IP Office™ Platform 9.1

Installing and Maintaining the Unified Communications Module

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

© 2016 AVAYA All Rights Reserved.

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.
For full support, please see the complete document, Avaya Support Notices for Hardware Documentation, document number 03–600759.
For full support, please see the complete document, Avaya Support Notices for Software Documentation, document number 03–600758.
To locate this document on our website, simply go to http://www.avaya.com/support and search for the document number in the search box.

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

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

Warranty
Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).
Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

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

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

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

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

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

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

Heritage Nortel Software
“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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

Virtualization
Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.
Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. “Instance” means one unique copy of the Software. For example, if the end user customer or Avaya channel partner would like to install two instances of the same type of Products, then two Products of that type must be ordered.

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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

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

Avaya Toll Fraud intervention
If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks
The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.
Avaya is a registered trademark of Avaya Inc.
All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

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

Contents

1. Overview

1.1 Module Versions 10
1.2 Using Linux 10
1.3 Additional Documentation 10
1.4 IP Address Notes 11
1.5 Small Community Networks 11
1.6 Licenses 12
1.7 Voicemail Pro Features 12
1.8 Supported Web Browsers 12
1.9 Password Authentication (Referred Authentication) 12

2. Module Installation

2.1 Quick Install 16
2.2 Downloading Module Software 18
2.3 Preparing a USB Installation Key 19
2.4 Checking/Entering Licenses 20
2.5 Changing the IP Office Time Settings 20
2.6 Changing the IP Office Security Settings 21
2.7 Shutting Down the IP Office System 22
2.8 Inserting the Module 23
2.9 Installing the Software 24
2.10 Using System Status Application 25
2.11 Igniting the Module Services 26
2.12 Adding a Certificate to the Browser 29
2.13 Logging Into Web Manager 31
2.14 Management Services Initial Configuration 33
2.15 Application Initial Configuration 34

3. Voicemail Pro Configuration

3.1 Adding Voicemail Licenses 37
3.2 IP Office Configuration 38
3.3 Installing the Voicemail Pro Client 39
3.4 Logging in to the Voicemail Server 40
3.5 Changing the Voicemail Server Password 41
3.6 Transferring Voicemail Server Settings 42
3.6.1 Transferring Custom Folders 44

4. one-X Portal for IP Office Configuration

4.1 Adding Licenses 48
4.2 Enabling one-X Portal for IP Office Users 49
4.3 Initial one-X Portal for IP Office Login 50
4.4 Initial AFA Login 51
4.5 If the one-X Portal for IP Office Service Status Remains Yellow 52
4.5.1 Portal Password at Default 52
4.5.2 Portal Password Not at Default 53
4.6 Transferring one-X Portal for IP Office Settings 54

5. Server Maintenance

5.1 Logging In 59
5.2 Logging Into Web Control Directly 61
5.3 Viewing the Module IP Address 62
5.4 Changing the IP Address Settings 62
5.5 Module LEDs 63
5.6 Module Buttons and Ports 67
5.7 Attaching a Monitor and Keyboard 68
5.8 Upgrading the Module 68
5.8.1 Web Manager Upgrade 69
5.8.2 USB Upgrade 73
5.9 Starting/Stopping Application Services 76
5.9.1 Starting a Service 76
5.9.2 Stopping a Service 76
5.9.3 Setting a Service to Auto Start 76
5.10 Changing the Linux Passwords 76
5.11 Shutting Down the Server 77
5.12 Rebooting the Server 77
5.13 Date and Time Settings 78
5.14 Creating Administrator Accounts 79
5.15 Setting the Menu Inactivity Timeout 79
5.16 Uninstalling an Application 80
5.17 Setting Up File Repositories 81
5.17.1 Source Files 81
5.17.2 Setting the Repository Locations 81
5.17.3 Uploading Local Files 82
5.17.4 Creating Remote Software Repositories 83
5.18 Downloading Log Files 84
5.19 SSH File Transfers 84

6. Web Manager

6.1 Logging In to Web Manager 87

7. Web Control/Platform View Menus

7.1 System 91
7.2 Logs 93
7.2.1 Debug Logs 94
7.2.2 Syslog Event Viewer 95
7.2.3 Download 95
7.3 Updates 96
7.3.1 Services 97
7.3.2 System 98
7.4 Settings: General 99
7.4.1 Software Repositories 99
7.4.2 Syslog 100
7.4.3 Certificates 100
7.4.4 Web Control 101
7.4.5 Backup and Restore 101
7.4.6 Voicemail Settings 101
7.4.7 ASG Settings 101
7.4.8 Watchdog 102
7.4.9 Set Login Banner 102
7.5 Settings: System 103
7.5.1 Network 103
7.5.2 Date and Time 104
7.5.3 Authentication 104
7.5.4 HTTP Server 105
7.5.5 Change Root Password 105
7.5.6 Change Local Linux Account Password 105
7.5.7 Password Rules Settings 105
7.5.8 Firewall 106
7.6 App Center 106

8. Document History

Index 111

Chapter 1.
Overview

1. Overview

This manual covers the installation, configuration and maintenance of a Unified Communications Module in an IP500 V2 system running IP Office Release 9.1 software. The module is a PC server that allows various Linux based IP Office applications to run as embedded applications within the IP Office control unit rather than requiring separate PCs.

Applications

The Unified Communications Module hosts the following applications:

- **Linux**
  This is the base operating system used. However, no specific Linux knowledge is required for installation and maintenance.
- **Management Services**
  This is a shell version of IP Office that allows basic configuration of services such as remote SSL VPN connections for server support. It also controls security settings for access to the server's menus. It does not support call features such as users, extensions or trunks.
- **one-X Portal for IP Office**
  This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely using web browser access. Each user who wants to use one-X Portal for IP Office requires a license 12.
- **Voicemail Pro**
  This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail.
- **IP Office Web Manager**
  You can configure and manage the server via browser access to the Web Manager menus. The menus also allow the launching of other clients used to configure and monitor the services run by the server.
- **Optional Services**
  Currently the Unified Communications Module does not support any optional services.

Capacity

The capacity of the Unified Communications Module is:

- **Number of Modules**
  Maximum one module per system.
- **Trunk Cards:**
  The module does not support a trunk daughter card.
- **IP Office Users:** The module supports up to 200 users when running Voicemail Pro and one-X Portal for IP Office. It supports more than 200 users when running just Voicemail Pro.
- **Simultaneous one-X Portal for IP Office Users:** 50.
- **Maximum voicemail ports:** The module provides 4 ports as standard. However, you can license additional ports. The module can support up to 20 ports when running Voicemail Pro and one-X Portal for IP Office. It can support up to 40 ports when running just Voicemail Pro.
- **Voicemail storage capacity:** Up to 800 hours of storage for messages, prompts and announcements.
- **Small Community Network:** Maximum 6 systems.

1.1 Module Versions

There are 2 versions of Unified Communications Module. Whilst the two types of card are physically different, they currently support the same embedded applications and application capacities. In this documentation, all references to Unified Communications Module cover both types of card unless otherwise stated.

- The original Unified Communications Module, Unified Communications Module v1 henceforth, is supported by IP500 V2 systems running IP Office Release 8.0 and higher.
- The Unified Communications Module v2 is supported by IP500 V2 systems running IP Office Release 9.0 and higher software.

1.2 Using Linux

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

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

1.3 Additional Documentation

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

Related Documents

- **Administering Avaya one-X Portal for IP Office™ Platform**
  This manual covers the installation and administration menus used for the one-X Portal for IP Office application. This manual is essential if the one-X Portal for IP Office needs configuring to support multiple IP Office servers in a Small Community Network.
- **Administering Avaya IP Office™ Platform Voicemail Pro**
  By default the voicemail server provides mailbox services to all users and hunt groups without any configuration. This manual covers the administration of the voicemail server using the Voicemail Pro client in order to enable additional features.
- **Administering Avaya IP Office™ Platform with Manager**
  IP Office Manager is the application used to configure IP Office systems and the Management Services service. This manual details how to use IP Office Manager and the full range of IP Office configuration settings.
- **Administering Avaya IP Office™ Platform with Web Manager**
  This covers the configuration of IP Office systems using the Web Manager menus.

Technical Bulletins

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

Other Documentation and Documentation Sources

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

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

1.4 IP Address Notes

During installation, you assign an IP address to the Unified Communications Module. The IP Office system has two physical LAN interfaces: LAN1 and LAN2.

- **The Unified Communications Module connects internally to the IP Office LAN1 network and must have an IP address the same subnet as that interface**.

Internal IP Addresses

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

- ***169.254.0.1***
  The one-X Portal for IP Office application uses this address for its connections to the IP Office. The Unified Communications Module uses it as its SNTP time source address.
- ***169.254.0.2***
  The IP Office and the one-X Portal for IP Office application use this address for their connections to the voicemail service.

User and Administration IP Addresses

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

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

LAN2 and NAT Limitation

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

1.5 Small Community Networks

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

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

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

1.6 Licenses

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

- **Essential Edition**
  This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
  The Voicemail Pro application requires this license. The license enables the application and 4 voicemail ports.
  - The Unified Communications Module v1 acts as an automatic **Preferred Edition** license for the IP Office system.
  - For the Unified Communications Module v2, a separately installed **Preferred Edition** license is required.
- **Preferred Edition Additional Voicemail Ports**
  These licenses add additional voicemail ports. You can add multiple licenses, up to 20 ports when running Voicemail Pro and one-X Portal for IP Office, or 40 ports when running just Voicemail Pro.
- **User Profile Licenses**
  For a user to use the one-X Portal for IP Office application, you must license and configure the user to one of the following user profiles in the IP Office configuration: ***Office Worker***, ***Teleworker*** or ***Power User***. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

1.7 Voicemail Pro Features

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

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

1.8 Supported Web Browsers

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

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

1.9 Password Authentication (Referred Authentication)

The password authentication for access to the services hosted by the server can use either each services' own security settings or use the security user accounts configured for the Management Services service running on the Unified Communications Module. The **Enable referred authentication** 104 setting controls the method used.

- **Enabled**
  With referred authentication enabled, the security settings of the Management Services service running on the Unified Communications Module control access to the following other services:
  - **Web control menus**
  - **Voicemail Pro admin**
  - **one-X Portal for IP Office admin**
  - **IP Office Web Manager**
- **Disabled**
  With referred authentication disabled, each service controls access to itself using its own local account settings.

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

Upgrading

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

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

Chapter 2.
Module Installation

2. Module Installation

The instructions in this section relate to the installation of a Unified Communications Module into an IP Office Release 9.1 system.

2.1 Quick Install

The following process is a summary of the steps for installing a Unified Communications Module. Use this process if you are familiar with IP Office operation and configuration. For a more detailed installation process, proceed from the following section, Downloading Module Software 18.

Allow up to 1 hour 30 minutes for the process, not including the downloading of the required software.

1. Prerequisites

Check that you have the following:

a. An IP500 V2 running IP Office Release 9.1 in Essential Edition mode. For a Unified Communications Module v2 the system must also have a **Preferred Edition** license 20.

b. A Windows PC with IP Office Manager networked to the IP Office system. Test by opening the configuration of the IP Office.

c. A 5mm Flat-blade screwdriver plus anti-static wrist strap and ground point for module insertion.

d. A 4GB USB memory key.

e. An IP address to assign to the module on the same subnet as the IP Office system's LAN1.

f. A hostname for the module to use on the customer's network.

g. The latest Unified Communications Module ISO image and USB software that match the IP Office release. See Downloading Module Software 18.

2. Prepare the USB Key for Installation

a. Using the downloaded software 18, prepare the USB installation key 19.

3. IP Office Configuration

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

a. Click **Control Unit** and select the **IP500 V2**. Note the **Version**. This should match the software you downloaded for the module.

b. Click **System** and then **LAN1** tab. On the **LAN Setting** sub-tab, note the **IP Address**.

c. Select the **System** tab. Set the **Time Setting Config Source** to either ***SNTP*** or ***None***. Click **OK**.

d. Click to save the configuration back to the IP Office.

4. IP Office Security

The installation of the one-X Portal for IP Office service assumes that the **EnhTcpaService** user is set to the default password ***EnhTcpaPwd1***. If this is not the case, set the IP Office security service user account back to that default password. You can change the password again after installation.

5. Shutdown the IP Office

Using IP Office Manager, shutdown the system (**File | Advanced | System Shutdown**). Only switch off power to the system when the each LED1 on the front of the unit and the CPU LED on the rear flash rapid red-amber. See System Shutdown 22.

6. Insert the Unified Communications Module and Software Installation Key

a. Insert the module 23 into an empty slot in the system.

b. Insert the USB memory key into the upper USB slot on the module.

c. Reapply power to the system and wait for the system to restart.

d. For the Unified Communications Module v2 connect System Status Application 25 to the IP Office as this shows the progress of the installation.

e. New Unified Communications Module v2 modules automatically start installing from the memory key during the system restart, skip to step h.

f. Once the system is running, shut down the UCM by pressing the top button on the module until the upper LED 63 starts to flash green. The shutdown is complete once all module LEDs are off except for the regular system heartbeat (an amber flash every 5 seconds).

g. Restart the module by pressing the upper button until both LEDs turn amber and then off.

h. Allow the process to run until the USB key no longer indicates any activity (approximately 50 minutes).

- During the restart, if necessary, the module firmware upgrades. The upper LED flashing amber-green with lower LED off indicates this. The restart, including firmware upgrade, takes approximately 25 minutes.
- ! **WARNING:** It is important that you allow this stage to complete even if no upgrade activity appears to be taking place. Wait at least 25 minutes.

7. Ignite the Unified Communications Module

a. Using a web browser, enter https:// followed by the LAN1 address of the IP Office and ***:7071***. For example ***https://<IP Office LAN1 address>:7071***. The login menu appears.

b. The default name and password are ***root*** and ***Administrator***.

c. Accept the license and click **Next**.

d. Enter IP address details valid for the same subnet used by LAN1 of the IP Office. Click **Next**.

e. Select which applications you want the module to run. Click **Next**.

f. Set the passwords for future access to the module. Click **Next**.

g. Accept the default time settings. Enter a hostname and click **Next**.

h. Check the settings and click **Apply**.

8. Configure the Server Applications

Check and configure the server applications. See Voicemail Pro Configuration 36 and one-X Portal for IP Office Configuration 48.

- ! **Important:** Check in the IP Office switch configuration that the **Voicemail Type** is set to ***Voicemail Pro on UC Module*** with the **Voicemail IP Address** set to match the module's IP address.

2.2 Downloading Module Software

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

- **ISO Image**
  You can use this type of file to reinstall the full set of software including the operating system. Before using an ISO image, you must backup all applications data. Note that the Unified Communications Module uses a separate ISO image from other Linux based IP Office products. You require this file when installing a Unified Communications Module. The Unified Communications Module v1 and Unified Communications Module v2 use the same ISO image.
- **Source ISO Image**
  Some components of the software are open source. To comply with the license conditions of that software, Avaya is required to make the source software available. However, this file is not required for installation.
- **RPM Files**
  Occasionally Avaya may make separate RPM files available for maintenance.
- **Rufus software**
  This additional software is downloadable from https://rufus.akeo.ie. You use it to load an ISO image onto a USB memory key from which the server can boot and run that ISO image.

To download software:

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

2.3 Preparing a USB Installation Key

Avaya supplies the Unified Communications Module v2 without any pre-installed software. Therefore, a USB memory key to install the new software is required for installation.

Whilst Avaya supplies the Unified Communications Module v1 with pre-installed software, that software is unlikely to match the software level of the IP Office system. Therefore, this manual assumes that a software install is part of the module installation.

This process uses a downloaded ISO image to create a bootable USB memory key for software installation.

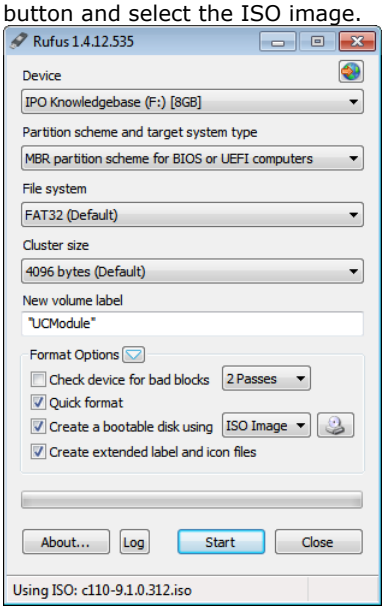
- **! WARNING**
  Using the USB Memory key overwrites any existing software and data on the server.

Prerequisites

- **4GB USB Memory Key**
  Note that this process reformats the memory key and erases all files. The module supports USB and USB2.
- **Rufus software**
  This additional software is downloadable from https://rufus.akeo.ie. You use it to load an ISO image onto a USB memory key from which the server can boot and run that ISO image.
- **Unified Communications Module ISO Image**
  You can download this software from the Avaya support website (http://support.avaya.com).

To create a bootable USB memory key:

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



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

7. **! Important: Copy the Installation Files**
   You must copy a number of files to a new location on the USB memory key.
   a. Using the file explorer, open the **USB** folder on the USB memory key. This folder contains 4 files, some of which are used for installation and other are used for upgrading.
   b. Select just the files **syslinux.cfg** and **avaya_autoinstall.conf**. Copy those two files to the top level (root) of the USB memory key, overwriting any existing files with those names.
8. Remove the USB memory key from the PC. The device is ready for use for full software installation.

2.4 Checking/Entering Licenses

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

- **Essential Edition**
  This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
  The Voicemail Pro application requires this license. The license enables the application and 4 voicemail ports.
  - The Unified Communications Module v1 acts as an automatic **Preferred Edition** license for the IP Office system.
  - For the Unified Communications Module v2, a separately installed **Preferred Edition** license is required.
- **Preferred Edition Additional Voicemail Ports**
  These licenses add additional voicemail ports. You can add multiple licenses, up to 20 ports when running Voicemail Pro and one-X Portal for IP Office, or 40 ports when running just Voicemail Pro.
- **User Profile Licenses**
  For a user to use the one-X Portal for IP Office application, you must license and configure the user to one of the following user profiles in the IP Office configuration: ***Office Worker***, ***Teleworker*** or ***Power User***. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

To check or enter a license:

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

2.5 Changing the IP Office Time Settings

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

To change the time settings:

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

2.6 Changing the IP Office Security Settings

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

- The one-X Portal for IP Office application uses the **Enhanced TSPI** service and **EnhTcpaService** user for its connection to the IP Office. The installation assumes that the **EnhTcpaService** user is enabled and has the default password of ***EnhTcpaPwd1***.
  - If the password is not at default during the Unified Communications Module installation, the one-X Portal for IP Office service will not start correctly and the service user account becomes locked. To resolve that, follow the steps below and then restart the one-X Portal for IP Office service.
  - Once the one-X Portal for IP Office service is operating correctly, you can change the **EnhTcpaPwd1** password.
- Voicemail Pro connects to the IP Office using the **Voicemail Password**. This is set in the IP Office system's security settings (System | Unsecured Interfaces) and must be matched by the password set in the voicemail servers preferences 41 after installation.

To change the security settings:

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

2.7 Shutting Down the IP Office System

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

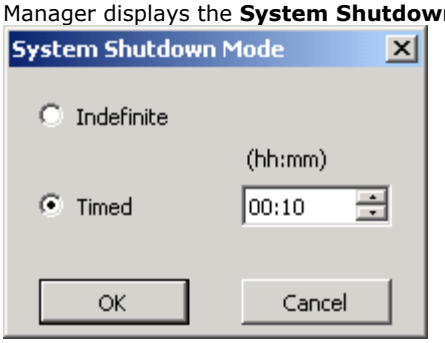
- **! WARNINGS**
  - You must always shutdown a system before switching it off. Simply removing the power cord or switching off the power input may cause the loss of data.
  - This is not a polite shutdown, it stops any user calls and services in progress.
  - The shutdown process takes up to a minute to complete. When shutting down a system with a Unified Communications Module installed, the shutdown can take up to 3 minutes while the card safely closes all open files and closes down its operating system. During this period, the module's LED 1 remains green.
  - Do not remove power from the system until the system LEDs are in the following states:
    - For the Unified Communications Module v2, the upper LED is off and the lower LED flashes red-amber.
    - For the Unified Communications Module v1, the LEDs are all off.
    - For all other card types, LED 1 flashes fast red-amber. For those base cards with a trunk daughter card installed, LED 9 also flashes fast red-amber.
    - The CPU LED on the rear of the system flashes fast red-amber.
    - The System SD and Optional SD memory card LEDs on the rear of the system are off.
  - To restart a system when shutdown indefinitely, or to restart a system before the timed restart, switch power to the system off and on again.

To shutdown the system using the AUX button:

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

To shutdown the system using IP Office manager:

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



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

To shutdown the system using the System Status Application:

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

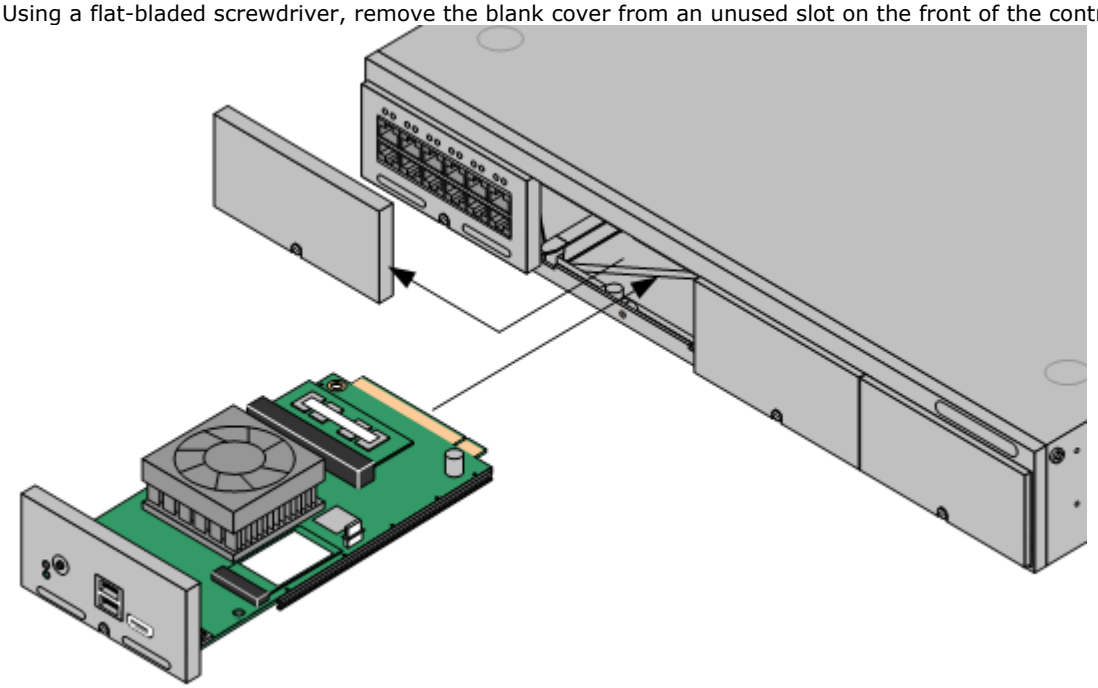
2.8 Inserting the Module

Once you have shutdown 22 the system, you can insert the module.

- **! WARNINGS**
  - Ensure that you take anti-static protection steps while handling circuit boards.
  - Never add or remove cards from the control unit while it has power connected.
- **Tools Required**
  - 5mm Flat-blade screwdriver.
  - Anti-static wrist strap and ground point.
  - USB Installation Key
  - PC with System Status Application connection to the IP Office system.
  - Monitor and HDMI or HDMI to DVI cable.

To insert the module:

1. For a Unified Communications Module v1, ensure that the plastic cover that fits over the external ports on the module's faceplate is in place.
2. Using a flat-bladed screwdriver, remove the blank cover from an unused slot on the front of the control unit.



3. Allowing the module to rest against the bottom of the slot, begin sliding it into the control unit. When half inserted, check that the module rails have engaged with the slot edges by trying to gently rotate it. If the module rotates, remove it and begin inserting it again.
4. While inserting the module, also check to ensure that cables on the module do not interfere with the insertion operation.
5. The module should slide in freely until almost fully inserted. At that point, apply pressure at the base of the front of the module to complete insertion.
6. Using a flat-bladed screwdriver, secure the module.
7. Reapply power to the system. Once the system has restarted, you can install the module software 24.

