Administering Avaya IP Office™ Platform Media Manager

Release 11.1.1
Issue 9
February 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if 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.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) 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 type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

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

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order, Documentation, or as authorized by Avaya in writing with a default of one (1) Cluster if not stated.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order, Documentation, or as authorized by Avaya in writing.

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

Shrinkwrap License (SR). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Transaction License (TR). End User may use the Software up to the number of Transactions as specified during a specified time period and as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Transaction” means the unit by which Avaya, at its sole discretion, bases the pricing of its licensing and can be, without limitation, measured by the usage, access, interaction (between client/server or customer/organization), or operation of the Software within a specified time period (e.g. per hour, per day, per month). Some examples of Transactions include but are not limited to each greeting played/message waiting enabled, each personalized promotion (in any channel), each callback operation, each live agent or web chat session, each call routed or redirected (in any channel). End User may not exceed the number of Transactions without Avaya’s prior consent and payment of an additional fee.

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 is the software contained within the list of Heritage Nortel Products located at https://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 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

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

Third Party Components

“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 products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, 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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or 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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya 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.

Contents

Part 1: Introduction

Chapter 1: IP Office Media Manager

IP Office Media Manager provides a facility to store and replay audio call recordings generated by Voicemail Pro. It stores recordings on a local drive. Recordings can also be archived to additional locations (DVD, Network-Attached Storage (NAS) or Google drive).

Media Manager archives and catalogs these recordings for administrators and users to search, play, and download when required. Recordings are available to system administrators through Web Manager. For users access can be configured through their web self-administration interface.

Media Manager is only supported running on the same server as Voicemail Pro.

- For a network based around a primary server, Media Manager is supported on the primary server and works with the Voicemail Pro on that server. It is not supported on the secondary server or any other server in the network.
- For a standalone IP500 V2 system or SCN of IP500 V2 systems, it is supported on the same IP Office Application server which is providing the central voicemail service for the network. It is not supported on a UCM module.

Contact Recorder

Contact Recorder is a previous application for archiving call recording. It has now been replaced by Media Manager. Customers upgrading systems with Contact Recorder must migrate their call recording database to Media Manager in order to be able to search and replay their existing call recordings through the Media Manager interface. See Migrating Contact Recorder on page 56. The existing recordings do not need to be moved.

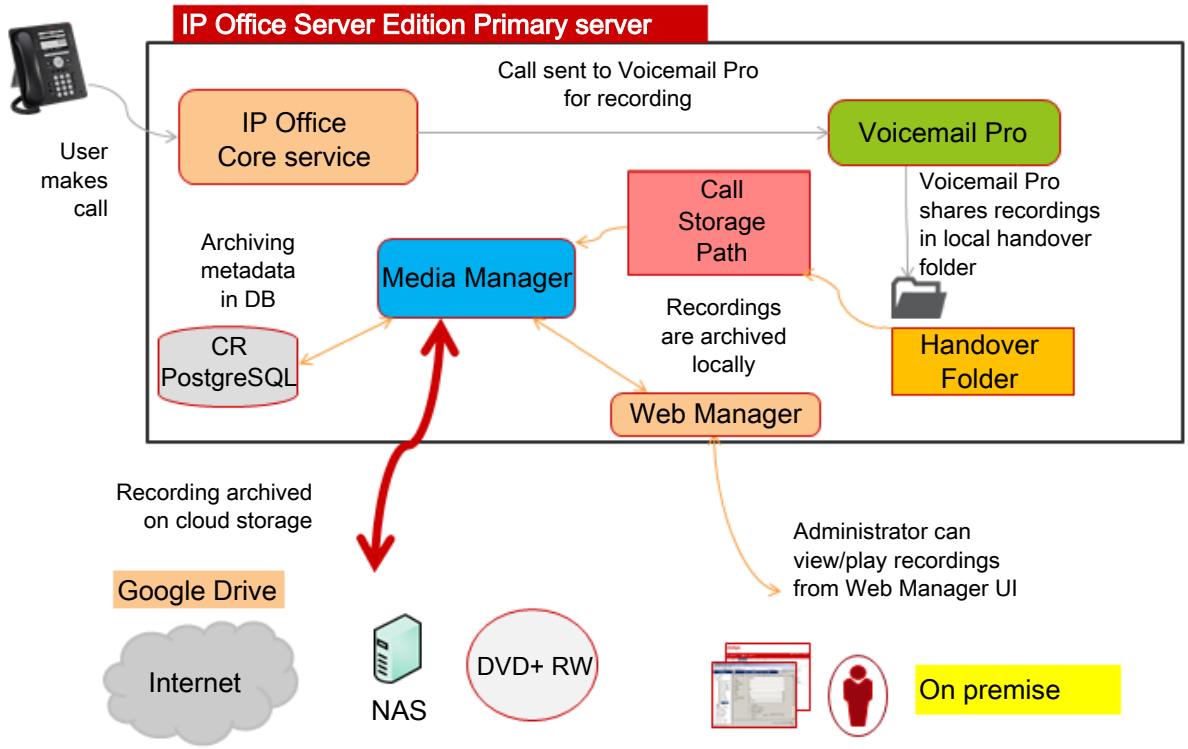
Related links

Media Manager Architecture on page 8
Resiliency on page 10
Administrator Access to Media Manager on page 10
Supported languages on page 10
Backup and restore on page 11

Media Manager Architecture

Media Manager archives and catalogs these recordings for administrators and users to search, play, and download when required. Recordings are available to system administrators through Web Manager. For users access can be configured through their Web Self-Admin interface.

The diagram below shows of simplified summary of the architecture of Media Manager operation.



1. The IP Office system requests that Voicemail Pro records the call.
   - The recording can be triggered automatically for specific users, groups, incoming call routes or account codes.
   - Recording can also be triggered by a voicemail callflow.
   - The recording can also be triggered manually by a user.
   - The call recording configuration settings indicate the destination for recordings. That is either a normal voicemail mailbox or Media Manager (using the setting **Voice Recording Library**).
2. The call is recorded by the voicemail service. For recordings where the destination is set as Media Manager, the recording is placed into a handover folder.
3. The Media Manager service constantly checks the handover folder:
   - Whenever a new recording is available, it copies the recording to its call storage folder.
   - Details of the call and call parties are added to the Media Manager database.
4. If Media Manager has been configured with an external connector, copies of new recordings are also regularly archived to the external location (DVD, NAS or Google Drive).

Related links

IP Office Media Manager on page 8

Resiliency

If the Server Edition Primary is unavailable, the archiving service and interfaces provided by Media Manager will also be unavailable. Archiving resumes when the Primary Server comes back into service. However, because Voicemail Pro is resilient, when the Primary Server is nonfunctional, the Secondary Server continues to record calls. These call recordings must be transferred to the primary server after it is functional. For transferring the recordings, you must configure the SFTP connection in the Voicemail Recording tab in Voicemail Pro System Preferences. For more information, see Voicemail Recording in *Administering Avaya IP Office™ Platform Voicemail Pro*.

Related links

IP Office Media Manager on page 8

Administrator Access to Media Manager

About this task

By default, the administrator account for IP Office systems is able to access the Media Manager settings using the IP Office Web Manager menu using the process below.

