



# **IP Office**

## **Unified Communications Module 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.

#### 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 reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller 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 thereto.

#### 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 RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 RESELLER; 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 types

**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 re-install or operate the software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

**Named User License (NU).** You may: (i) install and use 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

##### 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](mailto: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, and "Linux" is a registered trademark of Linus Torvalds.

#### 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 Unified Communications Module.....	10
1.2 Using Linux.....	12
1.3 Additional Documentation.....	12
1.4 Network Configuration Limitations.....	13
1.5 Small Community Networks.....	13
1.6 Licenses.....	14
1.7 Voicemail Pro Features.....	14

## 2. Module Installation

2.1 Installation Pre-requisites.....	17
2.2 IP Address Notes.....	18
2.3 IP Office Configuration.....	19
2.4 System Shutdown.....	20
2.5 Inserting the Module.....	21
2.6 Initializing the Module Services.....	22
2.7 System and Module Start Up.....	26
2.8 Logging on to the Web Menus.....	27
2.9 Changing the Web Password.....	28
2.10 Upgrading the Software.....	29

## 3. Voicemail Pro Configuration

3.1 Adding Voicemail Licenses.....	33
3.2 IP Office Configuration.....	34
3.3 Installing the Voicemail Pro Client.....	35
3.4 Logging in to the Voicemail Server.....	36
3.5 Changing the Voicemail Server Password.....	37
3.6 Transferring Voicemail Server Settings.....	38
3.7 ContactStore.....	40
3.8 Backup/Restore Limitations.....	40

## 4. one-X Portal for IP Office Configuration

4.1 Adding Licenses.....	45
4.2 Enabling one-X Portal for IP Office Users.....	46
4.3 Initial one-X Portal for IP Office Login.....	47
4.4 Initial AFA Login.....	48

## 5. Server Maintenance

5.1 Logging In.....	51
5.2 Changing the Web Password.....	52
5.3 Changing the Root Password.....	53
5.4 Setting the Password Rules.....	54
5.5 Starting/Stopping Application Services.....	55
5.5.1 Starting a Service.....	55
5.5.2 Stopping a Service.....	55
5.5.3 Setting a Service to Auto Start.....	55
5.6 Server Shutdown.....	56
5.7 Rebooting the Server.....	56
5.8 Changing the IP Address Settings.....	57
5.9 Date and Time Settings.....	58
5.10 Changing the Web Control Port.....	59
5.11 Setting the Menu Inactivity Timeout.....	60
5.12 Upgrading Applications.....	61
5.12.1 Loading Application Files onto the Server.....	61
5.12.2 Upgrading Application Files.....	62
5.13 Uninstalling an Application.....	63

5.14 File Repositories.....	64
5.14.1 Source Files.....	64
5.14.2 Setting the Repository Locations.....	64
5.14.3 Uploading Local Files.....	65
5.14.4 Creating Remote Software Repositories.....	66

## 6. Server Menus

6.1 Home.....	69
6.2 Logs.....	71
6.2.1 View.....	71
6.2.2 Download.....	72
6.3 Updates.....	73
6.3.1 Services.....	74
6.3.2 System.....	75
6.4 Settings.....	76
6.4.1 General.....	77
6.4.2 System.....	80
6.5 Apps Center.....	85

## 7. Module Maintenance

7.1 Module LEDs.....	89
7.2 Module Buttons.....	89
7.3 Module Removal.....	90
7.4 Attaching a Monitor and Keyboard.....	91
7.5 Transferring Voicemail Server Settings.....	92
7.6 Module Battery.....	94
7.7 Upgrading Software.....	95
7.8 Module Software Reinstallation.....	97
7.9 Module Password Reset.....	101

## 8. Additional Processes

8.1 Changing the Root Password.....	105
8.2 SSH File Transfers.....	106
8.3 Command Line.....	107
8.3.1 General Commands.....	108
8.3.2 Administrator Commands.....	110
8.3.3 Configuration Commands.....	111
Index.....	113



# **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. The module is supported by systems running in IP Office Essential Edition, IP Office Preferred Edition or IP Office Advanced Edition mode and acts as an automatic **PREFERRED EDITION** license for such systems.

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

## Linux

The base operating system installed is CentOS, a Linux operating system. However, no specific knowledge of Linux is required for installation or maintenance of the Unified Communications Module.

- **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 needs to be [licensed](#)<sup>[14]</sup>. The Unified Communications Module acts as an automatic **Preferred Edition** license that is normally required by the application.

- **Voicemail Pro**

This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system for which it is configured. In addition it can be customized to provide a range of call routing and voicemail services. The Voicemail Pro service is configured and managed remotely using the Windows Voicemail Pro client. A copy of the Voicemail Pro client can be [downloaded](#)<sup>[83]</sup> and installed from the server. The number of simultaneous connections to voicemail is [licensed](#)<sup>[14]</sup>. The Unified Communications Module acts as an automatic **Preferred Edition** license for Voicemail Pro application.

- **Web Control Menus**

The server's own settings are configured and managed remotely using web browser access to a set of menus.

## Unified Communications Module Capacity

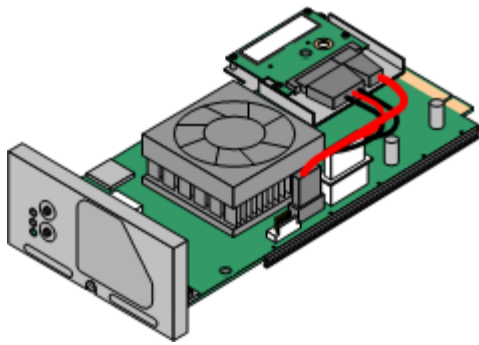
The capacity of the Unified Communications Module is:

- **IP Office Users:** Up to 200 users when running Voicemail Pro and one-X Portal for IP Office. More than 200 users when running just Voicemail Pro.
- **Simultaneous one-X Portal for IP Office Users:** 50.
- **Maximum voicemail ports:** Up to 20 ports when running Voicemail Pro and one-X Portal for IP Office. 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 Unified Communications Module

This module is supported for IP Office Release 8.0 Q1 2012 Service Pack and higher. The module is an embedded server that allows Linux based IP Office applications to be run within the IP Office control unit rather than requiring a separate PC.



- **Supports**

Voicemail Pro and or one-X Portal for IP Office applications. The module is only supported by systems running IP Office Essential Edition, IP Office Preferred Edition or IP Office Advanced Edition modes.

- **IP Office Users:** Up to 200 users when running Voicemail Pro and one-X Portal for IP Office. More than 200 users when running just Voicemail Pro.
- **Simultaneous one-X Portal for IP Office Users:** 50.
- **Maximum voicemail ports:** Up to 20 ports when running Voicemail Pro and one-X Portal for IP Office. Up to 40 ports when running just Voicemail Pro.
- **Small Community Network:** Maximum 6 systems.

- **Licenses**

The presence of this module acts as an automatic **Preferred Edition** license for the IP Office system, enabling 4 ports of voicemail. Additional voicemail ports can be licensed up to a maximum of 20. A separate **Essential Edition** license is still required as a pre-requisite.

- **IP500 Control Unit:** ✗
- **IP500 V2 Control Unit:** ✔ IP Office Release 8.0 Q1 2012 Service Pack or higher.
- **Maximum per Control Unit:** 1 per control unit.
- **IP500 Trunk Card Support:** ✗

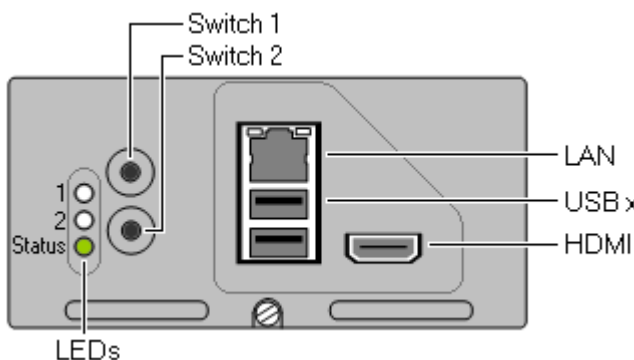
- **! WARNING: Do Not Remove the Port Cover Except for Maintenance**

The card is supplied with a removable plastic cover that locates over the external ports (LAN, USB and HDMI) on the faceplate of the card. This cover should always be in place during normal operation of the card. The cover should only be temporarily removed during maintenance actions that require access to the ports and should be replaced when the maintenance is completed.

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

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

### Ports



The card is supplied with a removable plastic cover that locates over the external ports (LAN, USB and HDMI) on the faceplate of the card. This cover should always be in place during normal operation of the card. The cover should only be temporarily removed during maintenance actions that require access to the ports and should be replaced when the maintenance is completed. Whilst removed, the following ports are accessible:

- **LAN**  
This port is not used.
- **USB**  
These USB2 ports can be used for the temporary connection of devices during [module maintenance](#)<sup>[88]</sup>. USB2 memory devices should be USB 2.0 compatible.
- **HDMI**  
This port can be used for temporary connection of a [video monitor](#)<sup>[91]</sup> during module maintenance.

## LEDs

The Unified Communications Module provides the following LEDs:

- **Upper 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 blink:** OK. IP Office heartbeat okay.
  - **Off with Amber blink:** Module shutdown. IP Office heartbeat okay.
  - If the module is already running when the system restarts, its 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, its lower LED remains off when the LEDs on the other base cards are solid red. The lower LED on the module then flashes red when the LEDs on the other base cards flash red during system initialization; before reverting to either green or off when the system reboot is complete.

## Buttons

The Unified Communications Module provides the following buttons:

- **Upper Button/Button 1**

This button can be used for the following functions:

  - **Shutdown**

If the module is running, pressing this button for more than 2 seconds will start a module shutdown. A completed shutdown is indicated by the lower LED changing to off with regular amber blinks only.
  - **Startup**

If the module has been shutdown, pressing this button will cause 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. See [Module Software Reinstallation](#)<sup>[97]</sup>.
- **Switch 2:** Not used.

---

## 1.2 Using Linux

Despite using a Linux based operating system, knowledge or experience of Linux by the installer and maintainer is not 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. Using the Linux command line to perform any other actions may cause unexpected operation of the Unified Communications Module and is not supported except when specifically instructed by Avaya.

## 1.3 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.

### Application Installation and Configuration

- **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 to be configured to support multiple IP Office servers in a Small Community Network.

- **Voicemail Pro Linux Installation Manual**

This manual covers scenarios where multiple servers are installed within a Small Community Network.

- **Voicemail Pro Administration Manual**

By default the voicemail server will provide mailbox services to all users and hunt groups without any configuration being needed. This manual covers the administration of the voicemail server using the Voicemail Pro client in order to enable additional features.

### Technical Bulletins

All releases of IP Office software are accompanied by a technical bulletin. The bulletin will include details of changes that may have occurred too late to be included in this documentation. The bulletins will also detail what has changed 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>

## 1.4 Network Configuration Limitations

The IP Office control unit has two physical LAN interfaces: LAN1 and LAN2. The ports labeled LAN and WAN respectively.

Traffic between the IP Office control unit and the Unified Communications Module is on LAN1 of the IP Office system. Scenarios where users of the Unified Communications Module applications, especially one-X Portal for IP Office, are accessing the IP Office and thus the Unified Communications Module via the IP Office system's LAN2 (WAN) port should be avoided for more than 30 users.

They should also be avoided where NAT is being applied to traffic between LAN1 and LAN2. These restrictions should be observed even when the IP Office system is in a Small Community Network where the H323 SCN trunks may be routed via the other LAN.

## 1.5 Small Community Networks

Up to 32 IP Office systems can be connected together using H323 SCN trunks to form a Small Community Network, supporting up to 1000 users. The servers in the system automatically share information about users and other features in order to act as a single system.

- The Unified Communications Module is only supported as an application server for a Small Community Network of up to 6 systems. It is also limited to supporting only 200 users if it is running the one-X Portal for IP Office application.

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**

Only a single instance of the one-X Portal for IP Office application is supported within a Small Community Network.

- When run on a Unified Communications Module, one-X Portal for IP Office is only supported for up to 200 users and 50 simultaneous sessions. To support more users and sessions (500), the one-X Portal for IP Office application needs to be installed on a separate server from the Unified Communications Module.
- 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. This additional configuration is covered in the one-X Portal for IP Office Installation Manual.

- **Voicemail Pro**

In an Small Community Network, one Voicemail Pro server is used to store all mailboxes and their related messages, greeting and announcements. This is referred to the centralized voicemail server. However, additional Voicemail Pro servers can be installed to perform some other specific roles as listed below. Full details of the setup for these roles is covered in the Voicemail Pro manuals.

- **Centralized Voicemail Server**

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

- **Fallback IP Office**

Without needing to install another Voicemail Pro server, the IP Office hosting the centralized voicemail server can be configured such that, if for any reason it is stopped or disabled, the centralized voicemail server switches to being controlled by another IP Office in the network.

- **Distributed Voicemail Servers**

Additional Voicemail Pro servers can be installed and associated with other IP Office systems to provide call services for that system. For example to record messages, play announcements, etc. However, any messages it records are then automatically transferred to and stored on the centralized server. The IP Office associated with the distributed server requires the appropriate licenses for voicemail server support.

- **Backup Voicemail Server**

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

---

## 1.6 Licenses

The use of various features are licensed, for example, which users are able to use the one-X Portal for IP Office application. These licenses are entered into the IP Office configuration.

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)**

This license is required for use of the Voicemail Pro application. It also enables 4 voicemail ports. It is also required as a pre-requisite for the user profile licenses required for one-X Portal for IP Office users. The Unified Communications Module acts as an automatic **Preferred Edition** license for the system.

- **Preferred Edition Additional Voicemail Ports**

These licenses can be used to add additional voicemail ports in addition to the 4 enabled by the **Preferred Edition (Voicemail Pro)** license above. Multiple licenses can be added, up to a total of 20 ports when running Voicemail Pro and one-X Portal for IP Office, or up to 40 ports when running just Voicemail Pro.

- **VMP Pro TTS (Linux Voicemail Pro)**

This license enables the use of text-to-speech facilities using the optional Linux TTS software. One license per simultaneous instance of TTS usage. This license is also used for user email reading.

- **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.

## 1.7 Voicemail Pro Features

Voicemail Pro runs on both Windows and Linux servers. For Voicemail Pro server running on Linux such as with the Unified Communications Module, the following Voicemail Pro features are not supported:

- **VB Scripting**
- **3rd Party Database Integration**
- **VPNM**
- **UMS Web Voicemail**  
(However, access via IMAP and one-X Portal for IP Office are available as alternatives.)
- **ContactStore**  
ContactStore is supported for IP Office Release 8.1 Feature Pack 1 and higher.

When logged into the voicemail server using the Voicemail Pro client, those features not supported are grayed out or hidden. If those features are present in an imported call flow, they will not function and calls attempting to use those features will be disconnected.

The Voicemail Pro client's backup and restore functions cannot currently be used to move voicemail data between a Linux based server and a Windows based server or vice versa. The client functions for importing and exporting module and the call flow database can be used.

For Small Community Network scenarios where multiple voicemail servers are present, for example distributed and backup server, a mix of Linux based and Windows based servers are allowed.

# **Chapter 2.**

## **Module Installation**

---

## 2. Module Installation

The Unified Communications Module installation consists of the following steps.

### Process Summary

1. [Check the you have meet the installation pre-requisites](#) <sup>17</sup>.
2. [Configure the IP Office](#) <sup>19</sup>.
3. [Shutdown the system](#) <sup>20</sup>.
4. [Insert the module](#) <sup>22</sup>.
5. [Initialize the module service](#) <sup>22</sup>.
6. [Log onto the module web menus](#) <sup>27</sup>.
7. [Change the web password](#) <sup>28</sup>.
8. [Upgrade the module software](#) <sup>29</sup>.



## 2.1 Installation Pre-requisites

- This manual assumes that the installer is already experienced with the installation of an IP500 V2 system, including the installation of IP500 base cards. It also assumes that the installer is familiar with the configuration of a IP Office system using IP Office Manager and System Status Application.
- This manual assumes that the IP Office system has already been installed and licensed for IP Office Essential Edition mode running IP Office Release 8.0 Q1 2012 Service Pack or higher.
- The Unified Communications Module defaults to using the IP Office system as its source for time and date information. Therefore the IP Office system must be configured to either use a specific external time server to obtain its time or to have its time set manually.

### Additional Documentation

Depending on the application to be supported by the Unified Communications Module, Voicemail Pro and or one-X Portal for IP Office, the following manuals are also required plus any information requirements specified in those manuals.

- **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 to be configured to support multiple IP Office servers in a Small Community Network.
- **Voicemail Pro Linux Installation Manual**  
This manual covers scenarios where multiple servers are installed within a Small Community Network.
- **Voicemail Pro Administration Manual**  
By default the voicemail server will provide mailbox services to all users and hunt groups without any configuration being needed. This manual covers the administration of the voicemail server using the Voicemail Pro client in order to enable additional features.

### Information Required

- **IP Office Service User Names and Passwords**  
Service user names and passwords for IP Office Manager and System Status Application access to the IP Office system.
- **IP Address Details**  
The IP address of the IP Office system's LAN1 interface is used for the initial configuration of the module. During that configuration separate IP address settings for the module are set.
- **Licenses**  
Check that you have the necessary [licenses](#) <sup>[14]</sup> for the expected operation. The licenses must match the **Dongle Serial Number** shown in the IP Office system's configuration.

### Tools Required

- **Windows PC**  
This PC or an existing PC is needed to run IP Office Manager and System Status Application. The PC needs to have a LAN connection to the IP Office control unit.
- **5mm Flat-blade Screwdriver**  
This is required to remove a slot cover from the front of the IP Office control unit and to secure the newly installed Unified Communications Module.
- **Anti-Static Wrist Strap and Ground Point**  
These should be used when inserting and removing cards from the IP Office control unit.

### Software Required

The following software should be downloaded from the Avaya support website section for the IP Office release being run by the IP Office system.

