



IP Office 9.0

Unified Communications Module 9.0 Installation and Maintenance

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. Unified Communications Module

- 1.1 Using Linux 10
- 1.2 Additional Documentation..... 10
- 1.3 IP Address Notes..... 11
- 1.4 Small Community Networks..... 11
- 1.5 Licenses 12
- 1.6 Voicemail Pro Features..... 12
- 1.7 Supported Web Browsers..... 12

2. Module Installation

- 2.1 Quick Install..... 14
- 2.2 Downloading Module Software..... 16
- 2.3 Checking/Entering Licenses..... 17
- 2.4 Changing the IP Office Time Settings..... 17
- 2.5 Shutting Down the IP Office System..... 18
- 2.6 Inserting the Module..... 19
- 2.7 Igniting the Module Services..... 20
- 2.8 Installing the Current Software Release ISO..... 22
 - 2.8.1 Preparing a USB2 Installation Key..... 22
 - 2.8.2 Installing a New Image from a USB2 Memory Key 23
- 2.9 Changing the Web Password..... 24
- 2.10 Logging in to the Web Menus..... 25

3. Module Maintenance

- 3.1 Rebooting the Module..... 29
- 3.2 Shutting Down the Module..... 29
- 3.3 Changing the IP Address..... 30
- 3.4 Module LEDs..... 31
- 3.5 Module Buttons..... 31
- 3.6 Attaching a Monitor and Keyboard..... 32
- 3.7 Viewing the Module IP Address..... 32
- 3.8 Upgrading 33
 - 3.8.1 Upgrading from a Zip File 33
 - 3.8.2 Upgrading from a USB2 Memory Key..... 35
- 3.9 The Module Battery..... 38
- 3.10 Using System Status Application..... 39

4. Voicemail Pro Configuration

- 4.1 Adding Voicemail Licenses..... 43
- 4.2 IP Office Configuration..... 44
- 4.3 Installing the Voicemail Pro Client..... 45
- 4.4 Logging in to the Voicemail Server..... 46
- 4.5 Changing the Voicemail Server Password..... 47
- 4.6 Transferring Voicemail Server Settings..... 48
- 4.7 ContactStore..... 50
- 4.8 Backup/Restore Limitations..... 51

5. one-X Portal for IP Office Configuration

- 5.1 Adding Licenses..... 54
- 5.2 Enabling one-X Portal for IP Office Users..... 55
- 5.3 Initial one-X Portal for IP Office Login..... 56
- 5.4 Initial AFA Login..... 57
- 5.5 Transferring one-X Portal for IP Office Settings..... 58

6. Server Maintenance

- 6.1 Logging In Directly 63
- 6.2 Changing the Web Password..... 64
- 6.3 Changing the Root Password..... 65
- 6.4 Starting/Stopping Application Services..... 66
 - 6.4.1 Starting a Service..... 66
 - 6.4.2 Stopping a Service..... 66
 - 6.4.3 Setting a Service to Auto Start..... 66
- 6.5 Server Shutdown..... 67
- 6.6 Rebooting the Server..... 67
- 6.7 Changing the IP Address Settings..... 68
- 6.8 Date and Time Settings..... 69
- 6.9 Setting the Menu Inactivity Timeout..... 70
- 6.10 Upgrading Applications..... 71
 - 6.10.1 Loading Application Files onto the Server..... 71
 - 6.10.2 Upgrading Application Files..... 72
- 6.11 Uninstalling an Application..... 73
- 6.12 File Repositories..... 74
 - 6.12.1 Source Files..... 74
 - 6.12.2 Setting the Repository Locations..... 74
 - 6.12.3 Uploading Local Files..... 75
 - 6.12.4 Creating Remote Software Repositories..... 76

7. Server Menus

- 7.1 System 81
- 7.2 Logs 84
 - 7.2.1 Debug Logs..... 85
 - 7.2.2 Syslog Event Viewer..... 86
 - 7.2.3 Download..... 87
- 7.3 Updates 88
 - 7.3.1 Services..... 89
 - 7.3.2 System..... 90
- 7.4 Settings 91
 - 7.4.1 General..... 92
 - 7.4.2 System..... 96
- 7.5 App Center..... 100

8. Additional Processes

- 8.1 SSH File Transfers..... 105
- 8.2 Windows to Linux Voicemail Transfer..... 106

9. Document History

- Index 109

Chapter 1.

Unified Communications Module

1. Unified Communications Module

The Unified Communications Module is an IP500 base card supported by IP500 V2 systems running IP Office Release 8.0 or higher software. IP500 V2 systems running in IP Office Essential Edition, IP Office Preferred Edition or IP Office Advanced Edition mode can support the Unified Communications Module. The card acts as an automatic **PREFERRED EDITION** license for the system.

The instructions in this document relate to the installation of IP Office Release 9.0 4Q13 Service Pack software.

The module is a PC server that allows various Linux based IP Office applications to run as embedded applications within the IP500 V2 control unit rather than requiring separate PCs. The Unified Communications Module hosts the following applications:

The Unified Communications Module installation installs the following components:

- **Linux**

This is the base operating system used by the server. However, no specific Linux knowledge is required for server installation and maintenance.

- **Management Services**

This service is currently not used on the Unified Communications Module but is present for future development.

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

This is a web browser based application that user's 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 requires a [license](#)^[12]. The Unified Communications Module acts the **Preferred Edition** license required to run the application.

- **Voicemail Pro**

This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail. The Unified Communications Module acts as the **Preferred Edition** license required to run the application.

Unified Communications Module Capacity

The capacity of the Unified Communications Module is:

- **Number of Modules**

Maximum one module per system.

- **Trunk Cards:**

The module does not support a trunk daughter card.

- **IP Office Users:** The module supports up to 200 users when running Voicemail Pro and one-X Portal for IP Office. It supports more than 200 users when running just Voicemail Pro.

- **Simultaneous one-X Portal for IP Office Users:** 50.

- **Maximum voicemail ports:** The module provides 4 ports as standard, however additional ports can be licensed. The module can support up to 20 ports when running Voicemail Pro and one-X Portal for IP Office. It can support up to 40 ports when running just Voicemail Pro.

- **Small Community Network:** Maximum 6 systems.

Linux is a registered trademark owned by Linus Torvalds.

1.1 Using Linux

Despite using a Linux based operating system, no knowledge or experience of Linux is required. The Unified Communications Module 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. Except when specifically instructed by Avaya, Avaya does not support use of the Linux desktop or command line to perform actions on the server.

1.2 Additional Documentation

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

Related Documents

- **one-X Portal for IP Office Administration Manual**
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.
- **Voicemail Pro Installation Manual**
This manual covers scenarios including multiple servers within a Small Community Network.
- **Voicemail Pro Administration Manual**
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.
- **IP Office Manager Manual**
IP Office Manager is the application used to configure the IP Office application. This manual details how to use IP Office Manager and the full range of IP Office configuration settings.

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 IP Address Notes

During installation, you assign an IP address to the Unified Communications Module. The IP Office system has two physical LAN interfaces: LAN1 and LAN2 with ports labeled LAN and WAN respectively. The Unified Communications Module connects internally to the LAN1 network of the system and needs to have an address on that subnet.

These notes detail how the IP addresses are used.

Internal IP Addresses

The IP Office applications use the following fixed addresses for internal connections. You need to be aware of them as they appear in the IP Office system and one-X Portal for IP Office configuration settings. These fixed are addresses from the IANA link local range.

- **169.254.0.1**
This address is used for the provider connections from the one-X Portal for IP Office application to the IP Office. It is also used as the SNTP time source address for the Unified Communications Module.
- **169.254.0.2**
This address is used for the connections to the voicemail server by the IP Office and the one-X Portal for IP Office application.

User and Administration IP Addresses

User and administrator access to the Unified Communications Module and the applications it hosts use the following addresses.

- **Unified Communications Module**
During installation, web browser access to the module's ignition menu uses the IP Office system's LAN1 IP address. The ignition process configures a separate IP address to use for all future access to the module and its applications. We strongly recommend that you use an IP address on the same subnet as the IP Office system's LAN1.
- **one-X Portal for IP Office**
Web browser access to the one-X Portal for IP Office service running on the module uses the module's IP address or DNS name suffixed with port :8080.
- **Voicemail Pro**
The Voicemail Pro client accesses the voicemail server service running on the module using the module's IP address.

LAN2 and NAT Limitation

Traffic between the IP Office control unit and the module uses LAN1 of the IP Office system. For systems with more than 30 users, avoid scenarios where users of the module applications, especially one-X Portal for IP Office, access the module applications via the IP Office system's LAN2 (WAN) port. This also applies when using NAT on traffic between LAN1 and LAN2.

1.4 Small Community Networks

Up to 32 IP Office systems can connect using H323 SCN trunks to form a Small Community Network, supporting up to 1000 users. However, when using the Unified Communications Module, the Small Community Network only support up to 6 systems and, if running the one-X Portal for IP Office application, 200 users.

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

- **one-X Portal for IP Office**
A Small Community Network only supports a single one-X Portal for IP Office. When run on a Unified Communications Module, one-X Portal for IP Office only supports up to 200 users and 50 simultaneous user sessions. To support more users and sessions, install the one-X Portal for IP Office application on a separate server PC. Following installation of the Unified Communications Module with one-X Portal for IP Office application on it, additional configuration steps are required to configure the one-X Portal for IP Office application with details of the other IP Office systems. Refer to the one-X Portal for IP Office Installation Manual.
- **Voicemail Pro**
In an Small Community Network, one Voicemail Pro server stores all mailboxes and their related messages, greeting and announcements. Additional Voicemail Pro servers installed in the network perform other specific roles. For full details, refer to the Voicemail Pro manuals.

1.5 Licenses

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

- **Essential Edition**
This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
The Voicemail Pro application normally requires this license. For the Unified Communications Module, the module acts as an automatic **Preferred Edition** license for the system. This enables 4 voicemail ports.
- **Preferred Edition Additional Voicemail Ports**
These licenses add additional voicemail ports in addition to the 4 enabled by the presence of the Unified Communications Module. You can add multiple licenses, up to 20 ports when running Voicemail Pro and one-X Portal for IP Office, or 40 ports when running just Voicemail Pro.
- **User Profile Licenses**
In order to log into and use the one-X Portal for IP Office application, a user must be configured and licensed to one of the following user profile roles in the IP Office configuration: **Office Worker**, **Teleworker** or **Power User**. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

1.6 Voicemail Pro Features

Voicemail Pro runs on both Windows and Linux servers. Voicemail Pro running on Linux, such as with the Unified Communications Module, does not support the following Voicemail Pro features:

- **VB Scripting**
- **3rd Party Database Integration**
- **VPNM**
- **UMS Web Voicemail**
However, as alternatives, users can browse voicemail via UMS IMAP or one-X Portal for IP Office.
- **ContactStore**
ContactStore is supported for IP Office Release 8.1 Feature Pack 1 and higher.

1.7 Supported Web Browsers

Avaya supports the following web browsers:

- Microsoft Internet Explorer 8 or higher with JavaScript enabled.
- Mozilla Firefox with JavaScript enabled.

Chapter 2.

Module Installation

2. Module Installation

The instructions in this document relate to the installation of IP Office Release 9.0 4Q13 Service Pack software.

2.1 Quick Install

The following process is a summary of the steps for installing a Unified Communications Module into an IP Office system. Use this process if you are familiar with IP Office operation and configuration. For a more detailed installation process, proceed from the following section, [Downloading Module Software](#)^[16].

Allow up to 2 hours for the process, not including the downloading of the required software.


1. Prerequisites

Check that you have the following:

- a. An IP500 V2 running IP Office Release 9.0 or higher in Essential Edition mode.
- b. A Windows PC with IP Office Manager networked to the IP Office system. Test by opening the configuration of the IP Office.
- c. A 5mm Flat-blade screwdriver plus anti-static wrist strap and ground point for module insertion.
- d. An 8GB USB2 memory key.
- e. An IP address to assign to the module on the same subnet as the IP Office system's LAN1.
- f. A hostname for the module to use on the customer's network.
- g. The latest Unified Communications Module upgrade ISO file and USB software that match the IP Office release. See [Downloading Module Software](#)^[16].

2. IP Office Configuration

Using IP Office Manager, check and change the following items in the IP Office configuration:

- a. Click **Control Unit** and select the **IP500 V2**. Note the **Version**. This should match the software you downloaded for the module.
- b. Click **System** and then **LAN1** tab. On the **LAN Setting** sub-tab, note the **IP Address**.
- c. Select the **System** tab. Set the **Time Setting Config Source** to either **SNTP** or **None**. Click **OK**.
- d. Click  to save the configuration back to the IP Office.

3. Shutdown the IP Office

Using IP Office Manager, shutdown the system (**File | Advanced | System Shutdown**). Only switch off power to the system when each LED1 on the front of the unit and the CPU LED on the rear flash rapid red-amber. See [System Shutdown](#)^[18].

4. Insert the Unified Communications Module

Insert the module into an empty slot in the IP Office system. Reapply power to the IP Office and wait for the system to restart. The lower LED on the module should be green with an amber flash every 5 seconds. See [Inserting the Module](#)^[19].

5. Ignite the Unified Communications Module

Using a web browser, log in to the LAN1 address of the IP Office system suffixed with :7070. For example **http://<IP Office LAN1 address>:7070**. See [Igniting the Module Services](#)^[20].

- a. Note the Release number shown after the **R** in the title bar.
 - The default name and password for Release 8.0 are **web** and **webcontrol**.
 - The default name and password for Release 8.1 or higher are **Administrator** and **Administrator**.
- b. Accept the license and click **Next**.
- c. Enter IP address details valid for the same subnet used by LAN1 of the IP Office. Click **Next**.
- d. Select which applications you want the module to run. Click **Next**.
- e. Enter a root password for the Linux running on the module. Click **Next**.
- f. Accept the default time settings. Enter a hostname and click **Next**.
- g. Check the settings and click **Apply**.

6. Upgrade the Unified Communications Module

Though shipped with pre-installed software, you **must** always upgrade the module to the latest maintenance release matching the software release of the IP Office.

- a. Using the downloaded **unetbootin** software and ISO file, prepare the USB2 installation key. See [Preparing a USB2 Installation Key](#)^[22].
- b. Remove the rubber cover from the front of the module.

- c. Press the top button on the module until the lower LED begins to flash. Wait until all LEDs on the card are off except for the amber flash every 5 seconds.
- d. Insert the USB2 memory key into a USB slot on the module.
- e. Press the top button on the module and hold. The upper two LEDs are orange. Release the button immediately after the upper two LEDs go out.
- f. The module boots from the USB key and installs the software from the USB2 memory key. Allow the process to run until the USB key no longer indicates any activity (approximately 45 minutes).
- g. The module restarts and after approximately 3 minutes:
 - **Lower status LED shows only regular IP Office heartbeat flashes:**
Remove the USB2 memory key. Restart the module by pressing the top button.
 - **Lower status LED green with regular IP Office heartbeat flashes:**
Remove the USB2 memory key.
- h. Replace the rubber cover.
- i. Repeat the ignition process in Step 5.

7. Change the Module Password

Change the passwords used for direct access to the server.

- a. See [Changing the Web Password](#)^[64].
- b. See [Changing the Root Password](#)^[65].

8. Configure the Server Applications

Check and configure the server applications. See [Voicemail Pro Configuration](#)^[42] and [one-X Portal for IP Office Configuration](#)^[54].

- a. **! Important:** Check and ensure that the IP Office switch configuration is set to the **Voicemail Type** of **Voicemail Lite/Pro** with the **Voicemail IP Address** of **169.254.0.2**.

2.2 Downloading Module Software

Avaya makes Unified Communications Module software for each IP Office release available from the Avaya support website (<http://support.avaya.com>) in a number of formats. For Unified Communications Module installation, you must download the ISO file and UNetBootin software.

- **ZIP File**

You can use this type of file to upgrade within an existing release. For example, to upgrade a server running 9.0 (x) to 9.0(y). The ZIP file contains RPM files that the module extracts after uploading the ZIP file.

- **! 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. Some releases include changes that require additional steps.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading.

- **ISO File**

You can use this type of file to reinstall the full set of software including the operating system. Before using an ISO file, you must backup all applications data. Note that the Unified Communications Module uses a separate ISO file from other Linux bases IP Office products. You require this file when installing a Unified Communications Module.

- **Source ISO File**

Some components of the software are open source. To comply with the license conditions of that software, Avaya are required to make the source software available. However, this file is not required for installation.

- **RPM Files**

Occasionally Avaya may make separate RPM files available. It uses these to upgrade individual software components on the module. RPM files install in the same way as a ZIP file.

- **UNetBootin software**

This additional software is downloadable from <http://unetbootin.sourceforge.net>. You use it to load an .iso image onto a USB memory key from which the server can boot.

To download software:



1. Browse to <http://support.avaya.com> and log in.
2. Select **Downloads & Documents**.
3. In the **Enter Your Product Here** box, enter **IP Office**.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. If shown, click **View downloads >**.
6. The resulting page lists the files available for download. Select the file to download.
7. Click **View documents >**.
8. Select the **Technical Tips** checkbox.
9. In the list of documents, download the IP Office Technical Bulletin for the IP Office release.

2.3 Checking/Entering Licenses

The Unified Communications Module requires an IP Office system running with an **Essential Edition** license at minimum. Additional licenses may be required for additional features.

- **Essential Edition**
This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
The Voicemail Pro application normally requires this license. For the Unified Communications Module, the module acts as an automatic **Preferred Edition** license for the system. This enables 4 voicemail ports.
- **Preferred Edition Additional Voicemail Ports**
These licenses add additional voicemail ports in addition to the 4 enabled by the presence of the Unified Communications Module. You can add multiple licenses, up to 20 ports when running Voicemail Pro and one-X Portal for IP Office, or 40 ports when running just Voicemail Pro.
- **User Profile Licenses**
In order to log into and use the one-X Portal for IP Office application, a user must be configured and licensed to one of the following user profile roles in the IP Office configuration: **Office Worker**, **Teleworker** or **Power User**. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.