However, permission to access Media Manager and the level of access can be configured for any IP Office service user. See Managing access on page 20.

Procedure

1. Log on to the Web Manager interface.
2. Click **Applications** > **Media Manager**.

Related links

IP Office Media Manager on page 8

Supported languages

The IP Office Media Manager user interface and documents are available in the following languages:

- US English
- Dutch
- Italian
- German
- Russian
- French

- Latin Spanish
- Brazilian Portuguese
- Simplified Chinese

Related links

IP Office Media Manager on page 8

Backup and restore

The IP Office web management menus include functions to backup and restore settings (for full details refer to the *Deploying IP Office Server Edition* manual). Those backup and restore facilities apply to Media Manager as follows:

- **Media Manager Configuration:** The configuration settings of the Media Manager application are included in the backup and restore processes when Media Manager is selected as a component of the operation.
- **Call Recordings Database:** The database of call recordings and their locations is included in the backup and restore processes when Media Manager is selected as a component of the operation.
- **Call Recordings:** The call recordings stored on the additional hard disk and archived onto any external connector are not included in the backup and restore processes.

Related links

IP Office Media Manager on page 8

Chapter 2: Media Manager Setup

Media Manager is only supported when an additional hard disk for storage of the recordings. Storage on the same disk as being used for the Voicemail Pro and other IP Office applications is not supported.

This documentation cannot cover the installation of the addition drive (or pair of drives if RAID is being used). Refer to the documentation for the specific server platform being used.

Related links

Licensing on page 12
Activating the additional hard disk on page 14
Starting the Media Manager service on page 15
Configuring Media Manager on page 15
Configuring the IP500 V2 System Address on page 18

Licensing

On subscription systems, no additional subscription or license is required.

On systems that use PLDS licensing, Media Manager requires a `VMPro Media Manager` license to operate. Upgraded systems with an existing `Voice Recordings Administrator` license (used for Contact Recorder) can continue to use that license.

- **Trial Period:** On systems without a license, Media Manager operates for a 90-day trial period. This time period starts when you start the Media Manager service in the system. After the trial period ends, IP Office Media Manager stops further recordings but keeps the recordings made during the trial period. A warning to this effect is displayed on the Web Manager screen. You can add a license any time during the trial period or after its expiry.

Applying licenses

For information about applying licenses, see the Applying licenses topic in *Administering Avaya IP Office™ Platform with Web Manager* or *Administering Avaya IP Office™ Platform with Manager*.

Related links

Media Manager Setup on page 12
Verifying Media Manager license on Web Manager on page 13
Verifying licenses on Voicemail Pro on page 13

Verifying Media Manager license on Web Manager

About this task

For systems using PLDS licensing, the presence of the appropriate licence can be checked in the IP Office system configuration.

Procedure

1. Log on to the Web Manager interface.
2. Click **System Settings** > **Licenses**.
3. Verify that the Media Manager license is listed as `VMPro Media Manager`.

   If your system is using WebLM licensing and the system does not display the license on the License screen, you can reserve a Media Manager license. To reserve a license, select the Remote server tab, set Media Manager to 1, and click **Update**.

Related links

Licensing on page 12

Verifying licenses on Voicemail Pro

About this task

If required, the presence of the appropriate licence or subscription for Media Manager support can also be checked using the Voicemail Pro client. This validates that the voicemail service will place recordings in the correct location for collection by Media Manager when required.

Procedure

1. Log on to the Web Manager interface.
2. Click **Applications** > **Voicemail Pro (Call Flow Management)**.
3. On the Voicemail Pro client, click **Help** > **About**.
4. Verify that Media Manager is listed as a licensed software. The license name is VRL (Media Manager).

Related links

Licensing on page 12

Activating the additional hard disk

About this task

Media Manager is only supported when using an additional hard disk for storage of the recordings. Storage on the same disk as being used for the Voicemail Pro and other IP Office applications is not supported. Whilst recording file storage uses the additional hard disk, the call recordings database is stored on the same hard disk as the Media Manager application.

For a new server with an addition hard disk (or pair of disks configured as a RAID pair), configuration and formatting of the addition drive is done as part of the new server's ignition process. Refer to the documentation for new server deployment. However, for an existing server to which an additional disk has been added post-ignition, use this procedure to activate the additional hard disk.

Procedure

1. On a client computer, browse to `https://<IP address of the server>:7071` in the browser.
2. Enter the **User Name** and **Password** for the administrator account and click **Login**.
3. Select **Settings** > **System**.
4. Scroll down to the **Additional Hard Drive Information** settings.
5. Select the **Activate** check box.
6. In the **Mount Point Path** enter a mount path for the additional drive.
   - The default recommended value is `/additional-hdd#1`. When you add a hard drive using that path, a partition with the path `/additional-hdd#1/partition1` is automatically created for Media Manager.
   - The path is used by setting it as the Media Manager application's **Call Storage Path** (**Applications** > **Media Manager** > **Configuration**).
7. If the disk is new, that is it does not contain any existing call recordings, then under **Format Hard Drive** select **Enable**.

   ⚠ Warning:

   - Do not format an existing drive that contains any call recordings. Doing so will erase all the existing call recordings without any option to recover those recordings.
8. Click **Save**.

Next steps

- Having added an additional hard drive, check that the Media Manager service is running. See Starting the Media Manager service on page 15.

Related links

Media Manager Setup on page 12

Starting the Media Manager service

About this task

Use this procedure to check that the Media Manager service has been started.

Procedure

1. On a client computer, browse to `https://<IP address of the server>:7071` in the browser.
2. Enter the **User Name** and **Password** for the administrator account and click **Login**.
3. Click **Show Optional Services**.
4. Check that the check box next to **Media Manager** is selected. This instructs the service to restart the service each time it is restarted.
5. Click the **Start** button next to **Media Manager**.
6. Wait until the button shows Stop, indicating that the Media Manager service to has started.

Next steps

- Having started the service, it can now be configured to collect and store recordings. See Configuring Media Manager on page 15.

Related links

Media Manager Setup on page 12

Configuring Media Manager

About this task

At minimum, Media Manager needs to be configured with the location from which is should collect call recordings made by the voicemail service and the location where it should then store those recordings. This is done through the web manager menus of the server hosting Media Manager.

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. In the **Handover Folder** field, check that the path is set to `/opt/vmpro/MM/VRL`. This is the path to which the voicemail service saves recordings it has been instructed to make available to Media Manager.
4. In the **Call Storage Path** field, enter the path `/additional-hdd#1/partition1`. This should match the path and partition set for the additional hard drive where Media Manager should store call recordings.
5. Edit any other Media Manager settings as required by the customer.

6. Click **Update**.

Next steps

- Having configured the service, on systems where it is running on an IP Office Application Server supporting voice for an IP500 V2 system, the address of the IP500 V2 system needs to be added. See Configuring the IP500 V2 System Address on page 18.

