IP Office™ Platform 9.1

Installing Avaya IP Office™ Platform Contact Recorder for IP Office

15-601011 Issue 10ah - (22 November 2016)

© 2013 - 2014 Avaya Inc.
All Rights Reserved.

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.
Documentation disclaimer
“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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://www.avaya.com/support or such successor site as designated by Avaya. 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.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN 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 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. Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.
License types
Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
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,” or such successor site as designated by Avaya. 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization
Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service 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”). As required, 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 or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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, or such successor site as designated by Avaya. 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, Hosted Service(s), 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, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya 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, or such successor site as designated by Avaya.

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

Contents

1. Contact Recorder for IP Office

1.1 Operation Overview 10
1.2 Server Requirements 11
1.3 Additional Documentation 12
1.4 Browser Access 13
1.5 Codecs 13
1.6 Pre-Requisisites 13

2. Contact Recorder for IP Office Installation

2.1 Downloading the Software 17
2.2 Checking the Boot Order 18
2.3 Preparing the Bootable Software Installer 18
2.3.1 Preparing a DVD 18
2.3.2 Preparing a USB Installation Key 19
2.4 Adding an Additional Hard Disk 20
2.4.1 HP DL360G7 21
2.4.2 HPDL120G7 22
2.4.3 Dell R210 22
2.4.4 Dell R620 23
2.5 Server Software Installation 24
2.6 Server Ignition 26
2.7 Adding a Certificate to the Browser 30
2.8 Logging Into Web Manager 32
2.9 Logging In Directly 33
2.10 IP Office Initial Configuration 34
2.11 IP Office Licensing 35
2.12 Checking the Voicemail Licenses 36
2.13 Adding the Application Server 36
2.14 Enabling the Contact Recorder for IP Office Service 37
2.15 Logging In to Contact Recorder for IP Office 38
2.16 Setting the File Paths 38
2.17 Configuring the Transfer from Voicemail Pro 39
2.18 Adding Users 40
2.19 Test Operation 41

3. Recording Configuration

3.1 Configuring the Advice of Call Recording Warning 44
3.2 Configuring the Recording Display 45
3.3 Changing the Recording Length 45
3.4 Configuring Manual Call Recording 46
3.4.1 Configurng the Manual Recording Destination 46
3.4.2 Triggering Manual Call Recording 47
3.5 Configuring Automatic Call Recording 49
3.5.1 User Automatic Recording 50
3.5.2 Hunt Group Automatic Recording 51
3.5.3 Incoming Call Route Automatic Recording 52
3.5.4 Account Code Automatic Call Recording 53
3.6 Pausing Recording 54
3.6.1 Configuring a Pause Recording Button 54
3.6.2 Setting the Auto Restart Delay 54
3.7 Customisable Callflow Options 54

4. Additional Processes

4.1 Enabling DVD Archiving 56
4.1.1 Identifying the Drive Path and UDI 56
4.1.2 Disabling the Media Detection Service 57
4.1.3 Entering the Drive in Contact Recorder for IP Office 58
4.2 Disabling HTTP Access 59

5. Document History

Index 65

Chapter 1.

Contact Recorder for IP Office

1. Contact Recorder for IP Office

The Voicemail Pro application can manually or automatically record calls. It places those recordings into a user or group's mailbox alongside normal voicemail messages.

Users can start manual call recording in a number of ways; programmable button, short code, one-X Portal for IP Office. Automatic call recording is configured on the IP Office system and applied to specific users, hunt groups, incoming call routes or account codes.

Contact Recorder for IP Office enhances call recording by transferring recordings to an separate archive from the normal mailboxes. Those recordings are then outside the control of voicemail housekeeping and do not impact on the space needed for voicemail messages.

Contact Recorder for IP Office maintains a database of the call details associated with each recordings it stores. Using a web browser, users can search the database and from the search results playback recordings.

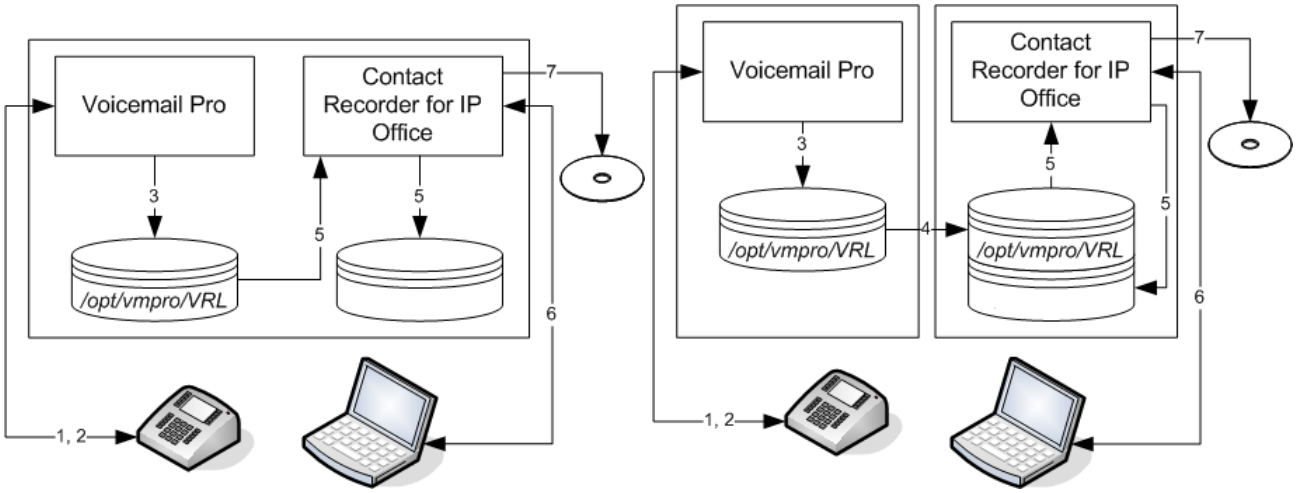
- The Contact Recorder for IP Office is supported in the following configurations:
  - For IP500 V2 systems, Contact Recorder for IP Office is supported on an IP Office Application Server. That includes IP500 V2 systems running a Unified Communications Module. Contact Recorder for IP Office is supported on the same server as Voicemail Pro if an additional hard drive is installed for Contact Recorder for IP Office use.
  - For Server Edition systems, Contact Recorder for IP Office is supported on the Server Edition Primary Server if an additional hard drive is installed for Contact Recorder for IP Office use. Otherwise it is supported on a separate IP Office Application Server.
    - It also includes running Contact Recorder for IP Office on a virtual machine. Details of adding an additional virtual hard disk are covered in the manual *"Deploying Server Edition Servers as Virtual Machines"*.

PCI Compliance

It is important to note that since Avaya is not a payment processor and since Contact Recorder for IP Office is not a payment processing application; neither Avaya nor Avaya Contact Recorder for IP Office can be certified as PCI compliant or PA-DSS compliant.

1.1 Operation Overview

Contact Recorder for IP Office must use a separate disk partition for file storage from that used by the Voicemail Pro. The diagram below interaction between the Voicemail Pro and Contact Recorder for IP Office applications.



Single Server Installation *Separate Server Installation*

1. The IP Office configuration indicates which calls to record and whether the recording should be sent to Contact Recorder for IP Office rather than put into a voicemail mailbox.
   - You can configure recording for individual users, hunt groups, incoming call routes or account codes.
   - The IP Office can optionally instruct the voicemail server to record authenticated files. These files are larger than standard recordings. However, authentication allows detection of whether anyone has subsequently modified the file.
2. When a matching call occurs, the Voicemail Pro performs the recording.
3. When recording is complete, the recording is placed in a temporary folder on the voicemail server.
4. If the two applications are on separate severs, the voicemail server is configured to transfer files in its temporary folder to the matching temporary folder on the Contact Recorder for IP Office server.
5. The Contact Recorder for IP Office collects any files that appear in the temporary folder on its server. It adds the recording to its own storage folder and adds call details from the file to its database.
6. Users can browse to the Contact Recorder for IP Office server and search the database to replay archived recordings.
   - Users can search for calls using fields such as date, length, parties involved, etc.
   - Each user can only see calls that include particular extension ranges.
   - Optionally, users can download and email copies of recordings from the search results.
7. By default Contact Recorder for IP Office stores recordings indefinitely and keeps call details in its database for 5 years. However, if space on the storage partition becomes limited, it starts deleting recordings on a first in first out basis. To avoid this, you can configure long term storage onto DVD disk, Blu-Ray disk or network attached storage.
   - Avaya supplied servers all include a DVD+/-RW drives suitable for archiving use.
   - The option to archive recordings on DVD or Blu-Ray disk is not supported when running Contact Recorder for IP Office on a virtual machine.

1.2 Server Requirements

The basic server specification depends on the type of server installed and the overall requirement determined for all IP Office applications supported by the server.

- If installed on an IP Office Application server, refer to the IP Office Application Server Installation and Maintenance Manual for server specifications.
- If installed on a Server Edition Primary Server, refer to the manual *"Deploying IP Office Server Edition"*.
- If deployed on a virtual machine, refer to the manual *"Deploying Server Edition Servers as Virtual Machine"*.

The additional server requirements for support of Contact Recorder for IP Office, in addition to those specified in the above manuals, are:

- **Additional Hard Disk**
  If Contact Recorder for IP Office is installed on the same server as Voicemail Pro, then Contact Recorder for IP Office must use a separate hard disk. Therefore, you need to install an additional hard disk.
  - This manual includes notes for the installation of additional hard drives in the following Avaya supplied servers. The *"Deploying Server Edition Servers as Virtual Machine"* manual specifies how to add an additional virtual hard disk during the deployment of a virtual server.
    - **HP ProLiant DL360G7 Server** 21
      Avaya supplies and supports additional 300GB hard disks (DL360G7 SRVR 300GB 10K SAS 2.5" HDD). You can fit either a single disk or, for RAID1 support, two additional disks.
    - **HP ProLiant DL120G7 Server** 22
      Avaya supplies and supports an additional 250GB hard disk (Order code 700506869).
    - **Dell PowerEdge R210 Server** 22
      Avaya supplies and supports an additional 500GB hard disk (R210 II XL 500GB 7200 HDD).
    - **Dell PowerEdge R620 Server** 23
      Avaya supplies and supports additional 600GB hard disks (Order code 700506757). You can fit either a single disk or, for RAID1 support, two additional disks.
- **Recordable Disk Drive**
  Long term archiving uses a DVD+RW or Blu-Ray -R disk drive. Alternatively, Contact Recorder for IP Office can archive to a network attached storage (NAS) drive. All the Avaya supplied servers include a DVD+/-RW disk drive.

1.3 Additional Documentation

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

Related Documents

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

Technical Bulletins

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

Other Documentation and Documentation Sources

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

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

1.4 Browser Access

The default paths for browser access to Contact Recorder for IP Office are ***http://<server_address>:9888*** and ***https://<server_address>:9444***. Users created in the Contact Recorder for IP Office configuration have roles that define the actions they can perform after logging in.

Contact Recorder for IP Office supports Microsoft Internet Explorer 8, 9 or 10. The playback function requires the browser to allow the download and installation of a number of ActiveX controls.

Contact Recorder for IP Office users with the appropriate permission can also download copies of call recordings from the browser.

