identification (SID)** used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

- **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.

3.4 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.

3.4.1 Starting a Service

To start a service:

1. [Login](#) 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.

3.4.2 Stopping a Service

To stop a service:

1. [Login](#) 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**.

3.4.3 Setting a Service to Auto Start

To set a service to auto start:

1. [Login](#) 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.

3.5 Changing the Linux Passwords

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

To change the server's Linux account passwords:

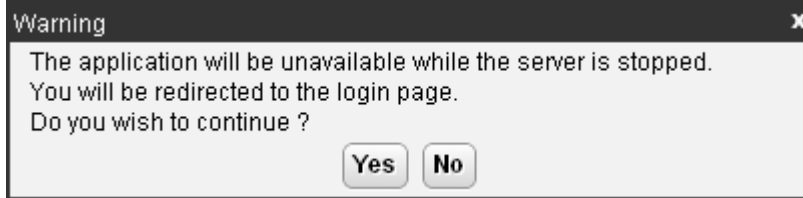
1. [Login](#) to the server's web configuration menus.
2. Select **Settings** and click on the **System** tab.
3. Use the **Change root Password** section to set the new password for the root account. The new password must conform to the [password rules settings](#).
4. Use the **Change Local Linux Account 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](#).
5. Click **Save**.

3.6 Shutting Down the Server

Use this process when it is necessary to switch off the IP Office Server Edition 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](#) ^[19] to the server's web configuration menus.
2. After logging in, select the [System](#) ^[45] page.
3. Click on **Shutdown**. The menu prompts you to confirm the action.



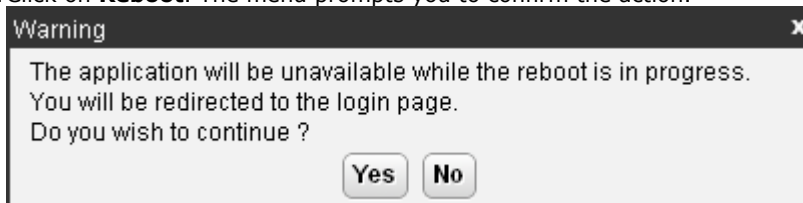
4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 2 minutes, the server shuts down.
7. Switch off power to the server.

3.7 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](#) ^[23] automatically restart after the reboot.

To reboot the server:

1. [Login](#) ^[19] to the server's web configuration menus.
2. After logging in, select the [System](#) ^[45] 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**.

3.8 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, shown by the **Virtualized** value on the [System](#) menu, this field is part of the **System Identification (SID)** used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.
 - **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.
5. Click **Save**.



3.9 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. Also allows access to the VNC menu.

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. Also allows access to the VNC menu.
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.

3.10 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.

3.11 Upgrading Applications

The preferred method for upgrading servers and server applications is to use the [Web Manager menus](#)^[40]. 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](#)^[33].

Once an .rpm file or files are available, the IP Office Server Edition 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](#)^[41].
- **! 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 Server Edition.

3.11.1 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](#)^[35].

- **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](#)^[19] 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](#)^[33] 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.

3.11.2 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	Current Version	Latest Available	Status	Actions			
apache-tomcat	7.0.0.32 build 10	7.0.0.32 build 10	up to date	Change Version Update Uninstall			
AvayaSystemConfig	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall			
AvayaVersioning	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall			
cli	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall			
cli-commands	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall			
imvirt	0.9.0.0 build 3	0.9.0.0 build 3	up to date	Change Version Update Uninstall			
ipphonebin	9.0.0.10 build 5519	9.0.0.10 build 5519	up to date	Change Version Update Uninstall			
jre	1.6.0_31.fcs	1.6.0_31.fcs	up to date	Change Version Update Uninstall			
ms	9.0.0.0 build 150	9.0.0.0 build 160	out of date	Change Version Update Uninstall			
one-X Portal	9.0.0.0 build 209	9.0.0.0 build 209	up to date	Change Version Update Uninstall			
oneXportal-config	-	9.0.0.0 build 160	not installed	Change Version Update Install			
TTSEnglish	7.0.0.25 build 1	7.0.0.25 build 1	up to 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**.

3.11.3 Upgrading Using USB

Upgrading the IP Office Server Edition through the use of [RPM or ZIP files is recommended](#)^[27]. However, if necessary, you can use a USB memory key to perform an upgrade.

3.11.3.1 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](#)^[41].

Prerequisites

- **4GB USB Memory Key**

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

- **Rufus software**

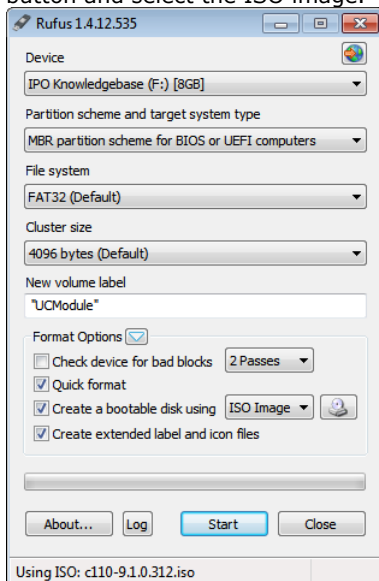
This additional software is downloadable from <https://rufus.akeo.ie>. You use it to load an ISO image onto a USB memory key from which the server can boot and run that ISO image.

- **Server Edition ISO Image**

You can download this software from the Avaya support website (<http://support.avaya.com>).

To create a bootable USB memory key:

1. Start the Rufus application
2. Under **Device**, select your USB device if not already selected.
3. Under **Partition scheme and target system type** select the **MBR partition scheme for BIOS or UEFI computers** option.
4. Under **File system** select **FAT32**.
5. Under **Cluster size** select **4096 bytes**.
6. Select **Create a bootable disk using** and select **ISO Image** from the drop-down list. Click on the adjacent button and select the ISO image.



7. Click **Start**.
8. When done, click **Close**.

- **! Important: Copy the Upgrade Files**

You must copy a number of files to a new location on the USB memory key.

-
- a. Using the file explorer, open the **USB** folder on the USB memory key. This folder contains 4 files, some of which are used for installation and other are used for upgrading.
 - b. Select just the files **syslinux.cfg** and **avaya_autoupgrade.conf**. Copy those two files to the top level (root) of the USB memory key, overwriting any existing files with those names.
8. Remove the USB memory key from the PC.

3.11.3.2 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](#)^[41].

To upgrade from a USB memory key:

1. Prepare a bootable USB upgrade key. See [Preparing a USB Upgrade Key](#)^[29].
2. Insert the USB upgrade key into a USB socket and [reboot the server](#)^[24].
3. Follow the same process as for Software Installation. However, when the upgrade menu appears, select **Upgrade** rather than **Install**.

