IP Office 9.0

IP Office Application Server 9.0 Installation and Maintenance

15-601011 Issue 07l - (27 January 2014)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents

1. IP Office Application Server

2. Application Server Software Installation

3. Pre-Built Application Server Installation

4. Voicemail Pro Configuration

5. one-X Portal for IP Office Configuration

6. Server Maintenance

7. Server Menus

8. Additional Processes

9. Document History

Chapter 1.
IP Office Application Server

1. IP Office Application Server

The IP Office Application Server is a single installation of selected IP Office 9.0 applications running on Linux. The Linux operating system is included as part of the installation. However, installation requires minimal Linux knowledge due to the inclusion of a web based management interface to allow the server to be managed remotely via web browser.

The IP Office Application Server installation installs the following components:

- **Linux**
  This is the base operating system used by the server. However, no specific Linux knowledge is required for server installation and maintenance.
  - **Web Manager**
    Server settings are configured and managed via web browser access to the web control menus detailed in this document.
  - **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 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 user's can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely using web browser access. Each user who wants to use one-X Portal for IP Office requires a license 14.
  - **Voicemail Pro**
    This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system. In addition, you can customize it to provide a range of call routing and voicemail services. Maintainers use the Windows Voicemail Pro client, downloadable from the server, to remotely configure the service. Licenses set the number of simultaneous connections to voicemail.
  - **Contact Recorder for IP Office**
    Contact Recorder for IP Office is an application used in conjunction with Voicemail Pro. It provides long term storage and retrieval of call recordings. The call recordings are made by Voicemail Pro. Those recordings and call details are then collected by Contact Recorder for IP Office and stored by it. For details on Contact Recorder for IP Office installation, refer to the Contact Recorder for IP Office Installation Manual.
    - The Contact Recorder for IP Office application should only be run on a separate application server. It should not be run on the same server as the Voicemail Pro application.

Installation Options

The IP Office Application Server can be supplied either pre-installed onto a suitable server or as a DVD for installation onto a customer supplied server. Both options are covered by this manual.

Linux is a registered trademark owned by Linus Torvalds.

1.1 Avaya Pre-Built Servers

The IP Office Application Server can be supplied pre-installed onto a suitable server. The general specification of the servers used is:

- **Form:** Rack mounted server PC.
- **RAM:** 12GB.
- **Hard Disk:** 250GB.
- **Ethernet Port:** Only a single port (eth0) is supported. This port is labeled as port 1 on the physical server.

Default Settings

The following are the default settings applied to the server applied shipment from Avaya:

- **DHCP Mode:** Off
- **IP Address:** 192.168.42.1
- **NetMask:** 255.255.255.0
- **Gateway:** Blank
- **Hostname:** The server MAC address.
- **DNS1:** Blank
- **DNS2:** Blank
- **Time Zone:** EST - Eastern Standard Time.
- **Root User Password:** Administrator

Applications Installed

- **Voicemail Pro**
  - **English and French Language TTS for Voicemail Pro**
- **one-X Portal for IP Office**

1.2 Non-Avaya Server Requirements

The following are the minimum server PC requirements.

- **IMPORTANT: Compatible Servers**
  Avaya cannot guarantee the compatibility of any particular server PC for the operating system. It is the installer's responsibility to ensure that the server platform is compatible. A list of tested servers is available at https://hardware.redhat.com/. The servers used by Avaya for product testing are:

  - HP ProLiant DL160
  - Dell Optiplex 780MT

	Minimum Specification	Recommended Specification
Processor	Intel 64-bit Dual Core 2.4GHz	Intel Pentium 64-bit Quad Core 2.4GHz or AMD Athlon 64 4000 + or equivalent.
RAM Memory	4GB	4GB
Hard Disk Space	30GB	30GB.

- **Operating System**
  The IP Office Application Server installs a Linux operating system, replacing any existing operating system on the PC.

- **Drives**
  DVD Drive for software installation. For Contact Recorder for IP Office, a DVD+RW or Blue Ray -R disc drive is recommended.

- **Other Requirements:**

  - The server PC must be configurable to boot from DVD or USB in order to overwrite any existing OS. This may require access to the BIOS in order to change the boot order of the PC.
  - The IP Office Application Server operates as a headless server, i.e without requiring any keyboard, video and mouse (KVM) connections after initial installation. Users and maintainers access the server remotely from other PCs.

1.3 Using Linux

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

1.4 Additional Documentation

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

Related Documents

- **one-X Portal for IP Office Administration Manual**
  This manual covers the installation and administration menus used for the one-X Portal for IP Office application. This manual is essential if the one-X Portal for IP Office needs configuring to support multiple IP Office servers in a Small Community Network.

- **Voicemail Pro Installation Manual**
  This manual covers voicemail server configuration and scenarios including multiple servers within a Small Community Network. Those scenarios can include a mix of Windows based and Linux based servers.

- **Voicemail Pro Administration Manual**
  By default the voicemail server provides mailbox services to all users and hunt groups without any configuration. This manual covers the administration of the voicemail server using the Voicemail Pro client in order to enable additional features.

- **IP Office Manager Manual**
  IP Office Manager is the application used to configure the IP Office application. This manual details how to use IP Office Manager and the full range of IP Office configuration settings.

- **Contact Recorder for IP Office Installation**
  Covers the additional steps required for installation and basic operation of the Contact Recorder for IP Office application.

- **Administering Contact Recorder for IP Office**
  Administration and operation of the optional Contact Recorder for IP Office service.

- **Using Contact Recorder for IP Office**
  Covers the use of Contact Recorder for IP Office.

Technical Bulletins

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

Other Documentation and Documentation Sources

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

- **Avaya Support Web Site** - http://support.avaya.com

- **Avaya IP Office Knowledge Base** - http://marketingtools.avaya.com/knowledgebase

1.5 Network Configuration Limitations

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

Scenarios where users of the one-X Portal for IP Office application are accessing it from the IP Office's other LAN should be avoided for more than 30 users.

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

1.6 Small Community Networks

Up to 32 IP Office systems can connect using H323 SCN trunks to form a Small Community Network, supporting up to 1000 users.

When installing a IP Office Application 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. The application can support up to 500 simultaneous one-X Portal for IP Office users. Following installation of the IP Office Application Server with one-X Portal for IP Office application on it, addition configuration steps are required to configure the one-X Portal for IP Office application with details of the other IP Office systems. Refer to the one-X Portal for IP Office Installation Manual.

- **Voicemail Pro**
  In an Small Community Network, one Voicemail Pro server stores all mailboxes and their related messages, greeting and announcements. Additional Voicemail Pro servers installed in the network perform other specific roles. For full details, refer to the Voicemail Pro manuals.

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

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

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

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

1.7 Licenses

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

- **Essential Edition**
  This license is a pre-requisite for the **Preferred Edition** license below.

- **Preferred Edition (Voicemail Pro)**
  This license is required for use of the Voicemail Pro application. It also enables 4 voicemail ports. It is also required as a pre-requisite for the user profile licenses required for one-X Portal for IP Office users.

- **Preferred Edition Additional Voicemail Ports**
  These licenses add additional voicemail ports in addition to the 4 enabled by the **Preferred Edition (Voicemail Pro)** license above.

- **Messaging TTS Pro**
  This license enables the use of text-to-speech facilities using the optional Linux TTS software and user email reading. One license per simultaneous instance of TTS usage.

- **User Profile Licenses**
  In order to log into and use the one-X Portal for IP Office application, a user must be configured and licensed to one of the following user profile roles in the IP Office configuration: ***Office Worker***, ***Teleworker*** or ***Power User***. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

1.8 Voicemail Pro Features

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

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

1.9 Supported Web Browsers

Avaya supports the following web browsers:

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

1.10 Password Authentication

For IP Office Release 9.0 and higher, the password authentication for access to the web control menus is done either against the web control menus' own database or against the security user accounts provided for IP Office Web Manager. You can select which is used using the **Enable referred authentication** setting in the web control menus (Settings | System 91).

- **Enabled**
  When **Enable referred authentication** is enabled, access to the web control menus is control by the IP Office Web Manager security settings. This allows you to access the web control menus from within IP Office Web Manager without needing to re-authenticate. You can still direct access the web control menus but only using the IP Office Web Manager names and passwords.

- **Disabled**
  When **Enable referred authentication** is not enabled, access to the web control menus is controlled by web control's own settings. Web control cannot be accessed through IP Office Web Manager except by launching it in a separate browser window and entering the separate web control name and password.

Upgrading

The authentication used when a server is upgraded from pre-IP Office Release 9.0 depends on the current status of the Administrator password:

- If the Administrator password is still default, Enable referred authentication is selected by default.
- If the Administrator password is not default, Enable referred authentication is not selected by default.

Chapter 2.

Application Server Software Installation

2. Application Server Software Installation

This section covers the installation of the IP Office Application Server software onto a customer supplied server PC. This process uses various software packages downloaded from Avaya to create an installation DVD or bootable USB2 memory key.

2.1 Downloading Software

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

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

  - **! Upgrade Warning**
    Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.

  - **! Backup Application Data**
    In all cases, always backup all application data to a separate location before upgrading.

- **ISO File**
  You can use this type of file to reinstall the full set of software including the operating system. Before using an ISO file, you must backup all applications data.

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

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

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

To download software:

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

2.2 Information Requirements

The following information is required during the installation process:

- **Server Applications**
  During the installation process, you can select which IP Office Application Server applications are installed. Note that for each application selected, the normal license requirements still apply. Refer to the separate installation manual for each application for details.
  - □ **Voicemail Pro**
    If selected for installation, refer to the Voicemail Pro Linux Installation Manual for details of setup and configuration of the Voicemail Pro application.
    - □ **Voicemail Text to Speech Prompts**
      During installation, you can select whether you want TTS prompt installed. If selected, you will be prompted to select the languages that you want installed. These are installed from a separate sets of DVDs or downloadable ISO files.
  - □ **one-X Portal for IP Office**
    If selected, the same information is required as for a Windows based installation of the one-X Portal for IP Office application. For example, IP address of IP Office Application Server system, LDAP server information and voicemail server address (if other than the IP Office Application Server address). Refer to the one-X Portal for IP Office Installation manual.
- **Server IP Address Settings**
  The IP Office Application Server supports IPv4 addressing obtain through either DHCP or static addressing.

	IPv4 Support
Use DHCP	□
IP Address	□ ______________________________
Prefix (Netmask)	□ ______________________________
Gateway	□ ______________________________
Primary DNS	□ ______________________________
Secondary DNS	□ ______________________________

- □ **Hostname**
  A hostname helps simplify access to the server and the applications it provides rather than requiring users to use the IP address.
- □ **Timezone**
  The timezone in which the server is located and whether the server should use UTC or local time.
- □ **Root Password**
  This password is used for configuration access to the server.
- □ **Client PC**
  The IP Office Application Server is designed and intended for remote configuration and management. It is not managed directly from the server. Therefore a client PC with a web browser on the same network as the server PC is required for configuration.
  - If Voicemail Pro server is one of the selected server applications, then the client PC must be a Windows based PC onto which the Voicemail Pro client application can be installed.

2.3 Checking the Boot Order

You install the software by placing it onto a DVD or USB2 memory key from which the server PC then boots. The normal default for servers is to boot from CD/DVD drive and, if unsuccessful, then boot from the first hard disk. This boot order is set in the BIOS settings of the server PC.

In order to add other devices to the list of those from which the server can boot or to change the order of usage, you need to change the server's BIOS settings. The method of accessing the BIOS varies between servers. Refer to the PC manufacturer's documentation.

- Typically, an option to access the BIOS settings of a server is displayed briefly when the server PC is started. For example "Press Del for setup" indicates that the server BIOS is accessed by press the Delete key while the message is displayed. This option is only available for a few seconds whilst the existing BIOS settings are loaded, after which the server looks for and begins to load boot software if it finds a boot source, for example existing boot software on its hard disk.

- Once the PC displays its BIOS settings, the normal boot up process stops. The BIOS settings typically consist of several pages. The settings for the order in which the server looks at different devices for a boot software source are normally set on the **Advanced BIOS Features** page.

- To boot from a DVD, ensure that the server's DVD drive is set as the boot device used before the server's hard disk.

- To boot from a USB2 memory key, set a USB option as the boot device used before the server's hard disk. Depending on the BIOS, there may be multiple USB options. Select ***USB-FDD***.

- The server's hard disk must remain in the list of boot devices. The server boots from the hard disk after the software installation.

2.4 Preparing the Bootable Software Installer

You can install the server software from either a DVD or a USB2 memory key. If not installing from an Avaya supplied DVD, you must download an ISO file from Avaya and use that to create the bootable DVD or USB2 memory key.

2.4.1 Preparing a DVD

To install from a DVD, you need to burn the .iso image file of the installation software onto a bootable DVD. The exact process for that depends on which software you use for the burning process. However, the following general recommendations apply:

- Do not use reusable DVDs.
- Burn the DVD at a slow speed such as 4x.

2.4.2 Preparing a USB2 Installation Key

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

Prerequisites

- **8GB USB2 Memory Key**
  Note that all existing files on this device will be erased.

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

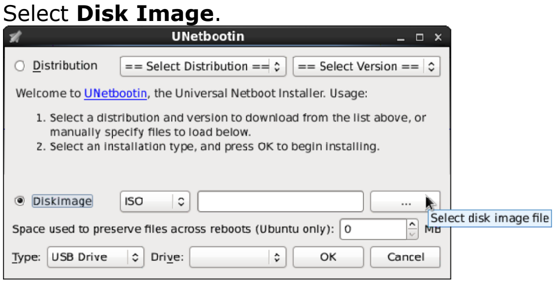
- **IP Office Application Server ISO File**
  You can download this software from the Avaya support website (http://support.avaya.com).

To create a bootable USB2 memory key:

1. Erase all files on USB2 memory key and reformat it as a FAT32 device.

2. Start the **unetbootin** application.

3. Select **Disk Image**.



UNetbootin

○ Distribution == Select Distribution == == Select Version ==

Welcome to UNetbootin, the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

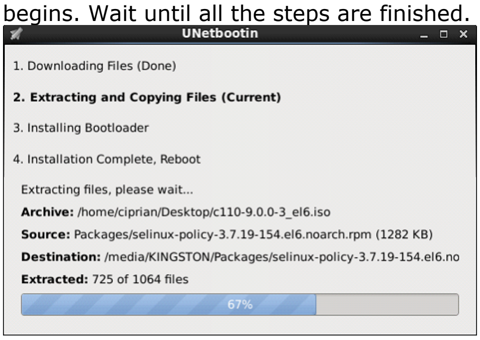
● Diskimage ISO ... Select disk image file

Space used to preserve files across reboots (Ubuntu only): 0 MB

Type: USB Drive Drive: OK Cancel

4. Click the **...** browse button and select the ISO file.

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



UNetbootin

1. Downloading Files (Done)

2. Extracting and Copying Files (Current)

3. Installing Bootloader

4. Installation Complete, Reboot

Extracting files, please wait...

Archive: /home/ciprian/Desktop/c110-9.0.0-3_el6.iso

Source: Packages/selinux-policy-3.7.19-154.el6.noarch.rpm (1282 KB)

Destination: /media/KINGSTON/Packages/selinux-policy-3.7.19-154.el6.no

Extracted: 725 of 1064 files

67%

6. When the process has ended, click **Exit**. Do not click **Reboot now**.

7. Using the file explorer, open the USB folder on the USB2 memory key.

8. Select the file **syslinux.cfg** and copy it to the top level (root) folder, overwriting any existing file with that name.

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

2.5 Server Software Installation

This process installs the Linux operating system onto the server and the Linux based applications. This installation process requires approximately 1 hour.

To install the server software from a bootable device:

1. Depending on the chosen method of installation:
   - If installing from a DVD, immediately after powering up the PC, insert the DVD into the DVD drive.
   - If installing from a USB2 memory key, insert the USB2 memory key into the first USB port and apply power to the PC.
2. The PC should boot and display the first IP Office Application Server installation screen.
   - If installing from a DVD and the PC does not boot from the DVD, the boot order of the server PC may need to be changed. See Checking the Boot Order 18.
   - If installing from a USB2 memory key and the PC does not boot from the USB2 memory key:
     - if the server has several USB ports, reboot with the USB2 memory key in another one of the ports.
     - the boot order of the server may need to be changed. See Checking the Boot Order.
3. The installer prompts whether it should check the installation media. Checking a DVD takes approximately 10 minutes.
   a. To skip the media check, select **Skip**.
   b. To proceed with a media check, select **OK**. When the check has completed, the installer provides options to check any other media, for example the TTS language DVDs.
4. Select the language that you want used for the installation process. Click **Next**.
5. Select the keyboard that matches the one you are using. Click **Next**.
6. Read the license agreement. If you accept the license agreement, click **Yes** and then click **Next**.
7. An upgrade menu appears if a previous release is already installed on the server. It details the existing installed options and the new installable options. Select either ***Install*** or ***Upgrade*** and click **Next**.
   - ***Install***
     This option overwrites the existing installation including any customer data.
   - ***Upgrade***
     This option upgrades the existing application and retains the existing customer data.
8. If you selected ***Install***, the installer asks you to confirm the process. Select the required option and click **Next**.
   - **Yes**
     If selected, the installation process continues, formatting the whole drive for its use.
   - **No**
     If selected, the install process offers to shutdown the server. Either remove the device from which you were booting to allow the server to restart normally or allow the installation process to start again.
   - **Advanced**
     If selected, during the installation process you can select adjust the hard disk partitioning. However, if used, the installer does not display the **Upgrade** option *(see Step 7)* when booting from an ISO in future.
9. If you selected **Install**, continue below. If you selected **Upgrade**, go to step 11.
   a. Set the host name for the server to use.
   b. Click **Configure Network**.
      a. Select the wired Ethernet connection that is being used (this is likely to be ***eth0***) and click **Edit**.
      b. Select the **IPv4 Settings** tab.
      c. To change the address shown, click on the address and change the settings.
      d. When finished setting the IP address details for the server, click **Apply**. Click **Close**. Click **Next**.
   c. Enter and confirm the password for the root administrator account. This is the root user password for access to the operating system. Ensure that you note the password set.
   d. Click **Next**. Click **Next** again.
   e. A menu for partitioning the server appears if you selected **Advanced** during step 8 above. The menu allows various options for partitioning of the server hard disk. However, if used, the installer does not display the **Upgrade** option *(see Step 7)* when booting from an ISO in future.
10. The process for formatting the disk starts. This runs for a couple of minutes.

11. The installer prompts you that it is about start installation of the software. Click **Next** to start.
12. When installation is complete, click **Next**.
13. Remove the DVD or USB2 memory key and then select **Reboot**.
14. Following the reboot, the server displays the address details for further configuration of the server. Use the address to start the server ignition process. See Server Ignition 23.

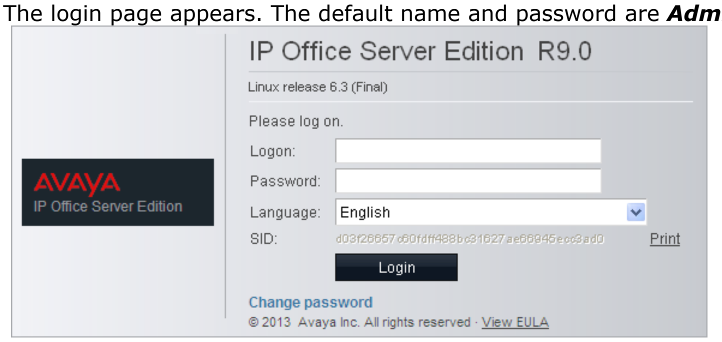
2.6 Server Ignition

Following installation, you must ignite the server. You do this by web browser access to the server.

To start server ignition:

1. From a client PC, start the browser and enter ***https://*** followed by the IP address of the server and ***:7071***. For example ***http://192.168.42.1:7071***.

2. The login page appears. The default name and password are ***Administrator*** and ***Administrator***.



IP Office Server Edition R9.0

Linux release 6.3 (Final)

Please log on.

Logon:

Password:

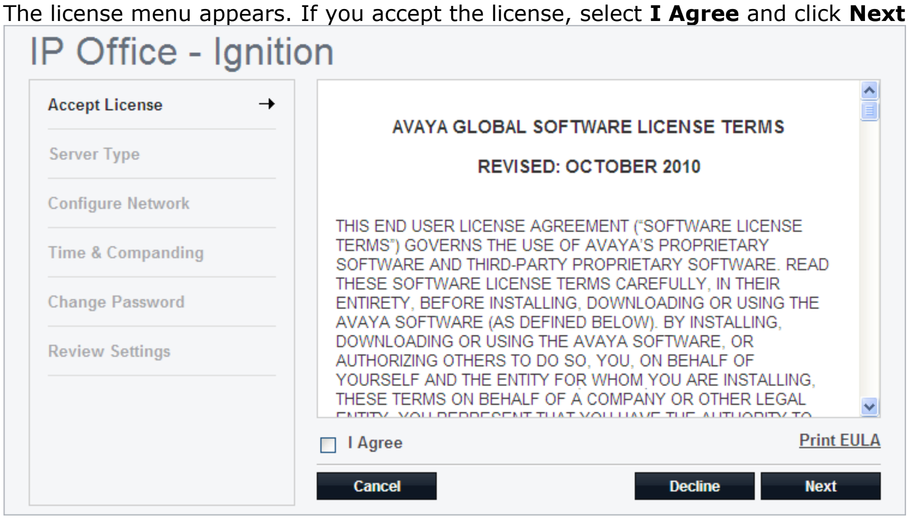
Language: English

SID: d03f26657c60fdff488bc31627ae66945ecc3ad0

© 2013 Avaya Inc. All rights reserved · View EULA

3. Click **Login**.

4. The license menu appears. If you accept the license, select **I Agree** and click **Next**.



IP Office - Ignition

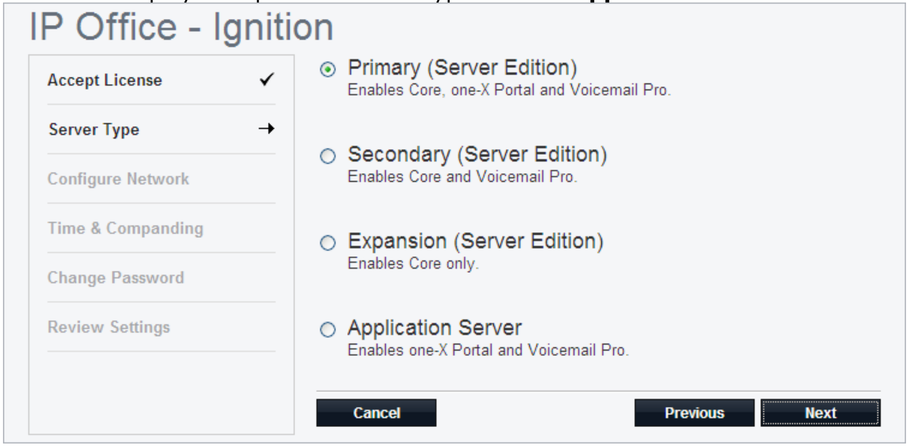
AVAYA GLOBAL SOFTWARE LICENSE TERMS

REVISED: OCTOBER 2010

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF AVAYA'S PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE AVAYA SOFTWARE (AS DEFINED BELOW). BY INSTALLING, DOWNLOADING OR USING THE AVAYA SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL

□ I Agree

5. The menu displays the possible server types. Select **Application Server** and click **Next**.



IP Office - Ignition

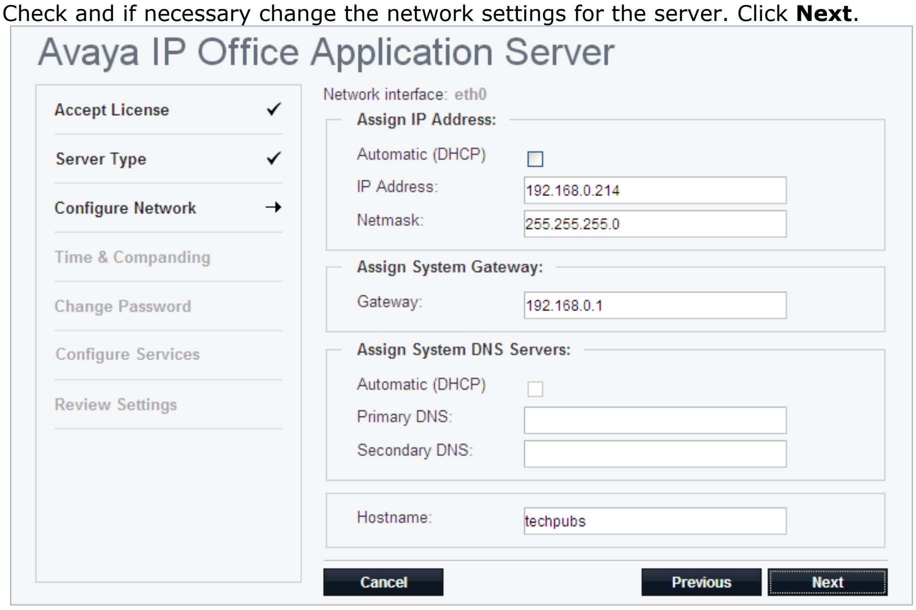
● Primary (Server Edition)
Enables Core, one-X Portal and Voicemail Pro.

