IP Office Platform 12.0

Installing and Maintaining an IP Office Unified Communications Module

15-601011 Issue 18b - (Thursday, December 5, 2024)

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

Documentation disclaimer
“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

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

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.
“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses
The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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 LLC.

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: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

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

Contents

1. Overview

1.1 What's New ... 7
1.2 Module Versions ... 7
1.3 Module Capacity ... 7
1.4 Using Linux ... 9
1.5 Additional Documentation ... 9
1.6 IP Address Notes ... 10
1.7 Small Community Networks ... 10
1.8 Licenses and Subscriptions ... 11
1.9 Supported Web Browsers ... 11
1.10 Password Authentication (Referred Authentication) ... 12

2. Module Installation

2.1 Quick Install ... 14
2.2 Prerequisites ... 16
2.3 Downloading Module Software ... 16
2.4 Preparing a USB Installation Key ... 17
2.5 Checking the Licenses ... 18
2.6 Changing the IP Office Time Settings ... 18
2.7 Changing the IP Office Security Settings ... 19
2.8 Shutting Down the IP Office System ... 20
2.9 Inserting the Module ... 21
2.10 Installing the Software ... 22
2.11 Igniting the Module Services ... 23
2.12 Adding a Certificate to the Browser ... 26
2.13 Server Initial Configuration ... 27
2.14 Application Initial Configuration ... 27

3. Voicemail Pro Configuration

3.1 Adding Voicemail Licenses ... 31
3.2 IP Office Configuration ... 32
3.3 Installing the Voicemail Pro Client ... 33
3.4 Enabling the Voicemail Pro Client ... 34
3.5 Logging in to the Voicemail Server ... 34
3.6 Changing the Voicemail Server Password ... 35
3.7 Transferring Voicemail Server Settings ... 36
  3.7.1 Transferring Custom Folders ... 38

4. one-X Portal for IP Office Configuration

4.1 Adding Licenses ... 40
4.2 Enabling one-X Portal for IP Office Users ... 41
4.3 Initial one-X Portal for IP Office Login ... 42
4.4 Initial AFA Login ... 43
4.5 If the Portal Service Status Remains Yellow ... 44
4.6 Transferring one-X Portal for IP Office Settings ... 45

5. Server Maintenance

5.1 Logging In ... 49
5.2 Logging Into Web Control Directly ... 50
5.3 Viewing the Module IP Address ... 51
5.4 Changing the IP Address Settings ... 51
5.5 Module LEDs ... 52
5.6 Module Buttons and Ports ... 55
5.7 Attaching a Monitor and Keyboard ... 55
5.8 Using System Status Application ... 56
5.9 Upgrading the Module ... 57
  5.9.1 Web Manager Upgrade ... 58
  5.9.2 USB Upgrade ... 62
5.10 Starting/Stopping Application Services ... 65
  5.10.1 Starting a Service ... 65
  5.10.2 Stopping a Service ... 65
  5.10.3 Setting a Service to Auto Start ... 65
5.11 Changing the Linux Passwords ... 66
5.12 Shutting Down the Server ... 67
5.13 Rebooting the Server ... 67
5.14 Date and Time Settings ... 68
5.15 Creating Administrator Accounts ... 69
5.16 Setting the Menu Inactivity Timeout ... 69
5.17 Upgrading ... 70
5.18 Uninstalling an Application ... 70
5.19 Setting Up File Repositories ... 72
  5.19.1 Source Files ... 72
  5.19.2 Setting the Repository Locations ... 72
  5.19.3 Uploading Local Files ... 73
  5.19.4 Creating Remote Software Repositories ... 74
5.20 Downloading Log Files ... 75
5.21 SSH File Transfers ... 76
5.22 Adding TTS Languages ... 77

6. Web Manager

6.1 Logging In to Web Manager ... 81

7. Addendum

7.1 Creating a USB Key using Rufus ... 84
Index ... 87

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 R12.0 or higher software. The module is a Linux-based server that allows various IP Office applications to run as embedded applications within the IP Office control unit rather than requiring a separate PC.

Important Support Notes

- The Unified Communications Module (UCM) cannot support the 64-bit Linux used for IP Office R12.0 and higher. Therefore, you cannot upgraded a UCM to run R12.0.x software. However, Avaya supports UCM modules running R11.1.3.2 software in IP Office R12.0 and higher systems with the following caveats:
  - If the existing Unified Communications Module is running pre-R11.1 software, you must upgrade it to R11.1.3.2 using the processes in the *"Upgrading Linux-based IP Office Systems to R11.1"* manual.
  - The IP Office system will output a UCM version mismatch alarm each time the IP Office is restarted. You can ignore this alarm.
  - There will be no future updates to the IP Office software components provided on the UCM modules.
  - There will be no any future updates for the CentOS operating system and no security CVE patches for UCM modules.

1.1 What's New

The Unified Communications Module can host the following applications:

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

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

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

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

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

- **Optional Services**
  The Unified Communications Module does not support any optional services (for example Media Manager, WebRTC Gateway or Web Client).

1.2 Module Versions

There are 2 versions of Unified Communications Module. Whilst the two versions are physically different, they support the same embedded applications and application capacities.

In this documentation, all references to Unified Communications Module cover both types of module unless otherwise specifically stated.

- The original Unified Communications Module, Unified Communications Module v1 henceforth, is no longer supported by Avaya.

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

1.3 Module Capacity

The capacity of the Unified Communications Module is:

- **Number of Modules**
  Maximum one module per system.

- **Trunk Cards:**
  The module does not support a trunk daughter card.

- **IP Office Users:**
  - Up to 200 users when running Voicemail Pro and one-X Portal for IP Office.
  - More than 200 users when running just Voicemail Pro.

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

- **Maximum voicemail ports:** For systems running in IP Office Subscription mode, the module provides the ports as listed below. For other modes, the module provides 4 ports as standard but can be licensed 11 for additional ports up to the limits below.
  - Up to 20 ports when running Voicemail Pro and one-X Portal for IP Office.
  - Up to 40 ports when running just Voicemail Pro.

- **Voicemail storage capacity:**
  - Up to 800 hours storage for messages, prompts and announcements.
  - An additional limit of 60 minutes applies for any individual mailbox.

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

1.4 Using Linux

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

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

1.5 Additional Documentation

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

Related Documents

- **Upgrading Linux-Based IP Office Systems to R12.0**
  Covers the special process required to upgrade pre-R11.1 Linux-based servers.
- **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** - https://ipofficekb.avaya.com
- **Avaya Documentation Web Site** - https://documentation.avaya.com

1.6 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.

1.7 Small Community Networks

Up to 32 IP500 V2 systems can connect using H323 SCN trunks to form a Small Community Network, supporting up to 1000 users. However, when using a Unified Communications Module, the Small Community Network only supports up to 6 systems. Also, if running the one-X Portal for IP Office application, it only supports up to 200 users.

When installing an IP Office Application Server 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.

1.8 Licenses and Subscriptions

For an IP Office Application Server supporting a standalone IP500 V2 or an Small Community Network of such systems, access to the IP Office Application Server services depends on system license or subscriptions.

Subscriptions

For an IP Office Application Server supporting an IP500 V2 running in IP Office Subscription mode:

- Use of the one-X Portal for IP Office services is limited to users with a **Unified Communications User** subscription.
- Use of the Voicemail Pro service does not require any subscriptions. However, the UMS and TTS Email Reading features are limited to users with a **Unified Communications User** subscription.

Licenses

For an IP Office Application Server supporting an IP500 V2 not running in IP Office Subscription mode, the use of various features is licensed, for example which users are able to use the one-X Portal for IP Office application. For such an installation it is important to understand the role of the licenses below. For a IP Office Subscription mode system

- **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.
- **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.

1.9 Supported Web Browsers

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

- **Microsoft Edge** / **Mozilla Firefox** / **Google Chrome** / **macOS Safari**.

1.10 Password Authentication (Referred Authentication)

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

The **Enable referred authentication** setting controls the method used.

- These settings are only accessible if logged in via referred authentication 12 or as the local Linux root. Therefore, when disabled, the setting can only be re-enabled by logging in using the local Linux root name and password.
    - **Enabled**
      This is the default for new installation. When 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 using its own local account settings.

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 12.0 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 16. 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 12.0. The system must have an **Essential Edition** and **Preferred Edition** license 18.

b. A Windows PC with IP Office Manager and System Status Application networked to the IP Office system. Test by opening the IP Office configuration and by connecting System Status Application.

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. The address must be on the same subnet as the IP Office system's LAN1.

f. A server host name for the module to use on the customer's network.

g. The latest Unified Communications Module ISO image that matches the IP Office release and the Avaya USB Creator tool. See Downloading Module Software 16.

2. Prepare the USB Key for Installation

a. Using the downloaded 16 Avaya USB Creator tool, prepare the USB installation key 17.

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 20.

6. Insert the Unified Communications Module and Software Installation Key

a. Insert the module 21 into an empty slot in the system.

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

c. Connect System Status Application 56 to the IP Office and select the menu for Unified Communications Module as this shows the installation progress.

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

e. Once the system is running, shut down the UCM by pressing the top button on the module until the upper LED 52 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).

f. Restart the module by pressing the upper button until both amber LEDs turn off. Alternatively in System Status Application click **USB Boot**.

g. Allow the process to run until the status in System Status Application shows *"Idle, card has not been ignited"*.

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***.

b. The login menu appears. 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 and the services it runs. Click **Next**.

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

h. Select to either generate certificates or upload the certificates that the module should use. Click **Next**.

i. Download the certificates generated if any. Check the settings and if okay click **Apply**.

j. Add the certificates 26 to your browser.

8. Initial Management Services Configuration

a. Using a web browser, enter https:// followed by the IP address given to the module during ignition and :7070.

b. The login menu appears. Enter ***Administrator*** and the password set for that user account during ignition.

c. Check that the details on the initial configuration menu are correct.

d. Click **Apply**.

9. Configure the Server Applications

Check and configure the server applications. See Voicemail Pro Configuration 30 and one-X Portal for IP Office Configuration 40.

- **! 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 Prerequisites

Check that you have the following:

a. An IP500 V2 running IP Office Release 12.0. The system must have an **Essential Edition** and **Preferred Edition** license 18.

b. A Windows PC with IP Office Manager and System Status Application networked to the IP Office system. Test by opening the IP Office configuration and by connecting System Status Application.

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. The address must be on the same subnet as the IP Office system's LAN1.

f. A server host name for the module to use on the customer's network.

g. The latest Unified Communications Module ISO image that matches the IP Office release and the Avaya USB Creator tool. See Downloading Module Software 16.

2.3 Downloading Module Software

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

- **ISO Image**
  You can use this type of file to install and upgrade the full set of software. Before using an ISO image, you must backup all applications data.
  - Note that the Unified Communications Module uses a different ISO file from other Linux-based IP Office products. Ensure that you download the C110 ISO file for Unified Communications Module installs and upgrades.
- **Source ISO Image**
  Some components of the software are open source. To comply with the license conditions of that software, Avaya is required to make the source software available. However, this file is not required for installation.
- **Avaya USB Creator Tool**
  This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade. Note: You must use the R11.1 version of this tool for R11.1 and higher systems.
- **Text-to-Speech Languages ISO Images**
  No TTS languages are installed by default. TTS languages can be added post installation, see Adding TTS Languages 77. Note: Pre-R11.1 TTS files are not compatible with R11.1 and higher.