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

Services				Check Now	Clear Local Cache	Update All
Application	Current Version	Latest Available	Status	Actions		
apache-tomcat	7.0.0.32 build 10	7.0.0.32 build 10	up to date	Change Version	Update	Uninstall
AvayaSystemConfig	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall
AvayaVersioning	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall
cli	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall
cli-commands	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall
imvirt	0.9.0.0 build 3	0.9.0.0 build 3	up to date	Change Version	Update	Uninstall
ipphonebin	9.0.0.10 build 5519	9.0.0.10 build 5519	up to date	Change Version	Update	Uninstall
jre	1.6.0_31.fcs	1.6.0_31.fcs	up to date	Change Version	Update	Uninstall
ms	9.0.0.0 build 150	9.0.0.0 build 160	out of date	Change Version	Update	Uninstall
one-X Portal	9.0.0.0 build 209	9.0.0.0 build 209	up to date	Change Version	Update	Uninstall
oneXportal-config	-	9.0.0.0 build 160	not installed	Change Version	Update	Install
TTSEnglish	7.0.0.25 build 1	7.0.0.25 build 1	up to 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](#), 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.

3.13 Setting Up File Repositories

The [Updates](#)^[50] and [Web Client](#)^[65] 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.

3.13.1 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 Server Edition 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](#)^[41].

		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^[65] 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.

3.13.2 Setting the Repository Locations

The IP Office Server Edition 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](#)^[50] and [AppCenter](#)^[65] 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](#)^[35]. 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 Server Edition) 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.

3.13.3 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](#)^[65] menu.
- **Operating System**
These are files used by the Linux operating system and its services.

3.13.3.1 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](#)^[35].

- **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](#)^[19] 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](#)^[33] 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.

3.13.3.2 Uploading Operating System Files

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

To upload operating system files:

1. [Login](#)^[19] 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](#)^[33] 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.

3.13.3.3 Uploading Windows Client Files

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

To upload Windows client files:

1. [Login](#)^[19] 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](#)^[33] 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.

3.13.4 Creating Remote Software Repositories

Alternatively to using [local files uploaded to the server](#)^[27] 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](#)^[33] 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 Server Edition 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 Server Edition 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.

3.14 Using VNC

Through the web control menus, you can start a virtual network connection (VNC) service. That service can then be used to view the server's graphical desktop, either through the web control menus or using a separate third-party VNC client such as TigerVNC.

- 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".

The process of using establishing the VNC connection divides into 2 parts.

1. [Starting the VNC service](#) ^[36].
2. [Viewing the desktop via VNC](#) ^[36].

3.14.1 Starting the VNC Service

Before using the VNC connection to the server desktop, the VNC service on the server needs to be started.

To start the VNC service:

1. Login and select the **VNC** tab.
2. Select **Settings**.
 - a. Enter the administrator password.
 - b. If planning to use a separate VNC client, note the port number setting.
3. Click **Apply**.
4. Click **Start VNC**.

3.14.2 Viewing the Desktop Via VNC

Once the VNC server has been started, you can use the web control menus as a VNC client to view the server's graphical desktop.

- **Java Required**
The VNC option requires your PC to have Java installed and your browser configured to allow use of Java.

To view the server desktop:

1. Login and select the **VNC** tab.
2. Select **Settings**.
3. Check that the **Start VNC** button is greyed out. That indicates that the VNC service is running. If the button is not greyed out, see [Starting the VNC Service](#) ^[36].
4. Select the **View** tab.
5. Enter the password. This must match the password that was used to start the VNC service.
6. Click **OK**.
7. The server desktop appears.
8. To end the connection at any time, click **Disconnect**.

3.14.3 Stopping the VNC Service

Before using the VNC connection to the server desktop, the VNC service on the server needs to be started.

To stop the VNC service:

1. Login and select the **VNC** tab.
2. Select **Settings**.
3. Click **Stop VNC**.

3.15 Downloading Log Files

The server collects and store log events. These are viewable through the [Logs](#)^[47] sub-menus. The [Download](#)^[49] sub-menu allows the archiving and download of the log files.

To create archive files:

1. [Login](#)^[19] 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 4.

Web Manager

4. 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](#)^[14].

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](#)^[41].

- **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.

4.1 Logging In to Web Manager

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

- **Microsoft Internet Explorer 10 and 11.**
- **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 IP Office passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. 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 IP Office service run on the IP Office Server Edition. With [Referred Authentication](#) ¹² 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**

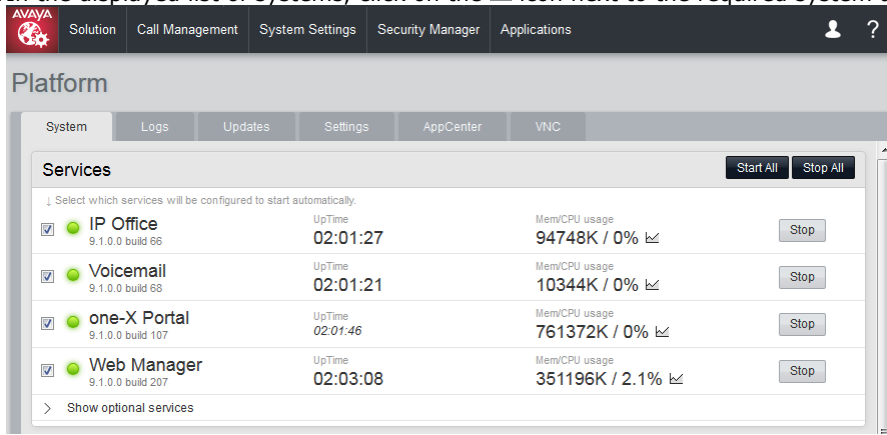
This sets the password for the IP Office security administrator account.

- **Change System Password**

This sets the **System** password for the IP Office.

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 Server Edition Web Control Menus interface. The top navigation bar includes the Avaya logo and menu items: Solution, Call Management, System Settings, Security Manager, and Applications. The main header is labeled "Platform". Below this, there are tabs for System, Logs, Updates, Settings, AppCenter, and VNC. The "Services" section is active, displaying a list of services with their status, uptime, and memory/CPU usage. Each service has a "Stop" button. A "Start All" button is also present at the top right of the services list.

Service Name	Version	Uptime	Mem/CPU usage	Action
<input checked="" type="checkbox"/> IP Office	9.1.0.0 build 66	02:01:27	94748K / 0%	Stop
<input checked="" type="checkbox"/> Voicemail	9.1.0.0 build 68	02:01:21	10344K / 0%	Stop
<input checked="" type="checkbox"/> one-X Portal	9.1.0.0 build 107	02:01:46	761372K / 0%	Stop
<input checked="" type="checkbox"/> Web Manager	9.1.0.0 build 207	02:03:08	351196K / 2.1%	Stop

> Show optional services

Chapter 5.