Related links

Media Manager Setup on page 12
Media Manager Configuration Settings on page 16

Applications > **Media Manager** > **Configuration**

Media Manager Configuration Settings

Applications > **Media Manager** > **Configuration**

Name	Description
Profile	Default = Blank The unique name that identifies a configuration profile.
Log Level	Default = INFO The type of log level. The options are: • INFO • DEBUG • ERROR
Handover Folder	Default = `/opt/vmpro/MM/VRL` The Voicemail Pro path from where IP Office Media Manager picks up the recordings. Voicemail Pro writes call recording files to this folder.
Call Storage Path	Default = Blank. The path to the additional hard drive partition that Media Manager should use to store the recordings after collecting them from the directory specified in the **Handover Folder**. If the additional drive was added using the path `/additional-hdd#1`, enter `/additional-hdd#1/partition1`. The additional drive path used can be seen using the Platform View menus of the server If you must change the value after you have already started recording, copy all the sub-directories and files in the old directory to the new directory before you resume recording.

Table continues…

Name	Description
Days to Retain Calls	Default = 180 days The number of days for which the database retains the call details. After the said period, the IP Office Media Manager deletes the call recordings. To disable the deletion of call recordings, enter **0** in this field. **Note:** • Media Manager deletes the call recordings as soon as the allocated storage is full.
Audit Retain Period (Days)	Default = 180 days The number of days for which the Audit Trail or recordings are retained in IP Office Media Manager. The minimum value for this field is 1 day and the maximum 365 days.
Active Connector	The connector that is currently being used for remote archiving. The drop-down menu lists all the available connectors where you can archive your recordings. Changing the connector results in a change in the archive destination. However, the recordings from the pervious archives are still available for the users.
Send Email	Default = No The option to select whether the system must send emails for alarms and events.
SMTP Mail Server	Default = Blank The SMTP mail server that IP Office Media Manager uses to send email messages about alarms and events. If you leave this field blank, system cannot send email messages for alarms and events.
SMTP Port	Default = Blank The SMTP port to which the service sends email messages.
Secured Connection	Default = No The option to indicate whether the connection is secured. A secured connection uses Transport Layer Security (TLS) protocol to communicate. The options are: • Yes • No
SMTP User Name	Default = Blank The user name for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the user name here.
SMTP Password	Default = Blank The password for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the password here.

Table continues…

Name	Description
SMTP Mail “From” Address	The address from which the SMTP emails containing the alarms and events originate.
Send Alarm/Event Emails To	The email addresses to which alarms and events must be sent. You can add more than one email address by adding a semi colon (;) between two email addresses.

Related links

Configuring Media Manager on page 15

Configuring the IP500 V2 System Address

About this task

Media Manager is supported with an IP500 V2 system (or network of such systems) by installing an IP Office Application Server to run both Voicemail Pro and Media Manager.

In order for user to be able to access recordings through self-administration, the address of the IP500 V2 connected to the voicemail server needs to be entered into the application server’s configuration using the process below.

Procedure

1. Log on to the **Web Manager** interface of the Linux Application server.
2. Click **Preferences**.
3. In the **IP Office IP Address** field, type the IP address of the IP500 V2 server.
4. Click **Update**.

Related links

Media Manager Setup on page 12

Part 2: Configuration

Chapter 3: Configuring Media Manager Access

Recordings can be access at 2 different levels:

- **System Administrators** – Administrators can access and manage all recordings. They do so through the IP Office Web Manager application.
  - Administrators can be given access to all recordings and to Media Manager configuration settings or to recordings only.
- **Extension Users** – Individual system users can be configured for access to recordings through their self-administration menus. The configuration includes settings what recordings the user can access and the range of functions they can perform on those recordings.

Related links

[Providing administrative access to Media Manager](#) on page 20
[Configuring user access through self-administration](#) on page 21

Providing administrative access to Media Manager

About this task

Use this procedure to control administrator access to Media Manager. There are two levels of access that can be applied; access to recordings only or access to recordings and all application settings.

The setting is applied via the settings of the security **Rights Group** to which the administrator belongs.

Note that the settings can include permissions to access other settings and services. This section covers only the minimum necessary for Media Manager access. For full details refer to the help with the IP Office Manager application.

Procedure

1. Start IP Office Manager.
2. Select **File** > **Advanced** > **Security Settings**.
3. From the list of systems displayed, select the system hosting the Media Manager service.
4. Select the **Rights Group** that you want to alter.

5. For Media Manager access, ensure the rights group has the following minimum rights:
   a. On the **Web Services** tab, select **Config Read All**.
   b. On the **External** tab, select either **Media Manager Administrator** or **Media Manager Standard**.
      - **Media Manager Standard** – This option allows members of the rights group to only access **Recordings** menu to search, play and download recordings. They can view the other Media Manager menus but cannot use the controls on those other menus.
      - **Media Manager Administrator** – This option allows members of the rights group to access all Media Manager menus and settings.
6. Click **OK**.
7. Click  .

Related links

Configuring Media Manager Access on page 20

Configuring user access through self-administration

About this task

Administrators can provide end users access to Media Manager recordings. Users can then view, listen, and download recordings using the Web Self-Administration menus.

Procedure

1. Log on to the Web Manager interface.
2. Click **Call Management** > **Users**.
3. Click the  icon next to the user to whom you want to provide Media Manager access.
4. In the navigation pane, click **Web Self-Administration**.
5. Click **Enable Web Self-Administration** if not enabled already.
6. Click **Enable Media Manager Replay**.
7. Click one of the following:
   - **Replay All Recordings** – This option allows the user to access all call recordings.
   - **Replay Own Recordings** – This option allows the user to access their own call recordings plus any specified using the following settings:
     - **Replay Recordings For Group** – Add those groups for which the user can access group recordings. The user does not need to be a member of the group.
     - **Replay Recordings For Others** – Enter a list of line numbers, account numbers and user extension numbers, separated by semi-colons. The list can be up to 128 characters long.

8. Click **Download Recordings** if you want the user to be able to download copies of recordings.

   Warning:

   - Downloaded recordings are outside the control of the Media Manager application's control and audit trail. Therefore, only allow recordings to be downloaded if assured that their usage will continue to comply with appropriate data protection and privacy requirements.

9. Click **Update**.

Next steps

- IP Office Server Edition users can access self–administration and recordings using the address: `https://<Server Edition>:7070/WebManagement/index.html`.
- IP500 V2 users need to access self-administration and recordings using two separate addresses:
  - Access general self–administration using the address: `https://<IP500_V2>:8443/WebMgmtEE/index.html`.
  - Access recordings self–administration using the address: `https://<Application_Server>:7070/WebManagement/index.html`.

Related links

Configuring Media Manager Access on page 20

Chapter 4: Managing Call Recording

Whilst Media Manager stores call recordings and manages their searching and playback, the actual recording of calls is performed by the Voicemail Pro service. Configuration of call recording is done through the Voicemail Pro client and the IP Office system configuration settings.

Related links

Switching the call recording warning on/off on page 23
Setting the maximum call recording length on page 24
Configuring the recording display on page 24
Configuring a user's manual call recording destination on page 25
Configuring automatic call recording for a user on page 26
Configuring auto recording for a hunt group on page 27
Configuring automatic call recording for an incoming call route on page 28
Configuring auto recording for account code on page 30

Switching the call recording warning on/off

In many countries, it is requirement to warn those involved in a call that they are being recorded. One method for doing this is to enable the `Advice of Call Recording (AOCR)` message provided by the Voicemail Pro server.