To download Avaya software:

1. Browse to ***https://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.

2.4 Preparing a USB Installation Key

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

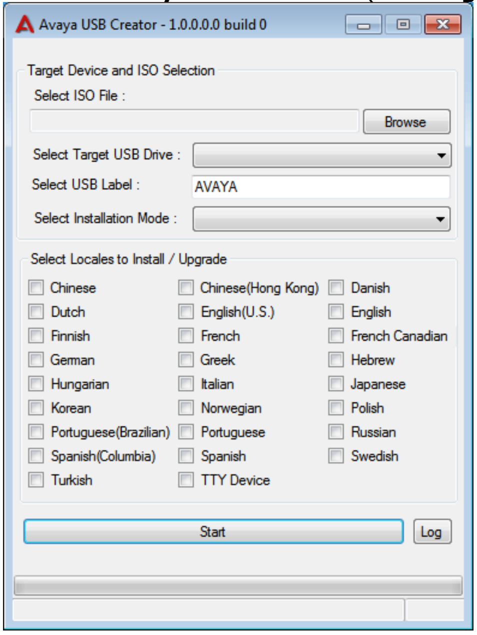
This process extracts a downloaded ISO image onto a USB memory key and then turns that memory key into a bootable device for software installation or upgrading.

Prerequisites

- **6GB USB Memory Key**
  Note that this process reformats the memory key and erases all existing files.
  - **64GB+ Memory Keys**
    This process can only be used with USB memory keys smaller than 64GB. For larger keys, see Creating a USB Key using Rufus 84.
- **Avaya USB Creator Tool**
  This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade. Note: You must use the R11.1 version of this tool for R11.1 and higher systems.
- **Unified Communications Module ISO Image**
  You can download this file from the Avaya support website, see Downloading Module Software 16.

To create a bootable USB memory key:

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



Avaya USB Creator - 1.0.0.0 build 0

Target Device and ISO Selection

Select ISO File :

Select Target USB Drive :

Select USB Label : AVAYA

Select Installation Mode :

Select Locales to Install / Upgrade

□ Chinese □ Chinese(Hong Kong) □ Danish
□ Dutch □ English(U.S.) □ English
□ Finnish □ French □ French Canadian
□ German □ Greek □ Hebrew
□ Hungarian □ Italian □ Japanese
□ Korean □ Norwegian □ Polish
□ Portuguese(Brazilian) □ Portuguese □ Russian
□ Spanish(Columbia) □ Spanish □ Swedish
□ Turkish □ TTY Device

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

2.5 Checking the 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.
- **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.

2.6 Changing the IP Office Time Settings

By default IP Office systems are configured to obtain time from its Voicemail Pro server which obtains that time from the Windows server on which it is installed. Obviously this option cannot be used when the voicemail server is running on a Unified Communications Module since the module gets its time from the IP Office. To support the module, the system must either use an external SNTP 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**. Refer to the IP Office Manager help for details.
4. Click on the save icon to send the configuration back to the IP Office.

2.7 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 35 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.

2.8 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.

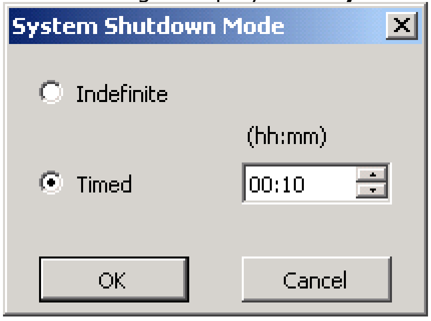
- **! WARNINGS**
  - You must always shutdown a system before switching it off. Simply removing the power cord or switching off the power input may cause the loss of data.
  - This is not a polite shutdown, it stops any user calls and services in progress.
  - The shutdown process takes up to a minute 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 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.



System Shutdown Mode

○ Indefinite

● Timed (hh:mm) 00:10

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.

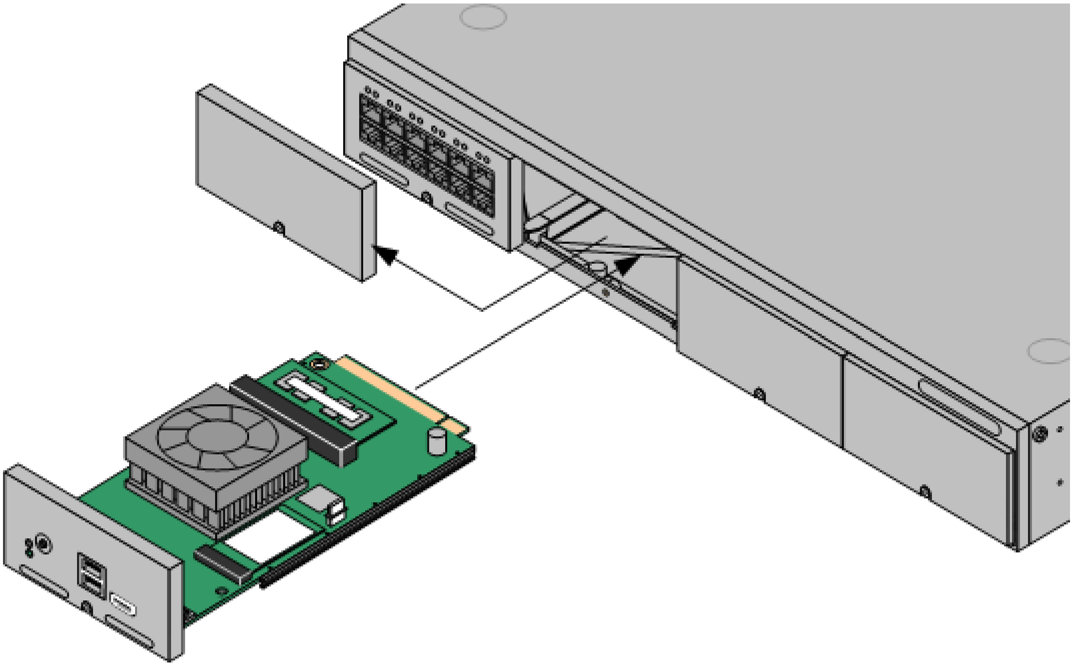
2.9 Inserting the Module

Once you have shutdown 20 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. Using a flat-bladed screwdriver, remove the blank cover from an unused slot on the front of the control unit.



2. 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.
3. While inserting the module, also check to ensure that cables on the module do not interfere with the insertion operation.
4. 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.
5. Using a flat-bladed screwdriver, secure the module.
6. Reapply power to the system.
7. Once the system has fully restarted, check the module LEDs. If the lower LED remains red, the module is not supported by the system. The most likely cause is that the system is not correctly licensed 18. Recheck the licenses and then restart the system.
8. Once the module's lower LED is green, proceed with installing the module software 22.

2.10 Installing the Software

To install software from the previously prepared USB memory key 17, 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.

- **! IMPORTANT**
  Ensure that you have met all the prerequisites 16 before beginning software installation.

To install a software image from a USB memory key:

1. Connect to the IP Office using System Status Application. Select **System | UC Modules** and select the module. The page shows the module status and other information.

2. Insert the USB memory key with the new ISO image file into the module's upper USB port.

3. The next step requires the module to boot from the USB memory key. This can be done in two ways:

   - **Using the module buttons:**
     Shut down the module by pressing the upper button on the module until the upper 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. Restart the module by pressing the upper button again and keeping it pressed until the two LEDs change from amber to off.

   - **Using System Status Application:**
     Click on the **Shutdown** button. Once the module has shut down, click the **USB Boot** button.

5. After up to 2 minutes initializing, the module boots using the files on the USB memory key. System Status Application should report *"USB Upgrade/Install"* and both upper and lower LEDs flash amber/green.

6. The progress of the software installation/upgrade is shown in System Status Application. The initial software installation process between 15 to 80 minutes depending on the number of languages being installed.

7. 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. 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 module automatically shutdown after a firmware upgrade. Restart the module by pressing the top button or using System Status Application 56.

   - **Lower status LED green except for regular IP Office heartbeat flashes:**
     This indicates that the module restarted without needing a firmware upgrade.

8. The software installation is complete when System Status Application shows the status "*Idle, card has not been ignited*".

9. Remove the USB memory key. You now need to ignite the module services 23.

2.11 Igniting the Module Services

Following software installation 22, 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***.

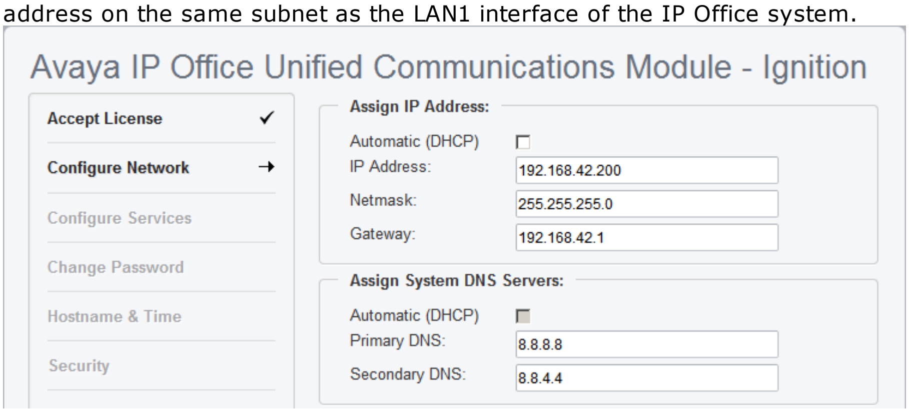
2. The login menu appears:

   a. 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.

   b. Enter the default password (***Administrator***).

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

3. 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.