To check or enter a license:

1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **License**.
3. Click **Add** and select **ADI**.
4. Enter the new license and click **OK**. You should add licenses by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.
5. The **Status** of the new license should show **Unknown** and the name the license should match the type of license entered. If the name shows as **Invalid**, the most likely cause is incorrect entry of the license key characters.
6. Click on the  save icon to send the configuration back to the IP Office.
7. Use Manager to receive the configuration again and check that the status of the license. It should now be **Valid**.

2.4 Changing the IP Office Time Settings

To support the module, the system must either use an external time server or to have its time and date set manually.

To change the time settings:

1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **System** and select the **System** tab.
3. Change the **Time Setting Config Source** value as follows:
 - **To Use an External Time Server**
Change the setting to **SNTP**. IP Office Manager displays the additional fields for setting the address of the time server or servers.
 - **To Set the Time Manually**
Change the setting to **None**. The system's time and date are now set through the menu of an Avaya phone user who has **System Phone Rights**.
4. Click on the  save icon to send the configuration back to the IP Office.

2.5 Shutting Down the IP Office System

Before adding or removing any hardware from the IP Office system, it must be shutdown using one of the shutdown methods below. Failing to shutdown the system correctly may cause lose of data.

• ! WARNINGS

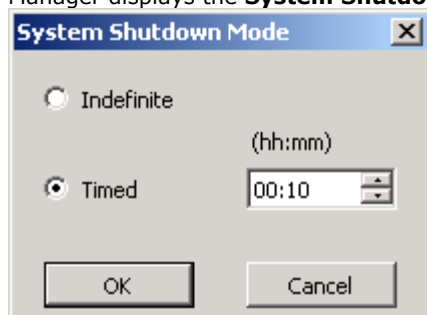
- You must always shutdown a system before switching it off. Simply removing the power cord or switching off the power input may cause the loss of data.
- This is not a polite shutdown, it stops any user calls and services in progress.
- The shutdown process takes up to a minute to complete. When shutting down a system with a Unified Communications Module installed, the shutdown can take up to 3 minutes while the card safely closes all open files and closes down its operating system. During this period, the module's LED 1 remains green.
- Do not remove power from the system until the system LEDs are in the following states:
 - LED 1 on each installed base card flashes fast red-amber. For those base cards with a trunk daughter card installed, LED 9 also flashes fast red-amber.
 - The CPU LED on the rear of the system flashes fast red-amber.
 - The System SD and Optional SD memory card LEDs on the rear of the system are off.
- To restart a system when shutdown indefinitely, or to restart a system before the timed restart, switch power to the system off and on again.

To shutdown the system using the AUX button:

When the **AUX** button on the rear of the system is pressed for more than 5 seconds, the IP500 V2 control unit will shutdown with the restart timer set to 10 minutes. Wait until the state of the LEDs on the system match those listed above before switching off power to the system.

To shutdown the system using IP Office manager:

1. Using IP Office Manager, select **File | Advanced | System Shutdown**.
2. Using the **Select IP Office** menu to select the system and enter the administrator name and password. IP Office Manager displays the **System Shutdown Mode** menu.



3. Select **Indefinite** and click **OK**.
4. Wait until the state of the LEDs on the system match those listed above before switching off power to the system.

To shutdown the system using the System Status Application:

1. Start System Status Application and access the system's status output.
2. In the navigation panel, select **System**.
3. At the bottom of the screen, select **Shutdown System**.
4. Select **Indefinite** and click **OK**.
5. Wait until the state of the LEDs on the system match those listed above before switching off power to the system. Switch off power to the system.

2.6 Inserting the Module

Once you have [shutdown](#) ^[18] the system, you can insert the module.

- **! WARNINGS**

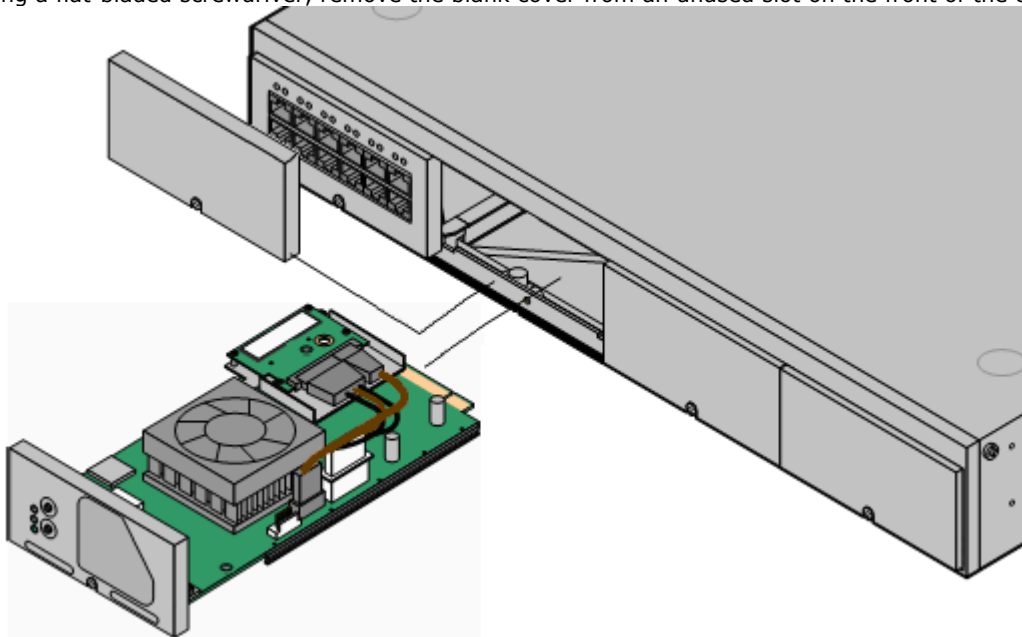
- Ensure that you take anti-static protection steps while handling circuit boards.
- Never add or remove cards from the control unit while it has power connected.

- **Tools Required**

- 5mm Flat-blade screwdriver.
- Anti-static wrist strap and ground point.

To insert the module:

1. If not already done, ensure that the plastic cover that fits over the external ports on the module's faceplate is in place.
2. Using a flat-bladed screwdriver, remove the blank cover from an unused slot on the front of the control unit.



3. Allowing the module to rest against the bottom of the slot, begin sliding it into the control unit. When half inserted, check that the module rails have engaged with the slot edges by trying to gently rotate it. If the module rotates, remove it and begin inserting it again.
4. While inserting the module, also check to ensure that cables on the module do not interfere with the insertion operation.
5. The module should slide in freely until almost fully inserted. At that point, apply pressure at the base of the front of the module to complete insertion.
6. Using a flat-bladed screwdriver, secure the module.
7. Reapply power to the system.
8. The module has started once the lower LED changes to green with regular amber flashes. You can now run the module [ignition](#) ^[20].

2.7 Igniting the Module Services

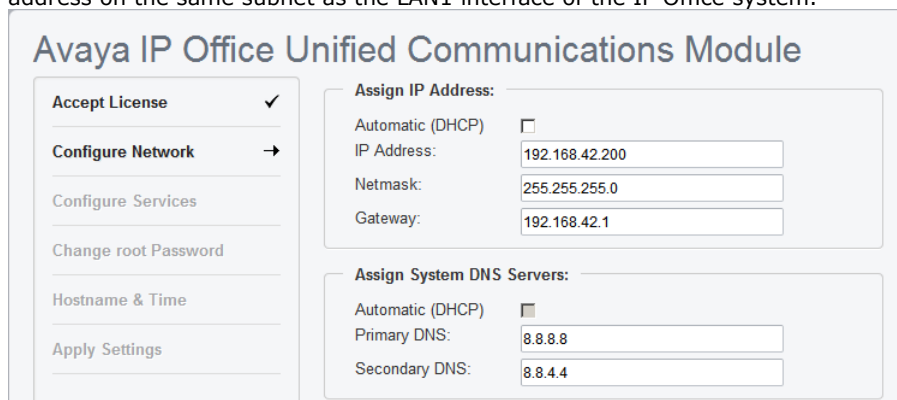
Following [insertion of the module](#)^[19], you need to run the module ignition process.

To ignite the module services:

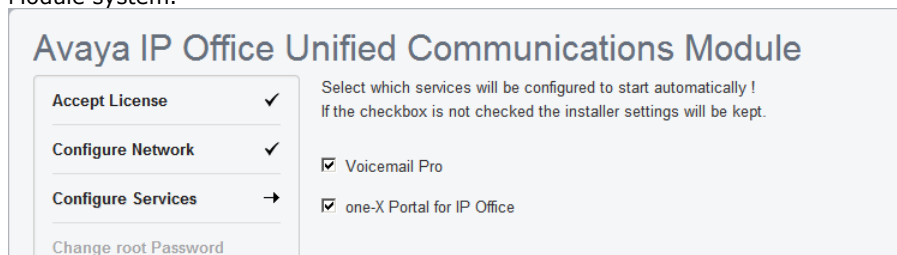
1. From a client PC, start the browser. Enter **http://** followed by the LAN1 IP address of the IP Office system and **:7070**. For example, enter **http://192.168.42.1:7070**.
2. The login menu appears.



- Note the release number shown after the **R** in the menu title. If this does not match the software release of the IP Office system, then following ignition, you must use the appropriate ISO file and a USB2 memory key to upgrade the card to match the IP Office system's release.
3. Enter the default name and password.
 - The default name and password for Release 8.0 are **web** and **webcontrol**.
 - The default name and password for Release 8.1 or higher are **Administrator** and **Administrator**.
 4. Click **Login**. If you accept the license, select **I Agree** and click **Next**.
 5. Enter the IP address and DNS settings that the module should use. Enter details that give the module an IP address on the same subnet as the LAN1 interface of the IP Office system.



6. Select the services that you want the Unified Communications Module to provide for the Unified Communications Module system.



7. Click **Next**. Enter and confirm a new root password. This is the root user password for access to the operating system.

The screenshot shows the 'Avaya IP Office Unified Communications Module' configuration interface. On the left, a sidebar contains a list of configuration steps: 'Accept License' (checked), 'Configure Network' (checked), 'Configure Services' (checked), and 'Change root Password' (active, indicated by a right-pointing arrow). The main content area has a heading 'Pick a new root password, and keep a record of it. Remember that the root password is a critical part of system security.' Below this, there are two input fields: 'New Password:' and 'New Password (verify):', both containing masked characters. At the bottom, it lists 'Password complexity requirements:' with a bullet point: '• must contain at least 8 characters.'

8. Click **Next**. Enter basic details for the module. Do not change the **Use NTP** and **NTP Server** settings. The default **169.254.0.1** setting is an internal address for the module to get its time from the IP Office system.

The screenshot shows the 'Avaya IP Office Unified Communications Module' configuration interface. The sidebar on the left has 'Change root Password' (disabled, indicated by a left-pointing arrow) and 'Hostname & Time' (active, indicated by a right-pointing arrow). The main content area contains the following settings: 'Hostname:' (uc-module), 'Date:' (2013-04-10), 'Time:' (10 : 56), 'Timezone:' (Europe/London), 'Use UTC Time:' (unchecked), 'Use NTP:' (checked), and 'NTP Server:' (169.254.0.1). There is an 'Apply Settings' button at the bottom left.

11. Click **Next**. A summary of the settings appears. Click **Apply**. Alternatively use the **Previous** and **Next** options to readjust the settings.

12. Once configuration is complete, the module will restart with the new settings. The module attempts to redirect your browser to the module's new IP address. Click **OK**.

- If the release number shown after the **R** in the module's login menu does not match the software release of the IP Office system, then following ignition, you must use the appropriate ISO file and a USB2 memory key to upgrade the card to match the IP Office system's release. See [Installing the Current Software Release ISO](#) [22].
- If the release number shown after the **R** in the module's login menu matches the software release of the IP Office system, you can continue with further configuration. See [Changing the Web Password](#) [24].

2.8 Installing the Current Software Release ISO

Avaya supplies the module with software pre-installed. However, that software may not match the software level of the IP Office system. Therefore, it may be necessary to reinstall the card software from a downloaded ISO file of the correct software to match the IP Office system's own software release.

Use this process if the release number shown after the **R** in the module's login menu does not match the software release of the IP Office system.

- **! WARNING**

This process overwrites all existing data and software on the module. Only use this process on an existing operational module after having backed up the application data to another location.

2.8.1 Preparing a USB2 Installation Key

This process uses a downloaded ISO file to create a bootable USB2 memory key for software installation. Using this device installs the software, overwriting any existing software and data on the server.

Prerequisites

- **8GB USB2 Memory Key**

Note that all existing files on this device will be erased.

- **UNetBootin software**

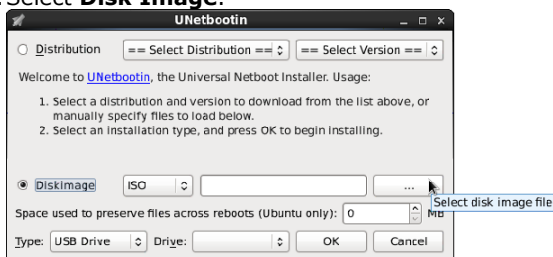
This additional software is downloadable from <http://unetbootin.sourceforge.net>. You use it to load an .iso image onto a USB memory key from which the server can boot.

- **Unified Communications Module ISO File**

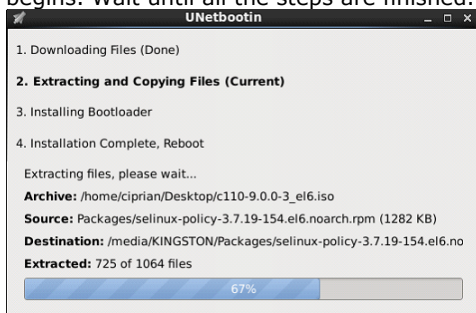
You can download this software from the Avaya support website (<http://support.avaya.com>).

To create a bootable USB2 memory key:

1. Erase all files on USB2 memory key and reformat it as a FAT32 device.
2. Start the **unetbootin** application.
3. Select **Disk Image**.



4. Click the **...** browse button and select the ISO file.
5. Click **OK**. If a warning appears announcing that all data from the USB2 memory key will be lost, click **Yes** to all. The process of transferring the files from the ISO image to the USB2 memory key and making that device bootable begins. Wait until all the steps are finished.



6. When the process has ended, click **Exit**. Do not click **Reboot now**.
7. Using the file explorer, open the USB folder on the USB2 memory key.
8. Select the files **syslinux.cfg** and **avaya_autoinstall.conf** and copy them to the top level (root) folder, overwriting any existing files with those names.

- **! WARNING**

Only use this option to create a USB2 memory key for full software installation. The installation process overwrites any existing data.

9. Remove the USB2 memory key from the PC. The device is ready for use for full software installation.

2.8.2 Installing a New Image from a USB2 Memory Key

To install software from the previously prepared USB2 memory key use the following process. This process reinstalls the module software and also upgrades the module firmware if necessary.

- **! WARNING**

This process overwrites all existing data and software on the module. Only use this process on an existing operational module after having backed up the application data to another location.

To install a software image from a USB2 memory key:

1. Prepare a bootable USB2 memory key for software installation. See [Preparing a USB2 Installation Key](#)^[22].
2. Remove the plastic cover from the front of the faceplate of the card. You must retain this cover and reattach it after completing this process.
 - We recommend connecting a monitor using an HDMI to HDMI cable or HDMI to DVI cable. This allows you to monitor the process and to confirm when it is completed.
3. Check that you have obtained backups of all application data (one-X Portal for IP Office, Voicemail Pro) from the module if it is already from an operating customer system.
4. Insert the USB2 memory key with the new image file into one of the USB ports located on the front of the module.
5. Shut down the module by pressing the upper button on the module until the lower LED starts to flash green. The shutdown is complete once all module LEDs are off except for regular (every 5 seconds) IP Office heartbeat amber flashes of the lower LED.
6. Restart the module by pressing the upper reset button again and keeping it pressed until the top two LEDs change from orange to off.
7. The module will reboot using the image files on the USB2 memory key.
8. After approximately 2 minutes, the top two LEDs change to alternately flashing green. The lower LED remains steady green. This installation process takes approximately 45 minutes.
9. After the software installation completes, the module restarts. During the restart, if necessary, the module's firmware is upgraded. The restart, including firmware upgrade, takes approximately 3 minutes. After this the upper 2 LEDs are off and the lower LED indicates the module's status as follows:
 - **Lower status LED shows only regular IP Office heartbeat flashes:**
This indicates that a firmware upgrade occurred after which the module automatically shutdown.
 - a. Remove the USB2 memory key. Remove any monitor connection.
 - b. Restart the module by press the top button or [using System Status Application](#)^[39].
 - **Lower status LED green with regular IP Office heartbeat flashes:**
This indicates that the module restarted without needing a firmware upgrade.
 - a. Remove the USB2 memory key. Remove any monitor connection.
10. Refit the plastic cover removed at the start of the process.
11. You now need to repeat the processes for [module initialization](#)^[20] as if this was a new module.

2.9 Changing the Web Password

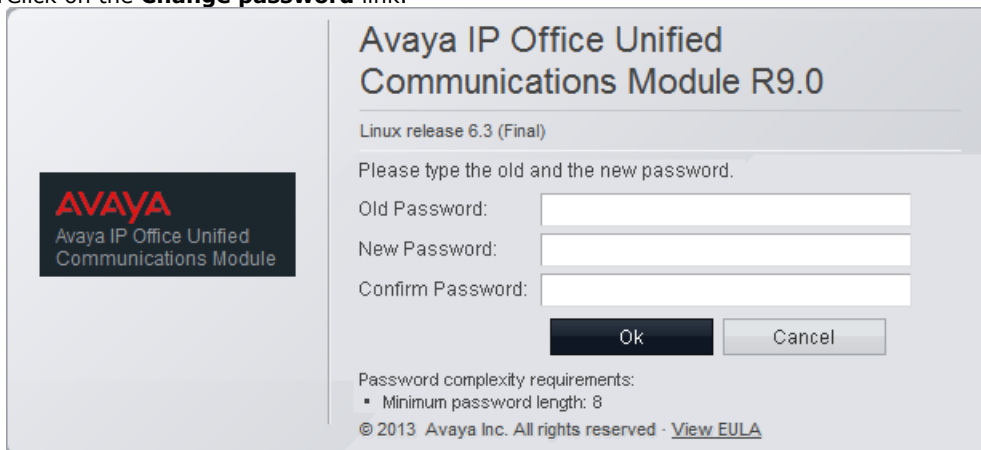
Following [ignition](#)^[20], you should change the web password from its default.