- The **Play Advice on Call Recording** option is enabled by default.
- When the call is using analogue trunks, on outgoing calls it can not be guaranteed that a caller hears an 'advice of recording' announcement. Analogue trunks do not support call status signalling, so the announcement is played as soon as the trunk is seized even if the call is ringing and has not been answered.

About this task

Use this procedure to enable advice of call recording.

Procedure

1. From the Voicemail Pro client, select **Administration** > **Preferences** > **General**.
2. Click **Play Advice on Call Recording** check box.
3. Click **OK**.

4. Click **Save & Make Live**.

Related links

Managing Call Recording on page 23

Setting the maximum call recording length

About this task

You can specify the maximum length of call recordings made by Voicemail Pro. The maximum limit is 5 hours.

Procedure

1. In the Voicemail Pro client, click **Administration** > **Preferences** > **General**.
2. In **Max. VRL Record Length (secs)**, type the time in seconds. The maximum value is 18000 seconds.
3. Click **OK**.
4. Click **Save & Make Live**.

Related links

Managing Call Recording on page 23

Configuring the recording display

About this task

Some Avaya terminals display **REC** when a call is being recorded. Use this procedure to hide this indication on supported phones.

Procedure

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. Select the **Hide auto recording** check box.
5. Save the configuration.

Related links

Managing Call Recording on page 23

Configuring a user's manual call recording destination

About this task

Users can manually trigger the recording of call using a variety of methods. Through the system configuration you can configure for each user, where manually recorded calls should be stored. The default otherwise is to place the recordings in the users own voicemail mailbox.

Procedure

1. Start IP Office Manager and load the system configuration.
2. On the navigation pane, click a **User**.
3. Click the **Voice Recording** tab.
4. In the **Destination** field, select the destination for the recordings.
   - For Media Manager, set the destination to either **Voice Recording Library** or **Voice Recording Library Authenticated**.
5. Click **OK**.
6. Save the configuration.

Related links

Managing Call Recording on page 23
Manual recording configuration settings on page 25

Manual recording configuration settings

Name	Description
Destination	The destination of the call recording. The options are: • **Mailbox**: Store the recordings in the voicemail mailbox selected. These recordings are accessed and managed through the normal mailbox controls and are not stored, viewed and managed through Media Manager. • **Voice Recording Library**: Transfer the recordings to Media Manager. The recordings are stored in OPUS file format and require approximately 100KB per minute. • **Voice Recording Library Authenticated**: This is a legacy setting. It operates the same as **Voice Recording Library**.

Related links

Configuring a user's manual call recording destination on page 25

Configuring automatic call recording for a user

About this task

For each user, you can configure automatic recording of their calls and the destination for those automatic recordings.

Procedure

1. Start IP Office Manager and load the system configuration.
2. On the navigation pane, click a **User**.
3. Click the **Voice Recording** tab.
4. For **Inbound** and **Outbound** calls, select the frequency of automatic call recording and the type (**External** and/or **Internal**) of calls recorded.
5. Use the **Time Profile** field to select a time profile that defines when the calls should be recorded. Otherwise, calls are recorded 24/7.
6. In the **Destination** field, select the destination for the recordings.
   - For Media Manager, set the destination to either **Voice Recording Library** or **Voice Recording Library Authenticated**.
7. Click **OK**.
8. Save the configuration.

Related links

Managing Call Recording on page 23
User automatic call recording settings on page 26

User automatic call recording settings

Name	Description
Inbound	This field sets the frequency of call recording: • **None**: Do not record. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls. If recording is not possible, returns busy tone to the caller. • **xx%**: Record calls, if a recording channel is available, at intervals matching the set percentage. For example, for 25%, record at least 1 call in every 4.
Outbound	
Auto Record Calls	This fields set the type of calls recorded. These can be **Internal**, **External** or **External & Internal**.

Table continues…

Name	Description
Destination	The destination of the call recording. The options are: • **Mailbox**: Store the recordings in the voicemail mailbox selected. These recordings are accessed and managed through the normal mailbox controls and are not stored, viewed and managed through Media Manager. • **Voice Recording Library**: Transfer the recordings to Media Manager. The recordings are stored in OPUS file format and require approximately 100KB per minute. • **Voice Recording Library Authenticated**: This is a legacy setting. It operates the same as **Voice Recording Library**.
Time Profile	You can use a time profile to specify when the automatic call recording settings are applied. If no time profile is selected, automatic call recording is applied all the time.

Related links

Configuring automatic call recording for a user on page 26

Configuring auto recording for a hunt group

About this task

You can configure automatic call recording for calls to a hunt group.

Procedure

1. Start IP Office Manager and load the system configuration.
2. On the navigation pane, select the hunt group.
3. Click the **Voice Recording** tab.
4. In the **Record Inbound** field, click the frequency of recording. For inbound calls, recording stops if the call goes to voicemail to leave a message.
5. Use the **Time Profile** field to select a time profile that defines when the calls should be recorded. Otherwise, calls are recorded 24/7.
6. In the **Recording (Auto)** field, click the destination for automatic call recordings.
   - For Media Manager, set the destination to either **Voice Recording Library** or **Voice Recording Library Authenticated**.
7. In the **Auto Record Calls** field, select the type of calls (**Internal** and/or **External**) to record.
8. Click **OK**.
9. Save the configuration.

Related links

Managing Call Recording on page 23
Hunt group call recording settings on page 28

Hunt group call recording settings

Name	Description
Record Inbound	This field sets the frequency of call recording: • **None**: Do not record. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls. If recording is not possible, returns busy tone to the caller. • **xx%**: Record calls, if a recording channel is available, at intervals matching the set percentage. For example, for 25%, record at least 1 call in every 4.
Record Time Profile	You can use a time profile to specify when the automatic call recording settings are applied. If no time profile is selected, automatic call recording is applied all the time.
Recording (Auto)	The destination of the call recording. The options are: • **Mailbox**: Store the recordings in the voicemail mailbox selected. These recordings are accessed and managed through the normal mailbox controls and are not stored, viewed and managed through Media Manager. • **Voice Recording Library**: Transfer the recordings to Media Manager. The recordings are stored in OPUS file format and require approximately 100KB per minute. • **Voice Recording Library Authenticated**: This is a legacy setting. It operates the same as **Voice Recording Library**.
Auto Record Calls	This fields set the type of calls recorded. These can be **Internal**, **External** or **External & Internal**.

Related links

Configuring auto recording for a hunt group on page 27

Configuring automatic call recording for an incoming call route

About this task

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

Procedure

1. Start IP Office Manager and load the system configuration.
2. On the navigation pane, click **Incoming Call Route**.
3. Click the **Voice Recording** tab.
4. In the **Record Inbound** field, click the frequency of recording. For inbound calls, recording stops if the call goes to voicemail to leave a message.
5. Use the **Time Profile** field to select a time profile that defines when the calls should be recorded. Otherwise, calls are recorded 24/7.
6. In the **Recording (Auto)** field, click the destination for automatic call recordings.
   - For Media Manager, set the destination to either **Voice Recording Library** or **Voice Recording Library Authenticated**.
7. Click **OK**.
8. Save the configuration.