Web Control/Platform View Menus

5. Web Control/Platform View Menus

The IP Office Server Edition 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](#)^[48]
This menu gives an overview of the status of the applications hosted on the server.
- [Logs](#)^[48]
This menu has sub-menus for viewing and managing log records and log files.
 - [Debug Logs](#)^[48]
View the current log files for the server and the application services hosted by the server.
 - [Syslog Event Viewer](#)^[49]
View Syslog log records received and or generated by the server.
 - [Download](#)^[49]
Create and download archive files of existing log records.
- [Updates](#)^[50]
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](#)^[53]
General server settings such as the locations of software update repositories.
 - [System](#)^[58]
View and manage the server setting for date, time and IP address details.
- [AppCenter](#)^[65]
You can download the installation packages for applications such as the Voicemail Pro client application from this page.
- [VNC](#)^[63]
This menu allows you to launch VNC connection to the server desktop.

5.1 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
Linux Downloads
VNC

Services

Start All Stop All

↓ Select which services will be configured to start automatically.

<input checked="" type="checkbox"/>	● IP Office 9.1.0.0 build 66	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% ⌵	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

Notifications

There are no notifications available

System

Shutdown Reboot

Usage ↑

Time →

Memory Usage

used (1647.62MB)
free (220.48MB)

Disk Usage

used (16569.04MB)
free (57010.1MB)

OS: Linux release 6.6 (Final)

Kernel Version: 2.6.32-358.23.2.el6.x86_64

UpTime: 52 minutes

Server Time: 09:15

Average CPU Load: 0.93 (1min), 0.60 (5min), 0.43 (15min)

Processor: Intel(R) Pentium(R) 4 CPU 3.20GHz

Speed: 3.1GHz

Cores: 2

Hard Disk Size: 71.8G

RAM: 1.8G

Disk RAID Levels: -

Disk Array Types: -

Quota available for backup data: None

Virtualized: No

Last Successful Logon: 2014-08-13 13:57:01

Unsuccessful Logon Attempts: 0

- **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.

- **IP Office**

This is a media gateway for voice and video calls using IP (H323 and SIP) trunks and telephones. The application is configured and managed remotely using the IP Office Server Edition Administrator Applications suite (IP Office Manager, System Status Application, System Monitor).

- **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 using web browser access. Each user who wants to use one-X Portal for IP Office needs to be licensed.

- **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. The number of simultaneous connections to voicemail is licensed.

- **IP Office 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. For servers that are part of a Server Edition network, the browseable menus for all the servers in the network are aggregated into one set of menus.

Using the Avaya IP Office™ Platform Server Edition Web Control Menus
IP Office™ Platform 9.1

Page 45
15-601011 Issue 10ab (19 January 2016)

- **Optional Services**

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

- **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.

- **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.

- **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.

- **Material Code:**

This field shows the material code for Avaya supplied servers. Avaya uses this code as part of the system registration with the Avaya Global Registration Tool (GRT).

- **Model Info:**

This field shows the model information for an Avaya supplied server.

- **System Manufacturer Serial No:**

This field shows the manufacturer's serial number for the server.

- **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.

5.2 Logs

This menu contains the following sub-menus:

- [Debug Logs](#) ⁴⁸
View the current log files for the server and the application services hosted by the server.
- [Syslog Event Viewer](#) ⁴⁹
View Syslog log records received and or generated by the server.
- [Download](#) ⁴⁹
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
2013-03-11 15:54:17	Administrator	logged in
2013-03-11 15:52:51	Administrator	logged out
2013-03-11 15:43:07	Administrator	logged in
2013-03-11 15:32:02	Administrator	logged out
2013-03-11 15:31:48	Administrator	set one-X Portal address to <148.147.170.168>
2013-03-11 15:31:11	Administrator	change autostart state for one-X Portal to off
2013-03-11 15:30:40	Administrator	install one-X Portal version 9.0.0.209
2013-03-11 15:29:44	Administrator	logged in
2013-03-11 15:27:29	Administrator	upload file to apps repository
2013-03-11 15:27:22	Administrator	upload file to apps repository

5.2.1 Debug Logs

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

The screenshot displays the 'Debug Logs' interface. At the top, there are navigation tabs: System, Logs, Updates, Settings, and AppCenter. Below these, there are sub-tabs: Debug Logs, Syslog Event Viewer, and Download. The main content area is divided into two sections: 'Application Log' and 'Audit Log'.

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
2013-03-11 15:54:17	Administrator	logged in
2013-03-11 15:52:51	Administrator	logged out
2013-03-11 15:43:07	Administrator	logged in
2013-03-11 15:32:02	Administrator	logged out
2013-03-11 15:31:48	Administrator	set one-X Portal address to <148.147.170.168>
2013-03-11 15:31:11	Administrator	change autostart state for one-X Portal to off
2013-03-11 15:30:40	Administrator	install one-X Portal version 9.0.0.209
2013-03-11 15:29:44	Administrator	logged in
2013-03-11 15:27:29	Administrator	upload file to apps repository
2013-03-11 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](#) 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 Server Edition menus.

- ### Audit Log

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

5.2.2 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. For example, in a Server Edition network, by default the Server Edition Secondary Server is configured to send its Syslog records to the Server Edition Primary Server.

You can use the [Settings | General](#) ^[54] 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.

Syslog Events

Host: All | Event Type: All | View: All | Tag: All | Refresh

Date	Host	Type	Tag	Message
2013-03-11 15:57:56	ServerEdition	SEC	Operating System	Administrator : TTY=unknown ; PWD=/opt/webcontrol ; USER=root ; COMMAND=/bin/chmod -R 777 /var/log/rsyslog/
2013-03-11 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'
2013-03-11 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'
2013-03-11 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'
2013-03-11 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 settings in the drop-down filters (**Host**, **Event Type**, **View** and **Tag**). Note however that the options within the filters are set when the menu is opened. To update the menu 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.

5.2.3 Download

You can access this menu by selecting **Logs** and then clicking the **Download** tab. You can use the menu to [create and download archives files](#) ^[37]. 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.

Debug Files | Select All | Create Archive | Delete Selected

There is no data available

There are no core dump files available.

Logs | Select All | Create Archive | Delete Selected

Name	Last Modified	Size	Delete
webmanagement_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:33	1019K	<input type="checkbox"/>
system_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:32	54.3K	<input type="checkbox"/>
webcontrol_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	287.3K	<input type="checkbox"/>
ipoffice_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	104.4K	<input type="checkbox"/>
voicemail_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	930K	<input type="checkbox"/>
install_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	10.2K	<input type="checkbox"/>
onex_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	1.1K	<input type="checkbox"/>

5.3 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](#) ⁵³ page.