2.9 Installing the Software

To install software from the previously prepared USB memory key 19, use the following process. This process reinstalls the module software and if necessary upgrades the module firmware.

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

To install a software image from a USB memory key:

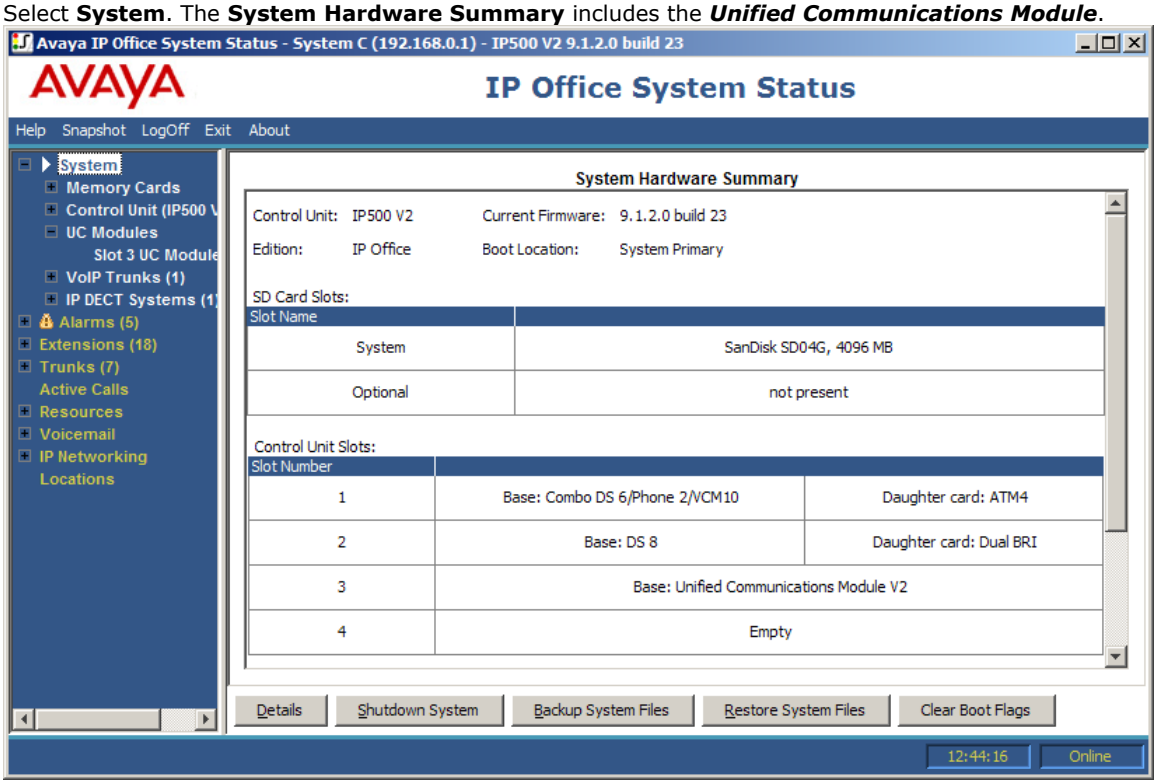
1. For a new Unified Communications Module v2, having inserted the module 23 and restarted the IP Office, the module automatically starts installing the software from the memory key if already inserted. Start System Status Application (step 3) if not already done and then skip to step 8.
2. For the Unified Communications Module v1, remove the plastic cover from the front of the module. Retain this and reattach it after completing this process.
3. Connect to the IP Office using System Status Application and select the details of the module 25. The page shows the module status. For the Unified Communications Module v2 it also shows the progress of an installation or upgrade.
4. For the Unified Communications Module v1 we also recommend connecting a monitor using an HDMI to HDMI cable or HDMI to DVI cable. Note that the module only activates the video port if it detects a monitor whilst restarting.
5. Insert the USB memory key with the new ISO image file into the module's upper USB port.
6. Shut down the module by pressing the upper button on the module until the LED starts to flash green. The shutdown is complete once all module LEDs are off except an amber flash of the lower LED every 5 seconds.
7. Restart the module by pressing the upper button again and keeping it pressed until the two LEDs change from amber to off.
8. After up to 2 minutes initializing, the module boots using the files on the USB memory key.
   - **Unified Communications Module v2:**
     System Status Application reports the module as *"Initializing"*, then *"USB Booting"* and then *"USB Upgrade/Install"*. Both LEDs flash amber/green. System Status Application displays a progress bar. If after 15 minutes this shows no progress, the most likely cause is that you did not complete the final stage of preparing the USB key, copying files from the USB folder.
   - **Unified Communications Module v1:**
     System Status Application reports the module as *"Running"*. The upper LEDs alternate between green and off.
9. The installation process can take up to 80 minutes. After the software installation completes, the module restarts. During the restart, if necessary the module's firmware upgrades. The restart, including firmware upgrade, takes approximately 25 minutes. During this, for the Unified Communications Module v2, System Status Application displays *"Applications starting"*.
   - **! WARNING:** It is important that you allow this stage to complete even if no upgrade activity appears to be taking place. Wait at least 25 minutes.
10. After this the LEDs indicate the module's status as follows:
    - **Lower status LED shows only regular IP Office heartbeat flashes:**
      This indicates that the mode automatically shutdown after a firmware upgrade. Restart the module by pressing the top button or using System Status Application 25.
    - **Lower status LED green except for regular IP Office heartbeat flashes:**
      This indicates that the module restarted without needing a firmware upgrade.
11. The software installation is complete when System Status Application shows details of the module memory and lists the one-X Portal for IP Office application. On the Unified Communications Module v2 the status shows "*Idle, card has not been ignited*". You now need to ignite the module services 26.
12. Remove the USB memory key.
13. Remove any monitor connection.
14. For the Unified Communications Module v1, refit the plastic cover removed at the start of the process.

2.10 Using System Status Application

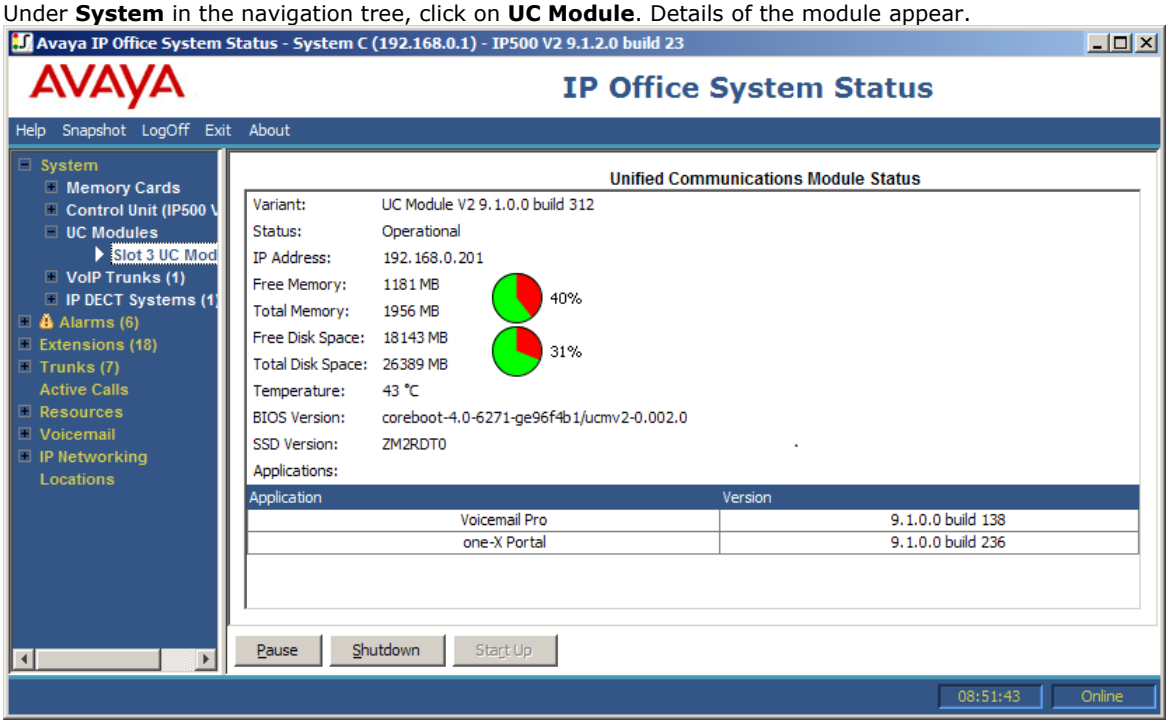
System Status Application displays the status of the Unified Communications Module. It also provides controls to shutdown and start up the module.

To check a Unified Communications Module using System Status Application:

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



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



Status Messages and Alarms

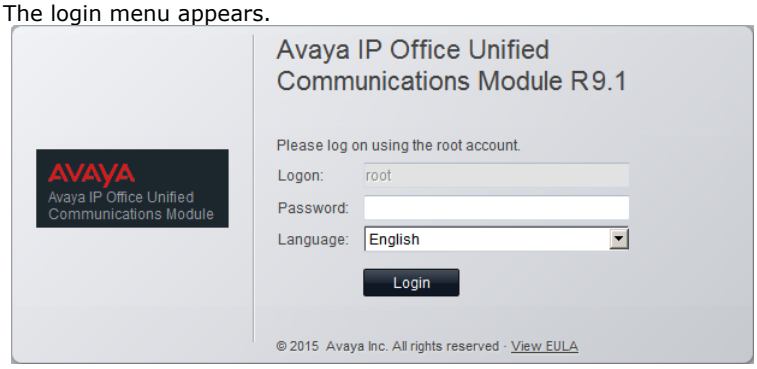
For the Unified Communications Module v2, System Status Application shows a range of status messages. For details see Module LEDs 63. For the module error states, it also creates an appropriate alarm in System Status Application.

2.11 Igniting the Module Services

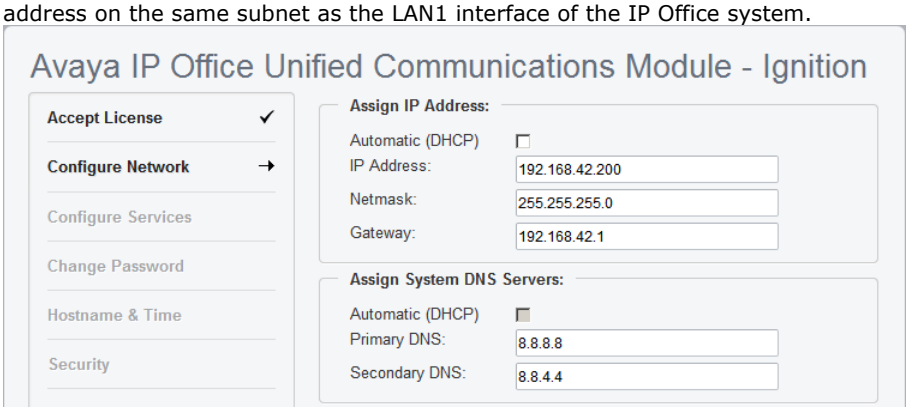
Following software installation 24, the module requires ignition. For a Unified Communications Module v2 this is indicated by the message *"Idle, card has not been ignited"* and the lower LED green.

To ignite the module services:

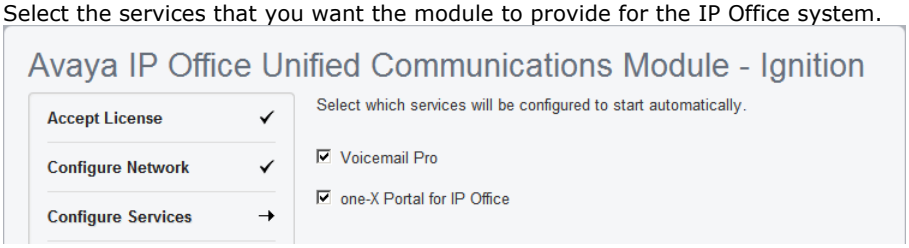
1. From a client PC, start the browser. Enter ***https://*** followed by the LAN1 IP address of the IP Office system and ***:7071***. For example, enter ***https://192.168.42.1:7071***.
2. The login menu appears.



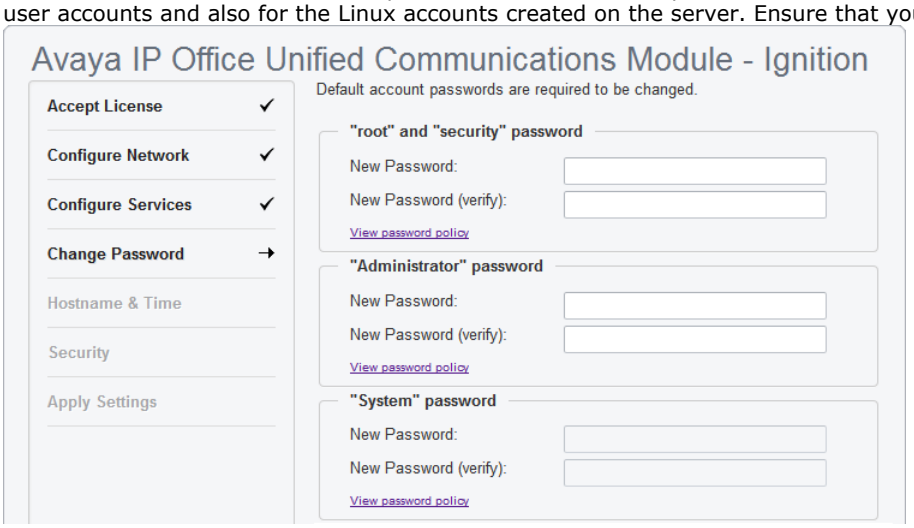
   - Note the release number shown after the **R** in the menu title. If this does not match the software release of the IP Office system, stop ignition and install the appropriate Unified Communications Module release to match the system.
3. Enter the default password (***Administrator***).
4. Click **Login**. If you accept the license, select **I Agree** and click **Next**.
5. Enter the IP address and DNS settings that the module should use. Enter details that give the module an IP address on the same subnet as the LAN1 interface of the IP Office system.



6. Select the services that you want the module to provide for the IP Office system.

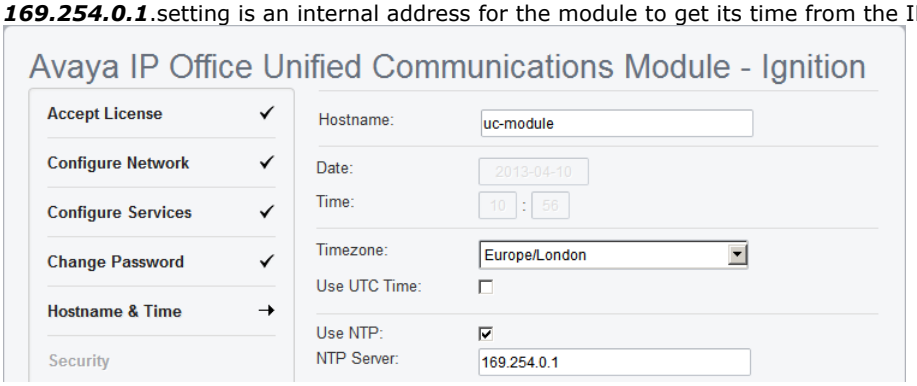


7. Click **Next**. Enter and confirm new passwords. These are the passwords for various Management Services service user accounts and also for the Linux accounts created on the server. Ensure that you note the passwords set.

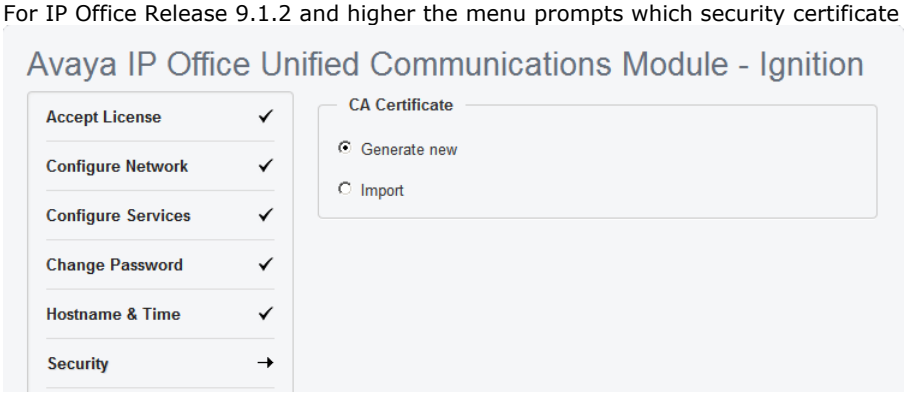


- The passwords must be 8 to 32 characters, containing at least two types of character (lower case, upper case, numeric and special characters) and no more the 3 consecutive characters.
  - **root/security password**
    This sets the password for both the Linux **root** user account and also the **security** account of the Management Services service.
  - **Administrator password**
    This sets the password for Linux **Administrator** account and also the **Administrator** account of the Management Services service run on the Unified Communications Module. With **Referred Authentication** 12 enabled (the default) this is also the default account used for Voicemail Pro and one-X Portal for IP Office administrator access.
  - **System password**
    This sets the **System** password for the Management Services.

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

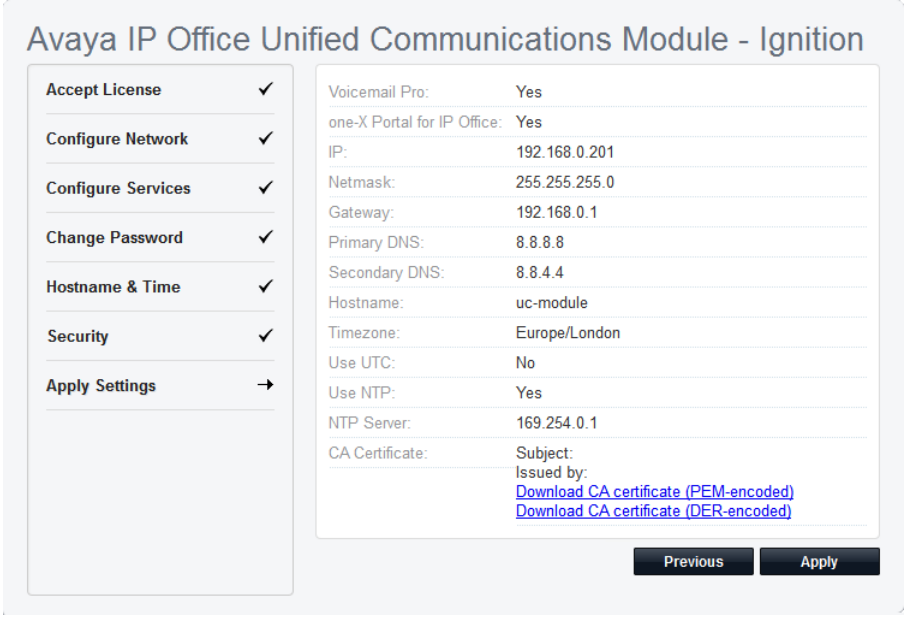


9. For IP Office Release 9.1.2 and higher the menu prompts which security certificate the server should use.



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

11. Click **Next**. A summary of the settings appears.



12. For IP Office Release 9.1.2 and higher, if **Generate New** was selected for the server's security certificate, download the security certificate files from the menu and store these safely. These certificates need to be used by the browser and other applications for future access to the server.

13. Click **Apply**. Click **OK** when displayed to access the server's IP Office Web Manager menus. Note that this can take up to 10 minutes.

14. For IP Office Release 9.1.2 and higher follow the instructions for adding a certificate to your browser 29.

2.12 Adding a Certificate to the Browser

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

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

If using the server's own generated certificate, you can downloaded from the ignition menu, or after ignition, from the **Certificates** 100 section of the **Settings | General** menu. The server provides it certificate as a PEM or CRT file.

To add a server security certificate to Firefox:

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

To add a server security certificate to Internet Explorer:

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

To add a server security certificate to Google Chrome:

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

To add a server security certificate to Mac Safari:

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

To add a server security certificate to Windows Safari:

1. From the browser, open the directory containing the certificate file.
2. Right-click the file and select **Install Certificate**. You may be prompted for admin credentials and/or a confirmation prompt.
3. On the first wizard screen, click **Next**.

4. On the **Certificate Store** screen select **Place all certificates in the following store**.
5. Click **Browse**.
6. Select the **Trusted Root Certification Authorities** option.
7. Click **OK**.
8. Click **Next**.
9. Click **Finish**. If another security warning dialog displays, click **Yes**.

2.13 Logging Into Web Manager

You can administer the Unified Communications Module using a web browser on a client PC with network access to the Unified Communications Module. Note that web manager is only available after you have ignited the server 26.

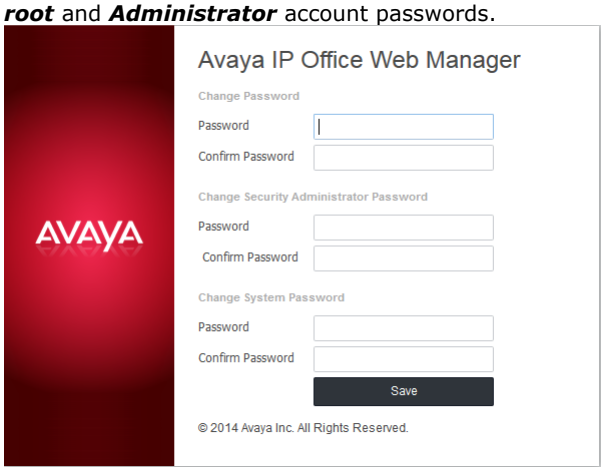
Avaya supports the following browsers for web access to the server menus:

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

To access Web Manager:

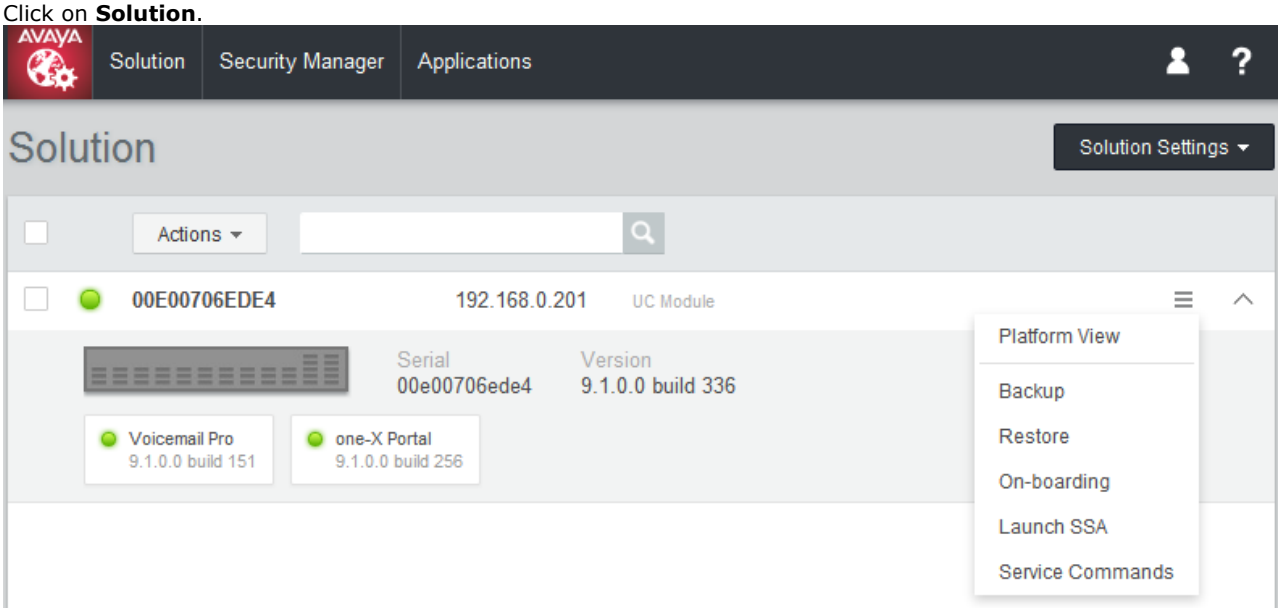
1. Log in to IP Office Web Manager.
   a. Enter **https://** followed by the module's IP address and then 7070. Alternatively, enter **https://** followed by the IP Office system address and from the menu click **IP Office Web Manager on UCM**.

   b. Enter the user name and password.
   c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. Note that this does not change the Linux ***root*** and ***Administrator*** account passwords.