1.5 Codecs

The IP Office configuration sets the destination for call recordings. The destination selected affects the codec used for the initial recording and the codec applied to the final recording file. The IP Office options are:

- **Mailbox**
  This is the default option. When selected, you can use the adjacent drop down list to select the destination user or hunt group mailbox. These files are typically 0.5MB to 1MB per minute.
- **Voice Recording Library**
  Use this option to have the recordings transferred to the VRL folder after recording (from which it can be collected by applications such as Contact Recorder for IP Office). This option produces a G.711 format file that Contact Recorder for IP Office converts to G.729A format after the file transfer. These files are typically 60KB per minute.
- **Voice Recording Library Authenticated**
  As above but this option produces a G.726 format file that contains file authentication information. Any subsequent editing of the file invalidates that information. Contact Recorder for IP Office does not convert the file to G.729A format after the file transfer. These files are typically 120KB per minute. This option is currently not supported with Linux based servers.

1.6 Pre-Requisisites

You must meet the following conditions before attempting to install Contact Recorder for IP Office.

1. Do not configure Contact Recorder for IP Office until after normal voicemail mailbox operation of the Voicemail Pro application has been tested and validated. The Voicemail Pro performs the call recording for Contact Recorder for IP Office and so is an essential pre-requisite.
2. The license requirements depend on the operating mode of the IP Office systems:
   - For Server Edition, the primary server needs a **VMPro Recordings Administrators** license. For IP Office Release 9.0, this is the only server in the Server Edition network that requires a license.
   - For non-Server Edition systems, each IP Office system requires a **VMPro Recordings Administrators** license.
3. The Contact Recorder for IP Office application must use a separate disk partition for file storage from that used by Voicemail Pro. This requires either the adding of an additional hard disk to the server or use of two separate servers.

Chapter 2.

Contact Recorder for IP Office Installation

2. Contact Recorder for IP Office Installation

This section summarises the processes required for Contact Recorder for IP Office installation.

Process Summary

The installation process divides into 4 main stages.

1. **Server Installation**
   This stage largely follows the standard installation process for a server. For full details, refer to the IP Office Application Server Installation Manual or Deploying IP Office Server Edition manual.

   a. **Downloading the software** 17
   Download the latest application software and related files.

   b. **Check the server boot order** 18
   Check that the server PC can boot from DVD or USB.

   c. **Preparing a bootable software installer** 18
   Create a bootable DVD or USB memory key.

   d. **Adding an additional hard disk** 20
   If installing Contact Recorder for IP Office on the same server as Voicemail Pro, an additional hard disk is required.

   e. **Server software installation** 24
   Install the server software.

   f. **Server ignition** 26
   Configure the server's role.

   g. **Logging in** 33
   Log in to the server's IP Office Web Manager menus.

2. **Enable Contact Recorder for IP Office**
   This stage enables the call archiving functionality of the Voicemail Pro and starts the Contact Recorder for IP Office service.

   a. **IP Office Licensing** 35
   Enter the licenses to support use of Contact Recorder for IP Office.

   b. **Checking the voicemail licensing** 36
   Check that the voicemail server has detected the licenses.

   c. **Adding the application server** 36
   If installing an application serve, add the application server to the IP Office Web Manager view of available servers.

   d. **Installing the Contact Recorder for IP Office service** 37
   Install and start the Contact Recorder for IP Office service.

3. **Configuring Contact Recorder for IP Office**
   This stage configures the handling and access to call recordings.

   a. **Logging in to Contact Recorder for IP Office** 38
   Log in to Contact Recorder for IP Office to perform basic initial configuration.

   b. **Setting the file paths for recordings** 38
   Set and check the files paths from which Contact Recorder for IP Office collects recordings and into which it stores those files.

   c. **Configuring the transfer of recordings** 39
   Configure the voicemail server so that it can transfer recording files for collection.

   d. **Add users** 40
   Add user to Contact Recorder for IP Office for the playback of recordings.

4. **Test operation** 41
   Test operation to verify the basic installation.

2.1 Downloading the 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.

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

To download software:

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

2.2 Checking the Boot Order

You install the software by placing it onto a DVD or USB 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 appears 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 appears. 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 USB 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.

2.3 Preparing the Bootable Software Installer

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

2.3.1 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.

2.3.2 Preparing a USB Installation Key

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

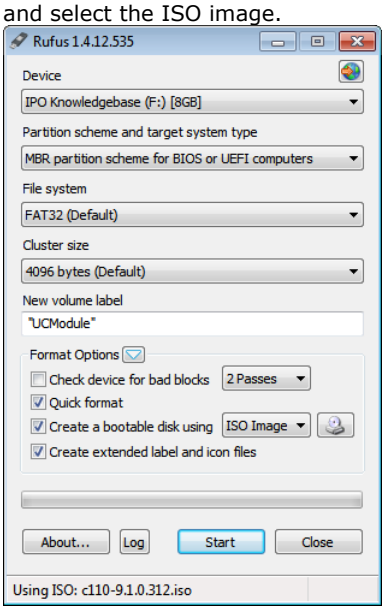
- **! WARNING**
  Using the USB Memory key overwrites any existing software and data on the server.

Prerequisites

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

To create a bootable USB memory key:

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



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

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

2.4 Adding an Additional Hard Disk

If Contact Recorder for IP Office is installed and enabled on the same server as Voicemail Pro, it must be configured to use a separate hard disk from Voicemail Pro. That requires the addition of an additional hard disk to the server (or a pair of hard disks if implementing RAID support).

The process for adding an additional hard disk depends on the type of server. This section only provides outline summaries. In all cases, for full details refer to the original equipment manufacturer's documentation.

Avaya supply the following servers:

- **HP ProLiant DL360G7 Server** 21
  Avaya supplies and supports additional 300GB hard disks (DL360G7 SRVR 300GB 10K SAS 2.5" HDD). You can fit either a single disk or, for RAID1 support, two additional disks.
- **HP ProLiant DL120G7 Server** 22
  Avaya supplies and supports an additional 250GB hard disk (Order code 700506869).
- **Dell PowerEdge R210 Server** 22
  Avaya supplies and supports an additional 500GB hard disk (R210 II XL 500GB 7200 HDD).
- **Dell PowerEdge R620 Server** 23
  Avaya supplies and supports additional 600GB hard disks (Order code 700506757). You can fit either a single disk or, for RAID1 support, two additional disks.

2.4.1 HP DL360G7

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Decide if you will be adding a single HDD or a RAID set as the second drive:
   - A single drive requires 1 hard disk in slot 3.
   - A RAID pair requires 2 hard disks, in slots 3 and 4 respectively, which then act as mirrored images of each other.
2. Go the HP support page for the DL360G7 and download the Server Guide: http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/action.process/public/psi/manualsDisplay/?sp4ts.oid=4091408&javax.portlet.action=true&spf_p.tpst=psiContentDisplay&javax.portlet.begCacheTok=com.vignette.cachetoken&spf_p.prp_psiContentDisplay=wsrp-interactionState%3DdocId%253Demr_na-c02065265%257CdocLocale%253Den_US&javax.portlet.endCacheTok=com.vignette.cachetoken

To install the additional hard disk(s):

1. Power down the server.
2. Remove the blank from slot 3. Also from slot 4 if installing a pair of drives for RAID. Refer to the server guide section *"Removing hard drive blanks"*.
3. Insert the new hard disk into slot 3. Also into slot 4 if installing a pair of drives for RAID. Refer to the server guide section *"Installing a SAS hard drive"*.
4. Power on the server.
5. When the "*Press any Key to view Option ROM Messages*" option appears, press any key.
6. Wait for the message "*Slot 0 HP Smart Array P4101 Controller Initializing*" to appear, then press **F8**.
7. From the **Main Menu** select **Create Logical Drive**. Select the following options:

Setting	Single Drive	RAID Pair
Available physical drive	***Bay 3***	***Bay 3 and Bay 4***
Raid Configurations	***RAID 0***	***Raid 1+0***
Parity Group Count	*Leave blank*	*Leave blank*
Spare	*Leave blank*	*Leave blank*
Maximum Boot partition	*Disable*	*Disable*

8. After the options have been selected, press **Enter** to save the configuration.
9. Press **F8** to confirm.
10. Select **Select View Logical Drive**. Ensure there are 2 drives listed, if not go back to step 7.
11. Press **Esc**.

2.4.2 HPDL120G7

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Go the HP support page for the DL360G7 and download the Server Guide:
   http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/action.process/public/psi/manualsDisplay/?sp4ts.oid=5075933&javax.portlet.action=true&spf_p.tpst=psiContentDisplay&javax.portlet.begCacheTok=com.vignette.cachetoken&spf_p.prp_psiContentDisplay=wsrp-interactionState%3DdocId%253Demr_na-c02790682%257CdocLocale%253Den_US&javax.portlet.endCacheTok=com.vignette.cachetoken

To install the additional hard disk:

1. Power down the server.
2. Remove the blank from slot 3. Refer to the server guide section *"Removing a blank drive"*.
3. Insert the new hard disk into slot 3. Refer to the server guide section *"Installing a hot-plug drive"*.
4. Power on the server.
5. When the "*Press any Key to view Option ROM Messages*" option appears, press any key.
6. Wait for the message "*Slot 1 HP Smart Array P212 Controller Initializing*" to appear, then press **F8**.
7. From the **Main Menu** select **Create Logical Drive**. Select the following options:

Setting	Single Drive
Available physical drive	***Bay 3***
Raid Configurations	***RAID 0***
Parity Group Count	*Leave blank*
Spare	*Leave blank*
Maximum Boot partition	*Disable*

8. After the options have been selected, press **Enter** to save the configuration.
9. Press **F8** to confirm.
10. Select **Select View Logical Drive**. Ensure there are 2 drives listed, if not go back to step 7.
11. Press **Esc**.

2.4.3 Dell R210

The following is an outline of the process for adding additional drives to an Dell R210 server. For full details refer to the manufacturers documentation.

To install an addition hard disk:

1. Go the Dell support page for the R210 and download the User Manual:
   ftp://ftp.dell.com/Manuals/all-products/esuprt_ser_stor_net/esuprt_poweredge/poweredge-r210_owner%27s%20manual_en-us.pdf
2. Power down the server.
3. Open the system. Refer to the server guide section *"Opening the system"*.
4. Install the 2nd hard drive under the optical drive. Refer to the server guide section *"Installing a Hard Drive"*.
5. Power on the server.
6. Press **F2** to get into the BIOS.
7. Scroll down to **SATA Settings** and press enter
8. Scroll down to **Port B** and change the setting from ***Off*** to ***Auto***.
9. Press **Esc**.
10. Select **Save Changes and Exit**.

2.4.4 Dell R620

The following is an outline of the process for adding additional drives to an HP DL360G7 server. For full details refer to the manufacturers documentation.