Avaya IP Office Unified Communications Module - Ignition

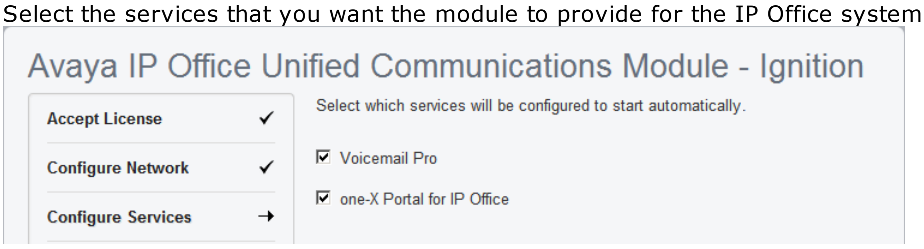
Assign IP Address:

Automatic (DHCP) □
IP Address: 192.168.42.200
Netmask: 255.255.255.0
Gateway: 192.168.42.1

Assign System DNS Servers:

Automatic (DHCP) □
Primary DNS: 8.8.8.8
Secondary DNS: 8.8.4.4

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



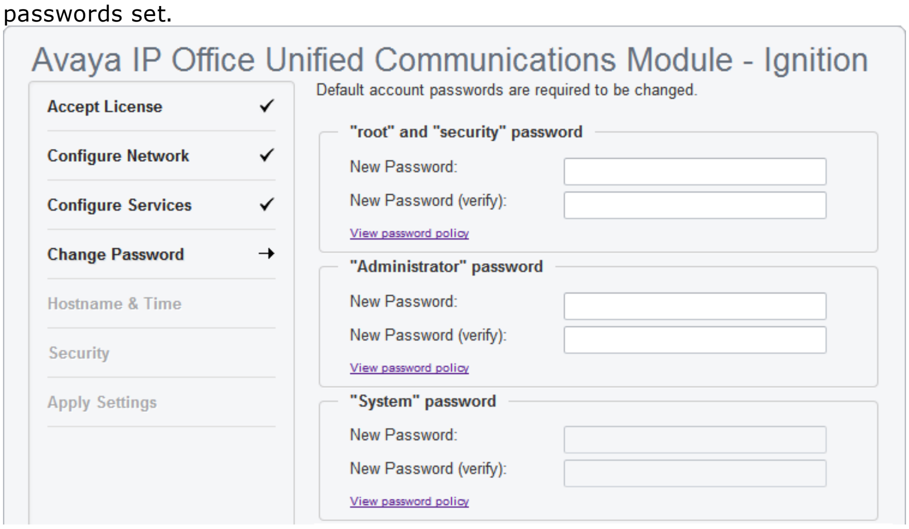
Avaya IP Office Unified Communications Module - Ignition

Select which services will be configured to start automatically.

☑ Voicemail Pro

☑ one-X Portal for IP Office

5. 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.



Avaya IP Office Unified Communications Module - Ignition

Default account passwords are required to be changed.

"root" and "security" password

New Password:
New Password (verify):
View password policy

"Administrator" password

New Password:
New Password (verify):
View password policy

"System" password

New Password:
New Password (verify):
View password policy

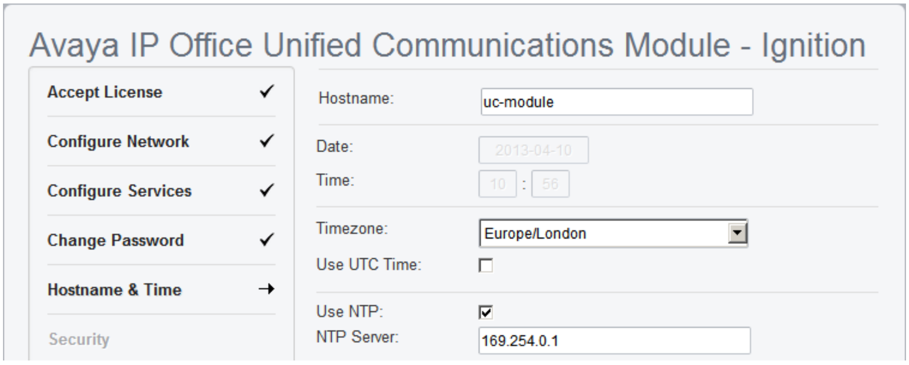
- The passwords must be 8 to 32 characters, containing at least two types of character (lower case, upper case, numeric and special characters) and no more the 3 consecutive characters.

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

- **Administrator password**
  This sets the password for Linux **Administrator** account and also the **Administrator** account of the Management Services service run on the 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.

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



Avaya IP Office Unified Communications Module - Ignition

Hostname: uc-module

Date: 2013-04-10

Time: 10 : 56

Timezone: Europe/London

Use UTC Time: □

Use NTP: ☑

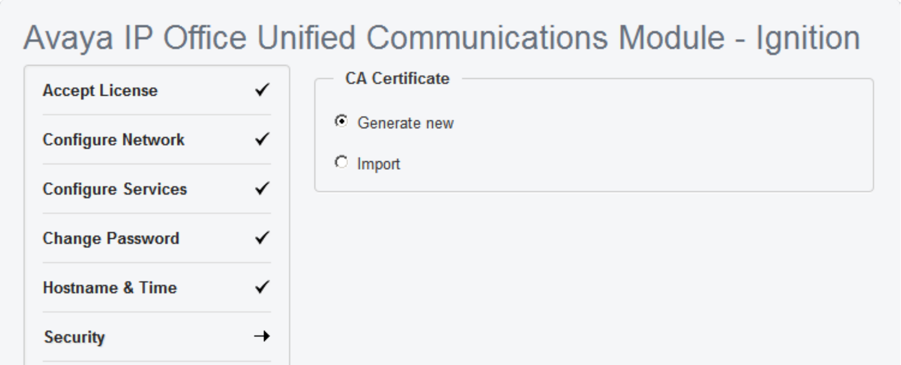
NTP Server: 169.254.0.1

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

  - For internal use, this value must be reachable by DNS within the customer network. If also supporting external client connections, it needs to be reachable by external DNS. Consult with the customer's IT support to ensure the name is acceptable and that routing to it has been configured correctly. External access must also include a firewall and/or SBC.

- **Use NTP/NTP Server**
  Do not change the settings. The default ***169.254.0.1***.setting is an internal address for the module to get its time its host system.

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



Avaya IP Office Unified Communications Module - Ignition

CA Certificate

● Generate new

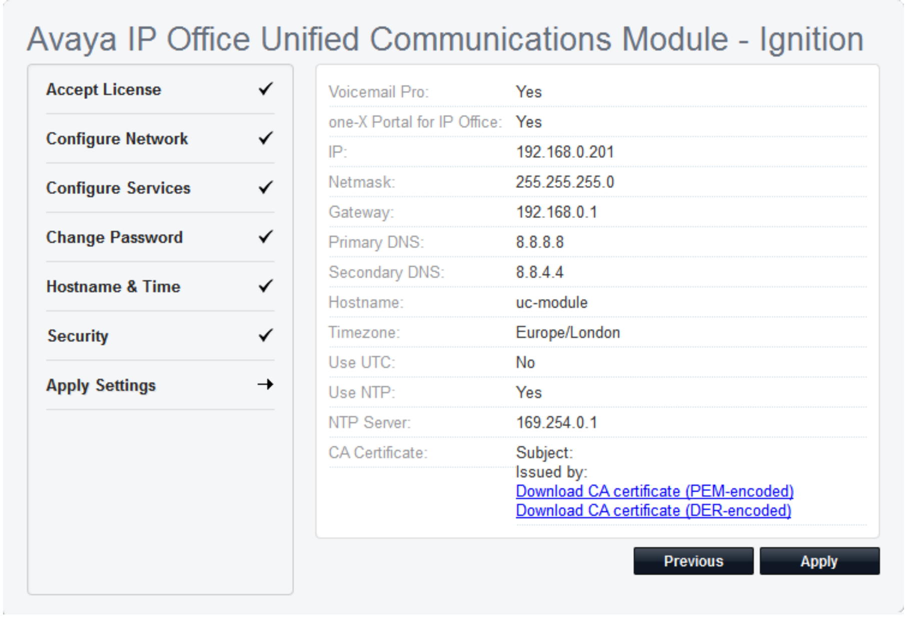
○ Import

- 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**.

8. Select whether you want the server to be supported by Avaya through their **EASG** service. Click **Next**.

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



Voicemail Pro:	Yes
one-X Portal for IP Office:	Yes
IP:	192.168.0.201
Netmask:	255.255.255.0
Gateway:	192.168.0.1
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4
Hostname:	uc-module
Timezone:	Europe/London
Use UTC:	No
Use NTP:	Yes
NTP Server:	169.254.0.1
CA Certificate:	Subject: Issued by: Download CA certificate (PEM-encoded) Download CA certificate (DER-encoded)

10. 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.

11. 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.

12. Follow the instructions for adding a certificate to your browser 26.

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** 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**.
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**.

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**.

2.13 Server Initial Configuration

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

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

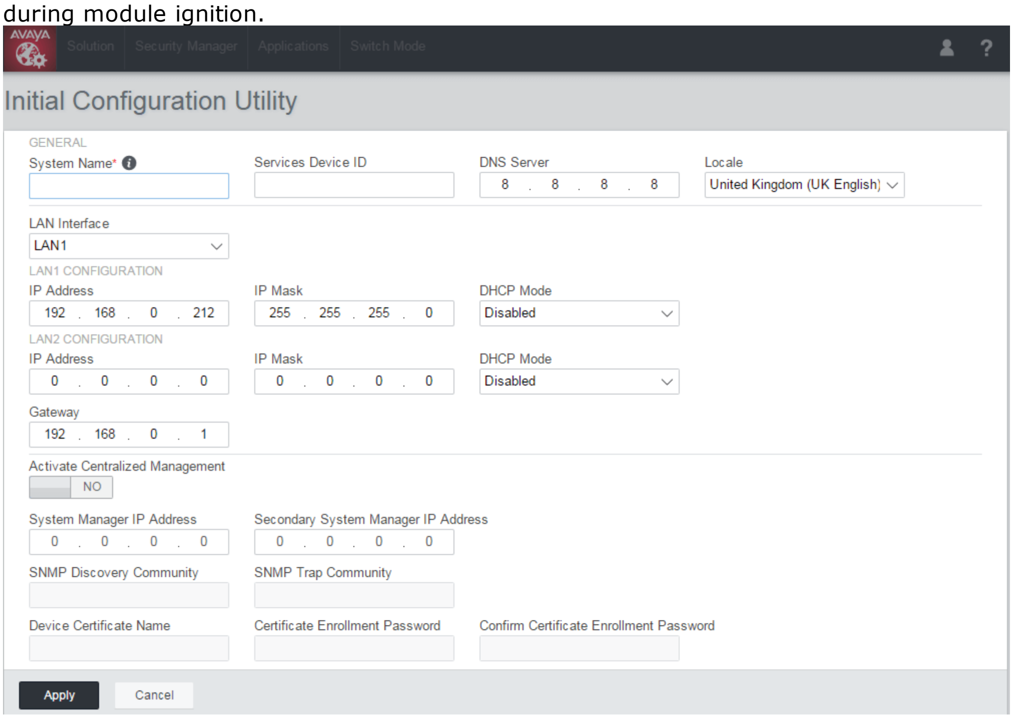
To perform initial configuration through IP Office Web Manager:

1. Log into 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 **Administrator** and the password that was created for that user during ignition.

2. Web manager displays the initial configuration menu for the Management Services service. If this does not appear, click **Solution**. Most of the settings are automatically completed using the values you entered during module ignition.



Initial Configuration Utility

GENERAL

System Name*:

Services Device ID:

DNS Server: 8 . 8 . 8 . 8

Locale: United Kingdom (UK English)

LAN Interface: LAN1

LAN1 CONFIGURATION

IP Address: 192 . 168 . 0 . 212

IP Mask: 255 . 255 . 255 . 0

DHCP Mode: Disabled

LAN2 CONFIGURATION

IP Address: 0 . 0 . 0 . 0

IP Mask: 0 . 0 . 0 . 0

DHCP Mode: Disabled

Gateway: 192 . 168 . 0 . 1

Activate Centralized Management: NO

System Manager IP Address: 0 . 0 . 0 . 0

Secondary System Manager IP Address: 0 . 0 . 0 . 0

SNMP Discovery Community:

SNMP Trap Community:

Device Certificate Name:

Certificate Enrollment Password:

Confirm Certificate Enrollment Password:

3. Check the values are as expected:

   - Check that **DHCP mode** is set to ***Disabled***.