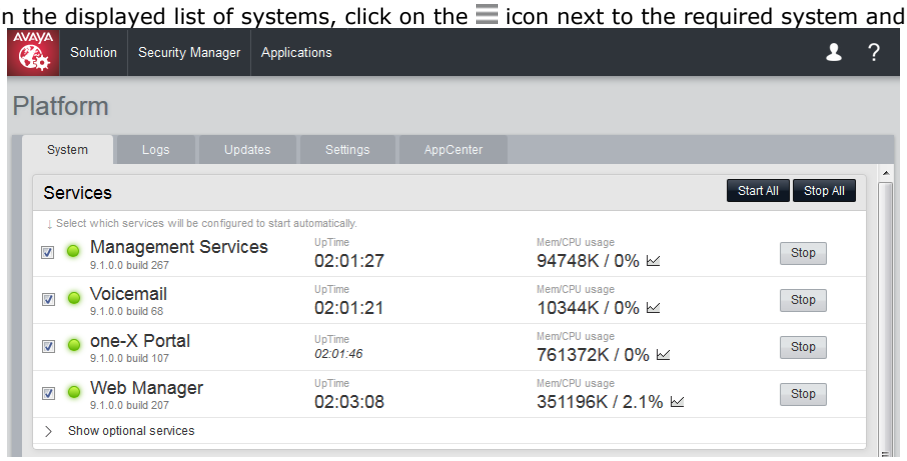


- ***Change Password***
  This sets the password for the **Administrator** account of the Management Services service run on the Unified Communications Module. With **Referred Authentication** 12 enabled (the default) this is also the default account used for Voicemail Pro, one-X Portal for IP Office and Web Manager administrator access.
- ***Change Security Administrator Password***
  This sets the password for the Management Services security administrator account.
- ***Change System Password***
  This sets the **System** password for the Management Services.

2. Click on **Solution**.



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

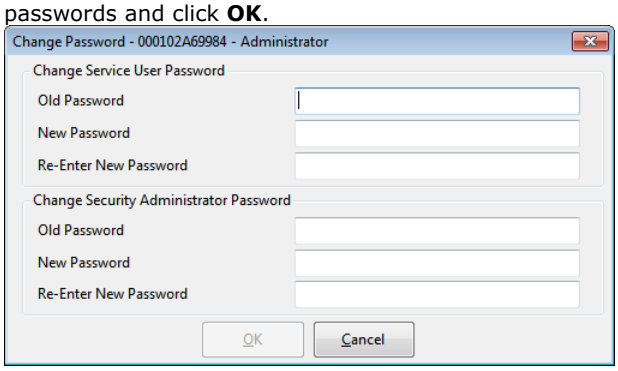


2.14 Management Services Initial Configuration

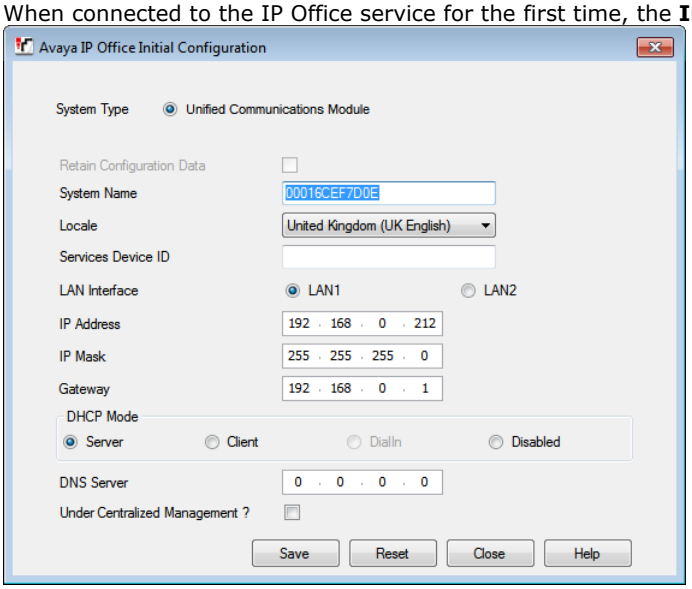
The Management Services service provided by the server requires initial configuration. This is especially important for servers centrally managed using Avaya System Manager.

To perform IP Office initial configuration:

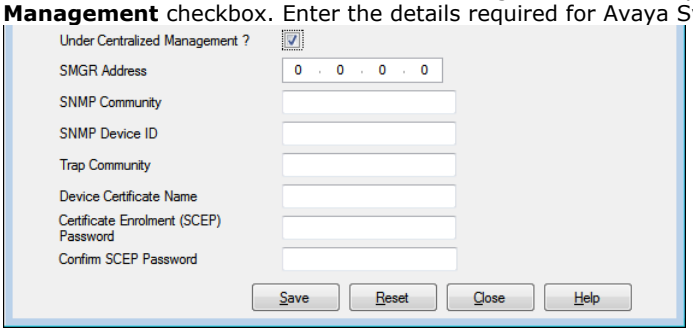
1. Start IP Office Manager. Click and use the **Select IP Office** menu to discover the available IP Office systems.
2. Select the tick box next to the Unified Communications Module. Click **OK**.
   - If any Management Services passwords are at their default values, a menu to change the default passwords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



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



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



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

2.15 Application Initial Configuration

Once operation of the module and its menu is confirmed, you can being the initial configuration of the applications. Refer to the following chapters based on the applications selected during the modules ignition:

1. **Voicemail Pro Initial Configuration** 36
2. **one-X Portal for IP Office Initial Configuration** 49

Chapter 3.
Voicemail Pro Configuration

3. Voicemail Pro Configuration

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

Details of IP Office and Voicemail Pro configuration are covered by the Voicemail Pro Installation manual and Voicemail Pro Administration manuals 10. This section of this manual covers only the minimum steps recommended to ensure that the voicemail server is operating.

Initial Configuration Summary

a. **IP Office Configuration**

   i. **Adding voicemail licenses** 37

   ii. **Check the Voicemail Type Setting** 38

b. **Voicemail Pro Configuration**

   i. **Install the Voicemail Pro client** 39

   ii. **Log in to the Voicemail Pro server** 40

   iii. **Change the voicemail server password** 41

IMPORTANT: Voicemail IP Address Note

The IP Office uses the address 169.254.0.2 to connect to the voicemail application on the Unified Communications Module. This is the address set for the voicemail server 38 in the IP Office configuration. Do not use this address for any other purpose. For all other access to the voicemail server use the IP address of the Unified Communications Module. To check the IP address, see Viewing the Module IP Address 62.

Transferring Settings from a Previous Server

For an IP Office system already configured to operate with an external Voicemail Pro server; you can transfer the settings, prompts and messages on the old server to the new server. See Transferring Voicemail Server Settings 42.

3.1 Adding Voicemail Licenses

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

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

- **Essential Edition**
  This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
  The Voicemail Pro application requires this license. The license enables the application and 4 voicemail ports.
  - The Unified Communications Module v1 acts as an automatic **Preferred Edition** license for the IP Office system.
  - For the Unified Communications Module v2, a separately installed **Preferred Edition** license is required.
- **Preferred Edition Additional Voicemail Ports**
  These licenses add additional voicemail ports. You can add multiple licenses, up to 20 ports when running Voicemail Pro and one-X Portal for IP Office, or 40 ports when running just Voicemail Pro.

To enter ADI licenses:

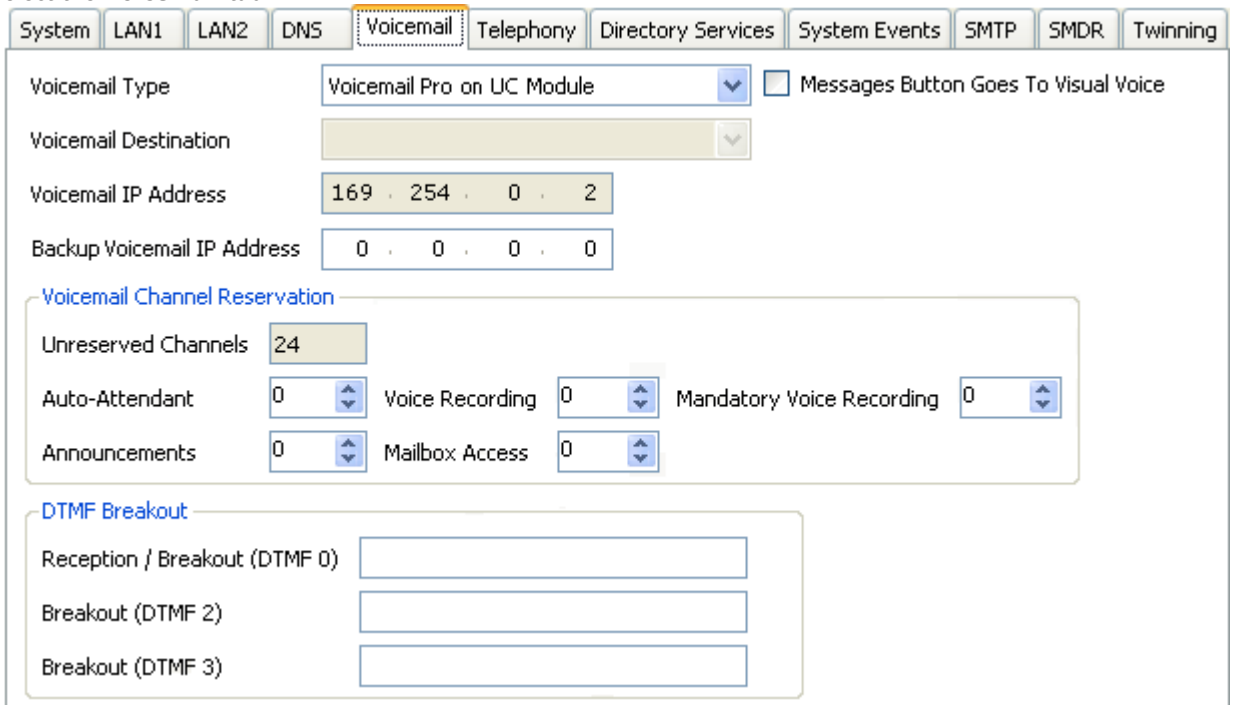
1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select **License**.
3. Click **Add** and select **ADI**.
4. Enter the new license and click **OK**. You should add licenses by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.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

3.2 IP Office Configuration

When you add a Unified Communications Module running Voicemail Pro to a system, the system automatically adjusts to use that voicemail server. However, you should confirm this by checking the **Voicemail Type** and **Voicemail IP Address** settings in the IP Office configuration.

To set the voicemail server address:

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



- Check that the **Voicemail Type** is set to ***Voicemail Pro on UC Module***.
- **! WARNING: IP Address**
  By default, when a configuration set to **Voicemail Pro on UC Module** is loaded, the IP address shown is the IP address of the Unified Communications Module. If for any reason, the **Voicemail Type** is changed, when set back to **Voicemail Pro on UC Module**, set the IP address to ***168.254.0.2***. This is the internal private IP address 11 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. You can license the Unified Communications Module up to 20 ports when running Voicemail Pro and one-X Portal for IP Office or 40 ports when running just Voicemail Pro.

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

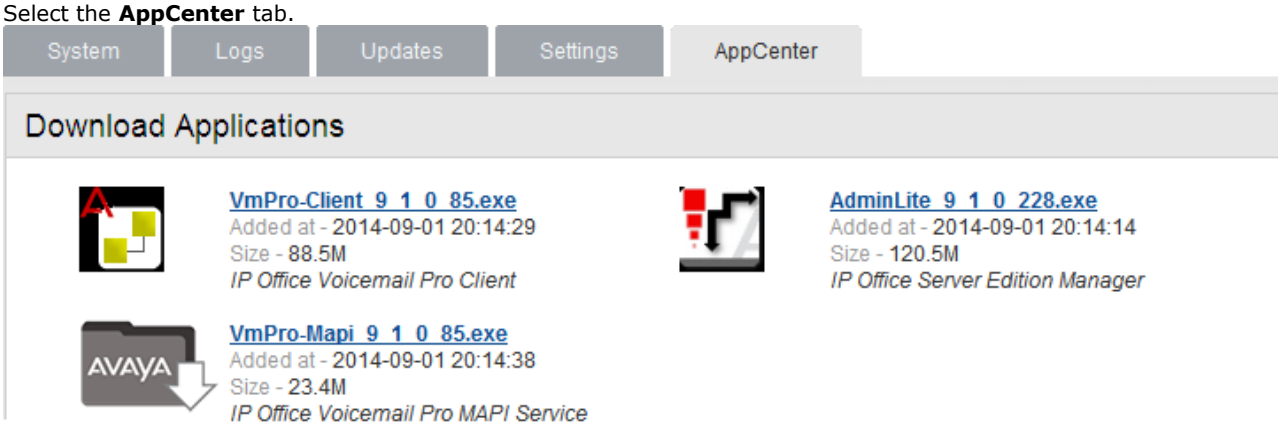
3.3 Installing the Voicemail Pro Client

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

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

To download and install the Voicemail Pro client:

1. Log in to wIP Office Web Manager 87. In the displayed list of systems, click on the ☰ icon next to the server and select **Platform View**.
2. Select the **AppCenter** tab.

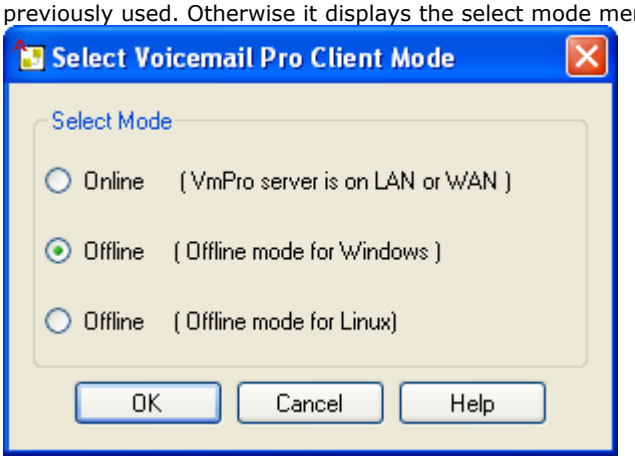


3. Click on the link for the Voicemail Pro client file in order to download the software package for installing the client.
4. Run the software package to install the Voicemail Pro client.

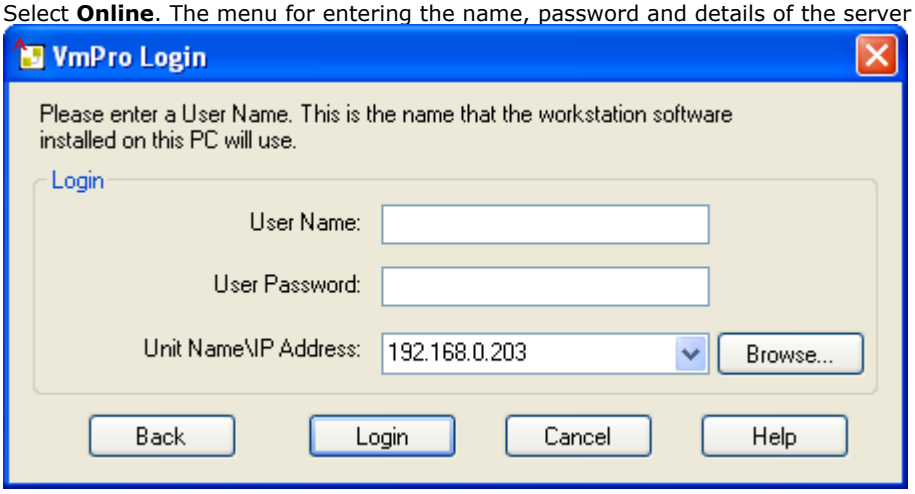
3.4 Logging in to the Voicemail Server

To login with the Voicemail Pro client:

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



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



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

3.5 Changing the Voicemail Server Password

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

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

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

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

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

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

3.6 Transferring Voicemail Server Settings

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

For the Unified Communications Module, once you have obtained a backup of the old server, you can load it onto the Unified Communications Module from a USB memory key. Otherwise, if the backup is too large for the USB memory key use SSH file transfer.

- **Backing Up/Restoring Custom Folders**
  If the existing voicemail server uses folders outside its default folders those folders are not included in the backup/restore processes. To transfer additional folders see Transferring Custom Folders 44.

To back up the old voicemail server:

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

To transfer the backup to a USB memory key:

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

- **Windows Server**
  You can select the backup location before starting the backup. The default location for backup files is ***C:\Program Files\Avaya\IP Office\Voicemail Pro\Backup\Scheduled***.
  1. Using **My Computer**, locate the previous manual backup. The date and time is part of the folder name for the backup.
  2. Right-click on the folder and select **Properties**. Check that the Size on disk is within the capacity of the USB memory key.
     - If not, copy the backup folder and all its contents onto a PC from which you can eventually load it onto the new server using an SSH file transfer.
     - If with the USB memory key capacity, Copy the backup folder and all its content onto a USB memory key. Do not put the folder into another folder or change the folder name.
- **Linux Server**
  The default location for backup files on a Linux server is ***/opt/vmpro/Backup/Scheduled***.
  1. Using an SSH file transfer tool 84, connect to the old server and browse to ***/opt/vmpro/Backup/Scheduled/Immediate***.
  2. Locate the manual backup taken above. The date and time is part of the folder name for the backup.
  3. Copy the folder and all its contents onto the PC running SSH.
  4. Right-click on the folder and select **Properties**. Check that the Size on disk is within the capacity of the USB memory key.
     - If not, copy the backup folder and all its contents onto a PC from which you can eventually load it onto the new server using an SSH file transfer.
     - If within the USB memory key capacity, copy the backup folder and all its content onto a USB memory key. Do not put the folder into another folder or change the folder name.

To shut down the old voicemail server:

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

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

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

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

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

To load the backup onto the new server using SSH:

If you copied the backup onto a PC, use the following method to transfer and then restore the backup.

1. Connect to the Unified Communications Module using an SSH File transfer tool 84.
2. Copy the backup folder into the folder ***/opt/vmpro/Backup/Scheduled/Immediate***.
3. Using a web browser, login 61 to the server.
4. Select **Settings**. On the **General** tab, select the **Restore** button for the Voicemail service. From the list of available backups, select the one just copied onto the server.
5. Click **OK**.
6. After completing the restore, use the **System** menu to ***Stop*** and then ***Start*** the voicemail service.

3.6.1 Transferring Custom Folders

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

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

To manually backup a custom folder:

1. Using an SSH file transfer tool 84, copy the folder ***Custom*** from ***/opt/vmpro*** to your PC to create a backup of the folder.

To manually restore a custom folder:

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

Chapter 4.

one-X Portal for IP Office Configuration

4. one-X Portal for IP Office Configuration

At this stage, whilst installed and started, the one-X Portal for IP Office server and IP Office still require some configuration. The following sections are a summary only. For full details, refer to the one-X Portal for IP Office Installation manual 10.

Initial Configuration Summary

a. **Add licenses** 48
   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** 49
   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** 50
   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.

IMPORTANT: one-X Portal for IP Office IP Address Note

The one-X Portal for IP Office application uses the IP address 169.254.0.1 for its internal connection to the IP Office system. Do not use this address for any other purpose such as external access to the one-X Portal for IP Office application. For all other access to the one-X Portal for IP Office server from elsewhere on the network, use the IP address of the Unified Communications Module. To check the address, see Viewing the Module IP Address 62.

4.1 Adding Licenses

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

To enter licenses:

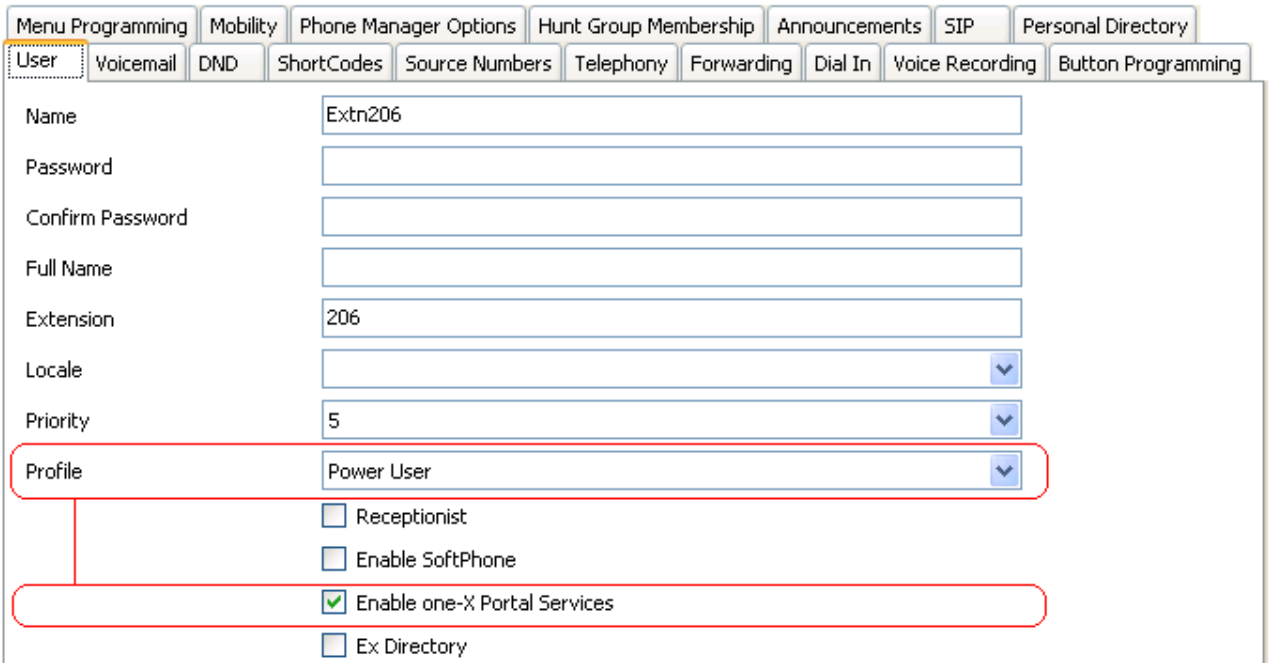
1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select **License**.
3. Click **Add** and select **ADI**.
4. Enter the new license and click **OK**. You should add licenses by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.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

4.2 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 48 for those roles.

To enable one-X Portal for IP Office users:

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



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

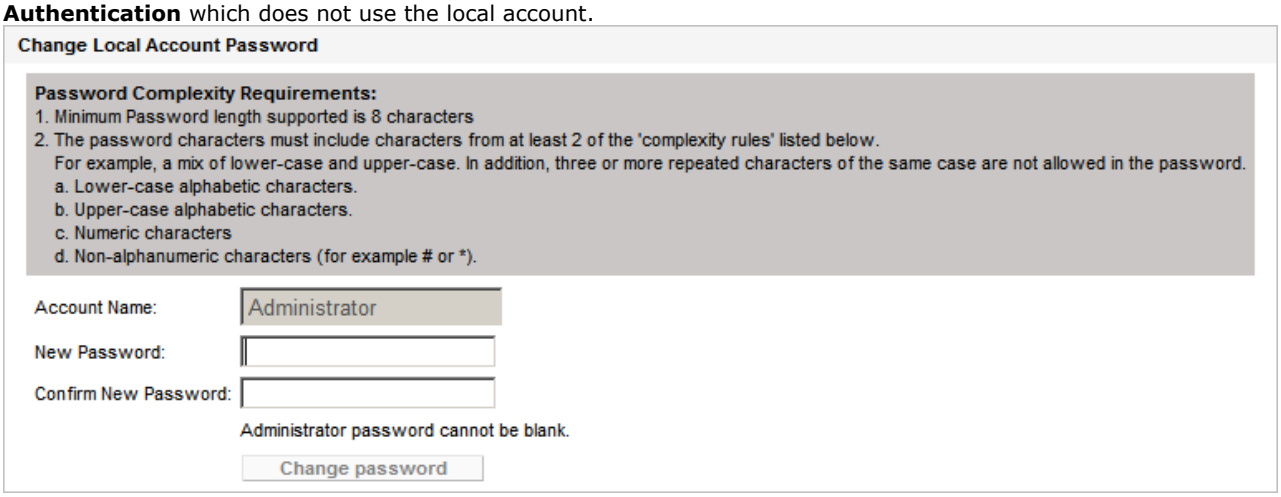
4.3 Initial one-X Portal for IP Office Login

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

- If you selected both the one-X Portal for IP Office and Voicemail Pro applications during the module initialization, they require no further configuration. When you log into the one-X Portal for IP Office administration, it takes you directly to the final step of changing the local administrator password.