- **Unified Communications Module Software Upgrade Image**  
The card ships with software pre-installed. However, that software may not match the release of the software required by the IP Office system. Various software files for each release can be downloaded from the Avaya support website (<http://support.avaya.com>). These include upgrade .zip files for the Unified Communications Module. You should obtain the upgrade .zip file that matches the software release of the IP Office system.

### Transferring Settings from Other Servers

If the module is replacing an existing Voicemail Pro and or one-X Portal for IP Office server, the settings from those servers can be transferred to the module. The methods for this are outlined in the sections [Transferring Voicemail Server Settings](#) <sup>[92]</sup> and Transferring one-X Portal for IP Office Settings.

---

## 2.2 IP Address Notes

During installation the Unified Communications Module is assigned an IP address. The Unified Communications Module can also use DHCP to obtain an address. It can also be given a DNS name.

The IP500 V2 system has two physical LAN interfaces: LAN1 and LAN2. The ports labeled LAN and WAN respectively. The Unified Communications Module is physically connected 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.

- **User and Administration IP Addresses**

User and administrator access to the Unified Communications Module and the applications hosted by the module use the following addresses.

- **Unified Communications Module**

A newly installed Unified Communications Module uses the IP Office system's LAN1 IP address for browser access to the module's initial configuration menu. During that initial configuration, an IP address for future access to the Unified Communications Module is set.

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

The one-X Portal for IP Office service running on the Unified Communications Module is accessed using the module's IP address or DNS name suffixed with :8080 as the port number.

- **Voicemail Pro**

The voicemail server service running on the Unified Communications Module is accessed by the Voicemail Pro client using the module's IP address.

- **Internal Addresses**

The following addresses are used only for internal connections between the IP Office system and the applications running on its Unified Communications Module. These addresses are fixed and normally automatically set. However you need to be aware of them as they appear in the IP Office system and one-X Portal for IP Office configuration settings.

- **one-X Portal for IP Office Connection: 169.254.0.1**

This address is used for the CSTA and DSML 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.

- **Voicemail Pro Connection: 169.254.0.2**

This address is used for as the internal address for connections to the voicemail server. It is set as the IP address of the voicemail server in the IP Office system's configuration. It is also used as the voicemail provider address by the one-X Portal for IP Office application.

### LAN2 and NAT Limitation

Traffic between the IP Office control unit and the Unified Communications Module is on LAN1 of the IP Office system. Scenarios where users of the Unified Communications Module applications, especially one-X Portal for IP Office, are accessing the IP Office and thus the Unified Communications Module via the IP Office system's LAN2 (WAN) port should be avoided for more than 30 users.

They should also be avoided where NAT is being applied to traffic between LAN1 and LAN2. These restrictions should be observed even when the IP Office system is in a Small Community Network where the H323 SCN trunks may be routed via the other LAN.

## 2.3 IP Office Configuration

The following are pre-requisites for the system supporting a Unified Communications Module.

- The IP Office system must be running IP Office Release 8.0 Q1 2012 Service Pack or higher software.
- The IP Office system must be configured and licensed for **Essential Edition** mode operation.
- The system must be configured to use either an external time server or to have its time and date set manually.

### Changing the System 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. For a system with an Unified Communications Module, the default **Time Setting Config Source** setting of **Voicemail Pro/Manager** should not be used. The value should be changed as follows:

- **To Use an External Time Server**  
Change the setting to **SNTP**. The additional fields for setting the address of the time server or servers to use are displayed.
- **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.


### Checking/Entering Licenses

The IP Office system requires an Essential Edition license.


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



2. Select **License**.

3. To add a license, click  and select **License**. Enter the new license and click **OK**. We recommend licenses are added by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.

4. 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.

5. Click on the  save icon to send the configuration back to the IP Office.

6. Use Manager to receive the configuration again and check that the status of the license. It should now be **Valid**.

---

## 2.4 System Shutdown

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 loss of configuration data.

### • ! WARNINGS

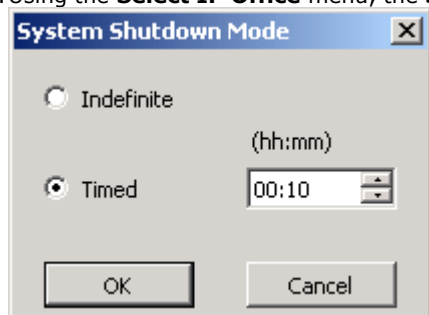
- A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause the loss of configuration data.
- This is not a polite shutdown, any user calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.
- 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.
- When shutdown, the LEDs shown on the system are as follows. Do not remove power from the system or remove any of the memory cards until the system is in this state:
  - LED1 on each IP500 base card installed will also flash red rapidly plus LED 9 if a trunk daughter card is fitted to the base card.
  - The CPU LED on the rear of the system will flash red rapidly.
  - The System SD and Optional SD memory card LEDs on the rear of the system are extinguished.
- 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.

### System Shutdown 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.

### System Shutdown Using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | System Shutdown**.
2. Using the **Select IP Office** menu, the **System Shutdown Mode** menu is displayed.



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.

### System Shutdown 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.

## 2.5 Inserting the Module

Once the system has been [shutdown](#)<sup>[20]</sup>, the module can be inserted.

### • ! WARNINGS

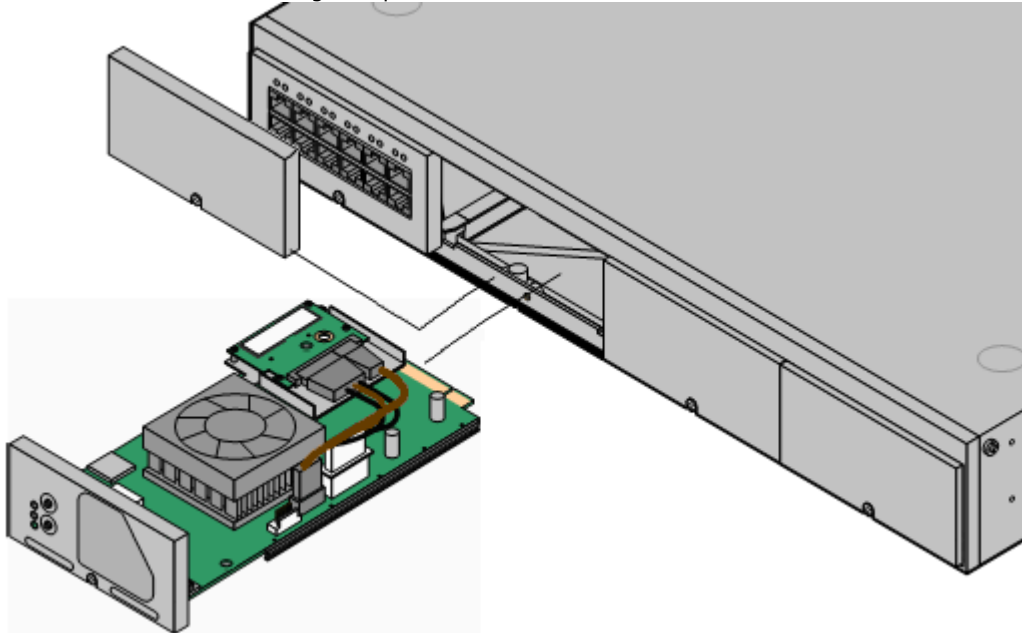
- Correct anti-static protection steps should be taken while handling circuit boards.
- Cards must never be added to or removed from the control unit while it has power connected.

### • Tools Required

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

### Installing the card:

1. If not already done, ensure that the plastic cover that fits over the external ports on the card's faceplate is in place. The plastic cover is supplied with the card.
2. Check that there is no power to the control unit. If the system is on, shutdown the system using one of the correct [shutdown methods](#)<sup>[20]</sup>.
  - Do not simply switch off power to a system. Whenever possible a system should be switched off using a correct shutdown method first.
3. Using a flat-bladed screwdriver, remove the cover from the slot on the front of the control unit that will be used for the module. This cover is no longer required but should be retained until installation has been completed.

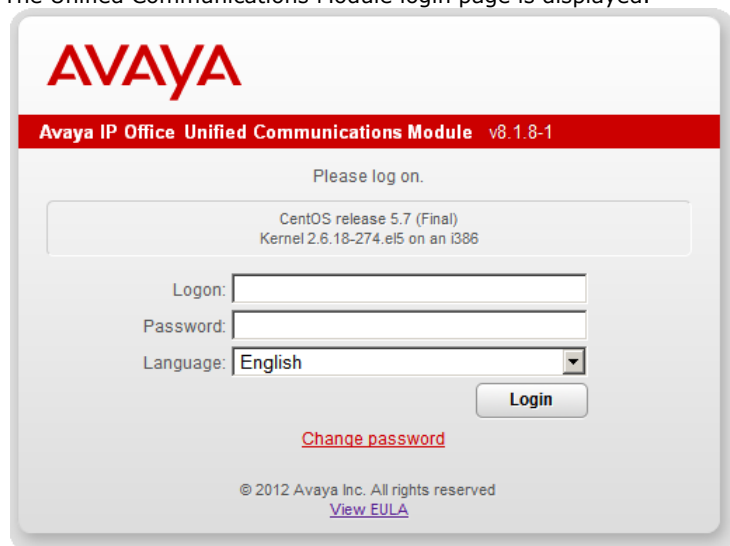


4. Allowing the module to rest against the bottom of the slot, begin sliding it into the control unit. When half inserted, check that the module rails have engaged with the slot edges by trying to gently rotate it. If the module rotates remove it and begin inserting it again.
5. While inserting the module, also check to ensure that cables on the module do not interfere with the insertion operation.
6. 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.
7. Using a flat-bladed screwdriver, secure the module.
8. Once the module is installed, reapply power to the system. The system will go through its normal start up process. The LEDs on the Unified Communications Module will also indicate the card's status, see [Module LEDs](#)<sup>[89]</sup>. The module is started once the lower LED changes to green with regular amber flashes.
9. The card now needs to be [initialized](#)<sup>[22]</sup>.

## 2.6 Initializing the Module Services

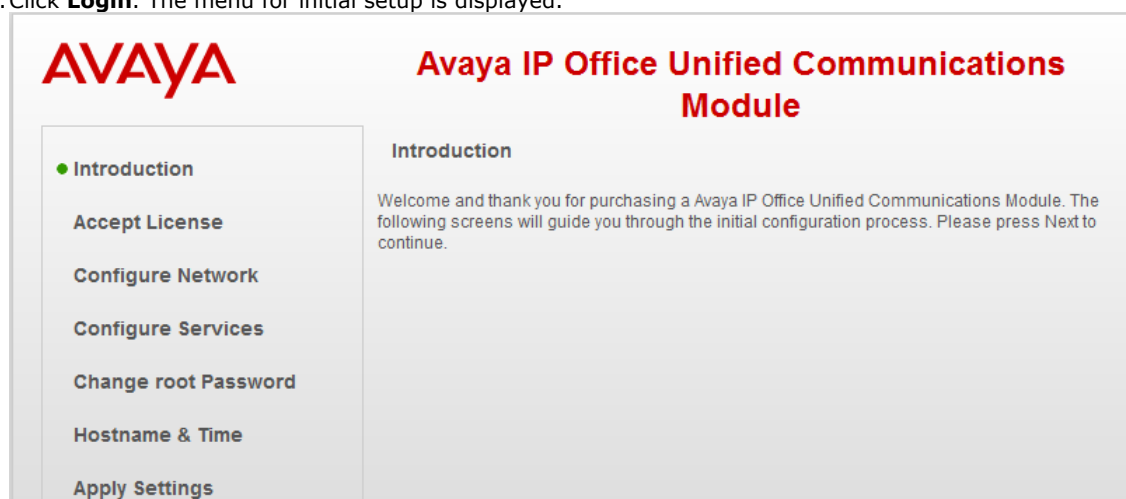
Following installation and start up of the newly installed module, the services provided by the module need to be started and initialized. This is done via web browser access to the module.

1. From a client PC, start the browser and enter **http://** followed by the LAN1 IP address of the IP Office system and **:7070**. For example **http://192.168.42.1:7070**.
  - The IP Office system's LAN1 address is used just for this initial configuration. During this process, you will set IP address details for the Unified Communications Module. They are then used for future access to the card. Note that only the LAN1 IP address should be used for this process, not the LAN2 IP address.
2. The Unified Communications Module login page is displayed.



The login page for the Avaya IP Office Unified Communications Module (v8.1.8-1) is displayed. It features the Avaya logo at the top. Below the logo, a red banner displays the module name and version. The page prompts the user to 'Please log on.' and shows the operating system details: 'CentOS release 5.7 (Final) Kernel 2.6.18-274.el5 on an i386'. There are input fields for 'Ligon:', 'Password:', and a 'Language:' dropdown menu set to 'English'. A 'Login' button is located below the password field. A link for 'Change password' is provided below the login button. At the bottom, it states '© 2012 Avaya Inc. All rights reserved' and includes a link to 'View EULA'.

3. Note the IP Office Release number shown after the **R** in the title bar of the login menu. If this does not match the software release of the IP Office system, then the software needs to be upgraded after completing the initialization. See [Upgrading the Software](#) <sup>[29]</sup>.
4. If the software release is as required, enter the default name and password.
  - The default name and password for cards installed with Release 8.1 or higher are **Administrator** and **Administrator**.
  - The default name and password for cards installed with Release 8.0 are **webcontrol** and **web**. Cards with Release 8.0 software need to be upgraded to Release 8.1 in order to operate correctly in a IP Office Release 8.1 system. This can be done by either [upgrading the individual components](#) <sup>[29]</sup> or [reinstalling the full card software](#) <sup>[97]</sup>.
5. Click **Login**. The menu for initial setup is displayed.



The initial setup menu for the Avaya IP Office Unified Communications Module is displayed. It features the Avaya logo and the module name. A sidebar on the left contains a list of menu items: 'Introduction' (selected), 'Accept License', 'Configure Network', 'Configure Services', 'Change root Password', 'Hostname & Time', and 'Apply Settings'. The main content area displays the 'Introduction' page, which includes a welcome message and instructions to press 'Next' to continue.

6. Click **Next**. If you accept the license, select **I Agree** and click **Next**.

7. Enter the IP address and DNS settings that the module should use. Refer to [IP Address Notes](#) <sup>18</sup> for details. These will be used for future access to the module and its applications. The Unified Communications Module should be assigned an IP address in the same subnet as the LAN1 interface of the IP Office system.

The screenshot shows the 'Avaya IP Office Unified Communications Module' configuration interface. On the left is a navigation menu with options: Introduction, Accept License, **Configure Network** (highlighted with a green dot), Configure Services, Change root Password, Hostname & Time, and Apply Settings. The main content area is titled 'Assign IP Address:' and contains a checkbox for 'Automatic (DHCP)' which is unchecked. Below this are three input fields: 'IP Address:' with the value '192.168.42.201', 'Netmask:' with '255.255.255.0', and 'Gateway:' with '192.168.42.1'. Below these is another section titled 'Assign System DNS Servers:' with a checkbox for 'Automatic (DHCP)' which is unchecked, and two input fields: 'Primary DNS:' with '8.8.8.8' and 'Secondary DNS:' with '8.8.4.4'.

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

The screenshot shows the 'Avaya IP Office Unified Communications Module' configuration interface. The left navigation menu is the same as in the previous screenshot, but 'Configure Services' is now highlighted with a green dot. The main content area is titled 'Configure Services' and contains two checkboxes: 'Voicemail Pro' which is checked, and 'one-X Portal for IP Office' which is also checked.

9. Click **Next**. Enter and confirm a new root password. This is the root user password for access to the operating system. It is not normally used during Unified Communications Module configuration and maintenance. Pick a new root password, and keep a record of it. Remember that the root password is a critical part of system security.

The screenshot shows the 'Avaya IP Office Unified Communications Module' configuration interface. The left navigation menu is the same, but 'Change root Password' is now highlighted with a green dot. The main content area is titled 'Change root Password' and includes a warning: '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 are two input fields: 'New Password:' and 'New Password (again):'. At the bottom, under 'Password complexity requirements:', there is a bullet point stating 'must contain at least 8 characters.'

10. Click **Next**. Enter basic details for the module.

The screenshot shows the 'Avaya IP Office Unified Communications Module' configuration interface. On the left is a sidebar with navigation links: Introduction, Accept License, Configure Network, Configure Services, Change root Password, Hostname & Time (selected with a green dot), and Apply Settings. The main area is titled 'Hostname & Time' and contains the following fields: Hostname (uc-module), Date (2012-08-17), Time (15:59), Timezone (Europe/London), Use UTC Time (unchecked), Use NTP (checked), and NTP Server (169.254.0.1).

- The default setting for the **NTP Server** is **169.254.0.1**. This is an internal address for the IP Office system. If this address is used, the IP Office system must be configured to get its time from an external source or to have its time set manually.