   - If the module will be under centralized management from Avaya System Manager, select the **Centralized Management** checkbox. Enter the details required for Avaya System Manager.

4. Click **Apply**. The service is restarted using the values set in the menu. After the restart the browser is redirected to the normal web management menus.

2.14 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** 30

2. **one-X Portal for IP Office Initial Configuration** 41

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 Administration Manual 9. This section only covers the minimum steps recommended to ensure that the voicemail server is operating.

Initial Configuration Summary

a. **IP Office Configuration**

   i. **Adding voicemail licenses** 31

   ii. **Check the Voicemail Type Setting** 32

b. **Voicemail Pro Configuration**

   i. **Install the Voicemail Pro client** 33

   ii. **Log in to the Voicemail Pro server** 34

   iii. **Change the voicemail server password** 35

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 32 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 51.

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 36.

3.1 Adding Voicemail Licenses

This section does not apply if the IP500 V2 is running in IP Office Subscription mode. For other systems:

- The Unified Communications Module automatically enables 4 ports for Voicemail Pro operation. You can license additional ports for up to 20 ports 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:

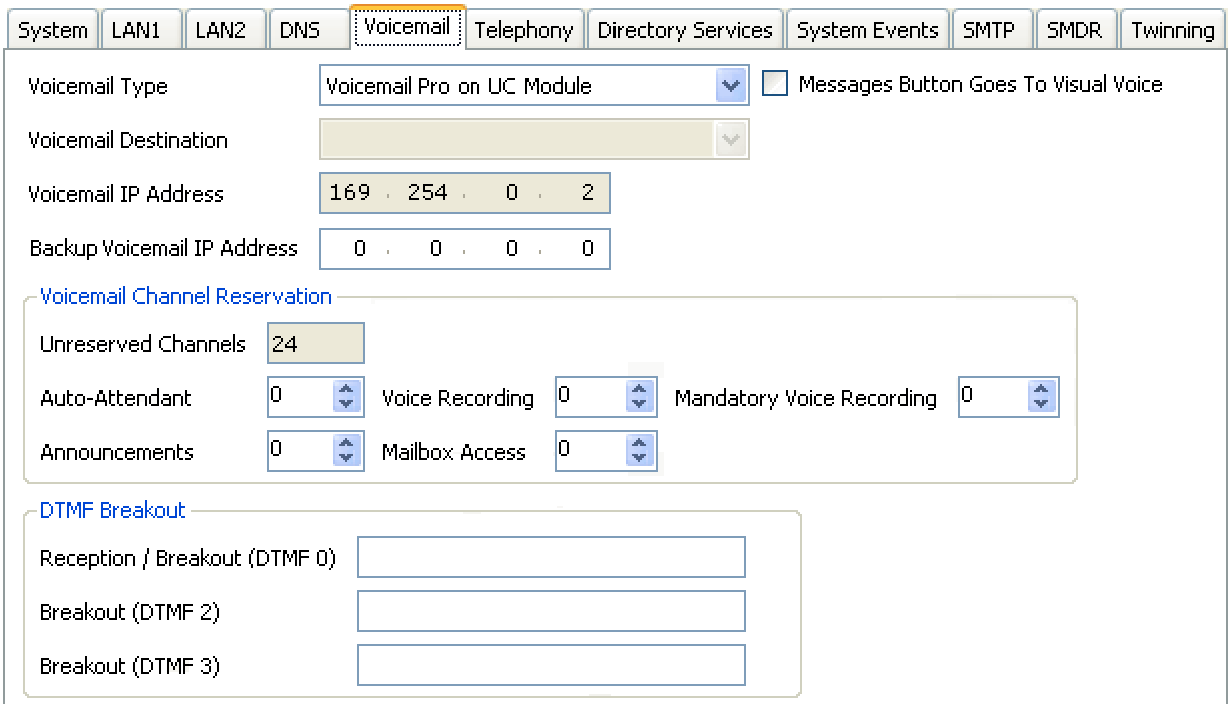
- **Essential Edition**
  This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
  The Voicemail Pro application requires this license. The license enables the application and 4 voicemail ports.
- **Preferred Edition Additional Voicemail Ports**
  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.

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.



Voicemail Type: Voicemail Pro on UC Module

□ Messages Button Goes To Visual Voice

Voicemail Destination:

Voicemail IP Address: 169 . 254 . 0 . 2

Backup Voicemail IP Address: 0 . 0 . 0 . 0

Voicemail Channel Reservation

Unreserved Channels: 24

Auto-Attendant: 0

Voice Recording: 0

Mandatory Voice Recording: 0

Announcements: 0

Mailbox Access: 0

DTMF Breakout

Reception / Breakout (DTMF 0):

Breakout (DTMF 2):

Breakout (DTMF 3):

- Check that the **Voicemail Type** is set to ***Voicemail 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 ***169.254.0.2***. This is the internal private IP address 10 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, up to 40 maximum. You can license the Unified Communications Module up to a maximum of 20 ports when running Voicemail Pro and one-X Portal for IP Office or a maximum of 40 ports when running just Voicemail Pro. For IP Office Subscription mode systems, the maximum number of supported ports are automatically available.

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

3.3 Installing the Voicemail Pro Client

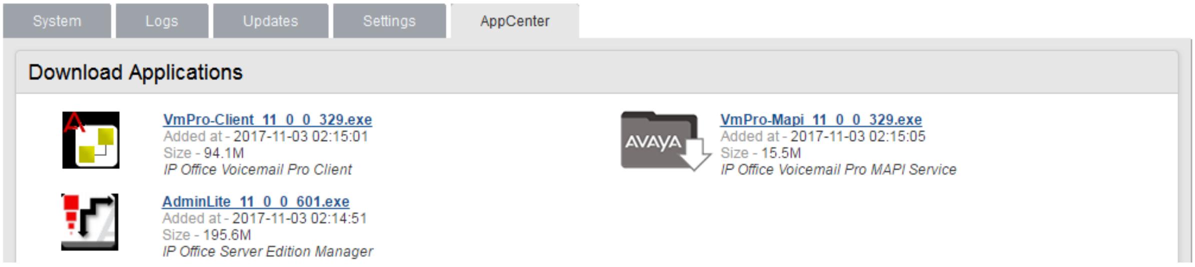
You can install the Voicemail Pro client onto a Windows PC. You can then use it to remotely administer the voicemail server.

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 81. In the displayed list of systems, click on the ≡ icon next to the server and select **Platform View**.

2. Select the **AppCenter** tab.



Download Applications

VmPro-Client_11_0_0_329.exe
Added at - 2017-11-03 02:15:01
Size - 94.1M
IP Office Voicemail Pro Client

VmPro-Mapi_11_0_0_329.exe
Added at - 2017-11-03 02:15:05
Size - 15.5M
IP Office Voicemail Pro MAPI Service

AdminLite_11_0_0_601.exe
Added at - 2017-11-03 02:14:51
Size - 195.6M
IP Office Server Edition Manager

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 Enabling the Voicemail Pro Client

For new systems, access to the voicemail settings using the Voicemail Pro client is disabled by default.

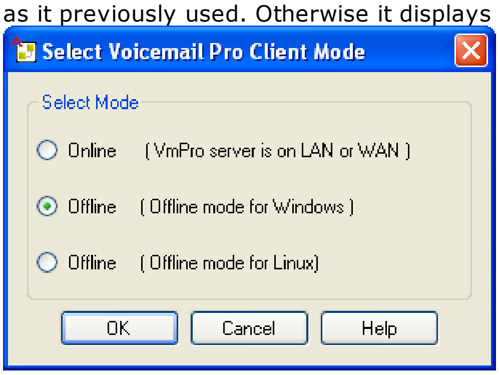
To enable access using the Voicemail Pro client:

1. Using a web browser, log into the web management menus of the Unified Communications Module.
2. Click **Applications** and select **Voicemail Pro - System Preferences**.
3. Select **Enable Voicemail Pro Client Interface**.
4. After making any changes, click **Update**. and then click **Yes**.

3.5 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.



Select Voicemail Pro Client Mode

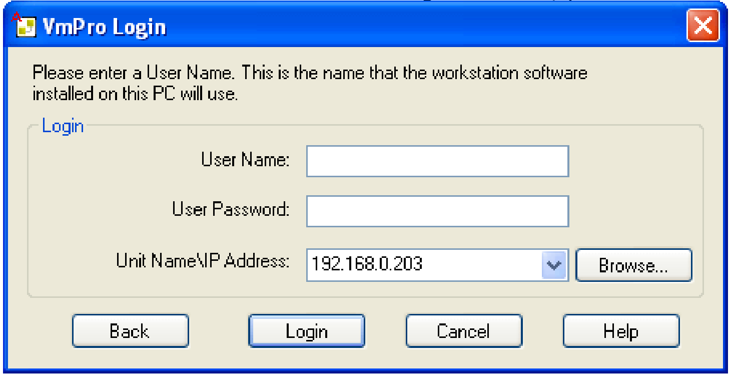
Select Mode

○ Online (VmPro server is on LAN or WAN)

● Offline (Offline mode for Windows)

○ Offline (Offline mode for Linux)

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



VmPro Login

Please enter a User Name. This is the name that the workstation software installed on this PC will use.

Login

User Name:

User Password:

Unit Name\IP Address: 192.168.0.203

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**.

3.6 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.

- For IP Office R11.1 FP1 and higher, the password for voicemail connection is enforced to 31 characters with restriction on repeated characters and enforcement of characters from different character types (lower case, upper case, numbers, extended characters).

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

1. Login 49 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.
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**.

3.7 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 38.

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 76, 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 76.
2. Copy the backup folder into the folder ***/opt/vmpro/Backup/Scheduled/OtherBackups***.
3. Using a web browser, login 50 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.

3.7.1 Transferring Custom Folders

Linux based servers do not include manually created folders in the backup or restore processes. Instead you need to copy any 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 76, 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 only does this directly on the server. Root access is not supported on remote connections.
      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 ine interface, enter **/opt/Avaya/clish**.
   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 9.

Initial Configuration Summary

a. **Add licenses** 40
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** 41
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** 42
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 51 .

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***, ***Power User*** or Unified Communications User.

