Administering Avaya IP Office™ Platform Media Manager

Release 12.0
Issue 24
November 2024

© 2022-2024, Avaya LLC
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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Part 1: Introduction 7
- **Chapter 1: IP Office Media Manager** 8
  - Media Manager Architecture 9
  - Media Manager Recording Capacity 10
  - Resilience 11
  - Administrator Access to Media Manager 11
  - Backup and restore 12
  - Encryption of recordings 12
  - Using Cloud-Based Storage/Bring Your Own Storage 12
  - Contact Recorder 13
- **Chapter 2: Media Manager Setup** 14
  - Licensing 14
  - Verifying Media Manager license on Web Manager 15
  - Verifying licenses on Voicemail Pro 15
  - Select local or centralized Media Manager 16
  - Activating an additional hard disk 16
  - Preparing cloud-based file storage 17
  - Starting the Media Manager service 18
  - Configuring Media Manager 18
  - Configuring the IP500 V2 System Address 19
- **Chapter 3: Media Manager Settings** 20
  - Media Manager Configuration Settings 20
  - Hosted Storage Type Configuration settings 22

Part 2: Recording Calls 24
- **Chapter 4: Managing Call Recording** 25
  - Switching the call recording warning on/off 25
  - Setting the maximum call recording length 26
  - Configuring the recording display 26
  - Configuring a user's manual call recording destination 27
  - Configuring automatic call recording for a user 27
  - Configuring auto recording for a hunt group 28
  - Configuring automatic call recording for an incoming call route 29
  - Configuring auto recording for account code 30

Part 3: Connectors and Archiving 32
- **Chapter 5: Managing Connectors for Recording Archiving** 33
  - Adding a Connector 33
    - Connectors 34
  - Modifying the details of a Connector 34

Deleting an existing Connector ... 35
Chapter 6: Archiving to DVD ... 36
Configuring DVD archiving ... 36
Chapter 7: Archiving to an External NAS ... 38
Configuring NAS archiving ... 38
Chapter 8: Archiving to Google Drive ... 40
Creating a Google drive for Media Manager ... 40
Configuring Google drive archiving ... 41
Chapter 9: Using Google Cloud bucket storage ... 42
Creating a Google Bucket for Media Manager ... 42
Configuring cloud-based storage as primary storage ... 43
Configuring a Google Cloud bucket archiving connector ... 44
Chapter 10: Using Azure Blob storage ... 46
Creating an Azure Blob for Media Manager ... 46
Configuring cloud-based storage as primary storage ... 47
Configuring an Azure Blob Storage archiving connector ... 48
Chapter 11: Using Amazon S3 storage ... 50
Creating an Amazon S3 bucket for Media Manager ... 50
Configuring cloud-based storage as primary storage ... 51
Configuring an Amazon S3 archiving connector ... 52
Part 4: Recordings and Alarms ... 54
Chapter 12: Administering Recordings ... 55
Configuring Media Manager Access ... 55
Providing administrator access to Media Manager ... 56
Configuring user access through the user portal ... 56
Accessing the recordings ... 57
Recordings Details ... 58
Searching recordings using the search text box ... 59
Filtering the recordings displayed ... 60
Filter Options ... 60
Playing a call recording ... 61
Downloading recordings ... 61
Verifying authentication of call recordings ... 62
Deleting recordings ... 63
Chapter 13: Using the Audit Trail ... 64
Viewing the Audit Trail ... 64
Audit field descriptions ... 65
Exporting the Audit Trail ... 65
Chapter 14: Alarms and notifications ... 67
Viewing alarms ... 68
Alarms ... 68

Part 5: Miscellaneous ... 69
Chapter 15: Migrating recordings to different storage ... 70
Migrating recordings from HDD to Google Cloud Bucket ... 70
Migrating recordings from HDD to Amazon S3 Bucket ... 71
Migrating recordings from HDD to Azure Blob ... 71
Migrating recordings from Google Cloud to HDD ... 71
Migrating recordings from Google Cloud to Azure Blob ... 72
Migrating recordings from Google Cloud to Amazon ... 72
Migrating recordings from Azure to HDD ... 72
Migrating recordings from Azure to Google ... 73
Migrating recordings from Azure to Amazon ... 73
Migrating recordings from Amazon to HDD ... 73
Migrating recordings from Amazon to Google ... 74
Migrating recordings from Amazon to Azure ... 74
Chapter 16: Contact Recorder Migration ... 75
Migration limitations ... 76
Migration prerequisites ... 77
Initiating Contact Recorder migration ... 77
Part 6: Further Help ... 79
Chapter 17: Additional Help and Documentation ... 80
Additional Manuals and User Guides ... 80
Getting Help ... 80
Finding an Avaya Business Partner ... 81
Additional IP Office resources ... 81
Training ... 82