○ Secondary (Server Edition)
Enables Core and Voicemail Pro.

○ Expansion (Server Edition)
Enables Core only.

○ Application Server
Enables one-X Portal and Voicemail Pro.

6. Check and if necessary change the network settings for the server. Click **Next**.



Network interface: eth0

Assign IP Address:

Automatic (DHCP) □
IP Address: 192.168.0.214
Netmask: 255.255.255.0

Assign System Gateway:

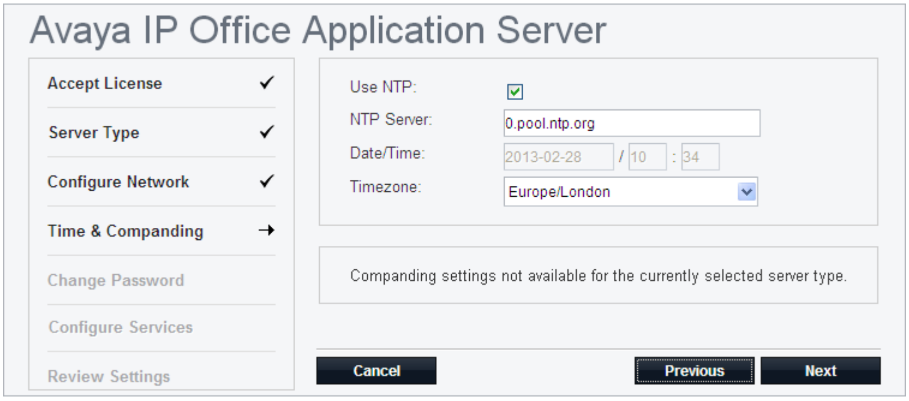
Gateway: 192.168.0.1

Assign System DNS Servers:

Automatic (DHCP) □
Primary DNS:
Secondary DNS:

Hostname: techpubs

7. Set the time source for the server.

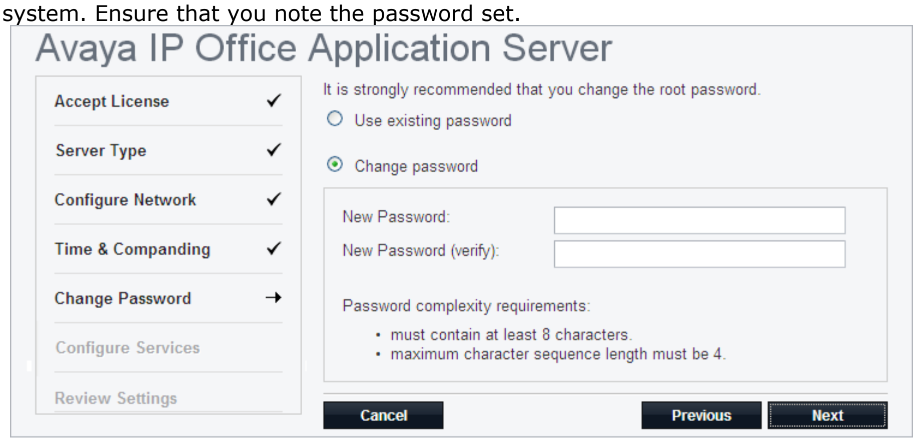


Use NTP: ☑
NTP Server: 0.pool.ntp.org
Date/Time: 2013-02-28 / 10 : 34
Timezone: Europe/London

Companding settings not available for the currently selected server type.

- Set the current time and date for the server or select to use the time provided by an NTP server.

8. Click **Next**. Enter and confirm a new password. This is the root user password for access to the Linux operating system. Ensure that you note the password set.



It is strongly recommended that you change the root password.

○ Use existing password

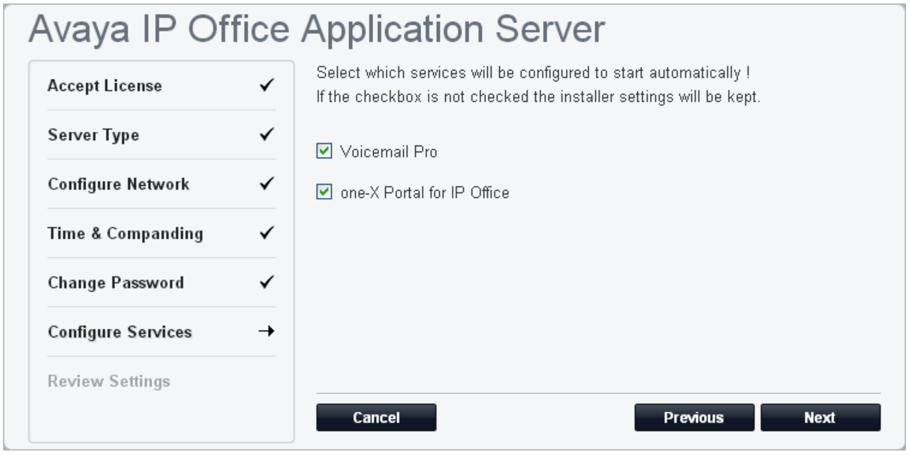
● Change password

New Password:
New Password (verify):

Password complexity requirements:

- must contain at least 8 characters.
- maximum character sequence length must be 4.

9. Select which applications should start automatically. Unselected services remain installed but not running unless manually started. If the intention is to also run Contact Recorder for IP Office on the application server, do not select Voicemail Pro.

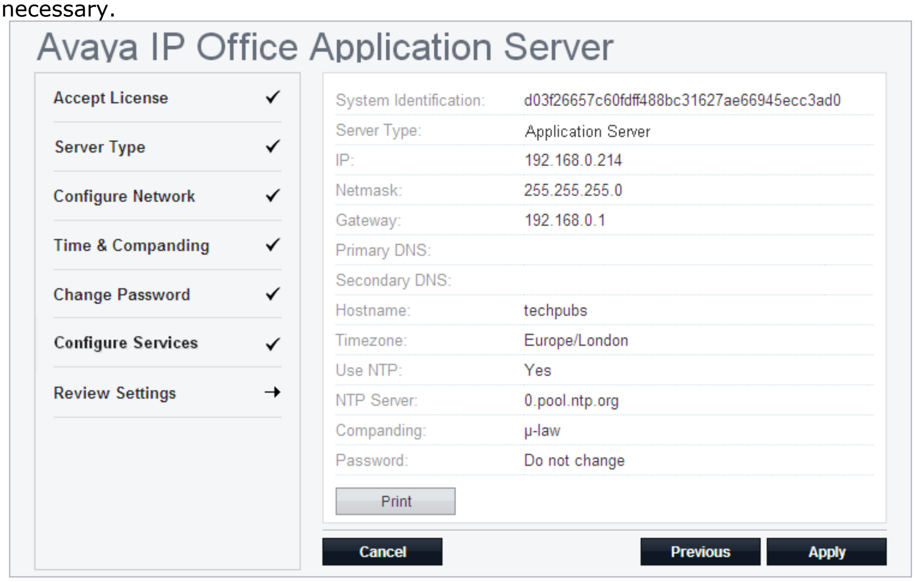


Select which services will be configured to start automatically !
If the checkbox is not checked the installer settings will be kept.

☑ Voicemail Pro

☑ one-X Portal for IP Office

10. Click **Next**. Check the displayed summary and use the **Previous** and **Next** options to readjust settings if necessary.



System Identification:	d03f26657c60fdff488bc31627ae66945ecc3ad0
Server Type:	Application Server
IP:	192.168.0.214
Netmask:	255.255.255.0
Gateway:	192.168.0.1
Primary DNS:	
Secondary DNS:	
Hostname:	techpubs
Timezone:	Europe/London
Use NTP:	Yes
NTP Server:	0.pool.ntp.org
Companding:	µ-law
Password:	Do not change

11. Click **Apply**. Click **OK** when displayed to access the server's web manager menus.

2.7 Logging In

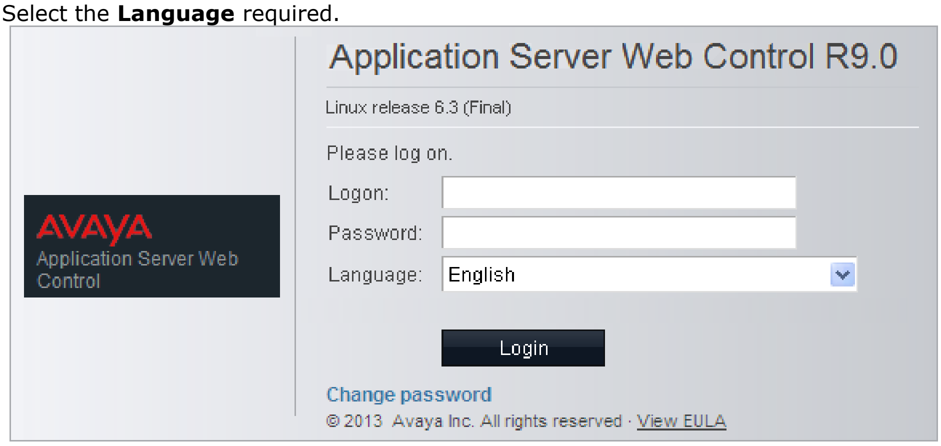
Administration of the IP Office Application Server is done using a web browser on a client PC with network access to the IP Office Application Server.

Avaya supports the following web browsers:

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

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

1. From a client PC, start the browser. Enter ***http://*** followed by the address of the IP Office Application Server and ***:7071***.
2. Select the **Language** required.



Application Server Web Control R9.0

Linux release 6.3 (Final)

Please log on.

Logon:

Password:

Language: English

AVAYA
Application Server Web Control
Login
Change password
© 2013 Avaya Inc. All rights reserved · View EULA

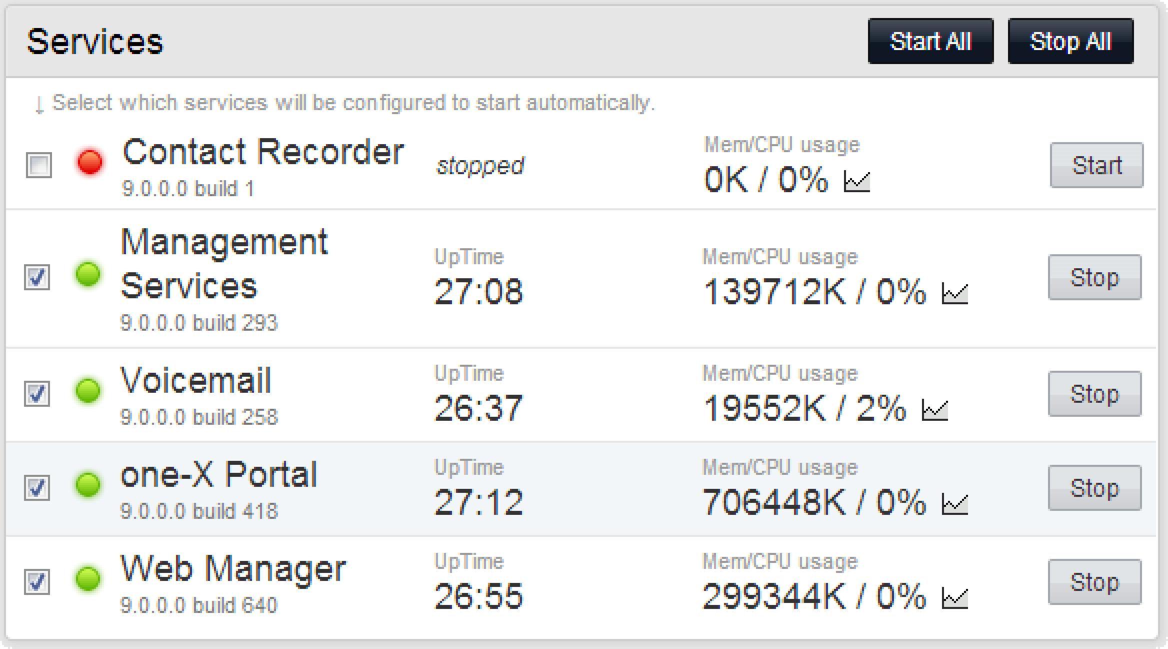
3. Enter the name and password for IP Office Application Server administration. The default name and password are ***Administrator*** and ***Administrator***. To change the password, select the **Change Password** 57 option.
4. If the login is successful, the server's **System** 75 page appears.

2.8 Checking the Services

After logging in to the IP Office Application Server, the **System** page provides a summary of the services that the server can provide and the status (started or stopped) of those services. By default all the application services are set to automatically start. However, they may still require individual configuration and the addition of licenses to the IP Office configuration.

To check the services:

1. Login and select the **System** menu.



↓ Select which services will be configured to start automatically.

□	●	Contact Recorder 9.0.0.0 build 1	*stopped*	Mem/CPU usage 0K / 0%	Start
☑	●	Management Services 9.0.0.0 build 293	UpTime 27:08	Mem/CPU usage 139712K / 0%	Stop
☑	●	Voicemail 9.0.0.0 build 258	UpTime 26:37	Mem/CPU usage 19552K / 2%	Stop
☑	●	one-X Portal 9.0.0.0 build 418	UpTime 27:12	Mem/CPU usage 706448K / 0%	Stop
☑	●	Web Manager 9.0.0.0 build 640	UpTime 26:55	Mem/CPU usage 299344K / 0%	Stop

2. Check that the expected services have been started. If not, each can be individually started using the **Start/Stop** buttons on the right.

3. Check the **Notifications** panel is not listing any errors that would indicate a problem with the installation.

4. If all the services are started as expected, each can be individually configured.

5. If the sever is running correctly, logout and then log in again using the **Change Password** 57 option.

2.9 Installing IP Office Manager

IP Office Manager is used to complete the ignition process. A compact version of IP Office Manager can be downloaded from the IP Office Application Server server if not already available.

To download and install IP Office Manager:

1. Select the **AppCenter** tab.

2. Locate the ***AdminLite... .exe*** file. The exact filename varies depending on the version of the application.

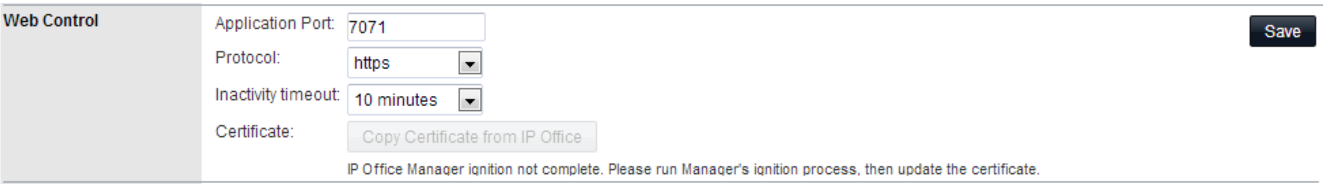
3. Click on the link to download the file. The method of downloading depends on the browser being used.

4. Run the downloaded file and follow the prompts to install IP Office Manager.

2.10 Certificate Generation

Certificates are used to control access to the server applications. A certificate is used for browser access to the web control menus, one-X Portal for IP Office application and SSH file services. An IP Office certificate is used for access to the IP Office application configuration using IP Office Manager and the web manager menus used for on-boarding.

The lack of valid certificate is indicated in the Web Control section of the **Settings | General** 86 tab.



Web Control

Application Port: 7071

Protocol: https

Inactivity timeout: 10 minutes

Certificate: Copy Certificate from IP Office

IP Office Manager ignition not complete. Please run Manager's ignition process, then update the certificate.

To perform initial configuration:

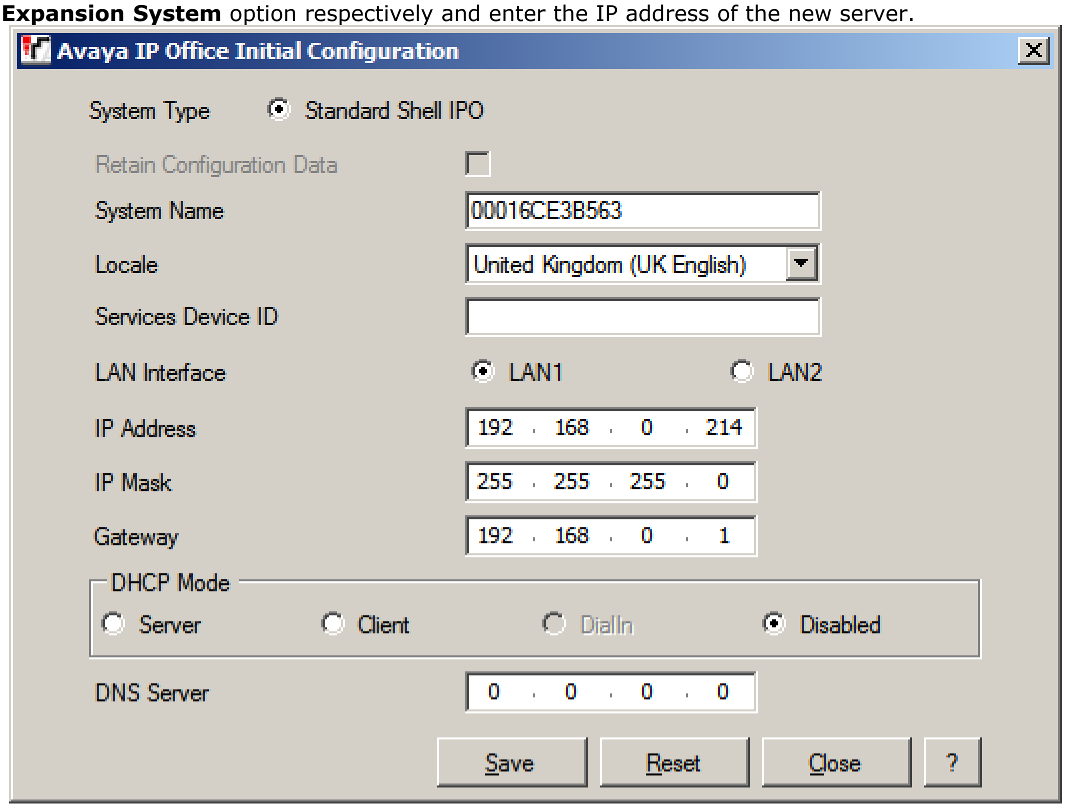
1. Start IP Office Manager.

2. Click and use the **Select IP Office** menu to discover the available IP Office systems.

3. Select the tick box next to the application server.

4. Click **OK**.

5. When connecting to a newly installed primary for the first time using IP Office Manager, the **Initial Configuration** menu is displayed. For a secondary server or expansion server, select the **Add Secondary Server** or **Add Expansion System** option respectively and enter the IP address of the new server.



Avaya IP Office Initial Configuration

System Type ● Standard Shell IPO

Retain Configuration Data □

System Name: 00016CE3B563

Locale: United Kingdom (UK English)

Services Device ID:

LAN Interface ● LAN1 ○ LAN2

IP Address: 192 . 168 . 0 . 214

IP Mask: 255 . 255 . 255 . 0

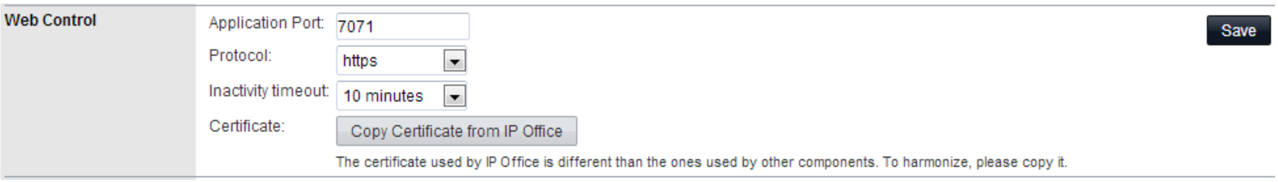
Gateway: 192 . 168 . 0 . 1

DHCP Mode: ○ Server ○ Client ○ DialIn ● Disabled

DNS Server: 0 . 0 . 0 . 0

6. Check that the settings match those required for the server and the IP Office. For full details of the menu refer to the IP Office Manager help. Click **Save**. When displayed, click **OK**.

7. Log in to the web control menus and select the **Settings | General** 86 tab. The **Web Control** section indicates that a certificate was found.



Web Control

Application Port: 7071

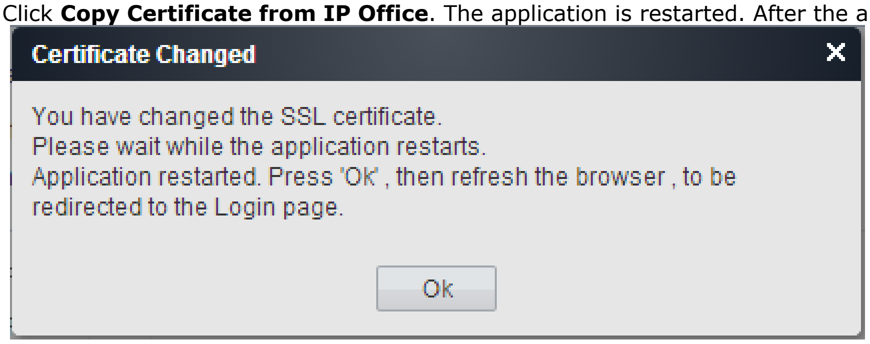
Protocol: https

Inactivity timeout: 10 minutes

Certificate: Copy Certificate from IP Office

The certificate used by IP Office is different than the ones used by other components. To harmonize, please copy it.

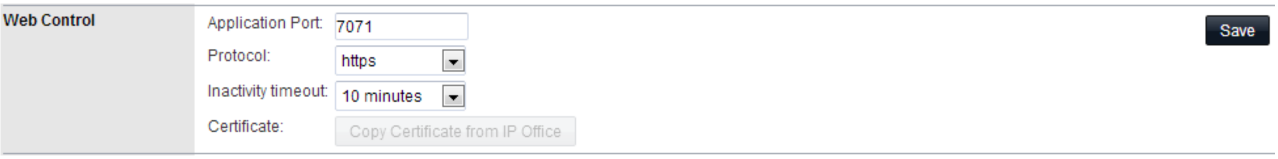
8. Click **Copy Certificate from IP Office**. The application is restarted. After the application is restarted click **OK**.



Certificate Changed

You have changed the SSL certificate.
Please wait while the application restarts.
Application restarted. Press 'Ok' , then refresh the browser , to be redirected to the Login page.

9. Login to web control again. Select the **Settings | General** tab and check that the **Web Control** section shows that the certificate is up to date.



Web Control

Application Port: 7071

Protocol: https

Inactivity timeout: 10 minutes

Certificate:

Chapter 3. Pre-Built Application Server Installation

3. Pre-Built Application Server Installation

While on a pre-built Avaya server the IP Office Application Server software is pre-installed, there are still some basic installation processes that must be completed before it can be used with the IP Office system. Those basic processes are covered in this and the two following chapters.