11. Click **Next**. A summary of the settings is displayed.

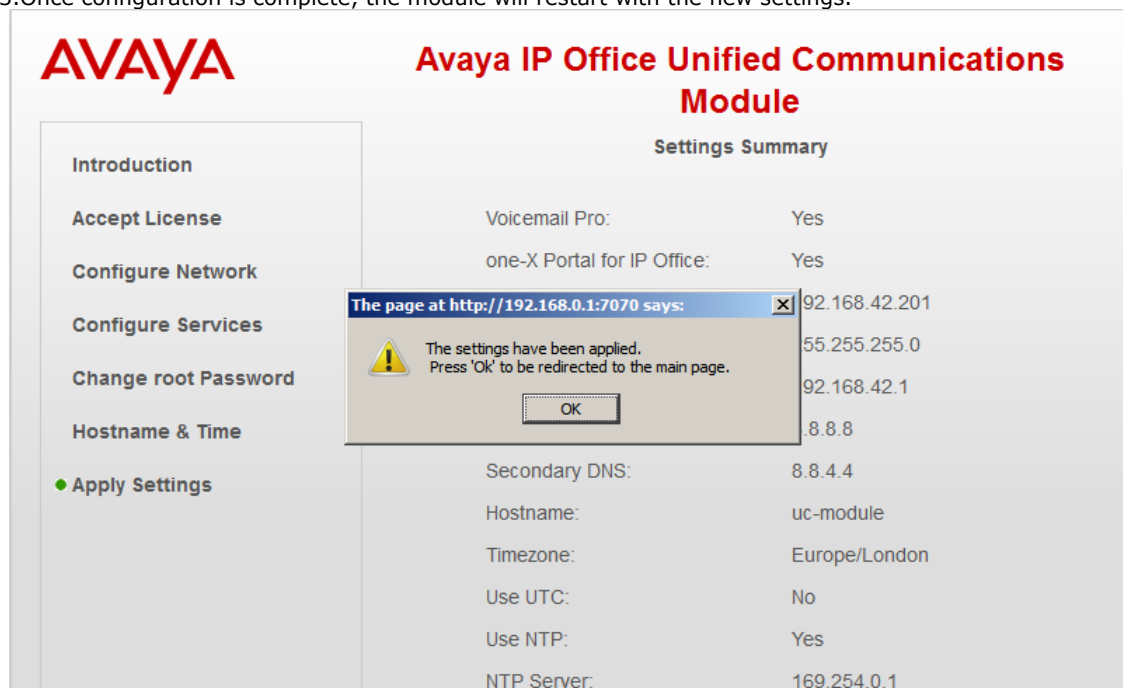
The screenshot shows the 'Settings Summary' page of the 'Avaya IP Office Unified Communications Module' configuration interface. The sidebar on the left has the same navigation links as the previous screen, with 'Apply Settings' now selected (indicated by a green dot). The main area, titled 'Settings Summary', displays a list of configuration parameters and their values:

Voicemail Pro:	Yes
one-X Portal for IP Office:	Yes
IP:	192.168.42.201
Netmask:	255.255.255.0
Gateway:	192.168.42.1
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4
Hostname:	uc-module
Timezone:	Europe/London
Use UTC:	No
Use NTP:	Yes
NTP Server:	169.254.0.1

12. Click **Apply**. Alternatively use the **Previous** and **Next** options to readjust the settings.



13. Once configuration is complete, the module will restart with the new settings.



14. The module will attempt to redirect your browser to the module's new IP address. If this does not succeed you will have to enter the new address manually. However, whichever way you will need to login again. You should now see the [server configuration menus](#)<sup>[74]</sup>.

15. Though the module and the selected services have been started, additional configuration to support those services may be required. See [Voicemail Pro Configuration](#)<sup>[32]</sup> and [one-X Portal for IP Office Configuration](#)<sup>[44]</sup>.

## 2.7 System and Module Start Up

The status of the Unified Communications Module can be checked using System Status Application.

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

The screenshot shows the 'IP Office System Status' application window. The title bar reads 'IP Office R8 System Status - System C (192.168.0.1) - IP500 V2 8.0 (301109)'. The AVAYA logo is in the top left. The main menu includes 'Help', 'Snapshot', 'LogOff', 'Exit', and 'About'. On the left, a navigation tree is expanded to 'System', which includes 'Memory Cards', 'Control Unit (IP500 V)', 'UC Modules', 'VoIP Trunks (1)', 'H.323 Extensions', 'SIP Extensions', 'Alarms (9)', 'Extensions (21)', 'Trunks (11)', 'Active Calls', 'Resources', 'Voicemail', and 'IP Networking'. The 'UC Modules' section is highlighted. The main content area is titled 'System Hardware Summary' and contains the following information:

Control Unit:	IP500 V2	Current Firmware:	8.0 (301109)
Edition:	IP Office	Boot Location:	System Primary
SD Card Slots:			
Slot Name			
System	SD04G, 4096 MB		
Optional	not present		
Control Unit Slots:			
Slot Number			
1	Base: Combo DS 6/Phone 2/VCM10	Daughter card: ATM4	
2	Base: DS 8	Daughter card: Dual BRI	
3	Base: UC Module		
4	Base: VCM64	Daughter card: Quad BRI	

3. Under **System** in the navigation tree, click on **UC Module**. Details of the module are displayed. The buttons at the bottom of the display can be used to shutdown and startup the module.

The screenshot shows the 'IP Office System Status' application window with the navigation tree expanded to 'System' > 'UC Modules' > 'Slot 3 UC'. The main content area is titled 'UC Processor Status' and displays the following information:

Variant:	UC Module	
Status:	Running	
Applications:	Voicemail Pro, one-X Portal	
Free Memory:	180 MB	
Total Memory:	2012 MB	
Free Disk Space:	23784 MB	
Total Disk Space:	29540 MB	
Temperature:	43 °C	

## 2.8 Logging on to the Web Menus

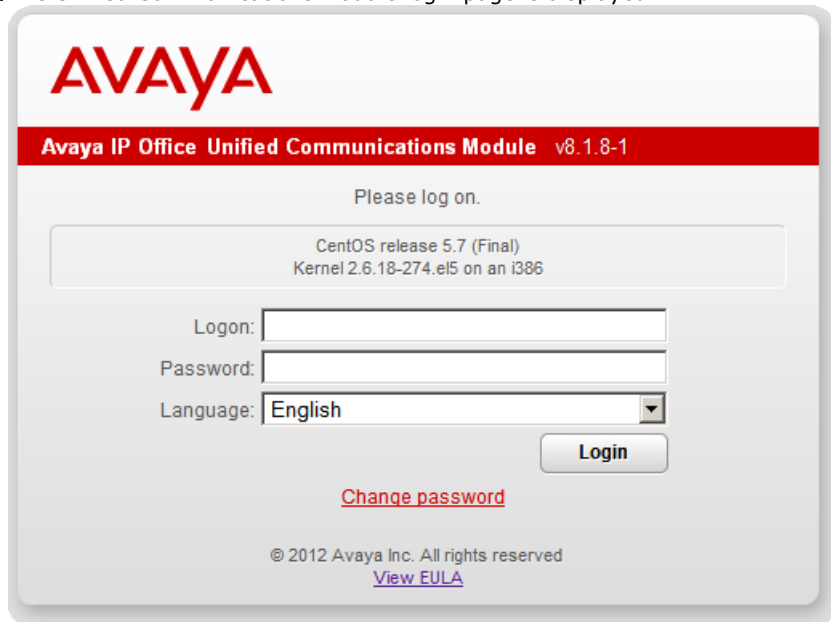
1. From a client PC, start the browser and enter **http://** followed by the address of the Unified Communications Module and **:7070**. The port number and protocol (**http** or **https**) used can be changed through the [Settings | General](#) menu after logging in.
2. The Unified Communications Module login page is displayed.

3. Select the **Language** required.
4. Enter the name and password for Unified Communications Module administration. The password can be changed by selecting the [Change Password](#) option.
  - The default name and password for cards installed with Release 8.1 or higher are **Administrator** and **Administrator**.
  - The default name and password for cards installed with Release 8.0 are **webcontrol** and **web**. Cards with Release 8.0 software need to be upgraded to Release 8.1 in order to operate correctly in a IP Office Release 8.1 system. This can be done by either [upgrading the individual components](#) or [reinstalling the full card software](#).
5. If the login is successful, the [Home](#) page for the server is displayed.

## 2.9 Changing the Web Password

From the Logon menu you can select the **Change Password** option to perform a password change. When selected, fields are displayed to entry the current password and for entry and confirmation of the new password. This password is also used for [SSH file access](#)<sup>[106]</sup> to the server.

1. From a client PC, start the browser and enter **http://** followed by the address of the Unified Communications Module and **:7070**. The port number and protocol (**http** or **https**) used can be changed through the [Settings | General](#)<sup>[77]</sup> menu after logging in.
2. The Unified Communications Module login page is displayed.



The login page features the Avaya logo at the top. Below it, a red banner reads 'Avaya IP Office Unified Communications Module v8.1.8-1'. The main heading is 'Please log on.'. A system information box displays 'CentOS release 5.7 (Final)' and 'Kernel 2.6.18-274.el5 on an i386'. The login form includes fields for 'Logon:', 'Password:', and a 'Language:' dropdown menu set to 'English'. A 'Login' button is positioned to the right of the password field. Below the form is a red link for 'Change password'. At the bottom, it shows '© 2012 Avaya Inc. All rights reserved' and a 'View EULA' link.

3. Select the **Language** required.
4. Click on the **Change password** link. The change password menu is displayed.



The change password page has the same header as the login page. The heading is 'Please type the old and the new password.'. The system information box is identical. The form contains three password fields: 'Old Password:', 'New Password:', and 'Confirm Password:', each filled with dots. 'Ok' and 'Cancel' buttons are below the fields. A section titled 'Password complexity requirements:' lists '• Minimum password length: 8'. The footer includes '© 2012 Avaya Inc. All rights reserved' and a 'View EULA' link.

5. Enter the current password and the new password.
  - The new password must meet the complexity requirements that are displayed on the menu. When logged in you can [change the password complexity requirements](#)<sup>[54]</sup> for future password changes through the **Settings** menu.
6. Click **OK**. The menu will confirm whether the change was successful or not.
7. If the new password is accepted, click **Cancel** to return to the **Login** menu and then [login](#)<sup>[51]</sup> with the new password.

## 2.10 Upgrading the Software

The Unified Communications Module is supplied with a full set of software pre-installed. However, this may not match the software level of the IP Office system or the latest set of application software available for the module. Therefore it may be necessary to upgrade the card after installation.

Upgrades for the Unified Communications Module will be made available as a set of **.rpm** files for the components being upgraded. Sets of **.rpms**, typically those for the applications, may be combined into a single **.zip** file that can be used for the upgrade, reducing the number of upgrade process steps. The upgrade files will be made available via the Avaya support website <http://support.avaya.com>.

- A single .zip file may be made available for upgrading the applications. Use of the zip file simplifies the number of repeated steps required for the upgrade process. Separate .rpm files may also be made available for voicemail language prompts and voicemail TTS languages. Refer to the IP Office Technical Bulletins for each release to confirm the new .zip and .rpms available and whether any other pre-requisite .rpm files are also needed. If an .iso file is available, individual .rpm files can be extracted from the .iso file is needed without having to install the .iso.
- Note that .rpm files are also used by other Linux based IP Office solutions. In all cases you must confirm that the .rpm file is specifically listed as compatible for use with the Unified Communications Module.

Using .zip or .rpm files is the recommended method for upgrading rather performing a [full .iso reinstallation](#)<sup>[97]</sup> as it is both quicker and does not remove the current user data. However, a full data backup is still recommended. It also has the advantage that it is done remotely from a PC logged in for web control rather than requiring physical access to the system to boot it from the new .iso image.

### • ! WARNINGS

#### • **Backup Application Data**

Before attempting the following process, all user data for the services provided by the Unified Communications Module should be backed-up to a safe location other than the Unified Communications Module.

##### • **Voicemail Pro**

The Voicemail Pro client can be used to perform a manual backup of the voicemail data including, if selected, user messages and prompts. The default location for the backup is on the Unified Communications Module. Therefore, following the backup, SSH file transfer should be used to copy the backup files to another PC.

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

The AFA menus supported by one-X Portal for IP Office can be used to perform a backup to another PC or to an FTP server.

##### • **Unified Communications Module**

Following the reinstall, the IP address settings of the module must be set again. Login to the modules web control menus and not the settings on the various menus.

#### • **Loss of Services**

During this process, the services provided by the Unified Communications Module are not available to users. Therefore users should be warned in advance or this process should be performed outside normal business hours.

#### • **Read the Technical Bulletins**

Ensure that you have read and understood all Avaya Technical Bulletins relevant to the software release. These will include notes and information that was not available at the time this document was created.

---

## Upgrading Software

1. Take a backup of the one-X Portal for IP Office and Voicemail Pro applications. The backup is done using the normal backup procedure for those applications.
2. Login to the web control menus.
3. Select the **Settings | General** menu.
  - a. In the **Web Control** section change the **Inactivity timeout** to **1 hour**. This ensures that the web control session does not timeout while downloading the updated applications files.
  - b. Click **Save**. It will be necessary to login to the web control menus again.
4. 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. When the file is uploaded, select the **Updates | Services** menu. Click on **Update All**.
  - d. Click **OK** when warned about services stopping.
  - e. After update is complete, the web control application will be restarted and the web session will end. A warning about restarting the session or an error timeout message may appear.
5. Login to the web control menus.
6. Select the **Updates | Services** menu.
  - a. Verify that all the application have been updated in the **Updates** window. If not, then individually update the application by clicking the **Update** button.
  - b. From the updates window, check that the **AvayaVersioning** application is installed. If not, click the Install button next to the application.
7. If voicemail is configured or likely to be configured to use a language other than English UK or English US, then a manual update of the prompt files for the language is required.
  - a. Select the **Setting | General** menu.
  - b. For the **Applications** options, select **Local**.
  - c. Select the .rpm file for the language. The .iso image can also be used, the prompt files being at the following location on the iso image **/avaya/vmpro**.
  - d. When the language file is uploaded, select the **Updates | Services** menu. Select the language in the list of services and click **Update**.
8. If for Voicemail Pro, text to speech (TTS) is being used, the TTSEnglish rpm also needs to be upgraded the same way. This is done in the same way as for the language prompt files in the section above.
9. Once all the new .rpm files have been installed, select **Home**. Check that the required services are running. Restart the services if necessary.
10. Verify that all the data from Voicemail Pro and one-X Portal for IP Office has migrated properly. Otherwise, restore the data from the backups taken at the start of the process.

# **Chapter 3.**

## **Voicemail Pro Configuration**

---

## 3. Voicemail Pro Configuration

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

Details of IP Office and Voicemail Pro configuration are covered by the Voicemail Pro Linux 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](#) <sup>33</sup>.
- ii. [Check the Voicemail Type Setting](#) <sup>34</sup>.

#### b. Voicemail Pro Configuration

- i. [Install the Voicemail Pro client](#) <sup>35</sup>.
- ii. [Log in to the Voicemail Pro server](#) <sup>36</sup>.
- iii. [Change the default administrator password](#) <sup>36</sup>.

### 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](#) <sup>38</sup>.

### 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](#) <sup>83</sup> menu. For full details refer to the Voicemail Pro Linux Installation manual.






### 3.1 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)**  
This license is required for use of the Voicemail Pro application. It also enables 4 voicemail ports. It is also required as a pre-requisite for the user profile licenses required for one-X Portal for IP Office users. The Unified Communications Module acts as an automatic **Preferred Edition** license for the system.
  - **Preferred Edition Additional Voicemail Ports**  
These licenses can be used to add additional voicemail ports in addition to the 4 enabled by the **Preferred Edition (Voicemail Pro)** license above. Multiple licenses can be added, up to a total of 20 ports when running Voicemail Pro and one-X Portal for IP Office, or up to 40 ports when running just Voicemail Pro.
  - **VMPPro TTS (Linux Voicemail Pro)**  
This license enables the use of text-to-speech facilities using the optional Linux TTS software. One license per simultaneous instance of TTS usage. This license is also used for user email reading.

#### Entering Licenses

1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **License**.
3. To add a license, click  and select **License**. Enter the new license and click **OK**. We recommend licenses are added by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.
4. 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.
5. Click on the  save icon to send the configuration back to the IP Office.
6. Use Manager to receive the configuration again and check that the status of the license. It should now be **Valid**.

## 3.2 IP Office Configuration

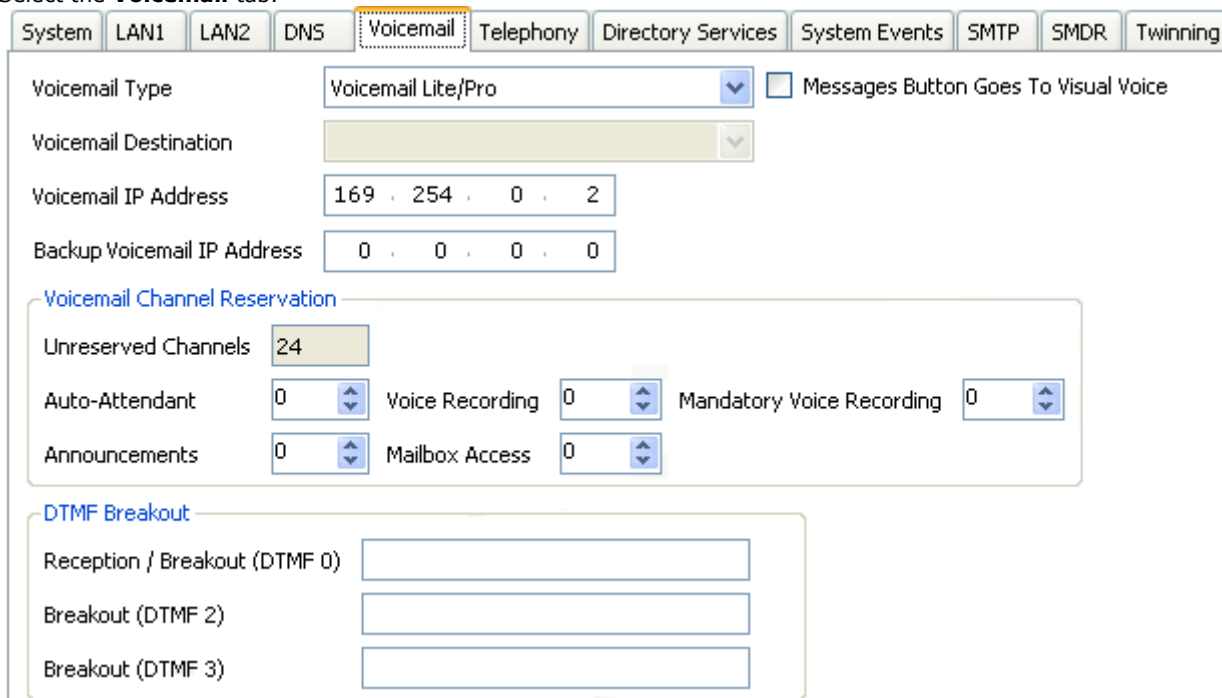
When a new Unified Communications Module running Voicemail Pro is added to a new system, the system configuration is automatically adjusted to use that voicemail server. However, this should be confirmed by checking the **Voicemail Type** and Voicemail IP Address settings in the IP Office configuration.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

If a different role is intended for the voicemail server (see [Small Community Networks](#)<sup>[13]</sup>), refer to the Voicemail Pro Installation Manual. This section only covers voicemail server support for the IP Office in which it is installed.