System
Logs
⚠ Updates
Settings
AppCenter

System

Check Now
Review Updates
Update All

OS	Version	Kernel Version	Last Update	Status
Linux	release 6.4 (Final)	2.6.32-279.22.1.el6.x86_64	-	up to date

Services

Check Now
Clear Local Cache
Update All

Application	Current Version	Latest Available	Status	Actions
apache-tomcat	7.0.0.32 build 10	7.0.0.32 build 10	up to date	Change Version Update Uninstall
AvayaSystemConfig	9.1.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall
AvayaVersioning	9.1.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall
cli	9.1.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall
cli-commands	9.1.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall
imvirt	0.9.0.0 build 3	0.9.0.0 build 3	up to date	Change Version Update Uninstall
IP Office	9.1.0.0 build 160	9.0.0.0 build 160	up to date	Change Version Update Uninstall
ipphonebin	9.1.0.10 build 5519	9.0.0.10 build 5519	up to date	Change Version Update Uninstall
jre	1.6.0_31.fcs	1.6.0_31.fcs	up to date	Change Version Update Uninstall
ms	9.1.0.0 build 150	9.0.0.0 build 160	out of date	Change Version Update Uninstall
one-X Portal	9.1.0.0 build 209	9.0.0.0 build 209	up to date	Change Version Update Uninstall
oneXportal-config	-	9.0.0.0 build 160	not installed	Change Version Update Install
TTSEnglish	7.0.0.25 build 1	7.0.0.25 build 1	up to date	Change Version Update Uninstall

The menu consists of 2 sections:

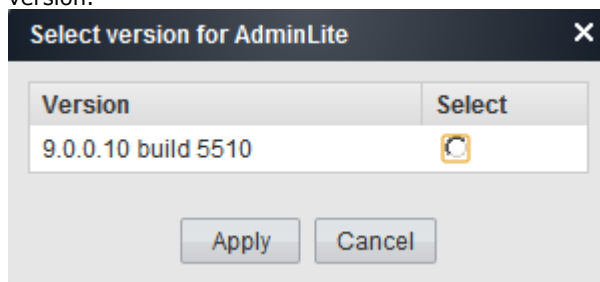
- [Services](#) ⁵¹
This section displays the current version of application files. It also shows whether update files are available.
- [System](#) ⁵²
This section displays the current version of the operating system and whether update files are available.

5.3.1 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	Current Version	Latest Available	Status	Actions			
apache-tomcat	7.0.0.32 build 10	7.0.0.32 build 10	up to date	Change Version	Update	Uninstall	
AvayaSystemConfig	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall	
AvayaVersioning	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall	
cli	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall	
cli-commands	9.0.0.0 build 160	9.0.0.0 build 160	up to date	Change Version	Update	Uninstall	
imvirt	0.9.0.0 build 3	0.9.0.0 build 3	up to date	Change Version	Update	Uninstall	
ipphonebin	9.0.0.10 build 5519	9.0.0.10 build 5519	up to date	Change Version	Update	Uninstall	
jre	1.6.0_31.fcs	1.6.0_31.fcs	up to date	Change Version	Update	Uninstall	
ms	9.0.0.0 build 150	9.0.0.0 build 160	out of date	Change Version	Update	Uninstall	
one-X Portal	9.0.0.0 build 209	9.0.0.0 build 209	up to date	Change Version	Update	Uninstall	
oneXportal-config	-	9.0.0.0 build 160	not installed	Change Version	Update	Install	
TTSEnglish	7.0.0.25 build 1	7.0.0.25 build 1	up to 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](#)^[33]. 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](#)^[33] 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](#)^[33].
- **Uninstall**
Clicking on this button uninstalls the selected application.
 - If there are installation files for the application in the application [file repository](#)^[33], 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 Server Edition 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.

5.3.2 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 6.3 (Final)	2.6.32-279.22.1.el6.x86_64	-	up to date			

- **Check Now**

Clicking this button makes the IP Office Server Edition 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.

The screenshot shows a window titled "System Updates" with a table of updates. Each row has a checkbox in the "Select" column, the update name in the "Name" column, and the version in the "Version" column. At the bottom of the window are four buttons: "Select All", "Unselect All", "Apply Selected Updates", and "Cancel".

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

- **Update All**

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

5.4 Settings: General

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

System	Logs	Updates	Settings	AppCenter	Linux Downloads	VNC
<div style="display: flex; justify-content: space-around;"> General System </div>						
Software Repositories	Operating System: <input checked="" type="checkbox"/> Local — File: <input type="text"/> Browse Add Applications: <input checked="" type="checkbox"/> Local — File: <input type="text"/> Browse Add Downloads: <input checked="" type="checkbox"/> Local — File: <input type="text"/> Browse Add					Save
Syslog	Log files age (days) General log files: <input type="text" value="1"/> Security log files: <input type="text" value="1"/> Audit log files: <input type="text" value="1"/> Operational log files: <input type="text" value="1"/> Debug log files: <input type="text" value="1"/> <input type="checkbox"/> Apply general settings to all file types <hr/> Max log size (MB) General log files: <input type="text" value="29"/> Security log files: <input type="text" value="29"/> Audit log files: <input type="text" value="29"/> Operational log files: <input type="text" value="29"/> Debug log files: <input type="text" value="29"/> <input type="checkbox"/> Apply general settings to all file types <hr/> Receiver Settings <input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> TCP Port: <input type="text" value="514"/> <input checked="" type="checkbox"/> TLS Port: <input type="text" value="6514"/> <input checked="" type="checkbox"/> UDP Port: <input type="text" value="514"/> <input checked="" type="checkbox"/> Forwarding Destination 1 <input checked="" type="radio"/> TCP <input type="radio"/> TLS <input type="radio"/> UDP IP Address:Port = <input type="text"/> : <input type="text" value="514"/> <input type="checkbox"/> Forwarding Destination 2 <hr/> Select Log Sources <input checked="" type="checkbox"/> Authentication and authorization privileges <input checked="" type="checkbox"/> Information stored by the Linux audit daemon (auditd) <input checked="" type="checkbox"/> NNTP(News)/UUCP(Usenet) protocols <input checked="" type="checkbox"/> Apache web server access_log and error_log					Save
Certificates	Certified Authority Settings <input checked="" type="radio"/> Create CA <input type="radio"/> Import CA Generate Download (PEM-encoded) Download (DER-encoded) <hr/> Certificate Settings <input checked="" type="checkbox"/> Renew automatically Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page. <input checked="" type="checkbox"/> Create certificate for a different machine Machine IP: <input type="text"/> Password: <input type="text"/> Confirm Password: <input type="text"/> Subject Name: <input type="text" value="iposever-00:01:6c:ef:7d:0e.avaya.com"/> Subject Alternative Name(s): <input type="text" value="DNS:iposever-00:01:6c:ef:7d:0e.avaya.com, IP:192.168.0.214"/> Duration (days): <input type="text" value="2555"/> Public Key Algorithm: <input type="text" value="RSA-2048"/> Secure Hash Algorithm: <input type="text" value="SHA-256"/> Password complexity requirements: • Minimum password length: 8 • Minimum number of uppercase characters: 1 • Minimum number of lowercase characters: 1 • Maximum allowed sequence length: 4 Generate Apply Download (PEM-encoded) Download (DER-encoded)					Save
Web Control	Inactivity timeout: <input type="text" value="1 hour"/>					Save
Backup and Restore	IP Office: Backup Restore Voicemail: Backup Restore WebRTC Gateway: Backup Restore					Save
Voicemail Settings	Debug level: <input type="text" value="Information"/>					Save
Contact Recorder Settings	Debug level: <input type="text" value="Information"/>					Save
ASG Settings	Status: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="radio"/> Dormant Port: <input type="text" value="2222"/> Service Listening: <input type="text" value="Any Tunnel"/> AFS Id: <input type="text"/> Import AFS file: <input type="text"/> Browse Upload					Save
Watchdog	Log files age (days): <input type="text" value="5"/>					Save
Set Login Banner	<input type="text" value="Server Edition 212"/>					Save
one-X Portal Settings	<input checked="" type="checkbox"/> Use Local IP					Save