Initial Configuration Summary

1. **Initial IP Office Application Server configuration:**
   a. Change the IP address settings to match the customer network 34.
   b. Change the default password used for web control access 35.
2. **Initial Voicemail Pro configuration:**
   a. **IP Office Configuration**
      i. Adding voicemail licenses 39.
      ii. Check the Voicemail Type Setting 40.
   b. **Voicemail Pro Configuration**
      i. Install the Voicemail Pro client 41.
      ii. Log in to the Voicemail Pro server 42.
      iii. Change the default administrator password 42.
3. **Initial one-X Portal for IP Office configuration:**
   a. **Add licenses** 48
   Those IP Office users who want to use the one-X Portal for IP Office application need to have their **Profile** set to ***Office Worker***, ***Teleworker*** or ***Power User*** and the **Enable one-X Portal Services** option selected. To do this requires the addition of licenses for those roles.
   b. **Enable one-X Portal for IP Office users** 49
   When licenses are available, the number of licenses allows the configuration of the equivalent number of users for those roles and then for one-X Portal for IP Office usage.
   c. **Initial one-X Portal for IP Office login** 50
   Having licensed and configured some users for one-X Portal for IP Office, you need to login as the one-X Portal for IP Office administrator in order to perform initial one-X Portal for IP Office configuration.
   d. **Initial AFA login** 51
   The one-X Portal for IP Office AFA interface is used for remote backup and restoration of the application. At minimum you should login in order to change the default password for the interface.

Transferring Settings

If the IP Office Application Server is a replacement for an existing Voicemail Pro and/or one-X Portal for IP Office server, additional steps are required to backup and restore the settings from the existing servers. You should read and understand the addition steps for the backup and restoration before beginning the IP Office Application Server installation.

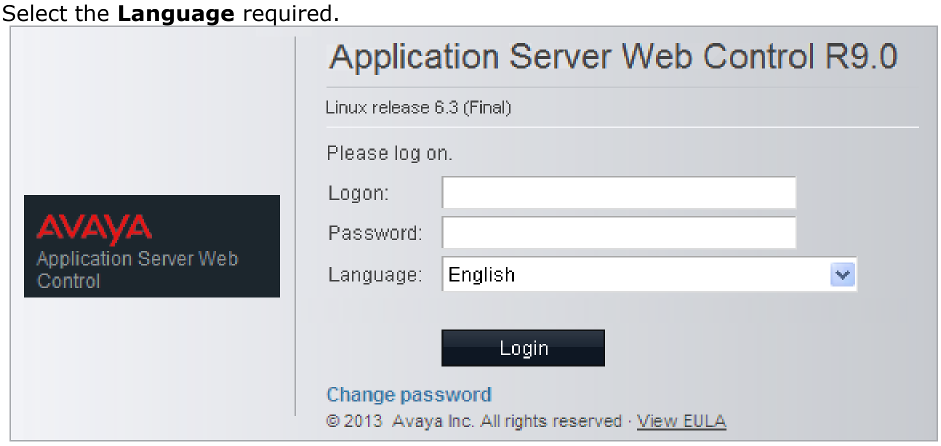
- **Transferring Voicemail Pro Settings** 44
- **Transferring one-X Portal for IP Office Settings** 52

3.1 Logging In

To login to the server's web control menus:

1. From a client PC, start the browser. Enter ***http://*** followed by the address of the IP Office Application Server and ***:7071***.

2. Select the **Language** required.



Application Server Web Control R9.0

Linux release 6.3 (Final)

Please log on.

Logon:

Password:

Language: English

AVAYA
Application Server Web Control
Login
Change password
© 2013 Avaya Inc. All rights reserved · View EULA

3. Enter the name and password for IP Office Application Server administration. The default name and password are ***Administrator*** and ***Administrator***. To change the password, select the **Change Password** 57 option.

4. If the login is successful, the server's **System** 75 page appears.

3.2 Changing the IP Address Settings

On shipment the IP Office Application Server has a default IP address of 192.168.42.1. This should be changed.

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

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

To change the IP address:

1. Login 56 to the server's web configuration pages.

2. Select **Settings**.

3. Select **System**.

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

   - **Network Interface**
     This drop down allows selection of network interfaces is currently being configured by the web form. Within the IP Office configuration, ***Eth0*** matches LAN1, ***Eth1*** matches LAN2. On the pre-built IP Office Application Server only ***Eth0*** is used. This port is labeled as port 1 on the physical server.

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

     - **! WARNING**
       For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

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

   - **IP Address**
     Displays the IP address set for the server. If DHCP is not being used, the field can be edited to change the setting.

     - **! WARNING**
       For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

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

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

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

   - **Automatically obtain DNS from provider**
     This setting is only used if **Use DHCP** is also selected. If selected, the server attempts to obtain DNS server details from the DHCP server.

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

3.3 Changing the Web Password

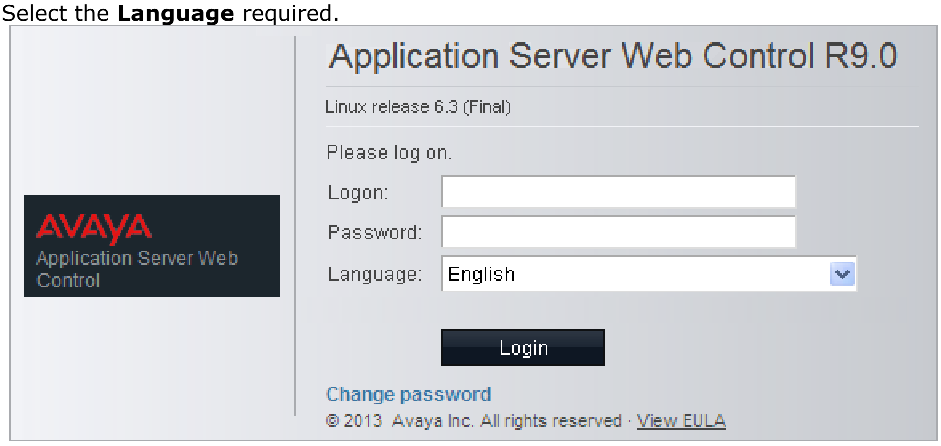
Changing the password from the web control log on menu changes the password stored by web control itself. Web control only uses that password if **Enable referred authentication** is not enabled. See Password Authentication 14.

If using IP Office Web Manager authentication (**Enable referred authentication** selected), you can change the user names and password used for access to web control through the IP Office Web Manager service user settings.

To change the browser password:

1. From a client PC, start the browser. Enter ***http://*** followed by the address of the IP Office Application Server and ***:7071***.

2. Select the **Language** required.



Application Server Web Control R9.0

Linux release 6.3 (Final)

Please log on.

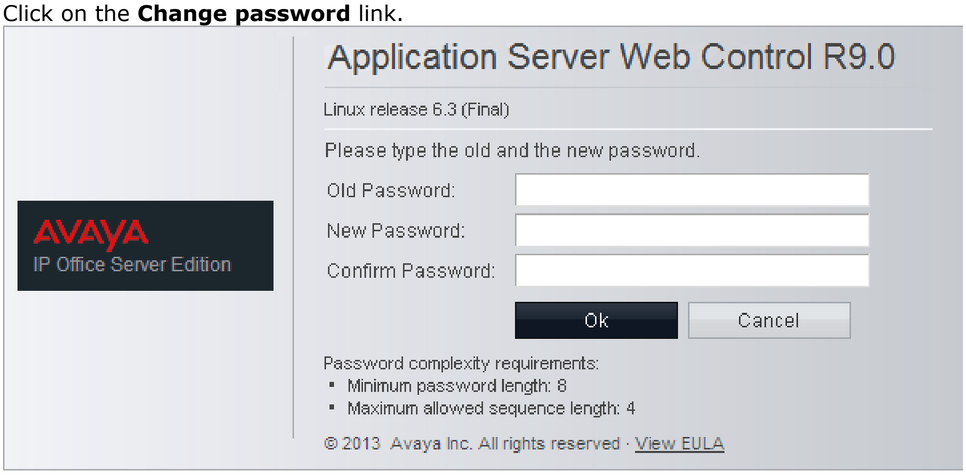
Logon:

Password:

Language: English

AVAYA
Application Server Web Control
Login
Change password
© 2013 Avaya Inc. All rights reserved · View EULA

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



Application Server Web Control R9.0

Linux release 6.3 (Final)

Please type the old and the new password.

Old Password:

New Password:

Confirm Password:

Password complexity requirements:
- Minimum password length: 8
- Maximum allowed sequence length: 4

4. Enter the current password and the new password. The new password must meet the complexity requirements displayed on the menu.

5. Click **OK**. The menu confirms whether the change was successful or not. If the new password is accepted, click **Cancel** to return to the **Login** menu. .

Chapter 4.
Voicemail Pro Configuration

4. Voicemail Pro Configuration

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

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

Voicemail Pro Initial Configuration

a. **IP Office Configuration**

   i. Adding voicemail licenses 39.

   ii. Check the Voicemail Type Setting 40.

b. **Voicemail Pro Configuration**

   i. Install the Voicemail Pro client 41.

   ii. Log in to the Voicemail Pro server 42.

   iii. Change the default administrator password 42.

Transferring Settings from a Previous Server

If the IP Office system was already configured to operate with an external Voicemail Pro server that is now being replaced, the settings, prompts and messages on the old server can be transferred to the new server. After completing the steps above, see Transferring Voicemail Server Settings 44.

Notes

For use of UMS options, the Voicemail Pro service needs to communicate with a MAPI proxy application installed on a Windows PC. The installation package for the MAPI proxy can be downloaded from the server's **Windows Client** 96 menu. For full details refer to the Voicemail Pro Linux Installation manual.

4.1 Adding Voicemail Licenses

The Voicemail Pro application will operate for up to 2 hours without a license. This allows a level of basic installation testing and configuration. However, for full operation the application must be licensed using licenses entered into the IP Office configuration.

For Voicemail Pro operation on IP Office Application Server, the following licenses are used:

- **Essential Edition**
  This license is a pre-requisite for the **Preferred Edition** license below.
- **Preferred Edition (Voicemail Pro)**
  This license is required for use of the Voicemail Pro application. It also enables 4 voicemail ports. It is also required as a pre-requisite for the user profile licenses required for one-X Portal for IP Office users.
- **Preferred Edition Additional Voicemail Ports**
  These licenses add additional voicemail ports in addition to the 4 enabled by the **Preferred Edition (Voicemail Pro)** license above.
- **Messaging TTS Pro**
  This license enables the use of text-to-speech facilities using the optional Linux TTS software and user email reading. One license per simultaneous instance of TTS usage.
- **User Profile Licenses**
  In order to log into and use the one-X Portal for IP Office application, a user must be configured and licensed to one of the following user profile roles in the IP Office configuration: ***Office Worker***, ***Teleworker*** or ***Power User***. Each role requires an available **Office Worker**, **Teleworker** or **Power User** license in the IP Office configuration.

To enter licenses:

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

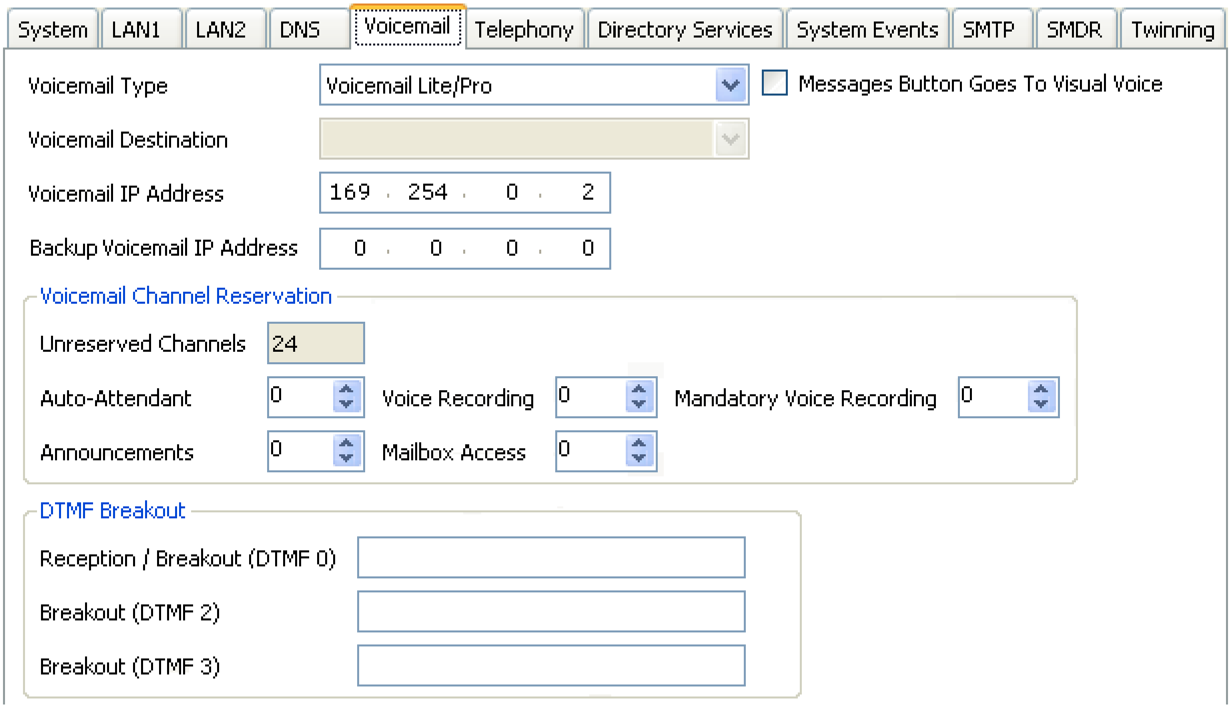
4.2 IP Office Configuration

When a IP Office Application Server running Voicemail Pro is added, the IP Office system configuration needs to be adjusted to use the voicemail server.

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

To set the voicemail server address:

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



Voicemail Type: Voicemail Lite/Pro

□ Messages Button Goes To Visual Voice

Voicemail Destination:

Voicemail IP Address: 169 . 254 . 0 . 2

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

Voicemail Channel Reservation

Unreserved Channels	24				
Auto-Attendant	0	Voice Recording	0	Mandatory Voice Recording	0
Announcements	0	Mailbox Access	0		

DTMF Breakout

Reception / Breakout (DTMF 0):

Breakout (DTMF 2):

Breakout (DTMF 3):

- The **Voicemail Type** should be set to ***Voicemail Lite/Pro***.
- The **Voicemail IP Address** should be set to match the IP address given to the server hosting Voicemail Pro. For simplicity, if you only have the one voicemail server, an address of 0.0.0.0 tells the IP Office to broadcast a request for the voicemail server and to use the server that replies.
- In the **Voicemail Channel Reservation** section, the number of channels will be 4 plus any additional channels licensed.

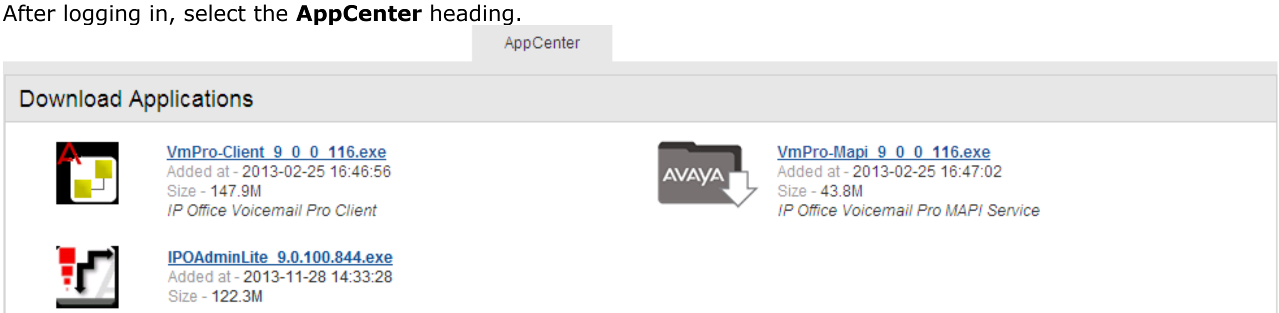
4. If any changes have been made, save the changes back to the IP Office system.

4.3 Installing the Voicemail Pro Client

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

To download and install the Voicemail Pro client:

1. Login to the server's web control menus. See Logging In Directly 56.
2. After logging in, select the **AppCenter** heading.



VmPro-Client_9_0_0_116.exe
Added at - 2013-02-25 16:46:56
Size - 147.9M
IP Office Voicemail Pro Client

VmPro-Mapi_9_0_0_116.exe
Added at - 2013-02-25 16:47:02
Size - 43.8M
IP Office Voicemail Pro MAPI Service

IPOAdminLite_9.0.100.844.exe
Added at - 2013-11-28 14:33:28
Size - 122.3M

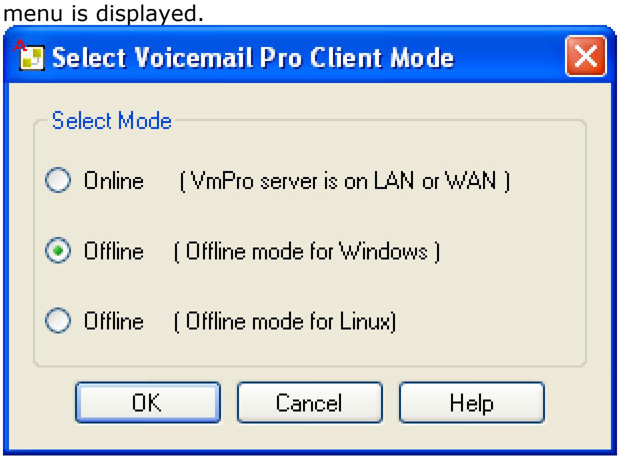
3. Click on the link for the Voicemail Pro client file in order to download the software package for installing the client.
4. Once the package has been downloaded, run it to install the Voicemail Pro client.

4.4 Logging in to the Voicemail Server

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

To login with the Voicemail Pro client:

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



Select Voicemail Pro Client Mode

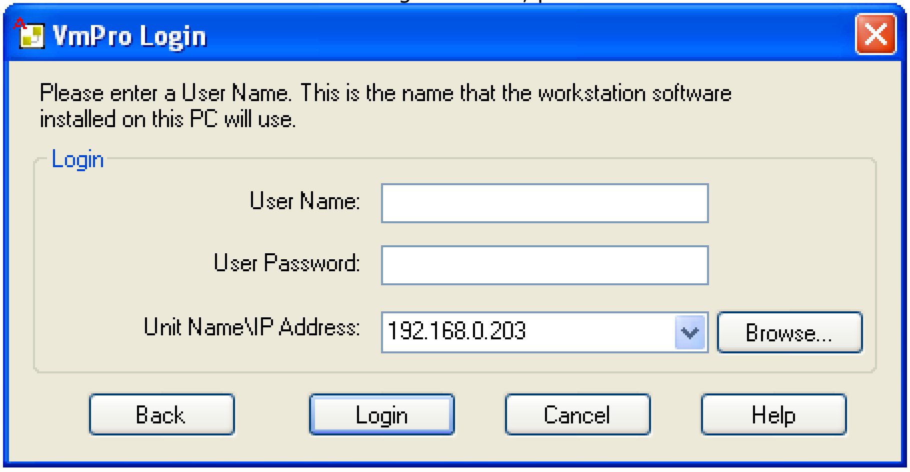
Select Mode

○ 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 is displayed.



VmPro Login

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

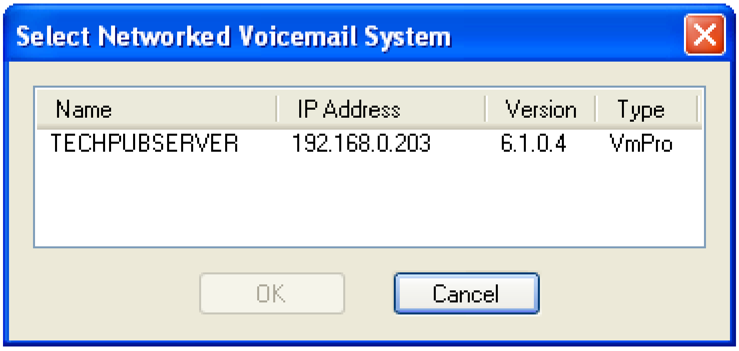
Login

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



Select Networked Voicemail System

Name	IP Address	Version	Type
TECHPUBSERVER	192.168.0.203	6.1.0.4	VmPro

6. Click Login. Note that if 3 unsuccessful logins are attempted using a particular administrator account name, that administrator account is locked for an hour.
7. The following menu may appear. Select **Download**.
8. You should now change the password 43.

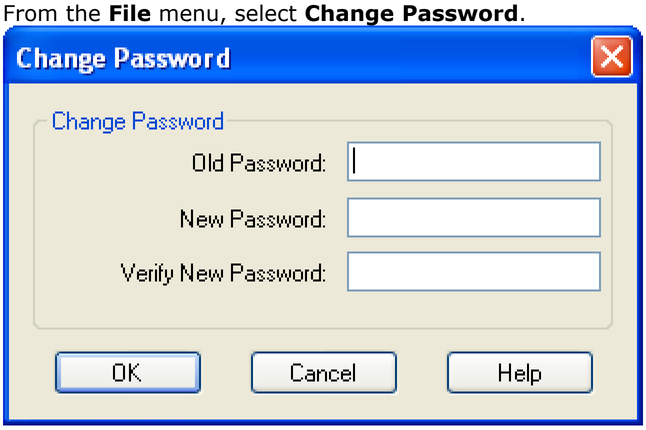
4.5 Changing the Voicemail Server Password

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

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

To change the Voicemail Pro Administrator password:

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



2. In the **New Password** box, type the new password.

3. In the **Confirm Password** box, retype the new password.

4. Click **OK**.

4.6 Transferring Voicemail Server Settings

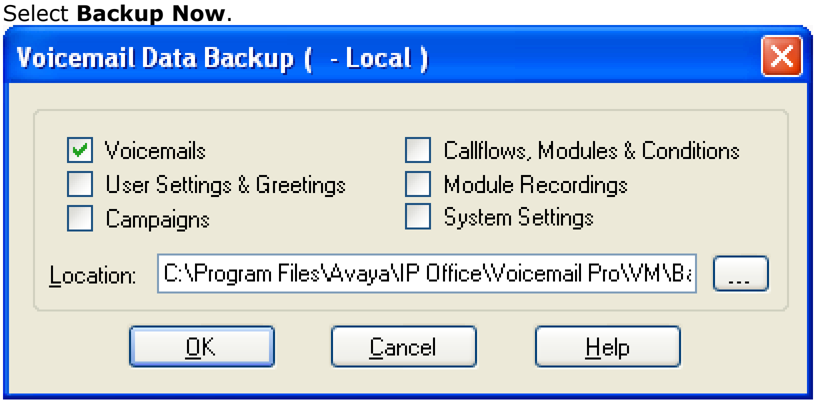
If the IP Office Application Server is replacing an existing voicemail server, a backup of all the settings, prompts and messages from that server can be transferred to the new server. If the existing server is a Linux based server, SSH file transfer is used to retrieve the backup files from the server.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

SSH File transfer is then used to transfer the backup file set onto the new server.

To back up the old voicemail server:

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

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



Voicemail Data Backup (- Local)

☑ Voicemails
□ User Settings & Greetings
□ Campaigns
□ Callflows, Modules & Conditions
□ Module Recordings
□ System Settings

Location: C:\Program Files\Avaya\IP Office\Voicemail Pro\VM\B

4. Select all the backup options for a complete backup and click **OK**. This will create a backup folder, the name of which includes the date and time of the backup and Immediate. For example ***VMPro_Backup_26012011124108_Immediate***.
5. The time to complete the backup will vary greatly depending on the number of mailboxes and messages being supported by the server.