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

2. Select  **System**.

3. Select the **Voicemail** tab.



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

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

Voicemail Destination

Voicemail IP Address 169 . 254 . 0 . 2

Backup Voicemail IP Address 0 . 0 . 0 . 0

**Voicemail Channel Reservation**

Unreserved Channels 24

Auto-Attendant 0 Voice Recording 0 Mandatory Voice Recording 0

Announcements 0 Mailbox Access 0

**DTMF Breakout**

Reception / Breakout (DTMF 0)

Breakout (DTMF 2)

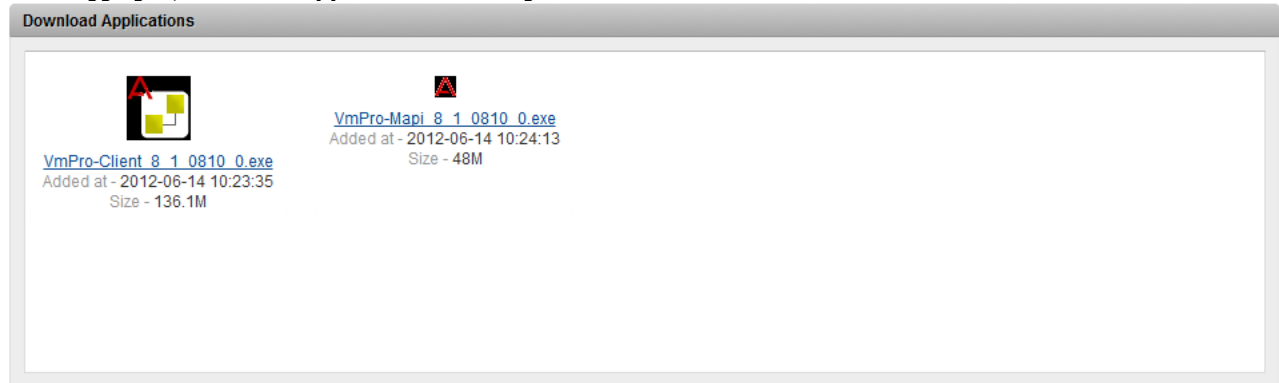
Breakout (DTMF 3)

- The **Voicemail Type** should be set to **Voicemail Lite/Pro**.
  - The **Voicemail IP Address** of 169.254.0.2 is an [internal IP address](#)<sup>[18]</sup> used for connection between the IP Office and the Unified Communications Module.
    - 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.

### 3.3 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.

1. From a client PC, start the browser and enter **http://** followed by the address of the server and **:7070**.
2. The server's web login page is displayed. Enter the name and password configured for server administration.
3. After logging in, select the **Apps Center** heading.



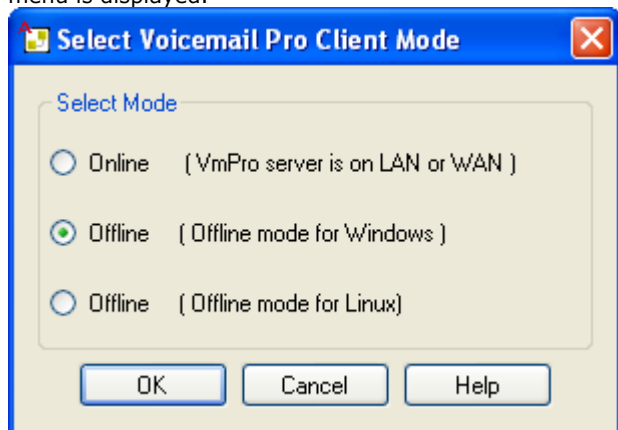
4. Click on the link for the Voicemail Pro client file in order to download the software package for installing the client.
5. Once the package has been downloaded, run it to install the Voicemail Pro client.

### 3.4 Logging in to the Voicemail Server

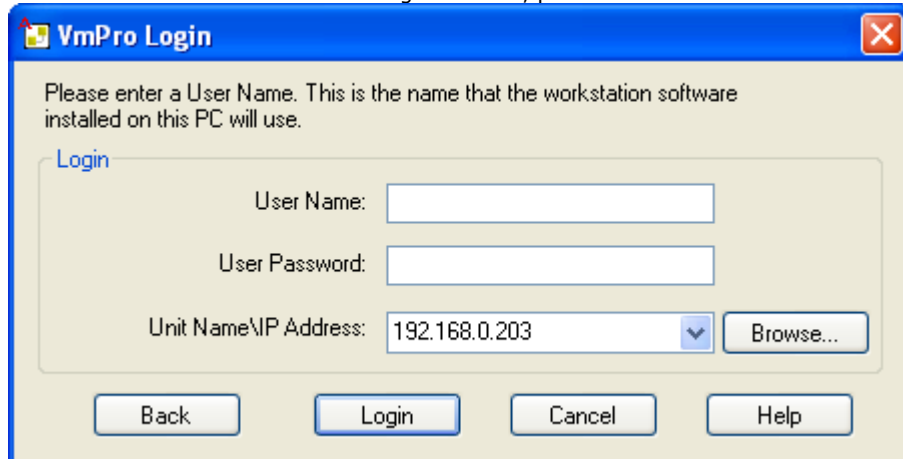
To connect to a remote voicemail server you will need to login using the name and password of an administrator account already configured on that server. The default account is **Administrator** and **Administrator**.

#### To Login with the Voicemail Pro Client

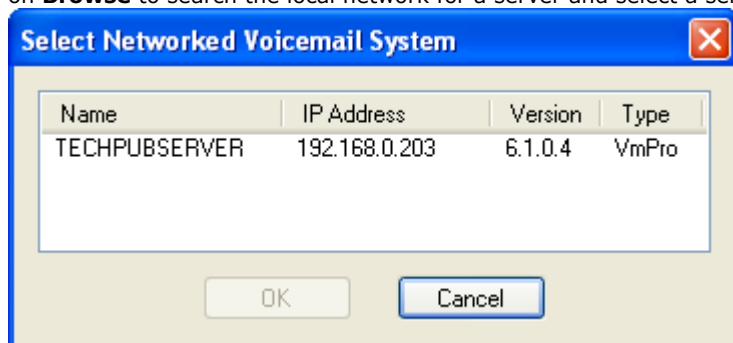
1. From the **Start** menu, select **Programs | IP Office | Voicemail Pro Client**.
2. The Voicemail Pro Client window opens. If the client has been started before, it will attempt to start in the same mode as it previously used. If it cannot do that or it is the first time the client has been started, 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](#)<sup>37</sup>.

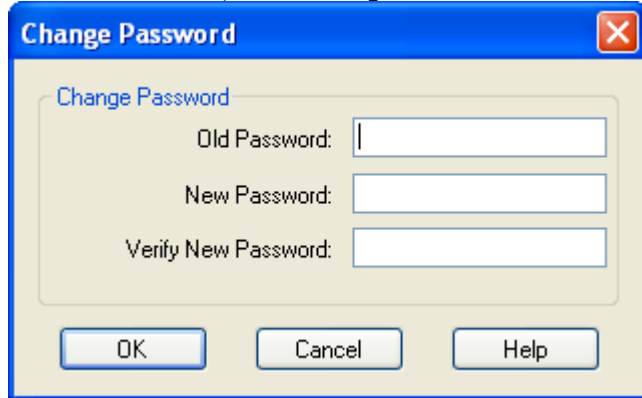
### 3.5 Changing the Voicemail Server Password

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**.

A screenshot of a 'Change Password' dialog box. The dialog has a blue title bar with the text 'Change Password' and a red close button. Inside the dialog, there is a section titled 'Change Password' with three text input fields: 'Old Password:', 'New Password:', and 'Verify New Password:'. Below the input fields are three buttons: 'OK', 'Cancel', and 'Help'.

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

---

## 3.6 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 device. Otherwise, if the backup is too large for the USB2 memory device, SSH file transfer can be used.

### Backing Up the Old Voicemail Server

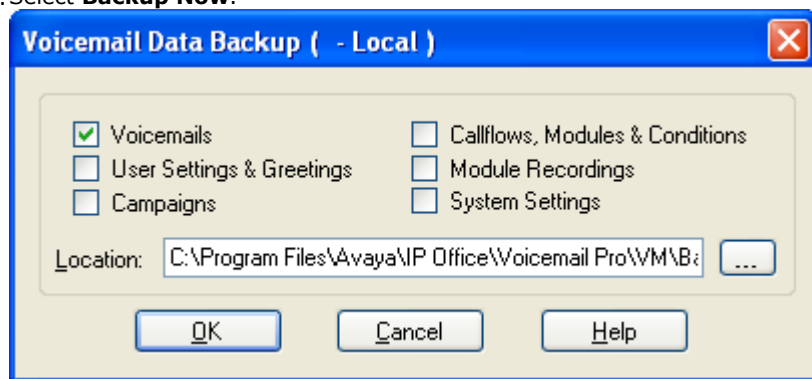
A full immediate backup of all the voicemail server settings, prompts and messages can be obtained using the Voicemail Pro client.

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.

### Shutting 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.

### Transferring the Backup to a USB2 Memory Device

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 device.

- 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 device capacity, Copy the backup folder and all its content onto a USB2 memory device. 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](#), 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 device.
  - 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 device capacity, Copy the backup folder and all its content onto a USB2 memory device. Do not put the folder into another folder or change the folder name.

### Loading the Backup onto the New Server from a USB2 Memory Device

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

1. Insert the USB2 memory device 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 device.
6. Select the backup on the USB2 memory device and click **OK**.
7. Do not remove the USB2 memory device until all USB2 memory device activity has ceased.
8. Once the restore has been completed, on the **Home** menu, **Stop** and then **Start** the voicemail service.

### 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 device, 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 **Home** menu, **Stop** and then **Start** the voicemail service.

---

## 3.7 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. That includes support for both normal and authenticated voice recording settings configured on the IP Office switch.

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.

## 3.8 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 used for prompts, that folder will not be 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.

### Manually Backing Up a Custom Folder

1. Using an [SSH file transfer tool](#)<sup>[106]</sup>, copy the folder **Custom** from **/opt/vmpro** to your PC to create a backup of the folder.

### Manually Restoring a Custom Folder

1. To restore the folder, again using an SSH file transfer tool, copy the folder to the **/home/webcontrol** folder on the server.
2. Using the SSH command line, you now need to copy the **Custom** folder from **/home/webcontrol** 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 at the on the server:**
      - a. At the **Command:** prompt, enter **login**.
      - b. At the **login:** prompt enter **webcontrol**.
      - c. At the **Password:** prompt, enter the password (the default is **web**).
    - **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 **webcontrol**.
        - 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](#)<sup>[52]</sup>, the default is **web**.
  - 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/webcontrol**.
  - 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 4.**

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

---

## 4. 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](#) <sup>45</sup>

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](#) <sup>46</sup>

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](#) <sup>47</sup>

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](#) <sup>48</sup>

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.

## 4.1 Adding Licenses



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

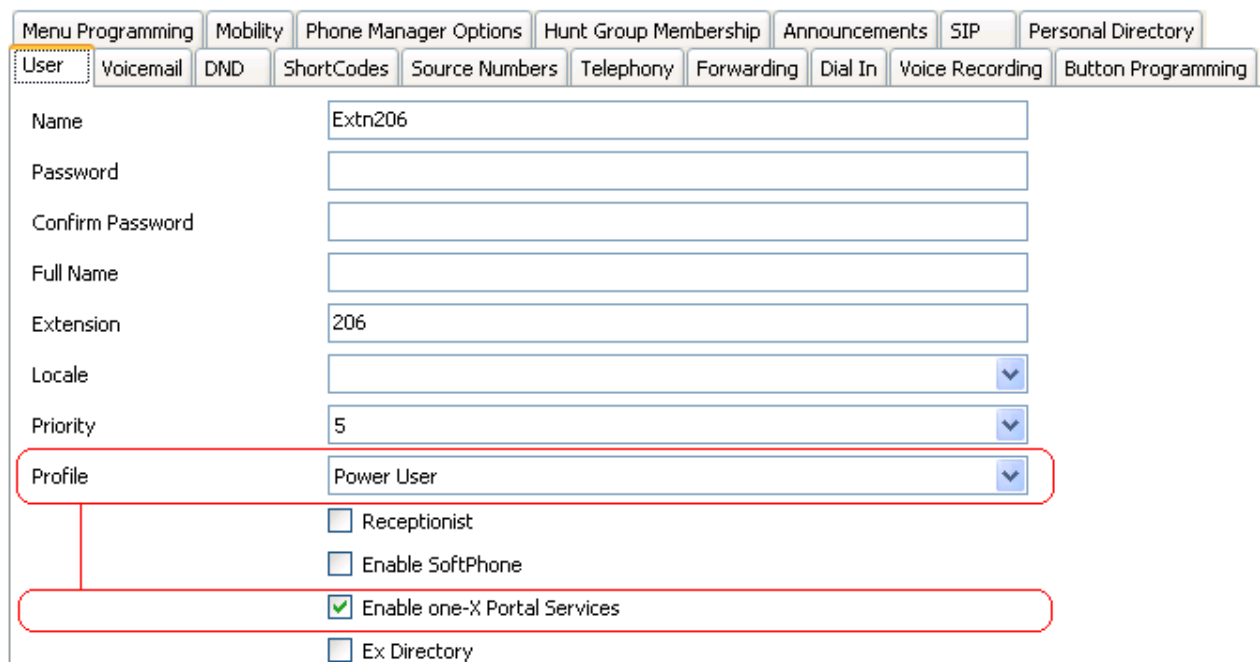
### Entering Licenses

1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select  **License**.
3. To add a license, click  and select **License**. Enter the new license and click **OK**. We recommend licenses are added by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.
4. 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.
5. Click on the  save icon to send the configuration back to the IP Office.
6. Use Manager to receive the configuration again and check that the status of the license. It should now be **Valid**.


## 4.2 Enabling one-X Portal for IP Office Users

Those users who want to use the one-X Portal for IP Office application need to have their **Profile** set to **Office Worker**, **Teleworker** or **Power User** and the **Enable one-X Portal Services** option selected. This requires [available licenses](#)<sup>[45]</sup> for those roles.

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			
<b>User</b>	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.

## 4.3 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](#)<sup>13</sup>, 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.

### one-X Portal for IP Office Login

1. Open a web browser and enter the IP address of the Unified Communications Module followed by **:8080/oneportal-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.

---

## 4.4 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.

### AFA Login

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.



# **Chapter 5.**

## **Server Maintenance**

---

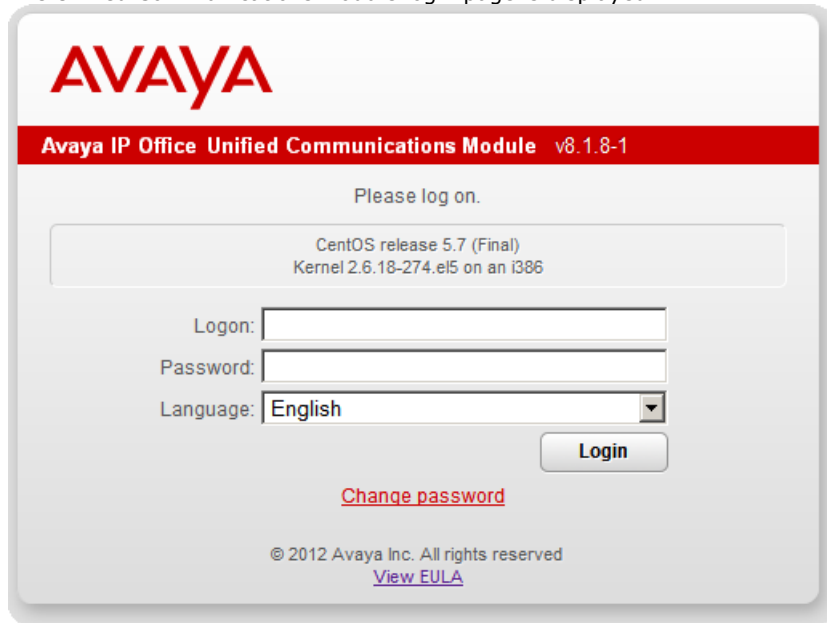
## 5. Server Maintenance

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.

- [Logging In](#) <sup>51</sup>
- [Changing the Web Password](#) <sup>52</sup>
- [Starting/Stopping Application Services](#) <sup>55</sup>
- [Server Shutdown](#) <sup>56</sup>
- [Rebooting the Server](#) <sup>56</sup>
- [Changing the IP Address Settings](#) <sup>57</sup>
- [Date and Time Settings](#) <sup>58</sup>
- [Upgrading an Application](#) <sup>61</sup>
- [Uninstalling an Application](#) <sup>63</sup>
- [Setting Update Repositories](#) <sup>64</sup>

## 5.1 Logging In

1. From a client PC, start the browser and enter **http://** followed by the address of the Unified Communications Module and **:7070**. The port number and protocol (**http** or **https**) used can be changed through the [Settings | General](#) menu after logging in.
2. The Unified Communications Module login page is displayed.