Part 1: Introduction

Chapter 1: IP Office Media Manager

IP Office Media Manager stores and replays audio call recordings generated by Voicemail Pro. It stores recordings on a local drive or cloud-based storage. Media Manager can also archive recordings to additional locations such as DVD, NAS, or cloud-storage.

Important:

- There are two types of Media Manager, **Local Media Manager** and **Centralized Media Manager**.
  - This document covers **Local Media Manager**, provided by the local IP Office, Voicemail Proand Media Manager services.
  - For details of the cloud-based **Centralized Media Manager** available for subscription IP Office systems, see the Administering Avaya IP Office™ Platform with Web Manager manual.

Media Manager archives and catalogs recordings for administrators and users to search, play, and download when required. All recordings are available to system administrators through Web Manager. Administrator can configure extension users for access to selected recording through the IP Office User Portal application.

IP Office only supports Media Manager running on the same server as Voicemail Pro.

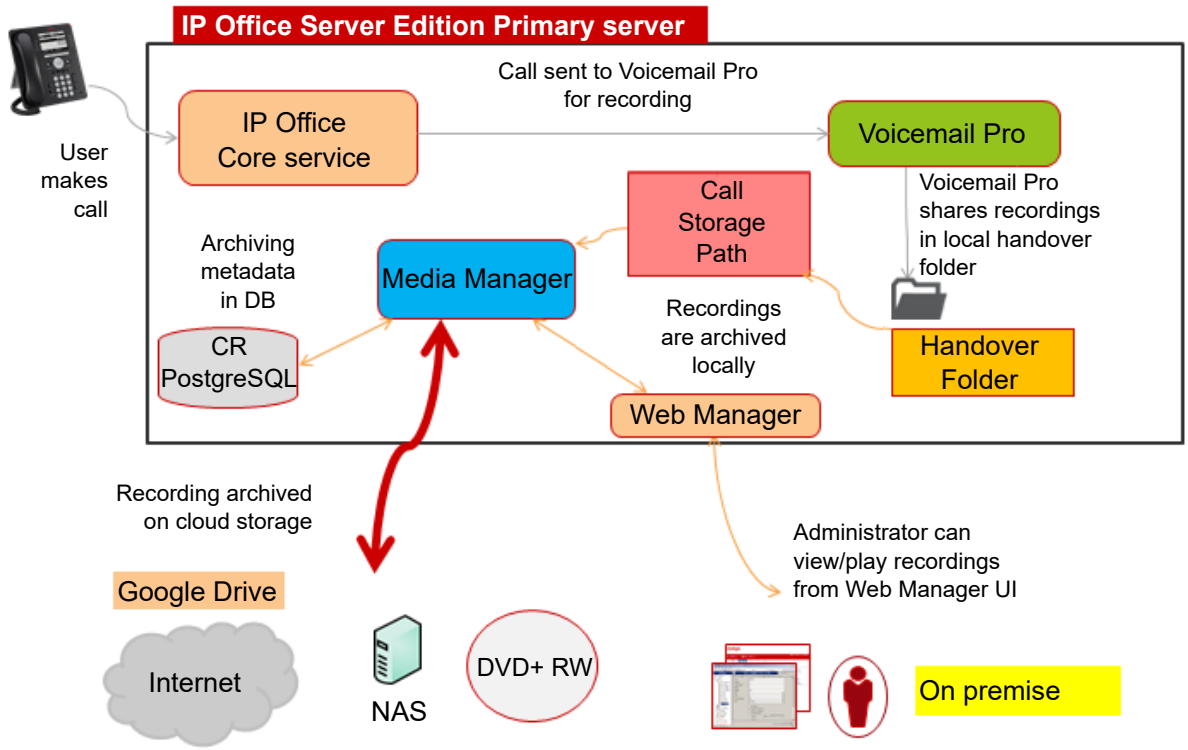
- For a network based around a primary server, support Media Manager on the primary server. They do not supportMedia Manager on the secondary server or any other server in the network.
- For a standalone IP500 V2 system or SCN of IP500 V2 systems, Media Manager is supported on the same IP Office Application server hosting Voicemail Pro for the network. Media Manager is not supported on a Unified Communications Module.