Related links

Managing Call Recording on page 23
Incoming Call Route call recording settings on page 29

Incoming Call Route call recording settings

Name	Description
Record Inbound	This field sets the frequency of call recording: • **None**: Do not record. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls. If recording is not possible, returns busy tone to the caller. • **xx%**: Record calls, if a recording channel is available, at intervals matching the set percentage. For example, for 25%, record at least 1 call in every 4.
Record Time Profile	You can use a time profile to specify when the automatic call recording settings are applied. If no time profile is selected, automatic call recording is applied all the time.

Table continues…

Name	Description
Recording Auto	The destination of the call recording. The options are: • **Mailbox**: Store the recordings in the voicemail mailbox selected. These recordings are accessed and managed through the normal mailbox controls and are not stored, viewed and managed through Media Manager. • **Voice Recording Library**: Transfer the recordings to Media Manager. The recordings are stored in OPUS file format and require approximately 100KB per minute. • **Voice Recording Library Authenticated**: This is a legacy setting. It operates the same as **Voice Recording Library**.

Related links

Configuring automatic call recording for an incoming call route on page 28

Configuring auto recording for account code

About this task

You can automatically record outgoing external calls that use a particular account code.

Procedure

1. Start IP Office Manager and load the system configuration.
2. On the navigation pane, click **Account Code**.
3. Click the **Voice Recording** tab.
4. In the **Record Outbound** field, click the frequency of recording.
5. Use the **Time Profile** field to select a time profile that defines when the calls should be recorded. Otherwise, calls are recorded 24/7.
6. In the **Recording (Auto)** field, click the destination for automatic call recordings.
   - For Media Manager, set the destination to either **Voice Recording Library** or **Voice Recording Library Authenticated**.
7. Click **OK**.
8. Save the configuration.

Related links

Managing Call Recording on page 23
Account code call recording settings on page 31

Account code call recording settings

Name	Description
Record Outbound	This field sets the frequency of call recording: • **None**: Do not record. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls. If recording is not possible, returns busy tone to the caller. • **xx%**: Record calls, if a recording channel is available, at intervals matching the set percentage. For example, for 25%, record at least 1 call in every 4.
Record Time Profile	You can use a time profile to specify when the automatic call recording settings are applied. If no time profile is selected, automatic call recording is applied all the time.
Recording (Auto)	The destination of the call recording. The options are: • **Mailbox**: Store the recordings in the voicemail mailbox selected. These recordings are accessed and managed through the normal mailbox controls and are not stored, viewed and managed through Media Manager. • **Voice Recording Library**: Transfer the recordings to Media Manager. The recordings are stored in OPUS file format and require approximately 100KB per minute. • **Voice Recording Library Authenticated**: This is a legacy setting. It operates the same as **Voice Recording Library**.

Related links

Configuring auto recording for account code on page 30

Part 3: Connectors and Archiving

Chapter 5: Managing Connectors for Recording Archiving

In addition to storing call recordings on an additional hard disk, Media Manager can also archive the recordings to an external store. This is done using connectors.

Related links

Adding a Connector on page 33
Modifying the details of a Connector on page 34
Deleting an existing Connector on page 35

Adding a Connector

About this task

IP Office Media Manager provides the option to remotely archive your call recordings.

Before you begin

Ensure you have configuration access to Web Manager.

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. Click **Add** and select one of the options as required:
   - **DVD Drive:** See Archiving to DVD on page 36.
   - **Google Drive:** See Archiving to Google Drive on page 40.
   - **Network-Attached Storage (NAS):** See Archiving to an External NAS on page 38.

Related links

Managing Connectors for Recording Archiving on page 33
Connector on page 34

Applications > **Media Manager** > **Connector**

Connector

Applications > **Media Manager** > **Connector**

Name	Description
Add	The drop-down menu to select a connector. The options are: • NAS • Google drive • DVD
Name	The name of the connector.
Type	The type of connector selected.
Active	The state of the connector.
Reachable	The field that indicates whether the connector is reachable.
Pending Files #	The files that are yet to be archived.
Lasts Successful Archive Time	The time when the last successful archive was done using the selected connector.

Related links

Adding a Connector on page 33

Modifying the details of a Connector

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. Click the icon corresponding to the connector you want to modify.
4. Update the details of the connector as required.
5. (Optional) Click **Test Connection** to verify the connection with the updated details and credentials.
6. Click **Update**.

Related links

Managing Connectors for Recording Archiving on page 33

Deleting an existing Connector

About this task

Use this procedure to delete an existing connector.

Warning:

Once any recording has been archived through a connector, you cannot delete that connector.

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. Click the icon corresponding to the connector you want to delete.
4. Click **Yes** on the confirmation dialog box.

Related links

Managing Connectors for Recording Archiving on page 33

Chapter 6: Archiving to DVD

IP Office Media Manager provides the option to archive audio call recordings generated by Voicemail Pro on a DVD drive. Media Manager makes the archived recordings available to the users through Web Manager and Web Self-Admin interface when required. Each DVD runs out of space after sometime so you must monitor the storage capacity and keep a blank DVD+RW available. Insert the blank DVD+RW after the filled up DVD is ejected. The recordings that are available during the change of DVD are archived after you insert a new DVD.

Related links

Configuring DVD archiving on page 36

Configuring DVD archiving

Before you begin

Ensure you have the DVD name, path, and DVD label handy.

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. Click **Add**.
4. Select **DVD**.
5. In the Add DVD Connector window:
   - In the **Name** field, type a name.
   - In the **Path** field, enter the file path for the DVD drives, for example, `/dev/sr0`.
   - In the **DVD Label** field, type the DVD label.
   -
6. If you want the archived recording to be copied in encrypted format, change the **Encrypt Recording** setting to **Yes**. Note that this setting cannot be reset back to **No** once changed.
7. Click **Create**. The system displays the connector in the list of connectors.
8. To start using the connector for archiving, on the Configuration screen, select the connector from the **Active Connector** field.

9. Click **Update**.

Related links

Archiving to DVD on page 36

Chapter 7: Archiving to an External NAS

IP Office Media Manager can archive call recordings to a Network-Attached Storage (NAS). The archived recordings on NAS are then made available to the users through Media Manager and web admin interface.

- Media Manager support NAS archiving of recordings at the maximum recording call rate.
- Media Manager runs a scheduling task to archive any new recordings every 5 minutes.

Tested example scenarios include:

- 18000 recordings of 5MB each takes approximately 1 hour to archive to an external NAS drive.
- 3000 recordings of 15MB each takes approximately 8 minutes to archive to an external NAS drive.

Note:

When you configure NAS or any connector for the archival process, and when the Media Manager file is processed from source to the destination, along with new recordings it also archives the old recording file into the configured NAS or connector driver.

If a recording file is deleted in the call storage path due to **Days to Retain Calls** or space limit, the media manager checks the recording file in the NAS or connector archival. If you cannot play the recording in NAS, then please contact your administrator.

Related links

Configuring NAS archiving on page 38

Configuring NAS archiving

Before you begin

Ensure you have the path, and user credentials of the file share created on the NAS..

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. Click **Add**.
4. Select **NAS**.