To shut down the old voicemail server:

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

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

To loading the backup onto the new server using SSH:

Use the following method to transfer and then restore the backup.

1. Connect to the IP Office Application Server using an SSH File transfer tool 101.
2. Copy the backup folder into the folder ***/opt/vmpro/Backup/Scheduled/OtherBackups***.
3. Using a web browser, login 56 to the server.
4. Select **Settings**. On the **General** tab, select the **Restore** button for the Voicemail service. From the list of available backups, select the one just copied onto the server.
5. Click **OK**.
6. Once the restore has been completed, on the **System** menu, ***Stop*** and then ***Start*** the voicemail service.

4.7 ContactStore

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

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

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

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

4.8 Backup/Restore Limitations

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

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

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

To manually backup a custom folder:

1. Using an SSH file transfer tool 101, copy the folder ***Custom*** from ***/opt/vmpro*** to your PC to create a backup of the folder.

To manually restore a custom folder:

1. To restore the folder, again using an SSH file transfer tool, copy the folder to the ***/home/Administrator*** folder on the server.

2. Using the SSH command line, you now need to copy the ***Custom*** folder from ***/home/Administrator*** to the ***/opt/vmpro*** folder. This is done by logging in as the root user.

    a. Login to the system's command line interface using the existing root user password. This can be done either directly on the server or remotely using an SSH client shell application.

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

        a. At the **Command:** prompt, enter **login**.

        b. At the **login:** prompt enter either ***Administrator*** or ***root***.

        c. At the **Password:** prompt, enter the password for the user entered above.

        d. To launch the Avaya command line interface, enter **/opt/Avaya/clish**.

    - **If logging in remotely:**

        a. Start your SSH shell application and connect to the IP Office Application Server PC. The exact method will depend on the application being used.

        - The **Host Name** is the IP address of the IP Office Application Server.

        - The **User Name** is ***web***.

        - The **Protocol** is ***SFTP/SSH***.

        - The **Port** is ***22***. If this is the first time the application has connected to the server, accept the trusted key.

        b. If this is the first time the application has connected to the IP Office Application Server, accept the trusted key.

        c. When prompted, enter the webcontrol user password 57, the default is ***webcontrol***.

    b. Enter **admin**. At the password prompt enter the admin password, the default is ***Administrator***. The prompt should change to ***Admin>***.

    c. Enter **root**. At the password prompt, enter the current root user password.

    d. The prompt should have changed to something similar to ***root@APPSDVD~]#***, indicating that you are now logged in as the root user.

    e. Change directory by entering **cd /home/Administrator**.

    f. Move the ***Custom*** sub-folder to ***/opt/vmpro*** by entering **mv Custom /opt/vmpro**.

3. Using the SSH file transfer tool again, verify that the ***Custom*** has been copied to ***/opt/vmpro*** as required.

Chapter 5.
one-X Portal for IP Office Configuration

5. one-X Portal for IP Office Configuration

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

one-X Portal for IP Office Initial Configuration

a. **Add licenses** 48
Those IP Office users who want to use the one-X Portal for IP Office application need to have their **Profile** set to ***Office Worker***, ***Teleworker*** or ***Power User*** and the **Enable one-X Portal Services** option selected. To do this requires the addition of licenses for those roles.

b. **Enable one-X Portal for IP Office users** 49
When licenses are available, the number of licenses allows the configuration of the equivalent number of users for those roles and then for one-X Portal for IP Office usage.

c. **Initial one-X Portal for IP Office login** 50
Having licensed and configured some users for one-X Portal for IP Office, you need to login as the one-X Portal for IP Office administrator in order to perform initial one-X Portal for IP Office configuration.

d. **Initial AFA login** 51
The one-X Portal for IP Office AFA interface is used for remote backup and restoration of the application. At minimum you should login in order to change the default password for the interface.

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

The IP address 169.254.0.1 is used for internal connected between the IP Office system and the one-X Portal for IP Office application on the Unified Communications Module. This address should not be used 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, the IP address of the Unified Communications Module should be used. To check the address, see Viewing the Module IP Address.

5.1 Adding Licenses

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

To enter licenses:

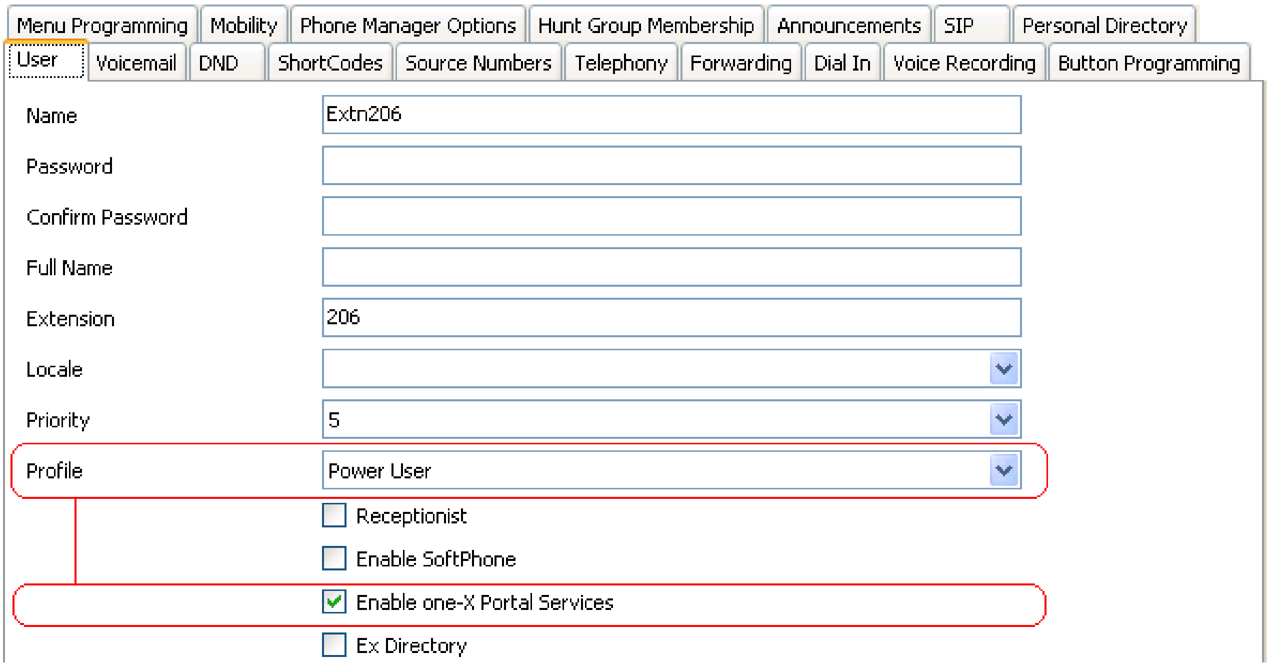
1. Start IP Office Manager and receive the configuration from the IP Office system.
2. Select **License**.
3. Click **Add** and select **ADI**.
4. Enter the new license and click **OK**. You should add licenses by cutting and pasting them from the supplied file. That avoids potential issues with mistyping.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

5.2 Enabling one-X Portal for IP Office Users

Those users who want to use the one-X Portal for IP Office application need to have their **Profile** set to ***Office Worker***, ***Teleworker*** or ***Power User*** and the **Enable one-X Portal Services** option selected. This requires available licenses 48 for those roles.

To enable one-X Portal for IP Office users:

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



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*** or ***Power User***.
7. Check that the **Enable one-X Portal Services** check box is selected.
8. Note the user **Name** and **Password**. These are used by the user to login to one-X Portal for IP Office.

10. Repeat the process for any other users who will be using one-X Portal for IP Office services.

11. Click on to save the updated configuration back to the IP Office system.

5.3 Initial one-X Portal for IP Office Login

The initial one-X Portal for IP Office configuration is done using web browser access to the administrator address.

To login to one-X Portal for IP Office:

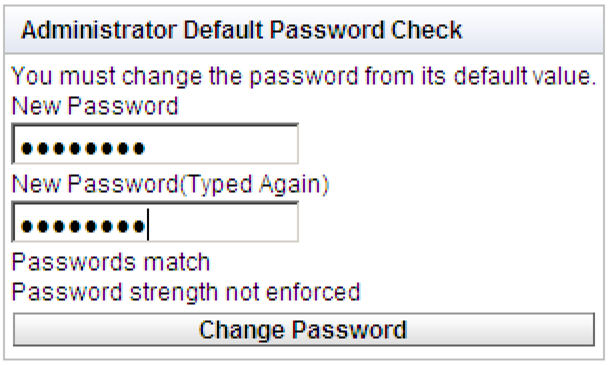
1. Open a web browser and enter the IP address of the IP Office Application Server followed by ***:8080/onexportal-admin.html***. This is the login path for the administrator access to the one-X Portal for IP Office application.

2. The login menu is displayed. If the message ***System is currently unavailable - please wait*** is displayed, the one-X Portal for IP Office application is still starting. When the message disappears, you can login.

3. Enter the default administrator name (***Administrator***) and password (***Administrator***) and click **Login**.

4. Follow the process for one-X Portal for IP Office initial configuration as described in the one-X Portal for IP Office Installation Manual.

5. As the final step, the one-X Portal for IP Office server will prompt you to change the password used for administrator access.



Administrator Default Password Check

You must change the password from its default value.

New Password

●●●●●●●●

New Password(Typed Again)

●●●●●●●●

Passwords match

Password strength not enforced

Change Password

6. Enter a new password and click **Change Password**.

7. 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.

8. Click on **Log Out**.

9. Click on **User Login** shown top-right.

10. The login window will display ***System in currently unavailable***. When this message is no longer displayed, attempt to login as a user.

5.4 Initial AFA Login

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

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

1. Open a web browser and enter the IP address of the IP Office Application Server followed by ***:8080/onexportal-afa.html***. This is the login path for the administrator access to the one-X Portal for IP Office AFA menus.

2. At the login menu, enter the name Superuser and the associated password. The default password is MyFirstLogin1_0. After logging with the default password you will be prompted the following information including a new password:

   - **Display Name**
     Enter a name for display in the one-X Portal for IP Office menus.

   - **Password/Confirm Password**
     Enter a password that will be used for future access.

   - **Backup Folder**
     This is the path to be used for backup and restore operations on the one-X Portal for IP Office server. Note that even if backing up and restoring to and from an FTP or local PC folder, this server folder is still used for temporary file storage.

5.5 Transferring one-X Portal for IP Office Settings

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

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

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

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

1. Browse to the old server using the address ***http://<server>:8080/onexportal-afa.html*** where *<server>* is the name or the IP address of the server.

2. At the login menu, enter the name **Superuser** and enter the associated password.

3. Select **DB Operations**.

4. Select **Backup**.

5. For **Backup To** select either ***FTP*** (an FTP server) or ***Local Drive*** (the PC from which you are browsing). If you select FTP, you will also need to complete address, name and password settings for uploading files to the FTP server.

6. Click **Backup**.

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

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

1. Browse to the new server using the address ***http://<server>:8080/onexportal-afa.html*** where *<server>* is the name or the IP address of the server.

2. At the login menu, enter the name **Superuser** and enter the associated password.

3. Select **DB Operations**.

4. Select **Restore**.

5. For **Restore From** select either ***FTP*** (an FTP server) or ***Local Drive*** (the PC from which you are browsing). If you select FTP, you will also need to complete address, name and password settings uploading files to the FTP server.

    - If you selected **FTP**:

        a. Click **Show Available Backups**.

        b. Select the backup to restore and click **Restore**.

    - If you selected **Local Drive**:

        a. Use the **Browse** option to select the backup file.

        b. Click **Restore**.

Chapter 6.
Server Maintenance

6. Server Maintenance

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

6.1 Accessing the menus

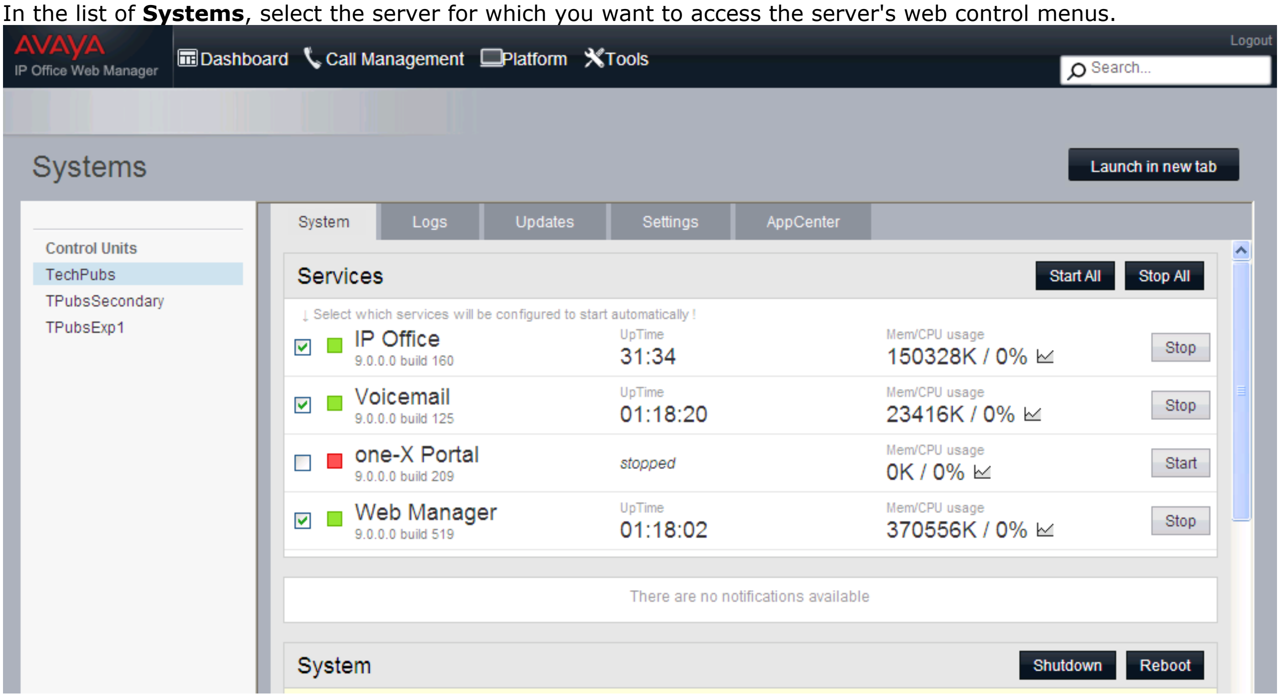
For IP Office Release 9.0, the web control menus for each server platform in the network can be accessed via IP Office Web Manager. This requires web control configured with **Enable referred authentication** selected which is the default for new systems. See Password Authentication 14.

Avaya supports the following web browsers:

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

To access the web control menus via IP Office Web Manager:

1. Log in to IP Office Web Manager.
   a. From a client PC, start the browser and enter ***https://*** followed by the address of the Server Edition primary server and then ***:7070***. For example: ***https://server.example.com:7070*** The server redirects the browser to the web manager pages.
   b. Enter the user name and password. The default name and password are ***Administrator*** and ***Administrator***.
2. Click **Platform**.
3. In the list of **Systems**, select the server for which you want to access the server's web control menus.



↓ Select which services will be configured to start automatically !

☑ 🟩	IP Office 9.0.0.0 build 160	UpTime 31:34	Mem/CPU usage 150328K / 0%	Stop
☑ 🟩	Voicemail 9.0.0.0 build 125	UpTime 01:18:20	Mem/CPU usage 23416K / 0%	Stop
□ 🟥	one-X Portal 9.0.0.0 build 209	stopped	Mem/CPU usage 0K / 0%	Start
☑ 🟩	Web Manager 9.0.0.0 build 519	UpTime 01:18:02	Mem/CPU usage 370556K / 0%	Stop

There are no notifications available

- The **Launch in new tab** button can be used to open the web control menus in a separate window. This may be necessary if the web control menus are set to use a different port or password.

6.2 Logging In Directly

This method of logging in is directly to the URL of the web control menus. For IP Office Release 9.0, it is preferable to access the web control menus via IP Office web management.

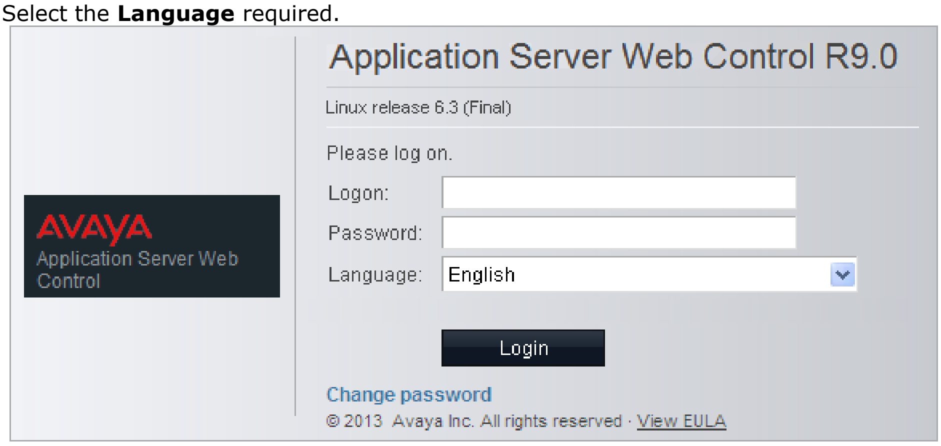
Avaya supports the following web browsers:

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

To login to the server web control menus:

1. From a client PC, start the browser. Enter ***http://*** followed by the address of the IP Office Application Server and ***:7071***.

2. Select the **Language** required.


AVAYA
Application Server Web Control
Application Server Web Control R9.0
Linux release 6.3 (Final)
Please log on.
Logon:
Password:
Login
Change password
© 2013 Avaya Inc. All rights reserved · View EULA

Language: English

3. Enter the name and password for IP Office Application Server administration. The default name and password are ***Administrator*** and ***Administrator***. To change the password, select the **Change Password** 57 option.

4. If the login is successful, the server's **System** 75 page appears.

6.3 Changing the Web Password

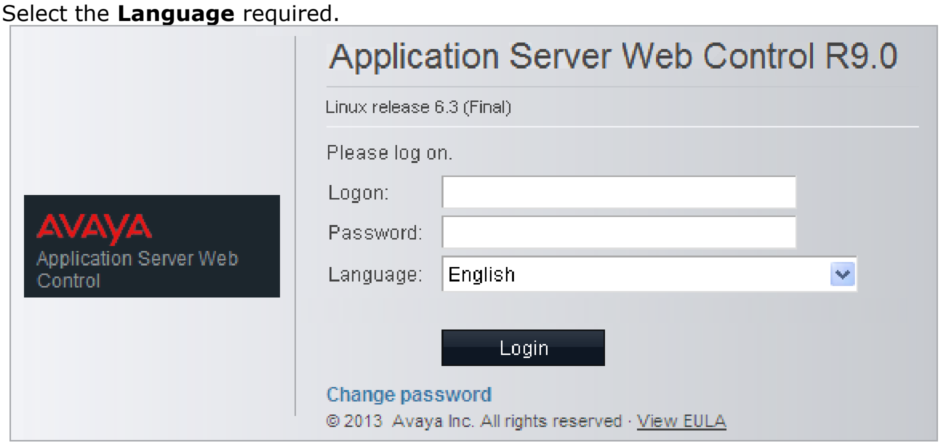
Changing the password from the web control log on menu changes the password stored by web control itself. Web control only uses that password if **Enable referred authentication** is not enabled. See Password Authentication 14.

If using IP Office Web Manager authentication (**Enable referred authentication** selected), you can change the user names and password used for access to web control through the IP Office Web Manager service user settings.

To change the browser password:

1. From a client PC, start the browser. Enter ***http://*** followed by the address of the IP Office Application Server and ***:7071***.

2. Select the **Language** required.



Application Server Web Control R9.0

Linux release 6.3 (Final)

Please log on.

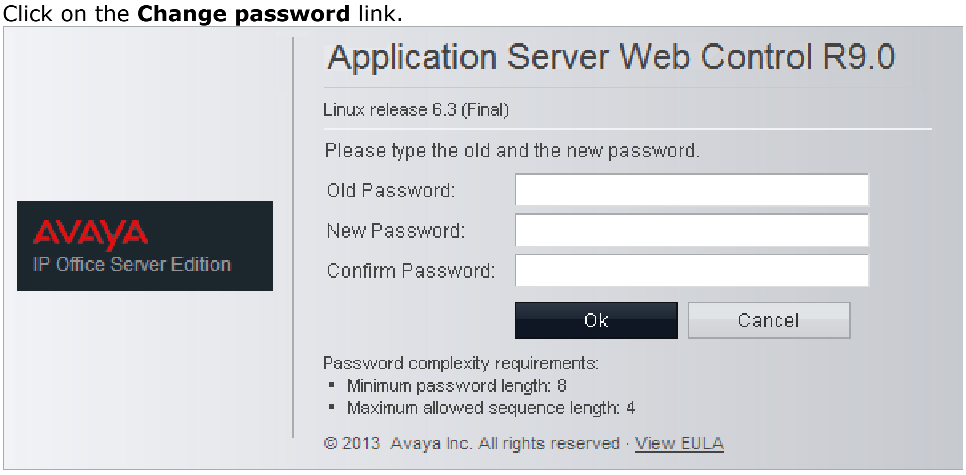
Logon:

Password:

Language: English

© 2013 Avaya Inc. All rights reserved · View EULA

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



Application Server Web Control R9.0

Linux release 6.3 (Final)

Please type the old and the new password.

Old Password:

New Password:

Confirm Password:

Password complexity requirements:
- Minimum password length: 8
- Maximum allowed sequence length: 4

© 2013 Avaya Inc. All rights reserved · View EULA

4. Enter the current password and the new password. The new password must meet the complexity requirements displayed on the menu.

5. Click **OK**. The menu confirms whether the change was successful or not. If the new password is accepted, click **Cancel** to return to the **Login** menu. .

6.4 Changing the Root Password

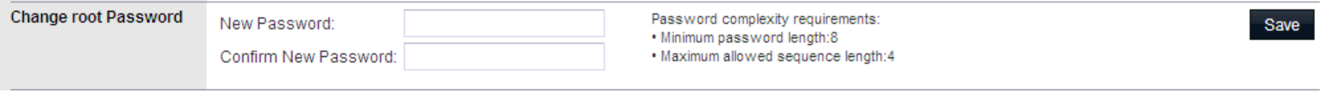
The root password for the server is set during the server installation. This is a password used for Linux command line access and so is not normally used during normal operation. However, for security you can change the root password through the web control menus.

To change the server root password:

1. Login 56 to the server's web configuration pages.

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

3. The new root password is set through the **Change Root Password** menu.



Change root Password

New Password:

Confirm New Password:

Password complexity requirements:
• Minimum password length:8
• Maximum allowed sequence length:4

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

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

4. Enter the new password.

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

6.5 Starting/Stopping Application Services

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

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

6.5.1 Starting a Service

To start a service:

1. Login 56 to the server's web configuration pages.
2. Select **System**. The services and their current status (running or stopped) are listed.
3. To start a particular service click on the **Start** button next to the service. To start all the services that are not currently running, click on the **Start All** button.

6.5.2 Stopping a Service

To stop a service:

1. Login 56 to the server's web configuration pages.
2. Select **System**. The services and their current status (running or stopped) are listed.
3. To start a particular service click on the **Stop** button next to the service. To stop all the services that are currently running, click on the **Stop All** button.
4. The service's status changes to stopping while it is being stopped. If it remains in this state too long, the service can be forced to stop by clicking on **Force Stop**.

6.5.3 Setting a Service to Auto Start

By default all the application services are automatically started.