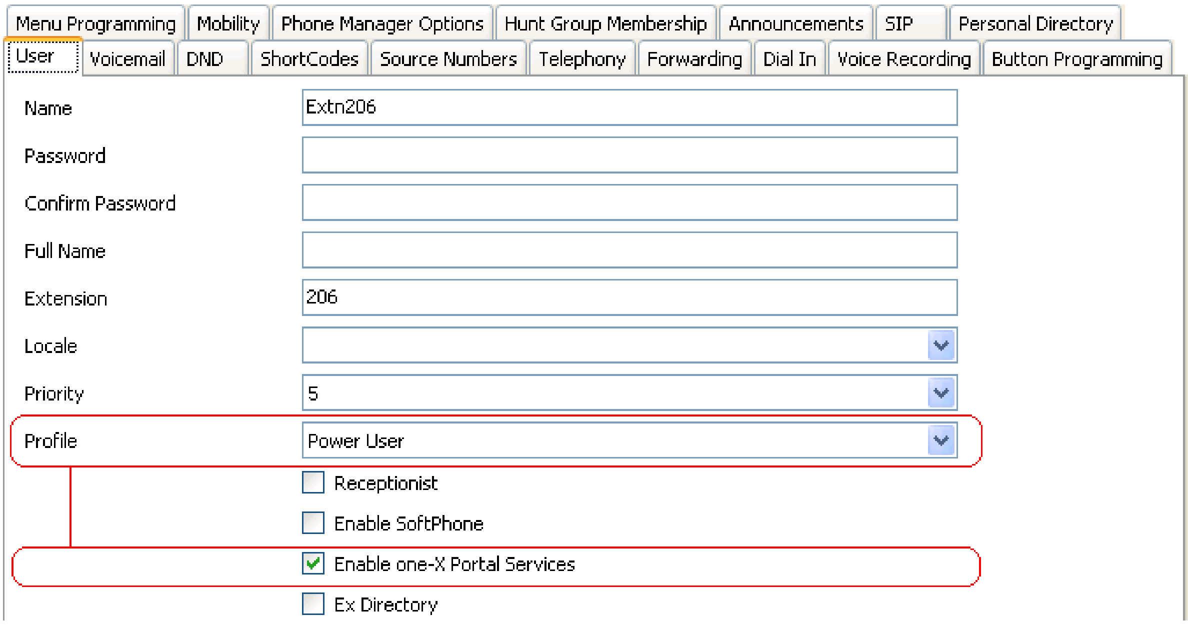
To do that requires the matching licenses or subscriptions in the system configuration.

4.2 Enabling one-X Portal for IP Office Users

Those users who want to use the one-X Portal for IP Office application need to have their **Profile** set to ***Office Worker***, ***Teleworker***, ***Power User*** or ***Unified Communications User***. The user's **Enable one-X Portal Services** option can then be enabled.

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.



Name	Extn206
Password	
Confirm Password	
Full Name	
Extension	206
Locale	
Priority	5
Profile	Power User

☐ Receptionist

☐ Enable SoftPhone

☑ Enable one-X Portal Services

☐ Ex Directory

6. Change the user's **Profile** to ***Office Worker***, ***Teleworker***, ***Power User*** or **Unified Communications 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.

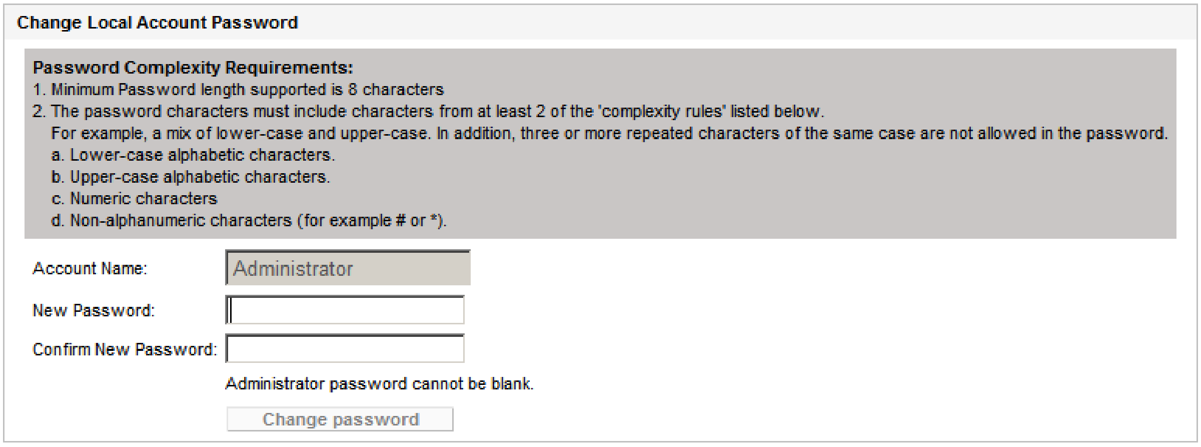
4.3 Initial one-X Portal for IP Office Login

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.



Change Local Account Password

Password Complexity Requirements:
1. Minimum Password length supported is 8 characters
2. The password characters must include characters from at least 2 of the 'complexity rules' listed below.
   For example, a mix of lower-case and upper-case. In addition, three or more repeated characters of the same case are not allowed in the password.
   a. Lower-case alphabetic characters.
   b. Upper-case alphabetic characters.
   c. Numeric characters
   d. Non-alphanumeric characters (for example # or *).

Account Name: Administrator

New Password:

Confirm New Password:

Administrator password cannot be blank.

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 9.
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.

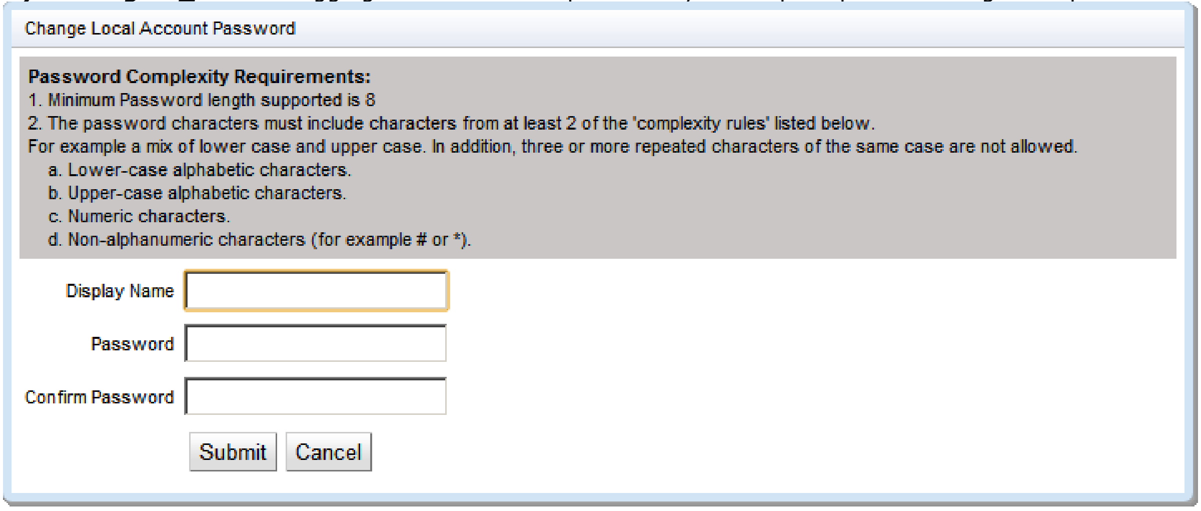
4.4 Initial AFA Login

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:



Change Local Account Password

Password Complexity Requirements:
1. Minimum Password length supported is 8
2. The password characters must include characters from at least 2 of the 'complexity rules' listed below.
For example a mix of lower case and upper case. In addition, three or more repeated characters of the same case are not allowed.
a. Lower-case alphabetic characters.
b. Upper-case alphabetic characters.
c. Numeric characters.
d. Non-alphanumeric characters (for example # or *).

- **Display Name**
  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 Portal Service Status Remains Yellow

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

The mismatch is between the **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 is using the default password.

To reset the portal and IP Office passwords:

1. Change the portal provider passwords to the new, strong password:
    a. Login to the portal services administrator menus. You can do this by logging in to the portal server's Web Manager menus, clicking on Applications and selecting one-X Portal.
    b. Click **Configuration** and select **Providers**.
    c. Set the **Provider Name** field to ***Telephony (CSTA)***.
    d. Click on the ✎ edit icon next to the listed provider.
    e. Set the **Password** and click **Save**.
    f. Set the **Provider Name** field to ***Directory (IP-Office)*** and repeat the process.
2. Stop the one-X Portal for IP Office service:
    a. Login to the server's web manager menus.
    b. From the Solution page, click on the ☰ icon next to the portal server and select **Platform View**.
    c. Stop the **one-X Portal** service. Wait until the status icon changes to red.
3. Change the password of the IP Office EnhTcpaService service user:
    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** to the same as was set for the portal providers above and click **Save**.
    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 10 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 10 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

This section covers basic maintenance tasks.

- Logging In 49
- Logging Into Web Control Directly 50
- Viewing the Module IP Address 51
- Changing the IP Address Settings 51
- Module LEDs 52
- Module Buttons and Ports 55
- Attaching a Monitor and Keyboard 55
- Using System Status Application 56
- Upgrading the Module 57
- Starting/Stopping Application Services 65
- Changing the Linux Passwords 66
- Shutting Down the Server 67
- Rebooting the Server 67
- Date and Time Settings 68
- Creating Administrator Accounts 69
- Setting the Menu Inactivity Timeout 69
- Uninstalling an Application 70
- Setting Up File Repositories 72
- Downloading Log Files 75
- SSH File Transfers 76
- Adding TTS Languages 77

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 Edge** / **Mozilla Firefox** / **Google Chrome** / **macOS 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.

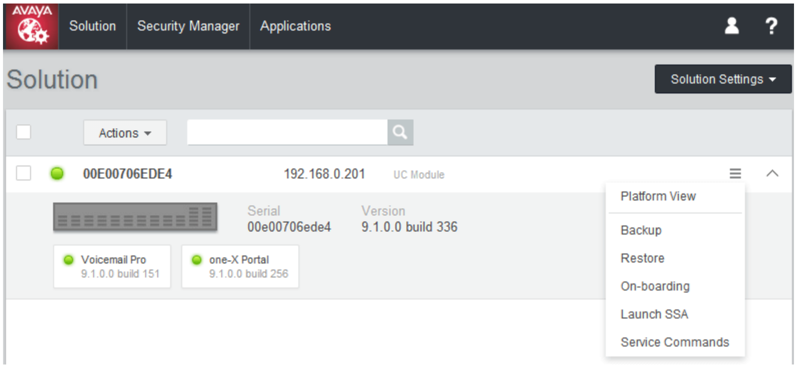
   c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. Note that this does not change the Linux ***root*** and ***Administrator*** account passwords.

   - ***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.

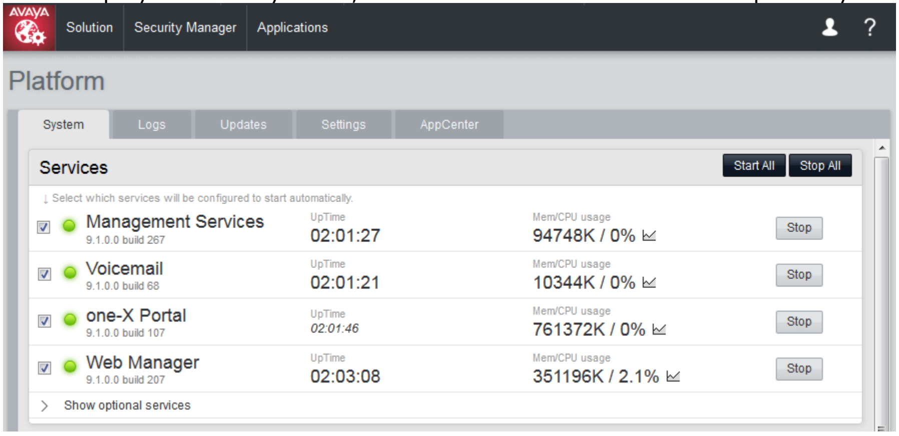
   - ***Change Security Administrator Password***
     This sets the password for the Management Services security administrator account.