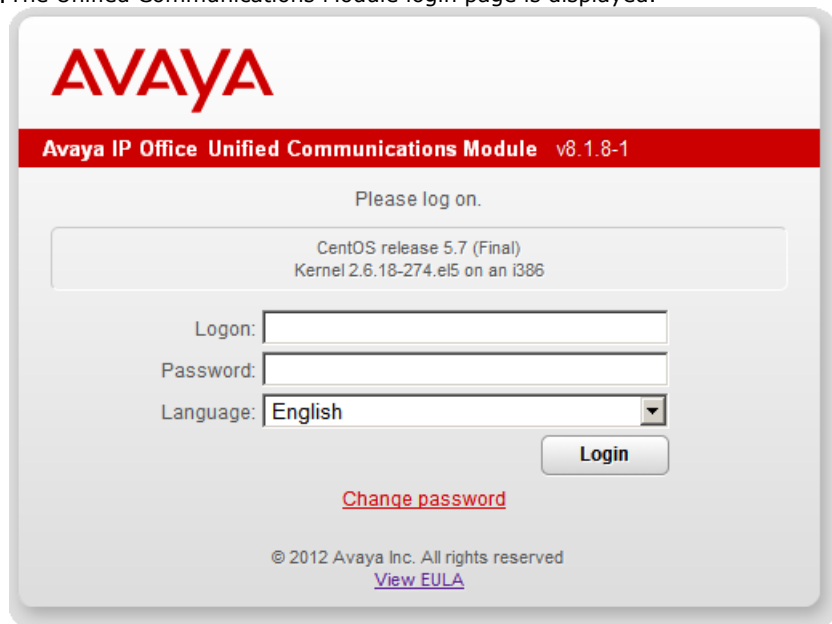
The image shows the login page for the Avaya IP Office Unified Communications Module. At the top is the Avaya logo in red. Below it is a red banner with the text "Avaya IP Office Unified Communications Module v8.1.8-1". The main content area is light gray and contains the text "Please log on." followed by a box displaying system information: "CentOS release 5.7 (Final)" and "Kernel 2.6.18-274.el5 on an i386". Below this are three input fields: "Ligon:" (with a typo in the label), "Password:", and "Language:" (with a dropdown menu showing "English"). To the right of the "Language:" field is a "Login" button. Below the input fields is a red link labeled "Change password". At the bottom, there is a copyright notice "© 2012 Avaya Inc. All rights reserved" and a link "View EULA".

3. Select the **Language** required.
4. Enter the name and password for Unified Communications Module administration. The password can be changed by selecting the [Change Password](#) option.
  - The default name and password for cards installed with Release 8.1 or higher are **Administrator** and **Administrator**.
  - The default name and password for cards installed with Release 8.0 are **webcontrol** and **web**. Cards with Release 8.0 software need to be upgraded to Release 8.1 in order to operate correctly in a IP Office Release 8.1 system. This can be done by either [upgrading the individual components](#) or [reinstalling the full card software](#).
5. If the login is successful, the [Home](#) page for the server is displayed.

## 5.2 Changing the Web Password

From the Logon menu you can select the **Change Password** option to perform a password change. When selected, fields are displayed to entry the current password and for entry and confirmation of the new password. This password is also used for [SSH file access](#)<sup>[106]</sup> to the server.

1. From a client PC, start the browser and enter **http://** followed by the address of the Unified Communications Module and **:7070**. The port number and protocol (**http** or **https**) used can be changed through the [Settings | General](#)<sup>[77]</sup> menu after logging in.
2. The Unified Communications Module login page is displayed.



The image shows the login page of the Avaya IP Office Unified Communications Module. At the top is the Avaya logo. Below it is a red banner with the text "Avaya IP Office Unified Communications Module v8.1.8-1". The main heading is "Please log on." Below this is a box containing system information: "CentOS release 5.7 (Final)" and "Kernel 2.6.18-274.el5 on an i386". There are three input fields: "Logon:" (text), "Password:" (password), and "Language:" (dropdown menu set to "English"). To the right of the language dropdown is a "Login" button. Below the input fields is a red link "Change password". At the bottom, it says "© 2012 Avaya Inc. All rights reserved" and "View EULA".

3. Select the **Language** required.
4. Click on the **Change password** link. The change password menu is displayed.



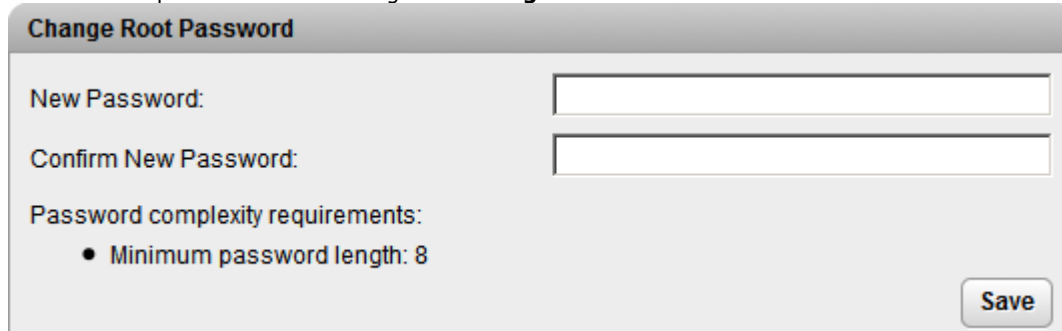
The image shows the change password page of the Avaya IP Office Unified Communications Module. At the top is the Avaya logo. Below it is a red banner with the text "Avaya IP Office Unified Communications Module v8.1.8-1". The main heading is "Please type the old and the new password." Below this is a box containing system information: "CentOS release 5.7 (Final)" and "Kernel 2.6.18-274.el5 on an i386". There are three input fields: "Old Password:" (password), "New Password:" (password), and "Confirm Password:" (password). Below the input fields are "Ok" and "Cancel" buttons. Below the buttons is the text "Password complexity requirements:" followed by a bullet point: "• Minimum password length: 8". At the bottom, it says "© 2012 Avaya Inc. All rights reserved" and "View EULA".

5. Enter the current password and the new password.
  - The new password must meet the complexity requirements that are displayed on the menu. When logged in you can [change the password complexity requirements](#)<sup>[54]</sup> for future password changes through the **Settings** menu.
6. Click **OK**. The menu will confirm whether the change was successful or not.
7. If the new password is accepted, click **Cancel** to return to the **Login** menu and then [login](#)<sup>[51]</sup> with the new password.

## 5.3 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.

1. [Login](#) <sup>[51]</sup> 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.



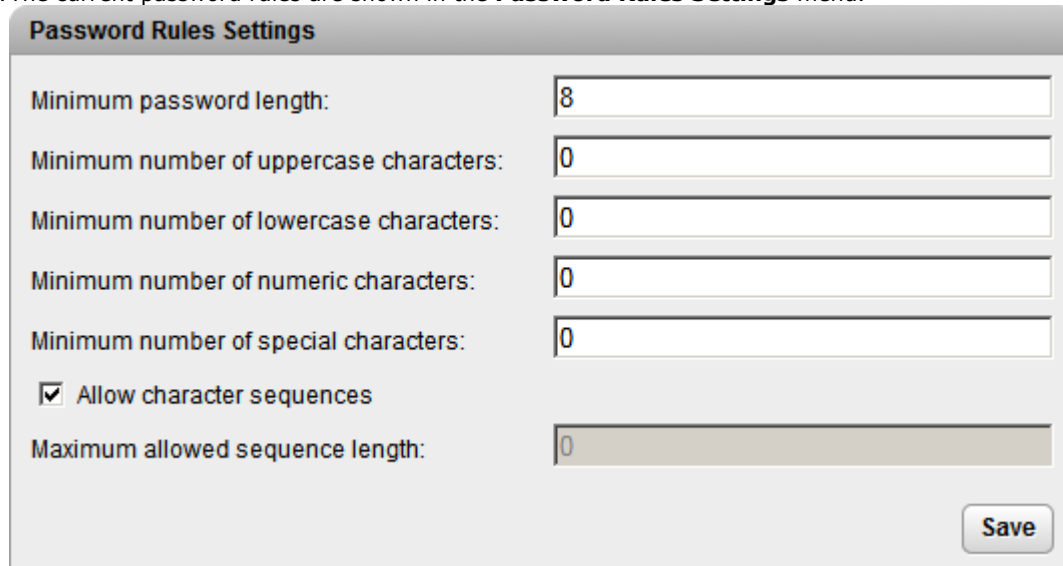
The screenshot shows a web form titled "Change Root Password". It contains two input fields: "New Password:" and "Confirm New Password:". Below these fields, there is a section for "Password complexity requirements:" which lists a single bullet point: "• Minimum password length: 8". A "Save" button is located in the bottom right corner of the form.

- **New Password**  
Enter the new password for the server's root account.
  - **Confirm New Password**  
Confirm the new password.
4. Note the rules displayed for the password entry, enter the new password. The password complexity requirements are set in the [Password Rules Settings](#) <sup>[54]</sup> menu. The rules set there are applied to changing both the [root password](#) <sup>[53]</sup> and changing the web control [administrator password](#) <sup>[52]</sup>.
  5. Click **Save**. The menu will confirm if the new password was accepted.

## 5.4 Setting the Password Rules

You can configure the rules applied to new passwords. These rules are applied when [changing the web administrator password](#)<sup>[52]</sup>. They are also applied when changing the [root password](#)<sup>[53]</sup>. The current rules are shown on the change password menus when someone attempts to change either password.

1. [Login](#)<sup>[51]</sup> to the server's web configuration pages.
2. Select **Settings** and click on the **System** tab.
3. The current password rules are shown in the **Password Rules Settings** menu.



**Password Rules Settings**

Minimum password length: 8

Minimum number of uppercase characters: 0

Minimum number of lowercase characters: 0

Minimum number of numeric characters: 0

Minimum number of special characters: 0

☒ Allow character sequences

Maximum allowed sequence length: 0

Save

- **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.


4. Adjust the rules are required and then click **Save**.

## 5.5 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.

### 5.5.1 Starting a Service


1. [Login](#)  to the server's web configuration pages.
2. Select **Home**. 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.

### 5.5.2 Stopping a Service

1. [Login](#)  to the server's web configuration pages.
2. Select **Home**. The services and their current status (running or stopped) are listed.
3. To stop a particular service click on the **Stop** button next to the service. To stop all the services that are currently running, click on the **Stop All** button.
4. The service's status changes to stopping 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**.

### 5.5.3 Setting a Service to Auto Start

By default all the application services are automatically started.

1. [Login](#)  to the server's web configuration pages.
2. Select **Home**. 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.

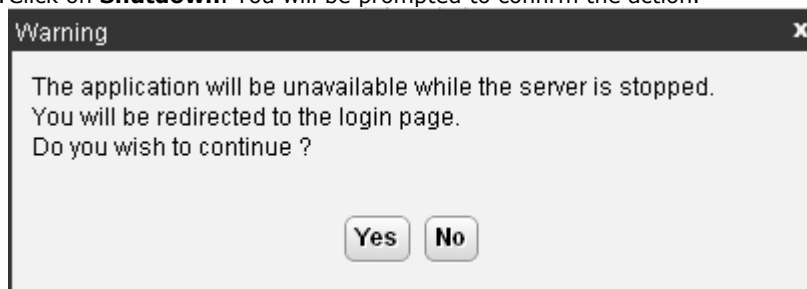
---

## 5.6 Server Shutdown

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.

For the Unified Communications Module, the card can be shutdown or started up using the upper switch on its front panel. See [Unified Communications Module](#) <sup>[10]</sup>.

1. [Login](#) <sup>[51]</sup> to the server's web configuration pages.
2. After logging select the [Home](#) <sup>[69]</sup> page. This page includes a server **Shutdown** button.
3. Click on **Shutdown**. You will be prompted to confirm the action.

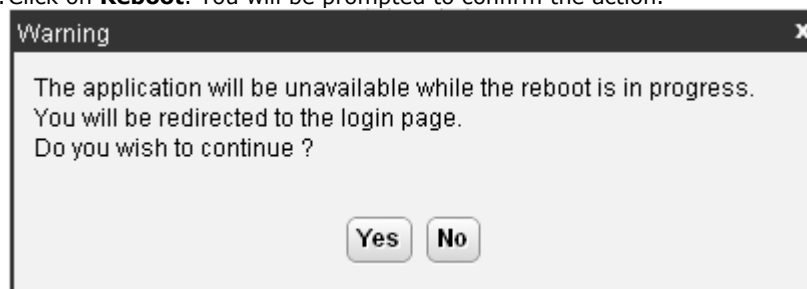


4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page will be displayed again. Do not login again as the Unified Communications Module will still be in the process of stopping services.
6. After a few minutes, typically no more than 2 minutes though this will vary depending on the hardware specification of the server, the server will shutdown.
7. Switch off power to the server.

## 5.7 Rebooting the Server

Rebooting the server will stop all currently running services and then stop and restart the server. Only those application services which are set to [Auto Start](#) <sup>[55]</sup> will be automatically restarted after the reboot.

1. [Login](#) <sup>[51]</sup> to the server's web configuration pages.
2. After logging select the [Home](#) <sup>[69]</sup> page. This page includes a server **Reboot** button.
3. Click on **Reboot**. You will be prompted to confirm the action.



4. Click **Yes** to confirm that you want to proceed with the reboot.
5. The login page will be displayed again. Do not login again immediately as the Unified Communications Module will still be in the process of stopping services prior to a reboot of the server.
6. After a few minutes, typically no more than 5 minutes though this will vary depending on the hardware specification of the server, you should be able to login again.
7. Once logged in you can manually restart any services required if not set to **Auto Start**.



## 5.8 Changing the IP Address Settings

The IP address and other network settings used by the server can be changed through the server's web configuration pages.

- **Warning**

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

- The port and protocol used to access the web control menus can also be [changed](#) <sup>[59]</sup>.

1. [Login](#) <sup>[51]</sup> to the server's web configuration pages.

2. Select **Settings**.

3. Select **System**.

4. The IP address settings are shown in the **Network** section.

- **Network Interface**

This drop down allows selection of network interfaces is currently being configured by the web form. This field is fixed to **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**

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

- **IP Address**

Displays the IP address set for the server. If DHCP is not being used, the field can be edited to change the setting. The Unified Communications Module is physically connected to the LAN1 network of the system and needs to have an address on that subnet. See [IP Address Notes](#) <sup>[18]</sup>.

- **Subnet Mask**

Displays the subnet mask applied to the IP address. If DHCP is not being used, the field can be edited to change the setting.

- **Default Gateway**

Displays the default gateway settings for routing. If DHCP is not being used, the field can be edited to change the setting.

- **System DNS**

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


- **Automatically obtain DNS from provider**

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


5. Click **Save**. The server PC is restarted.

---

## 5.9 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 [Home](#)  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 Officesystem to be configured to get its time from a specific external SNTP server or to have its time set manually.

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 [Home](#)  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**.

## 5.10 Changing the Web Control Port

By default, access to the web control menus uses http and port 7070. These can be changed if required.

- **Warning**

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

1. [Login](#)  to the server's web configuration pages.
2. Select **Settings**.
3. Select **General**.
4. The **Application Port** and **Protocol** settings are shown in the **Web Control** section.
  - **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 set it to a value already used by another service or application.
  - **Protocol**  
Select the protocol used for connection. The default is **http**. The options are **http** or **https**.
5. Click **Save**. The server will advise you that it is restarting the web service and that you will need to login again.


---

## 5.11 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.

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.

## 5.12 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](#)<sup>[64]</sup>.

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.

- **Warning**

Before upgrading or changing the version of any installed application or operating system components, you must ensure that you have read the appropriate Avaya Technical Bulletins for the software release. The Technical Bulletins detail supported versions of software and known issues or additional actions required for upgrading.

The options in this section cover the upgrading of individual components of the operating system and applications supported by the Unified Communications Module. If a full reinstallation is necessary, following a backup of user data, the server can be [reinstalled from a USB2 memory device](#)<sup>[92]</sup>.

### 5.12.1 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](#)<sup>[66]</sup>.


1. [Login](#)<sup>[51]</sup> 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](#)<sup>[64]</sup> 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.

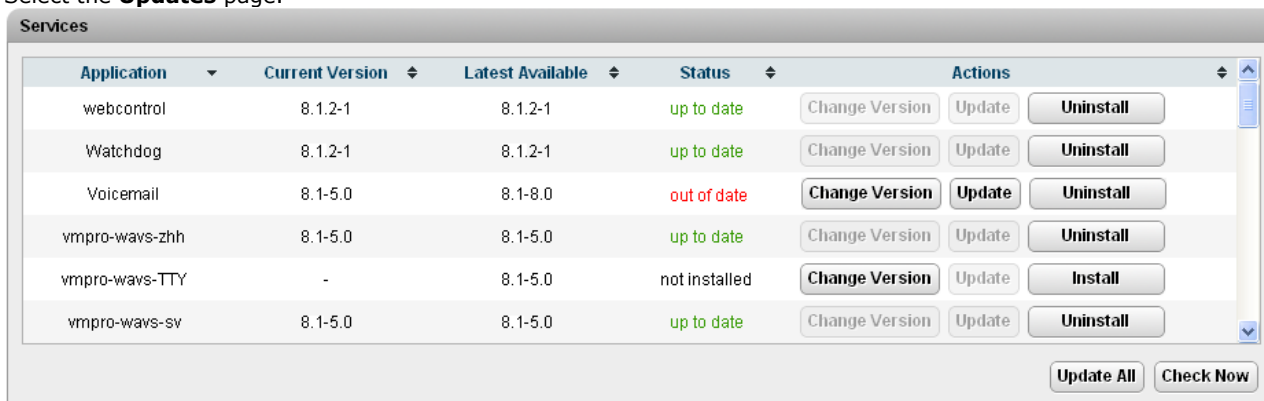
- **Voicemail Pro**

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.

## 5.12.2 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.

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



Application	Current Version	Latest Available	Status	Actions
webcontrol	8.1.2-1	8.1.2-1	up to date	<a href="#">Change Version</a> <a href="#">Update</a> <a href="#">Uninstall</a>
Watchdog	8.1.2-1	8.1.2-1	up to date	<a href="#">Change Version</a> <a href="#">Update</a> <a href="#">Uninstall</a>
Voicemail	8.1-5.0	8.1-8.0	out of date	<a href="#">Change Version</a> <a href="#">Update</a> <a href="#">Uninstall</a>
vmpro-wavs-zhh	8.1-5.0	8.1-5.0	up to date	<a href="#">Change Version</a> <a href="#">Update</a> <a href="#">Uninstall</a>
vmpro-wavs-TTY	-	8.1-5.0	not installed	<a href="#">Change Version</a> <a href="#">Update</a> <a href="#">Install</a>
vmpro-wavs-sv	8.1-5.0	8.1-5.0	up to date	<a href="#">Change Version</a> <a href="#">Update</a> <a href="#">Uninstall</a>

[Update All](#) [Check Now](#)

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**.