To set a service to auto start:

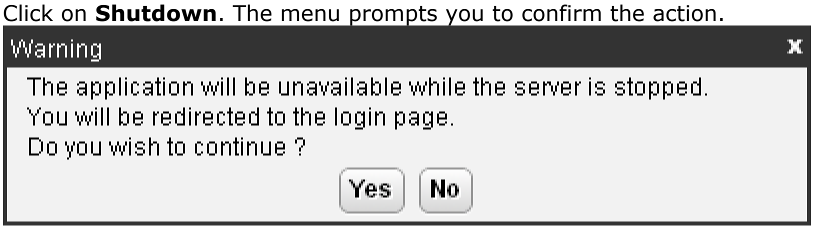
1. Login 56 to the server's web configuration pages.
2. Select **System**. The services and their current status (running or stopped) are listed.
3. Use the **Auto Start** check box to indicate whether a service should automatically start when the IP Office Application Server is started.

6.6 Server Shutdown

Use this process when it is necessary to switch off the IP Office Application Server for any period. Once the process has been completed, power to the server can be switched off. To restart the server, switch the server power back on.

To shutdown the server:

1. Login 56 to the server's web configuration pages.
2. After logging in, select the **Home** 75 page.
3. Click on **Shutdown**. The menu prompts you to confirm the action.



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

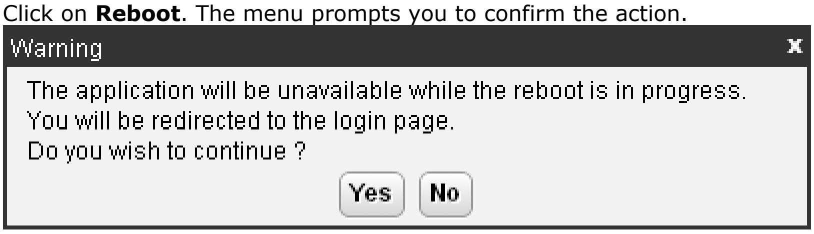
4. Click **Yes** to confirm that you want to proceed with the shutdown.
5. The login page appears again. Do not attempt to login again immediately.
6. After a few minutes, typically no more than 2 minutes, the server shuts down.
7. Switch off power to the server.

6.7 Rebooting the Server

Rebooting the server stops all currently running services and then stops and restarts the server. Only those application services set to **Auto Start** 59 automatically restart after the reboot.

To reboot the server:

1. Login 56 to the server's web configuration pages.
2. After logging in, select the **Home** 75 page.
3. Click on **Reboot**. The menu prompts you to confirm the action.



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**.

6.8 Changing the IP Address Settings

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

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

To change the IP address:

1. Login 56 to the server's web configuration pages.
2. Select **Settings**.
3. Select **System**.
4. Set the **Network** section as required.
   - **Network Interface**
     This drop down allows selection of network interfaces is currently being configured by the web form. Within the IP Office configuration, ***Eth0*** matches LAN1, ***Eth1*** matches LAN2. On the pre-built IP Office Application Server only ***Eth0*** is used. This port is labeled as port 1 on the physical server.
   - **Host Name**
     Sets the host name that the IP Office Application Server should use. This setting requires the local network to support a DNS server. Do not use ***localhost***.
     - **! WARNING**
       For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.
   - **Use DHCP**
     If selected, the IP address, subnet mask and default gateway information is obtained by the server making DHCP requests. The related fields are greyed out and cannot be set manually, instead they show the values obtained in response to the DHCP request.
   - **IP Address**
     Displays the IP address set for the server. If DHCP is not being used, the field can be edited to change the setting.
     - **! WARNING**
       For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.
   - **Subnet Mask**
     Displays the subnet mask applied to the IP address. If DHCP is not being used, the field can be edited to change the setting.
   - **Default Gateway**
     Displays the default gateway settings for routing. If DHCP is not being used, the field can be edited to change the setting.
   - **System DNS**
     Enter the address of the primary DNS server. This option is greyed out if the address of the DNS server is set to be obtained from the DHCP server (see below).
   - **Automatically obtain DNS from provider**
     This setting is only used if **Use DHCP** is also selected. If selected, the server attempts to obtain DNS server details from the DHCP server.
5. Click **Save**. The server restarts.

6.9 Date and Time Settings

The date and time settings used by the server PC can be changed through the server's web configuration pages. The current time being used by the server is shown on the **System** 75 menu.

To change the server date and time settings:

1. Login 56 to the server's web configuration pages.

2. Select **Settings**.

3. Select **System**.

4. The date and time settings are shown in the **Date Time** section.

   - **Date**
     Shows the current date being used by the server. If **Enable Network Time Protocol** is selected, this is the date obtained from the NTP server and cannot be manually changed.

   - **Time**
     Shows the current UTC time being used by the server. If **Enable Network Time Protocol** is selected, this is the time obtained from the NTP server and cannot be manually changed. The current time being used by the server is shown on the **System** 75 menu.

   - **Timezone**
     In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field is used to determine the appropriate offset that should be applied to the UTC time above. Note that changing the timezone can cause a Session expired message to appear in the browser.

     - **! WARNING**
       For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

   - **Enable Network Time Protocol**
     If this option is selected, the IP Office Application Server will attempt to obtain the current UTC time from the NTP servers listed in the **NTP Servers** list below. It will then use that time and make regular NTP requests to update the date and time. The following options are only used if **Enable Network Time Protocol** is selected.

     - **NTP Servers**
       This field is used to enter the IP address of an NTP server or servers which should be used when **Enable Network Time Protocol** is selected. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome, however it is your responsibility to make sure you are aware of the usage policy for any servers you choose. Choosing several unrelated NTP servers is recommended in case one of the servers you are using becomes unreachable or its clock is unreliable. The operating system uses the responses it receives from the servers to determine which are reliable.

       - The IP Office system can also use NTP to obtain its system time. Using the same servers for the IP Office Application Server and IP Office system is recommended.

     - **Synchronize system clock before starting service**
       When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, an immediate update of the server's clock to match the NTP obtained time is forced.

     - **Use local time source**
       When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, the server's hardware clock time is used as the current time rather than the NTP time.

5. Click **Save**.

6.10 Setting the Menu Inactivity Timeout

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

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

To change the menu inactivity timeout:

1. Login 56 to the server's web configuration pages.
2. Select **Settings**.
3. Select **General**.
4. The **Inactivity timeout** is shown in the **Web Control** section.
   - **Inactivity Timeout**
     Select the period of inactivity after which the web session is automatically logged out. Changing this value will require you to login again. The options are ***5 minutes***, ***10 minutes***, ***30 minutes*** and ***1 hour***.
5. Click **Save**. The server will advise you that it is restarting the web service and that you will need to login again.

6.11 Upgrading Applications

The application services hosted by the IP Office Application Server can be upgraded without having to reinstall or upgrade the whole server. This is done using files either uploaded to the server (local) or downloaded by the server from an HTTP folder (remote repository), see File Repositories 69.

Once an .rpm file or files are available, the IP Office Application Server web configuration pages will list the available versions and allow switching between versions or simple upgrading to the latest version.

- **! Upgrade Warning**
  Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.

- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading.

The options in this section cover the upgrading of individual components of the operating system and applications supported by the IP Office Application Server.

6.11.1 Loading Application Files onto the Server

This method uploads the .rpm file for an application onto the IP Office Application Server. The files can then be used to update the applications. The alternative is to use files loaded into a remote software repository 71.

To upload application files onto the server:

1. Login 56 to the server's web configuration pages.

2. Select the **Settings** menu and then the **General** sub-menu.

3. Check that the **Local** checkbox for **Applications** is selected.

4. Click on the **Browse** button and browse to the location of the file 69 that you want to load and select the file. The file name should now be listed in the **File** field.

5. Click **Add**. The server will now start uploading the file.

6. Repeat the process for any other files.

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

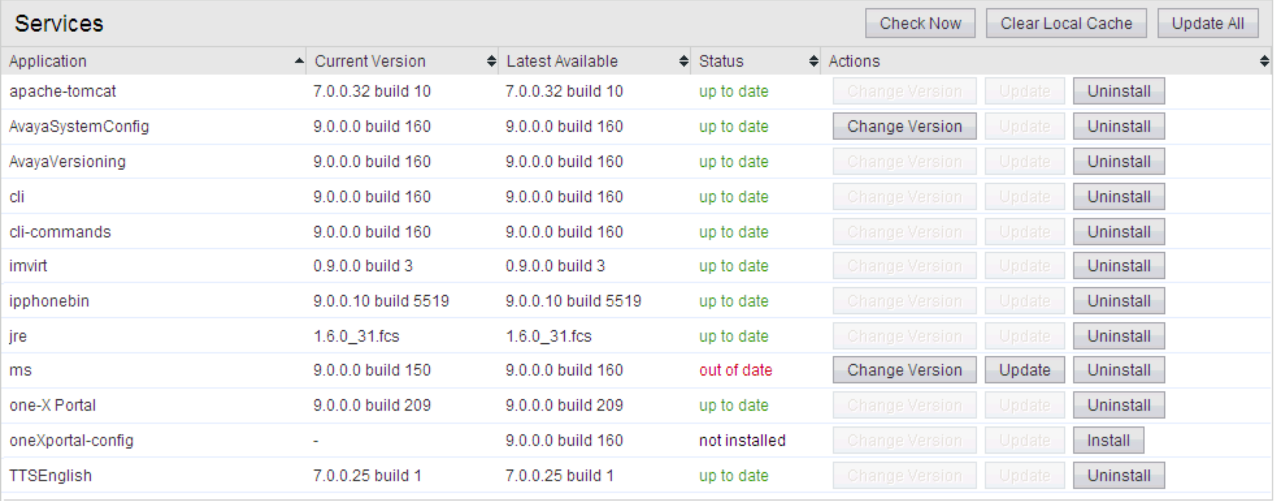
6.11.2 Upgrading Application Files

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

To upgrade application files:

1. Login 56 to the server's web configuration pages.

2. Select the **Updates** page.



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

3. The **Services** section displays the current version and latest available version of each application service.

   - Some applications may not support upgrading or downgrading whilst the application is currently installed. For those applications, the **Change Version** and **Update** buttons remain greyed out even if there are updates available in the application file repository. These applications must first be uninstalled using the **Uninstall** button before the **Change Version** and **Update** buttons become useable.

4. Select one of the following actions:

   - To update an application to the latest version available, click on **Update**.
   - To update all applications to the latest version available, click on **Update All**.
   - To change the current version of an application, click on **Change Version**. Select the version required and click **Apply**.

6.11.3 Upgrading Using USB

Upgrading the IP Office Application Server through the use of RPM or ZIP files is recommended 64. However, if necessary, a USB2 memory key can be used to perform an upgrade.

6.11.3.1 Preparing a USB2 Upgrade Key

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

- **! Upgrade Warning**
  Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.

- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading.

Prerequisites

- **8GB USB2 Memory Key**
  Note that all existing files on this device will be erased.

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

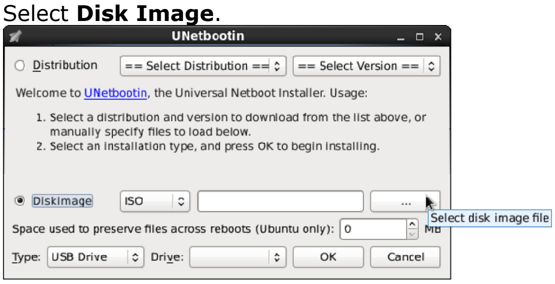
- **IP Office Application Server ISO File**
  You can download this software from the Avaya support website (http://support.avaya.com).

To create a bootable USB2 memory key:

1. Erase all files on USB2 memory key and reformat it as a FAT32 device.

2. Start the **unetbootin** application.

3. Select **Disk Image**.

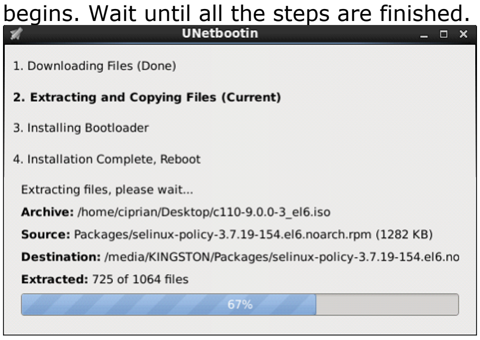


Welcome to UNetbootin, the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

4. Click the **...** browse button and select the ISO file.

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



1. Downloading Files (Done)

2. Extracting and Copying Files (Current)

3. Installing Bootloader

4. Installation Complete, Reboot

Extracting files, please wait...
Archive: /home/ciprian/Desktop/c110-9.0.0-3_el6.iso
Source: Packages/selinux-policy-3.7.19-154.el6.noarch.rpm (1282 KB)
Destination: /media/KINGSTON/Packages/selinux-policy-3.7.19-154.el6.no
Extracted: 725 of 1064 files

6. When the process has ended, click **Exit**. Do not click **Reboot now**.

7. Using the file explorer, open the USB folder on the USB2 memory key.

8. Select the file **syslinux.cfg** and copy it to the top level (root) folder, overwriting any existing file with that name.

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

6.11.3.2 Upgrading Using a USB2 Upgrade Key

- **! Upgrade Warning**
  Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.

- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading.

To upgrade from a USB2 memory key:

1. Prepare a bootable USB2 upgrade key. See Preparing a USB2 Upgrade Key 66.

2. Insert the USB2 upgrade key into a USB socket and reboot the server 60.

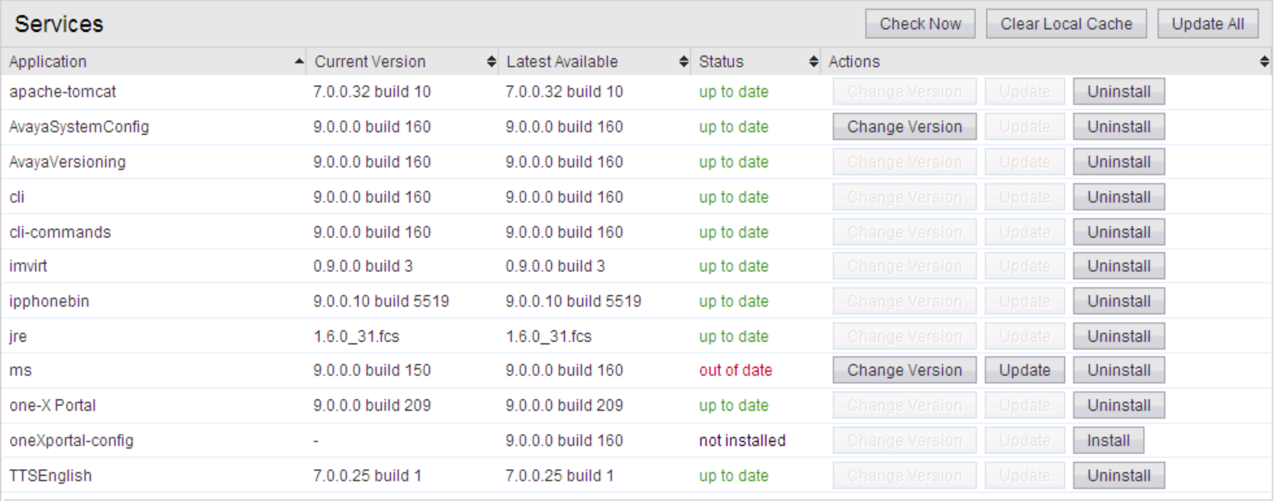
3. Follow the same process as for Software Installation 21. However, when the upgrade menu appears, select **Upgrade** rather than **Install**.

6.12 Uninstalling an Application

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

To uninstall an application:

1. Login 56 to the server's web configuration pages.
2. Select the **Updates** page.



Services

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

3. The **Services** section displays the current version and latest available version of each application service.
4. To uninstall a service, click on **Uninstall**.
   - If there are installation files for the application available in the application file repository 69, the button will change to become an **Install** button.
   - If there are no installation files for the application available in the file repository, the application is no longer listed.

6.13 File Repositories

The **Updates** 82 and **Web Client** 96 menus use files stored in the configured file repositories. Each repository can be either a set of files uploaded to the sever or the URL of a remote folder on an HTTP server.

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

6.13.1 Source Files

Update files may be made available individually in response to particular issues or to support new IP Office releases. The files are also included on the IP Office Application Server DVD. Files can be extracted from a DVD .iso image using an application such as WinZip.

- **! Upgrade Warning**
  Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.

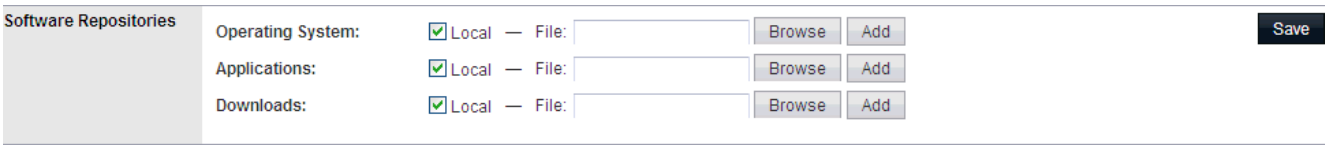
- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading.

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

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

6.13.2 Setting the Repository Locations

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



Software Repositories

Operating System: ☑ Local — File: Browse Add

Applications: ☑ Local — File: Browse Add

Downloads: ☑ Local — File: Browse Add

Save

The files uploaded or present in the file repositories are used by the **Updates** 82 and **AppCenter** 96 menus.

- **Repository**
  If the **Local** option is not selected, this field is used to set the URL of a remote HTTP file repository 71. Note that each repository must be different, the same URL must not be used for multiple repositories.

- **Local**
  This checkbox is used to set whether the file repository used is local (files stored on the IP Office Application Server or remote (a folder on a HTTP web server specified in the Repository field).

- **File / Browse / Add**
  If the Local option is selected, this field and adjacent buttons can be used to browse to a specific update file. When the file is located and selected, click **Add** to upload the file to the file store on the IP Office Application Server.

6.13.3 Uploading Local Files

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

6.13.3.1 Uploading Application Files

This method uploads the .rpm file for an application onto the IP Office Application Server. The files can then be used to update the applications. The alternative is to use files loaded into a remote software repository 71.

To upload application files onto the server:

1. Login 56 to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Applications** is selected.
4. Click on the **Browse** button and browse to the location of the file 69 that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.
   - **Voicemail Pro**
     Each version of the Voicemail Pro server application is split into separate .rpm files for the server and each of the prompt languages it supports. Unless advised otherwise, you should copy or upload the full set of files to the file repository.

6.13.3.2 Uploading Operating System Files

This method uploads the .rpm file for an application onto the IP Office Application Server. The files can then be used to update the IP Office applications. The alternative is to use files loaded into a remote software repository 71.

To upload operating system files:

1. Login 56 to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Operating System** is selected.
4. Click on the **Browse** button and browse to the location of the file 69 that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.

6.13.3.3 Uploading Windows Client Files

This method uploads the .rpm file for an application onto the IP Office Application Server. The files can then be used to update the IP Office applications. The alternative is to use files loaded into a remote software repository 71.

To upload Windows client files:

1. Login 56 to the server's web configuration pages.
2. Select the **Settings** menu and then the **General** sub-menu.
3. Check that the **Local** checkbox for **Downloads** is selected.
4. Click on the **Browse** button and browse to the location of the file 69 that you want to load and select the file. The file name should now be listed in the **File** field.
5. Click **Add**. The server will now start uploading the file.
6. Repeat the process for any other files.

6.13.4 Creating Remote Software Repositories

Alternatively to using local files uploaded to the server 64 for updates, the server can be configured to display the versions of files available for use in remote file folders hosted on an HTTP server.

To create an application update repository:

1. Create a folder on the web server for the remote file repository. For example a folder called ***Applications***.
2. If the folder is a sub-folder of the existing web site it will be browseable as part of that website's URL, ie. if the folder is a sub-folder of ***wwwroot***. If the folder is on a separate path, then it must be mapped to the web server URL path, the process for this will depend on the HTTP server being used.
3. The folder directory must be browseable. For example, in IIS right -click on the folder, select **Properties** and ensure that **Directory Browse** option is selected.
4. Copy the .rpm files from their source 69 into the folder.
5. From another PC, test that you can browse to the URL of the folder and that the list of files in the folder is displayed.
6. Login to the IP Office Application Server web configuration pages.
7. Select **Settings** and then **General**.
8. Uncheck the **Local** checkbox for **Applications**. Enter the URL of the HTTP server folder into the preceding field.
9. Click **Save**.
10. Select **Updates**.
11. If the server is able to access the HTTP folder, the details of the versions available will now reflect those available in that folder. The message ***repository error*** indicates that the IP Office Application Server was not able to connect to the folder or not able to list the files in the folder.

To create a Windows client repository:

The process is the similar to that shown above for application .rpm files. However a separate folder on the HTTP server must be used and the files placed in it are the .exe files used for installing the Windows applications.

To create an operating system repository:

The repository for operating system updates is different from those used for application updates and downloads. It must be a YUM repository, details of how to setup and configure a YUM repository will depend on the version of Linux being used on the HTTP server. Each time an .rpm file is added, deleted or changed, the directory must be updated using the **createrepo *<folder_path>*** command.

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

6.14 Using VNC

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

- VNC access using the root user account is not supported. Some applications, for example Wireshark, require root user permissions and so cannot be used when accessing the server via VNC.

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

1. Starting the VNC service 72.
2. Viewing the desktop via VNC 72.

6.14.1 Starting the VNC Service

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

To start the VNC service:

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

6.14.2 Viewing the Desktop Via VNC

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

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

To view the server desktop:

1. Login and select the **VNC** tab.
2. Select **Settings**.
3. Check that the **Start VNC** button is greyed out. That indicates that the VNC service is running. If the button is not greyed out, see Starting the VNC Service 72.
4. Select the **View** tab.
5. Enter the password. This must match the password that was used to start the VNC service.
6. Click **OK**.
7. The server desktop is displayed.
8. To end the connection at any time, click **Disconnect**.

6.14.3 Stopping the VNC Service

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

To stop the VNC service:

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

Chapter 7. Server Menus

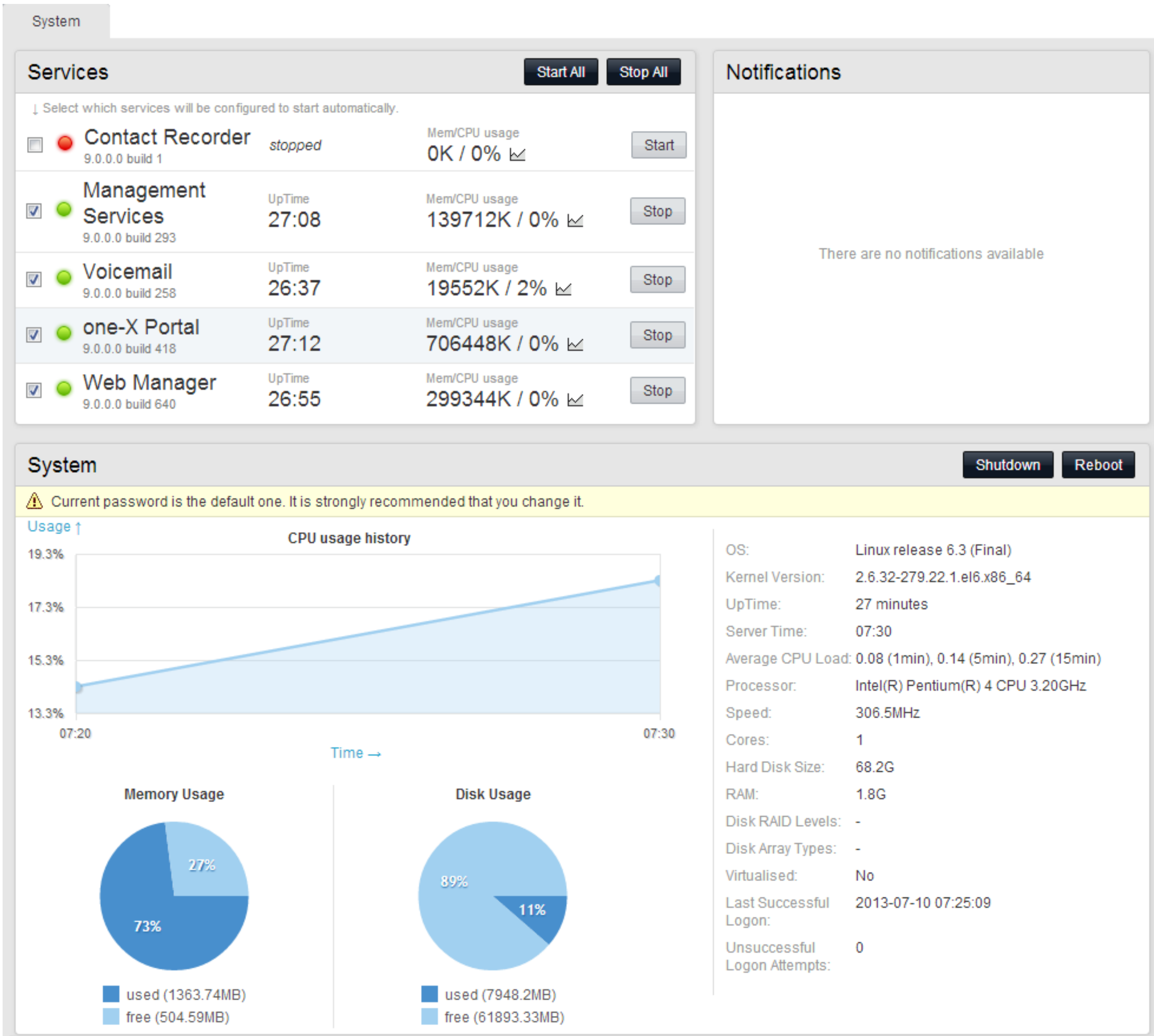
7. Server Menus

The IP Office Application Server web configuration pages are as follows:

- **System** 75
  This menu gives an overview of the current status of the applications hosted on the server.
- **Logs** 79
  This menu has sub-menus for viewing and managing log records and log files.
  - **Debug Logs** 79
    View the current log files for the server and the application services hosted by the server.
  - **Syslog Event Viewer** 80
    View Syslog log records received and or generated by the server.
  - **Download** 81
    Create and download archive files of existing log records.
- **Updates** 82
  Display the versions of applications and components installed and the alternate versions available.
- **Settings** 85
  This menu has sub-menus for various areas of server configuration and operation.
  - **General** 86
    General server settings such as the locations of software update repositories.
  - **System** 91
    View and manage the server setting for date, time and IP address details.
- **AppCenter** 96
  This page can be used to download the installation packages for Windows applications such as the Voicemail Pro client application.