Pre-installation:

1. Decide if you will be adding a single HDD or a RAID set as the second drive:
   - A single drive requires 1 hard disk in slot 2.
   - A RAID pair requires 2 hard disks, in slots 2 and 3 respectively, which then act as mirrored images of each other.
2. Go the Dell support page for the R620 and download the Owner's Manual: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCkQFjAA&url=ftp%3A%2F%2Fftp.dell.com%2FManuals%2Fall-products%2Fesuprt_ser_stor_net%2Fesuprt_poweredge%2Fpoweredge-r620_Owner%27s%2520Manual_en-us.pdf&ei=CIfyUr8-rprJAZLcgNgO&usg=AFQjCNFKsTF31-B8KstkroioXiCIaZfHYw&sig2=NmjBrZURDKi6zq59xerNAg&bvm=bv.60799247,d.aWc&cad=rjt

To install the additional hard disk(s):

1. Power down the server.
2. Remove the blank from slot 2. Also from slot 3 if installing a pair of drives for RAID. Refer to server guide section on *"Removing A 2.5 Inch Hard-Drive Blank"*.
3. Insert the new hard disk into slot 2. Also into slot 3 if installing a pair of drives for RAID. Refer to server guide section on *"Installing A Hot-Swap Hard Drive"*.
4. Power on the server.
5. When the RAID controller BIOS details appears, shown by ***"PowerEdge Expandable RAID Controller BIOS"***, press **Ctrl+R** to enter into the utility.
6. On the **VD Mgmt** tab, highlight the top line **PERC H710 Mini**.
7. Press **F2** and select **Create New VD**.
8. Select the following options:

Setting	Single Drive	RAID Pair
RAID Level	***RAID-0***	***RAID-1***
Select Disks	***00:01:02***	***00:01:02*** *and* ***00:01:03***
VD Size	*Leave as default*	*Leave blank*
Advanced settings	*Do not select*	*Leave blank*

9. Press **OK** if prompted.
10. Press **Esc** to leave the utility.
11. Reboot the system.

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 USB memory key, insert the USB memory key into the first USB port and apply power to the PC.
2. The PC should boot and display the first 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.
   - If installing from a USB memory key and the PC does not boot from the USB memory key:
     - if the server has several USB ports, reboot with the USB 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 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. This password is needed for the server ignition process.
   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 USB memory key and then select **Reboot**.
14. Following the reboot, the server displays "SELinux targetted policy relabel is required" and performs that process. When completed, the server reboots again.
15. After the second reboot, wait until the server displays the address details for further configuration of the server. Use the address to start the server ignition process. See Server Ignition 26.

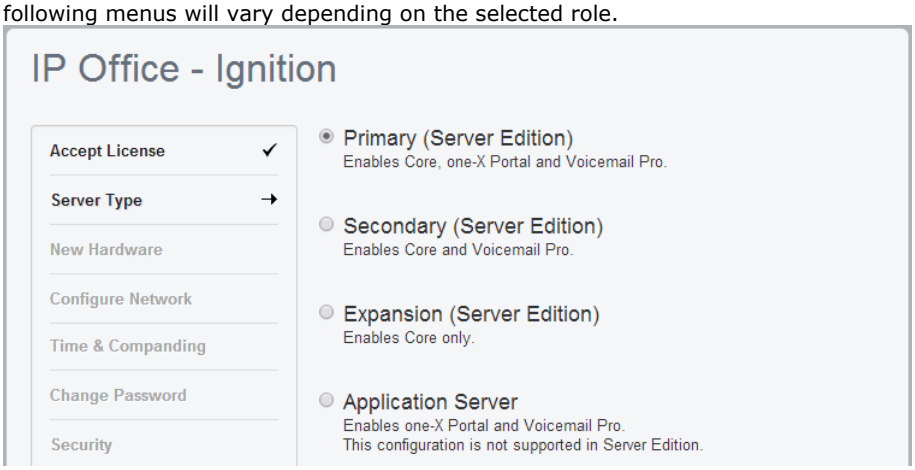
2.6 Server Ignition

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 ***https://192.168.42.1:7071***.
   - The browser may display a security warning. You must determine whether you want to continue.
2. The login page appears. The menu shows both the software level and the SID used for issuing licenses for the server.

3. Enter the password set for the root account during the software installation. Click **Login**.
4. The license menu appears. If you accept the license, select **I Agree** and click **Next**.
5. The menu displays the possible server types. Select the role that the server should perform and click **Next**. The following menus will vary depending on the selected role.



6. If an additional hard disk for Contact Recorder for IP Office was added to the server, details of the additional hardware appear. Otherwise the menu displays *"No new hardware available"*.

   For Contact Recorder for IP Office support it is recommended to accept the defaults. These are:

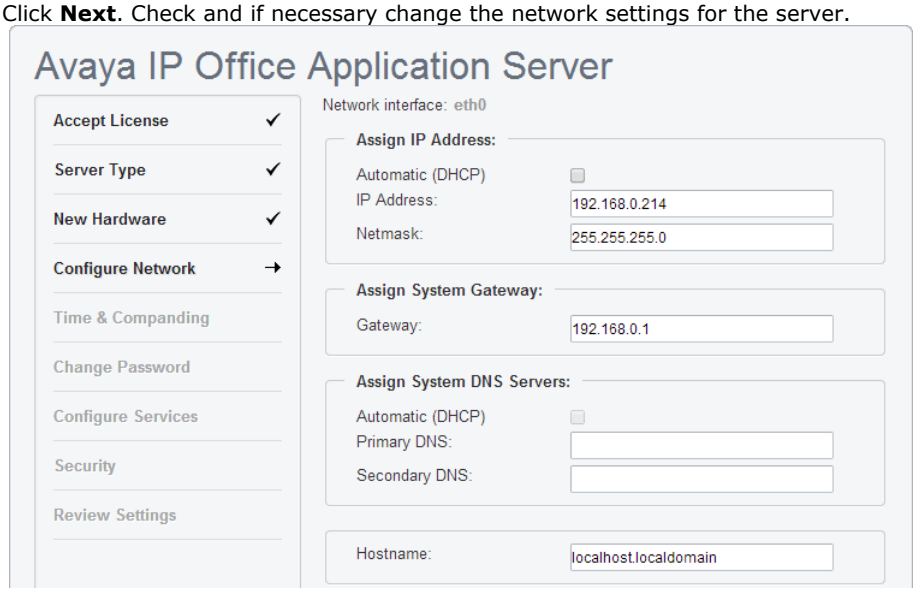
   a. Leave **Format Hard Drive** checked.

   b. Create a single partition for the whole disk. You can create up to 3 logical partitions on the physical disk.

   c. Leave the **Mount Point** name as ***/additional-hdd#1***. The full mount path name for each partition is automatically configured by the system adding ***/partition1***, ***/partition2***, etc. as a suffix. For example ***/additional-hdd#1/partition1***. Note that it is this partition name including ***/partition1*** that should be used for Contact Recorder settings.

   d. Select **Mount Hardware** to have the additional disk automatically mounted.

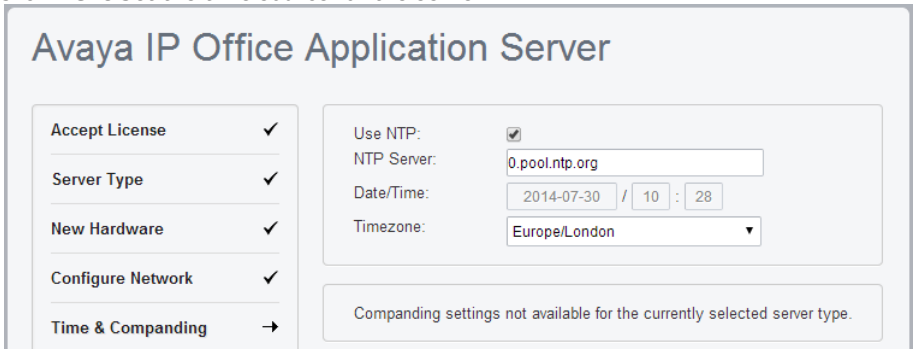
7. Click **Next**. Check and if necessary change the network settings for the server.



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

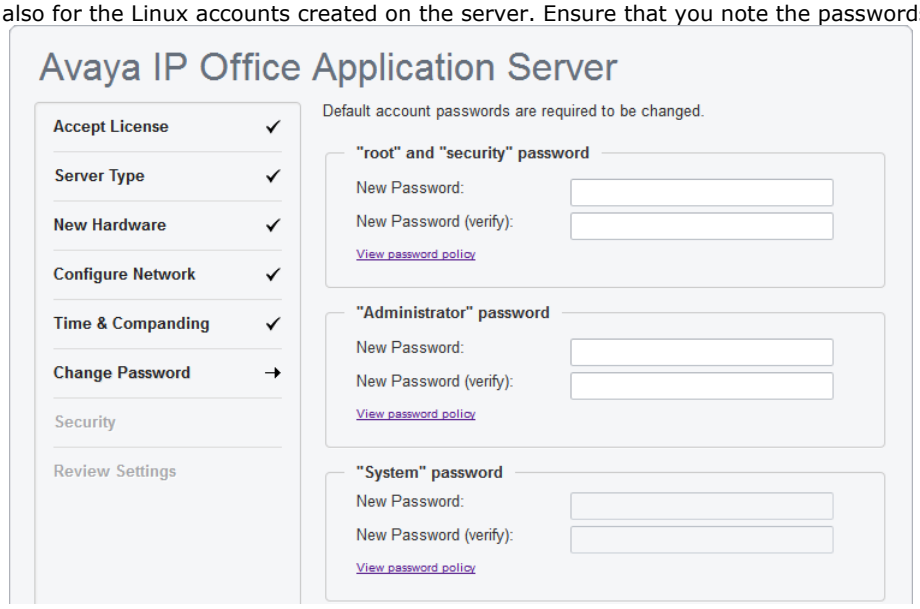
  - **! IMPORTANT: DNS Routing**
    For internal applications, this value must be reachable by DNS within the customer network. If the server will also be supporting external applications, the host name also needs to be reachable by external DNS. Consult with the customers IT support to ensure that the host name is acceptable and that routing to the host name has been configured correctly.

8. Click **Next**.Set the time source for the server.



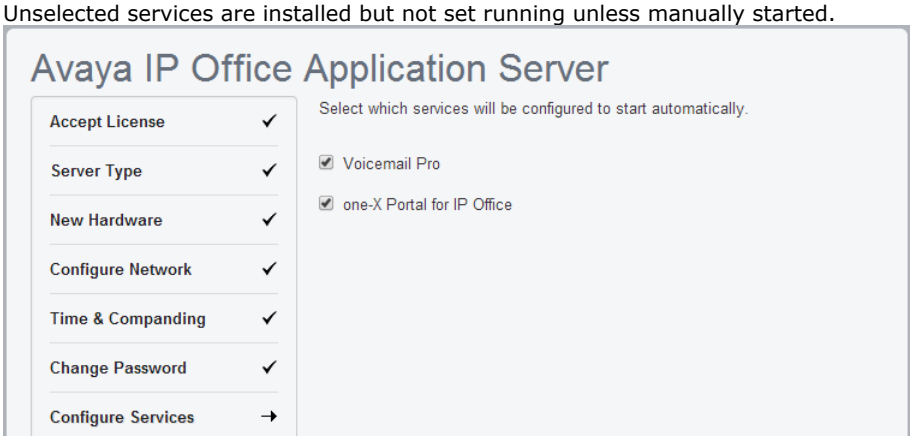
9. Set the current time and date for the server or select to use the time provided by an NTP server.

10. Click **Next**. Enter and confirm the passwords. These are the passwords for various IP Office service accounts and also for the Linux accounts created on the server. Ensure that you note the passwords set.