To login to one-X Portal for IP Office:

1. From within the server's Web Manager menus, click on **Applications** and select **one-X Portal**.
   - Alternatively, using a browser enter **https://** followed by the address of the Unified Communications Module and then ***:9443/onexportal-admin.html***.
2. The login menu appears. If the message ***System is currently unavailable - please wait*** appears, the one-X Portal for IP Office application is still starting. When the message disappears, you can login.
3. Enter **Administrator** and the password created for that user during the server ignition. Click **Login**.
   - The step above assumes that **Referred Authentication** 12 is enabled (the default for new installs). If not, then the default local account name and password stored by the one-X Portal for IP Office are **Administrator** and **Administrator**.
4. The server prompts you to change the local password. This is necessary even if you are using **Referred Authentication** which does not use the local account.



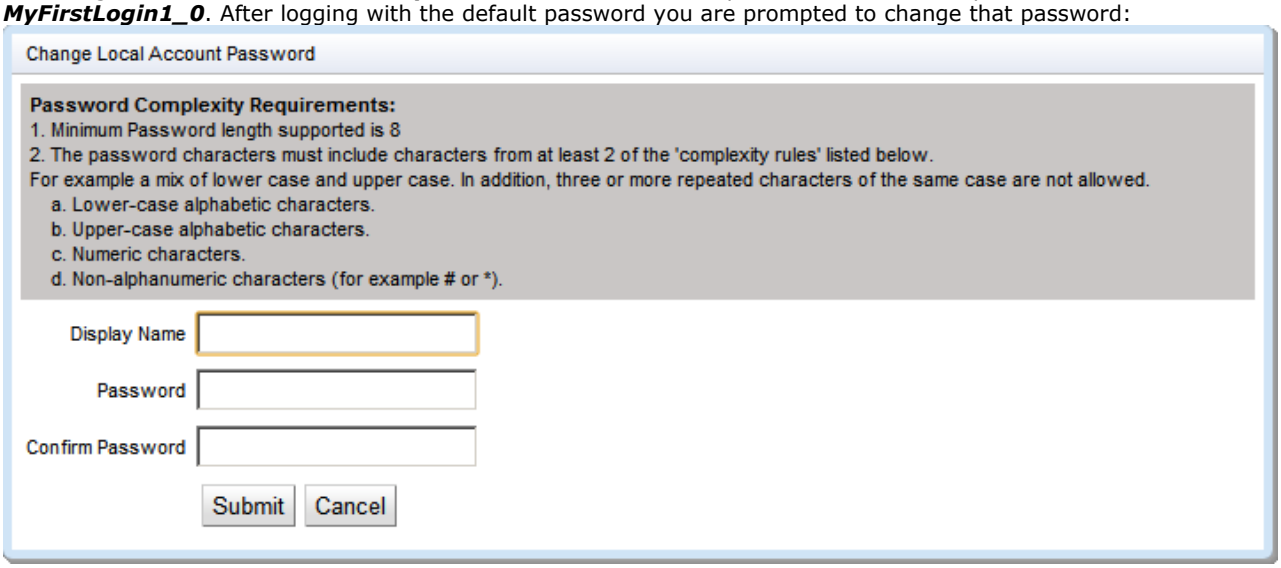
5. Enter and confirm a new password. Click **Change Password**.
6. You now have access to the one-X Portal for IP Office administration menus. For full details, refer to the one-X Portal for IP Office Administration manual 10.
7. Click on **Log Out**.
8. Click on **User Login** shown top-right.
9. The login window displays ***System in currently unavailable***. When this message is no longer displayed, attempt to login as a user.

4.4 Initial AFA Login

This process is only necessary if not using **Referred Authentication** 12 for administrator security. You can use the AFA menus to perform backup and restoration operations. Even if not used, you should login in order to change the menu's default password.

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

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



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

4.5 If the one-X Portal for IP Office Service Status Remains Yellow

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

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

With the Unified Communications Module, the portal service assumes that the IP Office uses the default password.

4.5.1 Portal Password at Default

You can use this process if you think that the one-X Portal for IP Office is already using the default service password.

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

1. Using Web Manager, you can access the configuration required.
2. Stop the one-X Portal for IP Office service:
    a. Login to the server's Web Manager menus.
    b. From the **Solution** page, click on the ☰ icon next to the portal server and select **Platform View**.
    c. Stop the **one-X Portal** service. Wait until the status icon changes to red.
3. Change the password of the **EnhTcpaService** back to its default:
    a. Login to the IP Office system's Web Manager menus.
    b. Click on **Security Manager** and select **Service Users**.
    c. Click on the ✎ edit icon for the **EnhTcpaService** user.
    d. Set the password back to ***EnhTcpaPwd1***.
    e. Change the **Account Status** back to ***Enabled***.
    f. Click **Update**.
4. Restart the one-X Portal for IP Office service:
    a. Select the platform view for the portal server again.
    b. Start the one-X Portal service. Wait for the status icon to change to green. This can take up to 5 minutes.

4.5.2 Portal Password Not at Default

You can use this process if you think that the one-X Portal for IP Office is not using the default service password.

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

1. Change the portal provider passwords back to the default:
    a. Login to the portal services administrator menus. You can do this by logging in to the portal server's Web Manager menus, clicking on **Applications** and selecting **one-X Portal**.
    b. Click **Configuration**. Select **Providers** and click **Get All**.
    c. Click on the **Edit** button for the ***Default-CSTA-Provider***.
        i. Click **IP Office(s) Assigned**.
        ii. Set the **Password** back to ***EnhTcpaPwd1*** and click **Close**.
        iii. Click **Close** again.
    d. Repeat the process for the ***Default-DSML-IPO-Provider***.
    e. Select the check boxes next to each of those two providers and then click **Put Selected**.
2. Stop the one-X Portal for IP Office service:
    a. Login to the server's Web Manager menus.
    b. From the **Solution** page, click on the ☰ icon next to the portal server and select **Platform View**.
    c. Stop the **one-X Portal** service. Wait until the status icon changes to red.
3. Change the password of the **EnhTcpaService** back to its default:
    a. Login to the IP Office system's Web Manager menus.
    b. Click on **Security Manager** and select **Service Users**.
    c. Click on the ✎ edit icon for the **EnhTcpaService** user.
    d. Set the password back to ***EnhTcpaPwd1***.
    e. Change the **Account Status** back to ***Enabled***.
    f. Click **Update**.
4. Restart the one-X Portal for IP Office service:
    a. Select the platform view for the portal server again.
    b. Start the one-X Portal service. Wait for the status icon to change to green. This can take up to 5 minutes.

4.6 Transferring one-X Portal for IP Office Settings

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

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

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

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

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

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

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

To reconfigure the restored settings:

The Unified Communications Module uses a number of internal IP addresses 11 for connections between the IP Office system and the applications it hosts. You need to reconfigure any settings restored from another server to use the internal IP addresses.

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

Chapter 5.
Server Maintenance

5. Server Maintenance

For IP Office Release 9.1, the web control menus (also called "platform view" or "web control panel (WCP)") are a sub-component of the server's Web Manager 86 menus through which they can be accessed.

- **Logging In** 59
- **Logging Into Web Control Directly** 61
- **Viewing the Module IP Address** 62
- **Changing the IP Address Settings** 62
- **Module LEDs** 63
- **Module Buttons and Ports** 67
- **Attaching a Monitor and Keyboard** 68
- **Upgrading the Module** 68
- **Starting/Stopping Application Services** 76
- **Changing the Linux Passwords** 76
- **Shutting Down the Server** 77
- **Rebooting the Server** 77
- **Date and Time Settings** 78
- **Creating Administrator Accounts** 79
- **Setting the Menu Inactivity Timeout** 79
- **Uninstalling an Application** 80
- **Setting Up File Repositories** 81
- **Downloading Log Files** 84
- **SSH File Transfers** 84

5.1 Logging In

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

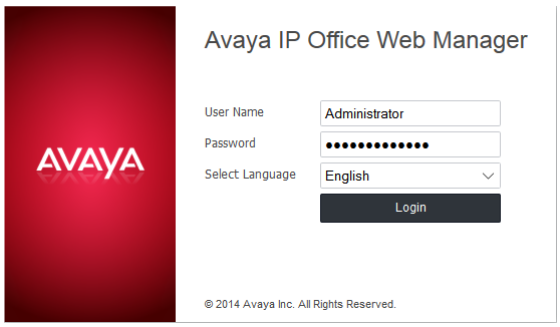
Avaya supports the following browsers for web access to the server menus:

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

To access Web Manager:

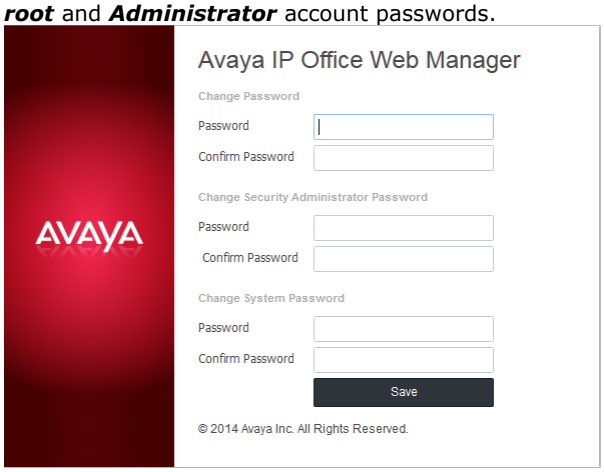
1. Log in to IP Office Web Manager.

   a. Enter **https://** followed by the module's IP address and then 7070. Alternatively, enter **https://** followed by the IP Office system address and from the menu click **IP Office Web Manager on UCM**.



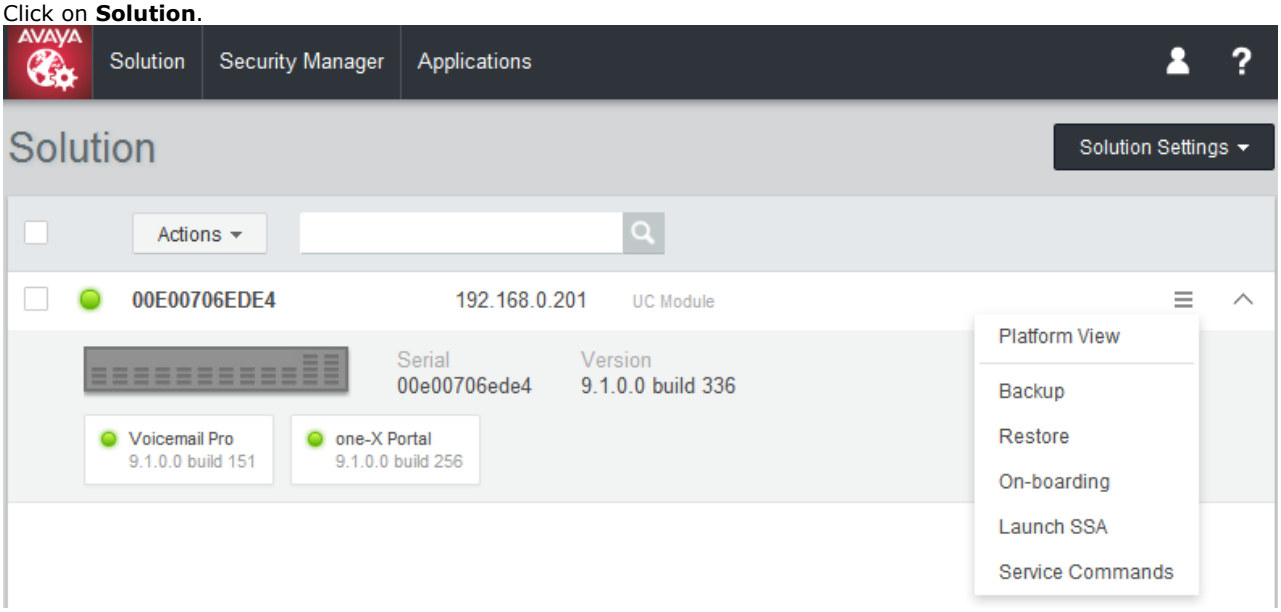
   b. Enter the user name and password.

   c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. Note that this does not change the Linux ***root*** and ***Administrator*** account passwords.

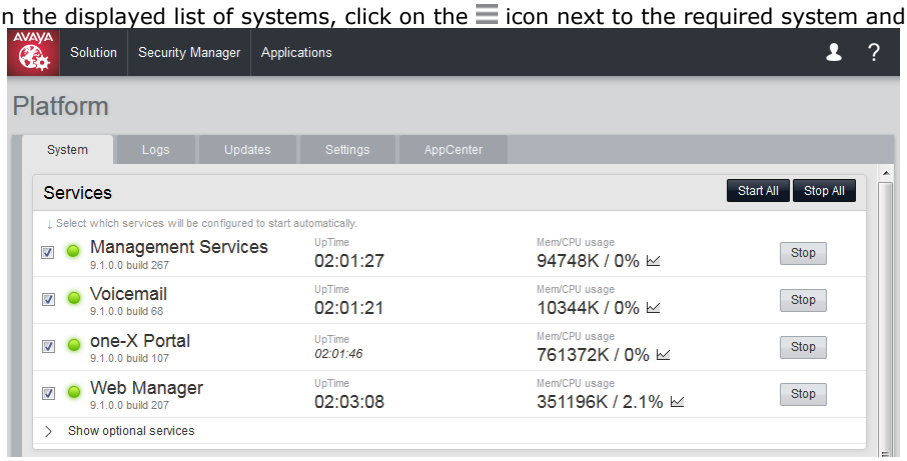


   - ***Change Password***
     This sets the password for the **Administrator** account of the Management Services service run on the Unified Communications Module. With **Referred Authentication** 12 enabled (the default) this is also the default account used for Voicemail Pro, one-X Portal for IP Office and Web Manager administrator access.
   - ***Change Security Administrator Password***
     This sets the password for the Management Services security administrator account.
   - ***Change System Password***
     This sets the **System** password for the Management Services.

2. Click on **Solution**.



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



5.2 Logging Into Web Control Directly

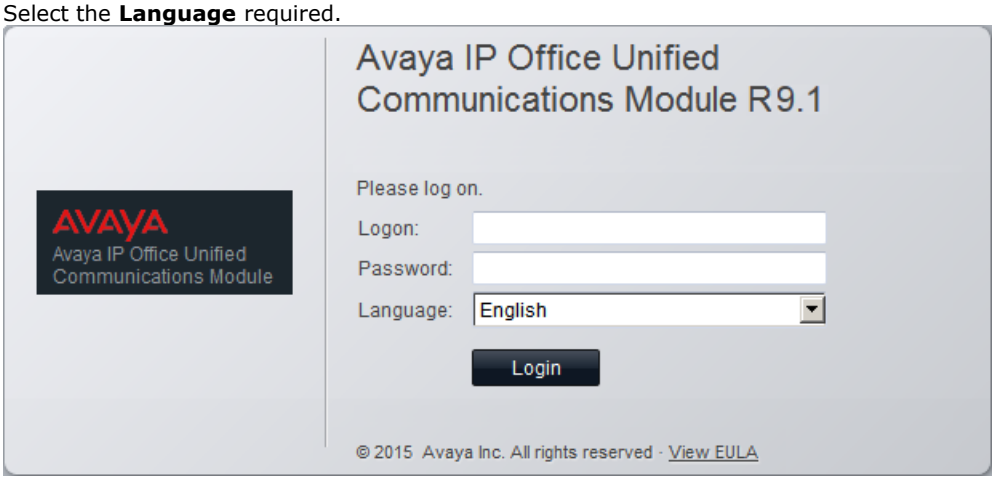
Use the following method to login directly to the server's web control menus rather than via the server Web Manager 59 menus. This method of logging may be necessary if the **Web Manager** service is not running on the server for some reason.

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

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

To login to the server web control menus:

1. From a client PC, start the browser. Enter ***https://*** followed by the address of the server and ***:7071***. If the IP address is unknown, see Viewing the Module IP Address 62.
   - If the browser displays a security warning, you may need to load the server's security certificate.
2. Select the **Language** required.



3. Enter the name and password for server administration.
4. If the login is successful, the server's **System** 91 page appears.

5.3 Viewing the Module IP Address

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

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

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

5.4 Changing the IP Address Settings

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

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

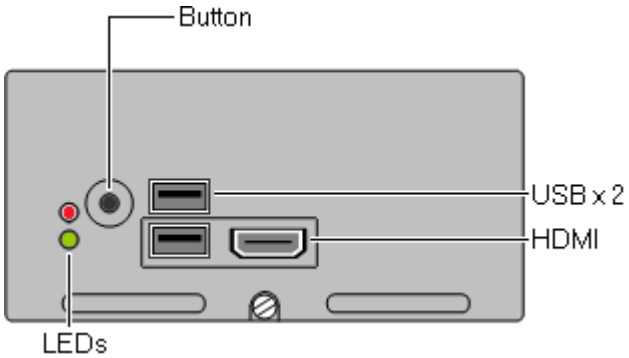
To change the IP address:

1. Login 59 to the server's web configuration menus.
2. Select **Settings**.
3. Select **System**.
4. Set the **Network** section as required.
   - **Network Interface**
     For the Unified Communications Module, this setting is fixed as ***eth0.1***.
     - **Enable Traffic Control**
       When enabled, the server throttles the rate at which it sends UDP packets from the IP Office service to IP Office System Monitor. This may be necessary if the IP Office System Monitor traces indicate a high number of lost packets.
   - **Host Name**
     Sets the host name that the Unified Communications Module should use. This setting requires the local network to support a DNS server. Do not use ***localhost***.
   - **Use DHCP**
     Do not use this setting with the Unified Communications Module.
   - **IP Address**
     Displays the IP address set for the server. The Unified Communications Module connects to the LAN1 interface of the IP Office and must have an address on that subnet. See IP Address Notes 11.
   - **Subnet Mask**
     Displays the subnet mask applied to the IP address.
   - **Default Gateway**
     Displays the default gateway settings for routing.
   - **System DNS**
     Enter the address of the primary DNS server.
   - **Automatically obtain DNS from provider**
     Not used.
5. Click **Save**. The server restarts.

5.5 Module LEDs

Unified Communications Module v2

The Unified Communications Module v2 uses the LED on its front panel to indicate the module's status. For the Unified Communications Module v2, all the LED states are also reflected by the status show in System Status Application.



Unified Communications Module v2

Key

- **Off**
- **On**
- **Flashing** (0.5 seconds on/0.5 seconds off).
- **Alternating** (Amber/Green - 1 second per. Red/Amber - 0.5 second per).

IP Office Heartbeat

- In addition to the LED states below, the lower LED also shows the IP Office system heartbeat (an amber flash every 5 seconds).

The **Status** columns below refer to the corresponding module status shown in System Status Application 25.

Shutdown Sequence LEDs

	LEDs		Description	Status
Shutting Down	Flashing green		Indicates that the module is shutting down.	*Shutting Down*
	Off			
Shutdown	Off		Indicates that the module has been shutdown.	*Shutdown*
	Off			
BIOS Upgrading	Amber-green		Indicates that the BIOS is upgrading.	
	Off			
IP Office Shutting Down	Off		Indicates that the IP Office system is shutting down.	–
	Red			
IP Office Shutdown	Off		Indicates that the IP Office system has shutdown.	–
	Red-amber			

Startup Sequence LEDs

	LEDs		Description	Status
IP Office power up	Off		The IP Office is initializing. The module remains in this state if not supported by the IP Office system after the system has started.	–
	Red			
Module starting	Amber		The module is powering up.	*Starting up*
	Amber			
Module initializing	Off		The module is initializing.	*Initialising*
	Flashing green			
Module booting	Flashing green		The module is booting its operating system. These LEDs are also shown near the end of the software installation process.	*OS Booting*
	Flashing green			
Module ignition required	Off		For a newly installed module, the module has started but module service ignition 26 has not been complete.	*Idle, card has not been ignited*
	Green			
Applications starting	Flashing green		The module is starting the applications.	*Applications stating*
	Green			
Module operational	Green		The module is operational.	*Operational*
	Green			

Startup Fault LEDs

	LEDs		Description	Status
Module not supported	Off		The IP Office system does not support the module. Check that the system is an IP500 V2 running IP Office Release 9.0 or higher in Essential Edition mode.	–
	Red			
Initialization fault	Red		The module has failed to start correctly.	*Initialising*
	Red			
No Boot Device	Flashing red		No boot device (internal or external) found. Changes to shutdown on a button press.	*No bootable device found.*
	Flashing green			
Boot failure	Red		The module failed to boot.	*OS Boot Fault*
	Flashing green			
Application start fault	Red		One of the modules applications failed to start correctly.	*Applications Start Fault*
	Green			
Application failure	Flashing red		One of the module applications failed.	*Software fault*
	Green			
IP Office Comms Fault	Flashing red		Indicates a loss of communications to the module. The module automatically reboots to try to recover. If the problem persists, reinstall the module software.	*Hardware Fault*
	Flashing red			

USB Install/Upgrade LEDs

	LEDs		Description	Status
Module starting		Amber	The module is powering up. Releasing the button just after these LEDs change to off instructs the module to boot from USB.	*Starting up*
		Amber		
Module initializing		Off	The module is initializing.	*Initialising*
		Flashing green		
Booting from USB		Flashing green	Booting from USB.	*USB Booting*
		Amber-green		
Upgrading from USB		Amber-green	Installing or upgrading the module. For an install or upgrade from USB System Status Application shows a progress bar.	*USB Upgrade/ Install or Web Manager Upgrade*
		Amber-green		
Completing Installation		Flashing green	Following installation of new software, the module reboots and then performs further tasks using the new software in order to complete the installation.	*Completing Installation*
		Flashing green		
Applications starting		Flashing green	The module is starting the applications.	*Applications starting*
		Green		
Module ignition required		Off	For a newly installed module, the module has started but module service ignition 26 has not been complete.	*Idle, card has not been ignited*
		Green		

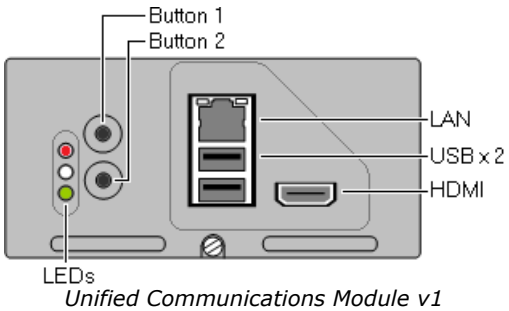
USB Install/Upgrade Fault LEDs

If any of these occur, exit the state by pressing the button to shut down the module. Then try the following in order. Ensure that the USB device is plugged in properly before starting the UCM. Try the USB device in the other UCM USB port. Rebuild the installation image on the USB device. Use a different USB device.