7.1 System

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



System

Services [Start All] [Stop All]

↓ Select which services will be configured to start automatically.

☐ ●	Contact Recorder 9.0.0.0 build 1	*stopped*	Mem/CPU usage 0K / 0%	[Start]
☑ ●	Management Services 9.0.0.0 build 293	UpTime 27:08	Mem/CPU usage 139712K / 0%	[Stop]
☑ ●	Voicemail 9.0.0.0 build 258	UpTime 26:37	Mem/CPU usage 19552K / 2%	[Stop]
☑ ●	one-X Portal 9.0.0.0 build 418	UpTime 27:12	Mem/CPU usage 706448K / 0%	[Stop]
☑ ●	Web Manager 9.0.0.0 build 640	UpTime 26:55	Mem/CPU usage 299344K / 0%	[Stop]

Notifications

There are no notifications available

System [Shutdown] [Reboot]

⚠ Current password is the default one. It is strongly recommended that you change it.

OS:	Linux release 6.3 (Final)
Kernel Version:	2.6.32-279.22.1.el6.x86_64
UpTime:	27 minutes
Server Time:	07:30
Average CPU Load:	0.08 (1min), 0.14 (5min), 0.27 (15min)
Processor:	Intel(R) Pentium(R) 4 CPU 3.20GHz
Speed:	306.5MHz
Cores:	1
Hard Disk Size:	68.2G
RAM:	1.8G
Disk RAID Levels:	-
Disk Array Types:	-
Virtualised:	No
Last Successful Logon:	2013-07-10 07:25:09
Unsuccessful Logon Attempts:	0

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

  - **Web Manager**
    Server settings are configured and managed via web browser access to the web control menus detailed in this document.

  - **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 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 user's can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely using web browser access. Each user who wants to use one-X Portal for IP Office requires a license 14.

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

  - **Contact Recorder for IP Office**
    Contact Recorder for IP Office is an application used in conjunction with Voicemail Pro. It provides long term storage and retrieval of call recordings. The call recordings are made by Voicemail Pro. Those recordings and call details are then collected by Contact Recorder for IP Office and stored by it. For details on Contact Recorder for IP Office installation, refer to the Contact Recorder for IP Office Installation Manual.

    - The Contact Recorder for IP Office application should only be run on a separate application server. It should not be run on the same server as the Voicemail Pro application.

- **Notifications**
  This table gives a summary of the most recent log messages generated by the services running on the IP Office Application Server. More detailed information is available through the **Logs** 79 page.

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

  - **OS/Kernel:**
    The overall version of the Linux operating system installed on the server and the version of the operating system kernel.

  - **Up Time:**
    This field shows the system running time since the last server start.

  - **Server Time:**
    This field shows the current time on the server.

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

  - **Speed**:
    Indicates the processor speed.

  - **Cores:**
    Indicates the number of processor cores.

  - **Hard Disk Size:**
    Indicates the hard disk size.

  - **RAM:**
    Indicates the amount of RAM memory.

  - **Disk RAID Levels:**
    Indicates the RAID type, if any, being used.

  - **Disk Array Types:**
    Indicates the type of disk array being used for RAID.

  - **Virtualized:**
    Indicates whether the server is running as a virtualized session.

  - **Last Successful Logon:**
    This field shows the date and time of the last successful logon, including the current logon.

  - **Unsuccessful Logon Attempts:**
    This field shows a count of unsuccessful logon attempts.

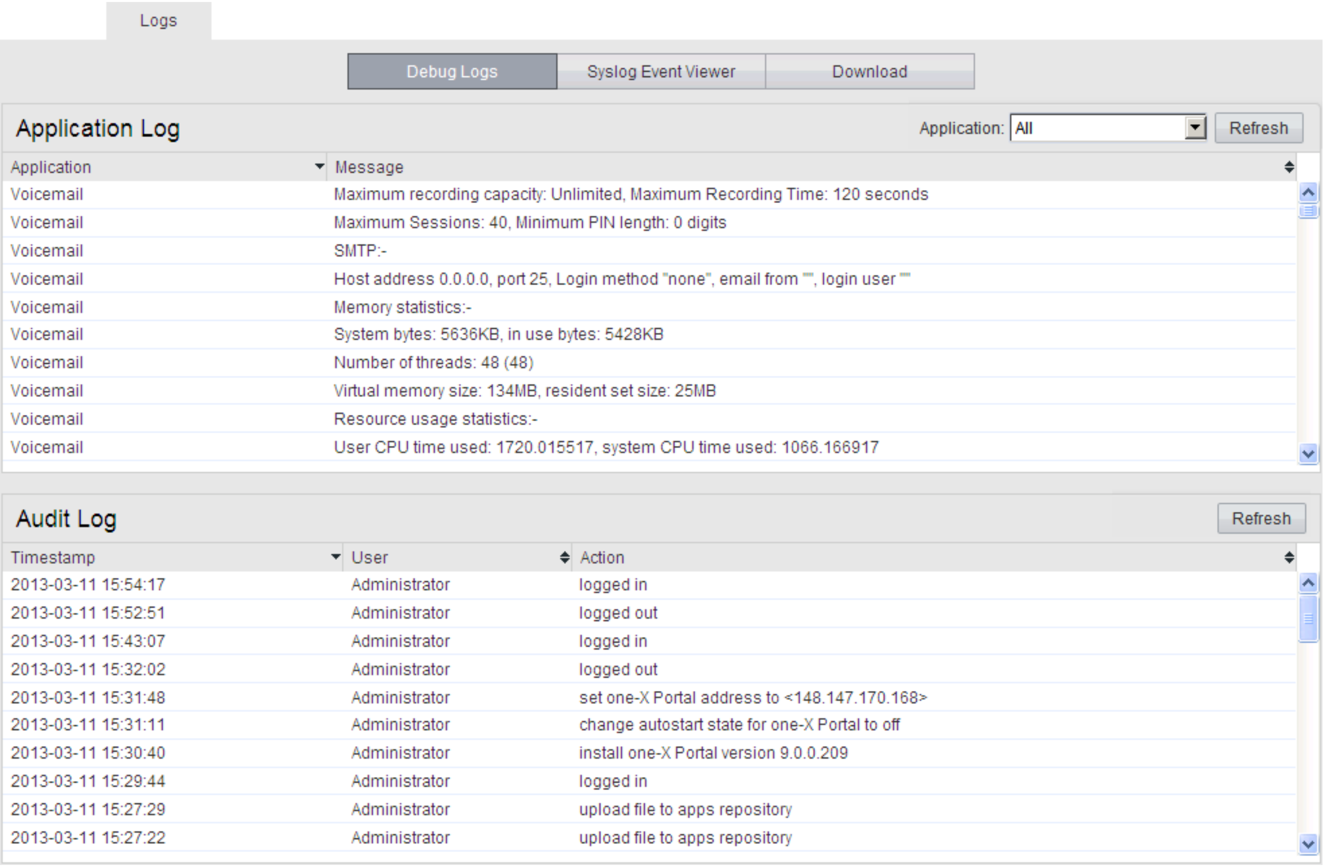
- **Shutdown**
  Selecting this button will start a process that will stop all the application services and then shutdown IP Office Application Server. This process should be used when it is necessary to switch off the IP Office Application Server for any period. Once the process has been completed, power to the server can be switched off. To restart the server, switch the server power back on.

- **Reboot**
  Selecting this button will start a process that will stop all the application services and then stop and restart the IP Office Application Server and services. Note that this stops all services. To stop and restart individual application services, use the buttons shown for each service in the **Services** panel above.

7.2 Logs

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

- **Debug Logs** 79
  View the current log files for the server and the application services hosted by the server.
- **Syslog Event Viewer** 80
  View Syslog log records received and or generated by the server.
- **Download** 81
  Create and download archive files of existing log records.



Application Log

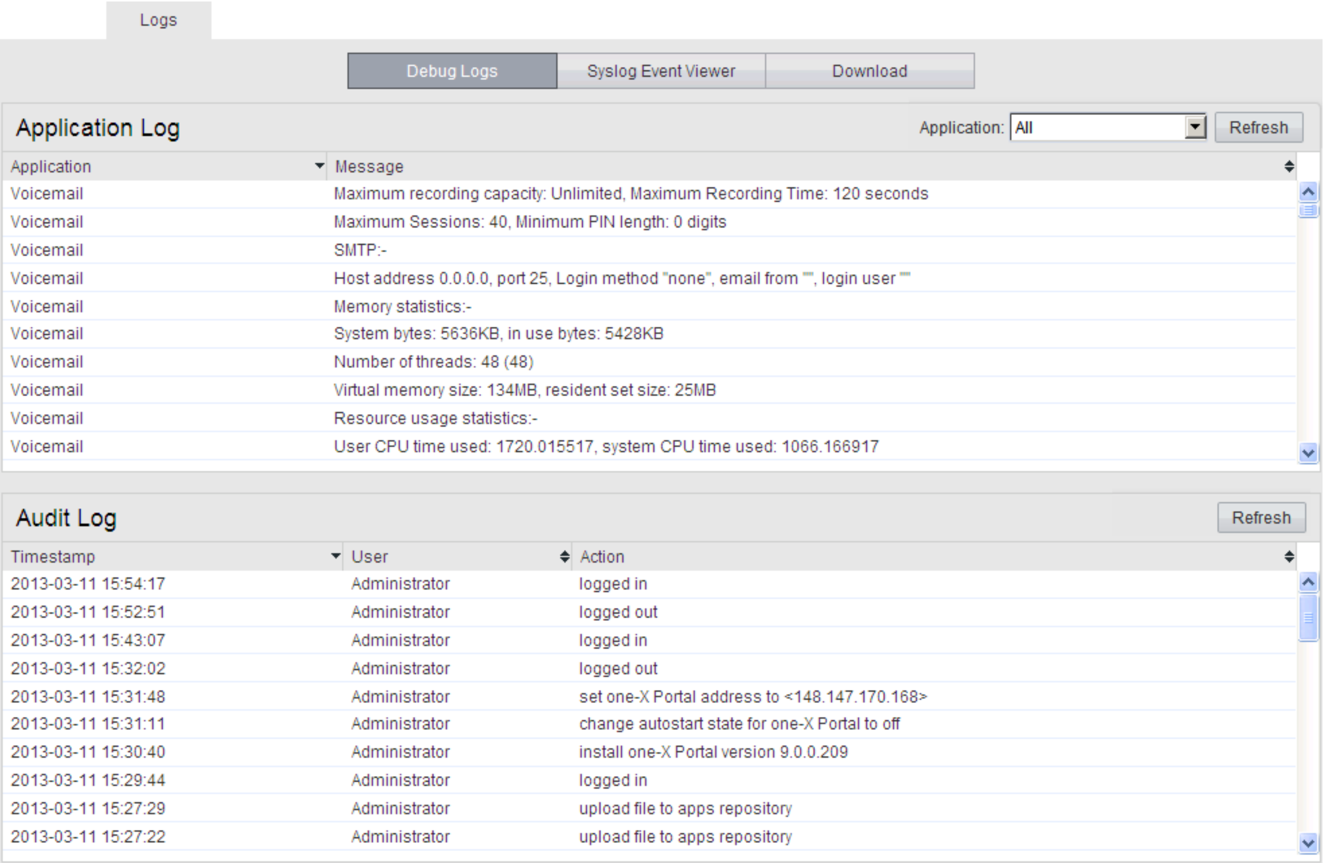
Application	Message
Voicemail	Maximum recording capacity: Unlimited, Maximum Recording Time: 120 seconds
Voicemail	Maximum Sessions: 40, Minimum PIN length: 0 digits
Voicemail	SMTP:-
Voicemail	Host address 0.0.0.0, port 25, Login method "none", email from "", login user ""
Voicemail	Memory statistics:-
Voicemail	System bytes: 5636KB, in use bytes: 5428KB
Voicemail	Number of threads: 48 (48)
Voicemail	Virtual memory size: 134MB, resident set size: 25MB
Voicemail	Resource usage statistics:-
Voicemail	User CPU time used: 1720.015517, system CPU time used: 1066.166917

Audit Log

Timestamp	User	Action
2013-03-11 15:54:17	Administrator	logged in
2013-03-11 15:52:51	Administrator	logged out
2013-03-11 15:43:07	Administrator	logged in
2013-03-11 15:32:02	Administrator	logged out
2013-03-11 15:31:48	Administrator	set one-X Portal address to <148.147.170.168>
2013-03-11 15:31:11	Administrator	change autostart state for one-X Portal to off
2013-03-11 15:30:40	Administrator	install one-X Portal version 9.0.0.209
2013-03-11 15:29:44	Administrator	logged in
2013-03-11 15:27:29	Administrator	upload file to apps repository
2013-03-11 15:27:22	Administrator	upload file to apps repository

7.2.1 Debug Logs

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



Application	Message
Voicemail	Maximum recording capacity: Unlimited, Maximum Recording Time: 120 seconds
Voicemail	Maximum Sessions: 40, Minimum PIN length: 0 digits
Voicemail	SMTP:-
Voicemail	Host address 0.0.0.0, port 25, Login method "none", email from "", login user ""
Voicemail	Memory statistics:-
Voicemail	System bytes: 5636KB, in use bytes: 5428KB
Voicemail	Number of threads: 48 (48)
Voicemail	Virtual memory size: 134MB, resident set size: 25MB
Voicemail	Resource usage statistics:-
Voicemail	User CPU time used: 1720.015517, system CPU time used: 1066.166917

Timestamp	User	Action
2013-03-11 15:54:17	Administrator	logged in
2013-03-11 15:52:51	Administrator	logged out
2013-03-11 15:43:07	Administrator	logged in
2013-03-11 15:32:02	Administrator	logged out
2013-03-11 15:31:48	Administrator	set one-X Portal address to <148.147.170.168>
2013-03-11 15:31:11	Administrator	change autostart state for one-X Portal to off
2013-03-11 15:30:40	Administrator	install one-X Portal version 9.0.0.209
2013-03-11 15:29:44	Administrator	logged in
2013-03-11 15:27:29	Administrator	upload file to apps repository
2013-03-11 15:27:22	Administrator	upload file to apps repository

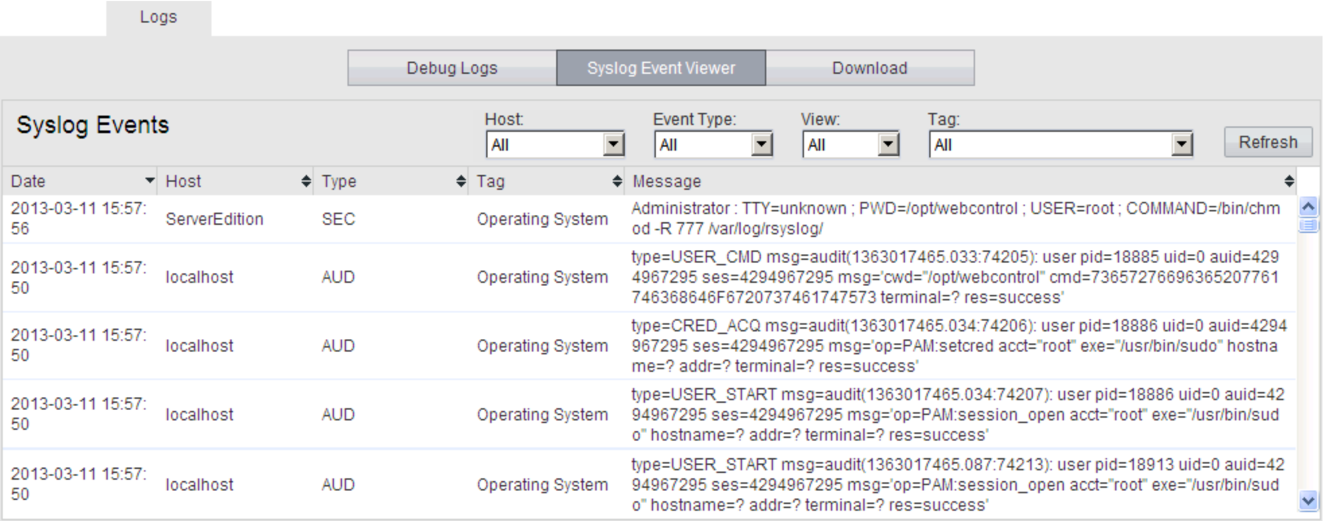
- **Application Log**
  This table lists the log records for a selected server application supported by the IP Office Application Server. The **Application** drop-down is used to select which records are shown. Clicking on a column header sorts the records using that column. The records shown are all those generated since the last time the log files were archived using the **Create Archive** command on the **Logs | Download** 81 page. For Voicemail Pro the level of log information output is set through the **Debug** section of the **Settings | General** 86 menu. For one-X Portal for IP Office the level of log information output is set through the applications own administration menus, not through the IP Office Application Server menus.

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

7.2.2 Syslog Event Viewer

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

The Settings | General 86 menu is used to configure the sending and receiving of Syslog records by the server to and from other servers. It is also used to configure how long the server keeps different types of records and how many.



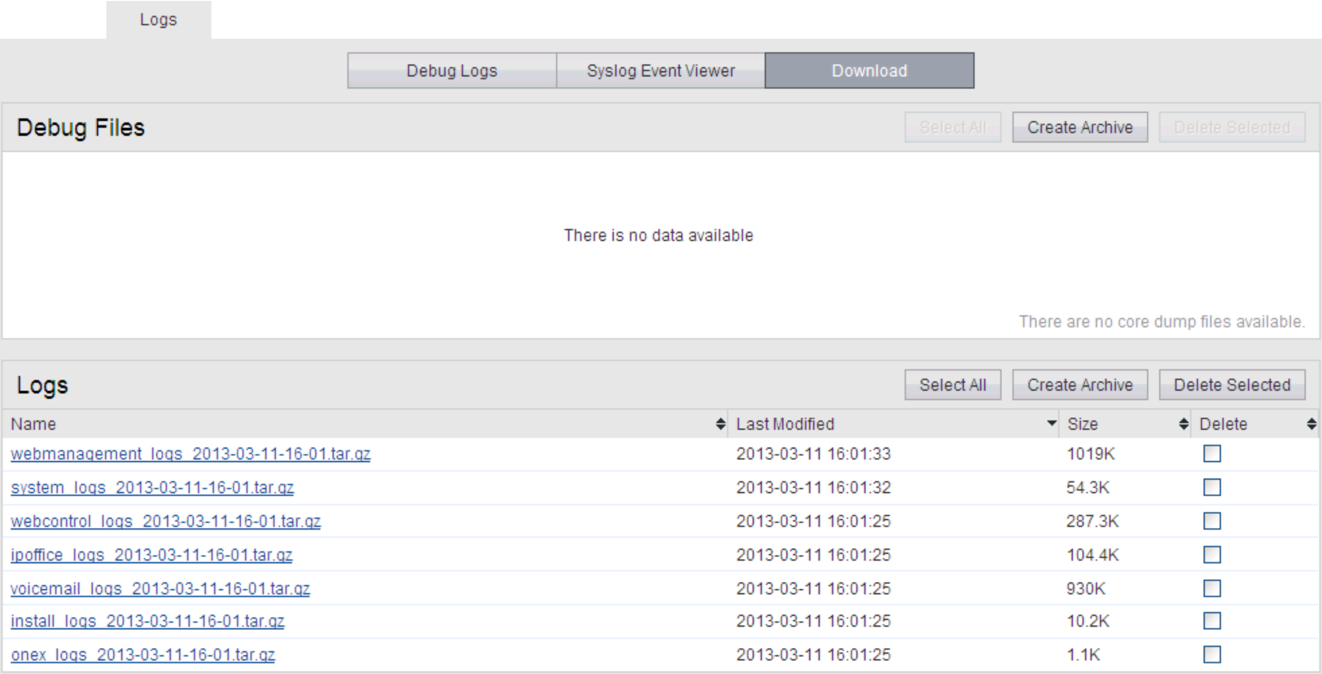
Host: All
Event Type: All
View: All
Tag: All

Date	Host	Type	Tag	Message
2013-03-11 15:57:56	ServerEdition	SEC	Operating System	Administrator : TTY=unknown ; PWD=/opt/webcontrol ; USER=root ; COMMAND=/bin/chmod -R 777 /var/log/rsyslog/
2013-03-11 15:57:50	localhost	AUD	Operating System	type=USER_CMD msg=audit(1363017465.033:74205): user pid=18885 uid=0 auid=4294967295 ses=4294967295 msg='cwd="/opt/webcontrol" cmd=736572766963652077617463686646F6720737461747573 terminal=? res=success'
2013-03-11 15:57:50	localhost	AUD	Operating System	type=CRED_ACQ msg=audit(1363017465.034:74206): user pid=18886 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'
2013-03-11 15:57:50	localhost	AUD	Operating System	type=USER_START msg=audit(1363017465.034:74207): user pid=18886 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:session_open acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'
2013-03-11 15:57:50	localhost	AUD	Operating System	type=USER_START msg=audit(1363017465.087:74213): user pid=18913 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:session_open acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'

7.2.3 Download

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

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



There is no data available

There are no core dump files available.

Name	Last Modified	Size	Delete
webmanagement_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:33	1019K	□
system_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:32	54.3K	□
webcontrol_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	287.3K	□
ipoffice_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	104.4K	□
voicemail_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	930K	□
install_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	10.2K	□
onex_logs_2013-03-11-16-01.tar.gz	2013-03-11 16:01:25	1.1K	□

To create archive files:

1. Click on the **Create Archive** button. Any log records recorded since the last creation of an archive are placed into archive files for each service.