To change the browser password:

1. From a client PC, start the browser. Enter **http://** followed by the address of the Unified Communications Module and **:7070**. If the IP address is unknown, see [Viewing the Module IP Address](#)^[32].
2. Select the **Language** required.



3. Click on the **Change password** link.



4. Enter the current password and the new password. The new password must meet the complexity requirements displayed on the menu.
5. Click **OK**. The menu confirms whether the change was successful or not. If the new password is accepted, click **Cancel** to return to the **Login** menu. .

2.10 Logging in to the Web Menus

Avaya supports the following web browsers:

- Microsoft Internet Explorer 8 or higher with JavaScript enabled.
- Mozilla Firefox with JavaScript enabled.

To log in to the module's web control menus:

1. From a client PC, start the browser. Enter **http://** followed by the address of the Unified Communications Module and **:7070**. If the IP address is unknown, see [Viewing the Module IP Address](#)^[32].
2. Select the **Language** required.



Avaya IP Office Unified Communications Module R9.0

Linux release 6.3 (Final)

Please log on.

Logon:

Password:

Language:

Login

[Change password](#)

© 2013 Avaya Inc. All rights reserved · [View EULA](#)

3. Enter the name and password for Unified Communications Module administration. To change the password, select the [Change Password](#)^[64] option.
 - The default name and password for Release 8.0 are **web** and **webcontrol**.
 - The default name and password for Release 8.1 or higher are **Administrator** and **Administrator**.
4. If the login is successful, the server's [System](#)^[81] page appears.

Chapter 3.

Module Maintenance

3. Module Maintenance

The following sections cover various Unified Communications Module maintenance processes:

- [Rebooting the Module Services](#) ^[29]
- [Shutting Down the Module](#) ^[29]
- [Changing the IP Address](#) ^[30]
- [Module LEDs](#) ^[31]
- [Module Buttons](#) ^[31]
- [Attaching a Monitor and Keyboard](#) ^[32]
- [The Module Battery](#) ^[38]
- [Viewing the Module IP Address](#) ^[32]
- [USB2 Upgrade](#) ^[35]
- [Using System Status Application](#) ^[39]

See also:

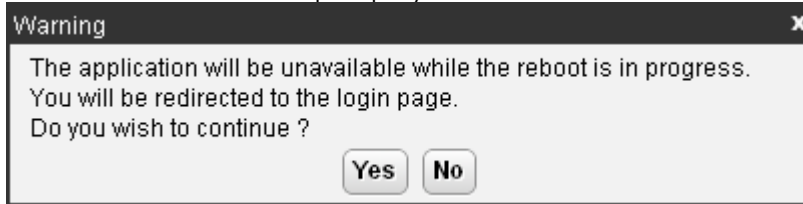
- [Changing the Web Password](#) ^[24]
- [Logging In](#) ^[25]
- [Upgrading from a Zip File](#) ^[33]
- [Reinstalling the Software from an ISO File](#) ^[22]

3.1 Rebooting the Module

Rebooting the server stops all currently running services and then stops and restarts the server. Only those application services set to **Auto Start** automatically restart after the reboot.

To reboot the server:

1. [Login](#) to the server's web configuration pages.
2. After logging in, select the [Home](#) 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**.

3.2 Shutting Down the Module

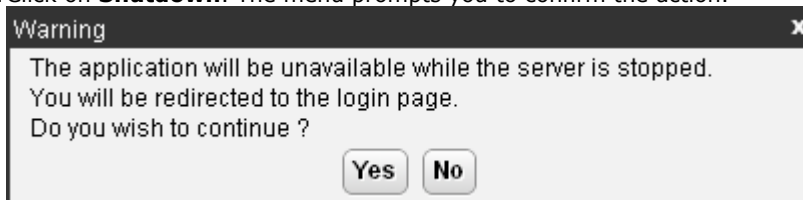
Use this process when it is necessary to switch off the Unified Communications Module for any period. For the Unified Communications Module, the module can be shutdown or started up using the upper switch on its front panel. See [Module Buttons](#).

- **! WARNING**

If the module is being shutdown in order to remove it from the system, you must also [shutdown the IP Office system](#).

To shutdown the server:

1. [Login](#) to the server's web configuration pages.
2. After logging in, select the [Home](#) 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.

3.3 Changing the IP Address

Using the server's web configuration pages, you can change the server's network settings.

- **Warning**

Changing IP address and other network settings will require you to login again.

To change the IP address:

1. [Login](#)^[63] to the server's web configuration pages.

2. Select **Settings**.

3. Select **System**.

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

- **Network Interface**

For the Unified Communications Module this setting is fixed as **eth0.1**.

- **Host Name**

Sets the host name that the Unified Communications Module should use. This setting requires the local network to support a DNS server. Do not use **localhost**.

- **Use DHCP**

Do not use this setting with the Unified Communications Module.

- **IP Address**

Displays the IP address set for the server. The Unified Communications Module connects to the system's LAN1 network system and must have an address on that subnet. See [IP Address Notes](#)^[114].

- **Subnet Mask**

Displays the subnet mask applied to the IP address.

- **Default Gateway**

Displays the default gateway settings for routing.

- **System DNS**

Enter the address of the primary DNS server.

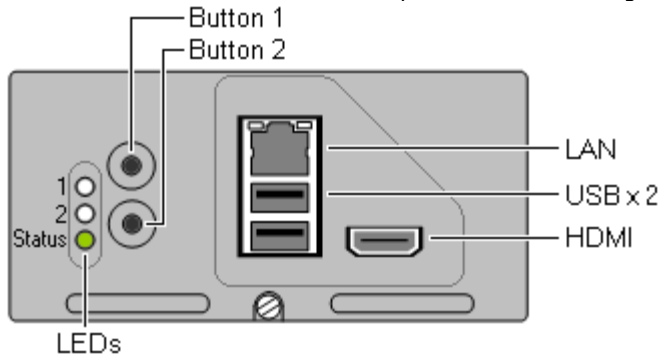
- **Automatically obtain DNS from provider**

Not used.

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

3.4 Module LEDs

The Unified Communications Module provides the following LEDs:



- **Upper 2 LEDs**

- **Orange:** Module BIOS starting.

- **Lower LED**

- **Solid Red:** Unpacking and initializing.
- **Flashing Red:** Module initialization.
- **Flashing Green:** Module operating system starting or shutting down.
- **Solid Green with Amber blinks:** OK. IP Office heartbeat okay.
- **Off with Amber blinks:** Module shutdown. IP Office heartbeat okay.
- If the module is already running when the system restarts, the lower LED remains green when the LEDs on the other base cards are solid red. If the module is not running when the system restarts, the lower LED remains off when the LEDs on the other base cards are solid red. During a system initialization, the lower LED flashes red when the LEDs on the other base cards flash red; before reverting to green or off when the system reboot is complete.

3.5 Module Buttons

The Unified Communications Module provides the following buttons:

- **Upper Button/Button 1**

You can use the buttons for the following functions:

- **Shutdown**

If the module is running, pressing this button for more than 2 seconds starts a module shutdown. The lower LED changing to off with regular amber blinks indicates a completed shutdown.

- **Startup**

If the module has been shutdown, pressing this button causes it to startup.

- **Alternate Boot**

When the module is about to boot, shown by both upper LEDs being orange, pressing and holding the switch until those LEDs change to off instructs the module to attempt to boot from any device attached to its USB ports.

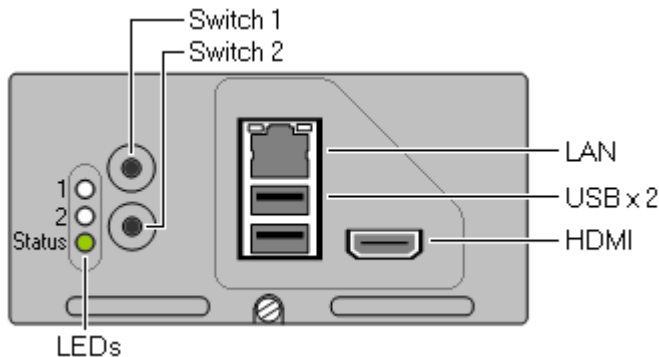
- **Button 2:** Not used.

3.6 Attaching a Monitor and Keyboard

Avaya designed the Unified Communications Module and its applications for remote maintenance only during normal operation. However, some processes may require direct attachment of a monitor and keyboard.

- **! WARNING: Do Not Remove the Port Cover Except for Maintenance**

Avaya supplies the card with a plastic cover located over the external ports (LAN, USB and HDMI). The cover must always be in place during normal card operation. You should only remove the cover temporarily during maintenance actions that require access to the ports. You must replace the cover when the maintenance is completed.



To attach a keyboard:

For maintenance and diagnostics purposes, you can attach a keyboard to either of the USB ports on the front of the module.


To attach a monitor:

For maintenance and diagnostics purposes, you can attach a monitor to the HDMI port on the front of the module. Use a HDMI to HDMI or HDMI to DVI cable.

3.7 Viewing the Module IP Address

During installation, the installer gives the Unified Communications Module an IP address on LAN1 of the IP Office. You can subsequently change the address through the card's web control menus. If for some reason the current address is unknown, you can view it as part of the IP Office configuration.

To view the card's IP address using IP Office Manager:

1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **Control Unit**.
3. Locate the **UC Module** in the list of installed units and select it.
4. The details pages lists information about the Unified Communications Module including its current IP address.

3.8 Upgrading

Avaya makes both ISO files and ZIP files available for each IP Office release. You can use these for upgrading a module. The file and method to use depends on the upgrade path.

- **Use a ISO file for:**
 - For full 9.0 installation using a USB2 memory key. See [Installing the Current Software Release ISO](#) ^[22].
 - For upgrading from 8.0 or 8.1 to 9.0. See [Upgrading from a USB2 Memory Key](#) ^[35].
 - For upgrading from 9.0.x to 9.0.y. See [Upgrading from a USB2 Memory Key](#) ^[35].
- **Use a ZIP file for:**
 - Upgrading from 9.0.x to 9.0.y using the module's web menus. See [Upgrading from a ZIP File](#) ^[33].

3.8.1 Upgrading from a Zip File

Avaya may make ZIP files available for upgrades of the module software. See [Downloading Software](#) ^[16]. The ZIP file contains RPM files that the module extracts after uploading the ZIP file.

You can use this type of file to upgrade within an existing release. For example, to upgrade a server running 9.0(x) to 9.0(y). To upgrade from a different release, for example from 8.0 or 8.1 to 9.0, you must use an ISO file. See [Upgrading from a USB2 Memory Key](#) ^[35].

- **! 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. Some releases include changes that require additional steps.
- **! Backup Application Data**
In all cases, always backup all application data to a separate location before upgrading.
- **! WARNING**
If the software upgrade causes a module firmware upgrade, the module will shutdown following that upgrade. Therefore, if upgrading remotely, ensure that you have access to the system using System Status Application in order to restart the module following the upgrade.

To upgrade the software:

1. Login to the web control menus.
2. Select the **Settings | General** menu.
 - a. In the **Web Control** section, change the **Inactivity timeout** to **1 hour**.
 - b. Click **Save**. It will be necessary to login to the web control menus again.
3. Select the **Setting | General** menu again.
 - a. For the **Applications** options, select **Local**.
 - b. Select **Browse** and browse to the upgrade ZIP file and click **Add**.
 - c. Select the **Updates | Services** menu. Click **Update All**.
 - d. During the upgrade, the server stops various services and requires you to login in again. Repeat the **Update All** process until the **Update All** button appears greyed out.
4. If additional services have been added they are not automatically installed. Install the new services as follows:
 - a. Select the **Updates | Services** menu. Install the new rpms in the following order. The order is critical, the **SSDFWUpgrade** package will not install correctly if **mailx** and **smartmontools** are not installed first:
 - i. Check the status of the **mailx** component. If not installed, click the adjacent **Install** button.
 - ii. Check the status of the **smartmontools** component. If not installed, click the adjacent **Install** button.
 - iii. Check the status of the **SSDFWUpgrade** component. If not installed, click the adjacent **Install** button.
 - b. Following installation, the module may automatically shut down. This is indicated by the lower status LED only showing the regular IP Office heartbeat flash. Restart the module by pressing the top button or [using System Status Application](#) ^[39].
 - c. Login to the web controls menu again if necessary. On the **Home** tab, the **Notifications** window shows the result of the SSD firmware upgrade is any:
 - "SSD Firmware upgrade successful. Power cycle was completed to finalize the changes"
 - "SSD Firmware not needed. SSD version is Ver703.o"
 - "SSD Firmware not needed. SSD version is S5FAR031"



3.8.2 Upgrading from a USB2 Memory Key

When upgrading within a release, for example from 9.0(x) to 9.0(y), you can upgrade the module remotely using a [ZIP file](#)^[33] or using a USB2 memory key as below. However, to upgrade from a different release, for example from 8.0 or 8.1 to 9.0, you must use an ISO file as below.

- **! 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. Some releases include changes that require additional steps.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading.

Process Summary

Once the IP Office system has been upgraded to the target release, for example 9.0, use the following process to upgrade the module to the same release.

1. **Download the software**

Download the ISO file and **unetbootin** software. See [Downloading Module Software](#)^[16].

2. **Backup the applications**

Backup the Voicemail Pro and one-X Portal for IP Office applications to a location other than the module. Refer to the separate documentation for the applications.

3. **Prepare the USB2 upgrade key**

Using the **unetbootin** software, create a bootable USB2 upgrade key loaded with the files from the downloaded ISO file. See [Preparing a USB2 Upgrade Key](#)^[36].

4. **Reboot the module**

Reboot the module from the USB2 upgrade key and let the module upgrade. See [Booting from a USB2 Upgrade Key](#)^[37].

5. **Check operation**

3.8.2.1 Preparing a USB2 Upgrade Key

This process uses a downloaded ISO file to create a bootable USB2 memory key for software upgrading. Using this device installs the software without, overwriting any existing software and data on the server.

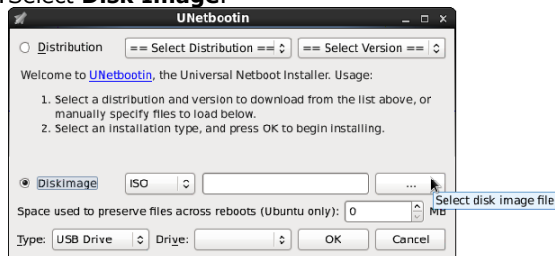
- **! Upgrade Warning**
Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.
- **! Backup Application Data**
In all cases, always backup all application data to a separate location before upgrading.

Prerequisites

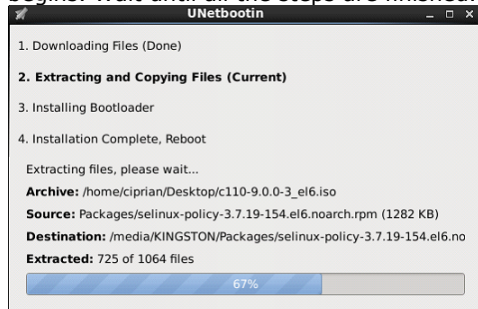
- **8GB USB2 Memory Key**
Note that all existing files on this device will be erased.
- **UNetBootin software**
This additional software is downloadable from <http://unetbootin.sourceforge.net>. You use it to load an .iso image onto a USB memory key from which the server can boot.
- **Unified Communications Module ISO File**
You can download this software from the Avaya support website (<http://support.avaya.com>).

To create a bootable USB2 memory key:

1. Erase all files on USB2 memory key and reformat it as a FAT32 device.
2. Start the **unetbootin** application.
3. Select **Disk Image**.



4. Click the ... browse button and select the ISO file.
5. Click **OK**. If a warning appears announcing that all data from the USB2 memory key will be lost, click **Yes** to all. The process of transferring files from the ISO image to the USB2 memory key and making that device bootable begins. Wait until all the steps are finished.



6. When the process has ended, click **Exit**. Do not click **Reboot now**.
7. Using the file explorer, open the USB folder on the USB2 memory key.
8. A number of files need to be copied to a new location on the USB2 memory key:
 - If upgrading within a release, for example from 9.0.x to 9.0.y, select the files **syslinux.cfg** and **avaya_autoupgrade.conf** and copy them to the top level (root) folder, overwriting any existing files with those names.
 - If installing a new release, for example from 8.0 or 8.1 to 9.0, select the files **syslinux.cfg** and **avaya_autoinstall.conf** and copy them to the top level (root) folder, overwriting any existing files with those names.
9. Remove the USB2 memory key from the PC. The device is ready for use for software upgrade.

3.8.2.2 Booting from a USB2 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. Some releases include changes that require additional steps.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading.

To upgrade from a USB2 memory key:

1. Prepare a bootable USB2 upgrade key. See [Preparing a USB2 Upgrade Key](#)^[36].
2. Remove the plastic cover from the front of the faceplate of the card. You must retain this cover and reattach it after completing this process.
 - We recommend connecting a monitor using an HDMI to HDMI cable or HDMI to DVI cable. This allows you to monitor the process and to confirm when it is completed.
3. Check that you have obtained backups of all application data (one-X Portal for IP Office, Voicemail Pro) from the module if it is already from an operating customer system.
4. Insert the USB2 memory key with the new image file into one of the USB ports located on the front of the module.
5. Shut down the module by pressing the upper button on the module until the lower LED starts to flash green. The shutdown is complete once all module LEDs are off except for regular (every 5 seconds) IP Office heartbeat amber flashes of the lower LED.
6. Restart the module by pressing the upper reset button again and keeping it pressed until the top two LEDs change from orange to off.
7. The module will reboot using the image files on the USB2 memory key.
8. After approximately 2 minutes, the top two LEDs change to alternately flashing green. The lower LED remains steady green. This installation process takes approximately 45 minutes.
9. After the software installation completes, the module restarts. During the restart, if necessary, the module's firmware is upgraded. The restart, including firmware upgrade, takes approximately 3 minutes. After this the upper 2 LEDs are off and the lower LED indicates the module's status as follows:
 - **Lower status LED shows only regular IP Office heartbeat flashes:**
This indicates that a firmware upgrade occurred after which the module automatically shutdown.
 - a. Remove the USB2 memory key. Remove any monitor connection.
 - b. Restart the module by press the top button or [using System Status Application](#)^[39].
 - **Lower status LED green with regular IP Office heartbeat flashes:**
This indicates that the module restarted without needing a firmware upgrade.
 - a. Remove the USB2 memory key. Remove any monitor connection.
10. Refit the plastic cover removed at the start of the process.