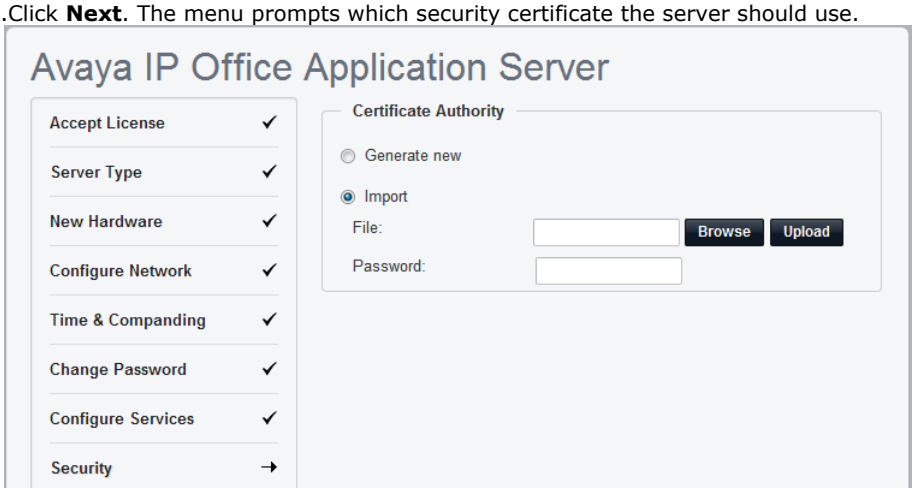


- The passwords must be 8 to 32 characters, containing at least two types of character (lower case, upper case, numeric and special characters) and no more the 3 consecutive characters.
    - **root/security password**
      This sets the password for both the Linux **root** user account and also the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

11. For a server set to be an IP Office Application server, select which applications should start automatically. Unselected services are installed but not set running unless manually started.

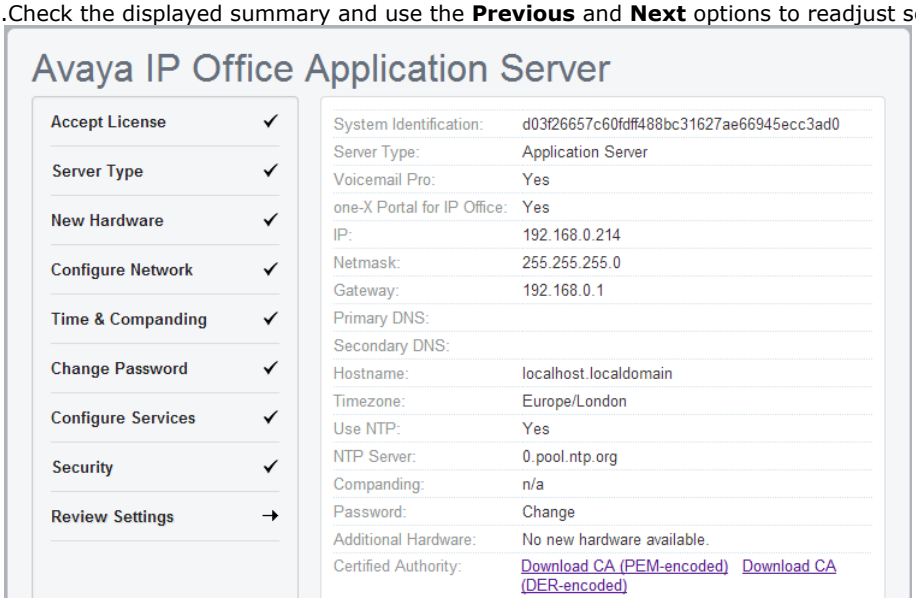


12. Click **Next**. The menu prompts which security certificate the server should use.



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

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



14. If **Generate New** was selected for the server's security certificate, download the security certificate files from the menu and store these safely. These certificates need to be used by the browser and other applications for future access to the server.

15. Follow the instructions for adding a certificate to your browser 30.

16. Click **Apply**. Click **OK** when displayed to access the server's Web Manager menus. Note that this can take up to 8 minutes.

2.7 Adding a Certificate to the Browser

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

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

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

To add a server security certificate to Firefox:

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

To add a server security certificate to Internet Explorer:

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

To add a server security certificate to Google Chrome:

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

To add a server security certificate to Mac Safari:

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

To add a server security certificate to Windows Safari:

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

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

2.8 Logging Into Web Manager

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 browsers for web access to the server menus:

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

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

1. Log in to IP Office Web Manager.

   a. Enter **https://** followed by the server address. Click on the **IP Office Web Manager** link.

   b. Enter the user name and password.

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

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

2. Click on **Solution**.

2.9 Logging In Directly

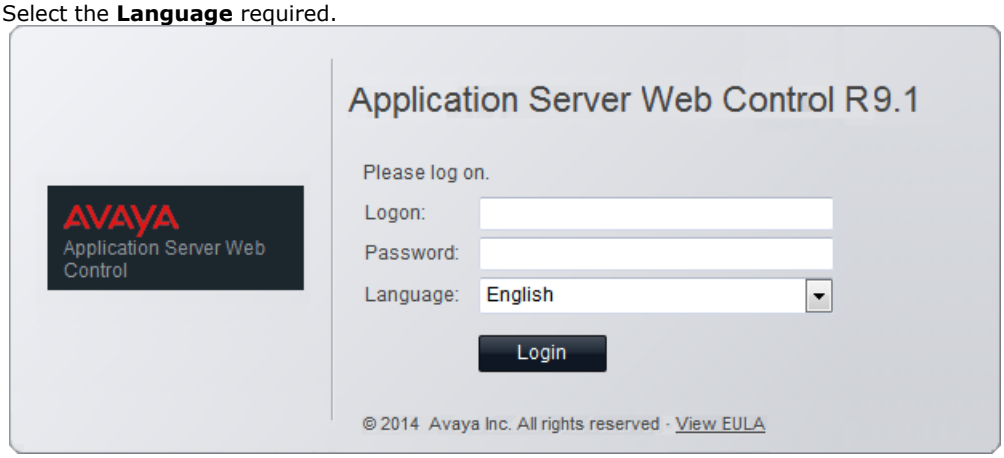
You can access the web control menus for the server directly using a web browser. This may be necessary if there is some issue with accessing the Web Manager menus.

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

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

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

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



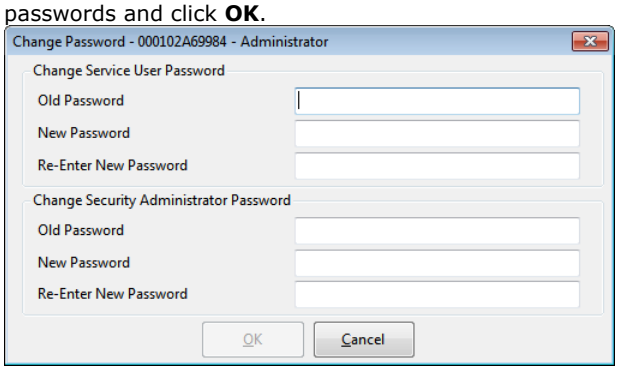
3. Enter the name and password for server administration.
4. If the login is successful, the server's **System** page appears.

2.10 IP Office Initial Configuration

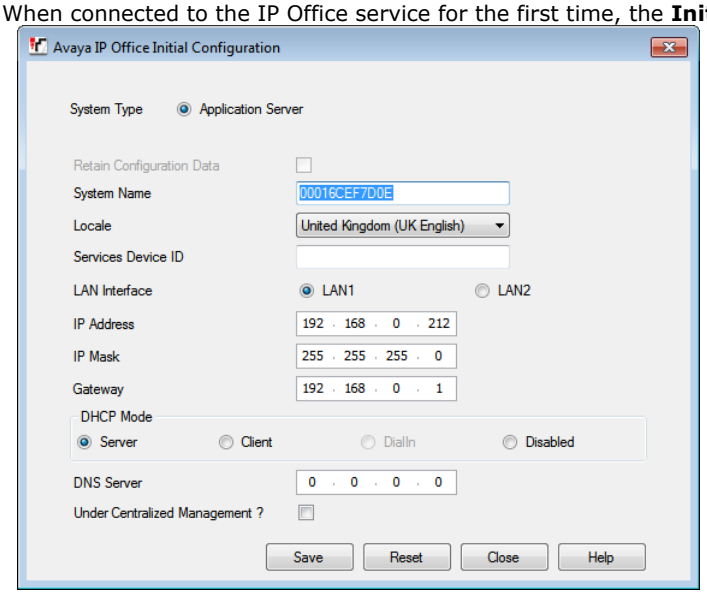
The Management Services service provided by the server requires initial configuration. This is especially important for servers centrally managed using Avaya System Manager.

To perform IP Office initial configuration:

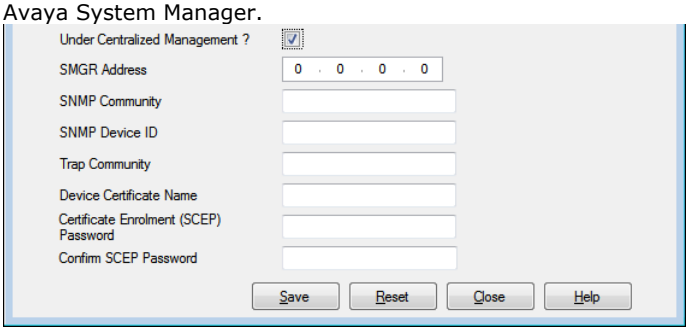
1. Start IP Office Manager. Click and use the **Select IP Office** menu to discover the available IP Office systems.
2. Select the tick box next to the application server. Click **OK**.
   - If any Management Services passwords are at their default values, a menu to change the default passwords appears.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



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



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



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

2.11 IP Office Licensing

The license requirements depend on type of IP Office system.

- For Server Edition systems, only the Server Edition Primary Server requires a **VMPro Recordings Administrators** license.
- For non-Server Edition systems, each system in the network requires a **VMPro Recordings Administrators** license.

Avaya base each license on the unique **System Identification** of the server. Therefore, you cannot use the license from one server on another server.