5.4.1 Software Repositories

The IP Office Server Edition 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](#) ^[50] and [AppCenter](#) ^[65] 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](#) ^[38]. 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 Server Edition) 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.

5.4.2 Syslog

These settings control the receiving and the forwarding of Syslog records by the server. These options are not shown for a Server Edition Expansion System (L).

- **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**. This setting is not applied to IP Office System Monitor records sent to Syslog.
 - **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**. This setting is not applied to IP Office System Monitor records sent to Syslog.
 - **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**

5.4.3 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. These menus are not available on Server Edition Secondary Server and Server Edition Expansion System (L) servers.

- **Create new**
If selected, the server generates its own security certificate.
- **Renew existing**
If selected, the server's current self-generated security certificate is renewed.
- **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.
- **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.
- **Generate and Apply**
When clicked, the server generates a new security certificate. 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 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.

5.4.4 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**.

5.4.5 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.

- **IP Office**
These control provides options to backup/restore the configuration settings of the IP Office 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 the 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.

5.4.6 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](#) ⁴⁹ 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**.

5.4.7 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**.

5.4.8 ASG Settings

The server uses these settings for connection from an Avaya Access Security Gateway. This Avaya service performs regular security and performance diagnostics against supported servers. You can import the required settings using an AFS file obtained from <https://rfa.avaya.com>.

- **Status**

Set the status of server listening for connections from the security gateway.

- **Active**

This setting enables listening for connections from an ASG server. The server automatically selects this state when you upload an AFS file.

- **Disabled**

This setting cancels any listening for connections from an ASG server.

- **Dormant**

This is the default state before uploading any AFS file.

- **Port**

Set the port on which the server listens for connections from the security gateway. The default is **2222**. For Avaya support do not change this value from the default.

- **Service Listening**

Select whether the server listens on any connection (**Any**) or just on SSLVPN 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.

- **AFS ID**

The server shows the ID after uploading an AFS file.

- **Import AFS file**

Use this control to upload settings and encryption keys provided in the form of an AFS file. Click **Browse** and select the file to upload. Then click **Upload**. Uploading a file sets the AFS ID and changes the **Status** to **Active**.

- **Reset ASG**

Clicking this button defaults the ASG settings and erases those imported from the AFS file.

5.4.9 Watchdog

- **Log files age (days)**

Sets the number of days that log file records are retained. This does not affect log file [archives](#)^[49]. Not applied to one-X Portal for IP Office.

5.4.10 one-X Portal Settings

The location of the one-X Portal for IP Office server, normally running on the Server Edition Primary Server, is required by other applications in the Server Edition network.

- **Use Local IP**

Select this option if the Server Edition Primary Server is hosting the one-X Portal for IP Office application. If not selected, the IP address of the server hosting the one-X Portal for IP Office must be indicated in the **Remote IP** field below.

- **Remote IP**

If **Use Local IP** is not selected, this field sets the IP address of the server hosting the one-X Portal for IP Office application.

5.4.11 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.

5.5 Settings: System

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

System	Logs	Updates	Settings	AppCenter	Linux Downloads	VNC
<div style="display: flex; justify-content: space-around;"> General System </div>						
Network	Network Interface: <input type="text" value="eth0"/> Create Subinterface Delete Subinterface					Save
Host Name: <input type="text" value="ServerEdition"/>						
<input type="checkbox"/> Use DHCP						
IP Address: <input type="text" value="148.147.170.200"/>						
Subnet Mask: <input type="text" value="255.255.255.0"/>						
Default Gateway: <input type="text" value="148.147.170.1"/>						
System DNS: <input type="text"/>						
<input type="checkbox"/> Automatically obtain DNS from provider						
Avaya IP Office LAN Settings	Avaya IP Office LAN1 <input type="checkbox"/> Enable traffic control Network Interface: <input type="text" value="eth0"/> Save					Save
Avaya IP Office LAN2 <input type="checkbox"/> Enable traffic control Network Interface: <input type="text" value="eth1"/> Save						
Date and Time	Date / Time: <input type="text" value="2013-07-05"/> / <input type="text" value="13"/> : <input type="text" value="38"/>					Save
Timezone: <input type="text" value="Europe/London"/>						
<input checked="" type="checkbox"/> Enable Network Time Protocol						
NTP Servers: <input type="text" value="0.pool.ntp.org"/>						
Authentication	<input checked="" type="checkbox"/> Enable referred authentication					Save
HTTP Server	<input checked="" type="checkbox"/> Enable HTTP file store for backup/restore					Save
Change root Password	New Password: <input type="text"/>					Save
Confirm New Password: <input type="text"/>						
Password complexity requirements: <ul style="list-style-type: none"> • Minimum password length: 8 • Minimum number of uppercase characters: 1 • Minimum number of lowercase characters: 1 • Maximum allowed sequence length: 4 						
Change Local Linux Account Password	Account Name: <input type="text" value="Administrator"/>					Save
New Password: <input type="text"/>						
Confirm New Password: <input type="text"/>						
Password complexity requirements: <ul style="list-style-type: none"> • Minimum password length: 8 • Minimum number of uppercase characters: 1 • Minimum number of lowercase characters: 1 • Maximum allowed sequence length: 4 						
Password Rules Settings	<input type="text" value="8"/> Minimum password length					Save
<input type="text" value="1"/> Minimum number of uppercase characters						
<input type="text" value="1"/> Minimum number of lowercase characters						
<input type="text" value="0"/> Minimum number of numeric characters						
<input type="text" value="0"/> Minimum number of special characters						
<input type="checkbox"/> Allow character sequences						
<input type="text" value="4"/> Maximum allowed sequence length						
System Identification	System ID (SID): d03f26657c60fdff488bc31627ae66945ecc3ad0 Licensing Mode: Internal					Save
Firewall Settings	Status: on <input checked="" type="checkbox"/> Activate <input type="checkbox"/> Enable filtering					Save
Enable TCP ports <input checked="" type="checkbox"/> 21 <input checked="" type="checkbox"/> 80 <input checked="" type="checkbox"/> 8000 <input checked="" type="checkbox"/> 8069 <input checked="" type="checkbox"/> 8080 <input checked="" type="checkbox"/> 9080						
Enable UDP ports <input checked="" type="checkbox"/> 69						
<input type="text" value="0"/> Minimum number of special characters						
<input type="checkbox"/> Allow character sequences						
<input type="text" value="4"/> Maximum allowed sequence length						
Additional Hardware Settings	Additional Hardware Info Name: /dev/sdb Vendor: VMware Product: Virtual disk User Capacity: 268,435,456,000 bytes [268 GB] Device Type: disk Mount Point Path: <input type="text" value="/additional-hdd#1"/>					Save
<input checked="" type="checkbox"/> Activate						

5.5.1 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.