3.9 The Module Battery

The Unified Communications Module includes a Lithium coin cell battery. If the module is no longer required, you remove and dispose of the battery correctly. You can remove the battery by bending the tab out the way and then pulling the battery upwards.

- **! WARNING: Card Remains Hot After System Shutdown**

When removing a Unified Communications Module from a system, take care not to touch the heat sink on the module. The heat sink remains hot for a long period after system shutdown.

- **! WARNING:**

There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the local instructions for recycling and disposal of batteries.

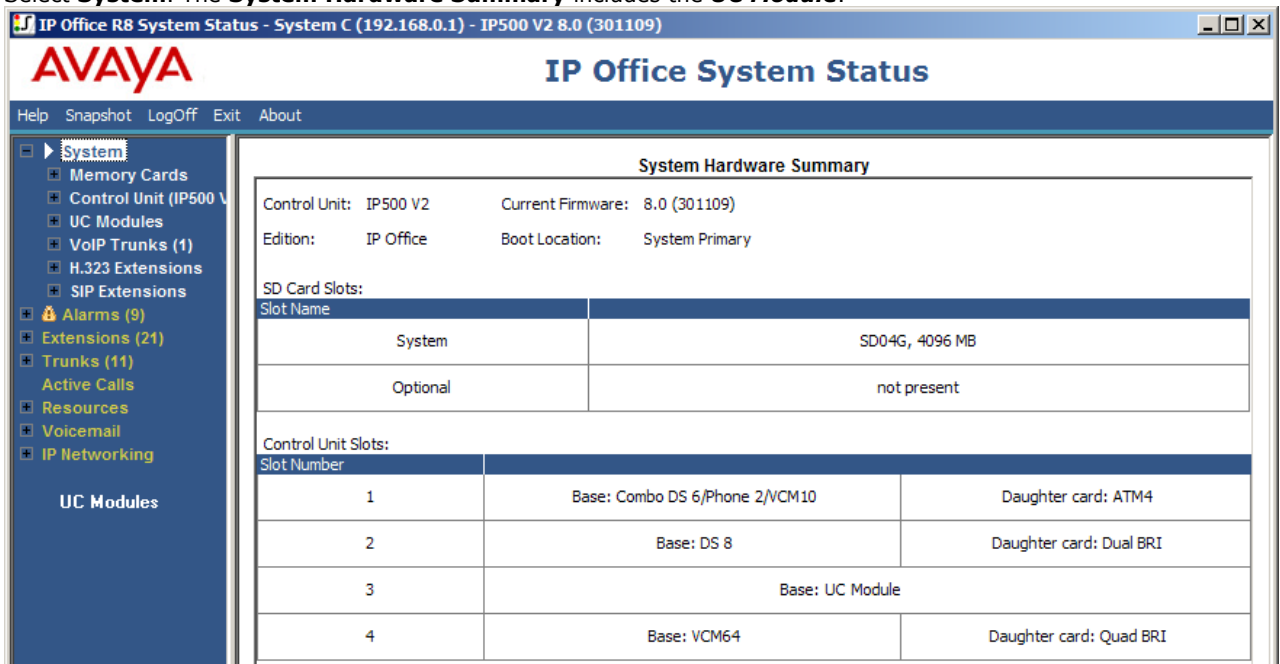


3.10 Using System Status Application

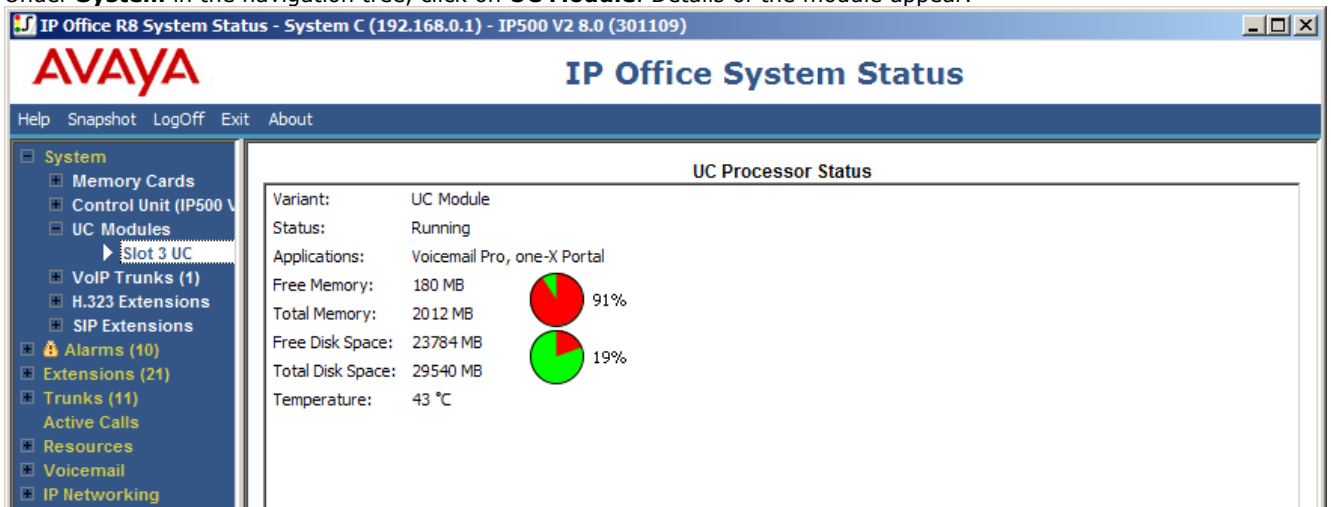
System Status Application displays the status of the Unified Communications Module.

To check a Unified Communications Module using System Status Application:

1. Using System Status Application, access the system.
2. Select **System**. The **System Hardware Summary** includes the **UC Module**.



3. Under **System** in the navigation tree, click on **UC Module**. Details of the module appear.



Chapter 4.

Voicemail Pro Configuration

4. 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. This section of this manual covers only the minimum steps recommended to ensure that the voicemail server is operating correctly and is secure. Those are:

Voicemail Pro Initial Configuration

a. IP Office Configuration

- i. [Adding voicemail licenses](#) ^[43].
- ii. [Check the Voicemail Type Setting](#) ^[44].

b. Voicemail Pro Configuration

- i. [Install the Voicemail Pro client](#) ^[45].
- ii. [Log in to the Voicemail Pro server](#) ^[46].
- iii. [Change the default administrator password](#) ^[46].

IMPORTANT: Voicemail IP Address Note

The IP address 169.254.0.2 is used for internal connected between the IP Office system and the voicemail application on the Unified Communications Module. This is the address that should be [set for the voicemail server](#) ^[44] in the IP Office configuration. This address should not be used for any other purpose such as external access to the voicemail server application. For all other access to the voicemail server from elsewhere on the network, the IP address of the Unified Communications Module should be used. To check the IP address, see [Viewing the Module IP Address](#) ^[32].

Transferring Settings from a Previous Server

If the IP Office system was already configured to operate with an external Voicemail Pro server that is now being replaced, the settings, prompts and messages on the old server can be transferred to the new server. After completing the steps above, see [Transferring Voicemail Server Settings](#) ^[48].

Notes

For use of UMS options, the Voicemail Pro service needs to communicate with a MAPI proxy application installed on a Windows PC. The installation package for the MAPI proxy can be downloaded from the server's [Windows Client](#) ^[100] menu. For full details refer to the Voicemail Pro Linux Installation manual.



4.1 Adding Voicemail Licenses

The Unified Communications Module automatically enables 4 port for Voicemail Pro operation. Additional ports can be licensed for up to 20 users when running Voicemail Pro and one-X Portal for IP Office, or up to 40 when running just Voicemail Pro.

For Voicemail Pro operation on Unified Communications Module, the following licenses are used:

- **Essential Edition**
This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
The Voicemail Pro application normally requires this license. For the Unified Communications Module, the module acts as an automatic **Preferred Edition** license for the system. This enables 4 voicemail ports.
- **Preferred Edition Additional Voicemail Ports**
These licenses add additional voicemail ports in addition to the 4 enabled by the presence of the Unified Communications Module. You can add multiple licenses, up to 20 ports when running Voicemail Pro and one-X Portal for IP Office, or 40 ports when running just Voicemail Pro.
- **User Profile Licenses**
In order to log into and use the one-X Portal for IP Office application, a user must be configured and licensed to one of the following user profile roles in the IP Office configuration: **Office Worker**, **Teleworker** or **Power User**. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

To enter licenses:


1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **License**.
3. Click **Add** and select **ADI**.
4. Enter the new license and click **OK**. You should add licenses by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.
5. The **Status** of the new license should show **Unknown** and the name the license should match the type of license entered. If the name shows as **Invalid**, the most likely cause is incorrect entry of the license key characters.
6. Click on the  save icon to send the configuration back to the IP Office.
7. Use Manager to receive the configuration again and check that the status of the license. It should now be **Valid**.

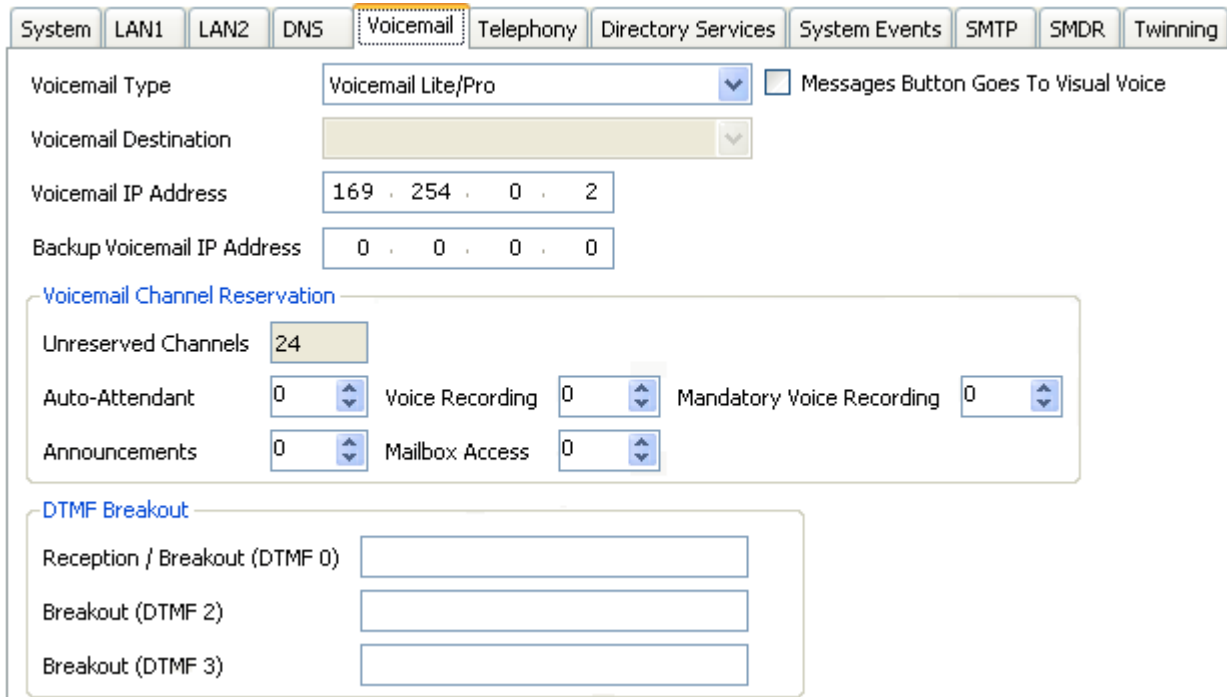
4.2 IP Office Configuration

When a new Unified Communications Module running Voicemail Pro is added to a new system, the system configuration is automatically adjusted to use that voicemail server. However, this should be confirmed by checking the **Voicemail Type** and Voicemail IP Address settings in the IP Office configuration. If the switch has previously been configured for a specific voicemail server address, those settings are not automatically changed and need to be manually updated.

If a different role is intended for the voicemail server (see [Small Community Networks](#)^[11]), refer to the Voicemail Pro Installation Manual. This section only covers voicemail server support for the IP Office in which it is installed.

To set the voicemail server address:

1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **System**.
3. Select the **Voicemail** tab.



The screenshot shows the configuration interface for the Voicemail tab. The tabs at the top are System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and Twinning. The Voicemail tab is selected. The configuration fields are as follows:

- Voicemail Type:** Voicemail Lite/Pro (dropdown menu)
- Voicemail Destination:** (empty dropdown menu)
- Voicemail IP Address:** 169 . 254 . 0 . 2
- Backup Voicemail IP Address:** 0 . 0 . 0 . 0
- Voicemail Channel Reservation:**
 - Unreserved Channels:** 24
 - Auto-Attendant:** 0
 - Voice Recording:** 0
 - Mandatory Voice Recording:** 0
 - Announcements:** 0
 - Mailbox Access:** 0
- DTMF Breakout:**
 - Reception / Breakout (DTMF 0):** (empty text box)
 - Breakout (DTMF 2):** (empty text box)
 - Breakout (DTMF 3):** (empty text box)

- The **Voicemail Type** should be set to **Voicemail Lite/Pro**.
- **! WARNING: IP Address**
The **Voicemail IP Address** of 169.254.0.2 is the [internal IP address](#)^[11] used for connection between the IP Office and the Unified Communications Module. This is the only address that should be used and should not be changed.
- In the **Voicemail Channel Reservation** section, the number of channels will be 4 plus any additional channels licensed. The Unified Communications Module can be licensed for up to 20 ports.

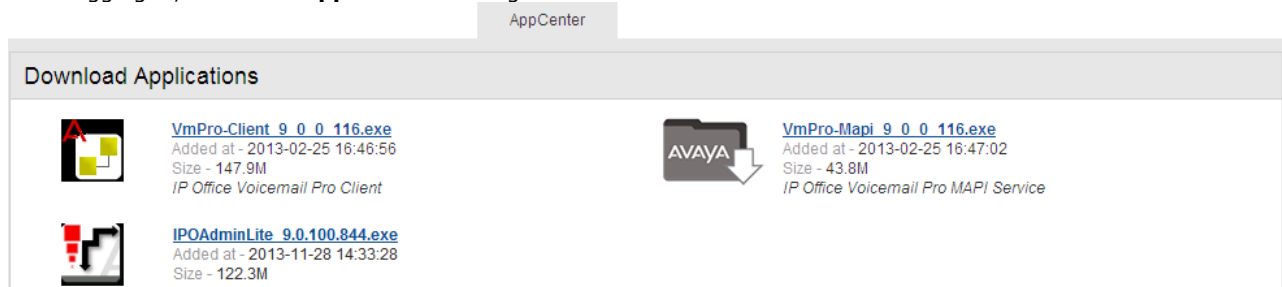
4. If any changes have been made, save the changes back to the IP Office system.

4.3 Installing the Voicemail Pro Client

The client for the Voicemail Pro server must be installed on a Windows PC. It can then be used to remotely administer the voicemail server. The software package for installing the client can be downloaded from the Unified Communications Module using the following process.

To download and install the Voicemail Pro client:

1. Login to the server's web control menus. See [Logging In Directly](#) ⁶³.
2. After logging in, select the **AppCenter** heading.



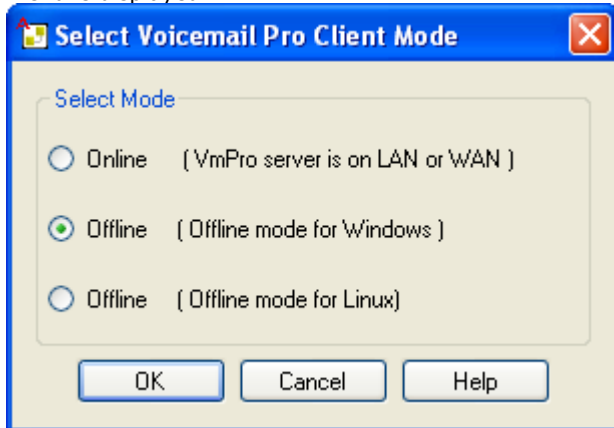
3. Click on the link for the Voicemail Pro client file in order to download the software package for installing the client.
4. Once the package has been downloaded, run it to install the Voicemail Pro client.

4.4 Logging in to the Voicemail Server

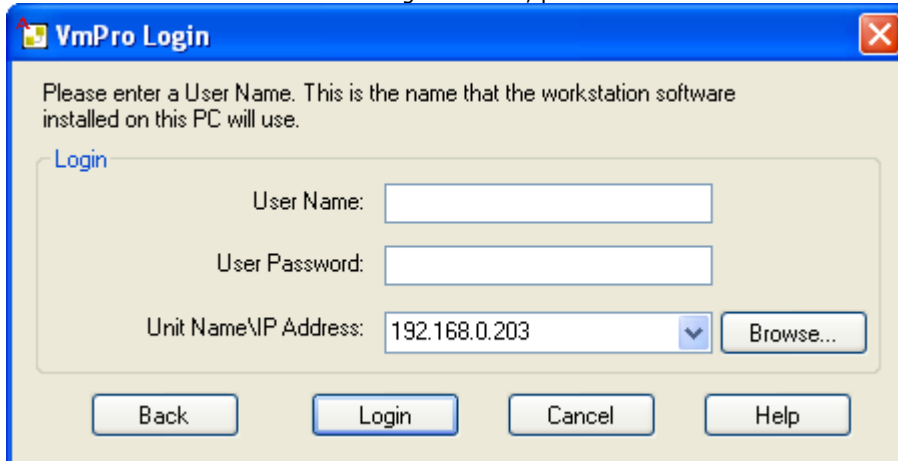
To connect to a remote voicemail server you will need to login using the name and password of an administrator account already configured on that server. The default account is **Administrator** and **Administrator**.