2. The new archive files are listed in the web page.

To download archive files:

1. Any archive file can be downloaded by clicking on the file name of the archive file.

2. The process for the download and the location to which the file is downloaded will depend on the browser being used.

To delete archive files:

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

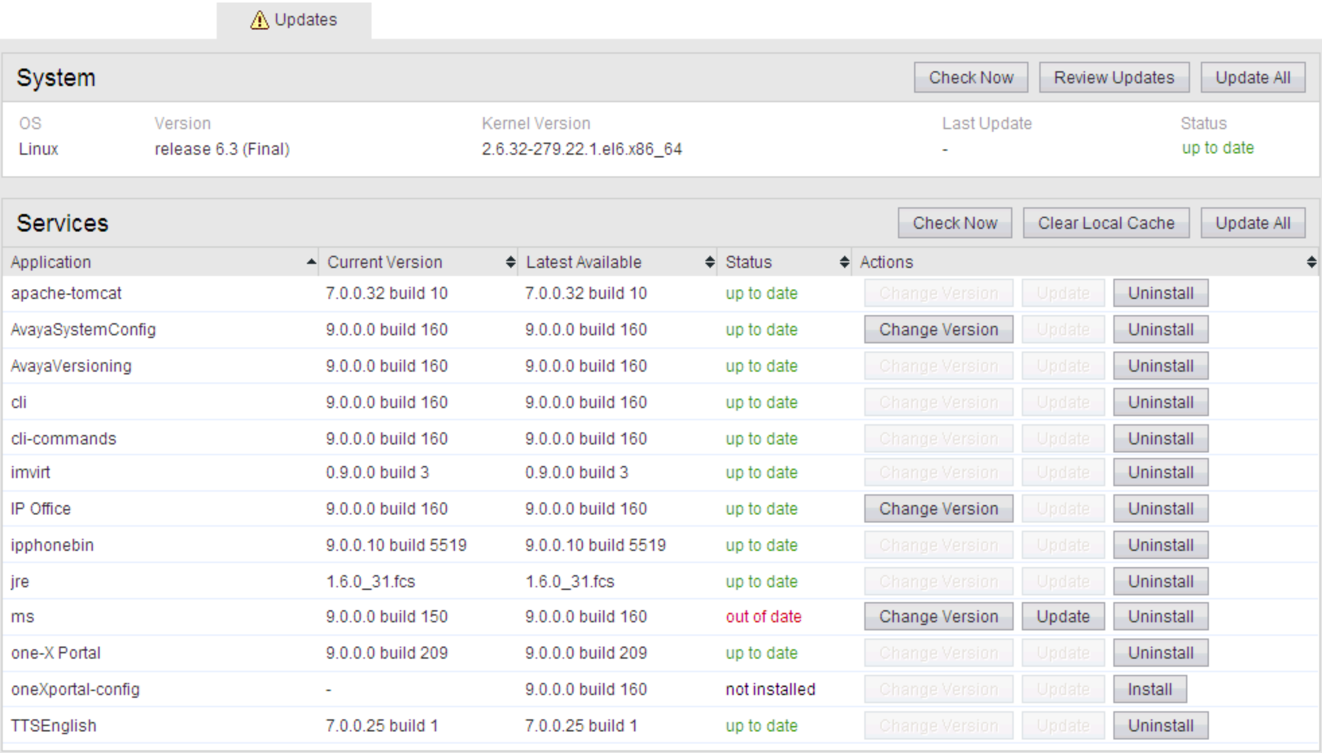
2. To delete the selected files, click on **Delete Selected**.

7.3 Updates

This menu is accessed by selecting **Updates**. The menu displays the different versions of server operating system files and application files available in the file repositories. The file repository locations are configured through the Settings | General 86 page.

- **! Upgrade Warning**
  Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps.

- **! Backup Application Data**
  In all cases, always backup all application data to a separate location before upgrading.



System

OS	Version	Kernel Version	Last Update	Status
Linux	release 6.3 (Final)	2.6.32-279.22.1.el6.x86_64	-	up to date

Services

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

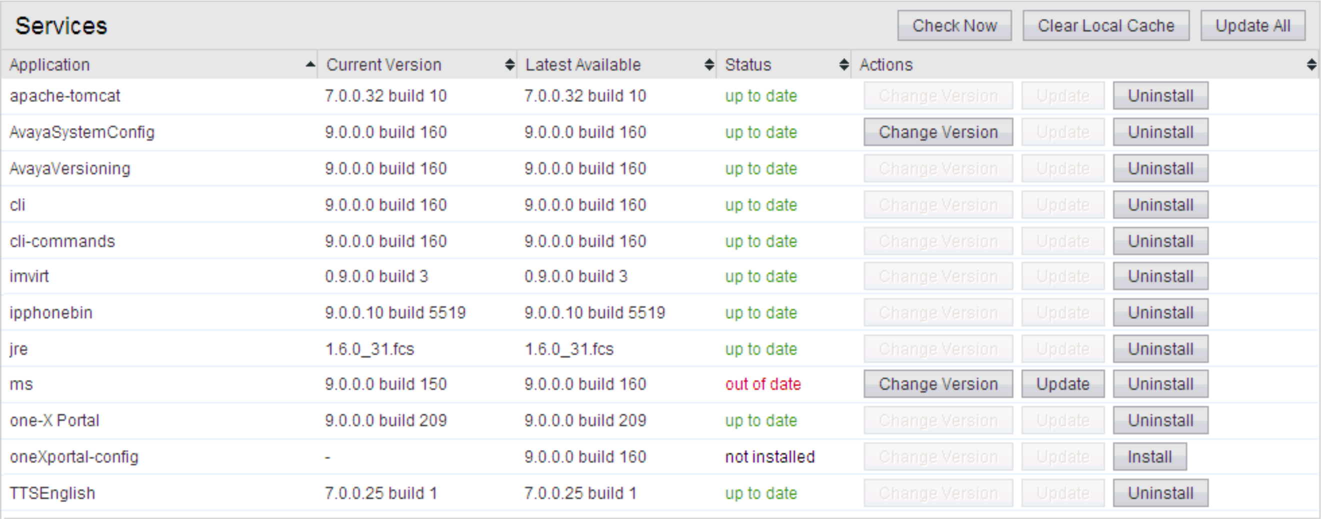
The menu is divided into 2 sections:

- **Services** 83
  This section displays the current version of application files and whether update files are available.

- **System** 84
  This section displays the current version of the operating system and whether update files are available.

7.3.1 Services

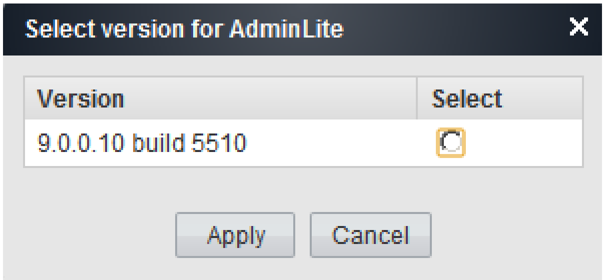
This menu is accessed by selecting **Updates**. The **Services** section shows details of the current version of each application installed and the latest version available.



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

  - The **Change Version**, **Update** and **Update All** buttons in the panel are not useable unless appropriate update files are available in the applications software repository 69. This also affects the availability of the **Install** button option.

- **Change Version**
  Clicking on this button shows the update files available for the related application in the server's file repository 69. The current version is selected. Selecting another version and clicking **Apply** will upgrade or downgrade to the selected version.



Version	Select
9.0.0.10 build 5510	○

- **Update**
  Clicking on this button will start an update of the related application to the latest available version in the application file repository 69.

- **Uninstall**
  Clicking on this button will uninstall the selected application.

  - If there are installation files for the application available in the application file repository 69, the button will change to become an **Install** button.

  - If there are no installation files for the application available in the file repository, the application is no longer listed.

- **Install**
  This button is displayed if an application is uninstalled and update files for the application are available in the file repository.

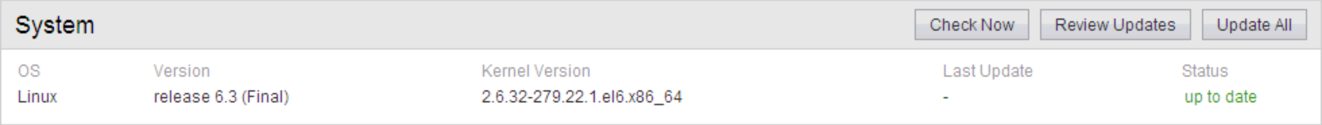
- **Check Now**
  Clicking this button makes the IP Office Application Server recheck the version of update files available in the file repository. Normally it does this automatically when the **Updates** page is loaded.

- **Clear Local Cache**
  This button can be used to remove older update installation files and other material that may accumulate on the server over time.

- **Update All**
  If this button is clicked, those applications that support upgrading without being uninstalled (see above) are updated to the latest versions available in the application file repository.

7.3.2 System

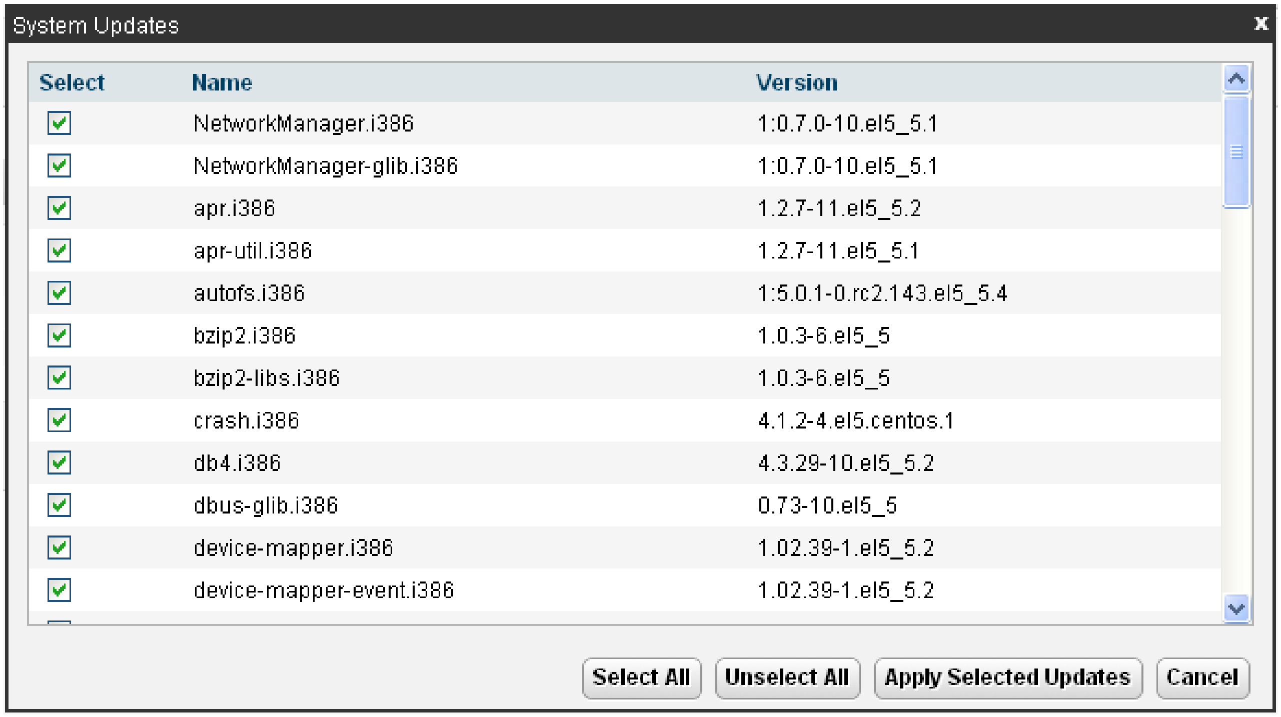
This menu is accessed by selecting **Updates**. The **System** section shows details of the operating system and whether there are updates available.



OS	Version	Kernel Version	Last Update	Status
Linux	release 6.3 (Final)	2.6.32-279.22.1.el6.x86_64	-	up to date

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

- **Review updates**
  Clicking this button will display a list of the available update files. This list allows selection of which updates you want to install.



Select	Name	Version
☑	NetworkManager.i386	1:0.7.0-10.el5_5.1
☑	NetworkManager-glib.i386	1:0.7.0-10.el5_5.1
☑	apr.i386	1.2.7-11.el5_5.2
☑	apr-util.i386	1.2.7-11.el5_5.1
☑	autofs.i386	1:5.0.1-0.rc2.143.el5_5.4
☑	bzip2.i386	1.0.3-6.el5_5
☑	bzip2-libs.i386	1.0.3-6.el5_5
☑	crash.i386	4.1.2-4.el5.centos.1
☑	db4.i386	4.3.29-10.el5_5.2
☑	dbus-glib.i386	0.73-10.el5_5
☑	device-mapper.i386	1.02.39-1.el5_5.2
☑	device-mapper-event.i386	1.02.39-1.el5_5.2

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

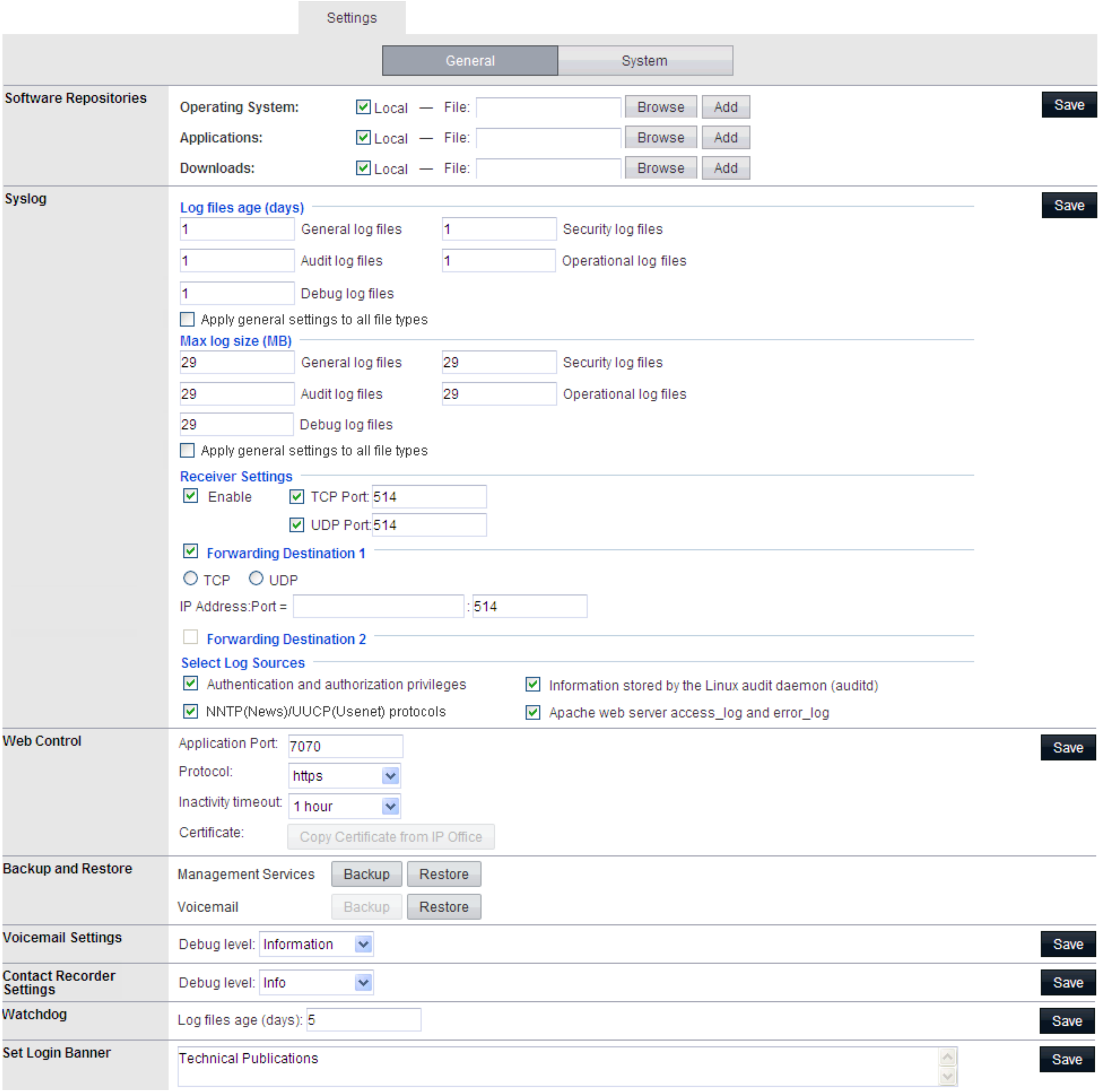
7.4 Settings

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

- **General** 86
  General server settings such as the locations of software update repositories.
- **System** 91
  View and manage the server setting for date, time and IP address details.

7.4.1 General

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



Software Repositories

Operating System: ☑ Local — File:

Applications: ☑ Local — File:

Downloads: ☑ Local — File:

Syslog

Log files age (days)

1 General log files | 1 Security log files

1 Audit log files | 1 Operational log files

1 Debug log files

□ Apply general settings to all file types

Max log size (MB)

29 General log files | 29 Security log files

29 Audit log files | 29 Operational log files

29 Debug log files

□ Apply general settings to all file types

Receiver Settings

☑ Enable ☑ TCP Port: 514

☑ UDP Port: 514

☑ Forwarding Destination 1

○ TCP ○ UDP

IP Address:Port = : 514

□ Forwarding Destination 2

Select Log Sources

☑ Authentication and authorization privileges

☑ Information stored by the Linux audit daemon (auditd)

☑ NNTP(News)/UUCP(Usenet) protocols

☑ Apache web server access_log and error_log

Web Control

Application Port: 7070

Protocol: https

Inactivity timeout: 1 hour

Certificate: Copy Certificate from IP Office

Backup and Restore

Management Services Backup Restore

Voicemail Backup Restore

Voicemail Settings

Debug level: Information

Contact Recorder Settings

Debug level: Info

Watchdog

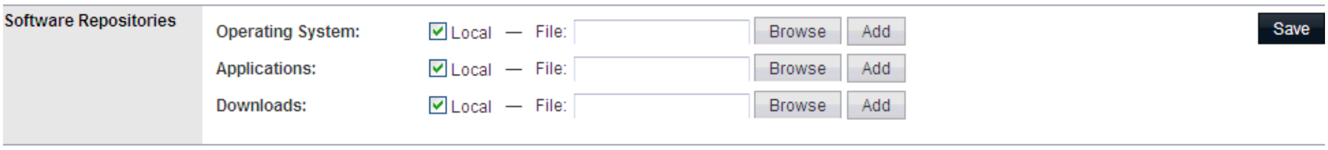
Log files age (days): 5

Set Login Banner

Technical Publications

Software Repositories

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



Software Repositories

Operating System: ☑ Local — File:

Applications: ☑ Local — File:

Downloads: ☑ Local — File:

The files uploaded or present in the file repositories are used by the **Updates** 82 and **AppCenter** 96 menus.

- **Repository**
  If the **Local** option is not selected, this field is used to set the URL of a remote HTTP file repository 71. Note that each repository must be different, the same URL must not be used for multiple repositories.

- **Local**
  This checkbox is used to set whether the file repository used is local (files stored on the IP Office Application Server or remote (a folder on a HTTP web server specified in the Repository field).

- **File / Browse / Add**
  If the Local option is selected, this field and adjacent buttons can be used to browse to a specific update file. When the file is located and selected, click **Add** to upload the file to the file store on the IP Office Application Server.

Web Control

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

- **Application Port**
  Change the port used for logging in. The default is ***7071***. If you change this value you must ensure that you do not select a value already used by another service or application.

- **Protocol**
  Select the protocol used for connection. The default is ***https***. The options are ***http*** or ***https***.

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

- **Certificate**
  This section indicates the status of the certificate provided by the IP Office application. Normally this is generated during initial installation of the server.

Backup and Restore

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

- **Management Services**
  These control provide options to backup/restore the configuration settings of the Management Services application running on the server.

- **Voicemail Pro Server**
  For the Voicemail Pro server, these controls can only be used to restore an existing backup. Using the Voicemail Pro client, the voicemail server can be configured to perform regular (daily, weekly and or monthly) automatic backups of selected options including messages and prompts. The Voicemail Pro client can also be used to perform an immediate backup. When the Restore button is selected, the backups available in the backup folder (*/opt/vmpro/Backup/Scheduled*) are listed. The backup name includes the date and time and whether the backup was a manual or scheduled backup. When the required backup is selected, clicking OK will start the restoration process. For details refer to the Voicemail Pro client help.

- **one-X Portal for IP Office**
  one-X Portal for IP Office has its own method of backup and restore that can be access through the one-X Portal for IP Offices web client administration.

Voicemail Settings

This section can be used to set the debug logging level used by the Voicemail Pro application if running. For the one-X Portal for IP Office application, the logging level is set through the applications own web administration menus. Log files are retrievable through the **Logs | Download** 81 menu.

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

Contact Recorder Settings

This section can be used to set the debug logging level used by the ContactStore for IP Office application if installed on the server.

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

Syslog

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

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

  - **Apply general settings to all file types**
    If selected, the setting for General log files is applied to all file types.

- **Max log size (MB)**
  Set the maximum total size of each type of records retained on the server before the oldest records of that type are automatically deleted. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**.

  - **Apply general settings to all file types**
    If selected, the setting for General log files is applied to all file types.

- **Receiver Settings**
  These settings control if and how the server can receive Syslog records.

  - **Enable**
    If selected, the server is able to receive Syslog records using the port configured below.

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

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

- **Forward Destination 1**
  These settings control whether the server forwards copies of Syslog records it receives to another server.

  - **Enable**
    If selected, the server will forward copies of the Syslog records it receives.

  - **IP Address**
    Sets the address of the destination server.

  - **Port**
    Set the destination port for the forwarded records.

  - **Protocol**
    Set the protocol, ***UDP*** or ***TCP***, for the forwarding.

- **Forward Destination 2**
  These settings control wether the server forwards copies of the Syslog records it receives to a second server. The settings are the same as for the first forwarding destination.

- **Select Log Sources**
  These options allow selection of which server reporting to include in the Syslog reports. The available options are:

  - **Authentication and authorization privileges**

  - **Information stored by the Linux audit daemon (auditd)**

  - **NNTP(News)/UUCP(Usenet) protocols**

  - **Apache web server access_log and error_log**

Watchdog

- **Log files age (days)**
  Sets the number of days that log file records are retained. This does not affect log file archives 81. Not applied to one-X Portal for IP Office which performs its own log file size limitation.