5. On the Add NAS Connector window:
    a. Enter a **Name** for the NAS connector.
    b. Enter the **Path** for the NAS connector. This is the path of the file share. The path must be in the format `IP address/SharePath`. For example: `148.147.54.1/Remote archive`.
    c. In the **User Name For Fileshare** field, enter the user name to access file share.
    d. In the **Password For Fileshare** field, enter the password for the user name to access file share.
    e. If you want the archived recording to be copied in encrypted format, change the **Encrypt Recording** setting to **Yes**. Note that this setting cannot be reset back to **No** once changed.
6. (Optional) Click **Test Connection** to test the connectivity to file share server using the credentials provided.
7. Click **Create**. The system displays the connector in the list of connectors.
8. To start using the connector for archiving, on the Configuration screen, select the connector from the **Active Connector** field.
9. Click **Update**.

Related links

Archiving to an External NAS on page 38

Chapter 8: Archiving to Google Drive

IP Office Media Manager can archive call recordings on a Google drive. The archived recordings on the Google drive are then made available to the users through Media Manager and Web Self-Admin interface. You must create a Google drive for Media Manager and configure the drive as a connector before you start archiving.

Related links

Creating a Google drive for Media Manager on page 40
Configuring Google drive archiving on page 41

Creating a Google drive for Media Manager

About this task

This section provides the high-level steps to create a Google drive for use by Media Manager.

Procedure

1. Navigate to https://console.developers.google.com/.
2. Create a project.
3. Click **Drive API** to enable the API.
4. Click **Credentials** > **Create Credentials** > **OAuth Client ID**.
5. On the Configure Consent screen, type the **Product Name**.
6. In the **Select Application Type** field, select **Web Application**.
7. In the **Authorized Redirect URIs** field, enter `https://<FQDN>:49001/Callback`.

   You must provide the FQDN and not an IP address.
8. Click **Create**.
9. Download and save the JSON file.

Next steps

Using the downloaded JSON file, create a connector to the Google drive. See Configuring Google drive archiving on page 41.

Related links

Archiving to Google Drive on page 40

Configuring Google drive archiving

Before you begin

Create a Google project and download the JSON file. See Creating a Google drive for Media Manager on page 40.

Procedure

1. Login to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Configuration**.
3. Click **Add**.
4. Select **Google**.
5. On the Add Google Connector window, in the **Name** field, type the name of the connector.
6. If you want the archived recording to be copied in encrypted format, change the **Encrypt Recording** setting to **Yes**. Note that this setting cannot be reset back to **No** once changed.
7. Click **Browse** and select the `JSON` file that you downloaded after creating your Google drive.
8. Click **Upload**.
9. Click **Create**. The system displays the connector in the list of connectors.
10. To start using the connector for archiving, on the Configuration screen, select the connector from the **Active Connector** field.
11. Click **Update**.

Related links

Archiving to Google Drive on page 40

Part 4: Recordings and Alarms

Chapter 9: Administering Recordings

The following processes can be performed by administrators who have access to Media Manager (see Configuring Media Manager Access on page 20).

Related links

Accessing the recordings

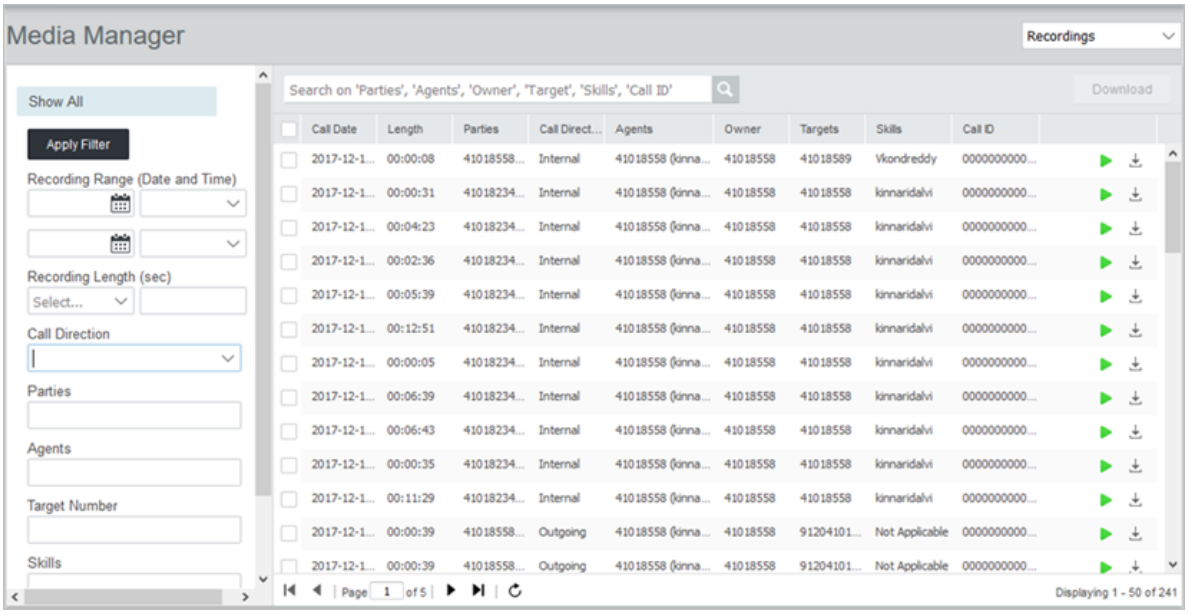
About this task

IP Office Media Manager catalogs the recordings and makes them available for administrators to view, play, and download. Administrators can use the **Web Manager** interface to access these recordings.

The audio files are stored in Opus file format, which is an audio format developed primarily for Internet streaming. The files can be played using Firefox, Microsoft Edge, and Google Chrome. The Opus files can also be played using Safari browser on iOS 11 and macOS High Sierra. The downloaded audio files can be played using VLC media player and Windows media player. However, Opus plug-in must be added to Windows media player to play Opus files.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. The system displays all the call recordings. See Recordings Details on page 44 for details.



Related links

Administering Recordings on page 43

Recordings Details

When displaying recordings, the following call details are displayed for each recording.

Name	Description
Checkbox	The checkbox can be used to select multiple recordings followed by clicking **Delete**or **Download**to delete or download all selected recordings.
Call Date	The date of the call.
Length	The duration of the recording.
Parties	The users that participated in a conference call.
Call Direction	The field indicates whether the call was Internal, Incoming, or Outgoing.
Agents	The agents involved in the call.
Owner	The owner of the recording. The owner is the extension or configuration item that triggered the recording of the call. • User extension • Hunt group extension • Line number • Account code
Targets	The phone numbers of the recipients of the call.

Table continues…

Name	Description
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.
	This icon is shown if the recording includes VRLA authentication information. Click the icon to display a status message. See Verifying authentication of call recordings on page 48.
	Play the individual recording.
	Download the individual recording. See Downloading recordings on page 47.

Related links

Administering Recordings on page 43

Searching recordings using the search text box

About this task

You can use the search box at the top of the screen to search for specific recordings.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. In the search field, type the values for the following. To type more than one value, separate each value with a comma:
   - **Parties**.
   - **Agents**.
   - **Owner**.
   - **Target**.
   - **Skills**.
   - **Call ID**.
4. Click the  icon.
5. The system displays all the recordings matching your search criteria.