To login with the Voicemail Pro client:

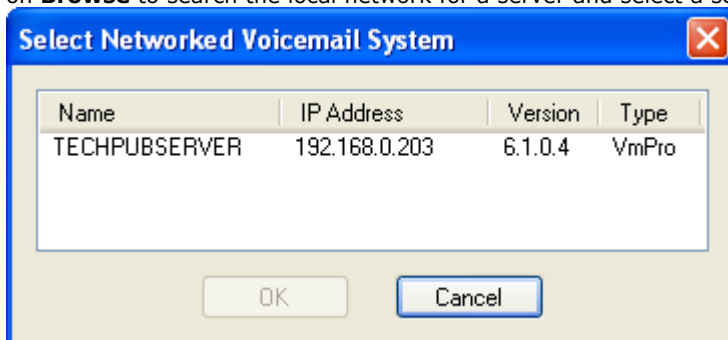
1. From the **Start** menu, select **Programs | IP Office | Voicemail Pro Client**.
2. The Voicemail Pro Client window opens. If the client has been started before, it will attempt to start in the same mode as it previously used. If it cannot do that or it is the first time the client has been started, the select mode menu is displayed.



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



4. Enter the **User Name** and **User Password** for an administrator account on the voicemail server. The default account is **Administrator** and **Administrator**.
5. In the **Unit Name\IP Address** field enter the DNS name or IP address of the voicemail server. Alternatively click on **Browse** to search the local network for a server and select a server from the results.



6. Click Login. Note that if 3 unsuccessful logins are attempted using a particular administrator account name, that administrator account is locked for an hour.
7. The following menu may appear. Select **Download**.
8. You should now [change the password](#) ⁴⁷.

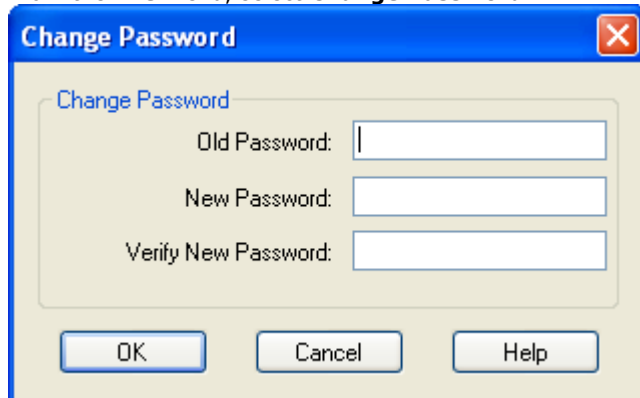
4.5 Changing the Voicemail Server Password

While logged in to the server using the Voicemail Pro client, you can change the password of the Voicemail Pro administrator account being used. The default password of the default account must be changed.

You can also create additional administrator accounts, refer to the Voicemail Pro Administrator manual.

To change the Voicemail Pro Administrator password:

1. From the **File** menu, select **Change Password**.



2. In the **New Password** box, type the new password.
3. In the **Confirm Password** box, retype the new password.
4. Click **OK**.

4.6 Transferring Voicemail Server Settings

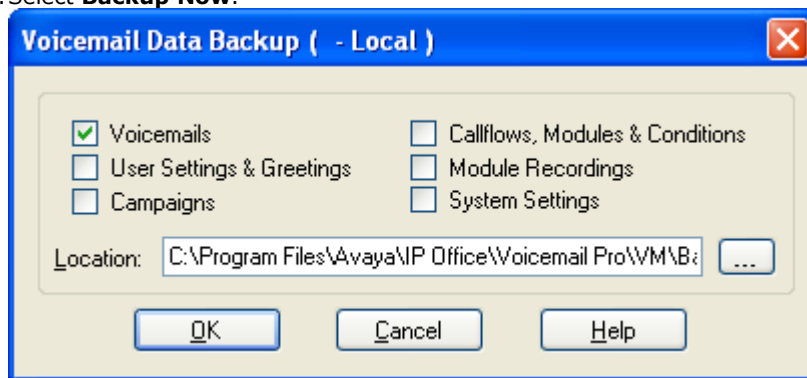
If the Unified Communications Module is replacing an existing voicemail server, a backup of all the settings, prompts and messages from that server can be transferred to the new server. If the existing server is a Linux based server, SSH file transfer is used to retrieve the backup files from the server. Otherwise, if Windows based, a direct folder copy on the server can be used.

For the Unified Communications Module, once a backup of the old server has been obtained, it can be loaded onto the Unified Communications Module from a USB2 memory key. Otherwise, if the backup is too large for the USB2 memory key, SSH file transfer can be used.

To back up the old voicemail server:

A full immediate backup of all the voicemail server settings, prompts and messages can be obtained using the Voicemail Pro client.

1. Connect to the old voicemail using the Voicemail Pro client.
 - **Hint:** The option **File | Voicemail Shutdown | Suspend Calls** can be used to display the number of currently active voicemail sessions. If necessary you can use the menu to stop any new sessions or to force the end of all sessions before taking the backup.
2. Select **Preferences | General**. Select the **Housekeeping** tab.
3. Select **Backup Now**.



4. Select all the backup options for a complete backup and click **OK**. 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**.
5. The time to complete the backup will vary greatly depending on the number of mailboxes and messages being supported by the server.

To shut down the old voicemail server:

Once the server has been backed up, it should be shutdown. This will release all the licenses it has currently obtained from the IP Office system.

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

To transferring the backup to a USB2 memory key:

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

• Windows Server

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

1. Using **My Computer**, locate the manual backup taken above. The date and time is part of the folder name for the backup.
2. Right-click on the folder and select **Properties**. Check that the Size on disk is within the capacity of the USB2 memory key.
 - If not, copy the backup folder and all its contents onto a PC from which you can eventually load it onto the new server using an SSH file transfer.
 - If with the USB2 memory key capacity, Copy the backup folder and all its content onto a USB2 memory key. Do not put the folder into another folder or change the folder name.

• Linux Server

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

1. Using an [SSH file transfer tool](#)^[105], connect to the old server and browse to is **/opt/vmpro/Backup/Scheduled/OtherBackups**.

2. Locate the manual backup taken above. The date and time is part of the folder name for the backup.
3. Copy the folder and all its contents onto the PC running SSH.
4. Right-click on the folder and select **Properties**. Check that the Size on disk is within the capacity of the USB2 memory key.
 - If not, copy the backup folder and all its contents onto a PC from which you can eventually load it onto the new server using an SSH file transfer.
 - If with the USB2 memory key capacity, Copy the backup folder and all its content onto a USB2 memory key. Do not put the folder into another folder or change the folder name.

To loading the backup onto the new server from a USB2 memory key:

If you were able to load the voicemail backup onto a USB2 memory key, you can load it onto the Unified Communications Module server directly from the USB2 memory key.

1. Insert the USB2 memory key into one of the Unified Communications Module's USB sockets.
2. Using a web browser, login to the server's web control menus.
3. Select **Settings**. On the **General** tab, select the **Restore** button for the Voicemail service. The list of available backups will include the one on the USB2 memory key.
6. Select the backup on the USB2 memory key and click **OK**.
7. Do not remove the USB2 memory key until all USB2 memory key activity has ceased.
8. Once the restore has been completed, on the **System** menu, **Stop** and then **Start** the voicemail service.

To loading the backup onto the new server using SSH:

If the backup has been copied onto a PC as it is too large to be loaded from a USB2 memory key, use the following method to transfer and then restore the backup.

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

4.7 ContactStore

IP Office Release 8.1 Feature Pack 1 and higher supports the use of a Windows based ContactStore for IP Office server with a Linux based Voicemail Pro server. In order to operate, the Linux based voicemail server automatically transfers recordings to a folder on the Windows ContactStore server using SFTP. The ContactStore application is configured to monitor and collect any recordings that appear in that folder and add them to its recordings database.

The voicemail server configuration is done through the **Voicemail Recording** tab (**Preferences | General**) of the Voicemail Pro client. The tab specifies the path and user name/password details for SFTP file transfers to a folder on the ContactStore server. This requires the ContactStore server to have an SFTP application running in order to receive files from the Linux based voicemail server. The tab appears in the Voicemail Pro client only when connected to a Linux based voicemail server. Refer to the Voicemail Pro administration manuals for details.

The ContactStore configuration is done through the usual Windows registry settings of the ContactStore application. The registry path for the applications VRL directory (**HKEY_LOCAL_MACHINE | SOFTWARE | Network Alchemy | Voicemail | Directories | VRLDir**) needs to be set to match the SFTP application folder on the ContactStore server to which the Linux based voicemail server has been configured to send recordings. Refer to the ContactStore installation manual.

For IP Office Release 9.0, instead of Windows based ContactStore for IP Office, an equivalent application called Contact Recorder for IP Office can be run on an IP Office application server.

4.8 Backup/Restore Limitations

If extra folders have been manually created on the voicemail server, on Linux based voicemail servers these folders are not included in the restore process. Instead, the extra folders need to be copied manually.

For example, if a folder containing custom prompts for use in call flows has been created separate from the default language folders, that custom prompts folder is not backed up or restored.

To resolve this, the extra folders must be backed up and restored manually. In the following example, a folder **Custom** is manually copied from an existing server to create a backup. It is then manually restored.

To manually backup a custom folder:

1. Using an [SSH file transfer tool](#)^[105], copy the folder **Custom** from **/opt/vmpro** to your PC to create a backup of the folder.

To manually restore a custom folder:

1. To restore the folder, again using an SSH file transfer tool, copy the folder to the **/home/Administrator** folder on the server.
2. Using the SSH command line, you now need to copy the **Custom** folder from **/home/Administrator** to the **/opt/vmpro** folder. This is done by logging in as the root user.
 - a. Login to the system's command line interface using the existing root user password. This can be done either directly on the server or remotely using an SSH client shell application.
 - **If logging in on the server:**
 - a. At the **Command:** prompt, enter **login**.
 - b. At the **login:** prompt enter either **Administrator** or **root**.
 - c. At the **Password:** prompt, enter the password for the user entered above.
 - d. To launch the Avaya command line interface, enter **/opt/Avaya/clish**.
 - **If logging in remotely:**
 - a. Start your SSH shell application and connect to the Unified Communications Module PC. The exact method will depend on the application being used.
 - The **Host Name** is the IP address of the Unified Communications Module.
 - The **User Name** is **web**.
 - The **Protocol** is **SFTP/SSH**.
 - The **Port** is **22**. If this is the first time the application has connected to the server, accept the trusted key.
 - b. If this is the first time the application has connected to the Unified Communications Module, accept the trusted key.
 - c. When prompted, enter the webcontrol user [password](#)^[64], the default is **webcontrol**.
 - b. Enter **admin**. At the password prompt enter the admin password, the default is **Administrator**. The prompt should change to **Admin>**.
 - c. Enter **root**. At the password prompt, enter the current root user password.
 - d. The prompt should have changed to something similar to **root@C110~**, indicating that you are now logged in as the root user.
 - e. Change directory by entering **cd /home/Administrator**.
 - f. Move the **Custom** sub-folder to **/opt/vmpro** by entering **mv Custom /opt/vmpro**.
3. Using the SSH file transfer tool again, verify that the **Custom** has been copied to **/opt/vmpro** as required.

Chapter 5.

one-X Portal for IP Office Configuration

5. one-X Portal for IP Office Configuration

At this stage, the one-X Portal for IP Office server software has been installed on the server and its service started. However, both the IP Office and the one-X Portal for IP Office services still require some basic configuration. The following sections are a summary applicable to most installations. For full details of one-X Portal for IP Office installation refer to the one-X Portal for IP Office Installation Manual.

one-X Portal for IP Office Initial Configuration

a. [Add licenses](#) ^[54]

Those IP Office users who want to use the one-X Portal for IP Office application need to have their **Profile** set to **Office Worker**, **Teleworker** or **Power User** and the **Enable one-X Portal Services** option selected. To do this requires the addition of licenses for those roles.

b. [Enable one-X Portal for IP Office users](#) ^[55]

When licenses are available, the number of licenses allows the configuration of the equivalent number of users for those roles and then for one-X Portal for IP Office usage.

c. [Initial one-X Portal for IP Office login](#) ^[56]

Having licensed and configured some users for one-X Portal for IP Office, you need to login as the one-X Portal for IP Office administrator in order to perform initial one-X Portal for IP Office configuration.



d. [Initial AFA login](#) ^[57]

The one-X Portal for IP Office AFA interface is used for remote backup and restoration of the application. At minimum you should login in order to change the default password for the interface.

5.1 Adding Licenses

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



To enter licenses:

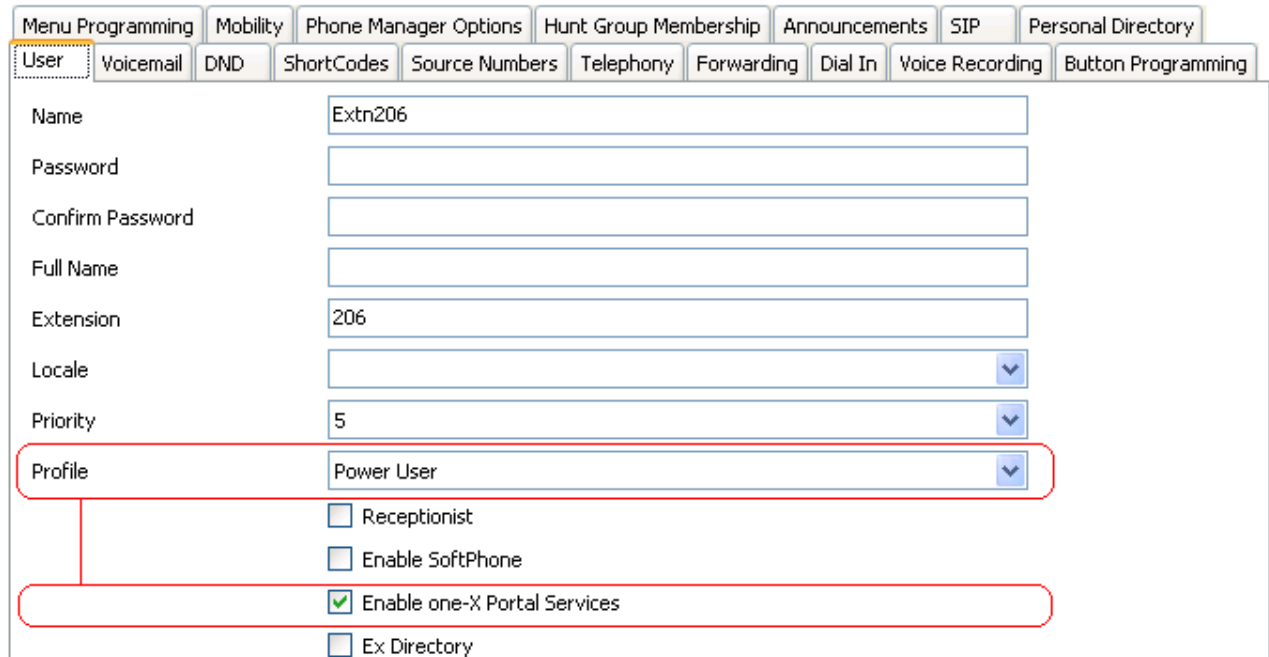
1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **License**.
3. Click **Add** and select **ADI**.
4. Enter the new license and click **OK**. You should add licenses by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.
5. The **Status** of the new license should show **Unknown** and the name the license should match the type of license entered. If the name shows as **Invalid**, the most likely cause is incorrect entry of the license key characters.
6. Click on the  save icon to send the configuration back to the IP Office.
7. Use Manager to receive the configuration again and check that the status of the license. It should now be **Valid**.

5.2 Enabling one-X Portal for IP Office Users


Those users who want to use the one-X Portal for IP Office application need to have their **Profile** set to **Office Worker**, **Teleworker** or **Power User** and the **Enable one-X Portal Services** option selected. This requires [available licenses](#) ⁵⁴ for those roles.

To enable one-X Portal for IP Office users:

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



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

6. Change the user's **Profile** to **Office Worker**, **Teleworker** or **Power User**.
7. Check that the **Enable one-X Portal Services** check box is selected.
8. Note the user **Name** and **Password**. These are used by the user to login to one-X Portal for IP Office.
10. Repeat the process for any other users who will be using one-X Portal for IP Office services.
11. Click on  to save the updated configuration back to the IP Office system.

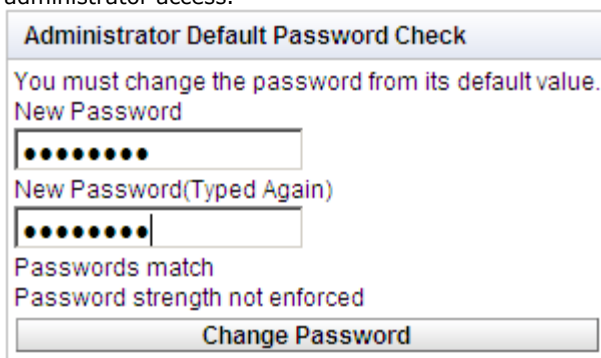
5.3 Initial one-X Portal for IP Office Login

The method of initial one-X Portal for IP Office configuration may vary:

- If both one-X Portal for IP Office and Voicemail Pro applications were selected as part of a module initialization, no further configuration is required. The applications and the IP Office are defaulted to interoperate. When you log into the one-X Portal for IP Office administration using the process below, you will be taken directly to the final step, changing the one-X Portal for IP Office administrator password.
- If the one-X Portal for IP Office is to also support additional IP Office servers in a [Small Community Network](#)^[11], after initial configuration as above, the process for adding additional IP Office systems must be used to add the other system. Refer to the one-X Portal for IP Office Installation Manual.

To login to one-X Portal for IP Office:

1. Open a web browser and enter the IP address of the Unified Communications Module followed by **:8080/onexportal-admin.html**. This is the login path for the administrator access to the one-X Portal for IP Office application.
2. The login menu is displayed. If the message **System is currently unavailable - please wait** is displayed, the one-X Portal for IP Office application is still starting. When the message disappears, you can login.
3. Enter the default administrator name (**Administrator**) and password (**Administrator**) and click **Login**.
4. As the final step, the one-X Portal for IP Office server will prompt you to change the password used for administrator access.