   - ***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**.



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

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 49 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 Edge** / **Mozilla Firefox** / **Google Chrome** / **macOS 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 51.
   - 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** 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.

The module's IP address can be checked in both System Status Application 56 and IP Office Manager.

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 known as "platform view"), you can change the server's network settings.

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

- *** IMPORTANT: Security Certificate Field** - Fields marked with a * symbol are used as part of the default security certificate generated by the server. If changed, the server generates a new default certificate, during which time access to the server is disrupted for several minutes. In addition, any applications using the certificate need to be updated with the new certificate.

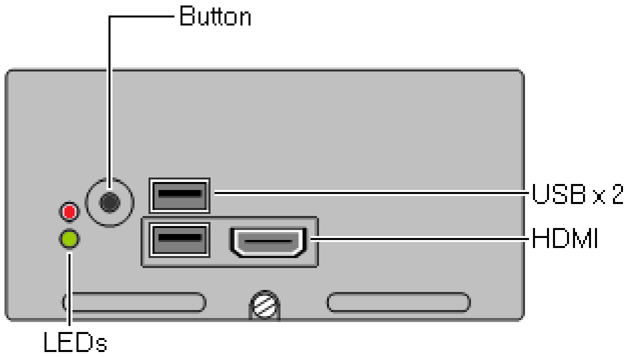
To change the IP address:

1. Login 49 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***.
   - **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***.
     - For internal use, this value must be reachable by DNS within the customer network. If also supporting external client connections, it needs to be reachable by external DNS. Consult with the customer's IT support to ensure the name is acceptable and that routing to it has been configured correctly. External access must also include a firewall and/or SBC.
   - **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 10.
   - **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**
     This control is not supported on the Unified Communications Module and so is greyed out.
5. Click **Save**. The server restarts.

5.5 Module LEDs

Unified Communications Module v2

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



Unified Communications Module v2

- ○ **Off**, 🔴 **On**, ✳ **Flashing** (0.5 seconds on/0.5 seconds off), ◐ **Alternating** (Amber/Green - 1 second per) (Red/Amber - 0.5 second per)
- 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** column below refers to the corresponding module status shown for an Unified Communications Module v2 in System Status Application 56.

Shutdown Sequence LEDs

	LEDs		Description	Status
Shutting Down*	✳	Flashing green	Indicates that the module is shutting down. The shutdown has two phases. A slow flash is used while the applications are shutting down, followed by a fast flash for the hardware 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. See also 'IP Office power up' and 'Module not supported' below.	–
	🔴	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 23 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 and correctly licensed 18 for the release it is running.	*Errored*
	🔴	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.*
	◐	Amber-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 crash*	✳	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*	◐	Amber-green	Installing or upgrading the module. For an USB install or upgrade, System Status Application also shows a progress bar in 5% increments (these are also reported in IP Office System Monitor).	*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		
Ignition required*	○	Off	For a newly installed module, the module has started but module service ignition 23 has not been complete.	*Idle, card has not been ignited*
	🟢	Green		

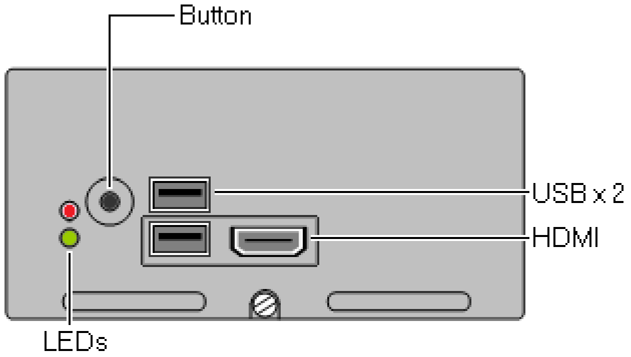
USB Install/Upgrade Fault LEDs

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		

5.6 Module Buttons and Ports

The Unified Communications Module provides the following buttons:



Unified Communications Module v2

Buttons

- **Button**
  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.

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.

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 adapter. Note that the module only activates the video port if it detects a monitor whilst restarting.

5.8 Using System Status Application

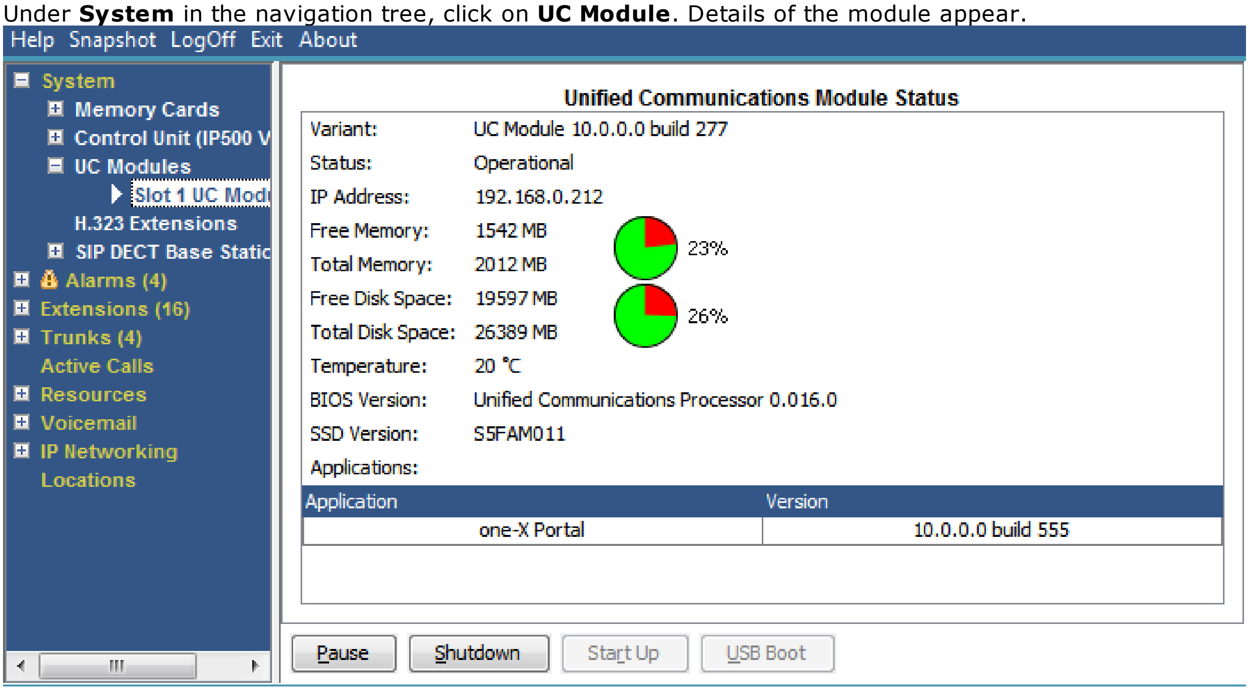
System Status Application displays the status of the Unified Communications Module, for details see Module LEDs 52. For the module error states, it also creates an appropriate alarm in System Status Application. It also provides controls to shutdown and start the module. including a reboot from USB.

To check a Unified Communications Module using System Status Application:

1. Using System Status Application, access the system.

2. Select **System**.

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



Unified Communications Module Status

Variant: UC Module 10.0.0.0 build 277
Status: Operational
IP Address: 192.168.0.212
Free Memory: 1542 MB
Total Memory: 2012 MB
Free Disk Space: 19597 MB
Total Disk Space: 26389 MB
Temperature: 20 °C
BIOS Version: Unified Communications Processor 0.016.0
SSD Version: S5FAM011
Applications:

Application	Version
one-X Portal	10.0.0.0 build 555

4. You can use the buttons are the bottom of the menu to control module operation in the following ways:

- **Pause**
  Pause menu updates. The button changes to **Resume** which restarts updates.

- **Shutdown**
  Shutdown the module.

- **Start Up**
  Start a module that has been shutdown.

- **USB Boot**
  Instructs a module that has been shutdown to boot from an attached USB memory key.

5.9 Upgrading the Module

Avaya makes an C110 ISO file available for each IP Office release. You can use this for upgrading modules.

- For modules being used by subscription mode systems, upgrading directly from Customer Operations Manager (COM) is support.

  - **! WARNING - Not Supported for Upgrades from Pre-R12.0**
    This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.

  - **! 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 81.

5.9.1 Web Manager Upgrade

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 C110 ISO file. Do not use other ISO files such as Server Edition ISO images.

- **! WARNING - Not Supported for Upgrades from Pre-R12.0**
  This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.

- **! Upgrade Warning**
  Upgrading 57 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.

Process Summary

1. **Upgrade the IP Office System**
   The IP Office system must be upgraded to the target software release before the module is upgraded, including the addition of any necessary upgrade licenses.

   - **Preferred License Change**
     On pre-IP Office Release 10 systems, the Unified Communications Module v1 granted the host system a virtual **Preferred Edition** license. That no longer applies for IP Office Release 10 and higher. Any systems being upgraded to IP Office Release 10 or higher must use the IP Office license migration process to retain the existing license.

2. **Download the software** 16
   Download the R11.1 USB creator software and C110 ISO image.

3. **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.

5. **Transfer the ISO image**
   Use one of the possible methods to transfer the ISO image to the module.

   - **Transfer from a remote file server** 59
   - **Transfer from a module path** 60
   - **Transfer from the browser** 60
   - **Transfer from a USB upgrade key** 61

6. **Upgrade the module** 61
   Select the upgrade server option in the Web Manager menus.

7. **Check operation** 80
   Log in to the server.

5.9.1.1 ISO Transfer from a Remote File Server

You can upload an ISO image to the server from a previously configured file server *(http, https, ftp, sftp* or *scp)*. 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 50 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**. 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 49 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 61.

5.9.1.2 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 server. 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 server path:

1. Login 49 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 ***Server Path***.
    a. In the **File path** field, enter the path to the previously uploaded ISO image. For example, ***/home/Administrator/abe-10.0.0.168.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 61.

5.9.1.3 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 49 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. From 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 61.

5.9.1.4 ISO Transfer from USB

You can copy an ISO file from a USB memory key inserted into one of the server's USB ports. This does not require the ISO file to be unpacked on the USB key.

To transfer the ISO from a USB Memory Key:

1. Login[49] 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. From 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[61].

5.9.1.5 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.

- **! WARNING - Not Supported for Upgrades from Pre-R12.0**
  This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.
- **Scheduled Upgrades**
  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[9].
- **No Application Services Available During Upgrades**
  During the upgrade, the services (one-X Portal for IP Office, Voicemail Pro and web control) are stopped and not restarted until after the module reboots.

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**
      Multi-server 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.

5.9.2 USB Upgrade

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

- **! WARNING - Not Supported for Upgrades from Pre-R12.0**
  This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.