- **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.

- **Host Name**

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

- ! WARNING**
 For a virtualized server, shown by the **Virtualized** value on the [System](#) ⁴⁵ menu, this field is part of the **System Identification (SID)** used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.
- 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.
- IP Address**
 Displays the IP address set for the server. If not using DHCP, you can edit the field to change the setting.
 - ! WARNING**
 For a virtualized server, shown by the **Virtualized** value on the [System](#) ⁴⁵ menu, this field is part of the **System Identification (SID)** used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.
- 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.

5.5.2 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**
 Select whether the web control menus should be used to adjust the IP Office LAN settings.
 - 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.

5.5.3 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, shown by the **Virtualized** value on the [System](#) ^[45] menu, this field is part of the **System Identification (SID)** used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.
- **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.

5.5.4 Authentication

- **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 IP Office service running on the IP Office Server Edition. See [Password Authentication](#) ^[12]. This setting controls which method is used.
 - **Enabled**
With referred authentication enabled, the security settings of the IP Office service running on the IP Office Server Edition 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.

5.5.5 Increase Root Partition

This menu is shown for virtualized servers. It allows the size of the virtual machines primary disk to be increased.

Note that the size must first be increased on the virtual machine using the vSphere client and the virtual machine then restarted. The matching change can then be made through this menu. For full details refer to the '*Deploying Server Edition Servers as Virtual Machines*' manual

- **Increase Partition Size**
The available additional disk space is indicated. Click the button to expand the disk space used by that size. After clicking **Save** the server must be restarted.

5.5.6 HTTP Server

- **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](#) 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.

5.5.7 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](#).

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

5.5.8 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.

Note that this is different from the **Administrator** account used for access to Web Manager and the IP Office 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 IP Office configuration is changed using those applications.

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

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

5.5.9 Password Rules Settings

- **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 .

5.5.10 System Identification

These settings are shown are for information only.

- **System ID (SID):**
This is the unique system reference used to validate licenses issued for this particular system. For a physical server this is a unique value based on the server hardware. For a virtual server this value is based on several factors including the LAN1 and LAN2 IP addresses, the host name and the timezone. If any of those are changed, the **System ID** changes and any existing licenses become invalid.

- **Licensing Mode:**

Indicates the licensing method used by the system. **Internal** indicates that the system uses the unique system ID. Currently **Internal** is the only supported option.

5.5.11 Firewall

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.
 - **80:** If selected, allow port TCP 80.
 - **8000:** If selected, allow port TCP 8000.
 - **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.

5.5.12 Additional Hardware

These additional settings appear on servers with an additional hard disk. Unified Communications Module servers do not support this.

- **Additional Hardware Info**
The fields vary depending on the type and location of the additional hard disk.
 - **Create Partitions**
Use of this option is not currently supported with additional hard disks used for the Contact Recorder for IP Office service.
 - **Mount Path Name**
This is the name assigned for the additional hard disk. You can then use the name for access to the drive. For Contact Recorder for IP Office set the name to **/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**.
 - **Activate**
Enabling this option automatically mounts the additional hard disk.

5.6 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](#)^[36]. 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.

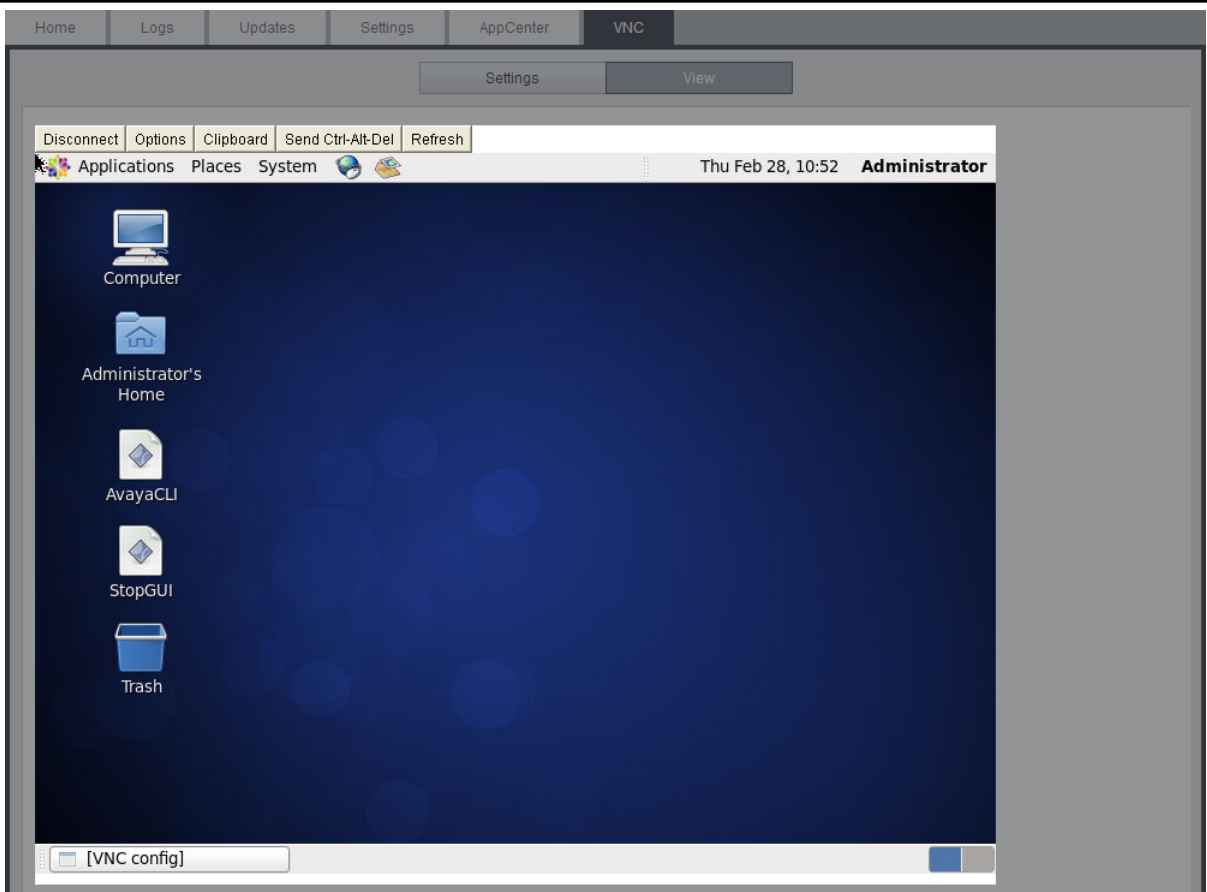
The screenshot shows the 'VNC' menu in the top navigation bar. Below it, there are 'Settings' and 'View' buttons. The 'Settings' button is active, displaying a 'VNC Settings' dialog box. The dialog box has three buttons: 'Start VNC', 'Stop VNC', and 'Apply'. It contains two input fields: 'Password:' with an empty text box, and 'Port:' with a text box containing the value '5807'.