To add a license:

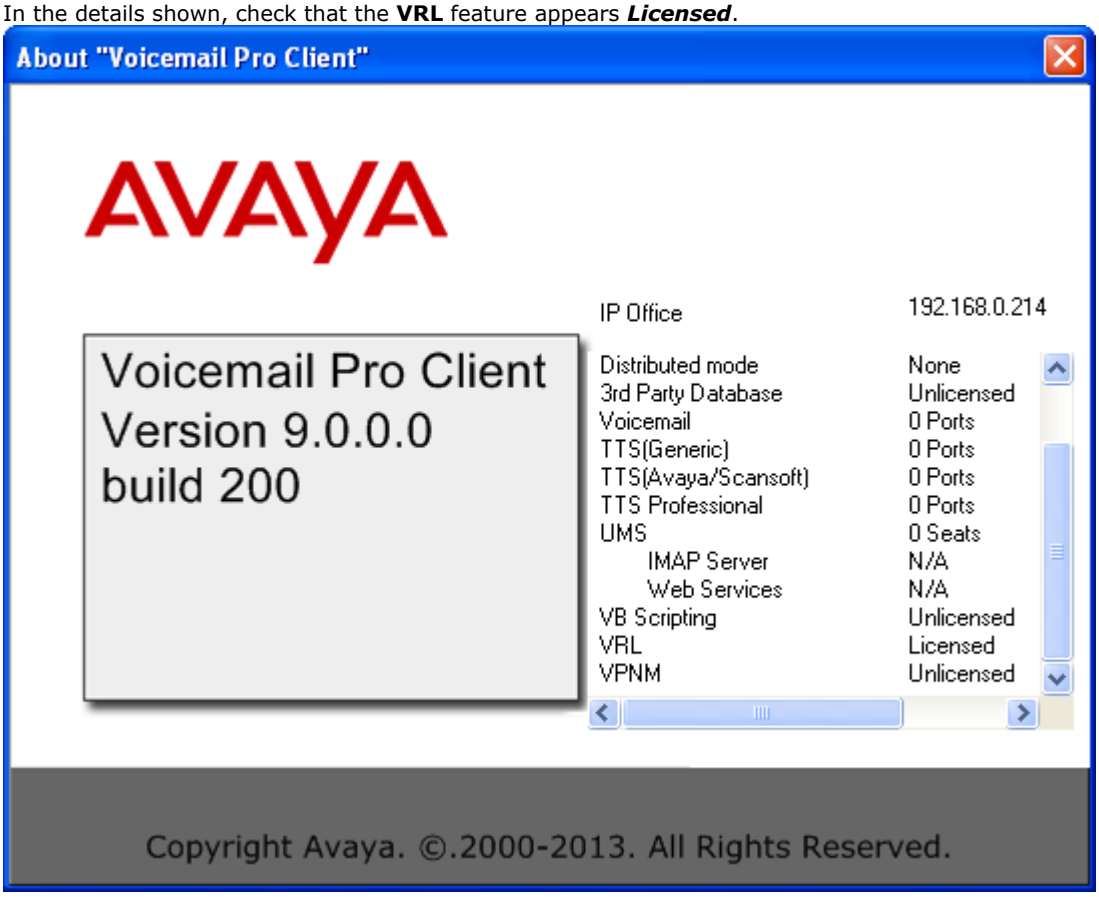
1. Start IP Office Manager and load the configuration from the server.
   a. In the navigation tree, expand the details of the server and select **License**.
   b. Click **Add**.
   c. Enter the supplied license for the system and click **OK**.
   d. The license **Feature** should list ***VMPro Recordings Administrator***. The **Status** should show ***Unknown***.
   e. Repeat this process for any other servers licensed.
2. Click to save the configuration file
3. Close and then reload the configuration.
4. Check that the **Status** of the licenses has now changed to ***Valid***.

2.12 Checking the Voicemail Licenses

The licenses entered in the IP Office system configurations enable various features including optional voicemail features. Using the Voicemail Pro client, you can check the features licensed for the voicemail server. The feature required for Contact Recorder for IP Office is support of **VRL** (Voice Recording Library).

To check the voicemail licenses:

1. Login to the voicemail server using the Voicemail Pro client.
2. Click **Help | About**.
3. In the details shown, check that the **VRL** feature appears ***Licensed***.



2.13 Adding the Application Server

For application server installations, the application server is not automatically included in the list of servers shown by IP Office Web Manager.

To add the application server to the solution menu:

1. Login to the Server Edition Primary Server server's Web Manager menus at *https://<server_address>:7070*.
2. From the **Solution Settings** drop-down list, select **Application Server**.
3. Enter the IP address of the application server.
4. Click **OK**.
5. The application server should now appear in the list of servers.

2.14 Enabling the Contact Recorder for IP Office Service

The server installation includes the component for Contact Recorder for IP Office. The server is installed by default but not enabled.

To enable the Contact Recorder for IP Office application:

1. Login to the primary server's Web Manager menus.
2. Click **Platform**.
3. Select the server from the list of servers.
4. Select the **System** tab. Click on **Show optional** services.
5. If the service **Contact Record** is not listed, use the following steps to add the service:
   a. Select the **Updates** tab.
   b. In the list of services, location the **Application** named ***Contact Recorder***. The status should show *not installed*.
   c. Click **Install**.
   d. Select the **System** tab.
6. For the ***Contact Recorder*** service.
   a. Select the automatic start check box.
   b. Click **Start** and check that the application status changes to started.

2.15 Logging In to Contact Recorder for IP Office

Contact Recorder for IP Office supports Microsoft Internet Explorer 8, 9 or 10. The playback function requires the browser to allow the download and installation of a number of ActiveX controls.

To log in to Contact Recorder for IP Office:

1. Start a web browser and enter the address for Contact Recorder for IP Office server.
   - For secure access, enter **https://<*server_address*>:9444**.
   - For unsecure access, enter **http://<*server_address*>:9888**.
2. Enter your user name. The default user name for administration is ***Administrator***.
3. Enter your password. For the ***Administrator***, the default password is blank.
4. Click **OK**.
   a. When logging in for the first time, the system prompts you to change your password.
   b. Enter the existing password and a new password.
   c. Click **OK**.
5. The menus displayed depend on the role assigned to the user name by the administrator.

2.16 Setting the File Paths

Contact Recorder for IP Office uses two key file paths, one for collecting recordings and one for storing those recordings.

To check the file transfer and storage addresses:

1. Login to Contact Recorder for IP Office as an administrator.
2. Select **General Setup**.
3. Check the **Handover Folder** setting. The path should be set to ***/opt/vmpro/VRL***.
   - **Separate Server Installation**
     If Contact Recorder for IP Office has been enabled on a separate server from Voicemail Pro, this is the folder to which Voicemail Pro should be configured to send recordings. See Configuring the Transfer of Recordings 39.
   - **Single Server Installation**
     If Contact Recorder for IP Office has been enabled on the same server as Voicemail Pro, both applications use the same default.
4. Check the **Call storage path** setting. This is the folder path which the Contact Recorder for IP Office uses to store recordings.
   - **Separate Server Installation**
     If Contact Recorder for IP Office has been enabled on a separate server from Voicemail Pro, this path should be set to **/CSIPORec** unless an additional disk has been added for its use, in which case use **/additional-hdd#1/partition1** (or the appropriate additional disk and disk partition intended for Contact Recorder for IP Office use as set in that server's web control menus (**Platform View | Settings | System | Additional Hardware Info | Mount Path Name** including ***/partitionX***).
   - **Single Server Installation**
     If Contact Recorder for IP Office has been enabled on the same server as Voicemail Pro by using an additional disk, the path should be set to **/additional-hdd#1/partition1** (or the appropriate additional disk and disk partition intended for Contact Recorder for IP Office use as set in that server's web control menus (**Platform View | Settings | System | Additional Hardware Info | Mount Path Name** including ***/partitionX***)).
5. If you change either path, you must restart the Contact Recorder for IP Office service. See below.

To restart the Contact Recorder for IP Office service:

1. Login to the primary server's Web Manager menus.
2. Click **Platform**.
3. Select the server from the list of servers.
4. Select the **System** tab.
5. For the ***Contact Recorder*** application, click **Stop**.
6. Wait until the service appears as ***stopped***. Click **Start**.

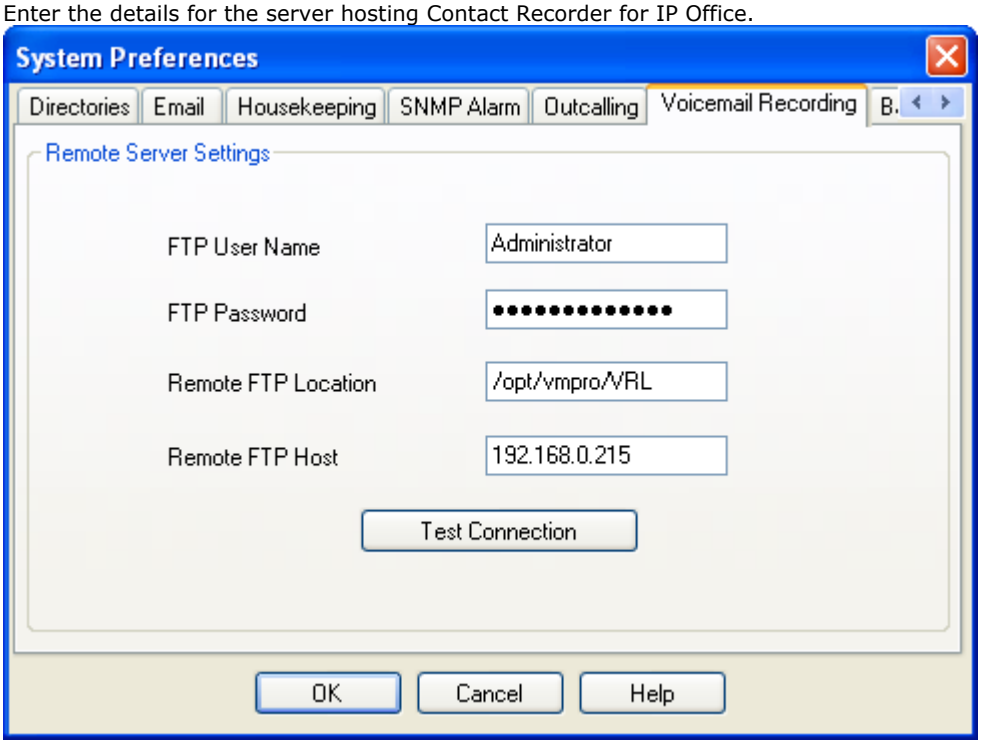
2.17 Configuring the Transfer from Voicemail Pro

If Contact Recorder for IP Office has been enabled on a separate server from Voicemail Pro, then the following additional Voicemail Pro configuration is required. This configures the automatic transfer of any files in the voicemail server's */opt/vmpro/VRL* folder to the matching folder on the server hosting Contact Recorder for IP Office.

If the Server Edition network includes a backup voicemail server on a Server Edition Secondary Server, that backup voicemail server does not require any direct configuration. It receives a copy of all the settings from the primary voicemail server including the settings below for transferring recordings to the Contact Recorder for IP Office.

To setup and test the transfer of recordings:

1. Login to the voicemail server using the Voicemail Pro client.
2. Click the **Preferences** icon and select **General**.
3. Select the **Voice Recording** tab.
4. Enter the details for the server hosting Contact Recorder for IP Office.



- **FTP User Name** / **FTP Password**
  Enter the details of a user account with read-write permissions for the folder (configured below) on the target server. The default is to use the server's **Administrator** account.
- **Remote FTP Location**
  Enter the location on the target server that Contact Recorder for IP Office checks for new transferred recordings (see Setting the File Paths 38). The default location is */opt/vmpro/VRL*.
- **Remote FTP Host**
  Enter the IP address or fully qualified domain name of the server hosting Contact Recorder for IP Office.