## 5.13 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.

1. [Login](#) <sup>51</sup> to the server's web configuration pages.
2. Select the **Updates** page.


Application	Current Version	Latest Available	Status	Actions
webcontrol	8.1.2-1	8.1.2-1	up to date	Change Version Update Uninstall
Watchdog	8.1.2-1	8.1.2-1	up to date	Change Version Update Uninstall
Voicemail	8.1-5.0	8.1-8.0	out of date	Change Version Update Uninstall
vmpro-wavs-zhh	8.1-5.0	8.1-5.0	up to date	Change Version Update Uninstall
vmpro-wavs-TTY	-	8.1-5.0	not installed	Change Version Update Install
vmpro-wavs-sv	8.1-5.0	8.1-5.0	up to date	Change Version Update Uninstall

Update All Check Now

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](#) <sup>64</sup>, 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.

## 5.14 File Repositories

The [Updates](#) <sup>[73]</sup> and [Web Client](#) <sup>[85]</sup> 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.

### 5.14.1 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.

- **Warning**

Before upgrading or changing the version of any installed application or operating system components, you must ensure that you have read the appropriate Avaya Technical Bulletins for the software release. The Technical Bulletins detail supported versions of software and known issues or additional actions required for upgrading.

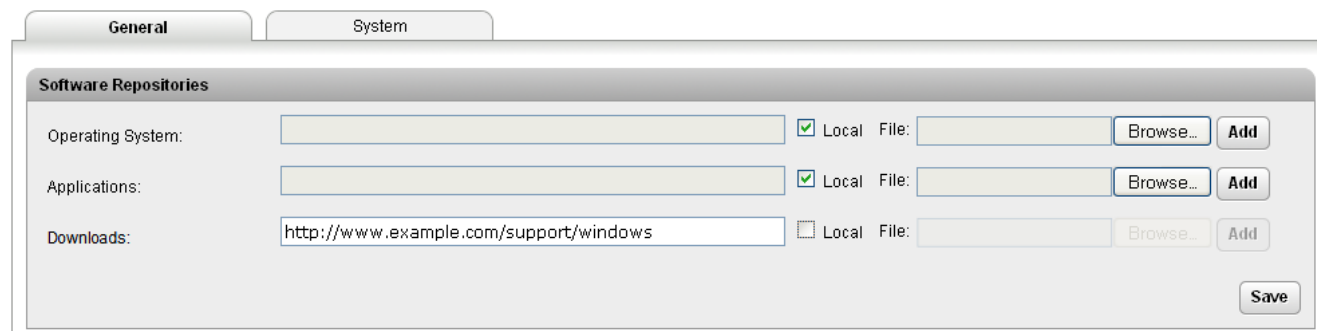
		File Type	DVD/.iso Folder
Application Files	Voicemail Pro	.rpm	\AVAYA\VMPro
	one-X Portal for IP Office	.rpm	\AVAYA\ONEX
Windows Client Files		.exe	\AVAYA\THICK_CL
Operation System Files		.rpm	\CENTOS

- **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.

### 5.14.2 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.



The files uploaded or present in the file repositories are used by the [Updates](#) <sup>[73]</sup> and [Apps Center](#) <sup>[85]</sup> menus.

- **Repository**

If the **Local** option is not selected, this field is used to set the URL of a [remote HTTP file repository](#) <sup>[66]</sup>. 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.



### 5.14.3 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.

#### 5.14.3.1 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](#) <sup>[66]</sup>.

1. [Login](#) <sup>[51]</sup> 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](#) <sup>[64]</sup> 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.

#### 5.14.3.2 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](#) <sup>[66]</sup>.

1. [Login](#) <sup>[51]</sup> 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](#) <sup>[64]</sup> 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.

#### 5.14.3.3 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](#) <sup>[66]</sup>.

1. [Login](#) <sup>[51]</sup> 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](#) <sup>[64]</sup> 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.

---

## 5.14.4 Creating Remote Software Repositories

Alternatively to using [local files uploaded to the server](#)<sup>[61]</sup> 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.

### Creating 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](#)<sup>[64]</sup> 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.

### Creating an 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.

### Creating 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 6.**

## **Server Menus**

---

## 6. Server Menus

The Unified Communications Module web configuration pages are as follows:

- [Home](#) <sup>69</sup>  
This menu gives an overview of the current status of the applications hosted on the server.
- [Logs](#) <sup>71</sup>  
This menu has sub-menus for viewing and managing log records and log files.
  - [View](#) <sup>71</sup>  
View the current log files for the server and the application services hosted by the server.
  - [Download](#) <sup>72</sup>  
Create and download archive files of existing log records.
- [Updates](#) <sup>73</sup>  
Display the versions of applications and components installed and the alternate versions available.
- [Settings](#) <sup>76</sup>  
This menu has sub-menus for various areas of server configuration and operation.
  - [General](#) <sup>77</sup>  
General server settings such as the locations of software update repositories.
  - [System](#) <sup>80</sup>  
View and manage the server setting for date, time and IP address details.
- [Apps Center](#) <sup>85</sup>  
This page can be used to download the installation packages for Windows applications such as the Voicemail Pro client application.

## 6.1 Home

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

**Services**

Name	Status	Up Time	Auto Start	Mem/CPU usage	Action
Voicemail	✓ running	45:26	<input checked="" type="checkbox"/>	<a href="#">10260 KB / 26.8 %</a>	Stop
one-X Portal	✗ stopped	-	<input type="checkbox"/>	<a href="#">0 KB / 0 %</a>	Start

Start All
Stop All

**Notifications**

Server

There are no notifications available

**System**

Info

OS: CentOS release 5.7 (Final)  
Kernel Version: 2.6.18-274.el5  
UpTime: 7 days 5 hours 20 minutes  
Server Time: 12:29  
Average CPU Load: 0.03 (1min), 0.01 (5min), 0.00 (15min)  
Last Successful Logon: 2012-02-07 12:28:08  
Unsuccessful Logon Attempts: 3

Shutdown  
Reboot

Usage

0.14 0.14 0.13

Memory Usage

used (80.28MB)  
free (2953.08MB)

Disk Usage

used (4263.32MB)  
free (64410.21MB)

- 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.

- 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](#) <sup>71</sup> 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 CentOS 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.

- 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.

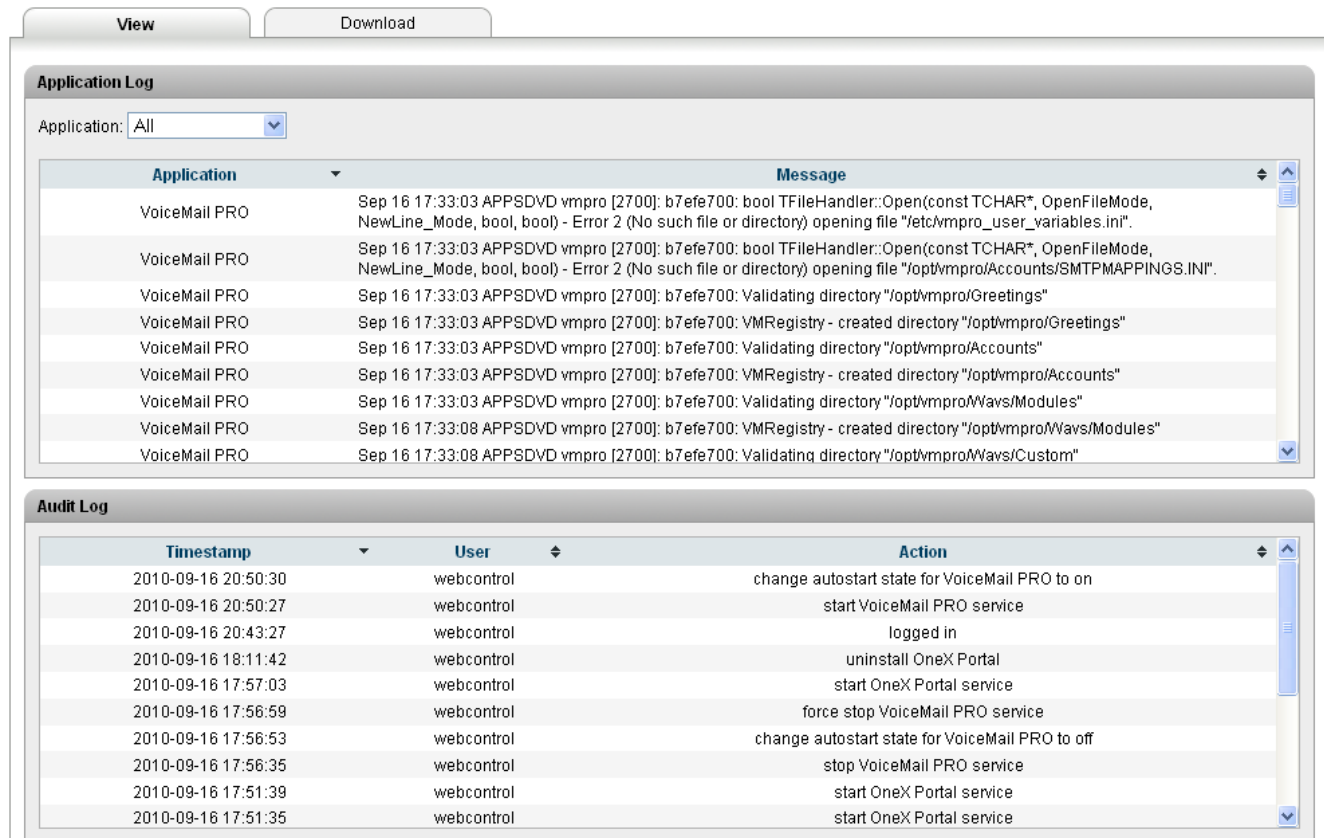
## 6.2 Logs

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

- [View](#)  View the current log files for the server and the application services hosted by the server.
- [Download](#)  Create and download archive files of existing log records.

### 6.2.1 View

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



**Application Log**



Application: All

Application	Message
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: bool TFileHandler::Open(const TCHAR*, OpenFileMode, NewLine_Mode, bool, bool) - Error 2 (No such file or directory) opening file "etc/vmpro_user_variables.ini".
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: bool TFileHandler::Open(const TCHAR*, OpenFileMode, NewLine_Mode, bool, bool) - Error 2 (No such file or directory) opening file "opt/vmpro/Accounts/SMTPMAPPINGS.INI".
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: Validating directory "opt/vmpro/Greetings"
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: VMRegistry - created directory "opt/vmpro/Greetings"
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: Validating directory "opt/vmpro/Accounts"
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: VMRegistry - created directory "opt/vmpro/Accounts"
VoiceMail PRO	Sep 16 17:33:03 APPSDVD vmpro [2700]: b7efe700: Validating directory "opt/vmpro/Wavs/Modules"
VoiceMail PRO	Sep 16 17:33:08 APPSDVD vmpro [2700]: b7efe700: VMRegistry - created directory "opt/vmpro/Wavs/Modules"
VoiceMail PRO	Sep 16 17:33:08 APPSDVD vmpro [2700]: b7efe700: Validating directory "opt/vmpro/Wavs/Custom"

**Audit Log**

Timestamp	User	Action
2010-09-16 20:50:30	webcontrol	change autostart state for VoiceMail PRO to on
2010-09-16 20:50:27	webcontrol	start VoiceMail PRO service
2010-09-16 20:43:27	webcontrol	logged in
2010-09-16 18:11:42	webcontrol	uninstall OneX Portal
2010-09-16 17:57:03	webcontrol	start OneX Portal service
2010-09-16 17:56:59	webcontrol	force stop VoiceMail PRO service
2010-09-16 17:56:53	webcontrol	change autostart state for VoiceMail PRO to off
2010-09-16 17:56:35	webcontrol	stop VoiceMail PRO service
2010-09-16 17:51:39	webcontrol	start OneX Portal service
2010-09-16 17:51:35	webcontrol	start OneX Portal service

- **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.

## 6.2.2 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.

View

Download

Debug Files

Name	Last Modified	Size	Delete
<a href="#">arc_core.vmprow.15906.tar.gz</a>	2010-09-29 10:41:35	1.0M	<input type="checkbox"/>

Select All

Create Archive

Delete Selected

Logs

Name	Last Modified	Size	Delete
<a href="#">system_logs_2010-09-30-15-59.tar.gz</a>	2010-09-30 15:59:47	11.6K	<input type="checkbox"/>
<a href="#">install_logs_2010-09-30-15-59.tar.gz</a>	2010-09-30 15:59:47	6.2K	<input type="checkbox"/>
<a href="#">webcontrol_logs_2010-09-30-15-59.tar.gz</a>	2010-09-30 15:59:47	3.5K	<input type="checkbox"/>
<a href="#">vmpro_logs_2010-09-30-15-59.tar.gz</a>	2010-09-30 15:59:47	8.1K	<input type="checkbox"/>

Select All

Create Archive

Delete Selected

### 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**.



## 6.3 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](#) <sup>77</sup> page.

- **Warning**

Before upgrading or changing the version of any installed application or operating system components, you must ensure that you have read the appropriate Avaya Technical Bulletins for the software release. The Technical Bulletins detail supported versions of software and known issues or additional actions required for upgrading.

The screenshot shows the 'Updates' menu divided into two sections: 'Services' and 'System'.

**Services Section:**

Application	Current Version	Latest Available	Status	Actions
webcontrol	8.1.2-1	8.1.2-1	up to date	Change Version   Update   Uninstall
Watchdog	8.1.2-1	8.1.2-1	up to date	Change Version   Update   Uninstall
Voicemail	8.1-5.0	8.1-5.0	out of date	Change Version   Update   Uninstall
vmpro-wavs-zhh	8.1-5.0	8.1-5.0	up to date	Change Version   Update   Uninstall
vmpro-wavs-TTY	-	8.1-5.0	not installed	Change Version   Update   Install
vmpro-wavs-sv	8.1-5.0	8.1-5.0	up to date	Change Version   Update   Uninstall

Buttons at the bottom of the Services section: Update All, Check Now

**System Section:**

OS	CentOS
Version	release 5.5 (Final)
Kernel Version	2.6.18-194.el5
Last Update	-
Status	updates available

Buttons at the bottom of the System section: Check Now, Review Updates, Update All

The menu is divided into 2 sections:

- **Services** <sup>74</sup>  
This section displays the current version of application files and whether update files are available.
- **System** <sup>75</sup>  
This section displays the current version of the operating system and whether update files are available.

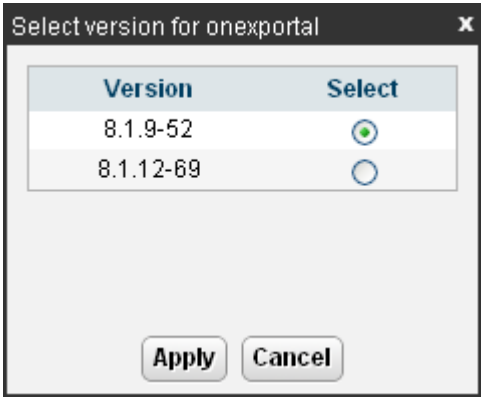
### 6.3.1 Services

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					
Application	Current Version	Latest Available	Status	Actions	
webcontrol	8.1.2-1	8.1.2-1	up to date	Change Version	Update Uninstall
Watchdog	8.1.2-1	8.1.2-1	up to date	Change Version	Update Uninstall
Voicemail	8.1-5.0	8.1-8.0	out of date	Change Version	Update Uninstall
vmpro-wavs-zhh	8.1-5.0	8.1-5.0	up to date	Change Version	Update Uninstall
vmpro-wavs-TTY	-	8.1-5.0	not installed	Change Version	Update Install
vmpro-wavs-sv	8.1-5.0	8.1-5.0	up to date	Change Version	Update Uninstall

Update All Check Now

- 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](#)<sup>[64]</sup>. 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](#)<sup>[64]</sup>. The current version is selected. Selecting another version and then 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](#)<sup>[64]</sup>.
- **Uninstall**  
Clicking on this button will uninstall the selected application.
  - If there are installation files for the application available in the application [file repository](#)<sup>[64]</sup>, 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.
- **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.

### 6.3.2 System

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

System	
OS	CentOS
Version	release 5.7 (Final)
Kernel Version	2.6.18-194.el5PAE
Last Update	-
Status	updates available

- **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.

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.

---

## 6.4 Settings

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

- [General](#)  77  
General server settings such as the locations of software update repositories.
- [System](#)  80  
View and manage the server setting for date, time and IP address details.

## 6.4.1 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.

General

System

Software Repositories

Operating System:  ☒ Local File:

Applications:  ☒ Local File:

Downloads:  ☒ Local File:

Watchdog

Log files age (days):

Debug

Voicemail debug level:

Web Control

Application Port:

Protocol:

Inactivity timeout:

Backup and Restore

Service	Action
Voicemail	<input type="button" value="Backup"/> <input type="button" value="Restore"/>

## 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.

The screenshot shows the 'Software Repositories' configuration window. It has two tabs: 'General' and 'System'. The 'General' tab is selected. Inside the window, there are three rows of configuration fields:

- Operating System:** A text field, a checked 'Local' checkbox, a 'File:' label, a text field, a 'Browse...' button, and an 'Add' button.
- Applications:** A text field, a checked 'Local' checkbox, a 'File:' label, a text field, a 'Browse...' button, and an 'Add' button.
- Downloads:** A text field containing 'http://www.example.com/support/windows', an unchecked 'Local' checkbox, a 'File:' label, a text field, a 'Browse...' button, and an 'Add' button.

A 'Save' button is located at the bottom right of the window.

The files uploaded or present in the file repositories are used by the [Updates](#) <sup>[73]</sup> and [Apps Center](#) <sup>[85]</sup> menus.