5. Enter a new password and click **Change Password**.
6. You now have access to the one-X Portal for IP Office administration menus. For full details refer to the one-X Portal for IP Office Administration manual.
7. Click on **Log Out**.
8. Click on **User Login** shown top-right.
9. The login window will display **System in currently unavailable**. When this message is no longer displayed, attempt to login as a user.

5.4 Initial AFA Login

The AFA menus provided by one-X Portal for IP Office are used to perform backup and restoration operations for the application. The default password used for the menus should be changed.

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

1. Open a web browser and enter the IP address of the Unified Communications Module followed by **:8080/onexportal-afa.html**. This is the login path for the administrator access to the one-X Portal for IP Office AFA menus.
2. At the login menu, enter the name Superuser and the associated password. The default password is MyFirstLogin1_0. After logging with the default password you will be prompted the following information including a new password:
 - **Display Name**
Enter a name for display in the one-X Portal for IP Office menus.
 - **Password/Confirm Password**
Enter a password that will be used for future access.
 - **Backup Folder**
This is the path to be used for backup and restore operations on the one-X Portal for IP Office server. Note that even if backing up and restoring to and from an FTP or local PC folder, this server folder is still used for temporary file storage.

5.5 Transferring one-X Portal for IP Office Settings

If the Unified Communications Module is replacing an existing one-X Portal for IP Office server, a backup of all the one-X Portal for IP Office settings can be transferred to the new server. The backup is obtained from the old server via web browser access. Web browser access to the new server is then also used to reload the same backup.

The backup and restore process can use either an intermediate FTP file server or can use files downloaded and restored to and from the browsing PC.

The one-X Portal for IP Office includes the IP addresses of the voicemail server and IP Office systems in the backed up one-X Portal for IP Office settings. However, the Unified Communications Module uses a different set of internal [IP addresses](#)^[11] for its voicemail server and IP Office connections. Therefore, after restoring the backup on the new server, the one-X Portal for IP Office provider IP addresses need to be changed.

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

The backup process will create a zip file with the date and time also added to the selected file name of the zip file.

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

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

Once a backup file has been obtained, a similar process can be used to load it onto the new server.

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

To reconfigure the restored settings:

The Unified Communications Module uses a number of internal [IP addresses](#)^[11] for connections between the IP Office system and the applications it hosts. Any one-X Portal for IP Office settings restored from another server must be reconfigured to use the internal IP addresses.

1. Browse to the new server using the address ***http://<server>:8080/onexportal-admin.html*** where *<server>* is the IP address of the Unified Communications Module.
2. Login with the administrator name and password.
3. Select Configuration and then Providers.
4. Click **Get All** to load the provider details from the one-X Portal for IP Office.
5. Click the **Edit** button next to the **Voicemail_Provider**.
 - a. Click **Voicemail Server Assigned**.
 - b. Change the existing **Voicemail Server IP Address** to **169.254.0.2** and click **Close**.
6. Click the **Edit** button next to the **Default-CSTA_Provider**.
 - a. Click **IP Office(s) Assigned**.
 - b. Change the existing **IP address** to **169.254.0.1** and click **Close**.

7. Click the **Edit** button next to the **Default-DSML-IPO-Provider**.
 - a. Click **IP Office(s) Assigned**.
 - b. Change the existing **IP address** to **169.254.0.1** and click **Close**.
8. Click the checkbox next to **ID** to select all the records. Click **Put Selected**.

Chapter 6.

Server Maintenance

6. Server Maintenance

The main configuration and control of the Unified Communications Module is done via web browser access. After logging in using the administrator name and password, you are able to view the status of the services provided by the server and to perform actions such as stopping or starting those services.

- [Changing the Web Password](#) ⁶⁴
- [Changing the Root Password](#) ⁶⁵
- [Starting/Stopping Application Services](#) ⁶⁶
- [Server Shutdown](#) ⁶⁷
- [Rebooting the Server](#) ⁶⁷
- [Changing the IP Address Settings](#) ⁶⁸
- [Date and Time Settings](#) ⁶⁹
- [Setting the Menu Inactivity Timeout](#) ⁷⁰
- [Upgrading an Application](#) ⁷¹
- [Uninstalling an Application](#) ⁷³
- [Setting Update Repositories](#) ⁷⁴

6.1 Logging In Directly

Use the following method to browse to and login to the web control menus of the Linux server running on the Unified Communications Module.

Avaya supports the following web browsers:

- Microsoft Internet Explorer 8 or higher with JavaScript enabled.
- Mozilla Firefox with JavaScript enabled.

To login to the server web control menus:

1. From a client PC, start the browser. Enter **http://** followed by the address of the Unified Communications Module and **:7070**. If the IP address is unknown, see [Viewing the Module IP Address](#)^[32].
2. Select the **Language** required.



Avaya IP Office Unified Communications Module R9.0

Linux release 6.3 (Final)

Please log on.

Logon:

Password:

Language:

[Change password](#)

© 2013 Avaya Inc. All rights reserved - [View EULA](#)

3. Enter the name and password for Unified Communications Module administration. To change the password, select the [Change Password](#)^[64] option.
 - The default name and password for Release 8.0 are **web** and **webcontrol**.
 - The default name and password for Release 8.1 or higher are **Administrator** and **Administrator**.
4. If the login is successful, the server's [System](#)^[81] page appears.

6.2 Changing the Web Password

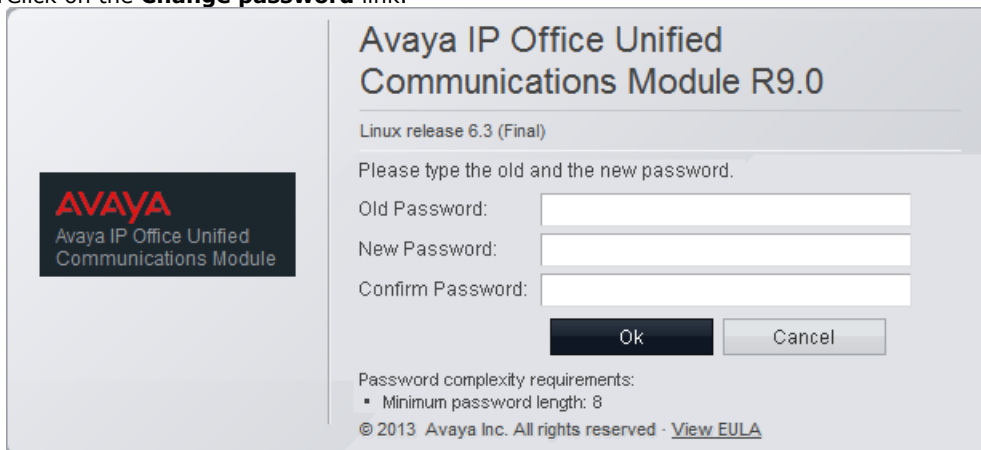
Following [ignition](#)^[20], you should change the web password from its default.

To change the browser password:

1. From a client PC, start the browser. Enter **http://** followed by the address of the Unified Communications Module and **:7070**. If the IP address is unknown, see [Viewing the Module IP Address](#)^[32].
2. Select the **Language** required.



3. Click on the **Change password** link.



4. Enter the current password and the new password. The new password must meet the complexity requirements displayed on the menu.
5. Click **OK**. The menu confirms whether the change was successful or not. If the new password is accepted, click **Cancel** to return to the **Login** menu. .

6.3 Changing the Root Password

The root password for the server is set during the server installation. This is a password used for Linux command line access and so is not normally used during normal operation. However, for security you can change the root password through the web control menus.

To change the server root password:

1. [Login](#) to the server's web configuration pages.
2. Select **Settings** and click on the **System** tab.
3. The new root password is set through the **Change Root Password** menu.

Change root Password	New Password: <input type="text"/>	Password complexity requirements: <ul style="list-style-type: none">• Minimum password length:8• Maximum allowed sequence length:4	Save
	Confirm New Password: <input type="text"/>		

- **New Password**
Enter the new password for the server's root account.
- **Confirm New Password**
Confirm the new password.

4. Enter the new password.
5. Click **Save**. The menu will confirm if the new password was accepted.

6.4 Starting/Stopping Application Services

The application services installed on the Unified Communications Module can be started and stopped individually. This may be necessary for maintenance or if a particular service is not currently required, for example if one-X Portal for IP Office has been installed but is not wanted or currently licensed.

The services can be set to automatically start after a server reboot. By default all the application services are automatically started.

6.4.1 Starting a Service

To start a service:

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

6.4.2 Stopping a Service

To stop a service:

1. [Login](#) to the server's web configuration pages.
2. Select **System**. The services and their current status (running or stopped) are listed.
3. To start 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 while it is being stopped. If it remains in this state too long, the service can be forced to stop by clicking on **Force Stop**.

6.4.3 Setting a Service to Auto Start

By default all the application services are automatically started.

To set a service to auto start:

1. [Login](#) to the server's web configuration pages.
2. Select **System**. The services and their current status (running or stopped) are listed.
3. Use the **Auto Start** check box to indicate whether a service should automatically start when the Unified Communications Module is started.

6.5 Server Shutdown

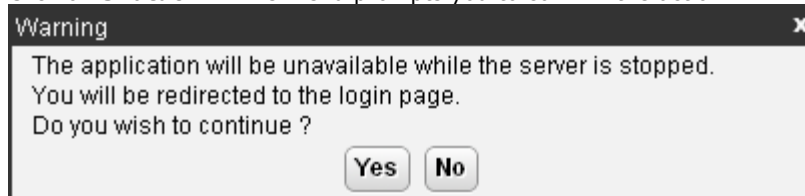
Use this process when it is necessary to switch off the Unified Communications Module for any period. For the Unified Communications Module, the module can be shutdown or started up using the upper switch on its front panel. See [Module Buttons](#) ^[31].

- **! WARNING**

If the module is being shutdown in order to remove it from the system, you must also [shutdown the IP Office system](#) ^[18].

To shutdown the server:

1. [Login](#) ^[63] to the server's web configuration pages.
2. After logging in, select the [Home](#) ^[81] page.
3. Click on **Shutdown**. The menu prompts you to confirm the action.



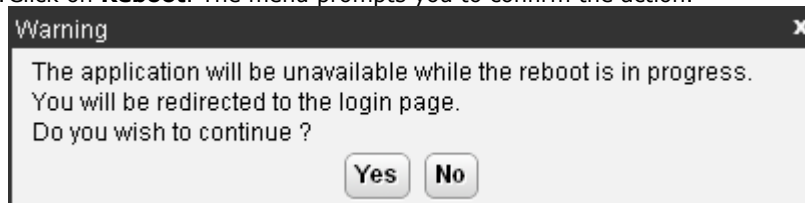
4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 2 minutes, the server shuts down.

6.6 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](#) ^[66] automatically restart after the reboot.

To reboot the server:

1. [Login](#) ^[63] to the server's web configuration pages.
2. After logging in, select the [Home](#) ^[81] page.
3. Click on **Reboot**. The menu prompts you to confirm the action.



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

6.7 Changing the IP Address Settings

Using the server's web configuration pages, you can change the server's network settings.

- **Warning**
Changing IP address and other network settings will require you to login again.

To change the IP address:

1. [Login](#)^[63] to the server's web configuration pages.
2. Select **Settings**.
3. Select **System**.
4. Set the **Network** section as required.
 - **Network Interface**
For the Unified Communications Module this setting is fixed as **eth0.1**.
 - **Host Name**
Sets the host name that the Unified Communications Module should use. This setting requires the local network to support a DNS server. Do not use **localhost**.
 - **Use DHCP**
Do not use this setting with the Unified Communications Module.
 - **IP Address**
Displays the IP address set for the server. The Unified Communications Module connects to the system's LAN1 network system and must have an address on that subnet. See [IP Address Notes](#)^[114].
 - **Subnet Mask**
Displays the subnet mask applied to the IP address.
 - **Default Gateway**
Displays the default gateway settings for routing.
 - **System DNS**
Enter the address of the primary DNS server.
 - **Automatically obtain DNS from provider**
Not used.
5. Click **Save**. The server restarts.

6.8 Date and Time Settings

The date and time settings used by the server PC can be changed through the server's web configuration pages. The current time being used by the server is shown on the [System](#) menu.

By default the Unified Communications Module is set to use NTP with the NTP server address set to 169.254.0.1 which is the IP Office system. This requires the IP Office system to be configured to get its time from a specific external SNTP server or to have its time set manually.

To change the server date and time settings:

1. [Login](#) to the server's web configuration pages.
2. Select **Settings**.
3. Select **System**.
4. The date and time settings are shown in the **Date Time** section.
 - **Date**
Shows the current date being used by the server. If **Enable Network Time Protocol** is selected, this is the date obtained from the NTP server and cannot be manually changed.
 - **Time**
Shows the current UTC time being used by the server. If **Enable Network Time Protocol** is selected, this is the time obtained from the NTP server and cannot be manually changed. The current time being used by the server is shown on the [System](#) menu.
 - **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 is used to determine the appropriate offset that should be applied to the UTC time above. Note that changing the timezone can cause a Session expired message to appear in the browser.
 - **Enable Network Time Protocol**
If this option is selected, the Unified Communications Module will attempt to obtain the current UTC time from the NTP servers listed in the **NTP Servers** list below. It will then use that time and make regular NTP requests to update the date and time. The following options are only used if **Enable Network Time Protocol** is selected.
 - **NTP Servers**
This field is used to enter the IP address of an NTP server or servers which should be used when **Enable Network Time Protocol** is selected. 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 make sure you are aware of the usage policy for any servers you choose. Choosing several unrelated NTP servers is recommended in case one of the servers you are using becomes unreachable or its clock is unreliable. The operating system uses the responses it receives from the servers to determine which are reliable.
 - The IP Office system can also use NTP to obtain its system time. Using the same servers for the Unified Communications Module and IP Office system is recommended.
 - The default time setting for the Unified Communications Module is to use NTP with the server address set to 169.254.0.1 which is the IP Office system. When this is set, the IP Office system must be configured to get its time from an external SNTP server or to have its time set manually.
 - **Synchronize system clock before starting service**
When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, an immediate update of the server's clock to match the NTP obtained time is forced.
 - **Use local time source**
When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, the server's hardware clock time is used as the current time rather than the NTP time.
5. Click **Save**.

6.9 Setting the Menu Inactivity Timeout

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

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

To change the menu inactivity timeout:

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

6.10 Upgrading Applications

The application services hosted by the Unified Communications Module can be upgraded without having to reinstall or upgrade the whole server. This is done using files either uploaded to the server (local) or downloaded by the server from an HTTP folder (remote repository), see [File Repositories](#)^[74].

Once an .rpm file or files are available, the Unified Communications Module 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. Some releases include changes that require additional steps.

- **! Backup Application Data**

In all cases, always backup all application data to a separate location before upgrading.

The options in this section cover the upgrading of individual components of the operating system and applications supported by the Unified Communications Module.

6.10.1 Loading Application Files onto the Server

This method uploads the .rpm file for an application onto the Unified Communications Module. The files can then be used to update the applications. The alternative is to use files loaded into a [remote software repository](#)^[76].

To upload application files onto the server:

1. [Login](#)^[63] to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Applications** is selected.
4. Click on the **Browse** button and browse to the [location of the file](#)^[74] that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.

- **Voicemail Pro**

Each version of the Voicemail Pro server application is split into separate .rpm files for the server and each of the prompt languages it supports. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

6.10.2 Upgrading Application Files

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

To upgrade application files:

1. [Login](#) to the server's web configuration pages.
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 the application is currently installed. For those applications, the **Change Version** and **Update** buttons remain greyed out even if there are updates available in the application file repository. These applications must first be uninstalled using the **Uninstall** button 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 on **Change Version**. Select the version required and click **Apply**.

6.11 Uninstalling an Application

The **Updates** menu can also be used to uninstall an application service. When uninstalled the application is removed from the list of available service unless files for reinstallation are present in the configured file repository.

To uninstall an application:

1. [Login](#) ⁶³ to the server's web configuration pages.
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 available in the application [file repository](#) ⁷⁴, the button will change to become an **Install** button.
- If there are no installation files for the application available in the file repository, the application is no longer listed.

6.12 File Repositories

The [Updates](#) [88] and [Web Client](#) [100] menus use files stored in the configured file repositories. Each repository can be either a set of files uploaded to the sever or the URL of a remote folder on an HTTP server.

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  icon is displayed on the **Updates** menu.

6.12.1 Source Files

Update files may be made available individually in response to particular issues or to support new IP Office releases. The files are also included on the Unified Communications Module DVD. Files can be extracted 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. Some releases include changes that require additional steps.
- ! Backup Application Data**
 In all cases, always backup all application data to a separate location before upgrading.

		File Type	DVD/.iso Folder
Application Files	Voicemail Pro	.rpm	\avaya\vmpro
	one-X Portal for IP Office	.rpm	\avaya\oneX
Windows Client Files		.exe	\avaya\thick_clients
Operation System Files		.rpm	\Packages

- Voicemail Pro**
 Each version of the Voicemail Pro server application is split into separate .rpm files for the server and each of the prompt languages it supports. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

6.12.2 Setting the Repository Locations

The Unified Communications Module can use either remote or local software repositories to store software update files. Separate repositories are configured for operating system updates, IP Office application installation files and Windows client files.

Software Repositories			
Operating System:	<input checked="" type="checkbox"/> Local	File: <input type="text"/>	<input type="button" value="Browse"/> <input type="button" value="Add"/>
Applications:	<input checked="" type="checkbox"/> Local	File: <input type="text"/>	<input type="button" value="Browse"/> <input type="button" value="Add"/>
Downloads:	<input checked="" type="checkbox"/> Local	File: <input type="text"/>	<input type="button" value="Browse"/> <input type="button" value="Add"/>

The files uploaded or present in the file repositories are used by the [Updates](#) [88] and [AppCenter](#) [100] menus.

- Repository**
 If the **Local** option is not selected, this field is used to set the URL of a [remote HTTP file repository](#) [76]. Note that each repository must be different, the same URL must not be used for multiple repositories.
- Local**
 This checkbox is used to set whether the file repository used is local (files stored on the Unified Communications Module or remote (a folder on a HTTP web server specified in the Repository field).
- File / Browse / Add**
 If the Local option is selected, this field and adjacent buttons can be used to browse to a specific update file. When the file is located and selected, click **Add** to upload the file to the file store on the Unified Communications Module.