	LEDs		Description	Status
No upgrade USB found		Flashing red	Having booted expecting a bootable USB device, no bootable device was detected.	*No bootable USB device found*
		Amber-green		
USB Boot failed		Flashing red	Following this the module shuts down.	*USB Boot Fault*
		Amber-green		
USB upgrade failed		Red	Following this the module shuts down.	
		Amber-green		
Boot failure		Red	The module could not boot from the attached USB device. Most likely the required ISO was not present.	*OS Boot Fault*
		Flashing green		

Unified Communications Module v1

The Unified Communications Module v1 provides the following LEDs:

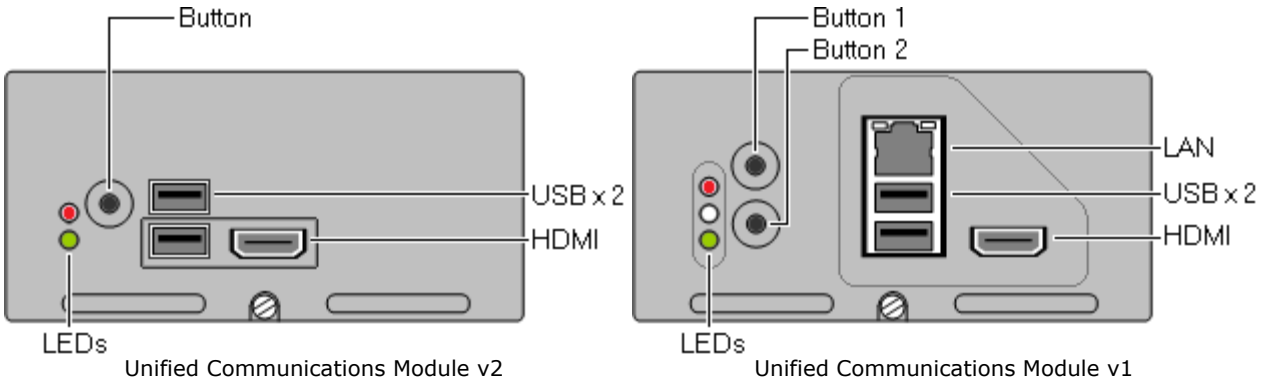


Unified Communications Module v1

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

5.6 Module Buttons and Ports

The Unified Communications Module provides the following buttons:



Unified Communications Module v2

Unified Communications Module v1

Buttons

- **Upper Button/Button 1**
  You can use the buttons for the following functions:
  - **Shutdown**
    If the module is running, pressing this button for more than 2 seconds starts a module shutdown. The lower LED changing to off with regular amber blinks indicates a completed shutdown.
  - **Startup**
    If the module has been shutdown, pressing this button causes it to startup.
  - **Alternate Boot**
    When the module is about to boot, pressing and holding the switch until the LEDs change to off instructs the module to attempt to boot from any device attached to its USB ports.
- **Button 2:** Not used. Not present on the Unified Communications Module v2.

Ports

- **HDMI**
  You can use this port to attach a monitor. Use a HDMI to HDMI cable, HDMI to DVI cable or HDMI cable with HDMI to DVI adapter. Note that the module only activates the port if it detects the monitor whilst restarting.
- **USB**
  Each module has two USB2 ports. You can use the USB ports for software installation and upgrades. You can also use the ports to connect a USB keyboard for maintenance if advised by Avaya.
- **LAN**
  Not used. Not present on the Unified Communications Module v2.

5.7 Attaching a Monitor and Keyboard

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

- **! WARNING: Do Not Remove the Port Cover Except for Maintenance**
  Avaya supplies Unified Communications Module v1 cards with a plastic cover located over the external ports (LAN, USB and HDMI). The cover must always be in place during normal card operation. You should only remove the cover temporarily during maintenance actions that require access to the ports. You must replace the cover when the maintenance is completed.

To attach a keyboard:

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

To attach a monitor:

For maintenance and diagnostics purposes, you can attach a monitor to the HDMI port on the front of the module. Use a HDMI to HDMI cable, HDMI to DVI cable or HDMI cable with HDMI to DVI adapater. Note that the module only activates the video port if it detects a monitor whilst restarting.

5.8 Upgrading the Module

Avaya makes an ISO image available for each IP Office release. You can use this for upgrading a module. The file and method to use depends on the upgrade path.

The table below summarizes the supported methods for upgrading a UCM from a previous release to IP Office Release 9.1.

From	To
	9.1
8.0.x	• USB Upgrade 73
8.1.x	• USB Upgrade 73
9.0.x	• USB Upgrade 73
9.1	• USB Upgrade 73 • Web Manager Upgrade 69

- **Web Manager Upgrade** 69
  You can use this method remotely. It includes options for scheduling the actual upgrade. This method is performed in two stages:
  1. Transferring the ISO image of the target software release to the module
  2. Triggering or scheduling the upgrade.
- **USB Upgrade** 73
  This method requires physical access to the module. It uses a specially prepared USB memory key onto which the ISO image of the target software release has been loaded.

- **! Disable one-X Portal for IP Office Logging before upgrading**
  You must disable one-X Portal for IP Office logging prior to upgrading. If you do not do this, one-X Portal for IP Office admin is very slow to respond after the upgrade. You can disable one-X Portal for IP Office logging through the one-X Portal for IP Office administrator menus by setting the **Master Logging Level** (**Diagnostics | Logging Configuration**) to ***OFF***.
- **! Password Change Required after Upgrading to 9.1+**
  When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See Logging Into Web Manager 87.

5.8.1 Web Manager Upgrade

For modules running IP Office Release 9.1, you can use the module's Web Manager menus to upgrade the module. This method allows the remote transfer of the ISO to the server from a file server using a range of protocols (HTTP, HTTPS, FTP, SFTP, SSH) or from the user's browser. You can then either select an immediate upgrade or configure a scheduled upgrade.

- **! WARNING**
  Only use a Unified Communications Module specific ISO image. Do not use other ISO images such as Server Edition ISO images.
- **! Upgrade Warning**
  Upgrading 68 shows a summary of the supported upgrade paths and methods. Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.
- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.
- **! Password Change Required after Upgrading to 9.1+**
  When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See Logging Into Web Manager 87.
- **! Disable one-X Portal for IP Office Logging before upgrading**
  You must disable one-X Portal for IP Office logging prior to upgrading. If you do not do this, one-X Portal for IP Office admin is very slow to respond after the upgrade. You can disable one-X Portal for IP Office logging through the one-X Portal for IP Office administrator menus by setting the **Master Logging Level** (**Diagnostics | Logging Configuration**) to ***OFF***.

Process Summary

1. **Download the software** 18
   Download the ISO image.
2. **Backup the applications**
   Backup the Voicemail Pro and one-X Portal for IP Office applications to a location other than the module. Refer to the IP Office Web Manager documentation 10 for details of the various backup methods.
3. **Disable one-X Portal for IP Office Logging**
   You must disable one-X Portal for IP Office logging prior to upgrading. If you do not do this, one-X Portal for IP Office admin is very slow to respond after the upgrade. You can disable one-X Portal for IP Office logging through the one-X Portal for IP Office administrator menus by setting the **Master Logging Level** (**Diagnostics | Logging Configuration**) to ***OFF***.
4. **Transfer the ISO image**
   Use one of the possible methods to transfer the ISO image to the module.
   - **Transfer from a remote file server** 70 (http, https, ftp, sftp, scp).
   - **Transfer from a module path** 71
   - **Transfer from the browser** 71
   - **Transfer from a USB upgrade key** 72
5. **Upgrade the module** 72
   Select the upgrade server option in the Web Manager menus.
6. **Check operation** 86
   Log in to the server.

5.8.1.1 ISO Transfer from a Remote File Server

You can upload an ISO image to the server from a previously configured file server. The process for this is the same for virtual and non-virtual machines. Refer to the IP Office Web Manager documentation for full details.

To configure a remote file server source:

1. Login to IP Office Web Manager 61 on the virtual machine.
3. Click on the **Solution Settings** drop-down and select **Remote Server Options**.
4. IP Office Web Manager lists the currently configured remote servers.
5. Click **Add Remote Server**.
6. Enter details for the remote file server hosting the ISO image. The details required vary depending on the protocol used by the server.
7. Click **OK**.
8. The new remote server is now included in the list of remote servers. Click **Close**.

To transfer the ISO from a remote file server:

1. Login 59 to the server's web configuration menus.
2. Click **Solutions**.
3. Click on the **Actions** drop-down and select **Transfer ISO**.
4. Click **Transfer from** and select ***Remote Location***.
   a. Click **Select Remote Server** and select the previously configured remote file server from the list.
   b. In the **File path** field, enter the path to the ISO image on that server.
   c. Click **OK**. The menu shows the progress of the download.
5. When the download has finished, the menu displays the available version. Click **Close**.
6. The servers listed in the **Solution** overview show an ⚠ icon and ***Upgrade Available***. Proceed to Upgrading from a downloaded ISO 72.

5.8.1.2 ISO Transfer from a Server Path

You can use SFTP/SSH to upload an ISO image directly to a folder on the server. The upload process is typically slow, taking several hours, but reliable.

To upload an ISO image using SSH/SFTP:

1. Start your SFTP or SSH file application and connect to the Unified Communications Module PC. The exact method depends on the application you are using.
    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 ***Administrator***.
        - The **Protocol** is ***SFTP/SSH***.
        - The **Port** is ***22***.
    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 Linux Administrator account password.
2. The default folder displayed after logging in is ***/home/Administrator***.
3. Upload the ISO image to the server.

To transfer the ISO from a UCM server path:

1. Login 59 to the server's web configuration menus.
2. Click **Solutions**.
3. Click on the **Actions** drop-down and select **Transfer ISO**.
4. Click **Transfer from** and select ***UCM Server Path***.
    a. In the **File path** field, enter the path to the previously uploaded ISO image. For example, ***/home/Administrator/Downloads/c110-9.1.0-209_el6.iso***.
    b. Click **OK**. The menu shows the progress of the download.
5. When the download has finished, the menu displays the available version. Click **Close**.
6. The servers listed in the **Solution** overview show an ⚠ icon and ***Upgrade Available***. Proceed to Upgrading from a downloaded ISO 72.

5.8.1.3 ISO Transfer from the Client Browser

We do not recommend this method of uploading an ISO image to the server for remote maintenance of servers not located on the same local network as the PC. The file transfer is slow and does not continue or automatically resume if the IP Office Web Manager session disconnects during the transfer.

To transfer the ISO from the browser client PC:

1. Login 59 to the server's web configuration menus.
2. Click **Solutions**.
3. Click on the **Actions** drop-down and select **Transfer ISO**.
4. Click **Transfer from** and select ***Client Machine***.
    a. For the **Select ISO** field, click **Browse**. Locate and select the ISO image and click **Open**.
    b. Click **OK**. The menu shows the progress of the download.
5. When the download has finished, the menu displays the available version. Click **Close**.
6. The servers listed in the **Solution** overview show an ⚠ icon and ***Upgrade Available***. Proceed to Upgrading from a downloaded ISO 72.

5.8.1.4 ISO Transfer from USB

Using a prepared USB upgrade key 74 inserted into the module's upper USB port you can transfer the keys contents into the module to then be used for an upgrade.

To transfer the ISO from the browser client PC:

1. Login 59 to the server's web configuration menus.
2. Click **Solutions**.
3. Click on the **Actions** drop-down and select **Transfer ISO**.
4. Click **Transfer from** and select ***USB UCM Server***.
   a. For the **Select ISO** field, click **Browse**. Locate and select the ISO image and click **Open**.
   b. Click **OK**. The menu shows the progress of the download.
5. When the download has finished, the menu displays the available version. Click **Close**.
6. The servers listed in the **Solution** overview show an ⚠ icon and ***Upgrade Available***. Proceed to Upgrading from a downloaded ISO 72.

5.8.1.5 Upgrading using the Transferred ISO Image

Having downloaded an ISO image to the server, IP Office Web Manager shows an ⚠ icon and ***Upgrade Available*** next to the server's details on the **Solution** menu.

- **Scheduled Upgrade**
  Through the IP Office Web Manager menus you can schedule actions such as upgrading rather than running them immediately. For details of scheduling actions, refer to the IP Office Web Manager documentation 10.

To start an upgrade using IP Office Web Manager:

1. Login to IP Office Web Manager.
2. The **Solution** overview appears. If not, select **Solution**.
3. Select the checkbox next to each server to upgrade.
   - **Note**
     Some upgrades require the primary server upgraded before any other servers. When that is the case, repeat this process until both the primary server and any other servers are upgrade.
4. Click on the **Actions** drop down and select **Upgrade**.
5. Set the **Upgrade from** option to ***Primary Server***. Click **OK**.
   a. Read the license warning and if okay to upgrade, click **Yes**.
   b. Read the license agreement for the upgrade and if okay select **Accept** and click **Next**.
6. Click **Close**.
7. The menu shows the progress of the upgrade.
8. The upgrade process typically requires the IP Office Web Manager server to restart, ending the current web browser connection. If this occurs, login to IP Office Web Manager again to check on the status of the upgrade.
9. If necessary, repeat the process to upgrade all the servers.

5.8.2 USB Upgrade

You can use a USB memory key to perform a local upgrade of a Unified Communications Module.

- **! Upgrade Warning**
  Upgrading 68 shows a summary of the supported upgrade paths and methods. Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.
- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.
- **! Password Change Required after Upgrading to 9.1+**
  When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See Logging Into Web Manager 87.

Process Summary

1. **Download the software** 18
   Download the USB software and ISO image.
2. **Backup the applications**
   Backup the Voicemail Pro and one-X Portal for IP Office applications to a location other than the module. Refer to the separate documentation for the applications and their current level of software.
3. **Disable one-X Portal for IP Office Logging**
   You must disable one-X Portal for IP Office logging prior to upgrading. If you do not do this, one-X Portal for IP Office admin is very slow to respond after the upgrade. You can disable one-X Portal for IP Office logging through the one-X Portal for IP Office administrator menus by setting the **Master Logging Level** (**Diagnostics | Logging Configuration**) to ***OFF***.
4. **Prepare the USB upgrade key** 74
   Using the downloaded software, create a bootable USB upgrade key from the downloaded ISO image.
5. **Reboot the module** 75
   Reboot the module from the USB upgrade key and let the module upgrade.
6. **Check operation** 86
   Log in to the server menus.

5.8.2.1 Preparing a USB Upgrade Key

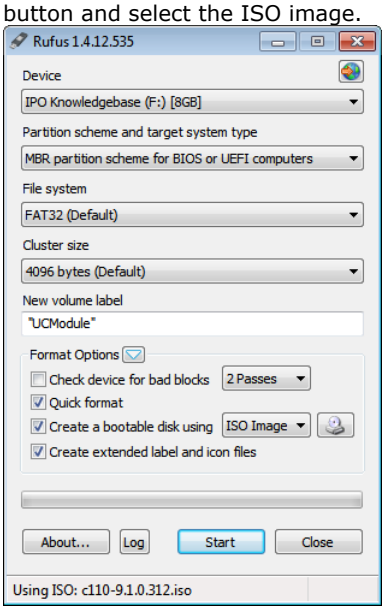
This process uses a downloaded ISO image to create a bootable USB memory key for software upgrading. You can then use the memory key for an upgrade by rebooting from USB 75 or you can transfer its contents to the module for a scheduled web manager upgrade 69.

Prerequisites

- **4GB USB Memory Key**
  Note that this process reformats the memory key and erases all files. The module supports USB and USB2.
- **Rufus software**
  This additional software is downloadable from https://rufus.akeo.ie. You use it to load an ISO image onto a USB memory key from which the server can boot and run that ISO image.
- **Unified Communications Module ISO Image**
  You can download this software from the Avaya support website (http://support.avaya.com).

To create a bootable USB memory key:

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



7. Click **Start**.
8. When done, click **Close**.
7. **! Important: Copy the Upgrade Files**
   You must copy a number of files to a new location on the USB memory key.
   a. Using the file explorer, open the **USB** folder on the USB memory key. This folder contains 4 files, some of which are used for installation and other are used for upgrading.
   b. Select just the files **syslinux.cfg** and **avaya_autoupgrade.conf**. Copy those two files to the top level (root) of the USB memory key, overwriting any existing files with those names.
8. Remove the USB memory key from the PC.

5.8.2.2 Booting from a USB Upgrade Key

Use the following process to reboot from a USB upgrade key.

To upgrade from a USB memory key:

1. Prepare a USB upgrade key 74.
2. For the Unified Communications Module v1, remove the plastic cover from the front of the module. Retain this and reattach it after completing this process.
3. Connect to the IP Office using System Status Application and select the details of the module 25. The page shows the module status. For the Unified Communications Module v2 it also shows the progress of an installation or upgrade.
4. For the Unified Communications Module v1 we also recommend connecting a monitor using an HDMI to HDMI cable or HDMI to DVI cable. Note that the module only activates the video port if it detects a monitor whilst restarting.
5. Insert the USB memory key with the new ISO image file into the module's upper USB port.
6. Shut down the module by pressing the upper button on the module until the LED starts to flash green. The shutdown is complete once all module LEDs are off except an amber flash of the lower LED every 5 seconds.
7. Restart the module by pressing the upper button again and keeping it pressed until the two LEDs change from amber to off.
8. After up to 2 minutes initializing, the module boots using the files on the USB memory key.
   - **Unified Communications Module v2:**
     System Status Application reports the module as *"Initializing"*, then *"USB Booting"* and then *"USB Upgrade/Install"*. Both LEDs flash amber/green. System Status Application displays a progress bar. If after 15 minutes this shows no progress, the most likely cause is that you did not complete the final stage of preparing the USB key, copying files from the USB folder.
   - **Unified Communications Module v1:**
     System Status Application reports the module as *"Running"*. The upper LEDs alternate between green and off.
9. The installation process can take up to 80 minutes. After the software installation completes, the module restarts. During the restart, if necessary the module's firmware upgrades. The restart, including firmware upgrade, takes approximately 25 minutes. During this, for the Unified Communications Module v2, System Status Application displays *"Applications starting"*.
   - **! WARNING:** It is important that you allow this stage to complete even if no upgrade activity appears to be taking place. Wait at least 25 minutes.
10. After this the LEDs indicate the module's status as follows:
    - **Lower status LED shows only regular IP Office heartbeat flashes:**
      This indicates that the mode automatically shutdown after a firmware upgrade. Restart the module by pressing the top button or using System Status Application 25.
    - **Lower status LED green except for regular IP Office heartbeat flashes:**
      This indicates that the module restarted without needing a firmware upgrade.
11. Login to the module via its IP Office Web Manager menus 87 and check the status of the services.
12. Remove the USB memory key.
13. Remove any monitor connection.
14. For the Unified Communications Module v1, refit the plastic cover removed at the start of the process.

5.9 Starting/Stopping Application Services

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

5.9.1 Starting a Service

To start a service:

1. Login 59 to the server's web configuration menus.
2. Select **System**. The menu lists the services and their status.
3. To start a particular service click on the **Start** button next to the service. To start all the services that are not currently running, click on the **Start All** button.

5.9.2 Stopping a Service

To stop a service:

1. Login 59 to the server's web configuration menus.
2. Select **System**. The menu lists the services and their status.
3. To start a particular service click on the **Stop** button next to the service. To stop all the services that are currently running, click on the **Stop All** button.
4. The service's status changes to ***Stopping***. If it remains in this state too long, you can force the service to stop by clicking on **Force Stop**.

5.9.3 Setting a Service to Auto Start

To set a service to auto start:

1. Login 59 to the server's web configuration menus.
2. Select **System**. The menu lists the services and their status.
3. Use the **Auto Start** check box to indicate whether a service should automatically start when the server starts.

5.10 Changing the Linux Passwords

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

To change the server's Linux account passwords:

1. Login 59 to the server's web configuration menus.
2. Select **Settings** and click on the **System** tab.
3. Use the **Change root Password** section to set the new password for the root account. The new password must conform to the password rules settings 105.
4. Use the **Change Local Linux Account Password** to set the new password for the ***Administrator*** account. Note that this is different from the ***Administrator*** account used for access to IP Office services. The new password must conform to the password rules settings 105.
5. Click **Save**.

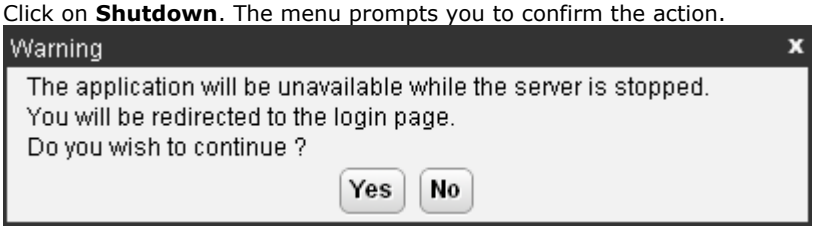
5.11 Shutting Down the Server

Use this process when it is necessary to switch off the Unified Communications Module for any period. For the Unified Communications Module, you can shutdown or restart the module using its buttons 67 or System Status Application 25, this process uses the modules web configuration menus.

- **! WARNING**
  If the shutdown is to remove the module from the system, you must also shutdown the IP Office system 22.

To shutdown the server:

1. Login 59 to the server's web configuration menus.
2. After logging in, select the **System** 91 page.
3. Click on **Shutdown**. The menu prompts you to confirm the action.



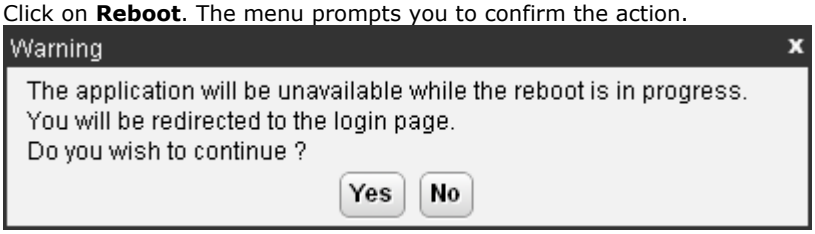
4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 2 minutes, the server shuts down.

5.12 Rebooting the Server

Rebooting the server stops all currently running services and then stops and restarts the server. Only those application services set to **Auto Start** 76 automatically restart after the reboot.

To reboot the server:

1. Login 59 to the server's web configuration menus.
2. After logging in, select the **System** 91 page.
3. Click on **Reboot**. The menu prompts you to confirm the action.



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

5.13 Date and Time Settings

You can change the date and time settings used by the server through the server's web configuration pages. The **System** 91 menu shows the server's current date and time.

By default the Unified Communications Module is set to use NTP with the NTP server address set to 169.254.0.1 (the IP Office system).

To change the server date and time settings:

1. Login 59 to the server's web configuration menus.
2. Select **Settings**.
3. Select **System**.
4. Select the **Date Time** section.
    - **Date**
      For a server not using NTP, this field shows the server's current date and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
    - **Time**
      For a server not using NTP, this field shows the server's current UTC time and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
    - **Timezone**
      In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field determines the appropriate offset applied to the UTC time above. Note that changing the timezone can cause a *"Session expired"* message to appear in the browser in which case you need to login again.
    - **Enable Network Time Protocol**
      When selected, the server obtains the current date and time from the NTP servers listed in the **NTP Servers** list below. It then uses that date and time and makes regular NTP requests for updates.
        - **NTP Servers**
          With **Enable Network Time Protocol** selected, use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome. However, it is your responsibility to comply with the usage policy of the chosen server. Choose several unrelated NTP servers in case one of the servers becomes unreachable or its clock unreliable. The server uses the responses it receives from each NTP server to determine reliability.
            - The IP Office system can also use NTP to obtain its system time.
            - The default time setting for the Unified Communications Module is to use NTP with the server address set to 169.254.0.1 (the IP Office system). When this is set, you must configure the IP Office to get its time from an external SNTP server or set its time manually.
        - **Synchronize system clock before starting service**
          Use this option to synchronize the system clock to an NTP time server before starting other services. Do not use this option if the time server cannot be reliably reached. Waiting for synchronization to occur may block use of the system until a timeout has passed.
        - **Use local time source**
          When not selected, external NTP takes priority over the internal system clock. If selected, the local system clock is used as the time source. Only use this option if system clock is synchronized with another reliable source, for example a radio controlled clock device.
5. Click **Save**.

5.14 Creating Administrator Accounts

The IP Office system's security configuration controls access to the web control menus. For a Unified Communications Module this refers to the security settings of the **Management Services** service run by the module, not those of the IP Office into which the module is installed.