View

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

The screenshot shows the 'VNC' menu in the top navigation bar. Below it, there are 'Settings' and 'View' buttons. The 'View' button is active, displaying a 'VNC Authentication' dialog box. The dialog box has a menu bar with 'Disconnect', 'Options', 'Clipboard', 'Send Ctrl-Alt-Del', and 'Refresh'. Below the menu bar, there is a 'Password:' label followed by an empty text box and an 'OK' button.

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



5.7 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](#) ⁵³ page.

The screenshot shows the 'AppCenter' tab selected in a navigation bar. Below the navigation bar is a section titled 'Download Applications' containing a grid of application cards. Each card includes an icon, a title, the date added, the size, and the application name.

Icon	Application Name	Added at	Size	Description
	Softphone Mac 4.0.1.1 CE4012b 73224.dmg	2014-08-11 02:31:17	45.1M	IP Office Video Softphone (Mac)
	Softconsole 9 1 0 104.exe	2014-08-11 02:31:19	0b	IP Office SoftConsole
	AdminLite 9 1 0 207.exe	2014-08-11 02:31:06	120.4M	IP Office Server Edition Manager
	DLink 1 0 0 5.exe	2014-08-11 02:31:20	3.5M	IP Office DevLink
	TAPI 1 0 0 40.exe	2014-08-11 02:31:19	10.6M	IP Office TAPI Service Provider
	VmPro-Mapi 9 1 0 68.exe	2014-08-11 02:31:16	23.4M	IP Office Voicemail Pro MAPI Service
	VmPro-Client 9 1 0 68.exe	2014-08-11 02:31:12	88.5M	IP Office Voicemail Pro Client

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 6.

Document History

6. Document History

Date	Issue	Changes
30th October 2014	10b	<ul style="list-style-type: none"> Updated for IP Office Release 9.1.
13th November 2014	10c	<ul style="list-style-type: none"> Incorrect reference to /CSIPOrec as mount point for additional hard disk.
14th November 2014	10d	<ul style="list-style-type: none"> Clarified that referred authentication applies to all services rather than just web control.
13th January 2015	10e	<ul style="list-style-type: none"> Alignment of the terminology of the upgrade paths table with the 9.1 GA technical bulletin. Removed availability of a ZIP file as an upgrade method between different 9.0.3/9.0.4 builds. Addition of the warning to disable one-X Portal logging prior to upgrading. Link from upgrading to logging into web management went to wrong version of logging into web management topic. Explanation of use of referred authentication^[12] expanded. Now also applicable for UCM for 9.1. Added screenshot of the UCM in web management Solution view. Note regarding the need for further configuration to use the VNC menu^[36] is running a virtual machine added. Extra steps in UCM V2 installation and upgrading added (module, including new module, needs manually controlled restart to enter software loading state). Reference to user required for UCM Ignition corrected to root. Zip upgrade method details removed (not used for 9.1).
14th January 2015	10f	<ul style="list-style-type: none"> UCM v1 battery removal/disposal note removed. USB2 terminology changed to USB (apparently USB1, 2 or 3 will work but with corresponding speed differences). Recommendation for USB install/upgrade changed to use upper USB socket. Use lower socket for keyboard. Incorrectly shown web control port and protocol options removed. Description of log archives corrected, contains all available logs, not just those since last archive creation. Application log menu shows the last 1000 log records. Expanded explanation of the passwords requested during ignition. USB utility instructions switched from UNetBootin to Rufus. Removed errant author only comments. Standardisation on 'amber' versus 'orange'.
17th February 2015	10g	<ul style="list-style-type: none"> Clarification of UCM v2 upper USB is USB3. All others are USB2. Put web management upgrade as first and preferred option for upgrading once system is on 9.1. Notes that to use monitor the monitor needs to be attached before module restart. Rufus URL changed to https: (http: works but frequently has problems). Various tidying. Removed errant "Use System Default" checkbox shown in screenshots of Application Server/Server Edition ignition.
3rd March 2015	10h	<ul style="list-style-type: none"> Removed mention of web collaboration as potential optional service. Processed raft of feedback in previous issue. Security steps in ignition added (based on seeing them in Build 9.1.2(412)).
13th March 2015	10i	<ul style="list-style-type: none"> Republish due to UCM module upgrade option incorrectly appearing in non-UCM documents.
14th April 2015	10j	<ul style="list-style-type: none"> Login Banner Text field is now blank by default (9.0 and 9.1). [80432] Change to certificate controls to allow the backup and restoration of the server's security certificate. [87145] Corrected /CSIPOrec to /CSIPORec. [82278]
15th April 2015	10k	<ul style="list-style-type: none"> Corrected Rufus URL. Removed USB3 references.
22nd April 2015	10l	<ul style="list-style-type: none"> Various text updates. Not technical changes. Some reordering of sections.
5th May 2015	10m	<ul style="list-style-type: none"> Merged the maintenance chapters for UCM and Linux servers. Added details for adding a certificate to Safari (Windows and Mac).
26th May 2015	10n	<ul style="list-style-type: none"> Updated download software page to match current support site design. [90569] Minor update to Rufus settings (basically stating the defaults). [90575] Rephrasing for fact that server certificates not available in 9.1.0GA but are available in 9.1FP (9.1.2). [90603]