6.12.3 Uploading Local Files

The processes below can be used to upload files to the server if it is being used as a repository for that type of file.

6.12.3.1 Uploading Application Files

This method uploads the .rpm file for an application onto the Unified Communications Module. The files can then be used to update the applications. The alternative is to use files loaded into a [remote software repository](#)^[76].

To upload application files onto the server:

1. [Login](#)^[63] to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Applications** is selected.
4. Click on the **Browse** button and browse to the [location of the file](#)^[74] that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.
 - **Voicemail Pro**
Each version of the Voicemail Pro server application is split into separate .rpm files for the server and each of the prompt languages it supports. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

6.12.3.2 Uploading Operating System Files

This method uploads the .rpm file for an application onto the Unified Communications Module. The files can then be used to update the IP Office applications. The alternative is to use files loaded into a [remote software repository](#)^[76].

To upload operating system files:

1. [Login](#)^[63] to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Operating System** is selected.
4. Click on the **Browse** button and browse to the [location of the file](#)^[74] that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.

6.12.3.3 Uploading Windows Client Files

This method uploads the .rpm file for an application onto the Unified Communications Module. The files can then be used to update the IP Office applications. The alternative is to use files loaded into a [remote software repository](#)^[76].

To upload Windows client files:

1. [Login](#)^[63] to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Downloads** is selected.
4. Click on the **Browse** button and browse to the [location of the file](#)^[74] that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.

6.12.4 Creating Remote Software Repositories

Alternatively to using [local files uploaded to the server](#)^[74] for updates, the server can be configured to display the versions of files available for use in remote file folders hosted on an 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. If the folder is a sub-folder of the existing web site it will be browseable as part of that website's URL, ie. if the folder is a sub-folder of **wwwroot**. If the folder is on a separate path, then it must be mapped to the web server URL path, the process for this will depend on the HTTP server being used.
3. The folder directory must be browseable. For example, in IIS right -click on the folder, select **Properties** and ensure that **Directory Browse** option is selected.
4. Copy the .rpm files from their [source](#)^[74] into the folder.
5. From another PC, test that you can browse to the URL of the folder and that the list of files in the folder is displayed.
6. Login to the Unified Communications Module web configuration pages.
7. Select **Settings** and then **General**.
8. Uncheck the **Local** checkbox for **Applications**. Enter the URL of the HTTP server folder into the preceding field.
9. Click **Save**.
10. Select **Updates**.
11. 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 Unified Communications Module 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 a separate folder on the HTTP server must be used and the files placed in it are the .exe files used for installing the Windows applications.

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 will depend on the version of Linux being used on the HTTP server. Each time an .rpm file is added, deleted or changed, the directory must be updated using the **createrepo <folder_path>** command.

In order to host the repository on a Windows web server, the folder must be setup and maintained on a Linux server where the **createrepo** command can be used and the folder then copied to the Windows server.

Chapter 7.

Server Menus

7. Server Menus

The Unified Communications Module web configuration pages are as follows:

- [System](#)^[81]
This menu gives an overview of the current status of the applications hosted on the server.
- [Logs](#)^[85]
This menu has sub-menus for viewing and managing log records and log files.
 - [Debug Logs](#)^[85]
View the current log files for the server and the application services hosted by the server.
 - [Syslog Event Viewer](#)^[86]
View Syslog log records received and or generated by the server.
 - [Download](#)^[87]
Create and download archive files of existing log records.
- [Updates](#)^[88]
Display the versions of applications and components installed and the alternate versions available.
- [Settings](#)^[91]
This menu has sub-menus for various areas of server configuration and operation.
 - [General](#)^[92]
General server settings such as the locations of software update repositories.
 - [System](#)^[96]
View and manage the server setting for date, time and IP address details.
- [AppCenter](#)^[106]
This page can be used to download the installation packages for Windows applications such as the Voicemail Pro client application.

7.1 System

This menu is accessed by selecting **System**. The menu provides an overview of the server status including the status of the application services running on the server.

System

Start All Stop All

Services

Select which services will be configured to start automatically.

	Management Services	stopped	Mem/CPU usage	
<input type="checkbox"/>	9.0.0.0 build 293		0K / 0%	Start
<input checked="" type="checkbox"/>	Voicemail 9.0.0.0 build 258	UpTime 26:37	Mem/CPU usage 19552K / 2%	Stop
<input checked="" type="checkbox"/>	one-X Portal 9.0.0.0 build 418	UpTime 27:12	Mem/CPU usage 706448K / 0%	Stop

Notifications

There are no notifications available

System

Shutdown Reboot

CPU usage history

Memory Usage

used (1011.99MB)
free (1001.48MB)

Disk Usage

used (7042.29MB)
free (20998.07MB)

OS:	Linux release 6.3 (Final)
Kernel Version:	3.0.4-0.appscard.el6
UpTime:	3 days 16 hours 29 minutes
Server Time:	06:27
Average CPU Load:	0.31 (1min), 1.30 (5min), 2.19 (15min)
Processor:	Genuine Intel(R) CPU @ 1.60GHz
Speed:	1.5GHz
Cores:	2
Hard Disk Size:	27.3G
RAM:	1.9G
Disk RAID Levels:	-
Disk Array Types:	-
Virtualized:	No
Last Successful Logon:	2013-12-10 06:10:47
Unsuccessful Logon Attempts:	0

Unified Communications Module 9.0 Installation and Maintenance
IP Office 9.0

Page 81
15-601011 Issue 07I (27 January 2014)

- **Services**

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

- **Management Services**

This service is currently not used on the Unified Communications Module but is present for future development.

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

This is a web browser based application that user's 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 requires a [license](#)^[12]. The Unified Communications Module acts the **Preferred Edition** license required to run the application.

- **Voicemail Pro**

This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail. The Unified Communications Module acts as the **Preferred Edition** license required to run the application.

- **Notifications**

This table gives a summary of the most recent log messages generated by the services running on the Unified Communications Module. More detailed information is available through the [Logs](#)^[85] page.

- **System**

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

- **OS/Kernel:**

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

- **Up Time:**

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

- **Server Time:**

This field shows the current time on the server.

- **Average CPU Load:**

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

- **Speed:**

Indicates the processor speed.

- **Cores:**

Indicates the number of processor cores.

- **Hard Disk Size:**

Indicates the hard disk size.

- **RAM:**

Indicates the amount of RAM memory.

- **Disk RAID Levels:**

Indicates the RAID type, if any, being used.

- **Disk Array Types:**

Indicates the type of disk array being used for RAID.

- **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 will start a process that will stop all the application services and then shutdown Unified Communications Module. This process should be used when it is necessary to switch off the Unified Communications Module for any period. Once the process has been completed, power to the server can be switched off. To restart the server, switch the server power back on.

- **Reboot**

Selecting this button will start a process that will stop all the application services and then stop and restart the Unified Communications Module and services. Note that this stops all services. To stop and restart individual application services, use the buttons shown for each service in the **Services** panel above.

7.2 Logs

This menu is accessed by selecting **Logs**. The menu is divided into two sub-menus:

- [Debug Logs](#) ^[85]
View the current log files for the server and the application services hosted by the server.
- [Syslog Event Viewer](#) ^[86]
View Syslog log records received and or generated by the server.
- [Download](#) ^[87]
Create and download archive files of existing log records.

Logs

Application Log
Application: All

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

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

7.2.1 Debug Logs

This menu is accessed by selecting **Logs** and then clicking on the **Debug Logs** tab. This menu can be used to view application logs and audit log records.

Logs

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

- **Application Log**

This table lists the log records for a selected server application supported by the Unified Communications Module. The **Application** drop-down is used to select which records are shown. Clicking on a column header sorts the records using that column. The records shown are all those generated since the last time the log files were archived using the **Create Archive** command on the [Logs | Download](#) page. 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 Unified Communications Module menus.

- **Audit Log**

This table lists the actions performed by users logged in through the Unified Communications Module's web browser interface. Clicking on a column header sorts the records using that column.

7.2.2 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.

The [Settings | General](#) ⁹² menu is used to configure the sending and receiving of Syslog records by the server to and from other servers. It is also used to configure how long the server keeps different types of records and how many.

Logs

Debug Logs Syslog Event Viewer Download

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'

7.2.3 Download

This menu is accessed by selecting **Logs** and then clicking on the **Download** tab. This menu is used to create, manage and download archives of previous log files.

The log files are compressed into an archive file which can then be downloaded by clicking on the link. The archive files are in **.tar.gz** format. The log files within this type of archive file can be extracted by a range of utility applications including WinZip.

The screenshot shows a web interface for managing logs. At the top, there are three tabs: 'Debug Logs', 'Syslog Event Viewer', and 'Download'. The 'Download' tab is active. Below the tabs, there are three buttons: 'Select All', 'Create Archive', and 'Delete Selected'. The main content area is divided into two sections. The top section is titled 'Debug Files' and contains the text 'There is no data available'. The bottom section is titled 'Logs' and contains a table of log archives. The table has columns for Name, Last Modified, Size, and Delete. The table lists seven log archives, each with a link to download the file.

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"/>

To create archive files:

1. Click on the **Create Archive** button. Any log records recorded since the last creation of an archive are placed into archive files for each service.
2. The new archive files are listed in the web page.

To download archive files:

1. Any archive file can be downloaded by clicking on the file name of the archive file.
2. The process for the download and the location to which the file is downloaded will depend on the browser being used.

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**.

7.3 Updates

This menu is accessed by selecting **Updates**. The 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](#) page.

- ! 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. Some releases include changes that require additional steps.
- ! Backup Application Data**
 In all cases, always backup all application data to a separate location before upgrading.

⚠ Updates

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			

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			
IP Office	9.0.0.0 build 160	9.0.0.0 build 160	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 menu is divided into 2 sections:

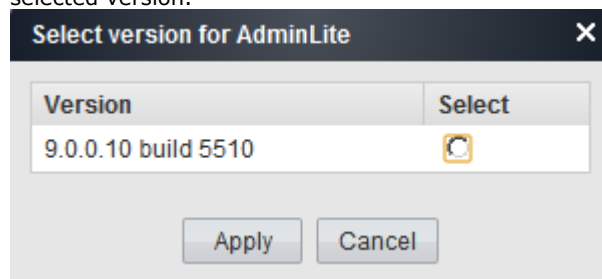
- Services** ⁸⁹
 This section displays the current version of application files and whether update files are available.
- System** ⁹⁰
 This section displays the current version of the operating system and whether update files are available.

7.3.1 Services

This menu is accessed 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](#)^[74]. This also affects the availability of the **Install** button option.
- **Change Version**
Clicking on this button shows the update files available for the related application in the server's [file repository](#)^[74]. The current version is selected. Selecting another version and clicking **Apply** will upgrade or downgrade to the selected version.



- **Update**
Clicking on this button will start an update of the related application to the latest available version in the application [file repository](#)^[74].
- **Uninstall**
Clicking on this button will uninstall the selected application.
 - If there are installation files for the application available in the application [file repository](#)^[74], the button will change to become an **Install** button.
 - If there are no installation files for the application available in the file repository, the application is no longer listed.
- **Install**
This button is displayed if an application is uninstalled and update files for the application are available in the file repository.
- **Check Now**
Clicking this button makes the Unified Communications Module 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**
This button can be used to remove older update installation files and other material that may accumulate on the server over time.
- **Update All**
If this button is clicked, those applications that support upgrading without being uninstalled (see above) are updated to the latest versions available in the application file repository.

7.3.2 System

This menu is accessed by selecting **Updates**. The **System** section shows details of the operating system and whether there are updates available.

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 Unified Communications Module 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 close button (X) in the top right corner. The window contains a table with the following columns: "Select", "Name", and "Version". All checkboxes in the "Select" column are checked. Below the table 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.

7.4 Settings

This menu is accessed by selecting **Setting**. The menu has two tabs for various areas of server configuration and operation.

- [General](#) ⁹²
General server settings such as the locations of software update repositories.
- [System](#) ⁹⁶
View and manage the server setting for date, time and IP address details.

7.4.1 General

This menu is accessed by selecting **Settings** and then clicking on the **General** tab. This menu is used for a wide variety of server settings.

Settings

General System	
Software Repositories	<p>Operating System: <input checked="" type="checkbox"/> Local — File: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Add"/></p> <p>Applications: <input checked="" type="checkbox"/> Local — File: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Add"/></p> <p>Downloads: <input checked="" type="checkbox"/> Local — File: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Add"/></p>
Syslog	<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Save"/></div> <p>Log files age (days)</p> <p>1 <input type="text"/> General log files 1 <input type="text"/> Security log files</p> <p>1 <input type="text"/> Audit log files 1 <input type="text"/> Operational log files</p> <p>1 <input type="text"/> Debug log files</p> <p><input type="checkbox"/> Apply general settings to all file types</p> <p>Max log size (MB)</p> <p>29 <input type="text"/> General log files 29 <input type="text"/> Security log files</p> <p>29 <input type="text"/> Audit log files 29 <input type="text"/> Operational log files</p> <p>29 <input type="text"/> Debug log files</p> <p><input type="checkbox"/> Apply general settings to all file types</p> <p>Receiver Settings</p> <p><input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> TCP Port: 514 <input type="text"/></p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> UDP Port: 514 <input type="text"/></p> <p><input checked="" type="checkbox"/> Forwarding Destination 1</p> <p><input type="radio"/> TCP <input type="radio"/> UDP</p> <p>IP Address:Port = <input type="text"/> : 514 <input type="text"/></p> <p><input type="checkbox"/> Forwarding Destination 2</p> <p>Select Log Sources</p> <p><input checked="" type="checkbox"/> Authentication and authorization privileges <input checked="" type="checkbox"/> Information stored by the Linux audit daemon (auditd)</p> <p><input checked="" type="checkbox"/> NNTP(News)/UUCP(Usenet) protocols <input checked="" type="checkbox"/> Apache web server access_log and error_log</p>
Web Control	<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Save"/></div> <p>Application Port: <input type="text" value="7070"/></p> <p>Protocol: <input type="text" value="https"/> <input type="button" value="v"/></p> <p>Inactivity timeout: <input type="text" value="1 hour"/> <input type="button" value="v"/></p> <p>Certificate: <input type="button" value="Copy Certificate from IP Office"/></p>
Backup and Restore	<p>Management Services <input type="button" value="Backup"/> <input type="button" value="Restore"/></p> <p>Voicemail <input type="button" value="Backup"/> <input type="button" value="Restore"/></p>
Voicemail Settings	<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Save"/></div> <p>Debug level: <input type="text" value="Information"/> <input type="button" value="v"/></p>
Contact Recorder Settings	<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Save"/></div> <p>Debug level: <input type="text" value="Info"/> <input type="button" value="v"/></p>
Watchdog	<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Save"/></div> <p>Log files age (days): <input type="text" value="5"/></p>
Set Login Banner	<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Save"/></div> <p>Technical Publications <input type="button" value="v"/></p>

Software Repositories

The Unified Communications Module can use either remote or local software repositories to store software update files. Separate repositories are configured for operating system updates, IP Office application installation files and Windows client files.

Software Repositories	
Operating System:	<input checked="" type="checkbox"/> Local — File: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Add"/>
Applications:	<input checked="" type="checkbox"/> Local — File: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Add"/>
Downloads:	<input checked="" type="checkbox"/> Local — File: <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Add"/>

The files uploaded or present in the file repositories are used by the [Updates](#)^[88] and [AppCenter](#)^[100] menus.

- Repository**
 If the **Local** option is not selected, this field is used to set the URL of a [remote HTTP file repository](#)^[76]. Note that each repository must be different, the same URL must not be used for multiple repositories.
- Local**
 This checkbox is used to set whether the file repository used is local (files stored on the Unified Communications Module or remote (a folder on a HTTP web server specified in the Repository field).
- File / Browse / Add**
 If the Local option is selected, this field and adjacent buttons can be used to browse to a specific update file. When the file is located and selected, click **Add** to upload the file to the file store on the Unified Communications Module.

Web Control

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

- Application Port**
 Change the port used for logging in. The default is **7070**. If you change this value you must ensure that you do not select a value already used by another service or application.
- Protocol**
 Select the protocol used for connection. The default is **https**. The options are **http** or **https**.
- Inactivity Timeout**
 Select the period of inactivity after which the web session is automatically logged out. Changing this value will require you to login again. The options are **5 minutes**, **10 minutes**, **30 minutes** and **1 hour**.
- Certificate**
 This control is not used with the Unified Communications Module.

Backup and Restore

These controls allow you to backup and restore the application settings being used selected IP Office applications.

- Management Services**
 These control provide options to backup/restore the configuration settings of the Management Services application running on the server.
- Voicemail Pro Server**
 For the Voicemail Pro server, these controls can only be used to restore an existing backup. Using the Voicemail Pro client, the voicemail server can be configured to perform regular (daily, weekly and or monthly) automatic backups of selected options including messages and prompts. The Voicemail Pro client can also be used to perform an immediate backup. When the Restore button is selected, the backups available in the backup folder (*/opt/vmpro/Backup/Scheduled*) are listed. The backup name includes the date and time and whether the backup was a manual or scheduled backup. When the required backup is selected, clicking OK will start the restoration process. For details refer to the Voicemail Pro client help.
- one-X Portal for IP Office**
 one-X Portal for IP Office has its own method of backup and restore that can be access through the one-X Portal for IP Offices web client administration.

Voicemail Settings

This section can be used to set 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](#)^[87] menu.

- Debug Level**
 This control is used to set 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 **Critical**.

Syslog

This section can be used to control the receiving and the forwarding of Syslog records.

- **Log files age (days)**

Set the number of days each type of record is retained on the server before being automatically deleted. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**.

- **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 retained on the server before the oldest records of that type are automatically deleted. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**.

- **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 is able to receive Syslog records using the port configured below.

- **TCP Port**

Sets the port number used for receiving Syslog records if the **Protocol** is set to **TCP**.

- **UDP Port**

Sets the port number used for receiving Syslog records if the **Protocol** is set to **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**

Sets the address of the destination server.