- **Repository**

If the **Local** option is not selected, this field is used to set the URL of a [remote HTTP file repository](#) <sup>[66]</sup>. 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.

## Watchdog

- **Log files age (days)**

Sets the number of days that log file records are retained. This does not affect log file [archives](#) <sup>[72]</sup>. Not applied to one-X Portal for IP Office which performs its own log file size limitation.

## 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 set it to a value already used by another service or application.

- **Protocol**

Select the protocol used for connection. The default is **http**. 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**.

## Voicemail Settings

This section can be used to set the debug logging level used by certain applications. For the one-X Portal for IP Office the logging level is set through the applications own web administration menus. Log files are retrievable through the [Logs | Download](#) <sup>[72]</sup> menu.

- **Debug Level**

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

## Backup and Restore

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

- **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.



## 6.4.2 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.

General

System

Network

Network Interface:

Host Name:

☐ Use DHCP

IP Address:

Subnet Mask:

Default Gateway:

System DNS:

☐ Automatically obtain DNS from provider

Save

Password Rules Settings

Minimum password length:

Minimum number of uppercase characters:

Minimum number of lowercase characters:

Minimum number of numeric characters:

Minimum number of special characters:

☒ Allow character sequences

Maximum allowed sequence length:

Save

Date and Time

Date:

Time:  :

Timezone:

☒ Enable Network Time Protocol

NTP Servers:

☐ Synchronize system clock before starting service

☒ Use local time source

Save

Change Root Password

New Password:

Confirm New Password:

Password complexity requirements:

- Minimum password length: 8

Save



## Network

- **Network Interface**

This drop down allows selection of network interfaces is currently being configured by the web form. This field is fixed to **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**

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

- **IP Address**

Displays the IP address set for the server. If DHCP is not being used, the field can be edited to change the setting. The Unified Communications Module is physically connected to the LAN1 network of the system and needs to have an address on that subnet. See [IP Address Notes](#) <sup>18</sup>.

- **Subnet Mask**

Displays the subnet mask applied to the IP address. If DHCP is not being used, the field can be edited to change the setting.

- **Default Gateway**

Displays the default gateway settings for routing. If DHCP is not being used, the field can be edited to change the setting.

- **System DNS**

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

- **Automatically obtain DNS from provider**


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

-

---

## 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 [Home](#)  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.

## 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.

## Change Root Password

- **New Password**

Enter the new password for the server's root account.


- **Confirm New Password**

Confirm the new password.

---

## 6.5 Apps Center

This menu is accessed by selecting **Apps Center**. 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](#)  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.

---


# **Chapter 7.**

## **Module Maintenance**

---

## 7. Module Maintenance

The following sections cover various Unified Communications Module maintenance processes:

- [Module LEDs](#)  89
- [Module Buttons](#)  89
- [Module Removal](#)  90
- [Attaching a Monitor and Keyboard](#)  91
- [Loading Windows Voicemail Server Settings](#)  92
- [Module Battery](#)  94
- [Module Software Reinstall](#)  97



## 7.1 Module LEDs

The Unified Communications Module provides the following LEDs:

- **Upper 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 blink:** OK. IP Office heartbeat okay.
  - **Off with Amber blink:** Module shutdown. IP Office heartbeat okay.
  - If the module is already running when the system restarts, its 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, its lower LED remains off when the LEDs on the other base cards are solid red. The lower LED on the module then flashes red when the LEDs on the other base cards flash red during system initialization; before reverting to either green or off when the system reboot is complete.

## 7.2 Module Buttons

The Unified Communications Module provides the following buttons:

- **Upper Button/Button 1**

This button can be used for the following functions:

  - **Shutdown**

If the module is running, pressing this button for more than 2 seconds will start a module shutdown. A completed shutdown is indicated by the lower LED changing to off with regular amber blinks only.
  - **Startup**

If the module has been shutdown, pressing this button will cause 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. See [Module Software Reinstallation](#) <sup>97</sup>.
- **Switch 2:** Not used.

---

## 7.3 Module Removal

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 loss of configuration data.

### • ! WARNINGS

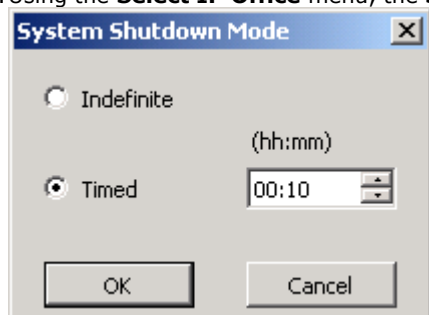
- A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause the loss of configuration data.
- This is not a polite shutdown, any user calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.
- 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.
- When shutdown, the LEDs shown on the system are as follows. Do not remove power from the system or remove any of the memory cards until the system is in this state:
  - LED1 on each IP500 base card installed will also flash red rapidly plus LED 9 if a trunk daughter card is fitted to the base card.
  - The CPU LED on the rear of the system will flash red rapidly.
  - The System SD and Optional SD memory card LEDs on the rear of the system are extinguished.
- 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.

### System Shutdown 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.

### System Shutdown Using IP Office Manager

1. Using IP Office Manager, select **File | Advanced | System Shutdown**.
2. Using the **Select IP Office** menu, the **System Shutdown Mode** menu is displayed.



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.

### System Shutdown Using the System Status Application

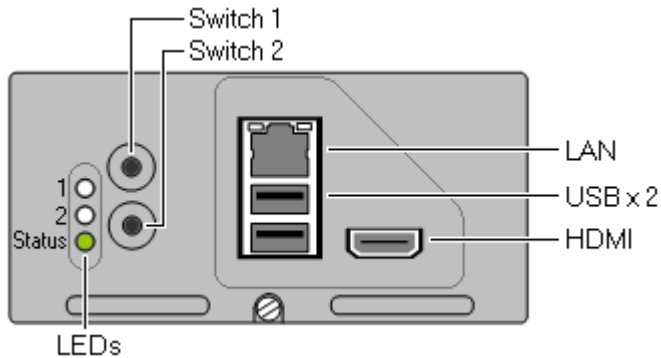
1. Start System Status Application and access the system's status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Shutdown System**.
4. Select **Indefinite** and click **OK**.
5. Wait until the state of the LEDs on the system match those listed above before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

## 7.4 Attaching a Monitor and Keyboard

The Unified Communications Module and its applications are designed for remote maintenance only, via web browser and or client applications running on a PC networked to the IP Office system. However, during some processes may require direct attachment of a monitor and keyboard. When that is necessary, the USB and HDMI ports can be used.

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

The card is supplied with a removable plastic cover that locates over the external ports (LAN, USB and HDMI) on the faceplate of the card. This cover should always be in place during normal operation of the card. The cover should only be temporarily removed during maintenance actions that require access to the ports and should be replaced when the maintenance is completed.



### Attaching a Keyboard

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

### Attaching a Monitor

For maintenance and diagnostics purposes, a HDMI monitor can be attached to the HDMI port on the front of the module. Alternatively, a HDMI to DVI cable can be used.

---

## 7.5 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 device. Otherwise, if the backup is too large for the USB2 memory device, SSH file transfer can be used.

### Backing Up the Old Voicemail Server

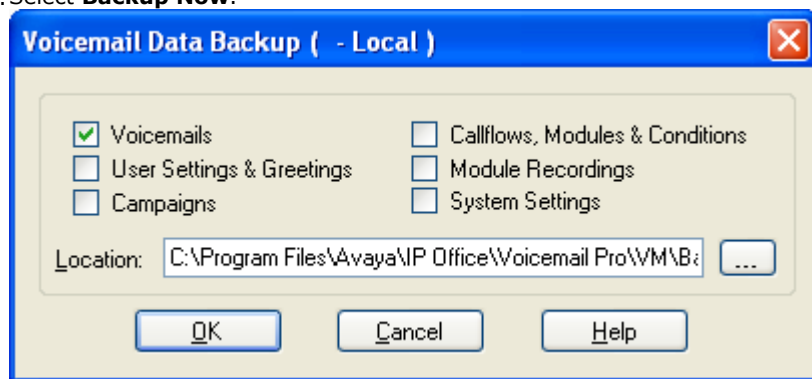
A full immediate backup of all the voicemail server settings, prompts and messages can be obtained using the Voicemail Pro client.

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.

### Shutting 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.

### Transferring the Backup to a USB2 Memory Device

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 device.

- 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 device capacity, Copy the backup folder and all its content onto a USB2 memory device. 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](#)<sup>[106]</sup>, 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 device.
  - 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 device capacity, Copy the backup folder and all its content onto a USB2 memory device. Do not put the folder into another folder or change the folder name.

### Loading the Backup onto the New Server from a USB2 Memory Device

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

1. Insert the USB2 memory device 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 device.
6. Select the backup on the USB2 memory device and click **OK**.
7. Do not remove the USB2 memory device until all USB2 memory device activity has ceased.
8. Once the restore has been completed, on the **Home** menu, **Stop** and then **Start** the voicemail service.

### 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 device, use the following method to transfer and then restore the backup.

1. Connect to the Unified Communications Module using an [SSH File transfer tool](#)<sup>[106]</sup>.
2. Copy the backup folder into the folder **`/opt/vmpro/Backup/Scheduled/OtherBackups`**.
3. Using a web browser, [login](#)<sup>[51]</sup> 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 **Home** menu, **Stop** and then **Start** the voicemail service.

---

## 7.6 Module Battery

The Unified Communications Module includes a Lithium coin cell battery. If the module is no longer required, care must be taken to ensure that the battery is removed and disposed of correctly. The battery can be removed from its holder by bending the tab out the way and then pulling the battery upwards.

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

When removing an Unified Communications Module from a system, care should be taken 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.



## 7.7 Upgrading Software

Upgrades for the Unified Communications Module will be made available as a set of **.rpm** files for the components being upgraded. Sets of **.rpms**, typically those for the applications, may be combined into a single **.zip** file that can be used for the upgrade, reducing the number of upgrade process steps. The upgrade files will be made available via the Avaya support website <http://support.avaya.com>.

- A single .zip file may be made available for upgrading the applications. Use of the zip file simplifies the number of repeated steps required for the upgrade process. Separate .rpm files may also be made available for voicemail language prompts and voicemail TTS languages. Refer to the IP Office Technical Bulletins for each release to confirm the new .zip and .rpms available and whether any other pre-requisite .rpm files are also needed. If an .iso files is available, individual .rpm files can be extracted from the .iso file is needed without having to install the .iso.
- Note that .rpm files are also used by other Linux based IP Office solutions. In all cases you must confirm that the .rpm file is specifically listed as compatible for use with the Unified Communications Module.

Using .zip or .rpm files is the recommended method for upgrading rather performing a [full .iso reinstallation](#)<sup>[97]</sup> as it is both quicker and does not remove the current user data. However, a full data backup is still recommended. It also has the advantage that it is done remotely from a PC logged in for web control rather than requiring physical access to the system to boot it from the new .iso image.

### • ! WARNINGS

#### • **Backup Application Data**

Before attempting the following process, all user data for the services provided by the Unified Communications Module should be backed-up to a safe location other than the Unified Communications Module.

#### • **Voicemail Pro**

The Voicemail Pro client can be used to perform a manual backup of the voicemail data including, if selected, user messages and prompts. The default location for the backup is on the Unified Communications Module. Therefore, following the backup, SSH file transfer should be used to copy the backup files to another PC.

#### • **one-X Portal for IP Office**

The AFA menus supported by one-X Portal for IP Office can be used to perform a backup to another PC or to an FTP server.

#### • **Unified Communications Module**

Following the reinstall, the IP address settings of the module must be set again. Login to the modules web control menus and not the settings on the various menus.

#### • **Loss of Services**

During this process, the services provided by the Unified Communications Module are not available to users. Therefore users should be warned in advance or this process should be performed outside normal business hours.

#### • **Read the Technical Bulletins**

Ensure that you have read and understood all Avaya Technical Bulletins relevant to the software release. These will include notes and information that was not available at the time this document was created.

---

## Upgrading Software

1. Take a backup of the one-X Portal for IP Office and Voicemail Pro applications. The backup is done using the normal backup procedure for those applications.
2. Login to the web control menus.
3. Select the **Settings | General** menu.
  - a. In the **Web Control** section change the **Inactivity timeout** to **1 hour**. This ensures that the web control session does not timeout while downloading the updated applications files.
  - b. Click **Save**. It will be necessary to login to the web control menus again.
4. 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. When the file is uploaded, select the **Updates | Services** menu. Click on **Update All**.
  - d. Click **OK** when warned about services stopping.
  - e. After update is complete, the web control application will be restarted and the web session will end. A warning about restarting the session or an error timeout message may appear.
5. Login to the web control menus.
6. Select the **Updates | Services** menu.
  - a. Verify that all the application have been updated in the **Updates** window. If not, then individually update the application by clicking the **Update** button.
  - b. From the updates window, check that the **AvayaVersioning** application is installed. If not, click the Install button next to the application.
7. If voicemail is configured or likely to be configured to use a language other than English UK or English US, then a manual update of the prompt files for the language is required.
  - a. Select the **Setting | General** menu.
  - b. For the **Applications** options, select **Local**.
  - c. Select the .rpm file for the language. The .iso image can also be used, the prompt files being at the following location on the iso image **/avaya/vmpro**.
  - d. When the language file is uploaded, select the **Updates | Services** menu. Select the language in the list of services and click **Update**.
8. If for Voicemail Pro, text to speech (TTS) is being used, the TTSEnglish rpm also needs to be upgraded the same way. This is done in the same way as for the language prompt files in the section above.
9. Once all the new .rpm files have been installed, select **Home**. Check that the required services are running. Restart the services if necessary.
10. Verify that all the data from Voicemail Pro and one-X Portal for IP Office has migrated properly. Otherwise, restore the data from the backups taken at the start of the process.



## 7.8 Module Software Reinstallation

A full reinstall of the module software can be done using a .iso image file copied onto on a specially prepared USB2 memory device. The Unified Communications Module can be made to boot from the USB2 memory device at which point it will load and run the .iso file.

When necessary, Avaya will make such images available along with appropriate installation notes for setting up the USB2 memory device. This method of upgrading should only be used when absolutely necessary. Upgrading by [uploading and installing new .rpm files](#)<sup>[95]</sup> should always be used where possible.

This process takes at least 45 minutes.

- **! Warnings**

- **Backup Application Data**

- Before attempting the following process, all user data for the services provided by the module should be backed-up to a safe location other than the Unified Communications Module.

- **Voicemail Pro**

- The Voicemail Pro client can be used to perform a manual backup of the voicemail data including, if selected, user messages and prompts. The default location for the backup is on the Unified Communications Module. Therefore, following the backup, [SSH file transfer](#)<sup>[106]</sup> should be used to copy the backup files to another PC.

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

- The AFA menus supported by one-X Portal for IP Office can be used to perform a backup to another PC or to an FTP server.

- **Unified Communications Module**

- Following the reinstall the IP address settings of the module must be set again. Login to the modules web control menus and not the settings on the various menus.

- **Loss of Services**

- During this process, the services provided by the Unified Communications Module are not available to users. Therefore users should be warned in advance or this process should be performed outside normal business hours.

- **Read the Technical Bulletins**

- Ensure that you have read and understood all Avaya Technical Bulletins relevant to the software release. These will include notes and information that was not available at the time this document was created.

- **Monitoring the Process**

- A suitable monitor for use with an HDMI to HDMI cable or HDMI to DVI cable is recommended. This will allow you to monitor the process and to confirm when the process has been completed.

---

## Preparing a USB2 Memory Device using Windows

The USB Initiator application can be used to install the necessary files and folders onto a USB2 memory device. The new .iso file for the Unified Communications Module can then be placed onto the USB2 memory device.

### 1. Install the USB Initiator application:

- a. From the Avaya support web site (<http://support.avaya.com>) download the USB Initiator application. The download will be located in the set of IP Office application downloads.
- b. Unzip the download to a temporary directory.
- c. Double-click on **setup.exe** file to install the application.

### 2. Prepare the USB2 memory device:

- a. Insert the USB2 memory device into a USB port on the PC.
- b. Select **Start | All Programs | IP Office | UC Module USB Initiator**.
- c. Select the USB2 memory device from the list of detected devices.
- d. For **Mode** select **Install**. The **Rescue** option is used for a separate [password reset process](#)<sup>[10]</sup>.
- The **Mode** option is only available with the UC USB Initiator version 2.0.3 or higher. If not present, download and install a new version of the USB initiator software.
- e. Click **Create USB Installer**. The USB initiator will load various files and folders onto the USB memory device.
- If the USB2 memory device is already correctly formatted for use with the Unified Communications Module, clicking **Create USB Installer** only loads any files that are missing from the USB2 memory device. To force a complete reload of all files regardless of whether the files are already installed, select **Recreate image** before clicking **Create USB Installer**.

### 3. Load the image file:

- a. From the Avaya support web site (<http://support.avaya.com>) download the new .iso image file for the Unified Communications Module.
- b. View the files on the USB2 memory device using file manager or similar. Open the **C110iso** folder.
- c. Copy the .iso file into the **C110iso** folder. Note that there should only be one .iso file in the folder.

### 4. The USB2 memory device can now be used as the source from which the Unified Communications Module boots.

## Preparing a USB2 Memory Device using Linux

The USB Initiator application includes the files necessary to also manually prepare a USB2 memory device on a Linux PC. Within the zip file for the application download, copy the contents of the /Manual folder. This contains the files ks.cfg and syslinux.cfg.

The following assumes that the USB2 memory device mounts as /dev/sdb with the partition /dev/sdb1. Those values may vary depending on the PC configuration.