Related links

Media Manager Architecture on page 9
Media Manager Recording Capacity on page 10
Resilience on page 11
Administrator Access to Media Manager on page 11
Backup and restore on page 12
Encryption of recordings on page 12
Using Cloud-Based Storage/Bring Your Own Storage on page 12
Contact Recorder on page 13

Media Manager Architecture

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.
   - IP Office can automatically trigger recording for specific users, groups, incoming call routes, or account codes.
   - Voicemail Pro can trigger recording as part of a voicemail callflow.
   - Users can manually trigger recording.
   - The call recording configuration settings indicate the destination for recordings. That is either a voicemail mailbox or Media Manager (using the setting **Voice Recording Library**).
2. Voicemail Pro records the call. For recordings where the destination is set as **Voice Recording Library**, the recording is placed into a handover folder.
3. The Media Manager service constantly checks the handover folder:
   - Whenever a new recording is available, Media Manager moves the recording to its call storage folder. That can be a local hard drive or a folder in cloud-based storage.
   - Media Manager adds details of the call to the Media Manager database.

4. System administrators can access recordings using Web Manager. They can configure user access to recordings using the IP Office user portal application.
5. If Media Manager has been configured with an external connector, it copies new recordings to the external location.

Related links

IP Office Media Manager on page 8

Media Manager Recording Capacity

Media Manager requires an additional drive which it use as the location of its primary call storage folder. Media Manager uses this location to store recordings after transferring them from the temporary storage folder used by Voicemail Pro.

Important:

- Avaya does not support Media Manager using the same drive that is hosting the Voicemail Pro service. Doing so will cause space conflicts with other IP Office applications and risks losing recordings during other IP Office maintenance activities.

You must either:

- Add an additional drive to the server hosting the Voicemail Pro service. Avaya recommends you add a pair of drives configured for RAID.
- Configure a cloud-based service as the primary call storage. Media Manager supports the following:
  - Google Bucket
  - Azure Blob
  - Amazon S3 Bucket
- **Warning:**
  - When using storage other than an additional hard-disk in the IP Office system, you must check the file aging policies of that other storage, as they may differ from the file aging policy applied by the Media Manager settings.

In operation, you can optimize the use of the primary call storage by having Media Manager also copy recordings to separate archive storage, which can be a DVD, NAS or cloud-based storage. After a time, the primary call storage will contain just the newest recordings whilst the archive contains old recordings.

Estimating the storage capacity required

The required capacity for the storage you use for Media Manager depends on factors that will vary between different customers. You need to estimate the typical number and length of calls recordings that the customer's business will generate.

You also need to include how long the customer wants to retain recordings, and how the customer wants to use recordings in the primary call storage and those in a separate archive (if installed).

For both types of storage, you can use the following figures:

- Media Manager recordings require 60KB a minute for non-authenticated files, 120KB a minute for authenticated files.
- For the primary call storage, the minimum size Avaya support is 30GB. However, Avaya recommends 300GB or larger.

Related links

IP Office Media Manager on page 8

Resilience

If the Server Edition Primary is unavailable, Media Manager is also unavailable. However, if you have configured Voicemail Pro resilience, the secondary server continues to record calls but cannot transfer them to the primary server.

Access to recordings resumes when the primary server comes back into service. After that, the two servers use SFTP to transfer call recordings made during resilience from the secondary server to the primary server.

For more information, see the Administering IP Office Voicemail Pro and IP Office Resilience Overview manuals.

Related links

IP Office Media Manager on page 8

Administrator Access to Media Manager

By default, the IP Office administrator can access the Media Manager settings and recordings using the IP Office Web Manager. They can also configure additional administrators for access. They can also configure individual extension users for access to recordings through User Portal.

For more information, see Managing access on page 56.