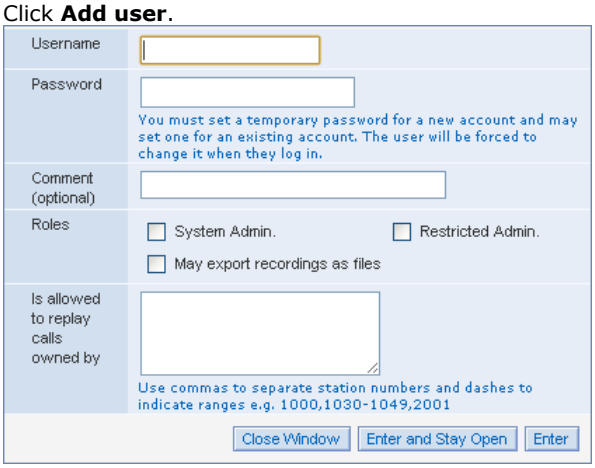
5. Click **Test Connection**.
6. Click **OK**.

2.18 Adding Users

Users for Contact Recorder for IP Office are configured either directly in Contact Recorder for IP Office or via using Windows domain authentication. For the later, refer to the Contact Recorder for IP Office Administering Contact Recorder for IP Office manual. The example below is only for adding a user directly into the Contact Recorder for IP Office configuration.

To add additional users:

1. Login to Contact Recorder for IP Office as an administrator.
2. Select **System**.
3. Click **Add user**.



- **Username**
  Enter a user name for the user's account.
- **Password**
  Enter a password of at least 8 characters (the default setting). This is only a temporary password. When the user logs in using this password, the system prompts them to set a new password.
- **Roles**
  The selected role for the user affects which menus they can access when logged in to Contact Recorder for IP Office. Users with no admin role only see the menus for searching for recordings.
  - **System Admin**
    This type of user has full access to the application settings.
  - **Restricted Admin**
    This type of user can see the system status and alarms; eject DVDs and administer non-admin user accounts. They cannot change the system configuration settings.
  - **May export recordings as files**
    If selected, the user is able to export recordings from the search results rather than just replay.
- **Is allowed to replay calls owned by**
  Use this field to enter the list of extensions that the user is allowed to search for and replay recordings. Enter a comma-separated list of individual station or agent numbers. You can also use a hyphen to separate the ranges. If you have several users with the same replay rights, you can select the text in this area and right-click to copy it to the clipboard. You can then paste it into the next account, saving a lot of typing and potential for error. Note that the number of digits is important. For example, giving a user rights over 0000-9999 does not give them rights over any 2, 3, or 5 digit numbers. Some typical examples are:
  - ***4000***
    This user can only replay calls involving extension 4000. This is a typical entry for entry for someone to only be able to replay their own recordings.
  - ***4000-4019***
    This user can only replay calls involving extensions in the range 4000 to 4019. This is a typical entry for a supervisor of a group of agent with those numbers.
  - ***4000,4003,4010-4019,4124-4128***
    This user can replay calls involving a more complex range of numbers. This is a typical entry for a supervisor where the originally assigned numbering plan has grown over time.
  - ***1000-9999***
    This user can replay any calls with a 4-digit extension number. This is a typical entry for a senior manager with search and replay rights over all recordings.

4. If you want to add multiple users, click **Enter and Stay Open**, otherwise click **Enter**.

2.19 Test Operation

Before proceeding any further, test basic call recording operation.

To test operation:

1. Create a test user in Contact Recorder for IP Office who has playback right for your test extension. See Adding Users 40.
2. Using IP Office Manager, configure automatic call recording of the test extension user's internal calls. See User Automatic Recording 50.
3. Make a test call from that user. You should hear the advice of call recording warning. See Configuring the Advice of Call Recording Warning 44.
4. Wait a minute for the call recording to transfer from the voicemail server to the Contact Recorder for IP Office server.
5. Log in to Contact Recorder for IP Office as the test user. Search for the recording.

Chapter 3.
Recording Configuration

3. Recording Configuration

This section covers configuration of which calls the system records.

Processes:

- Configuring the advice of call recording warning 44
- Configuring the recording display 45
- Changing the maximum recording length 45
- Configuring manual call recording for users 46
- Configuring automatic call recording 49
  - To configure automatic user recording 50
  - To configure automatic hunt group recording 51
  - To configure incoming call route recording 52
  - To configure account code recording 53

3.1 Configuring the Advice of Call Recording Warning

In many locations, it is a local or national requirement to warn all parties involved in a call about call recording.

- The voicemail server provides an advice of call recording warning by default.
- If any other party joins the call after it starts, for example in a conference call, the advice of call recording warning repeats each time a new party joins the call.
- For each language installed on the voicemail server, the server uses the file named ***aor_00.wav*** to provide the warning.
- Analogue trunks do not support call status signaling. Since the advice of recording warning plays as soon as the trunk, even if the remote end is still ringing, the called party may not always hear the warning.

To switch the advice of call recording warning on or off:

1. From the Voicemail Pro client, click or select **Administration** > **Preferences** > **General**.
2. Click **Play Advice on Call Recording** to switch this option on (checked) or off (unchecked).
3. Click **OK**.
4. Click **Save & Make Live**.

3.2 Configuring the Recording Display

Some Avaya terminals display **REC** when involved in a recorded call.

To hide the auto record indication

1. Open the system configuration in IP Office Manager.
2. In the navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. Check **Hide auto recording**. This hides the display of **REC** of phones that support that feature when recording a call.
5. Save the configuration back to the IP Office system.

3.3 Changing the Recording Length

The maximum length of call recordings made by Voicemail Pro is adjustable.

To change the recording length:

1. Start the Voicemail Pro client and connect to the voicemail server.
2. Click or select **Administration > Preferences** > **General**.
3. The **Max. VRL Record Length (secs)** setting sets the maximum length for recordings. The maximum setting is 18000 seconds (300 minutes).
4. Click **OK**.
5. Click **Save & Make Live**.

3.4 Configuring Manual Call Recording

You can configure Contact Recorder for IP Office as the destination for call recordings manually triggered by a user.

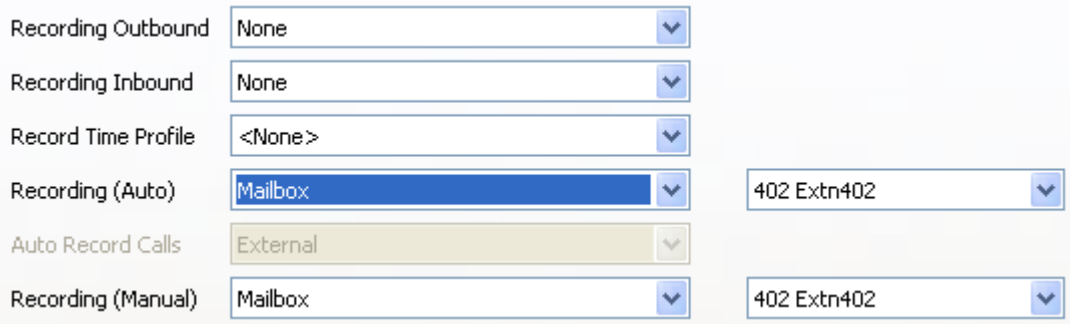
- Configuring the manual recording destination 46
- Triggering manual call recording 47
  - Using IP Office SoftConsole 47
  - Using a programmable button 48
  - Using a short code 48

3.4.1 Configurng the Manual Recording Destination

By default user's can use manual call recording at any time. They do this using a variety of methods for triggering manual call recording 47. To use manual call recording with Contact Recorder for IP Office, you must change the destination of the recording.

To configure a user's recording options:

1. Start IP Office Manager and load the configuration from the primary server.
2. Click **User** and select the individual user.
3. Select the **Voice Recording** tab.



4. Use **Recording (Manual)** to specify the destination for the recordings. By default, this is a user's own mailbox.
   - **Mailbox**
     This is the default option. When selected, you can use the adjacent drop down list to select the destination user or hunt group mailbox. These files are typically 0.5MB to 1MB per minute.
   - **Voice Recording Library**
     Use this option to have the recordings transferred to the VRL folder after recording (from which it can be collected by applications such as Contact Recorder for IP Office). This option produces a G.711 format file that Contact Recorder for IP Office converts to G.729A format after the file transfer. These files are typically 60KB per minute.
   - **Voice Recording Library Authenticated**
     As above but this option produces a G.726 format file that contains file authentication information. Any subsequent editing of the file invalidates that information. Contact Recorder for IP Office does not convert the file to G.729A format after the file transfer. These files are typically 120KB per minute. This option is currently not supported with Linux based servers.
5. Click **OK**.
6. Click to merge the configuration change back to the IP Office.

3.4.2 Triggering Manual Call Recording

There are several ways to start manually recording a telephone call.

- Using one-X Portal for IP Office 47
- Using IP Office SoftConsole 47
- Using a Programmable Button 48
- Using a Short Code 48

3.4.2.1 Using one-X Portal for IP Office

A user can use one-X Portal for IP Office to stop and start manual call recording.

To start call recording using one-X Portal for IP Office:

1. Using the **Calls** gadget on the **Main** tab, select the call tab for the connected call. It will be the tab with two connected handsets icon on the right.
2. To start recording the call, click on the record button on the right. If the button displays as an icon then recording is not available for some reason.
3. Once recording has started, the button changes to an icon. Click on this to end recording. Call recording also automatically stops if you park, transfer or turn the call in to a conference. If you hold the call, call recording is paused while the call is on hold.

3.4.2.2 Using IP Office SoftConsole

The SoftConsole operator can manually record all or part of a current telephone call.

- Press the button on the toolbar. The button acts as a toggle. Press the button again to stop recording.
- Select **Actions** > **Record Call**. This action toggles and so also stops recording.
- Press **F5** to start recording. Press **F5** again to stop the recording.

3.4.2.3 Using a Programmable Button

You can program the call record function against a DSS key.

To set a DSS key for manual recording:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the Navigation pane, click **User** and select the individual user.
3. Select the **Button Programming** tab.
4. Select the required DSS key and click **Edit**.
5. Click browse for the **Action**. The Button Programming window opens.
6. Select **Advanced | Call | Call Record**. Click **OK**.
7. In the **Action Data** field, enter the description to appear on the telephone display.
8. Click **OK**.
9. Click to save the configuration file.

3.4.2.4 Using a Short Code

The short code feature **Call Record** triggers manual call recording. The example short code (*95) can be set up as a user or system short code.

Field	Contains...
Code	*95
Feature	Call Record
Telephone Number	[Leave blank]
Line Group Id	0

To use the short code

1. During a call, put the caller on hold.
2. Dial the short code. The held call is automatically reconnected and recording begins.

3.5 Configuring Automatic Call Recording

You can configure the IP Office system to automatically record calls based on the user, hunt group, incoming call route or account code.

Trigger	Incoming	Outgoing	Duration
Incoming Call Route	Yes	–	For the call duration or up to 1 hour.
Hunt Group	Yes	–	Until ended or until transferred to a user outside the hunt group or its overflow group.
User	Yes	Yes	Until the user ends or transfers call.
Account Code	–	Yes	Until the user ends or transfers calls.

- Individual calls may match several recording criteria. In that case:
  - If the destinations for the recordings are different, separate recordings occur with the durations as indicated above.
  - If the destinations for the recordings are the same, the system makes a single recording using either the incoming call route, hunt group or user duration in that order of priority.
- Multiple recordings of the same call use multiple voicemail channels.
- Time profiles can control when automatic call recording is used.
- For inbound calls, recording will not take place if the call goes to normal voicemail to leave a mailbox message.
- If set to mandatory call recording, busy tone if returned to the caller when no voicemail ports are available to do the recording.
- Where calls have been answered using a Line appearance button, the call recording uses the voicemail setting of the original call route destination.