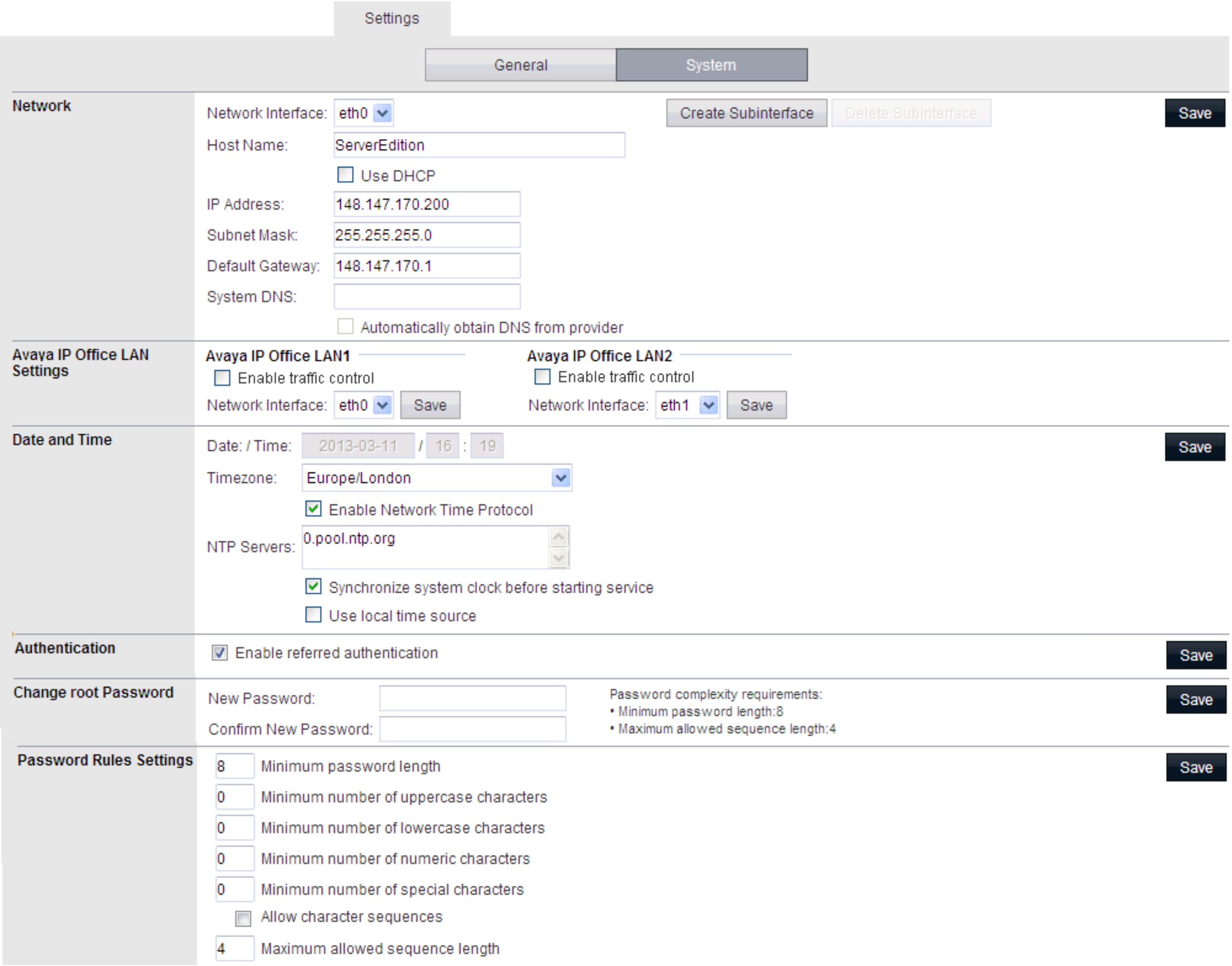
Set Login Banner

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

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

7.4.2 System

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



Network

Network Interface: eth0
Create Subinterface | Delete Subinterface | Save
Host Name: ServerEdition
☐ Use DHCP
IP Address: 148.147.170.200
Subnet Mask: 255.255.255.0
Default Gateway: 148.147.170.1
System DNS:
☐ Automatically obtain DNS from provider

Avaya IP Office LAN Settings

Avaya IP Office LAN1
☐ Enable traffic control
Network Interface: eth0 | Save

Avaya IP Office LAN2
☐ Enable traffic control
Network Interface: eth1 | Save

Date and Time

Date: / Time: 2013-03-11 / 16 : 19 | Save
Timezone: Europe/London
☑ Enable Network Time Protocol
NTP Servers: 0.pool.ntp.org
☑ Synchronize system clock before starting service
☐ Use local time source

Authentication

☑ Enable referred authentication | Save

Change root Password

New Password:
Confirm New Password:
Password complexity requirements:
- Minimum password length:8
- Maximum allowed sequence length:4

Save

Password Rules Settings

Save
8 Minimum password length
0 Minimum number of uppercase characters
0 Minimum number of lowercase characters
0 Minimum number of numeric characters
0 Minimum number of special characters
☐ Allow character sequences
4 Maximum allowed sequence length

Network

- **Network Interface**
  This drop down allows selection of network interfaces is currently being configured by the web form. Within the IP Office configuration, ***Eth0*** matches LAN1, ***Eth1*** matches LAN2. On the pre-built IP Office Application Server only ***Eth0*** is used. This port is labeled as port 1 on the physical server.

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

  - **! WARNING**
    For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

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

- **IP Address**
  Displays the IP address set for the server. If DHCP is not being used, the field can be edited to change the setting.

  - **! WARNING**
    For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

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

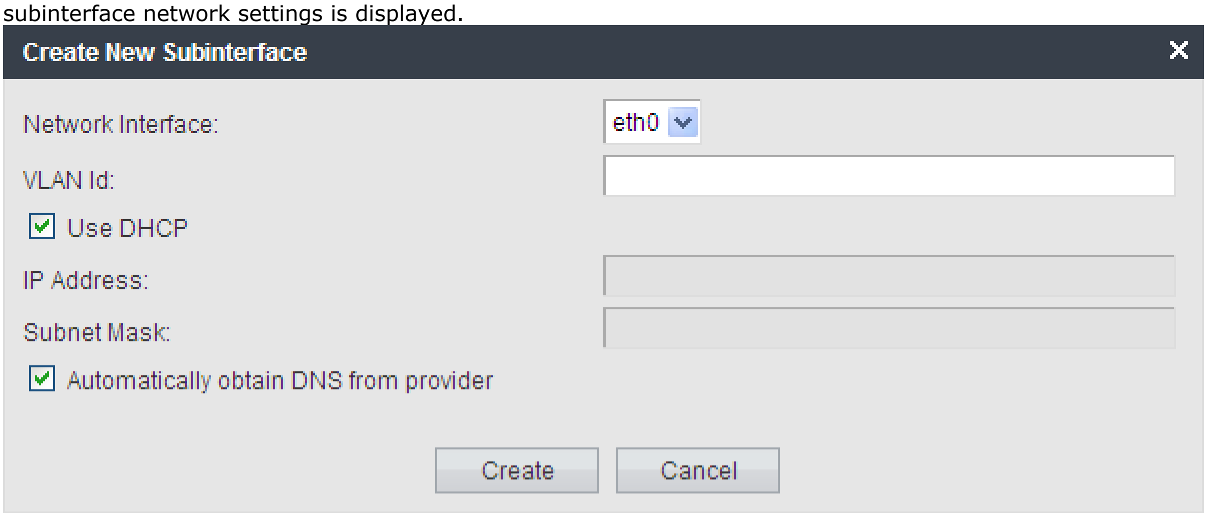
- **Default Gateway**
  Displays the default gateway settings for routing. If DHCP is not being used, the field can be edited to change the setting.

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

- **Automatically obtain DNS from provider**
  This setting is only used if **Use DHCP** is also selected. If selected, the server attempts to obtain DNS server details from the DHCP server.

-

- **Create Subinterface**
  This control can be used to create an additional VLAN subnet on the same port. When clicked, the menu for the subinterface network settings is displayed.



Create New Subinterface

Network Interface: eth0

VLAN Id:

☑ Use DHCP

IP Address:

Subnet Mask:

☑ Automatically obtain DNS from provider

- **Delete Subinterface**
  Delete the subinterface.

Avaya Office LAN Settings

- **Avaya Office LAN1**
  These settings are used for the LAN1 interface of the Management Services application run by the server. LAN1 is also referred to as LAN.

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

  - **Network Interface**
    Use the drop-down to select which port on the server should be used for LAN1.

- **Avaya Office LAN2**
  These settings are used for the LAN2 interface of the Management Services application run by the server. LAN2 is also referred to as WAN.

Date Time

These settings are used to set or obtain a UTC date and time value for use by the IP Office Application Server and services.

- **Date**
  Shows the current date being used by the server. If **Enable Network Time Protocol** is selected, this is the date obtained from the NTP server and cannot be manually changed.

- **Time**
  Shows the current UTC time being used by the server. If **Enable Network Time Protocol** is selected, this is the time obtained from the NTP server and cannot be manually changed. The current time being used by the server is shown on the **System** 75 menu.

- **Timezone**
  In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The **Timezone** field is used to determine the appropriate offset that should be applied to the UTC time above. Note that changing the timezone can cause a Session expired message to appear in the browser.

  - **! WARNING**
    For a virtualized server, shown by the **Virtualized** value on the System 75 menu, this field is part of the **System Identification** (**SID**) used for licensing. Changing this value also changes the **System Identification** and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new **System Identification**.

- **Enable Network Time Protocol**
  If this option is selected, the IP Office Application Server will attempt to obtain the current UTC time from the NTP servers listed in the **NTP Servers** list below. It will then use that time and make regular NTP requests to update the date and time. The following options are only used if **Enable Network Time Protocol** is selected.

  - **NTP Servers**
    This field is used to enter the IP address of an NTP server or servers which should be used when **Enable Network Time Protocol** is selected. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome, however it is your responsibility to make sure you are aware of the usage policy for any servers you choose. Choosing several unrelated NTP servers is recommended in case one of the servers you are using becomes unreachable or its clock is unreliable. The operating system uses the responses it receives from the servers to determine which are reliable.

    - The IP Office system can also use NTP to obtain its system time. Using the same servers for the IP Office Application Server and IP Office system is recommended.

  - **Synchronize system clock before starting service**
    When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, an immediate update of the server's clock to match the NTP obtained time is forced.

  - **Use local time source**
    When using NTP, the time obtained by the operating system is used to gradually change the server's hardware clock time. If this option is selected, the server's hardware clock time is used as the current time rather than the NTP time.

Authentication

- **Enable referred authentication**
  This setting controls whether access to the web control menus is authenticated through the web control menus' own settings or using those of IP Office Web Manager. See Password Authentication 14.

  - **Enabled**
    When **Enable referred authentication** is enabled, access to the web control menus is control by the IP Office Web Manager security settings. This allows you to access the web control menus from within IP Office Web Manager without needing to re-authenticate. You can still direct access the web control menus but only using the IP Office Web Manager names and passwords.

  - **Disabled**
    When **Enable referred authentication** is not enabled, access to the web control menus is controlled by web control's own settings. Web control cannot be accessed through IP Office Web Manager except by launching it in a separate browser window and entering the separate web control name and password.

Change Root Password

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

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

Password Rules Settings

- **Minimum password length**
  This field set the minimum length of new passwords. Note that the combined requirements of the fields below for particular character types may create a requirement that exceed this value. Note also that the maximum password length is 31 characters.

- **Minimum number of uppercase characters**
  This field sets the number of uppercase alphabetic characters that new passwords must contain.

- **Minimum number of lowercase characters**
  This field sets the number of lowercase alphabetic characters that new passwords must contain.

- **Minimum number of numeric characters**
  This field sets the number of numeric characters that new passwords must contain.

- **Minimum number of special characters**
  This field sets the number of non-alphanumeric characters that new passwords must contain.

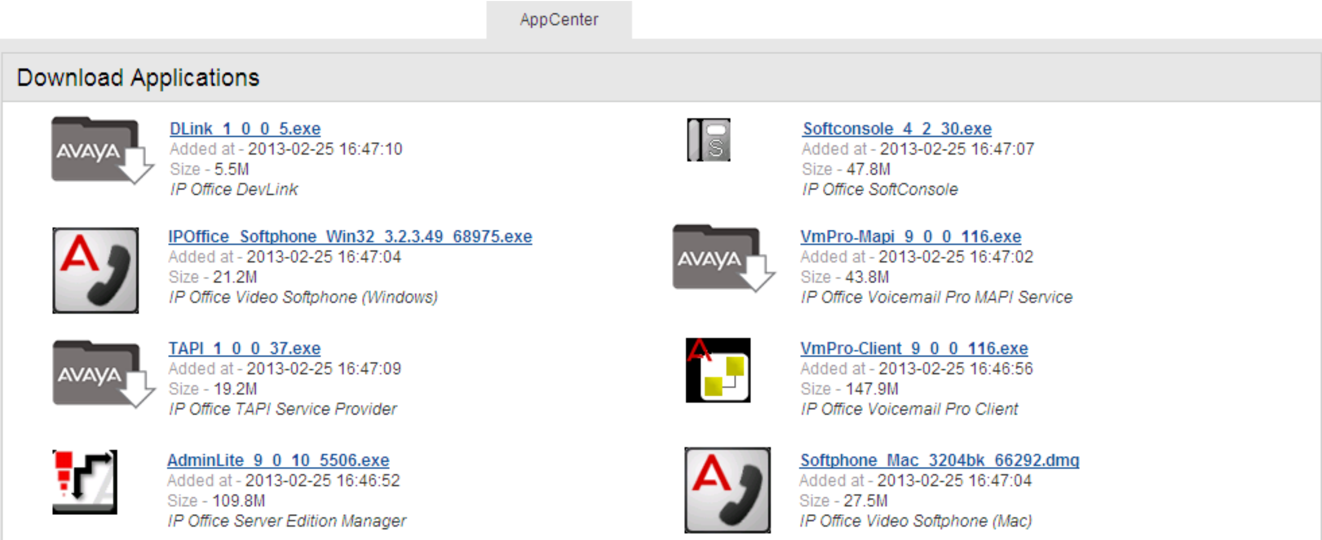
- **Allow character sequences**
  If this option is selected, character sequences such as ***1234*** or ***1111*** or ***abcd***, are allowed in new passwords without any restriction. When not selected, the maximum length of any sequence is set by the field below.

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

7.5 App Center

This menu is accessed by selecting **AppCenter**. The menu is used to download files for use on the local PC. For example, the Voicemail Pro client used to administer the Voicemail Pro server application.

The file repository location is configured through the Settings | General 86 page.



AppCenter

Download Applications

DLink_1_0_0_5.exe
Added at - 2013-02-25 16:47:10
Size - 5.5M
IP Office DevLink

Softconsole_4_2_30.exe
Added at - 2013-02-25 16:47:07
Size - 47.8M
IP Office SoftConsole

IPOffice_Softphone_Win32_3.2.3.49_68975.exe
Added at - 2013-02-25 16:47:04
Size - 21.2M
IP Office Video Softphone (Windows)

VmPro-Mapi_9_0_0_116.exe
Added at - 2013-02-25 16:47:02
Size - 43.8M
IP Office Voicemail Pro MAPI Service

TAPI_1_0_0_37.exe
Added at - 2013-02-25 16:47:09
Size - 19.2M
IP Office TAPI Service Provider

VmPro-Client_9_0_0_116.exe
Added at - 2013-02-25 16:46:56
Size - 147.9M
IP Office Voicemail Pro Client

AdminLite_9_0_10_5506.exe
Added at - 2013-02-25 16:46:52
Size - 109.8M
IP Office Server Edition Manager

Softphone_Mac_3204bk_66292.dmg
Added at - 2013-02-25 16:47:04
Size - 27.5M
IP Office Video Softphone (Mac)

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

- ***VmPro...ClientOnly.exe***
  This is the installation package for the Voicemail Pro client application used to administer the Voicemail Pro server application.

- ***VmPro...Mapi.exe***
  This is the installation package for the MAPI proxy. This can be installed on a Windows PC in the same network as the Windows Exchange server. It allows the Linux based Voicemail Pro server to access UMS services. Refer to the Voicemail Pro installation manual.

- ***IPOAdminLite...***
  This is the installation package for the IP Office Manager application. Note that this is an installer for IP Office Manager, System Monitor and System Status Application tools only. It is not the full IP Office Administration and User package used with other IP Office systems.

- ***DLink...***
  This is the installation package for the IP Office DevLink 3rd-party TAPI interface.

- ***Flare...***
  This is the installation package for the IP Office Flare application.

- ***TAPI...***
  This is the installation package for the IP Office 1st -party TAPI interface.

- ***Softconsole...***
  This is the installation package for the IP Office SoftConsole application. This is an application used by receptionist and operator type users to answer and distribute incoming calls.

- ***...Softphone...***
  This is a SIP softphone application for use by individual users. Separate installation packages are provided for Windows and Mac PCs.

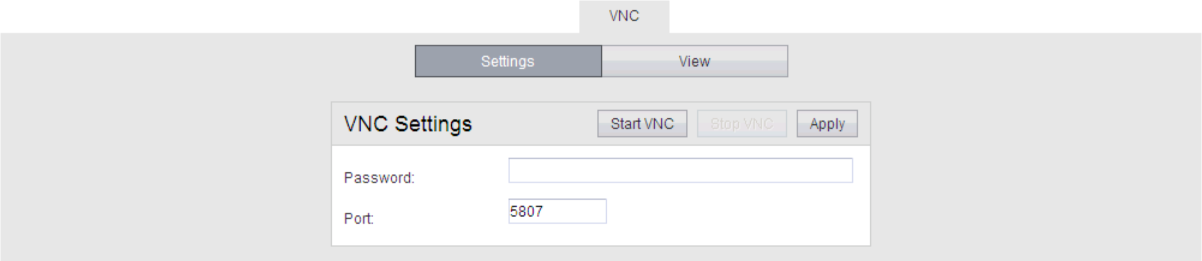
7.6 VNC

This menu allows you to configure VNC access to the server's graphical desktop. You can then use the VNC access either through these menus or using a separate third-party such as TigerVNC. See Using VNC 72.

- VNC access using the root user account is not supported. Some applications, for example Wireshark, require root user permissions and so cannot be used when accessing the server via VNC.

Settings

This menu is used to start and stop the VNC service supported on the server. The Port settings must be matched by the VNC client used to access the desktop.



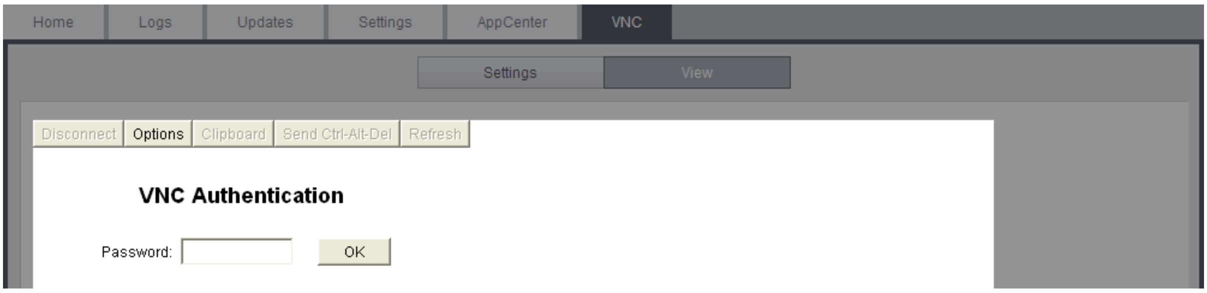
VNC Settings

Password:

Port: 5807

View

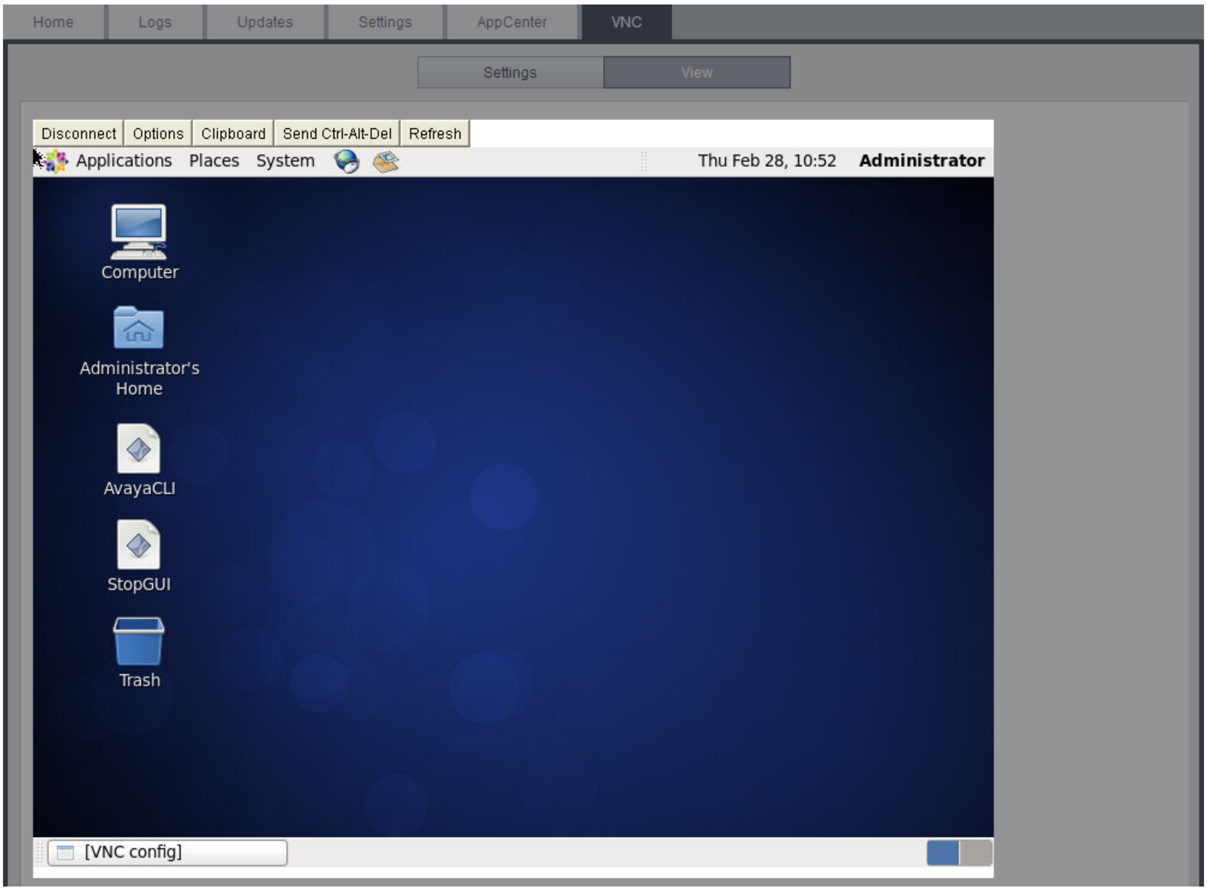
This menu is used to connect to and display the desktop using VNC.



VNC Authentication

Password:

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



Chapter 8. Additional Processes

8. Additional Processes

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

- **SSH File Transfers** 101
- **Windows to Linux Voicemail Transfer** 102

8.1 SSH File Transfers

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

To start SSH file transfers:

1. Start your SFTP or SSH file application and connect to the IP Office Application Server PC. The exact method will depend on the application being used.

   a. Enter the details for the IP Office Application Server:

      - The **Host Name** is the IP address of the IP Office Application Server.
      - The **User Name** is ***web***.
      - The **Protocol** is ***SFTP/SSH***.
      - The **Port** is ***22***. If this is the first time the application has connected to the server, accept the trusted key.

   b. If this is the first time the application has connected to the IP Office Application Server, accept the trusted key.

   c. When prompted, enter the webcontrol user password 57, the default is ***webcontrol***.

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

8.2 Windows to Linux Voicemail Transfer

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

1. On the Windows voicemail server:
    a. Using the Voicemail Pro client, perform an immediate backup on the Windows voicemail server, selecting to backup all types of file.
    b. This will create a backup folder, the name of which includes the date and time of the backup and Immediate. For example ***VMPro_Backup_26012011124108_Immediate***. The default path for such folders is ***C:\Program Files\Avaya\IP Office\Voicemail Pro\Backup\Scheduled***.
    c. Within Windows, locate the folder just created by the backup and copy the folder to the PC with your SSH file transfer tool.
2. Connect to the server using a SSH File transfer tool 101.
3. Copy the Windows backup folder into the folder ***/opt/vmpro/Backup/Scheduled/OtherBackups***.
4. Using a web browser, login 56 to the IP Office Application Server.
5. Select **Settings**.
6. On the **General** tab, select the **Restore** button for the **Voicemail** service. From the list of available backups, select the one just copied onto the server.
7. Click **OK**.

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

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

Chapter 9. Document History

9. Document History

Date	Issue	Changes
10th December 2013	**07g**	• Corrected name of applications download menu to **AppCenter**. • • Note about voicemail server use of 169.254.0.2 address removed. Not applicable to application server.
12th December 2013	**07h**	• Minor spelling corrections.
13th December 2013	**07i**	• Minor spelling corrections.
8th January 2014	**07j**	• Minor spelling corrections.
16th January 2014	**07k**	• Minor spelling corrections.
24th January 2014	**07l**	• Minor corrections.

Index

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