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

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

To view and adjust rights group settings:

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

To change a service user's rights group memberships:

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

5.15 Setting the Menu Inactivity Timeout

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

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

To change the menu inactivity timeout:

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

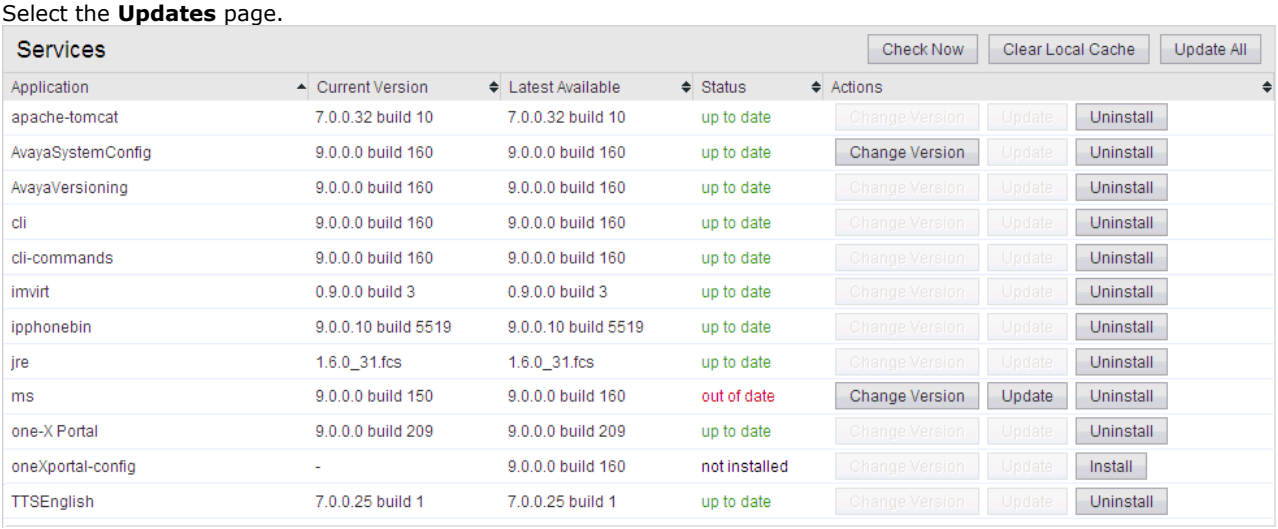
5.16 Uninstalling an Application

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

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

To uninstall an application:

1. Login 59 to the server's web configuration menus.
2. Select the **Updates** page.



3. The **Services** section displays the current version and latest available version of each application service.
4. To uninstall a service, click on **Uninstall**.
   - If there are installation files for the application in the application file repository 81, the button becomes an **Install** button.
   - If there are no installation files for the application in the file repository, the menu no longer list the application.

5.17 Setting Up File Repositories

The **Updates** 96 and **Web Client** 106 menus use files stored in the configured file repositories. A repository is a set of files uploaded to the server or the URL of a remote HTTP server folder.

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

5.17.1 Source Files

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

- **! Upgrade Warning**
  Upgrading 68 shows a summary of the supported upgrade paths and methods. Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path and for any additional information that may not be in this manual.
- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading. You can do this using the Web Manager menus.
- **! Password Change Required after Upgrading to 9.1+**
  When upgrading from a pre-Release 9.1 system, on first login to Web Manager, the server prompts you to change the default passwords in the same way as for a new installation. See Logging Into Web Manager 87.

		DVD/.ISO Folder	Description
Applications	**Voicemail Pro**	\avaya\vmpro	• These are files used by the IP Office applications and services provided by the server.
	one-X Portal for IP Office	\avaya\oneX	
Downloads		\avaya\thick_clients	• These are files used to provide the downloads from the **App Center** 106 menu.
Operating System		\Packages	• These are files used by the Linux operating system and its services.

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

5.17.2 Setting the Repository Locations

The Unified Communications Module can use either remote or local software repositories to store software update files. The server has separate repositories for operating system updates, IP Office application installation files and Windows client files. The **Updates** 96 and **AppCenter** 106 menus use the files present in the appropriate repository.

- **Repository**
  If not using the **Local** option, this field sets the URL of a remote HTTP file repository 83. Note that you cannot use the same URL for more than one repository.
- **Local**
  This checkbox sets whether the file repository used is local (files stored on the Unified Communications Module) or remote (a folder on a HTTP web server specified in the Repository field).
- **File / Browse / Add**
  With **Local** selected, you can use this field and adjacent buttons to browse for a specific update file. After selecting the file, click **Add** to upload the file to the server's file store.

5.17.3 Uploading Local Files

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

- **Application**
  These are files used by the IP Office applications and services provided by the server.
- **Downloads**
  These are files used to provide the downloads from the **App Center** 106 menu.
- **Operating System**
  These are files used by the Linux operating system and its services.

5.17.3.1 Uploading Application Files

This method uploads the RPM file for an application onto the server. You can then use the file to update the application. The alternative is to use files loaded into a remote software repository 83.

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

To upload application files onto the server:

1. Login 59 to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Applications**.
4. Click on the **Browse** button and browse to the location of the file 81 that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

5.17.3.2 Uploading Operating System Files

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

To upload operating system files:

1. Login 59 to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Operating System**.
4. Click on the **Browse** button and browse to the location of the file 81 that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

5.17.3.3 Uploading Windows Client Files

This method uploads the .rpm file for an application onto the Unified Communications Module.

To upload Windows client files:

1. Login 59 to the server's web configuration menus.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Select the **Local** checkbox for **Downloads**.
4. Click on the **Browse** button and browse to the location of the file 81 that you want to load and select the file. The **File** field now lists the file name.
5. Click **Add**. The server starts uploading the file.
6. Repeat the process for any other files.

5.17.4 Creating Remote Software Repositories

Alternatively to using local files uploaded to the server for updates, the server can use files stored in folders on a remote HTTP server.

To create an application update repository:

1. Create a folder on the web server for the remote file repository. For example a folder called ***Applications***.
2. The folder directory must be browseable. For example, on a Microsoft Internet Information Services server, right-click on the folder, select **Properties** and select the **Directory Browse** option.
3. Copy the .rpm files from their source 81 into the folder.
4. From another PC, test that you can browse to the URL of the folder and that the list of files in the folder appears.
5. Login to the Unified Communications Module web configuration pages.
6. Select **Settings** and then **General**.
7. Uncheck the **Local** checkbox for **Applications**. Enter the URL of the HTTP server folder into the preceding field.
8. Click **Save**.
9. Select **Updates**.
10. If the server is able to access the HTTP folder, the details of the versions available will now reflect those available in that folder. The message ***repository error*** indicates that the Unified Communications Module was not able to connect to the folder or not able to list the files in the folder.

To create a Windows client repository:

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

To create an operating system repository:

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

5.18 Downloading Log Files

The server collects and store log events. These are viewable through the **Logs** 93 sub-menus. The **Download** 95 sub-menu allows the archiving and download of the log files.

To create archive files:

1. Login 59 to the server's web configuration menus.
2. Select **Logs**.
3. Select **Download**.
4. Click on the **Create Archive** button. The button remains greyed out while the archive creation is running:
   - For debug files, the archive contains any debug records since the last creation of a debug archive.
   - For log files, the server creates a separate archive file for each service. The archive file contains all log files available on the server.

To download archive files:

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

To delete archive files:

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

5.19 SSH File Transfers

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

To start SSH file transfers:

1. Start your SFTP or SSH file application and connect to the Unified Communications Module PC. The exact method depends on the application 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 ***Administrator***.
      - The **Protocol** is ***SFTP/SSH***.
      - The **Port** is ***22***.

   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 Linux Administrator account password.
2. The default folder displayed after logging in is **/home/Administrator**.

Chapter 6.
Web Manager

6. Web Manager

The primary method for server management is through its Web Manager menus. For details of using Web Manager refer to separate IP Office Web Manager documentation 10.

Through Web Manager you can perform the following actions. Note that access to some functions depends on the security rights of the account used to login to Web Manager 87.

- **Backup Applications**
  You can configure backups of the server applications to a remote server. These backups can use a variety of protocols (HTTP, HTTPS, FTP, SFTP, SCP). In addition to selecting the application services included in a backup, you can schedule backups.
- **Restore Previous Backups**
  You can use control the restoration of a previous backups.
- **Upgrade the Server**
  You can use the menus to upload a new ISO image and then use that image file to upgrade the server.
- **Launch Other Applications**
  You can launch the other administrator applications used by the server or the applications it runs:
  - **IP Office Manager**
    If installed on the user PC, Web Manager can launch IP Office Manager.
  - **Voicemail Pro Client**
    If installed on the user PC, Web Manager can launch the voicemail client to allow configuration of the voicemail server and editing of voicemail call flows.
  - **one-X Portal for IP Office**
    You can access the administration menus for the one-X Portal for IP Office service from within Web Manager.
  - **System Status Application**
    You can start System Status Application without needing to install it on the user PC.
  - **Web Control**
    You can access the server's web control menus through Web Manager.
- **Configure Voicemail Server Preferences**
  For server's running the Voicemail Pro service, you can set the voicemail server preferences using Web Manager.
- **Security User**
  Web Manager can configure the security privileges of IP Office service user accounts.
- **File Management**
  Web Manager can upload files to the server. This includes the uploading of custom voicemail prompts.

6.1 Logging In to Web Manager

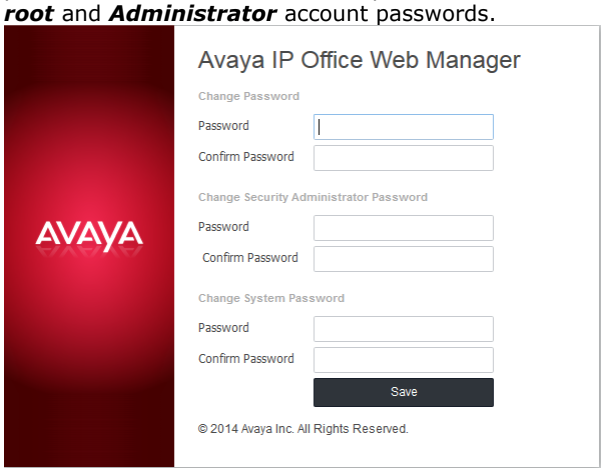
Avaya supports the following browsers for web access to the server menus:

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

To access Web Manager:

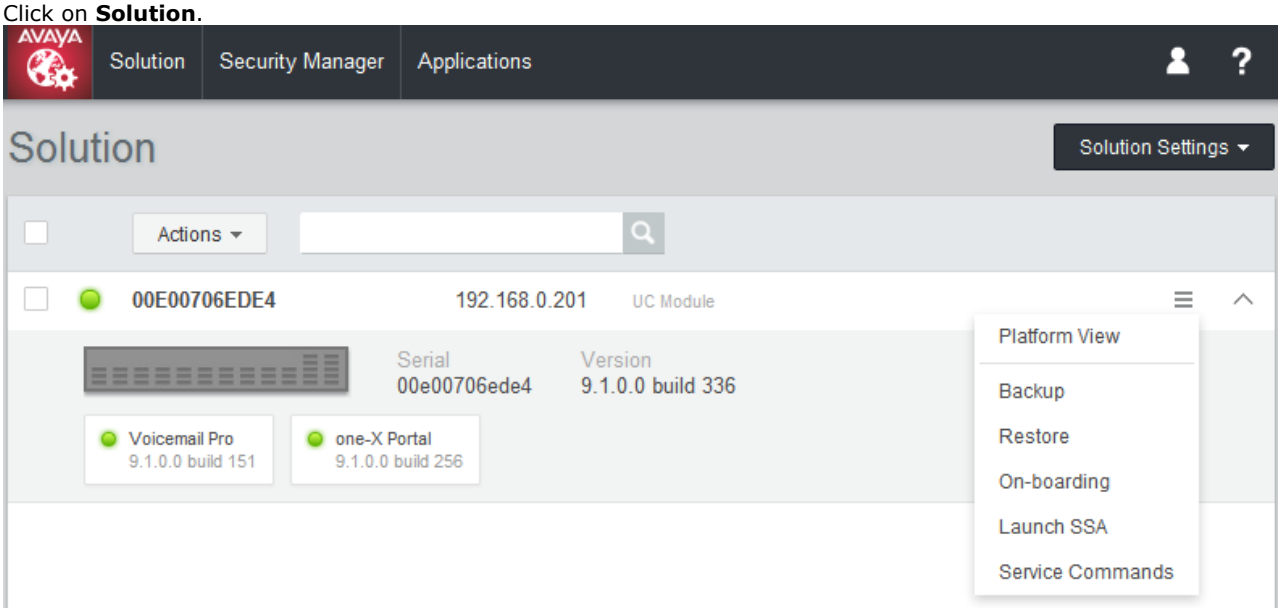
1. Log in to IP Office Web Manager.
   a. Enter **https://** followed by the module's IP address and then 7070. Alternatively, enter **https://** followed by the IP Office system address and from the menu click **IP Office Web Manager on UCM**.

   b. Enter the user name and password.
   c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. Note that this does not change the Linux ***root*** and ***Administrator*** account passwords.

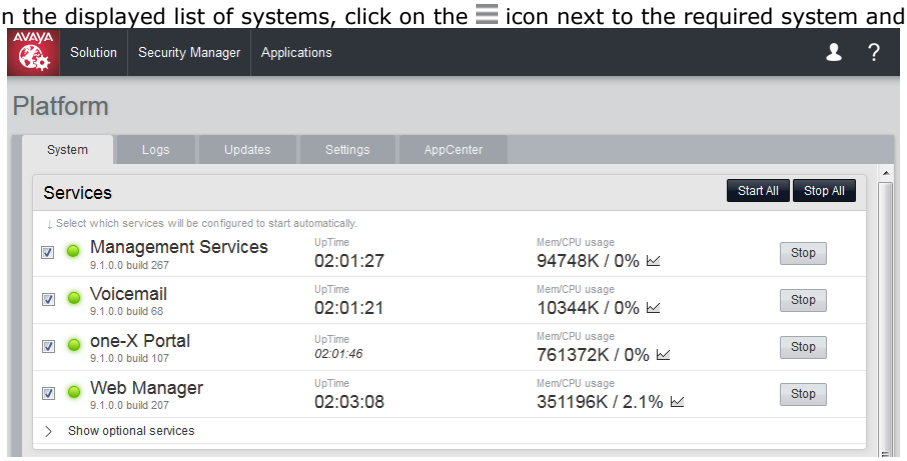


   - ***Change Password***
     This sets the password for the **Administrator** account of the Management Services service run on the Unified Communications Module. With **Referred Authentication** 12 enabled (the default) this is also the default account used for Voicemail Pro, one-X Portal for IP Office and Web Manager administrator access.
   - ***Change Security Administrator Password***
     This sets the password for the Management Services security administrator account.
   - ***Change System Password***
     This sets the **System** password for the Management Services.

2. Click on **Solution**.



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



Chapter 7.

Web Control/Platform View Menus

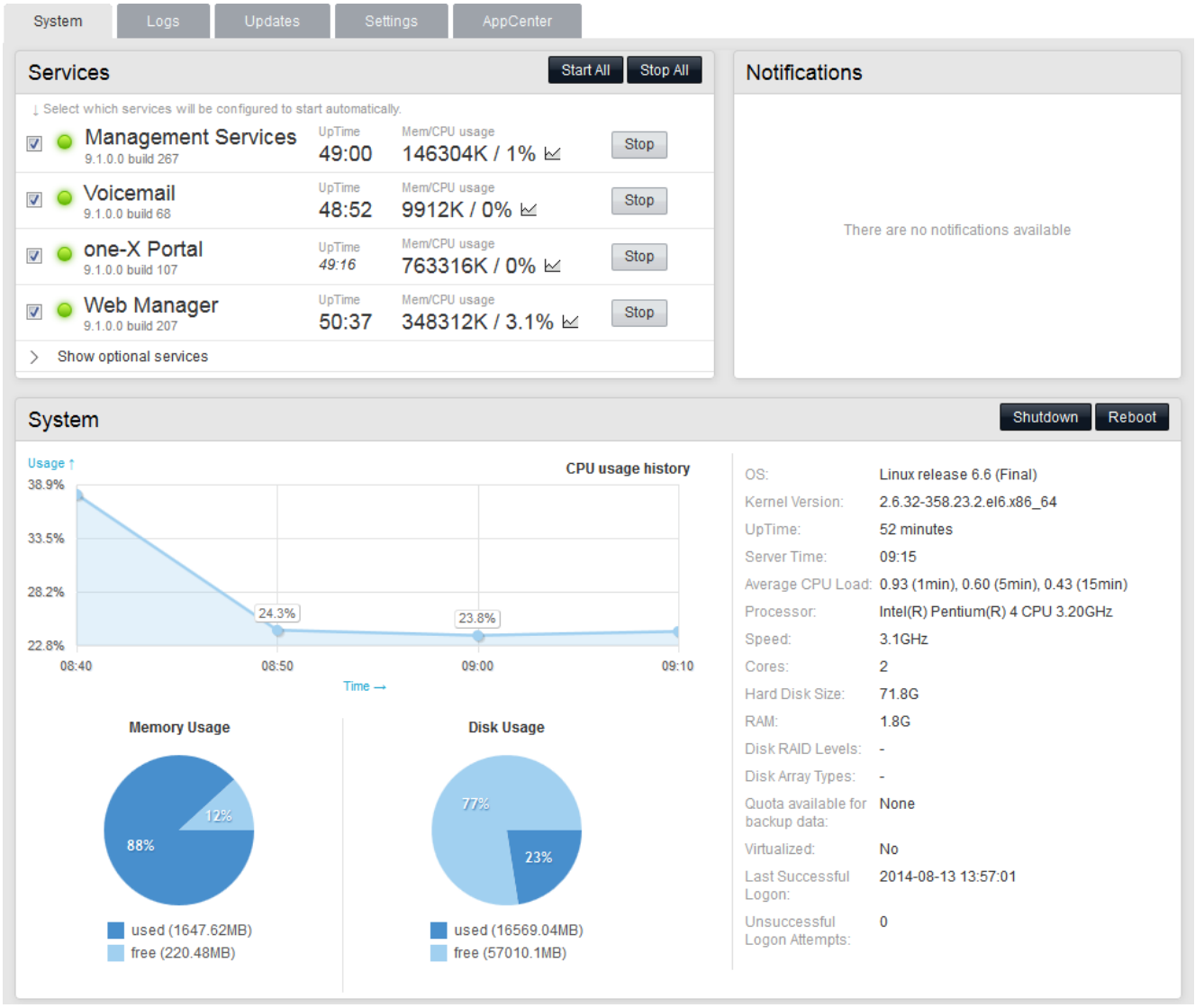
7. Web Control/Platform View Menus

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

- **System** 91
  This menu gives an overview of the status of the applications hosted on the server.
- **Logs** 94
  This menu has sub-menus for viewing and managing log records and log files.
  - **Debug Logs** 94
    View the current log files for the server and the application services hosted by the server.
  - **Syslog Event Viewer** 95
    View Syslog log records received and or generated by the server.
  - **Download** 95
    Create and download archive files of existing log records.
- **Updates** 96
  Display the versions of applications and components installed and the alternate versions available.
- **Settings**
  This menu has sub-menus for various areas of server configuration and operation.
  - **General** 99
    General server settings such as the locations of software update repositories.
  - **System** 103
    View and manage the server setting for date, time and IP address details.
- **AppCenter** 106
  You can download the installation packages for applications such as the Voicemail Pro client application from this page.

7.1 System

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



- **Services**
  This table lists the services supported by the server. In addition to showing the status of the service, it also contains buttons to start/stop each service. Clicking on the link for **Mem/CPU usage** will display a summary graph of CPU and memory usage by the application.
  - **Management Services**
    This is a shell version of IP Office that allows basic configuration of services such as remote SSL VPN connections for server support. It also controls security settings for access to the server's menus. It does not support call features such as users, extensions or trunks.
  - **one-X Portal for IP Office**
    This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely using web browser access. Each user who wants to use one-X Portal for IP Office requires a license 12.
  - **Voicemail Pro**
    This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail.
  - **IP Office Web Manager**
    You can configure and manage the server via browser access to the Web Manager menus. The menus also allow the launching of other clients used to configure and monitor the services run by the server.

- **Optional Services**
  Currently the Unified Communications Module does not support any optional services.

- **Notifications**
  This table shows important messages.

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

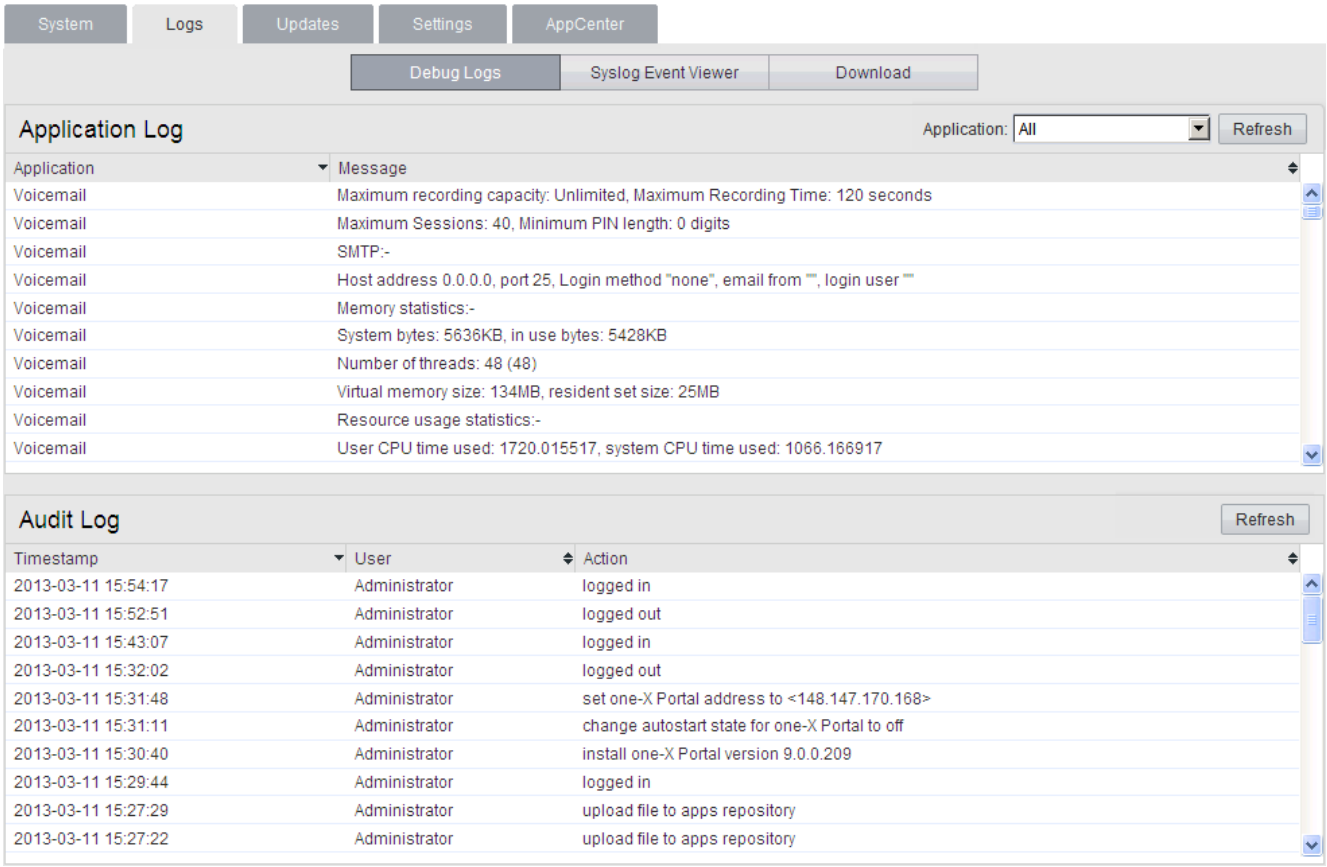
    - **OS/Kernel:**
      The overall version of the Linux operating system installed on the server and the version of the operating system kernel.
    - **Up Time:**
      This field shows the system running time since the last server start.
    - **Server Time:**
      This field shows the current time on the server.
    - **Average CPU Load:**
      This field shows the average CPU load (percentage use) for the preceding minute, 5 minute and 15 minute periods.
    - **Speed**:
      Indicates the processor speed.
    - **Cores:**
      Indicates the number of processor cores.
    - **Hard Disk Size:**
      Indicates the hard disk size.
    - **RAM:**
      Indicates the amount of RAM memory.
    - **Disk RAID Levels:**
      Indicates the RAID type, if any.
    - **Disk Array Types:**
      Indicates the type of disk array used for RAID.
    - **Quota available for backup data:**
      Displays the amount of space reserved for local backups if **Enable HTTP file store for backup/restore** 105 is enabled.
    - **Virtualized:**
      Indicates whether the server is running as a virtualized session.
    - **Last Successful Logon:**
      This field shows the date and time of the last successful logon, including the current logon.
    - **Unsuccessful Logon Attempts:**
      This field shows a count of unsuccessful logon attempts.

  - **Shutdown**
    Selecting this button starts a process that stops all services and then shuts down the server.
  - **Reboot**
    Selecting this button starts a process that stops all services and then stops and restart the server.