To configure automatic call recording:

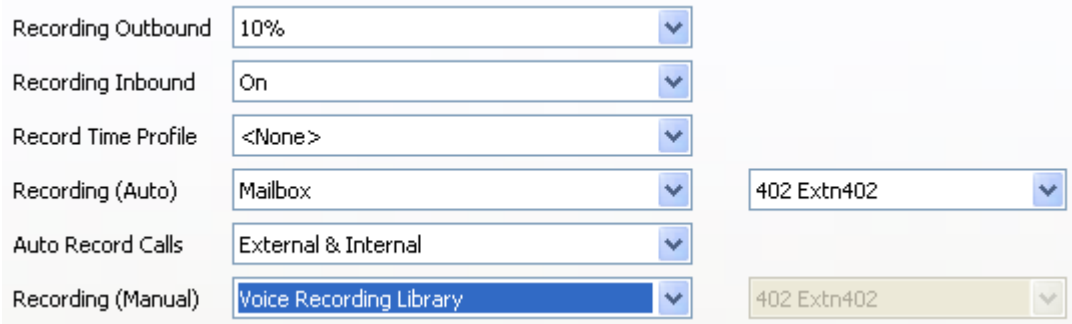
- To configure automatic user recording 50
- To configure automatic hunt group recording 51
- To configure incoming call route recording 52
- To configure account code recording 53

3.5.1 User Automatic Recording

You can automatically record calls to and from a user. You can select just external calls or all calls.

To set automatic call recording for a user:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the navigation pane, click **User**. Select the required user.
3. Select the **Voice Recording** tab.



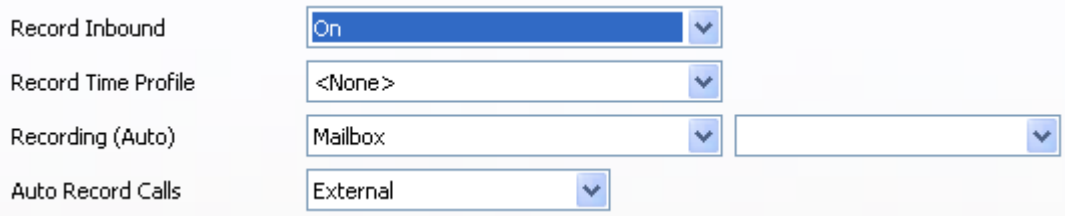
4. From the **Record Inbound** and **Record Outbound** drop-down lists, select the recording frequency.
   - **None:** Do not record.
   - **On:** Record all calls if possible.
   - **Mandatory:** Record all calls. If recording is not possible, return busy tone to the caller.
   - **xx%:** Record calls at intervals matching the set percentage. For example, for every other call select ***50%***.
   - For inbound calls, recording will not take place if the call also goes to normal voicemail.
5. Use **Record Time Profile** to select a time profile that specifies when automatic call recording is active. If not set, recording is active at all times.
6. Use **Auto Record Calls** to select whether ***External*** or ***External & Internal*** calls are included.
7. Use **Recording (Auto)** to specify the destination for the recordings. By default, this is a user's own mailbox.
   - **Mailbox**
     This is the default option. When selected, you can use the adjacent drop down list to select the destination user or hunt group mailbox. These files are typically 0.5MB to 1MB per minute.
   - **Voice Recording Library**
     Use this option to have the recordings transferred to the VRL folder after recording (from which it can be collected by applications such as Contact Recorder for IP Office). This option produces a G.711 format file that Contact Recorder for IP Office converts to G.729A format after the file transfer. These files are typically 60KB per minute.
   - **Voice Recording Library Authenticated**
     As above but this option produces a G.726 format file that contains file authentication information. Any subsequent editing of the file invalidates that information. Contact Recorder for IP Office does not convert the file to G.729A format after the file transfer. These files are typically 120KB per minute. This option is currently not supported with Linux based servers.
8. Click **OK**.
9. Click to send the configuration back to the IP Office.

3.5.2 Hunt Group Automatic Recording

You can automatically record calls answered by any member of a hunt group. You can select just external calls or all calls.

To set automatic call recording for a hunt group:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the Navigation pane, click **Hunt Group**.
3. Select the required hunt group.
4. Select the **Voice Recording** tab.



5. Use **Record Time Profile** to select a time profile that specifies when automatic call recording is active. If not set, recording is active at all times.
6. Use **Auto Record Calls** to select whether ***External*** or ***External & Internal*** calls are included.
7. From the **Record Inbound** drop-down list, select the recording frequency.
   - **None:** Do not record.
   - **On:** Record all calls if possible.
   - **Mandatory:** Record all calls. If recording is not possible, return busy tone to the caller.
   - **xx%:** Record calls at intervals matching the set percentage. For example, for every other call select ***50%***.
   - For inbound calls, recording will not take place if the call also goes to normal voicemail.
8. Use **Recording (Auto)** to specify the destination for the recordings.
   - **Mailbox**
     This is the default option. When selected, you can use the adjacent drop down list to select the destination user or hunt group mailbox. These files are typically 0.5MB to 1MB per minute.
   - **Voice Recording Library**
     Use this option to have the recordings transferred to the VRL folder after recording (from which it can be collected by applications such as Contact Recorder for IP Office). This option produces a G.711 format file that Contact Recorder for IP Office converts to G.729A format after the file transfer. These files are typically 60KB per minute.
   - **Voice Recording Library Authenticated**
     As above but this option produces a G.726 format file that contains file authentication information. Any subsequent editing of the file invalidates that information. Contact Recorder for IP Office does not convert the file to G.729A format after the file transfer. These files are typically 120KB per minute. This option is currently not supported with Linux based servers.
9. Click **OK**.
10. Click to send the configuration back to the IP Office.

3.5.3 Incoming Call Route Automatic Recording

You can automatically record incoming external calls routed by a particular incoming call route.

To set automatic call recording for an incoming call route:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the Navigation pane, click **Incoming Call Route**.
3. Select the required incoming call route.
4. Select the **Voice Recording** tab.

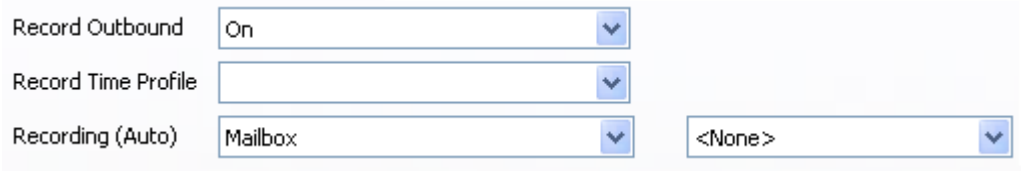
5. From the **Record Inbound** drop-down list, select the recording frequency.
   - **None:** Do not record.
   - **On:** Record all calls if possible.
   - **Mandatory:** Record all calls. If recording is not possible, return busy tone to the caller.
   - **xx%:** Record calls at intervals matching the set percentage. For example, for every other call select ***50%***.
   - For inbound calls, recording will not take place if the call also goes to normal voicemail.
6. Use **Record Time Profile** to select a time profile that specifies when automatic call recording is active. If not set, recording is active at all times.
7. Specify the destination for the recordings or select the option to place the recordings in the voice recording library.
   - **Mailbox**
     This is the default option. When selected, you can use the adjacent drop down list to select the destination user or hunt group mailbox. These files are typically 0.5MB to 1MB per minute.
   - **Voice Recording Library**
     Use this option to have the recordings transferred to the VRL folder after recording (from which it can be collected by applications such as Contact Recorder for IP Office). This option produces a G.711 format file that Contact Recorder for IP Office converts to G.729A format after the file transfer. These files are typically 60KB per minute.
   - **Voice Recording Library Authenticated**
     As above but this option produces a G.726 format file that contains file authentication information. Any subsequent editing of the file invalidates that information. Contact Recorder for IP Office does not convert the file to G.729A format after the file transfer. These files are typically 120KB per minute. This option is currently not supported with Linux based servers.
8. Click **OK**.
9. Click to send the configuration back to the IP Office.

3.5.4 Account Code Automatic Call Recording

You can automatically record outgoing external calls that use a particular account code. Note, in a Server Edition network, by default every system in the network shares the same account codes.

To set automatic call recording for an outgoing account call:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the Navigation pane, click **Account Code**.
3. Select the required account code.
4. Select the **Voice Recording** tab.



5. From the **Record Outbound** drop-down list, select the recording frequency.
   - **None:** Do not record.
   - **On:** Record all calls if possible.
   - **Mandatory:** Record all calls. If recording is not possible, return busy tone to the caller.
   - **xx%:** Record calls at intervals matching the set percentage. For example, for every other call select ***50%***.
   - For inbound calls, recording will not take place if the call also goes to normal voicemail.
6. Select the **Recording Time Profile** to select a time profile that specifies when automatic call recording is active. If not set, recording applies at all times.
7. Use the **Recording (Auto)** option to select the destination for the recording.
   - **Mailbox**
     This is the default option. When selected, you can use the adjacent drop down list to select the destination user or hunt group mailbox. These files are typically 0.5MB to 1MB per minute.
   - **Voice Recording Library**
     Use this option to have the recordings transferred to the VRL folder after recording (from which it can be collected by applications such as Contact Recorder for IP Office). This option produces a G.711 format file that Contact Recorder for IP Office converts to G.729A format after the file transfer. These files are typically 60KB per minute.
   - **Voice Recording Library Authenticated**
     As above but this option produces a G.726 format file that contains file authentication information. Any subsequent editing of the file invalidates that information. Contact Recorder for IP Office does not convert the file to G.729A format after the file transfer. These files are typically 120KB per minute. This option is currently not supported with Linux based servers.
8. Click **OK**.
9. Click to send the configuration back to the IP Office.

3.6 Pausing Recording

Sometimes it is a requirement to pause call recording. For example, when recording calls where the user asks the caller to reveal sensitive information such as a credit card number.

To do this, you can assign a pause recording button to a user's phone. The user can use the button with manually and automatically recorded calls.

The button status indicates when call recording is paused. Pressing the button again restarts call recording. The system can also automatically restart recording after a set delay.

If the voicemail system provides an advice of call recording warning 44, pausing recording triggers a *"Recording paused"* prompt and a repeat of the advice of call recording warning when recording resumes.

3.6.1 Configuring a Pause Recording Button

To pause recording, you need to configure a pause recording button for the user.

To configure a pause recording button:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the Navigation pane, click **User** and select the individual user.
3. Select the **Button Programming** tab.
4. Select the required DSS key and click **Edit**.
5. Click browse for the **Action**. The Button Programming window opens.
6. Select **Advanced | Call | Pause Recording**. Click **OK**.
7. In the **Action Data** field, enter the description to appear on the telephone display.
8. Click **OK**.
9. Click to save the configuration file.

3.6.2 Setting the Auto Restart Delay

By default, the system automatically restarts a paused recording after 15 seconds.

To set the auto restart delay for paused recording:

1. Start IP Office Manager and load the configuration from the primary server.
2. In the Navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. Set **Auto Restart Paused Recording** to the required time in seconds or never.
5. Save the configuration back to the IP Office system.