- **! Upgrade Warning**
  Upgrading 57 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.

Process Summary

1. **Upgrade the IP Office System**
   The IP Office system must be upgraded to the target software release before the module is upgraded, including the addition of any necessary upgrade licenses.

   - **Preferred License Change**
     On pre-IP Office Release 10 systems, the Unified Communications Module v1 granted the host system a virtual **Preferred Edition** license. That no longer applies for IP Office Release 10 and higher. Any systems being upgraded to IP Office Release 10 or higher must use the IP Office license migration process to retain the existing license.

2. **Download the software** 16
   Download the R11.1 USB creator software and C110 ISO image.

3. **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.

5. **Prepare the USB upgrade key** 63
   Using the downloaded software, create a bootable USB upgrade key from the downloaded ISO image.

6. **Reboot the module** 64
   Reboot the module from the USB upgrade key and let the module upgrade.

7. **Check operation** 80
   Log in to the server menus.

5.9.2.1 Preparing a USB Upgrade Key

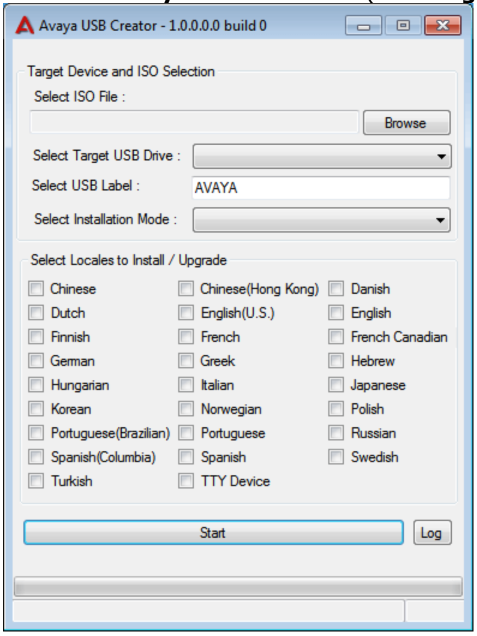
This process uses a downloaded ISO image to create a bootable USB memory key for software upgrading. You can then use the memory key for an upgrade by rebooting from USB 64 or you can transfer its contents to the module for a scheduled web manager upgrade 58.

Prerequisites

- **6GB USB Memory Key**
  Note that this process reformats the memory key and erases all existing files.
  - **64GB+ Memory Keys**
    This process can only be used with USB memory keys smaller than 64GB. For larger keys, see Creating a USB Key using Rufus 84.
- **Avaya USB Creator Tool**
  This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade. Note: You must use the R11.1 version of this tool for R11.1 and higher systems.
- **Unified Communications Module ISO Image**
  You can download this file from the Avaya support website, see Downloading Module Software 16.

To create a bootable USB memory key:

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



Avaya USB Creator - 1.0.0.0 build 0

Select USB Label : AVAYA

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

5.9.2.2 Booting from a USB Upgrade Key

Use the following process to reboot from a USB upgrade 63 key.

- **! WARNING - Not Supported for Upgrades from Pre-R12.0**
  This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.

To upgrade from a USB memory key:

1. Connect to the IP Office using System Status Application. Select **System | UC Modules** and select the module. The page shows the module status and other information.
2. Insert the USB memory key with the new ISO image file into the module's upper USB port.
3. The next step requires the module to boot from the USB memory key. This can be done in two ways:
   - **Using the module buttons:**
     Shut down the module by pressing the upper button on the module until the upper 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. Restart the module by pressing the upper button again and keeping it pressed until the two LEDs change from amber to off.
   - **Using System Status Application:**
     Click on the **Shutdown** button. Once the module has shut down, click the **USB Boot** button.
5. After up to 2 minutes initializing, the module boots using the files on the USB memory key. System Status Application should report *"USB Upgrade/Install"* and both upper and lower LEDs flash amber/green.
6. The progress of the software installation/upgrade is shown in System Status Application. The initial software installation process between 15 to 80 minutes depending on the number of languages being installed.
7. 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. 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 module automatically shutdown after a firmware upgrade. Restart the module by pressing the top button or using System Status Application 56.
   - **Lower status LED green except for regular IP Office heartbeat flashes:**
     This indicates that the module restarted without needing a firmware upgrade.
8. Login to the module via its IP Office Web Manager menus 81 and check the status of the services.
9. Remove the USB memory key.

5.10 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.

5.10.1 Starting a Service

Note that some services are linked and so cannot be started or auto-started if the other related service is not also started or set to auto-start.

To start a service:

1. Login 49 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.

5.10.2 Stopping a Service

Note that some services are linked and so cannot be started or auto-started if the other related service is not also started or set to auto-start.

To stop a service:

1. Login 49 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**.

5.10.3 Setting a Service to Auto Start

Note that some services are linked and so cannot be started or auto-started if the other related service is not also started or set to auto-start.

To set a service to auto start:

1. Login 49 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.

5.11 Changing the Linux Passwords

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

- These settings are only accessible if logged in via referred authentication 12 or as the local Linux root. Therefore, when disabled, the setting can only be re-enabled by logging in using the local Linux root name and password.

To change the server's Linux account passwords:

1. Login 49 to the server's web configuration menus.

2. Select **Settings** and click on the **System** tab.

   - Use the **Change root Password** section to set the new password for the root account.

   - 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.

3. In both cases, you must first enter the existing password and then enter and confirm the new password. The new password must conform to the password rules settings.

4. After entering the old and new passwords, click **Save**.

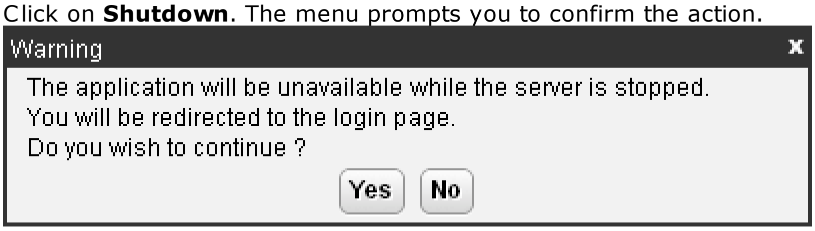
5.12 Shutting Down the Server

For the Unified Communications Module, you can shutdown or restart the module using its buttons 55 or System Status Application 56, 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 20.

To shutdown the server:

1. Login 49 to the server's web configuration menus.
2. After logging in, select the **System** page.
3. Click on **Shutdown**. The menu prompts you to confirm the action.


Warning

The application will be unavailable while the server is stopped.
You will be redirected to the login page.
Do you wish to continue ?

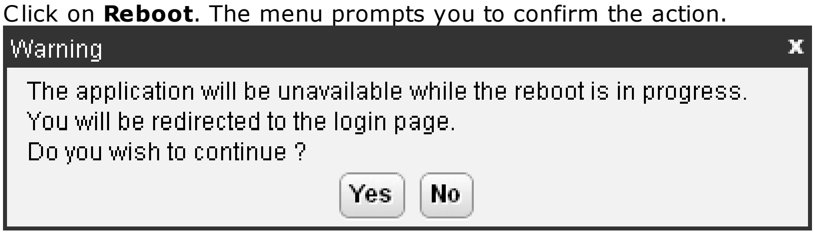
4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 2 minutes, the server shuts down.

5.13 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** 65 automatically restart after the reboot.

To reboot the server:

1. Login 49 to the server's web configuration menus.
2. After logging in, select the **System** page.
3. Click on **Reboot**. The menu prompts you to confirm the action.


Warning

The application will be unavailable while the reboot is in progress.
You will be redirected to the login page.
Do you wish to continue ?

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**.

5.14 Date and Time Settings

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

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 49 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.
   - **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.
   - **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**.

5.15 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.

5.16 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 49 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.

5.17 Upgrading

The preferred method for upgrading servers and server applications is to use the Web Manager menus 80. However, you can use the previous web control methods for legacy installations.

You can upgrade individual application services without having to reinstall or upgrade the whole server. This is done using either an .rpm file or a .zip file of multiple .rpm's uploaded to the server (local) or downloaded by the server from an HTTP folder (remote repository), see File Repositories 72.

Once an .rpm file or files are available, the Unified Communications Module web configuration pages will list the available versions and allow switching between versions or simple upgrading to the latest version.

- **! WARNING - Not Supported for Upgrades from Pre-R12.0**
  This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.

- **! Upgrade Warning**
  Upgrading 57 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.

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

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

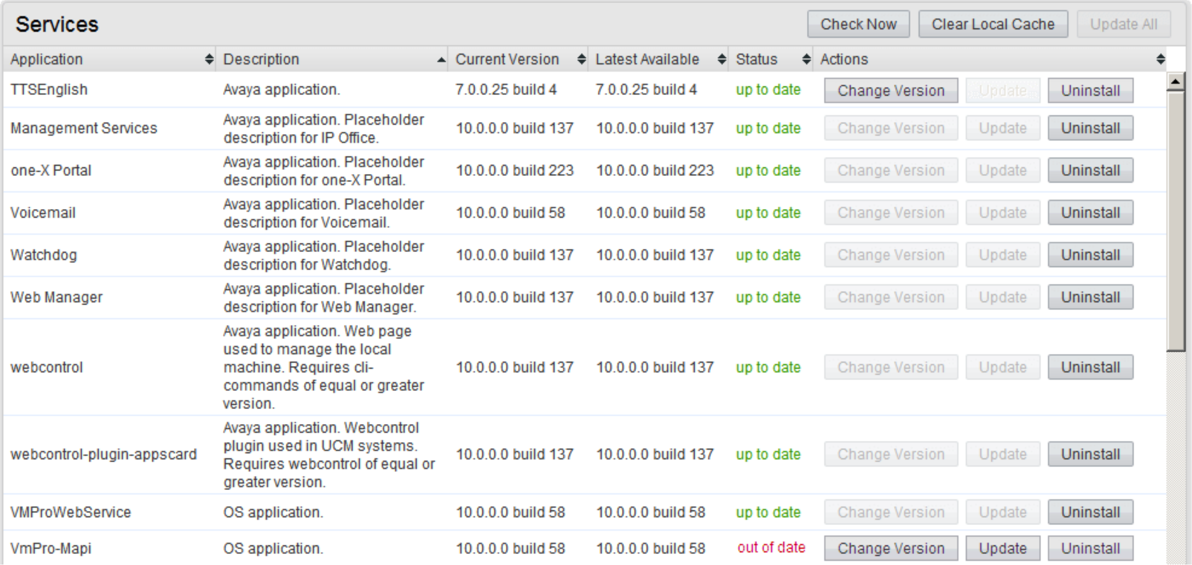
5.18 Uninstalling an Application

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 49 to the server's web configuration menus.
2. Select the **Updates** page.



Services

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

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

- If there are installation files for the application in the application file repository, 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.

5.19 Setting Up File Repositories

The **Updates** and **Web Client** 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.

5.19.1 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.

- **! WARNING - Not Supported for Upgrades from Pre-R12.0**
  This method of upgrading is not supported for upgrading from pre-R12.0 releases. For example, from R11.1 to R12.0. The sever must be upgraded using the processes in the **Upgrading Linux-Based IP Office Systems to R12.0** manual.