- **Port**

Set the destination port for the forwarded records.

- **Protocol**

Set the protocol, **UDP** 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**

Watchdog

- **Log files age (days)**

Sets the number of days that log file records are retained. This does not affect log file [archives](#)^[87]. Not applied to one-X Portal for IP Office which performs its own log file size limitation.

Set Login Banner

The login menu includes a text item that is defaulted to indicate the version of Linux installed. However, that text change be changed to show a custom message, for example to indicate the server's role in a network. This may be useful in a network with multiple servers.

- **Login Banner Text**

Use this field to set the text that should be displayed on the login menu. After changing the text click **Save**.

7.4.2 System

This menu is accessed by selecting **Settings** and then clicking on the **System** tab. This menu is used to adjust server settings such as its IP address settings and time settings.

Settings

GeneralSystem

Network	Network Interface: eth0.1 Create Subinterface Delete Subinterface	Save														
	Host Name: uc-module <input type="checkbox"/> Use DHCP															
	IP Address: 192.168.0.201															
	Subnet Mask: 255.255.255.0															
	Default Gateway: 192.168.0.1															
	System DNS: 8.8.8.8.8.4.4 <input type="checkbox"/> Automatically obtain DNS from provider															
Avaya IP Office LAN Settings	<table style="width: 100%;"><tr><td style="width: 50%; vertical-align: top;">Avaya IP Office LAN1 <input type="checkbox"/> Enable traffic control Network Interface: eth0 Save</td><td style="width: 50%; vertical-align: top;">Avaya IP Office LAN2 <input type="checkbox"/> Enable traffic control Network Interface: none Save</td></tr></table>	Avaya IP Office LAN1 <input type="checkbox"/> Enable traffic control Network Interface: eth0 Save	Avaya IP Office LAN2 <input type="checkbox"/> Enable traffic control Network Interface: none Save													
Avaya IP Office LAN1 <input type="checkbox"/> Enable traffic control Network Interface: eth0 Save	Avaya IP Office LAN2 <input type="checkbox"/> Enable traffic control Network Interface: none Save															
Date and Time	Date / Time: 2013-12-10 / 06 : 47 Timezone: Europe/London <input checked="" type="checkbox"/> Enable Network Time Protocol NTP Servers: 169.254.0.1 <input checked="" type="checkbox"/> Synchronize system clock before starting service <input type="checkbox"/> Use local time source	Save														
Change root Password	New Password: Confirm New Password: 	<small>Password complexity requirements:</small> <ul style="list-style-type: none">• Minimum password length: 8• Maximum allowed sequence length: 4	Save													
Password Rules Settings	<table style="width: 100%;"><tr><td style="width: 20px; text-align: center;"><input style="width: 20px;" type="text" value="8"/></td><td>Minimum password length</td></tr><tr><td style="text-align: center;"><input style="width: 20px;" type="text" value="0"/></td><td>Minimum number of uppercase characters</td></tr><tr><td style="text-align: center;"><input style="width: 20px;" type="text" value="0"/></td><td>Minimum number of lowercase characters</td></tr><tr><td style="text-align: center;"><input style="width: 20px;" type="text" value="0"/></td><td>Minimum number of numeric characters</td></tr><tr><td style="text-align: center;"><input style="width: 20px;" type="text" value="0"/></td><td>Minimum number of special characters</td></tr><tr><td style="text-align: center;"><input type="checkbox"/></td><td>Allow character sequences</td></tr><tr><td style="text-align: center;"><input style="width: 20px;" type="text" value="4"/></td><td>Maximum allowed sequence length</td></tr></table>	<input style="width: 20px;" type="text" value="8"/>	Minimum password length	<input style="width: 20px;" type="text" value="0"/>	Minimum number of uppercase characters	<input style="width: 20px;" type="text" value="0"/>	Minimum number of lowercase characters	<input style="width: 20px;" type="text" value="0"/>	Minimum number of numeric characters	<input style="width: 20px;" type="text" value="0"/>	Minimum number of special characters	<input type="checkbox"/>	Allow character sequences	<input style="width: 20px;" type="text" value="4"/>	Maximum allowed sequence length	Save
<input style="width: 20px;" type="text" value="8"/>	Minimum password length															
<input style="width: 20px;" type="text" value="0"/>	Minimum number of uppercase characters															
<input style="width: 20px;" type="text" value="0"/>	Minimum number of lowercase characters															
<input style="width: 20px;" type="text" value="0"/>	Minimum number of numeric characters															
<input style="width: 20px;" type="text" value="0"/>	Minimum number of special characters															
<input type="checkbox"/>	Allow character sequences															
<input style="width: 20px;" type="text" value="4"/>	Maximum allowed sequence length															

Network

- **Network Interface**

For the Unified Communications Module this setting is fixed as **eth0.1**.

- **Host Name**

Sets the host name that the Unified Communications Module should use. This setting requires the local network to support a DNS server. Do not use **localhost**.

- **Use DHCP**

Do not use this setting with the Unified Communications Module.

- **IP Address**

Displays the IP address set for the server. The Unified Communications Module connects to the system's LAN1 network system and must have an address on that subnet. See [IP Address Notes](#)^[11].

- **Subnet Mask**

Displays the subnet mask applied to the IP address.

- **Default Gateway**

Displays the default gateway settings for routing.

- **System DNS**

Enter the address of the primary DNS server.

- **Automatically obtain DNS from provider**

Not used.

- **Create Subinterface**

This control is not supported on the Unified Communications Module and so is greyed out.

- **Delete Subinterface**

This control is not supported on the Unified Communications Module and so is greyed out.

Avaya Office LAN Settings

- **Avaya Office LAN1**

These settings are used for the LAN1 interface of the Management Services 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.

Date Time

These settings are used to set or obtain a UTC date and time value for use by the Unified Communications Module and services.

- **Date**
Shows the current date being used by the server. If **Enable Network Time Protocol** is selected, this is the date obtained from the NTP server and cannot be manually changed.
- **Time**
Shows the current UTC time being used by the server. If **Enable Network Time Protocol** is selected, this is the time obtained from the NTP server and cannot be manually changed. The current time being used by the server is shown on the [System](#) ^{F81} menu.
- **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 is used to determine the appropriate offset that should be applied to the UTC time above. Note that changing the timezone can cause a Session expired message to appear in the browser.
- **Enable Network Time Protocol**
If this option is selected, the Unified Communications Module will attempt to obtain the current UTC time from the NTP servers listed in the **NTP Servers** list below. It will then use that time and make regular NTP requests to update the date and time. The following options are only used if **Enable Network Time Protocol** is selected.
 - **NTP Servers**
This field is used to enter the IP address of an NTP server or servers which should be used when **Enable Network Time Protocol** is selected. 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 make sure you are aware of the usage policy for any servers you choose. Choosing several unrelated NTP servers is recommended in case one of the servers you are using becomes unreachable or its clock is unreliable. The operating system uses the responses it receives from the servers to determine which are reliable.
 - The IP Office system can also use NTP to obtain its system time. Using the same servers for the Unified Communications Module and IP Office system is recommended.
 - The default time setting for the Unified Communications Module is to use NTP with the server address set to 169.254.0.1 which is the IP Office system. When this is set, the IP Office system must be configured to get its time from an external SNTP server or to have its time set manually.
 - **Synchronize system clock before starting service**
When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, an immediate update of the server's clock to match the NTP obtained time is forced.
 - **Use local time source**
When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, the server's hardware clock time is used as the current time rather than the NTP time.

Change Root Password

- **New Password**
Enter the new password for the server's root account.
- **Confirm New Password**
Confirm the new password.

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**

If this option is selected, character sequences such as **1234** or **1111** or **abcd**, are allowed in new passwords without any restriction. When not selected, the maximum length of any sequence is set by the field below.

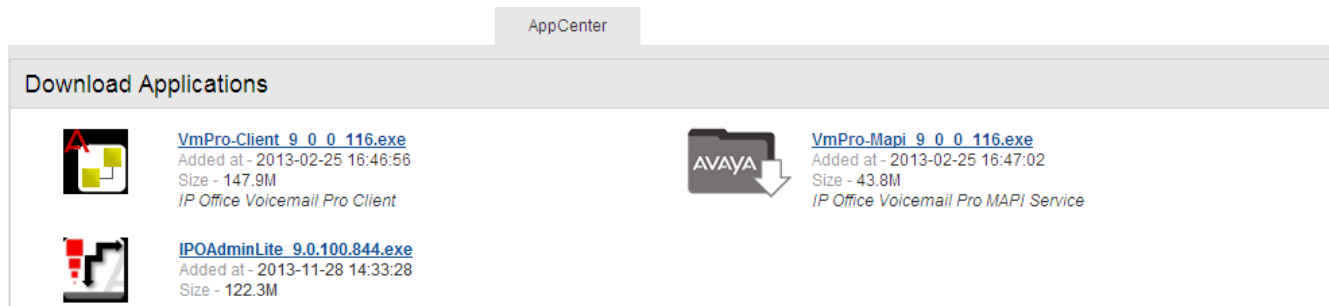
- **Maximum allowed sequence length**

This field is used to set the maximum allowed length of any character sequence when **Allow character sequences** is not selected.

7.5 App Center

This menu is accessed by selecting **AppCenter**. The menu is used 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](#) ⁹² page.



The files included in the installation may vary. Typical files are listed below. 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 can be 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.

Chapter 8.

Additional Processes

8. Additional Processes

This section details processes that are not normally required but may be useful. These should only be attempted if you are confident with Linux commands and managing a Linux based system.

- [SSH File Transfers](#) ¹⁰⁵

8.1 SSH File Transfers

The directory structure of files on the server can be accessed using any file transfer tool that supports SFTP/SSH. For example WS_FTP or SSH Secure Shell.

To start SSH file transfers:

1. Start your SFTP or SSH file application and connect to the Unified Communications Module PC. The exact method will depend on the application being used.
 - a. Enter the details for the Unified Communications Module:
 - The **Host Name** is the IP address of the Unified Communications Module.
 - The **User Name** is **web**.
 - The **Protocol** is **SFTP/SSH**.
 - The **Port** is **22**. If this is the first time the application has connected to the server, accept the trusted key.
 - b. If this is the first time the application has connected to the Unified Communications Module, accept the trusted key.
 - c. When prompted, enter the webcontrol user [password](#)^[64], the default is **webcontrol**.
2. The default folder displayed after logging in is **/home/Administrator**.

8.2 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](#)^[105].
3. Copy the Windows backup folder into the folder **/opt/vmpro/Backup/Scheduled/OtherBackups**.
4. Using a web browser, [login](#)^[63] to the Unified Communications Module.
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**.

Chapter 9.

Document History

9. Document History

Date	Issue	Changes
10th December 2013	07g	<ul style="list-style-type: none">• Corrected name of applications download menu to AppCenter.• Correct mention of 4GB USB2 memory key to 8GB.• Correct IP Office software release mentions to 9.0.• Corrected operation of web link for UNetBootin software.
12th December 2013	07h	<ul style="list-style-type: none">• Minor spelling corrections.• In response to customer requests, reinstated the sections on the server menus and options.
13th December 2013	07i	<ul style="list-style-type: none">• Minor spelling corrections.
8th January 2014	07j	<ul style="list-style-type: none">• Minor spelling corrections.• Clarified Unified Communications Module USB upgrade if from pre-9.0 release needs to use full data backup and then full reinstall.
16th January 2014	07k	<ul style="list-style-type: none">• Minor spelling corrections.• Clarify role of Management Services on Unified Communications Module.
24th January 2014	07l	<ul style="list-style-type: none">• Update upgrade process for upgrades that include SSD firmware update.

Index

1

169.254.0.1 11
169.254.0.2 11

3

3rd Party database integration 12

A

Add
 Sub-interface 96
Additional documentation 10
Address
 DNS 30, 68, 96
 IP 30, 68, 96
Administrator
 Login 54
Application
 Auto-start 66
 Install 71
 Repositories 74, 92
 Start 66
 Stop 66
 Uninstall 73
 Upgrade 71, 72
Application files
 Upload files 71, 75
Application Logs 85
Archive 87
Attach
 Monitor and keyboard 32
Audit Log 85
Auto-start 66

B

Backup 92, 106
 Custom folders 51
 one-X Portal for IP Office 58
 Voicemail 48
Batteries 38
Boot
 from USB 23, 37
Browser 12
Bulletins 10
Buttons 31

C

CentOS 10
Change
 IP Address 30, 68
 Password 24, 64
Change Password
 Web Browser Password 64
Check
 Software version 89, 90
Clients 100
Configuration
 one-X Portal for IP Office 54
 Voicemail Pro 42
ContactStore 12
Cover 32
CPU
 Usage 81
Create a USB device 22, 36
Create Archive 87
Custom folders
 Backup/restore 51

D

Database integration 12
Date 69, 96
Default
 Gateway 30, 68, 96
 Password 14, 20, 25, 63
Delete
 Sub-interface 96
DHCP 30, 68, 96
Disk
 Usage 81
DNS 30, 68, 96
Download
 Logs 87
 Software 16
 Windows Clients 100

F

Forward
 Syslog records 92

G

Gateway 30, 68, 96
General 92

H

Home 81
Host Name 30, 68, 96
HTTPS 92

I

Inactivity timeout 70, 92
Initial configuration 54
Install
 Application 71
 Service 71
IP Address 30, 32, 44, 68, 96
IP Office
 Check 54
 Select 54
ISO 16

J

Javascript 12

K

Keyboard 32

L

LAN2 11
LEDs 31
Linux 10
Local 92
Log Files Age 92
Logging In 63
Login 25, 46, 63
 Administrator 54
 Banner text 92
Logs 84
 Application 85
 Archive 87
 Audit 85
 Download 87
 Log Files Age 92

M

Mask 30, 68, 96
Memory
 Usage 81
Menu
 Download 87

- Menu
 - General 92
 - Home 81
 - Logs 84
 - Logs Download 87
 - Logs View 85
 - Services 89
 - Settings 91
 - System 90, 96
 - Updates 88
 - Updates Services 89
 - Updates System 90
 - View 85
 - Windows Clients 100
- Menus
 - Inactivity timeout 70, 92
- Module
 - Batteries 38
 - Buttons 31
 - Cover 32
 - LEDs 31
 - Restart 29, 67
 - Shutdown 29, 67
- Monitor 32
- N**
- NAT 11
- Network
 - Change IP address 30, 68
 - Sub-interface 96
- Network Time Protocol 69, 96
- no Remote 46
- Notifications 81
- NTP 69, 96
- O**
- one-X Portal for IP Office
 - Auto-start 66
 - Backup/restore 58
 - Configuration 54
 - Start 66
 - Stop 66
- Operating system
 - Repositories 74, 92
 - Upload files 75
- P**
- Password
 - Change 24, 54, 64
 - Default 14, 20, 25, 63
 - Root password 65
 - Rules 96
 - Web Browser Password 64
- Port 92
 - Web Control 92
- Protocol 92
- R**
- RAM
 - Usage 81
- Reboot 29, 67, 81
- Recieve
 - Syslog 92
- Related documents 10
- Remote Software Repositories 76
- Remove
 - Sub-interface 96
- Repositories 74, 76, 92
- Repository 92
 - Restart 29, 67
 - Restore 92, 106
 - Custom folders 51
 - one-X Portal for IP Office 58
 - Voicemail 48
 - Root password
 - Change 65
 - Rules 96
 - RPM 16
 - Rules 96
- S**
- Send
 - Syslog records 92
- Server
 - NTP 69, 96
 - Port 92
 - Protocol 92
 - Reboot 67, 81
 - Shutdown 67, 81
- Server Name 46
- Service
 - Auto-start 66
 - Install 71
 - Start 66
 - Stop 66
 - Uninstall 73
 - Upgrade 71
- Services 89
 - Start 81
 - Status 81
 - Stop 81
- Set
 - Login banner 92
- Settings 91
- SFTP 105
- Shutdown 29, 67, 81
- SNMP 92
- SNMP Support 92
- Software 46
 - Downloading 16
 - Install from USB 23, 37
 - Repositiories 74, 92
 - Repositories 76
 - Unetbootin 16, 22, 36
 - USB 16, 22, 36
- Software Repositories 92
- Software version
 - Check 89, 90
- SSH access 105
- Start 29, 67
 - Auto-start 66
 - Service 66
- Start Services 81
- Status 81
- Stop
 - Service 66
- Stop Services 81
- Sub-interface 96
- Subnet Mask 30, 68, 96
- Supported
 - Browsers 12
- syslinux.cfg 22, 36
- Syslog
 - Settings 92
 - View 86
- System 90, 96

-
- T**
- Technical bulletins 10
 - Time
 - Timezone 69, 96
 - Timeout 70, 92
- U**
- UMS 12
 - Uninstall
 - Application 73
 - Service 73
 - Unit Name/IP Address 46
 - Update
 - Check version 89, 90
 - Services 89
 - System 90
 - Updates
 - Services 88
 - System 88
 - Upgrade
 - Application files 72
 - Upgrading Applications 71
 - Upload
 - Application files 71, 75
 - Operating system 75
 - Windows client files 75
 - Usage
 - CPU 81
 - Disk 81
 - Memory 81
 - USB
 - Create a bootable... 22, 36
 - Load software 23, 37
 - Software 16, 22, 36
 - USB Initiator 16
- V**
- Version
 - Check 89, 90
 - View
 - Syslog records 86
 - View Logs 85
 - Voicemail 106
 - Auto-start 66
 - Backup/restore 48
 - Start 66
 - Stop 66
 - Voicemail IP Address 44
 - Voicemail Pro
 - Configuration 42
 - Limitations 12
 - Voicemail Pro Client
 - run 46
 - Voicemail Pro Client window 46
 - Voicemail Pro Login window 46
 - Voicemail Pro Server
 - connect 46
 - Voicemail Type 44
 - VPNM 12
- W**
- WAN 46
 - Watchdog 92
 - Web browser 12
 - Web Control Port 92
 - Windows 106
 - Windows client
 - Repositories 74, 92
 - Windows client files
 - Upload files 75
 - Windows Clients 100
 - Workstation 46
- Z**
- ZIP 16

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.

© 2014 Avaya Inc. All rights reserved.