Related links

Administering Recordings on page 43

Filtering the recordings displayed

About this task

When displaying recordings, you can user the search filters shown on the left to display only matching recordings.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. Set the filter options as required. For details of the filters, see Filter Options on page 46.
4. Click **Apply Filter**. The system displays the recordings matching your search filter criteria.
5. To remove the filter, click **Show All**.

Related links

Administering Recordings on page 43
Filter Options on page 46

Filter Options

This following options can be used when applying a filter (see Filtering the recordings displayed on page 46) to the recordings.

Name	Description
Recording Range (Date and Time)	The date and time range between which the call was recorded. Use the calendars to select the dates and the adjacent drop-down menus to specify the time.
Recording Length	The length of the recording. Select one of the signs and enter the time in seconds. The available signs are: • **=** Equal to the recording length you have specified. • **<** Less than the recording length you have specified. • **>** Greater than the recording length you have specified. • **>=** Greater than or equal to the recording length you have specified. • **<=** Less than or equal to the recording length you have specified.
Call Direction	The direction of the call, that is, whether the call is **Internal**, **Incoming**, or **Outgoing**.
Parties	The parties involved in the call. For more than one party, type the names separated by a comma.
Agents	The agents involved in the call. For more than one agent, type the names of agents separated by a comma.

Table continues…

Name	Description
Target Number	The phone number of the recipient of the call.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Related links

Filtering the recordings displayed on page 46

Playing a call recording

About this task

You can play recordings from the displayed list.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. If necessary, search the recordings to show the recordings required (see Searching recordings using the search text box on page 45 and Filtering the recordings displayed on page 46).
4. To play a recording, click the ▶ icon adjacent to the recording. A playback panel is displayed at the top of the menu and can be used to control the playback of the selected recording.

Related links

Administering Recordings on page 43

Downloading recordings

About this task

You can download recordings from Media Manager. The files are downloaded in `OPUS` file format.

⚠ Warning:

- Downloaded recordings are outside the control of the Media Manager application's control and audit trail. Therefore, only allow recordings to be downloaded if assured that their usage will continue to comply with appropriate data protection and privacy requirements.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. If necessary, search the recordings to show the recordings required (see Searching recordings using the search text box on page 45 and Filtering the recordings displayed on page 46).
4. Do any one of the following:
   - To download a single recording, click the icon next to the recording. The recording is downloaded as an individual `OPUS` file.
   - To download multiple recordings, select the check box next to the recording you want to download and then click **Download**.
     - The files are downloaded as a zipped file.
     - The zip files also includes a HTML file containing call details for each recording. When the zipped file is unpack to a folder, this HTML file can be opened in a browser and used to playback the recordings.

Related links

Administering Recordings on page 43

Verifying authentication of call recordings

About this task

All recordings stored by Media Manager include a unique checksum value based on the original contents of the file. If the file is edited or changed in anyway, that checksum is no longer valid.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. If necessary, search the recordings to show the recordings required (see Searching recordings using the search text box on page 45 and Filtering the recordings displayed on page 46).
4. To check the status of the recording authentication, click the icon. The system displays one of the following messages:
   - `Selected Record is VRLA authenticated.`
   - `Selected Record is not VRLA authenticated.`

Related links

Administering Recordings on page 43

Deleting recordings

About this task

Use this procedure to delete unwanted recordings from Media Manager. The recordings are deleted from the local storage and the metadata of the deleted recordings are erased from the database. Recordings stored at remote locations cannot be deleted.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Recording**.
3. If necessary, search the recordings to show the recordings required (see Searching recordings using the search text box on page 45 and Filtering the recordings displayed on page 46).
4. Do any one of the following:
   - To delete a recording, select the recording and click the **Delete**.
   - To delete multiple recordings, select the check box next to the recordings you want to delete and click **Delete**.
5. Click **Yes** when you are prompted to confirm.

Related links

Administering Recordings on page 43

Chapter 10: Using the Audit Trail

The Audit trail feature in Media Manager keeps track of the activities around the recordings in the library. For example, using the audit trail you can track who:

- Searched for a recording
- Replayed a recording
- Downloaded a recording
- Deleted a recording

For each event, the audit trail displays the user name, date, time, and the type of user action. The audit trail is maintained for a predefined number of days set in the application settings.

Related links

Viewing the Audit Trail on page 50
Exporting the Audit Trail on page 52

Viewing the Audit Trail

About this task

Administrators can set the Retention days using the **Audit Retain Period (Days)** field in the Configuration screen. The **Audit Trail** menu is available only to Customer Administrators.

Use this procedure to search for recordings and customize the search results using filters the recordings for:

- a specific period of time
- specific events
- specific users

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Audit**.
3. Use any of the following options separately or together. Do the following to search and filter customize the recordings search results:
   - Use the calendars to set the **Start Date** and the **End Date**.

- Click **Event Type**, and select the type of events you want to include in the Audit trail.
- In the **Search on 'User Name'** box, type a **User Name**, and click the **Search** icon.

4. Click **Apply Filter**.

Result

The **Audit Tail** displays all the recordings matching your filter criteria.

Related links

Using the Audit Trail on page 50
Audit field descriptions on page 51

Audit field descriptions

Name	Description
Search on "User Name"	The text box to search the audit records of users. Type the user name to search the users' activities in the recording library.
User Name	The name of the user who used the recording.
Timestamp	The time when the recording was used.
User Action	The type of user action on a recording. This specifies whether a recording was replayed, downloaded, deleted, or searched.
Details	The details of a recording, such as the owner of the recording, the media name, and the calling party name.
Start Date	The date after which the event occurred. Use the calendars to select the dates and the adjacent drop-down menus to specify the time.
End Date	The date before which the event occurred. Use the calendars to select the dates and the adjacent drop-down menus to specify the time.
Event Type	The type of events to view. The available event types are: • **Delete** • **Download** • **Replay** • **Search**
Export	The option to export the filtered audit results as a compressed `CSV` file on your computer.

Related links

Viewing the Audit Trail on page 50

Exporting the Audit Trail

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Audit**.
3. Use the filter options as required to customize your search results.
4. Click **Apply Filter**.

   The **Audit Trail** displays all the recordings matching your filter criteria.
5. Click **Export**.
6. In the **Exports records** dialog box, type a password.
7. Click **Export**.

Result

Media Manager exports the file as a zipped compressed and password -protected `CSV` file to your computer.

Related links

Using the Audit Trail on page 50

Chapter 11: About alarms and notifications

IP Office Media Manager can provide notification about alarms and events to an email account configured on the **Applications** > **Media Manager** > **Configuration** screen (see Configuring Media Manager on page 15).

The table below lists the basic alarms. The items in { } brackets are replaced with actual values in the alarms sent.

Error Type	Possible Alarm Text
DISK_SPACE_ERROR	• Failed to calculate disk space • Not enough space on the local disk available for Media Manager. Will attempt to free {0} GB. • Failed to rename file {fileName1} to {fileName2}.
FILE_PARSE_ERROR	• Failed to parse file {fileName}. due to unsupported file format.
FILE_ENCODE_ERROR	• Failed to encode file {fileName} from codec {1} to {fileName2}.
CONFIGURATION_ERROR	• System configuration for attribute {attributename} is invalid.
SYSTEM_RESTART	• Service restarted on {service time} • Service started on {service time} • Service shutdown on {service time}
FILE_ERROR	• Failed to delete file(s). • Failed to copy file {fileName1} to {fileName2}.
INTERNAL_SERVICE_ERROR	• Failed to start internal service {service time}. • Failed to stop internal service {service time}.
CONFIGURATION_CHANGED	• Media Manager application configuration is changed.