Date	Issue	Changes
		<ul style="list-style-type: none"> Slight restructure to skip "step phrase" in UCM quick install description. [90605] Minor text enhancement to clarify that security is via shell "IP Office" on the UCM. [93333]
27th May 2015	10o	<ul style="list-style-type: none"> Minor text changes. [90606] one-X Portal AFA login is also under referred authentication control and by default uses Administrator account password. [90604] Clarification of Voicemail backup transfer from old to new server process and reinstatement of SSH file transfer details. [90598] Removed errant <<< >>> markup.
2nd June 2015	10p	<ul style="list-style-type: none"> Correction to System Settings screenshot for application server. Correct server maintenance topic incorrectly being included in Contact Recorder output.
16th June 2015	10q	<ul style="list-style-type: none"> Minor update to match redesign of Avaya support website.
1st July 2015	10r	<ul style="list-style-type: none"> Correction: UCM USB ISO transfer for upgrades needs to be fully prepared USB memory key, not just plain ISO file. "Web Manager Upgrade" status shown in SSA for upgrades via web manager menus.
7th September 2015	10s	<ul style="list-style-type: none"> Correction to mount path name for additional disks^[62]. Full name is derived disk mount path specified plus partition number, for example <i>/additional-hdd#1/partition1</i>. [99975] Various minor text layout fixes.
8th September 2015	10t	<ul style="list-style-type: none"> Various minor text layout fixes. Fixed unplanned mention of Unified Communications Module in non-UCM outputs from the common doc source.
29th September 2015	10u	<ul style="list-style-type: none"> Republished with errant author's notes text now hidden.
30th September 2015	10v	<ul style="list-style-type: none"> Correct of web control login from http to https.
30th October 2015	10w	<ul style="list-style-type: none"> Warning added that voicemail restore^[55] fails if VMPro client is connected. [99893] Note that Syslog Event Viewer^[49] filters are set when page is opened. Reload page to update.
2nd November 2015	10x	<ul style="list-style-type: none"> Republish to resynch publishing system.
6th November 2015	10y	<ul style="list-style-type: none"> Note that virtual servers either use NTP time or virtual server platform time. [100563]
8th December 2015	10z	<ul style="list-style-type: none"> Correction to description of Synchronize system clock before starting service and Use local time source. Clarifications to the password set and password change field descriptions to clarify which change IP Office and or Linux accounts.
21st December 2015	10aa	<ul style="list-style-type: none"> Emphasis that security reset may disrupt calls and services.
19th January 2016	10ab	<ul style="list-style-type: none"> Correct if path to download archived log files.

Index

3

3rd Party database integration 12

A

Add

Sub-interface 58

Additional documentation 11

Address

DNS 22, 58

IP 22, 58

Application

Auto-start 23

Install 27

Repositories 33, 54

Start 23

Stop 23

Uninstall 32

Upgrade 27, 28

Application files

Upload files 27, 34

Application Logs 48

Archive 49

Audit Log 48

Auto-start 23

B

Backup 16, 54

Browser 12

Bulletins 11

C

CentOS 11

Change

IP Address 22

Check

Software version 51, 52

Clients 65

Configuration

Voicemail Pro 14

ContactStore 12

CPU

Usage 45

Create a USB device 29

Create Archive 49

D

Database integration 12

Date 25, 60

Default

Gateway 22, 58

Password 21

Delete

Sub-interface 58

DHCP 22, 58

Disk

Usage 45

DNS 22, 58

Download

Logs 49

Windows Clients 65

E

Enable Traffic Control 22, 58

F

Forward

Syslog records 54

G

Gateway 22, 58

General 54

H

Home 45

Host Name 22, 58

I

Inactivity timeout 26, 55

Install

Application 27

Service 27

Interface 22, 58

IP Address 22, 58

J

Javascript 12

L

Linux 11

Local 54

Log Files Age 54

Logging In 21

Login 21

Banner text 54

Logs 47

Application 48

Archive 49

Audit 48

Download 49

Log Files Age 54

M

Mask 22, 58

Memory

Usage 45

Menu

Download 49

General 54

Home 45

Logs 47

Logs Download 49

Logs View 48

Services 51

System 52, 58

Updates 50

Updates Services 51

Updates System 52

View 48

Windows Clients 65

Menus

Inactivity timeout 26, 55

Module

Restart 24

Shutdown 24

N

Network 22, 58

Change IP address 22

Sub-interface 58

Network Time Protocol 25, 60

Notifications 45

NTP 25, 60

O

one-X Portal for IP Office

Auto-start 23

Start 23

Stop 23

- Operating system
 - Repositories 33, 54
 - Upload files 34
- P**
- Password
 - Default 21
 - Root password 23
 - Rules 61
- Port
 - Web Control 54
- R**
- RAM
 - Usage 45
- Reboot 24, 45
- Recieve
 - Syslog 54
- Related documents 11
- Remote
 - Server desktop 63
- Remote Software Repositories 35
- Remove
 - Sub-interface 58
- Repositories 33, 35, 54
- Repository 54
- Restart 24
- Restore 16, 54
- Root password
 - Change 23
 - Rules 61
- Rules 61
- S**
- Send
 - Syslog records 54
- Server
 - NTP 25, 60
 - Reboot 24, 45
 - Shutdown 24, 45
- Server desktop
 - Remote 63
- Service
 - Auto-start 23
 - Install 27
 - Start 23
 - Stop 23
 - Uninstall 32
 - Upgrade 27
- Services 51
 - Start 45
 - Status 45
 - Stop 45
- Set
 - Login banner 54
- Shutdown 24, 45
- SNMP 54
- SNMP Support 54
- Software
 - Repositories 33, 54
 - Repositories 35
 - Unetbootin 29
 - USB 29
- Software Repositories 54
- Software version
 - Check 51, 52
- Start 24
 - Auto-start 23
 - Service 23
- Start Services 45
- Status 45
- Stop
 - Service 23
- Stop Services 45
- Sub-interface 58
- Subnet Mask 22, 58
- Supported
 - Browsers 12
- syslinux.cfg 29
- Syslog
 - Settings 54
 - View 49
- System 52, 58
- T**
- Technical bulletins 11
- Time
 - Timezone 25, 60
- Timeout 26, 55
- Traffic Control 22, 58
- U**
- UMS 12
- Uninstall
 - Application 32
 - Service 32
- Update
 - Check version 51, 52
 - Services 51
 - System 52
- Updates
 - Services 50
 - System 50
- Upgrade
 - Application files 28
- Upgrading Applications 27
- Upload
 - Application files 27, 34
 - Operating system 34
 - Windows client files 34
- Usage
 - CPU 45
 - Disk 45
 - Memory 45
- USB
 - Create a bootable... 29
 - Software 29
- V**
- Version
 - Check 51, 52
- View
 - Syslog records 49
- View Logs 48
- VNC 63
- Voicemail 16
 - Auto-start 23
 - Start 23
 - Stop 23
- Voicemail Pro
 - Configuration 14
 - Limitations 12
- VPNM 12
- W**
- Watchdog 54
- Web browser 12

- Web Control Port 54
- Windows 16
- Windows client
 - Repositories 33, 54
- Windows client files
 - Upload files 34
- Windows Clients 65

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

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

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

© 2016 Avaya Inc. All rights reserved.