- **! Upgrade Warning**
  Upgrading 57 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.

		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** 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.

5.19.2 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** and **AppCenter** 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. 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.

5.19.3 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** menu.

- **Operating System**
  These are files used by the Linux operating system and its services.

5.19.3.1 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[74].

- **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[49] 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[72] 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.

5.19.3.2 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[49] 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[72] 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.

5.19.3.3 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[49] 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[72] 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.

5.19.4 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 72 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.

5.20 Downloading Log Files

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

To create archive files:

1. Login 49 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**.

5.21 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**.

5.22 Adding TTS Languages

The Voicemail Pro application can use Text-to-speech (TTS). However, the IP Office image file used to create virtual machines does not include the TTS languages. The TTS languages are downloadable as 3 separate DVD's.

To use TTS languages, you need to upload and install the additional languages on the virtual machines running the Voicemail Pro application. In a Server Edition network, that applies to the Server Edition Primary Server and Server Edition Secondary Server servers.

- **! WARNING**
  - TTS files from pre-11.1 releases are not compatible with R11.1.
  - During this process, the server needs to restart the voicemail service each time it installs a new TTS language.

Checking the TTS Languages Installed

1. Access the server's web control/platform view menus. See Logging In 49 or Logging Into Web Control Directly 50.
2. Select **Updates**.
3. In the list of **Services**, each TTS language is shown with the prefix ***TTS***.

Downloading the TTS Languages

1. The supported TTS languages can be downloaded as a set of 3 ISO files from support.avaya.com. See Downloading Module Software 16.
2. Select the IP Office release and locate the ***Text-to-Speech for IP Office Server Edition and Application Server*** link.
3. Download the ISO image containing the languages required:
   - **DVD 1:** English, Spanish, French, German, Italian.
   - **DVD 2:** Swedish, Norwegian, Finnish, Dutch, Danish, Portuguese, Greek.
   - **DVD 3:** Chinese, Polish, Russian.
4. The individual RPM installation files for each file can be extracted from the ISO files by treating them as zipped archives.

Adding a New Language

Note that this process will cause the voicemail service to be restarted, ending all calls currently being handled by the voicemail service.

1. Access the server's web control/platform view menus. See Logging In 49 or Logging Into Web Control Directly 50.
2. Select **Settings | General**.
3. In the **Software Repositories** section, click on the **Browse** button for **Application**. Browse to and select the RPM file for the required language and click **OK**.
4. Click **Add**.
5. Select **Updates**.
6. In the **Services** section, locate the newly added TTS language. Click **Install**.

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 9.

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 81.

- **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 Edge** / **Mozilla Firefox** / **Google Chrome** / **macOS 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.

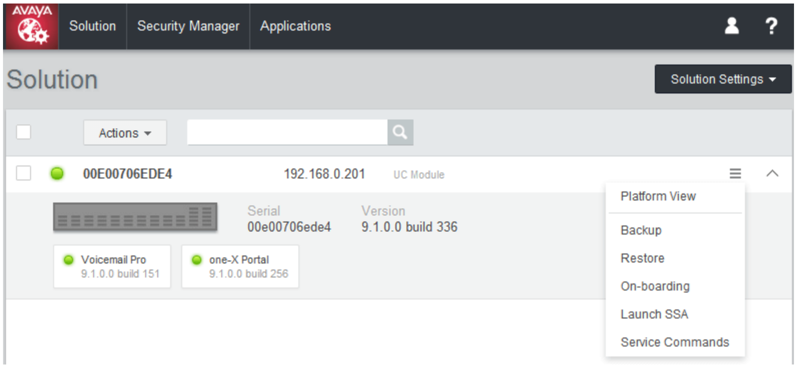
   c. If any of the Management Services passwords are default, the server requests you to change those passwords. For a new server, the passwords are set during ignition. Note that this does not change the Linux ***root*** and ***Administrator*** account passwords.

   - ***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**.



00E00706EDE4 192.168.0.201 UC Module

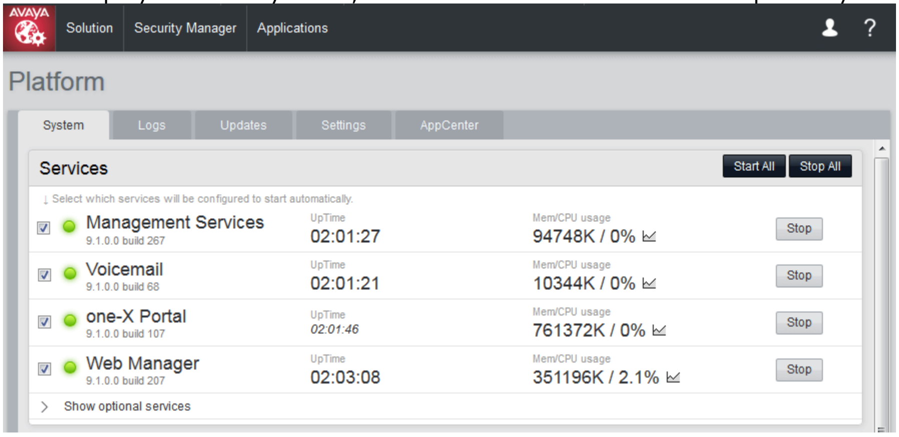
Serial: 00e00706ede4

Version: 9.1.0.0 build 336

Voicemail Pro 9.1.0.0 build 151

one-X Portal 9.1.0.0 build 256

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



↓ Select which services will be configured to start automatically.

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

Chapter 7. Addendum

7. Addendum

- Creating a USB Key using Rufus 84

7.1 Creating a USB Key using Rufus

The Avaya USB Creator utility cannot be used with 64GB and larger USB memory keys. When that is the case, use the following process.

- **! WARNING**
  This process will erase all existing files and folders on the USB key without any chance of recovery.

Tools & Equipment Required:

- **Rufus USB Creation software**
  The Avaya USB Creator software application cannot be used for the R11.0.4.5 to R11.1 SP2 upgrades of PC-based servers. Instead, downloaded and use Rufus from https://rufus.ie/.

- **IP Office USB PC ISO File**
  This ISO file's name is prefixed with "*c110*" followed by the IP Office version.

Process

1. Insert the USB memory key into a Windows PC.
2. Start Rufus.
3. Use the **Device** field to select the USB memory key.
4. Click **SELECT** and select the ISO file.
   - Ensure that you select the correct ISO file. For PC servers, the file name is prefixed with "*c110*" followed by the software version.
5. Select the following other options:
   a. **Volume label:** Change this to ***AVAYA*** with no quotation marks.
   b. **File System:** Leave this as ***FAT32***.
6. Click **Start**.
7. The progress of the unpacking of the ISO file onto the USB memory key is displayed. Allow this process to continue without any interruption. It takes approximately 4 to 10 minutes depending on the size of the USB memory key.
8. When Rufus has completed the process and shows "*READY*", click **CLOSE**.
9. Open the USB memory key in file manager.
10. Open the USB folder.
    a. **For an installation key:** Copy and paste the *avaya_autoinstall.conf* and *syslinux.cfg* files to the root folder of the USB memory key.
    b. **For an upgrade key:** Copy and paste the *avaya_autoupgrade.conf* and *syslinux.cfg* files to the root folder of the USB memory key.
       - **! WARNING**
         Do not copy any other files. Copying any other files will cause the USB to run a new install, erasing all existing files on the server.
11. The USB upgrade key is now ready for use.

Index

1

169.254.0.1 10
169.254.0.2 10

A

Additional documentation 9
Address
  DNS 51
  IP 51
Administrator
  Login 40
Application
  Auto-start 65
  Install 70
  Repositories 72
  Start 65
  Stop 65
  Uninstall 70
  Upgrade 70
Application files
  Upload files 73
Attach
  Monitor and keyboard 55
Auto-start 65

B

Backup
  Custom folders 38
  one-X Portal for IP Office 45
  Voicemail 36
Boot
  from USB 22, 64
Browser 11
Bulletins 9
Buttons 55

C

Change
  IP Address 51
Configuration
  one-X Portal for IP Office 40
  Voicemail Pro 30
Create a USB device 17, 63
Custom folders
  Backup/restore 38

D

Date 68
Default
  Gateway 51
  Password 50
DHCP 51
DNS 51
Download
  Software 16

E

Enable Traffic Control 51

G

Gateway 51

H

Host Name 51

I

Inactivity timeout 69
Initial configuration 40
Install
  Application 70
  Service 70
Interface 51
IP Address 32, 51
IP Office
  Check 40
  Select 40
ISO 16

J

Javascript 11

K

Keyboard 55

L

LAN2 10
Linux 9
Logging In 50
Login 34, 50
  Administrator 40

M

Mask 51
Menus
  Inactivity timeout 69
Module
  Buttons 55
  Restart 67
  Shutdown 67
Monitor 55

N

NAT 10
Network 51
  Change IP address 51
Network Time Protocol 68
no Remote 34
NTP 68

O

one-X Portal for IP Office
  Auto-start 65
  Backup/restore 45
  Configuration 40
  Start 65
  Stop 65
Operating system
  Repositories 72
  Upload files 73

P

Password
  Change 40
  Default 50
  Root password 66

R

Reboot 67
Related documents 9
Remote Software Repositories 74
Repositories 72, 74
Restart 67
Restore
  Custom folders 38
  one-X Portal for IP Office 45
  Voicemail 36
Root password
  Change 66

RPM 16

S

Server
- NTP 68
- Reboot 67
- Shutdown 67

Server Name 34

Service
- Auto-start 65
- Install 70
- Start 65
- Stop 65
- Uninstall 70
- Upgrade 70

SFTP 76

Shutdown 67

Software 34
- Downloading 16
- Install from USB 22, 64
- Repositiories 72
- Repositories 74
- Unetbootin 16, 17, 63
- USB 16, 17, 63

SSH access 76

Start 67
- Auto-start 65
- Service 65

Stop
- Service 65

Subnet Mask 51

Supported
- Browsers 11

syslinux.cfg 17, 63

T

Technical bulletins 9

Time
- Timezone 68

Timeout 69

Traffic Control 51

Transfer an ISO file
- Direct upload 60
- Remote file server 59
- SSH/SFTP transfer 60

U

Uninstall
- Application 70
- Service 70

Unit Name/IP Address 34

Upgrading Applications 70

Upload
- Application files 73
- Operating system 73
- Windows client files 73

USB
- Create a bootable... 17, 63
- Load software 22, 64
- Software 16, 17, 63

USB Initiator 16

V

Virtual DVD
- Direct upload 60
- Remote file server 59
- SSH/SFTP transfer 60

Voicemail
- Auto-start 65
- Backup/restore 36
- Start 65
- Stop 65

Voicemail IP Address 32

Voicemail Pro
- Configuration 30

Voicemail Pro Client
- run 34

Voicemail Pro Client window 34

Voicemail Pro Login window 34

Voicemail Pro Server
- connect 34

Voicemail Type 32

W

WAN 34

Web browser 11

Windows client
- Repositories 72

Windows client files
- Upload files 73

Workstation 34

Template: 20th December 2023