3.7 Customisable Callflow Options

In customized voicemail callflows, the voicemail server uses a **Leave Mail** action to record a message. The action's settings include the option to have the resulting message sent to Contact Recorder for IP Office.

Chapter 4.
Additional Processes

4. Additional Processes

4.1 Enabling DVD Archiving

When recording storage space is limited, the Contact Recorder for IP Office automatically deletes recordings on a first in first out (FIFO) basis. To avoid this and to conserve space on the server, Contact Recorder for IP Office can archive older recordings to a DVD+RW disc (single layer), to a Blu Ray -R disc (single layer) or to network attached storage.

This section covers using the server's own DVD drive as the archive destination. For other options, refer to the Administering Contact Recorder for IP Office manual 12.

Process Summary

1. Identifying the drive path and udi 56
2. Disabling the media detection service 57
3. Entering the drive in Contact Recorder for IP Office 58

4.1.1 Identifying the Drive Path and UDI

The file path for DVD drives, for example ***/dev/sr0***, can vary between servers. The process below determines the drive path and **udi** for the drive.

To identify the DVD drive name:

1. At the physical server, start its desktop:
   a. Enter the command **startx**.
   b. Login as the **Administrator**.
2. We need to obtain a list of all the drives mounted on the server:
   a. Click **Applications** and select **System Tools | Terminal**. This starts a command line window.
   b. In the terminal window, enter **lshal -l > hal.txt**. This outputs the details of all the mounted drives to a text file called **hal.txt**.
3. We can now get the details of the DVD drive from the text file:
   a. Double click on home folder on the desktop.
   b. Locate the file ***hal.txt*** and double-click on it. The file opens in the gedit file editor.
   c. Use the find function to search for ***cdrom***. If this fails, try searching for ***cdrom1*** or ***dvd***.
   d. The file consists of sections of data, each starting with ***udi =***. Locate the first such section containing your search string and a line similar to ***block.device = '/dev/sr0' (string)***. That value is the drive path for the drive.
4. We can test whether the value shown for block.device is the path for the DVD drive.
   a. In the terminal window, enter the path as part of an eject command. For our example, enter **eject /dev/sr0**. The drive tray should open.
   b. Enter **eject -t /dev/sr0** to close the drive tray.
5. If necessary, continue searching the ***hal.txt*** file for the correct path for the drive.
6. Once you have identified the drive, note the **udi** value shown above **block.device**. This will be something like ***/org/freedesktop/Hal/devices/storage_model_DVD_RW_DW_Q30A***. For example, ***udi = '/org/freedesktop/Hal/devices/storage_model_DVD_RW_DW_Q30A'***.
7. The ***udi*** value is needed in the following process, highlight the value (the part between the ' ' marks) and select **Edit | Copy**.
8. Having identified the drive path and obtained the drive's **udi**, see Disabling the Media Detection Service 57.

4.1.2 Disabling the Media Detection Service

The HAL media detection service interferes with Contact Recorder for IP Office.

To disable a drive from the media detection service:

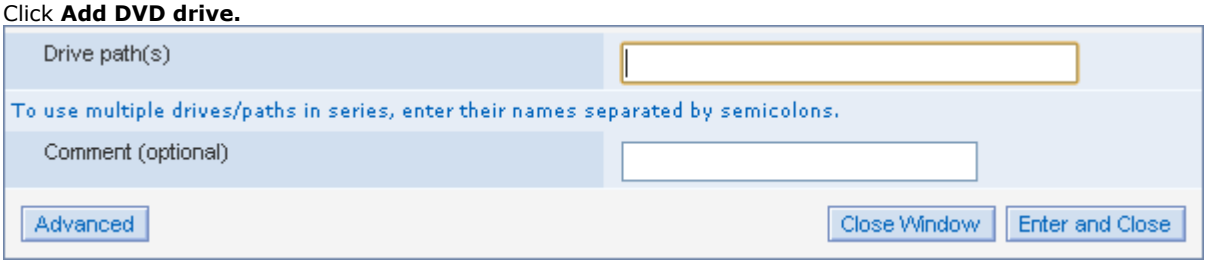
1. Use the process in Identifying the Drive Path 56 to also identify the drive's **uid**.
2. In the terminal window, check the current value of the drive's **media_check_enabled** flag.
   a. Enter **hal-get-property --udi <*udi*> --key storage.media_check_enabled**, replacing ***<udi>*** with the drive's udi value.
   b. For example, ***hal-get-property --udi /org/freedesktop/Hal/devices/storage_model_DVD_RW_DW_Q30A --key storage.media_check_enabled***.
   c. The response will be either ***true*** or ***false***. If ***false***, then media detection for the drive is already disabled.
3. If ***true***, the media detection service needs to be disabled:
   a. Enter **hal-set-property --udi <*udi*> --key storage.media_check_enabled --bool false**, replacing ***<udi>*** with the drive's udi value.
   b. For example, ***hal-set-property --udi /org/freedesktop/Hal/devices/storage_model_DVD_RW_DW_Q30A --key storage.media_check_enabled --bool false***.
4. Repeat step 2 to check that the response is now ***false***.
5. You must configure the server to repeat the command used in step 3 when rebooted. You can do this by adding the command to the file */etc/rc.local*.
   a. Select the whole ***hal-set-property...*** line in the terminal window and select **Edit | Copy**.
   b. Double-click on **Computer**, then **Filesystem** and then **etc**.
   c. Locate the file *rc.local*. Right-click on the file and select **Open with gedit**.
   d. Add a new line at the end of the file and select **Edit | Paste** to paste in the **hal-set-property** command used in step 3.
   e. Click **Save** and close the editor.

4.1.3 Entering the Drive in Contact Recorder for IP Office

Having identified a drive's path 56 and disabled media detection 57 on that drive, you can add the drive path to Contact Recorder for IP Office.

To enable archiving to the DVD:

1. Login to Contact Recorder for IP Office as an administrator.
2. Select **Operations**.
3. Click **Add DVD drive.**



- **Drive path(s)**
  Enter the path for the server's DVD drive. For example */dev/sr0*.

4. Click **Enter and Close**.

4.2 Disabling HTTP Access

You can disable HTTP access to Contact Recorder for IP Office.

To disable HTTP access:

1. Login to Contact Recorder for IP Office as an administrator.
2. Select **System**.
3. Click the **Edit link for Allow unencrypted (http) access?** and deselect the option.
4. Click **Enter**.

Chapter 5.
Document History

5. Document History

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

Date	Issue	Changes
		• Slight restructure to skip "step phrase" in UCM quick install description. [90605] • Minor text enhancement to clarify that security is via shell "IP Office" on the UCM. [93333]
27th May 2015	**10o**	• Minor text changes. [90606] • one-X Portal AFA login is also under referred authentication control and by default uses Administrator account password. [90604] • Clarification of Voicemail backup transfer from old to new server process and reinstatement of SSH file transfer details. [90598] • Removed errant <<< >>> markup.
2nd June 2015	**10p**	• Correction to System Settings screenshot for application server. • Correct server maintenance topic incorrectly being included in Contact Recorder output.
16th June 2015	**10q**	• Minor update to match redesign of Avaya support website.
1st July 2015	**10r**	• Correction: UCM USB ISO transfer for upgrades needs to be fully prepared USB memory key, not just plain ISO file. • "Web Manager Upgrade" status shown in SSA for upgrades via web manager menus.
7th September 2015	**10s**	• Correction to mount path name for additional disks. Full name is derived disk mount path specified plus partition number, for example ***/additional-hdd#1/partition1***. [99975] • Various minor text layout fixes.
8th September 2015	**10t**	• Various minor text layout fixes. Fixed unplanned mention of Unified Communications Module in non-UCM outputs from the common doc source.
29th September 2015	**10u**	• Republished with errant author's notes text now hidden.
30th September 2015	**10v**	• Correct of web control login from http to https.
30th October 2015	**10w**	• Warning added that voicemail restore fails if VMPro client is connected. [99893] • Note that Syslog Event Viewer filters are set when page is opened. Reload page to update.
2nd November 2015	**10x**	• Republish to resynch publishing system.
6th November 2015	**10y**	• Note that virtual servers either use NTP time or virtual server platform time. [100563]
8th December 2015	**10z**	• Correction to description of **Synchronize system clock before starting service** and **Use local time source**. • Clarifications to the password set and password change field descriptions to clarify which change IP Office and or Linux accounts.
21st December 2015	**10aa**	• Emphasis that security reset may disrupt calls and services.
19th January 2016	**10ab**	• Correction of path to download archived log files.
5th February 2016	**10ac**	• Syslog retention of monitor server records clarified.
5th April 2016	**10ad**	• Warning added regarding firewall blocking of port 8000. [106719]
17th May 2016	**10ae**	• Additional emphasis on the default Contact Recorder file path setting.
7th July 2016	**10af**	• Note that Change Password and Enable Referred Authentication options not available if logged in as local Administrator account. [109634] • Emphasis on fields that cause default security certificate regeneration (IP address and Host Name fields). • Note that Backup and Restore options (Settings | General) do not appear when web control menus accessed via platform view.
14th October 2016	**10ag**	• For call recording, incoming call routes are no longer centralized. [110388] • VRLA still not supported with Linux systems. [110378] • Non-PCI compliant notice added.
22nd November 2016	**10ah**	• Correction, voicemail licenses are for ports, not users.

Index

9

9444 13
9888 13

A

Account Code 49
Action Data 46
active during 46
ActiveX 13
Additional documentation 12
Agent Mode 46
Automatic 49
Automatic call recording 9

B

BIOS 18
Boot
  BIOS order 18
Browser 13
Bulletins 12
Button Programming
  Select 46
Button Programming tab 46
Button Programming window 46

C

call 49
  pressed during 46
call involving 46
Call Recording 9, 46
Call Route
  Incoming 49
call This 46
CallRecord 46
channels 49
Codec 13
Contact Recorder for IP Office 9
Create
  DVD 18
Create a USB device 19

D

Default
  Password 33
Default Recording 49
DSS 46
DSS key
  set 46
DSS key during 46
DVD 18

E

Explorer 13

F

Force Account Code 46
Func 46

G

G.711 13
G.726 13
G.729 13

I

Ignite 26
Incoming Call Route 49
Internet Explorer 13

L

Line Group ID 46
Linux
  Installation 24
Locale 46
Login 33

M

Manual Call Recording
  Starting 46
Manual Recording Mailbox 46
Manual Recording Options
  Setting 46
Menu key 46

P

Password
  Default 33
Playback 13
Priority 49

R

Recor 46
Record Call 46
Recording 9
Recording Library 46
Recording Library options 46
Recording Warning 46
Related documents 12
Role 26
Root password
  Set 26

S

Series 46
Server
  Ignite 26
  Role 26
  Type 26
Set
  Root password 26
Shortcode 46
SoftConsole 46
Software
  Unetbootin 17, 19
  USB 17, 19
Start Recording 46
Stop Recording 46
syslinux.cfg 19

T

Technical bulletins 12
Transfer 49
Type 26

U

USB
  Create a bootable... 19
  Software 17, 19
user presses 46
Using DSS Keys 46
Using Short Codes 46

V

Voice Recording
  Select 46
Voice Recording Library 46
VRL 46
VRL application 46

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

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

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

© 2016 Avaya Inc. All rights reserved.