1. Make sure that the pen is not mounted by entering `#umount /dev/sdb1`

2. Enter the following to make the partition bootable:

```
#fdisk /dev/sdb
a # toggle bootable flag
1 # partition number
w # write to disk
```

3. Enter the following to install syslinux:

```
#syslinux -s /dev/sdb1
#dd if=/usr/share/syslinux/mbr.bin of=/dev/sdb
```

4. Mount the USB2 memory device by entering the following:

```
#mkdir /tmp/cdimage
#mkdir /tmp/stick
#mount -ro loop apc-8.iso /tmp/cdimage
#mount /dev/sdb1 /tmp/stick
```

5. Copy the new .iso image and other related files to the USB2 memory device by entering the following:

```
#cd /tmp/stick
#mkdir ApcIso
#cd -
#cp apc-8.iso /tmp/stick/ApcIso
#cd -
#cp -rv /tmp/cdimage/isolinux syslinux
#cp -rv /tmp/cdimage/images ApcIso/
#rm -f syslinux/isolinux.bin
#rm -f syslinux/isolinux.cfg
#cp [provided syslinux.cfg] syslinux/
#cp [provided ks.cfg] .
#cd
#umount /tmp/cdimage
#umount /tmp/stick
```

6. Wait until all file operations have completed. This may take several minutes.

## Backing Up the Existing Application Data

If the module is already being used for customer operations, you need to backup the Voicemail Pro and one-X Portal for IP Office settings. Do this using the processes outlined in [Transferring Voicemail Server Settings](#)<sup>[92]</sup> and Transferring one-X Portal for IP Office Settings.

---

## Bootimg and Loading a New Image from a USB2 memory device

1. Using either of the processes above prepare a USB2 memory device with the required .iso file.
2. Remove the plastic cover from the front of the faceplate of the card. The cover must be retained and must be reattached after this process is completed.
3. Connecting a suitable monitor for use with an HDMI to HDMI cable or HDMI to DVI cable is recommended. This will allow you to monitor the process and to confirm when the process has been completed.
4. 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.
5. Insert the USB2 memory device with the new images file into one of the USB ports located on the front of the module.
6. 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) amber flashes of the lower LED.
7. Restart the module by pressing the upper reset button again and keeping it pressed until the top two LEDs change from orange to off.
8. The module will reboot using the image files on the USB2 memory device.
9. After a short period the top two LEDs will change to alternately flashing green as the upgrade process takes place. The lower LED will be steady green. This process takes approximately 45 minutes.
10. When the two top LED stop alternately flashing green, wait a few additional minutes for any USB2 memory device activity to cease. If you have a monitor connected to the module, completion of the upgrade is shown by the **Login>** prompt appearing on the monitor.
11. Remove the USB2 memory device and monitor connection. Refit the plastic cover that was removed at the start of the process.
12. You now need to repeat the processes for [module initialization](#) <sup>[22]</sup> as if this was a new module.

## Restoring the Application Data

Any previously backed up settings and data for the Voicemail Pro and one-X Portal for IP Office applications can now be restored. Do this using the processes outlined in [Transferring Voicemail Server Settings](#) <sup>[92]</sup> and Transferring one-X Portal for IP Office Settings.

## 7.9 Module Password Reset

If necessary, it is possible to reset the root and web control passwords of the Unified Communications Module. To do this requires physical access to the card in order to restart the Unified Communications Module with a specially prepared USB memory device. This process does not [reinstall the software](#) <sup>[97]</sup> on the Unified Communications Module.

### Preparing a USB Password Reset Key

#### 1. Install the USB Initiator application:

- a. From the Avaya support web site (<http://support.avaya.com>) download the USB Initiator application. The download will be located in the set of IP Office application downloads.
- b. Unzip the download to a temporary directory.
- c. Double-click on **setup.exe** file to install the application.

#### 2. Prepare the USB2 memory device:

- a. Insert the USB2 memory device into a USB port on the PC.
- b. Select **Start | All Programs | IP Office | UC Module USB Initiator**.
- c. Select the USB2 memory device from the list of detected devices.
- d. For **Mode** select **Rescue**. The **Install** option is used for a separate [software reinstallation process](#) <sup>[97]</sup>.
  - The **Mode** option is only available with the UC USB Initiator version 2.0.3 or higher. If not present, download and install a new version of the USB initiator software.
- e. Click **Create USB Installer**. The USB initiator will load various files and folders onto the USB memory device.
  - If the USB2 memory device is already correctly formatted for use with the Unified Communications Module, clicking **Create USB Installer** only loads any files that are missing from the USB2 memory device. To force a complete reload of all files regardless of whether the files are already installed, select **Recreate image** before clicking **Create USB Installer**.

### Bootting from a USB2 memory device

1. Using the process above prepare a USB2 memory device set for the **Rescue** mode.
2. Remove the plastic cover from the front of the faceplate of the card. The cover must be retained and must be reattached after this process is completed.
3. Insert the USB2 memory device into one of the USB ports located on the front of the module.
4. 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) amber flashes of the lower LED.
5. Restart the module by pressing the upper reset button again and keeping it pressed until the top two LEDs change from orange to off.
6. The module will reboot.
7. When the two top LED stop alternately flashing green, wait a few additional minutes for any USB2 memory device activity to cease.
8. Remove the USB2 memory device. Refit the plastic cover that was removed at the start of the process.



# **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.

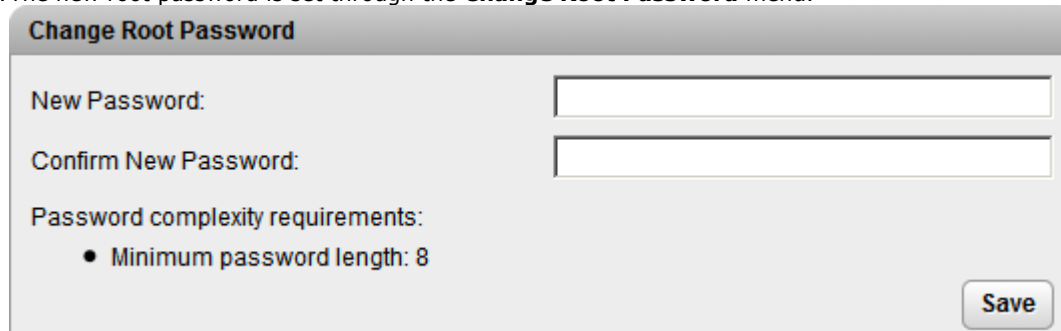
- [Changing the Root Password](#) <sup>105</sup>
- [SSH File Transfers](#) <sup>106</sup>
- [Command Line Controls](#) <sup>107</sup>



## 8.1 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.

1. [Login](#) <sup>[51]</sup> 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.

A screenshot of a web form titled "Change Root Password". The form has a light gray background and a darker gray header. It contains two text input fields: "New Password:" and "Confirm New Password:". Below these fields, there is a section for "Password complexity requirements:" which lists a single bullet point: "• Minimum password length: 8". In the bottom right corner of the form, there is a "Save" button.

- **New Password**  
Enter the new password for the server's root account.
  - **Confirm New Password**  
Confirm the new password.
4. Note the rules displayed for the password entry, enter the new password. The password complexity requirements are set in the [Password Rules Settings](#) <sup>[54]</sup> menu. The rules set there are applied to changing both the [root password](#) <sup>[53]</sup> and changing the web control [administrator password](#) <sup>[52]</sup>.
  5. Click **Save**. The menu will confirm if the new password was accepted.

---

## 8.2 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.

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 **webcontrol**.
    - 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](#) <sup>52</sup>, the default is **web**.
2. The default folder displayed after logging in is **/home/webcontrol**.

## 8.3 Command Line

There are a range of Unified Communications Module commands that can be performed from the server's command line when logged in as the webcontrol user. The commands are grouped into three tiered sets, each set protected by a separate password.

- **General Commands** <sup>[108]</sup>

These commands are used mainly to display information about the server and the services it is running. Access to these commands is controlled by the webcontrol user password.

- **Administrator Commands** <sup>[110]</sup>

These commands allow you to stop, start, restart and update the services. Access to these commands is controlled by the webcontrol user password and an additional administrator password.

- **Configuration Commands** <sup>[111]</sup>

These commands allow you to change server settings. Access to these commands is controlled by the webcontrol user password, the administrator password and an additional configurator password.

1. Log in to the server's webcontrol user account:

- **If logging in at the on the server:**

- At the **Command:** prompt, enter **login**.
- At the **login:** prompt enter **webcontrol**.
- At the **Password:** prompt, enter the password (the default is **web**).

- **If logging in remotely:**

- 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 **webcontrol**.
  - 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.
- If this is the first time the application has connected to the Unified Communications Module, accept the trusted key.
- When prompted, enter the webcontrol user **password** <sup>[52]</sup>, the default is **web**.

2. You should now be at the **>** prompt. From this prompt you can perform various **general commands** <sup>[108]</sup>.

---

### 8.3.1 General Commands

In the commands below, *<application>* is replaced with name of the required application: **voicemail**, **onexportal**, **watchdog** or **all**.

At the > prompt, the following commands can be used:

- **admin**  
Change to the [Admin >](#) <sup>[110]</sup> prompt. The administrator password is required.
- **exit**  
Exit the > prompt. At this level this is the same as logging out.
- **help**  
Display general help on entering commands.
- **history**  
Display the history of commands used in the current session.
- **list**  
Display a list of commands.
- **logout**  
End the session and logout.
- **password**  
Change the webcontrol password.
- **show <application>**  
Show information about the application including its current status, version, boot on start setting and any watchdog alarms for the application.

```
> show voicemail
Voicemail Pro is running.
Boot at startup: on.
Version: 6.0.6.19
Watchdog alarms:
[15:24:19 - 21 Apr 2010] Voicemail Pro crashed, restarting.
```

- **show backup <application>**  
Show information about the backups available for the entered application.

```
> show backup voicemail
<Backups>
/opt/vmpro/Backup/Scheduled/Immediate/VMPro_Backup_07122011075040|Immediate|Immediate|2011-12-07
</Backups>
```

- **show config**  
Show a summary of the applications being supported by the Unified Communications Module.

```
> show config
Services Repository: http://www.avaya.com/support/ipoffice/
OS Repository: http://www.avaya.com/support/centos/
Applications Version Boot at startup
Voicemail Pro: 6.0.20.1, on.
one-X Portal: 6.0.20.1, off.
Watchdog: 6.0.6.19, on.
CLI 6.0.6.1 -
Operating System: CentOS 5.4
Kernel version: 2.6.18-92.1.18.el5
Last updated: 2010-04-27 - 15:30
```

- **show logging <application>**  
Show logging information for the application. This includes both audit trail commands, watchdog alarms and the applications own log output.

```
> show logging voicemail
# Last command:
[15:24:19 - 21 Apr 2010] Voicemail Pro starting...
[15:25:00 - 21 Apr 2010] Voicemail Pro started.
# Watchdog alarms:
[15:24:19 - 21 Apr 2010] Voicemail Pro crashed, restarting.
# Voicemail Pro log file:
...
```

- **show status <application>**  
Show the status (running, starting or stopped) of the application.

```
> show status voicemail
Voicemail Pro is running.
```

- **show time**

Show the current date and time on the server.

```
> show time  
Current date and time: 15:30:00 - 21 Apr 2010
```

- **show updates <application>**

Show the current version of the application and the versions available in the updates repository.

```
> show updates voicemail  
Current Voicemail Pro Version: 6.0.6.19  
Available Versions:  
- Voicemail Pro 6.0.7.1  
- Voicemail Pro 6.0.8.3  
- Voicemail Pro 6.0.9.5
```

- **top**

Return to the `>` prompt.

---

## 8.3.2 Administrator Commands

The **Admin>** prompt is accessed by entering **admin** at the [> general command prompt](#)<sup>[108]</sup> and then entering the administrator password (the default password is **Administrator**).

In the commands below, *<application>* is replaced with name of the required application: **voicemail**, **onexportal**, **watchdog** or **all**.

At the **Admin>** prompt, the following commands can be used:

- **auditlog**  
Display a log of application commands executed.
- **configure**  
Change to the [Configure>](#)<sup>[111]</sup> prompt. The configurator password is required.
- **exit**  
Exit the **Admin>** prompt and return to the [> prompt](#)<sup>[108]</sup>.
- **forcestop** *<application>*  
Stop the specified application. This is a forced shutdown of the application. For a polite shutdown use the **stop** command.
- **help**  
Display general help on entering commands.
- **history**  
Display the history of commands used in the current session.
- **list**  
Display a list of commands.
- **logout**  
End the session and logout.
- **password**  
Change the administrator password required to access the **Admin>** prompt.
- **restart** *<application>*  
Restarts specified application.
- **root**  
Access the root user account. The root user password is required.
- **start** *<application>*  
Start the specified application.
- **stop** *<application>*  
Stop the specified application. This is a controlled shutdown of the application. The command prompt is redisplayed once the application is stopped. To force a shutdown of an application user **forcestop**.
- **update** *<application>* *<version>*  
Begin an update of the specified application to a specified version. The versions available for upgrade can be shown using the **show updates** *<application>* command. In addition to the standard applications, **cli** can also be specified.
- **top**  
Return to the [>](#)<sup>[108]</sup> prompt.

### 8.3.3 Configuration Commands

The **Configure>** prompt is accessed by entering **configure** at the [Admin> prompt](#)<sup>[110]</sup> and then entering the configurator password (the default password is **Configurator**).

In the commands below, *<application>* is replaced with name of the required application: **voicemail**, **onexportal**, **watchdog** or **all**.

At the **Configure>** prompt, the following commands can be used:

- **autostart** *<application>* *<on/off>*  
Change the autostart settings of an application.
- **backup** *<application>*  
Backup the application. This command is currently only supported for the **onexportal** application.
- **exit**  
Exit the **Configure>** prompt and return to the [Admin>](#)<sup>[110]</sup> command prompt.
- **help**  
Display general help on entering commands.
- **history**  
Display the history of commands used in the current session.
- **list**  
Display a list of commands.
- **logout**  
End the session and logout.
- **password**  
Change the configuration password required to access the **Configure>** prompt.
- **install** *<application>*  
Install an application from the repository.
- **repository** *<type>* *<link>*  
Set the location for the updates repository.
  - The *<type>* value indicates the repository:
    - **os**  
Operating system repository.
    - **services**  
Applications repository.
  - The *<link>* value indicates the repository location.
- **restore** *<application>*  
Restore an application. This command is currently only supported for the onexportal application.
- **search**  
Search for an application and display basic information if found on the server.
- **show**  
Display a list of installed applications.
- **startup** *<application>* *<on/off>*  
Set the start on boot up setting for an application.
- **uninstall** *<application>*  
Uninstall an application.
- **top**  
Return to the [>](#)<sup>[108]</sup> prompt.

---



# Index

## A

Address  
     DNS 57, 80  
     IP 57, 80  
 Administrator  
     Login 44  
 Application  
     Install 61  
     Uninstall 63  
     Upgrade 61  
 Application Logs 71  
 Archive 72  
 Audit Log 71  
 Auditlog 110  
 Autostart 111

## B

Backup 77, 111

## C

CentOS 12  
 Change Password  
     Root Password 105  
     Web Browser Password 52  
 Clients 85  
 clish 107  
 Configuration  
     one-X Portal for IP Office 44  
     Voicemail Pro 32  
 CPU  
     Usage 69  
 Create Archive 72

## D

Date 58, 80  
 Default  
     Gateway 57, 80  
     Password 27, 51  
 DHCP 57, 80  
 Disk  
     Usage 69  
 DNS 57, 80  
 Download  
     Logs 72  
     Windows Clients 85

## F

Forcestop 110

## G

Gateway 57, 80  
 General 77

## H

Home 69  
 Host Name 57, 80

## I

Initial configuration 44  
 Install  
     Application 61  
     Service 61  
 IP Address 57, 80  
 IP Office  
     Check 44  
     Select 44

## L

Linux 12

Local 77  
 Log Files Age 77  
 Logging In 51  
 Login 36  
     Administrator 44  
 Logs 71  
     Application 71  
     Archive 72  
     Audit 71  
     Download 72  
     Log Files Age 77

## M

Mask 57, 80  
 Memory  
     Usage 69  
 Menu  
     Download 72  
     General 77  
     Home 69  
     Logs 71  
     Logs Download 72  
     Logs View 71  
     Services 74  
     Settings 76  
     System 75, 80  
     Updates 73  
     Updates Services 74  
     Updates System 75  
     View 71  
     Windows Clients 85

## N

Network Time Protocol 58, 80  
 no Remote 36  
 Notifications 69  
 NTP 58, 80

## O

one-X Portal for IP Office  
     Configuration 44

## P

Passwd 105  
 Password 110, 111  
     Change 44  
     Root Password 105  
     Web Browser Password 52  
 Port  
     Web Control 77

## R

RAM  
     Usage 69  
 Reboot 56, 69  
 Remote Software Repositories 66  
 Repositories 66  
 Repository 77, 111  
 Restart 110  
 Restore 77, 111  
 Root 110

## S

Server  
     NTP 58, 80  
     Reboot 56, 69  
     Shutdown 56, 69  
 Server Name 36  
 Service  
     Install 61

---

- Service
  - Uninstall 63
  - Upgrade 61
- Services 74
  - Start 69
  - Starting 55
  - Status 69
  - Stop 69
  - Stopping 55
- Settings 76
- SFTP 106
- Show 108
- Shutdown 56, 69
- SNMP 77
- SNMP Support 77
- Software 36
  - Repositories 66
- Software Repositories 77
- SSH access 106
- Start 110
- Start Services 69
- Startup 111
- Status 69
- Stop 110
- Stop Services 69
- Subnet Mask 57, 80
- System 75, 80

## **T**

- Time
  - Timezone 58, 80

## **U**

- Uninstall
  - Application 63
  - Service 63
- Unit Name/IP Address 36
- Update 110
  - Services 74
  - System 75
- Updates
  - Services 73
  - System 73
- Upgrading Applications 61
- Usage
  - CPU 69
  - Disk 69
  - Memory 69

## **V**

- View Logs 71
- Voicemail Pro
  - Configuration 32
  - Limitations 14
- Voicemail Pro Client
  - run 36
- Voicemail Pro Client window 36
- Voicemail Pro Login window 36
- Voicemail Pro Server
  - connect 36

## **W**

- WAN 36
- Watchdog 77
- Web Control Port 77
- Windows Clients 85
- Workstation 36



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.

© 2013 Avaya Inc. All rights reserved.