7.2 Logs

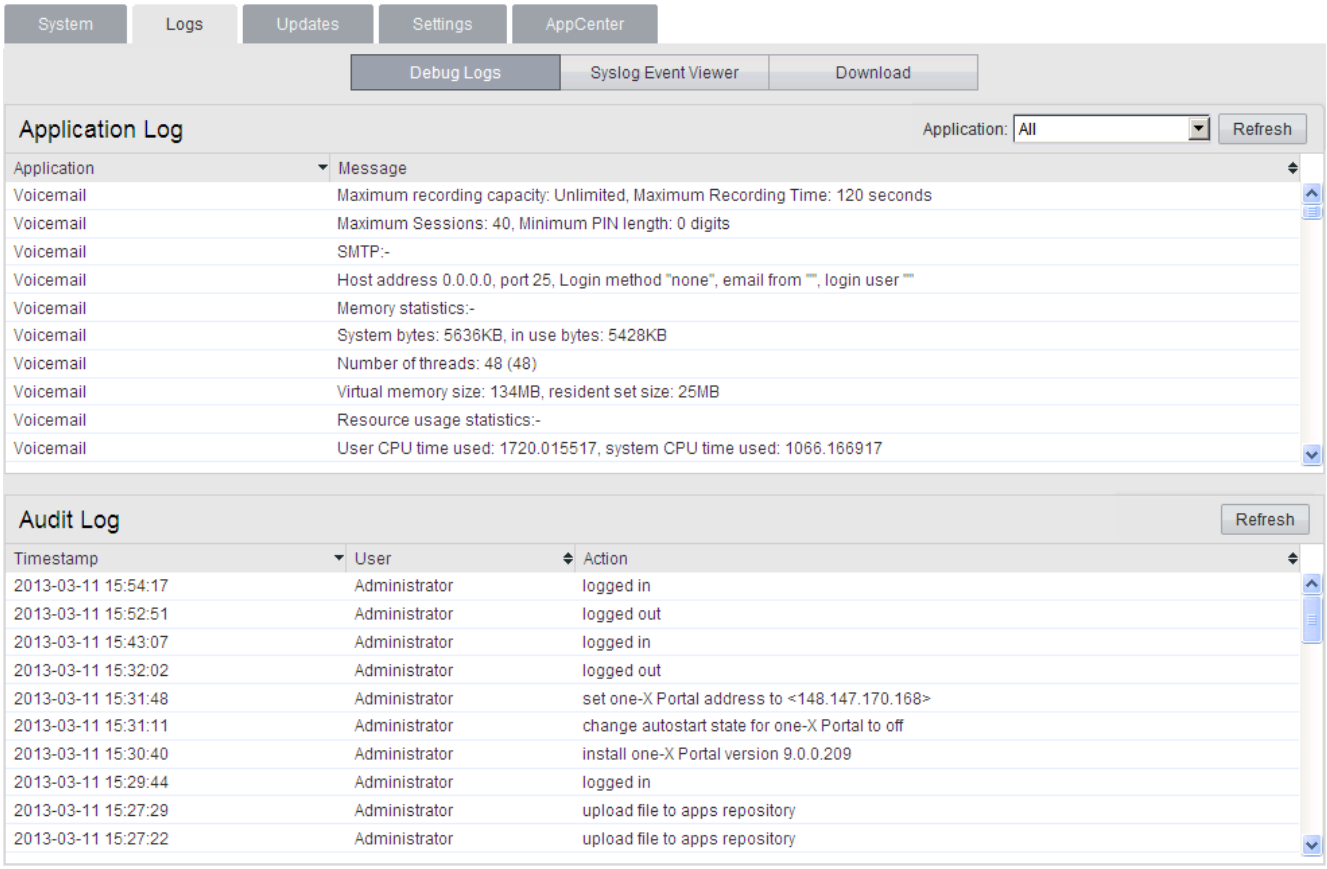
This menu contains the following sub-menus:

- **Debug Logs** 94
  View the current log files for the server and the application services hosted by the server.
- **Syslog Event Viewer** 95
  View Syslog log records received and or generated by the server.
- **Download** 95
  Create and download archive files of existing log records.



7.2.1 Debug Logs

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

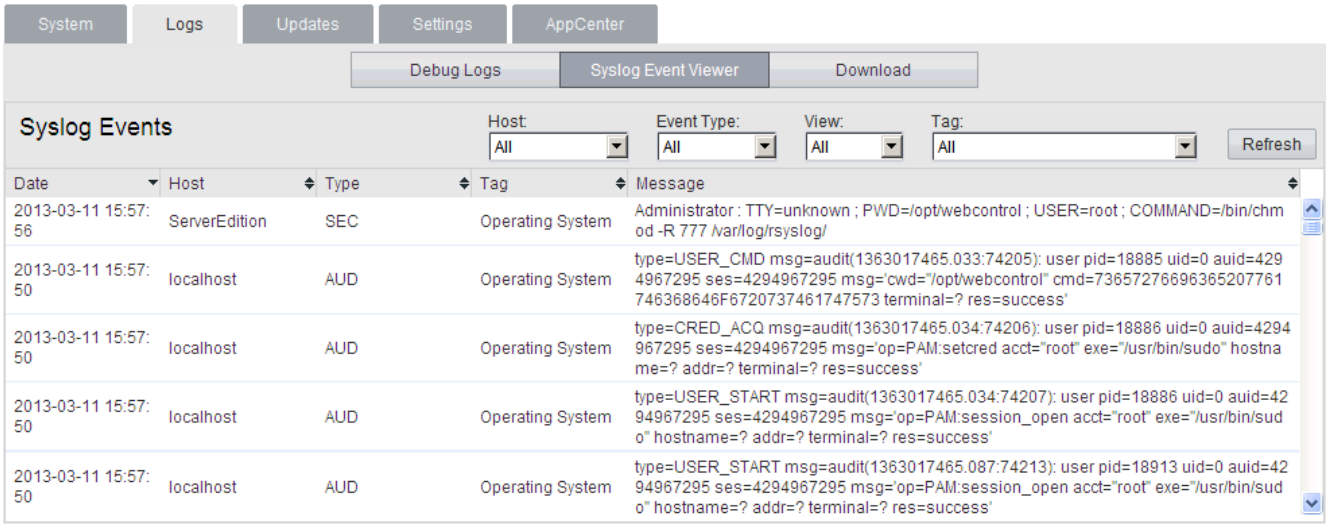


- **Application Log**
  This table lists the last 1000 log records for a selected server application. The **Application** drop-down selects the records shown. Clicking on a column header sorts the records using that column.For Voicemail Pro the level of log information output is set through the **Debug** section of the **Settings | General** 101 menu. For one-X Portal for IP Office the level of log information output is set through the applications own administration menus, not through the Unified Communications Module menus.
- **Audit Log**
  This table lists the actions performed by users logged in through the Unified Communications Module's web browser interface. Clicking on a column header sorts the records using that column.

7.2.2 Syslog Event Viewer

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

You can use the Settings | General 106 menu to configure the sending and receiving of Syslog records to and from other servers. You can also configure how long the server keeps different types of records and how many records it keeps.

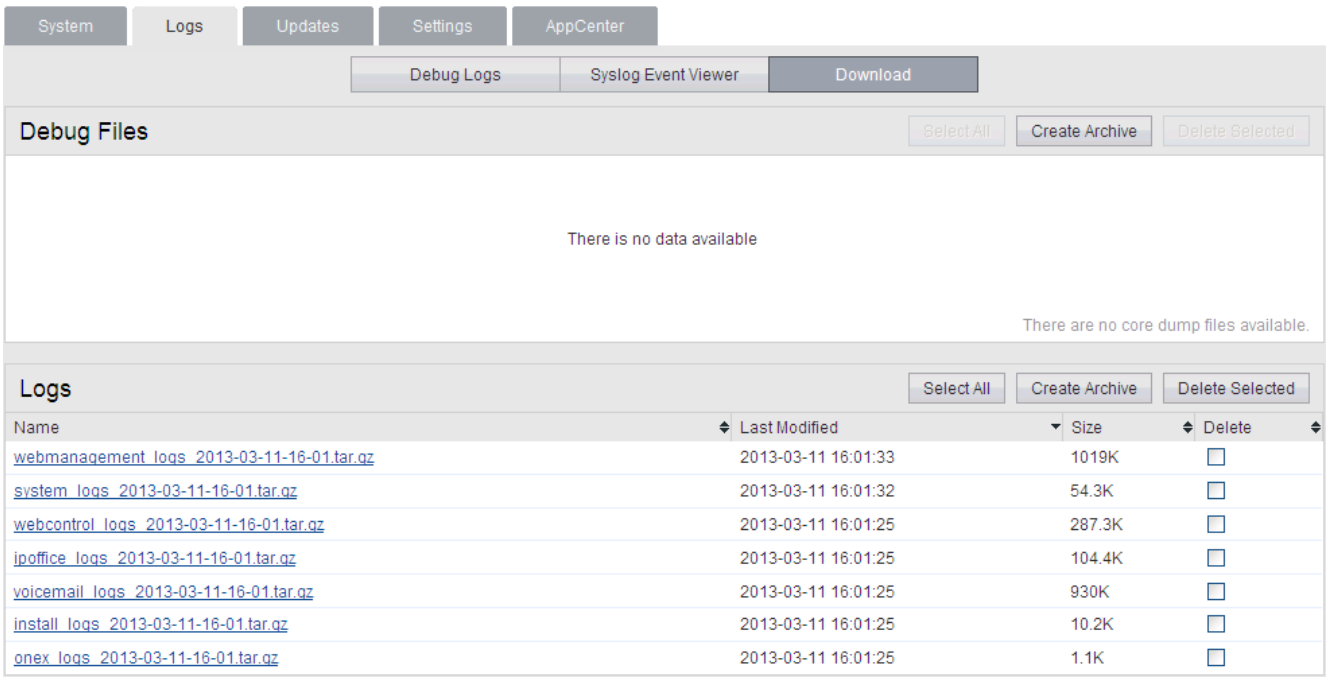


- The **Refresh** button is used to update the table of records shown using the settings in the drop-down filters (**Host** , **Event Type**, **View** and **Tag**). Note however that the options within the filters are set when the menu is opened. To update the menu options, selects another menu and then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

7.2.3 Download

You can access this menu by selecting **Logs** and then clicking the **Download** tab. You can use the menu to create and download archives files 84. For support issues, Avaya will require the archive files downloaded from the server.

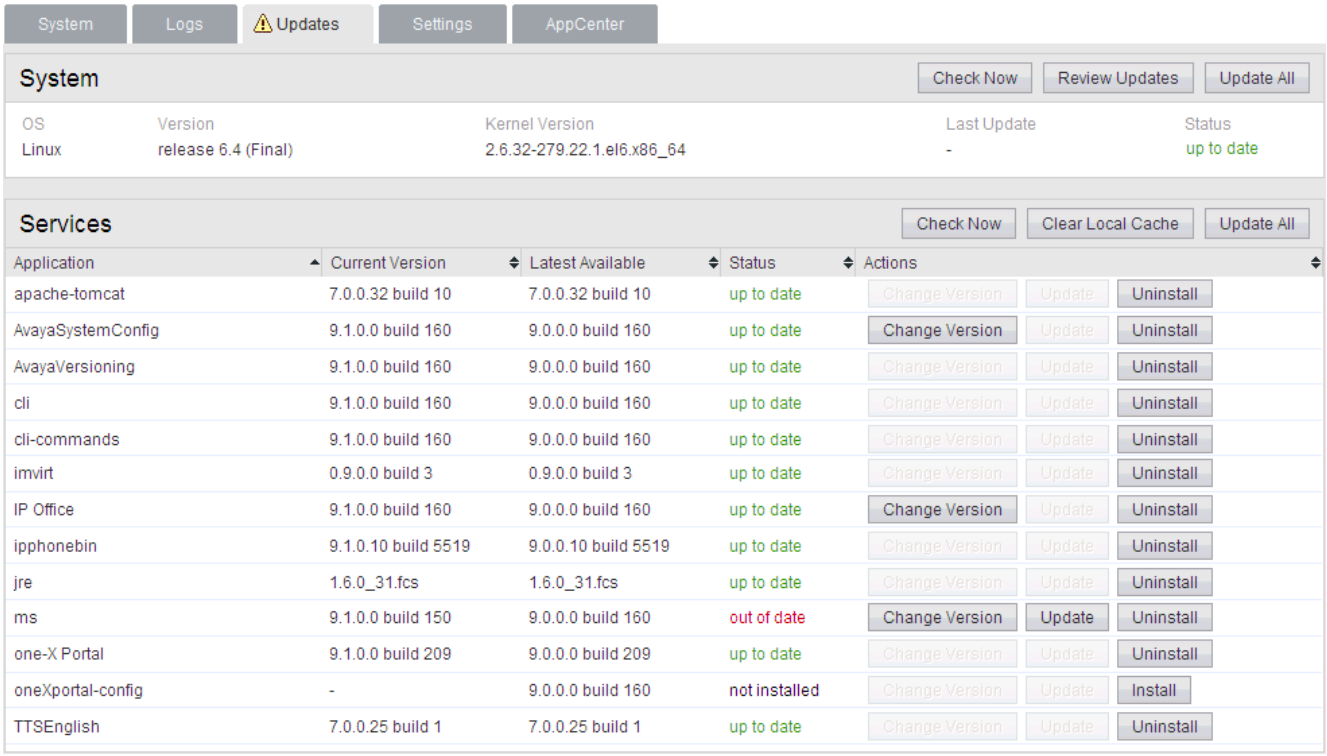
The server compresses the log files into a ***.tar.gz*** format file. You can then download the file by clicking on the link.



7.3 Updates

This menu displays the different versions of server operating system files and application files available in the file repositories. The file repository locations are configured through the Settings | General 99 page.

- **Important**
  These menus should only be used for updates when directed by Avaya. The recommend method for updating is through the use of full .ISO file. See Upgrading 68.

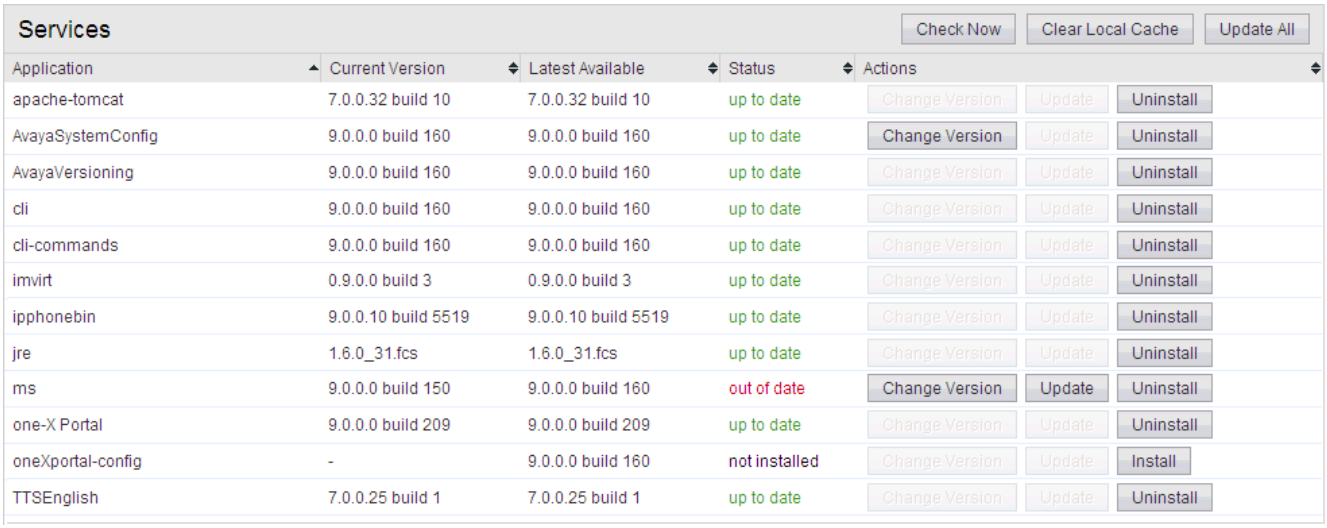


The menu consists of 2 sections:

- **Services 97**
  This section displays the current version of application files. It also shows whether update files are available.
- **System 98**
  This section displays the current version of the operating system and whether update files are available.

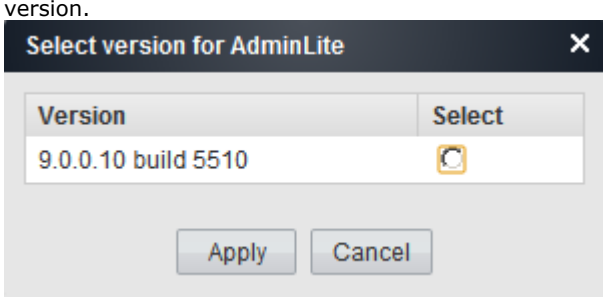
7.3.1 Services

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



- 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 81. This also affects the availability of the **Install** button option.

- **Change Version**
  Clicking on this button shows the update files available for the application in the server's file repository 81 with the current version selected. Selecting another version and clicking **Apply** upgrades or downgrades to that version.



- **Update**
  Clicking on this button starts an update of the related application to the latest available version in the application file repository 81.

- **Uninstall**
  Clicking on this button uninstalls the selected application.
  - If there are installation files for the application in the application file repository 81, the button becomes an **Install** button.
  - If there are no installation files for the application in the file repository, the menu no longer list the application.

- **Install**
  This button appears for uninstalled applications if the server has files for the application the application file repository.

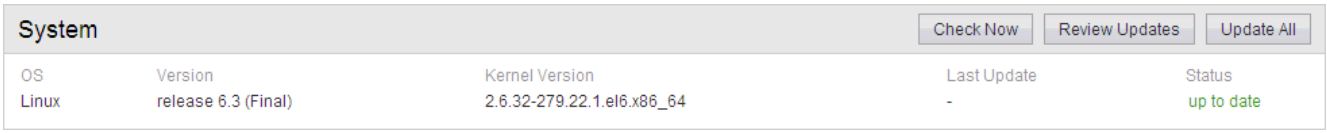
- **Check Now**
  Clicking this button makes the Unified Communications Module recheck the version of update files available in the file repository. Normally it does this automatically when the **Updates** page is loaded.

- **Clear Local Cache**
  Clicking this button removes older update installation files and other material that may accumulate on the server over time.

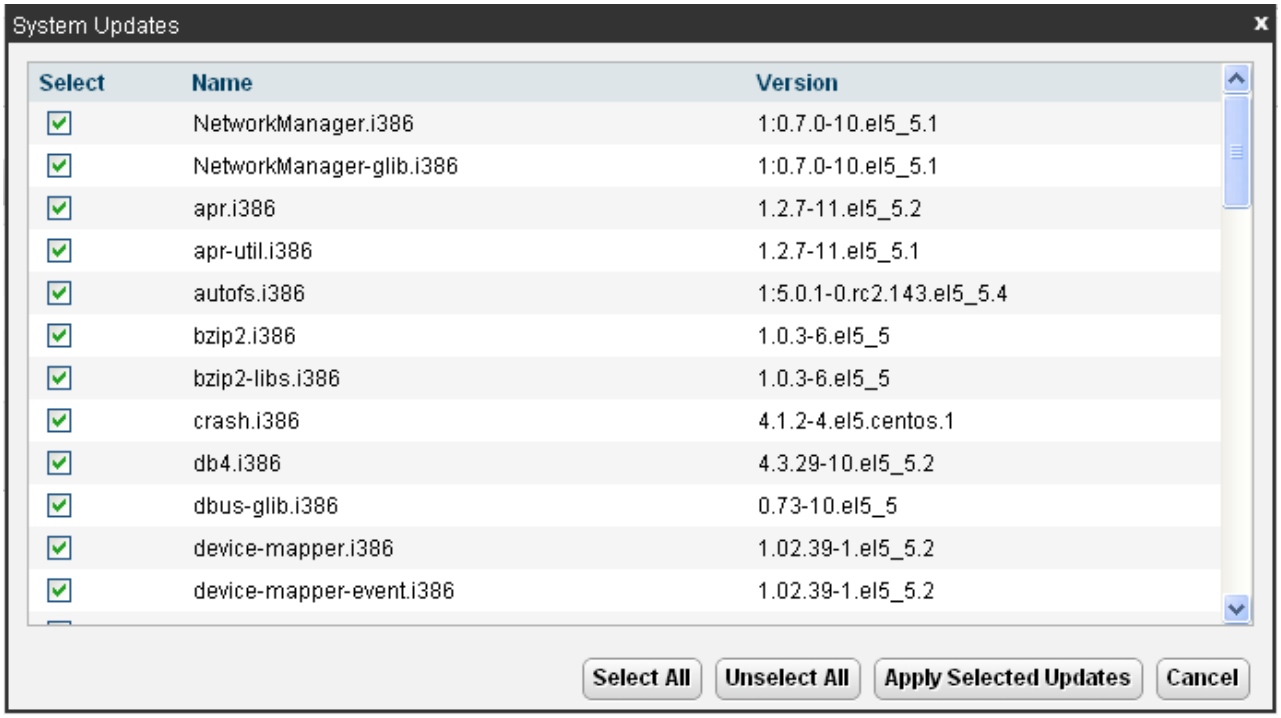
- **Update All**
  Clicking this button upgrade those applications that support upgrading without being uninstalled (see above) to the latest versions available in the application file repository.

7.3.2 System

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



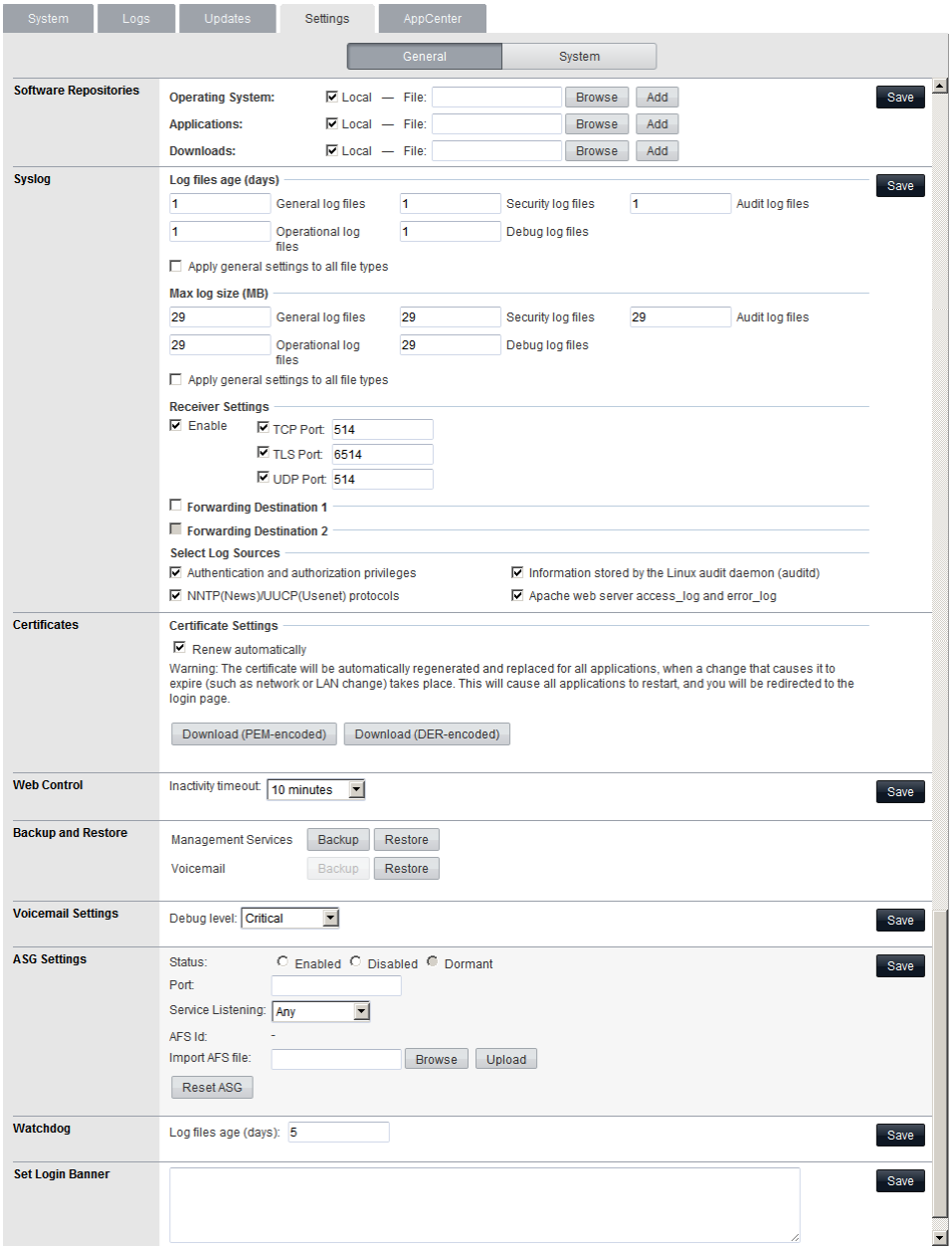
- **Check Now**
  Clicking this button makes the Unified Communications Module recheck the version of update files available in the file repository. Normally it does this automatically when the **Updates** page is loaded.
- **Review updates**
  Clicking this button will display a list of the available update files. This list allows selection of which updates you want to install.