Related links

Viewing alarms on page 54

Viewing alarms

Procedure

1. Log on to the **Web Manager** user interface.
2. Click **Applications** > **Media Manager** > **Alarms**.

   The system displays all the available alarms with descriptions.

Related links

About alarms and notifications on page 53
Alarms on page 54

Applications > **Media Manager** > **Alarms**

Alarms

Applications > **Media Manager** > **Alarms**

Name	Description
Date	The date on which the alarm was generated.
Severity	The severity of the alarm. The options are: • Information • Warnings • Minor Alarms • Major Alarms • Critical Alarms
Description	A brief description about the alarm.

Related links

Viewing alarms on page 54

Part 5: Miscellaneous

Chapter 12: Contact Recorder Migration

IP Office Release 11.0 and later do not support Contact Recorder. However, existing customers of Contact Recorder can migrate their call record database to Media Manager, which is the only archiving solution in IP Office Release 11.0 and later. ContactStore migration is not supported.

The migration process only migrates the information about the existing recordings and where they are located. It does not move the actual recordings.

VRLA records migrated from Contact Recorder can still be verified for tampering using the Media Manager interface. Thus Media Manager becomes a single interface for all call records, whether archived through Media Manager for newer recordings or the older recordings archived through Contact Recorder.

Note:

You must take a backup of the Contact Recorder database before upgrading your IP Office to Release 11.0 or later. Once you upgrade IP Office to Release 11.0 or later, you will not be able to access or back up Contact Recorder database.

Migration of Connectors

During migration, IP Office also migrates the Connectors that are configured with Contact Recorder. Since Contact Recorder does not have a naming system for it's Connectors, Media Manager provides a name and timestamp to the migrated Connectors. The name is in the format `MigratedX-Timestamp`.

Migrating multiple times

Normally, migration gets completed in one attempt and a summary of the migration is provided on the user interface. However, in case of a network failure or system shutdown midway through a migration, administrators have the option of performing the migration again. If migration is initiated for a second time IP Office identifies and removes the migrated data from the previous unsuccessful migration before starting afresh. Connector configurations too are deleted unless they have been renamed. If you change this default name of a Connector, Media Manager does not recognize the renamed Connector when you migrate again, and creates new one while the renamed Connector still exists in the database.

Availability of Contact Recorder features in Media Manager

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Search by administrator	Search by administrators using Target Number, Skills, Agent, and Call ID	Yes	Yes

Table continues…

Functionality	Description	Availability in Contact Recorder	Availability in Media Manager
Search through Web Self-Admin	Search by users using the search filters Target Number, Skills, Agent, and Call ID	Yes	Yes
Web Self-Admin search results	A maximum of 100 results are displayed.	Yes	Yes
Call sets	Facility to save search results for retrieving in the future.	Yes	No
Email	Attaching recordings to emails.	Yes	No
Bulk Export	Exporting multiple recordings and the related details	Yes	Yes
Owner	Available as a search option.	No	Yes
Audit Trail	Available for tracking the use of recordings.	Yes	Yes
Windows Domain Authentication	-	Yes	No

Related links

Migration limitations on page 57
Migration prerequisites on page 58
Initiating Contact Recorder migration on page 58

Migration limitations

IP Office Release 11.0 and later has the following limitations while migrating Contact Recorder database to Media Manager:

- Alarms and system configuration data such as Call storage path and SMTP Configuration are not migrated.
- Connector passwords are not migrated. IP Office sets the password to blank during migration. Administrators must configure the Connectors after migration is complete.
- Contact Recorder allows one media file to be archived at multiple remote locations. Since Media Manager supports only one Active Connector, it keeps the latest Connector associated with a media file.

Related links

Contact Recorder Migration on page 56

Migration prerequisites

- Since IP Office Release 11.0 and later do not support Contact Recorder, you must back up Contact Recorder prior to upgrading your IP Office.
- If you have your Contact Recorder on your primary hard disk, you must provision a secondary HDD before migrating to Media Manager as Media Manager supports only secondary HDD to store the media files. After migration, the recordings must be moved to the secondary HDD and the Call Storage Path must be updated to a partition on the secondary HDD.
- The secondary HDD must be activated through the Web Control menus. For more information on adding secondary HDD and activating the HDD, see Activating additional hard drives on page 14.
- Administrator initiating the migration must have Media Manager Administrator rights.
- Media Manager and Contact Recorder must be on the same server.

Related links

Contact Recorder Migration on page 56

Initiating Contact Recorder migration

Before you begin

Ensure you have backed up the Contact Recorder database before upgrading to IP Office Release 11.0 or later releases.

Procedure

1. Log on to the **Web Manager** interface.
2. Click **Applications** > **Media Manager** > **Migration**

   IP Office prompts you to confirm migration of your Contact Recorder database.
3. Click **Yes** to confirm.

   IP Office displays a message `Media Manager migration has started` and shows the completion percentage of migration. After the migration process is over, a summary of the process is provided.

Next steps

- Call Storage Path does not get migrated. Administrators must ensure that the Call Storage Path for Media Manager and Contact Recorder are the same. If they are different, media files from the Contact Recorder Call Storage Path must be copied to the Media Manager Call Storage Path while maintaining the internal directory structure of Contact Recorder. This ensures playback of the recordings archived through Contact Recorder.
- If any NAS configuration has been migrated, administrators must configure the password for the NAS after migration.

- Administrators must select an Active Connector to be used for remote archiving.

Related links

Contact Recorder Migration on page 56

Chapter 13: Resources

Documentation resources

For a listing of documentation resources related to IP Office,

- Download documents from the Avaya Support website at http://support.avaya.com.
- IP Office documentation is also available on the IP Office Knowledgebase at https://ipofficekb.avaya.com.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs

- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

https://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

https://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

https://ipofficekb.avaya.com provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on https://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

https://www.iaug.org is the official discussion forum for Avaya product users.

Change history

Issue	Date	Summary of changes
1	June 2017	First release
2	February 2018	Updates for Release 11.0: • Added a new chapter for migrating Contact Recorder database. • Removed the topic about configuring Media Manager as the archiving solution. • Removed the topic about Media Manager and Contact Recorder co-residency. • Removed instructions on backing up Contact Recorder. • Added references to the *Installing and Maintaining the Avaya IP Office Application Server* guide for instructions on adding additional hard drive.
3	February 2019	Updates for Release 11.0 FP4: • Added a new topic for Deleting recordings in the chapter Accessing and using recordings. • Added a new chapter with instructions on using the Audit Trail. • Updated the Configuration topic to add the new field - “Audit Retain Period (Days)”.
4	April 2020	Updates for Release 11.1 • Updated Network-Attached Storage (NAS) section • Added about alarms and events. • Updated Deleting an existing connector
8	August 2020	• General refresh of layout to improve readability. • Addition of process to replace additional hard disk with larger disk. • Addition of process to install additional hard disk post server ignition.
9	February 2021	Updated Network-Attached Storage (NAS) section

Index

S

V

W