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

7.4 Settings: General

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



7.4.1 Software Repositories

The Unified Communications Module can use either remote or local software repositories to store software update files. The server has separate repositories for operating system updates, IP Office application installation files and Windows client files. The **Updates** 96 and **AppCenter** 106 menus use the files present in the appropriate repository.

- **Repository**
  If not using the **Local** option, this field sets the URL of a remote HTTP file repository 83. Note that you cannot use the same URL for more than one repository.
- **Local**
  This checkbox sets whether the file repository used is local (files stored on the Unified Communications Module) or remote (a folder on a HTTP web server specified in the Repository field).
- **File / Browse / Add**
  With **Local** selected, you can use this field and adjacent buttons to browse for a specific update file. After selecting the file, click **Add** to upload the file to the server's file store.

7.4.2 Syslog

These settings control the receiving and the forwarding of Syslog records by the server.

- **Log files age (days)**
  Set the number of days the server retains each type of record before automatically deleting it. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. This setting is not applied to IP Office System Monitor records sent to Syslog.
  - **Apply general settings to all file types**
    If selected, the setting for General log files is applied to all file types.
- **Max log size (MB)**
  Set the maximum total size of each type of records the server retains before automatically deleting the oldest records. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. This setting is not applied to IP Office System Monitor records sent to Syslog.
  - **Apply general settings to all file types**
    If selected, the setting for **General log files** is applied to all file types.
- **Receiver Settings**
  These settings control if and how the server can receive Syslog records.
  - **Enable**
    If selected, the server can receive Syslog records using the port configured below.
  - **TCP Port**
    Sets the port number used for receiving Syslog records using ***TCP***.
  - **TLS Port**
    Sets the port number used for receiving Syslog records using ***TLS***.
  - **UDP Port**
    Sets the port number used for receiving Syslog records using ***UDP***.
- **Forward Destination 1**
  These settings control whether the server forwards copies of Syslog records it receives to another server.
  - **Enable**
    If selected, the server will forward copies of the Syslog records it receives.
  - **IP Address: Port**
    Sets the address of the destination server and the destination port for the forwarded records.
  - **Protocol**
    Set the protocol, ***UDP***, ***TLS*** or ***TCP***, for the forwarding.
- **Forward Destination 2**
  These settings control whether the server forwards copies of the Syslog records it receives to a second server. The settings are the same as for the first forwarding destination.
- **Select Log Sources**
  These options allow selection of which server reporting to include in the Syslog reports. The available options are:
  - **Authentication and authorization privileges**
  - **Information stored by the Linux audit daemon (auditd)**
  - **NNTP(News)/UUCP(Usenet) protocols**
  - **Apache web server access_log and error_log**

7.4.3 Certificates

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

- **Renew automatically**
  If selected, the server automatically generates a new security certificate following any major change such as changes to its LAN settings. The server automatically applies the new certificate to the application services run on the server.
- **Download (PEM-encoded)**
  Download the certificate as a PEM file. You can then apply the certificate to any remote device that needs to establish secure encrypted connection with the server.
- **Download (DER-encoded)**
  Download the certificate as a CRT file. You can then the certificate to any remote device that needs to establish secure encrypted connection with the server.

7.4.4 Web Control

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

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

7.4.5 Backup and Restore

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

- **Management Services**
  These control provides options to backup/restore the configuration settings of the Management Services application running on the server.
- **Voicemail Pro Server**
  For the Voicemail Pro server, these controls can only be used to restore an existing backup. Using the Voicemail Pro client, you can configure the voicemail server to perform regular (daily, weekly and or monthly) automatic backups of selected options including messages and prompts. You can also use the Voicemail Pro client to perform an immediate backup.
  - Selecting the **Restore** button displays the backups available in the backup folder (*/opt/vmpro/Backup/Scheduled*). The backup name includes the date and time and whether the backup was a manual or scheduled backup. Selecting a backup and clicking **OK** starts the restoration process. For details, refer to the Voicemail Pro client help.
  - **Warning: Close the Voicemail Pro client before restoring**
    The restoration process requires the voicemail service to shutdown and restart. This does not occur if any Voicemail Pro client is connected to the service during the restore and leads to an incorrect restoration of files.
- **one-X Portal for IP Office**
  one-X Portal for IP Office has its own method of backup and restore. You can access this through the one-X Portal for IP Office web client administration menus.

7.4.6 Voicemail Settings

This setting sets the debug logging level used by the Voicemail Pro application if running. For the one-X Portal for IP Office application, the logging level is set through the applications own web administration menus. Log files are retrievable through the **Logs | Download** 95 menu.

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

7.4.7 ASG Settings

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

- **Status**
  Set the status of server listening for connections from the security gateway.
  - ***Active***
    This setting enables listening for connections from an ASG server. The server automatically selects this state when you upload an AFS file.
  - ***Disabled***
    This setting cancels any listening for connections from an ASG server.
  - ***Dormant***
    This is the default state before uploading any AFS file.
- **Port**
  Set the port on which the server listens for connections from the security gateway. The default is ***2222***. For Avaya support do not change this value from the default.
- **Service Listening**
  Select whether the server listens on any connection (***Any***) or just on SSLVPN tunnels (***Any Tunnel***).
  - ***Any***
    If selected, the server listens on any connection. This setting is deprecated as it is less secure than ***Any Tunnel***.

- ***Any Tunnel***
  If selected, the server only listens on SSL VPN connections. This requires the IP Office configuration to include an SSL VPN tunnel.

- **AFS ID**
  The server shows the ID after uploading an AFS file.

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

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

7.4.8 Watchdog

- **Log files age (days)**
  Sets the number of days that log file records are retained. This does not affect log file archives 95. Not applied to one-X Portal for IP Office.

7.4.9 Set Login Banner

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

7.5 Settings: System

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

7.5.1 Network

- **Network Interface**
  For the Unified Communications Module, this setting is fixed as ***eth0.1***.
  - **Enable Traffic Control**
    When enabled, the server throttles the rate at which it sends UDP packets from the IP Office service to IP Office System Monitor. This may be necessary if the IP Office System Monitor traces indicate a high number of lost packets.
- **Host Name**
  Sets the host name that the Unified Communications Module should use. This setting requires the local network to support a DNS server. Do not use ***localhost***.
- **Use DHCP**
  Do not use this setting with the Unified Communications Module.
- **IP Address**
  Displays the IP address set for the server. The Unified Communications Module connects to the LAN1 interface of the IP Office and must have an address on that subnet. See IP Address Notes 11.
- **Subnet Mask**
  Displays the subnet mask applied to the IP address.
- **Default Gateway**
  Displays the default gateway settings for routing.

- **System DNS**
  Enter the address of the primary DNS server.
- **Automatically obtain DNS from provider**
  Not used.
- **Create Subinterface**
  You can use this control to create an additional VLAN subnet on the same port. Clicking the button displays the menu for the subinterface network settings. This control is not supported on the Unified Communications Module and so is greyed out.
- **Delete Subinterface**
  Delete the subinterface. This control is not supported on the Unified Communications Module and so is greyed out.

7.5.2 Date and Time

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

- **Date**
  For a server not using NTP, this field shows the server's current date and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
- **Time**
  For a server not using NTP, this field shows the server's current UTC time and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
- **Timezone**
  In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field determines the appropriate offset applied to the UTC time above. Note that changing the timezone can cause a *"Session expired"* message to appear in the browser in which case you need to login again.
- **Enable Network Time Protocol**
  When selected, the server obtains the current date and time from the NTP servers listed in the **NTP Servers** list below. It then uses that date and time and makes regular NTP requests for updates.
  - **NTP Servers**
    With **Enable Network Time Protocol** selected, use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome. However, it is your responsibility to comply with the usage policy of the chosen server. Choose several unrelated NTP servers in case one of the servers becomes unreachable or its clock unreliable. The server uses the responses it receives from each NTP server to determine reliability.
    - The IP Office system can also use NTP to obtain its system time.
    - The default time setting for the Unified Communications Module is to use NTP with the server address set to 169.254.0.1 (the IP Office system). When this is set, you must configure the IP Office to get its time from an external SNTP server or set its time manually.
  - **Synchronize system clock before starting service**
    Use this option to synchronize the system clock to an NTP time server before starting other services. Do not use this option if the time server cannot be reliably reached. Waiting for synchronization to occur may block use of the system until a timeout has passed.
  - **Use local time source**
    When not selected, external NTP takes priority over the internal system clock. If selected, the local system clock is used as the time source. Only use this option if system clock is synchronized with another reliable source, for example a radio controlled clock device.

7.5.3 Authentication

- **Enable referred authentication**
  The password authentication used for access to the some services hosted by the server use either each services' own security settings or the security user accounts configured in the Management Services service running on the Unified Communications Module. See Password Authentication 12. This setting controls which method is used.
  - **Enabled**
    With referred authentication enabled, the security settings of the Management Services service running on the Unified Communications Module control access to the following other services:
    - **Web control menus**
    - **Voicemail Pro admin**

- **one-X Portal for IP Office admin**
- **IP Office Web Manager**

- **Disabled**
  With referred authentication disabled, each service controls access to itself using its own local account settings.

7.5.4 HTTP Server

- **Enable HTTP file store for backup/restore**
  If selected, the server can act as the 'remote server' destination for HTTP/HTTPS backups configured through the Web Manager menus. When enabled, the **System** 91 menu displays the quota available for backups. Servers with Voicemail Pro only support this option on disks larger than 155GB. Servers without Voicemail Pro only support this option on disks larger than 95GB.

7.5.5 Change Root Password

Server installation creates two Linux user accounts; ***root*** and ***Administrator***. You can use these fields to change the ***root*** account password. The new password must conform to the password rules 105.

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

7.5.6 Change Local Linux Account Password

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

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

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

The new password must conform to the password rules 105.

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

7.5.7 Password Rules Settings

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

7.5.8 Firewall

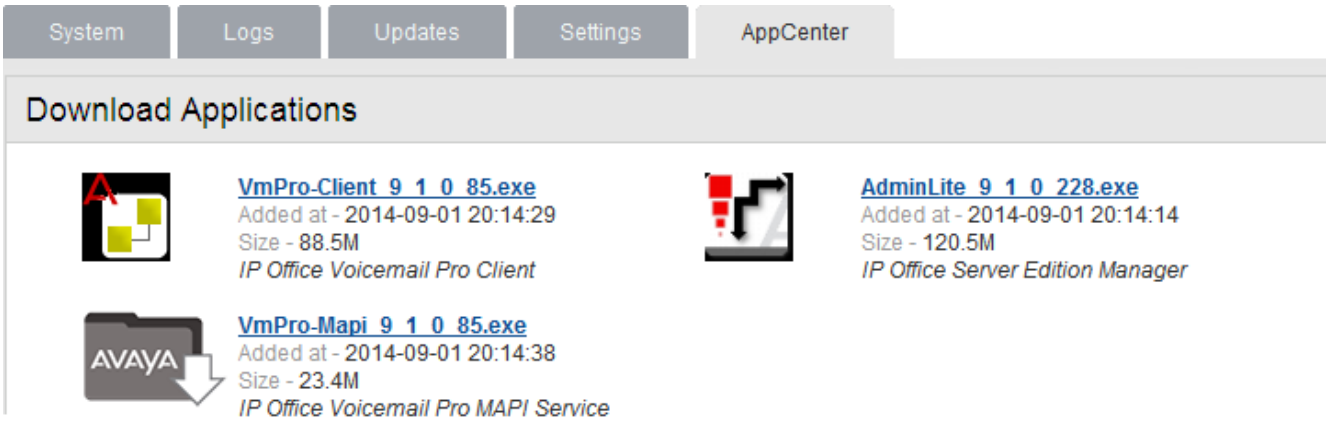
The server can apply firewall controls to the incoming traffic it receives.

- **Activate**
  Sets whether the firewall is active.
- **Enabled Filtering**
  Sets whether the firewall should apply filtering to the traffic received by the server.
- **Enable TCP ports**
  Select whether the server allows the following TCP ports when the firewall is active.
  - **21:** If selected, allow port TCP 21.
  - **80:** If selected, allow port TCP 80.
  - **8000:** If selected, allow port TCP 8000.
  - **8069:** If selected, allow port TCP 8069.
  - **8080:** If selected, allow port TCP 8080.
  - **9080:** If selected, allow port TCP 9080.
- **Enable UDP ports**
  Select whether the server allows the following UDP ports when the firewall is active.
  - **69:** If selected, allow port UDP 69.

7.6 App Center

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

The file repository location is configured through the Settings | General 99 page.



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

- ***VmPro...ClientOnly.exe***
  This is the installation package for the Voicemail Pro client application used to administer the Voicemail Pro server application.
- ***VmPro...Mapi.exe***
  This is the installation package for the MAPI proxy. This is installed on a Windows PC in the same network as the Windows Exchange server. It allows the Linux based Voicemail Pro server to access UMS services. Refer to the Voicemail Pro installation manual.
- ***IPOAdminLite...***
  This is the installation package for the IP Office Manager application. Note that this is an installer for IP Office Manager, System Monitor and System Status Application tools only. It is not the full IP Office Administration and User package used with other IP Office systems.

Chapter 8.
Document History

8. Document History

Date	Issue	Changes
30th October 2014	**10b**	• Updated for IP Office Release 9.1.
13th November 2014	**10c**	• Incorrect reference to **/CSIPOrec** as mount point for additional hard disk.
14th November 2014	**10d**	• Clarified that referred authentication applies to all services rather than just web control.
13th January 2015	**10e**	• Alignment of the terminology of the upgrade paths table 68 with the 9.1 GA technical bulletin. • Removed availability of a ZIP file as an upgrade method between different 9.0.3/9.0.4 builds. • Addition of the warning to disable one-X Portal logging prior to upgrading. • Link from upgrading to logging into web management went to wrong version of logging into web management topic. • Explanation of use of referred authentication 12 expanded. Now also applicable for UCM for 9.1. • Added screenshot of the UCM in web management Solution view. • Note regarding the need for further configuration to use the VNC menu is running a virtual machine added. • Extra steps in UCM V2 installation and upgrading added (module, including new module, needs manually controlled restart to enter software loading state). • Reference to user required for UCM Ignition corrected to root. • Zip upgrade method details removed (not used for 9.1).
14th January 2015	**10f**	• UCM v1 battery removal/disposal note removed. • USB2 terminology changed to USB (apparently USB1, 2 or 3 will work but with corresponding speed differences). • Recommendation for USB install/upgrade changed to use upper USB socket. Use lower socket for keyboard. • Incorrectly shown web control port and protocol options removed. • Description of log archives corrected, contains all available logs, not just those since last archive creation. • Application log menu shows the last 1000 log records. • Expanded explanation of the passwords requested during ignition. • USB utility instructions switched from UNetBootin to Rufus. • Removed errant author only comments. • Standardisation on 'amber' versus 'orange'.
17th February 2015	**10g**	• Clarification of UCM v2 upper USB is USB3. All others are USB2. • Put web management upgrade as first and preferred option for upgrading once system is on 9.1. • Notes that to use monitor the monitor needs to be attached before module restart. • Rufus URL changed to https: (http: works but frequently has problems). • Various tidying. • Removed errant "Use System Default" checkbox shown in screenshots of Application Server/Server Edition ignition.
3rd March 2015	**10h**	• Removed mention of web collaboration as potential optional service. • Processed raft of feedback in previous issue. • Security steps in ignition added (based on seeing them in Build 9.1.2(412).
13th March 2015	**10i**	• Republish due to UCM module upgrade option incorrectly appearing in non-UCM documents.
14th April 2015	**10j**	• Login Banner Text field is now blank by default (9.0 and 9.1). [80432] • Change to certificate controls to allow the backup and restoration of the server's security certificate. [87145] • Corrected **/CSIPOrec** to **/CSIPORec**. [82278]
15th April 2015	**10k**	• Corrected Rufus URL. • Removed USB3 references.
22nd April 2015	**10l**	• Various text updates. Not technical changes. Some reordering of sections.
5th May 2015	**10m**	• Merged the maintenance chapters for UCM and Linux servers. • Added details for adding a certificate to Safari (Windows and Mac).
26th May 2015	**10n**	• Updated download software page to match current support site design. [90569] • Minor update to Rufus settings (basically stating the defaults). [90575] • Rephrasing for fact that server certificates not available in 9.1.0GA but are available in 9.1FP (9.1.2). [90603]

Date	Issue	Changes
		• Slight restructure to skip "step phrase" in UCM quick install description. [90605] • Minor text enhancement to clarify that security is via shell "IP Office" on the UCM. [93333]
27th May 2015	**10o**	• Minor text changes. [90606] • one-X Portal AFA login is also under referred authentication control and by default uses Administrator account password. [90604] • Clarification of Voicemail backup transfer from old to new server process and reinstatement of SSH file transfer details. [90598] • Removed errant <<< >>> markup.
2nd June 2015	**10p**	• Correction to System Settings screenshot for application server. • Correct server maintenance topic incorrectly being included in Contact Recorder output.
16th June 2015	**10q**	• Minor update to match redesign of Avaya support website.
1st July 2015	**10r**	• Correction: UCM USB ISO transfer for upgrades needs to be fully prepared USB memory key, not just plain ISO file. • "Web Manager Upgrade" status shown in SSA for upgrades via web manager menus.
7th September 2015	**10s**	• Correction to mount path name for additional disks. Full name is derived disk mount path specified plus partition number, for example ***/additional-hdd#1/partition1***. [99975] • Various minor text layout fixes.
8th September 2015	**10t**	• Various minor text layout fixes. Fixed unplanned mention of Unified Communications Module in non-UCM outputs frm the common doc source.
29th September 2015	**10u**	• Republished with errant author's notes text now hidden.
30th September 2015	**10v**	• Correct of web control login from http to https.
30th October 2015	**10w**	• Warning added that voicemail restore 101 fails if VMPro client is connected. [99893] • Note that Syslog Event Viewer 95 filters are set when page is opened. Reload page to update.
2nd November 2015	**10x**	• Republish to resynch publishing system.
6th November 2015	**10y**	• Note that virtual servers either use NTP time or virtual server platform time. [100563]
8th December 2015	**10z**	• Correction to description of **Synchronize system clock before starting service** and **Use local time source**. • Clarifications to the password set and password change field descriptions to clarify which change IP Office and or Linux accounts.
21st December 2015	**10aa**	• Emphasis that security reset may disrupt calls and services.
19th January 2016	**10ab**	• Correct if path to download archived log files.

Index

1

169.254.0.1 11
169.254.0.2 11

3

3rd Party database integration 12

A

Add
  Sub-interface 103
Additional documentation 10
Address
  DNS 62, 103
  IP 62, 103
Administrator
  Login 48
Application
  Auto-start 76
  Repositories 81, 99
  Start 76
  Stop 76
  Uninstall 80
Application files
  Upload files 82
Application Logs 94
Archive 95
Attach
  Monitor and keyboard 68
Audit Log 94
Auto-start 76

B

Backup 100
  Custom folders 44
  one-X Portal for IP Office 54
  Voicemail 42
Boot
  from USB 24, 75
Browser 12
Bulletins 10
Buttons 67

C

CentOS 10
Change
  IP Address 62
Check
  Software version 97, 98
Clients 106
Configuration
  one-X Portal for IP Office 48
  Voicemail Pro 36
ContactStore 12
Cover 68
CPU
  Usage 91
Create a USB device 19, 74
Create Archive 95
Custom folders
  Backup/restore 44

D

Database integration 12
Date 78, 104
Default
  Gateway 62, 103
  Password 61
Delete
  Sub-interface 103
DHCP 62, 103
Disk
  Usage 91
DNS 62, 103
Download
  Logs 95
  Software 18
  Windows Clients 106

E

Enable Traffic Control 62, 103

F

Forward
  Syslog records 100

G

Gateway 62, 103
General 100

H

Home 91
Host Name 62, 103

I

Inactivity timeout 79, 101
Initial configuration 48
Interface 62, 103
IP Address 38, 62, 103
IP Office
  Check 48
  Select 48
ISO 18

J

Javascript 12

K

Keyboard 68

L

LAN2 11
LEDs 63
Linux 10
Local 100
Log Files Age 100
Logging In 61
Login 40, 61
  Administrator 48
  Banner text 100
Logs 93
  Application 94
  Archive 95
  Audit 94
  Download 95
  Log Files Age 100

M

Mask 62, 103
Memory
  Usage 91
Menu
  Download 95
  General 100
  Home 91
  Logs 93
  Logs Download 95
  Logs View 94
  Services 97
  System 98, 103

Menu
Updates 96
Updates Services 97
Updates System 98
View 94
Windows Clients 106
Menus
Inactivity timeout 79, 101
Module
Buttons 67
Cover 68
LEDs 63
Restart 77
Shutdown 77
Monitor 68
N
NAT 11
Network 62, 103
Change IP address 62
Sub-interface 103
Network Time Protocol 78, 104
no Remote 40
Notifications 91
NTP 78, 104
O
one-X Portal for IP Office
Auto-start 76
Backup/restore 54
Configuration 48
Start 76
Stop 76
Operating system
Repositories 81, 99
Upload files 82
P
Password
Change 48
Default 61
Root password 76
Rules 105
Port
Web Control 100
R
RAM
Usage 91
Reboot 77, 91
Recieve
Syslog 100
Related documents 10
Remote Software Repositories 83
Remove
Sub-interface 103
Repositories 81, 83, 99
Repository 100
Restart 77
Restore 100
Custom folders 44
one-X Portal for IP Office 54
Voicemail 42
Root password
Change 76
Rules 105
RPM 18
Rules 105
S
Send
Syslog records 100
Server
NTP 78, 104
Reboot 77, 91
Shutdown 77, 91
Server Name 40
Service
Auto-start 76
Start 76
Stop 76
Uninstall 80
Services 97
Start 91
Status 91
Stop 91
Set
Login banner 100
SFTP 84
Shutdown 77, 91
SNMP 100
SNMP Support 100
Software 40
Downloading 18
Install from USB 24, 75
Repositiories 81, 99
Repositories 83
Unetbootin 18, 19, 74
USB 18, 19, 74
Software Repositories 100
Software version
Check 97, 98
SSH access 84
Start 77
Auto-start 76
Service 76
Start Services 91
Status 91
Stop
Service 76
Stop Services 91
Sub-interface 103
Subnet Mask 62, 103
Supported
Browsers 12
syslinux.cfg 19, 74
Syslog
Settings 100
View 95
System 98, 103
T
Technical bulletins 10
Time
Timezone 78, 104
Timeout 79, 101
Traffic Control 62, 103
Transfer an ISO file
Direct upload 71
Remote file server 70
SSH/SFTP transfer 71
U
UMS 12
Uninstall
Application 80

Uninstall
Service 80
Unit Name/IP Address 40
Update
Check version 97, 98
Services 97
System 98
Updates
Services 96
System 96
Upload
Application files 82
Operating system 82
Windows client files 82
Usage
CPU 91
Disk 91
Memory 91
USB
Create a bootable... 19, 74
Load software 24, 75
Software 18, 19, 74
USB Initiator 18

V

Version
Check 97, 98
View
Syslog records 95
View Logs 94
Virtual DVD
Direct upload 71
Remote file server 70
SSH/SFTP transfer 71
Voicemail
Auto-start 76
Backup/restore 42
Start 76
Stop 76
Voicemail IP Address 38
Voicemail Pro
Configuration 36
Limitations 12
Voicemail Pro Client
run 40
Voicemail Pro Client window 40
Voicemail Pro Login window 40
Voicemail Pro Server
connect 40
Voicemail Type 38
VPNM 12

W

WAN 40
Watchdog 100
Web browser 12
Web Control Port 100
Windows client
Repositories 81, 99
Windows client files
Upload files 82
Windows Clients 106
Workstation 40

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

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

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

© 2016 Avaya Inc. All rights reserved.