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, refer to the Deploying IP Office Server Edition. For Media Manager, the backup options include:

	Description
Media Manager Configuration	The IP Office backup and restore processes can include the configuration settings of Media Manager application.
Call Recordings Database	The IP Office backup and restore processes can include the Media Manager call details database
Call Recordings	The IP Office backup and restore processes do not include the call recordings.

Related links

IP Office Media Manager on page 8

Encryption of recordings

For IP Office R11.1 and higher, Media Manager encrypts all recordings stored in its primary call storage folder.

- You can only play encrypted recordings through IP Office interfaces such as IP Office Web Manager or the User Portal.
- Media Manager decrypts recordings when downloaded using the IP Office interfaces. Recordings download using any other method, such as SSH access, remain encrypted.

For external archive connectors, you can select whether encryption is used.

- If encryption is enabled on a connector, it cannot be switched off.
- If encryption is not enabled on a connector, you must ensure that access to recording in the remote archive complies with local data protection and privacy requirements.

Related links

IP Office Media Manager on page 8

Using Cloud-Based Storage/Bring Your Own Storage

For the local Media Manager service, you can use cloud-based storage if required. You can use this for the Media Manager service's primary call storage folder and/or for archive storage.

Media Manager supports the following types of cloud-based storage:

- Google Bucket
- Azure Blob

- Amazon S3 Bucket

To retain the recordings in primary storage indefinitely, you can set **Days to Retain Calls** to zero.

Warning:

- When using storage other than an additional hard-disk in the IP Office system, you must check the file aging policies of that other storage, as they may differ from the file aging policy applied by the Media Manager settings.

Files that are archived are copied from those in the primary storage. For playback, Media Manager uses the original recording in the primary storage unless it has been deleted in which cases it uses the archive copy.

Related links

IP Office Media Manager on page 8

Contact Recorder

Contact Recorder is a previous IP Office application for archiving call recording.

To be able to search and replay existing call recordings through the Media Manager, the customer must migrate the Contact Recorder call recording database to Media Manager. The existing recordings do not need to be moved. See Migrating Contact Recorder on page 75.

Related links

IP Office Media Manager on page 8

Chapter 2: Media Manager Setup

Media Manager uses the same hard drive as the IP Office service for its call recording database. However, for the actual call recordings, separate storage is required. That can be either:

- An additional hard disk (or pair of drives for RAID). Storage on the same disk used by Voicemail Pro and other IP Office applications is not supported. This documentation cannot cover the installation of the addition drive. Refer to the documentation for the specific server platform.
- An external cloud-based file store (Google bucket, Amazon S3 or Azure Blob).

Related links

Licensing on page 14
Verifying Media Manager license on Web Manager on page 15
Verifying licenses on Voicemail Pro on page 15
Select local or centralized Media Manager on page 16
Activating an additional hard disk on page 16
Preparing cloud-based file storage on page 17
Starting the Media Manager service on page 18
Configuring Media Manager on page 18
Configuring the IP500 V2 System Address on page 19

Licensing

Non-subscription IP Office systems require the following licenses:

- Standalone IP500 V2 system requires a Media Manager subscription.
- IP Office Server Edition, the primary server requires a Media Manager subscription.
- IP Office Select using dual-active voicemail servers, both the primary and secondary servers need a Media Manager license.

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 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. 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 Manager or Administering Avaya IP Office™ Platform with Web Manager.

Related links

Media Manager Setup on page 14

Verifying Media Manager license on Web Manager

About this task

For systems using PLDS licensing, you can check the presence of the appropriate license in the IP Office system configuration.

Procedure

1. Log on to the Web Manager interface.
2. Click **System Settings** > **Licenses**.
3. Verify that the `VMPro Media Manager` exists.
   - 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

Media Manager Setup on page 14

Verifying licenses on Voicemail Pro

About this task

You can check the presence of the Media Manager license or subscription 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 the VRL (Media Manager) license is listed.

Related links

Media Manager Setup on page 14

Select local or centralized Media Manager

Use the following process to select which application the IP Office uses to store call recordings.

Procedure

1. Select **System Settings** and then **System**.
2. Select **Media Archival Solution** and select the source required:

Option	Description
Local Media Manager	Use the local Media Manager service running on the same server as the voicemail service. • This is the version of Media Manager covered by this documentation.
Centralized Media Manager	Use the centralized service provided by the cloud-based servers for subscription IP Office systems. • This version of Media Manager is not covered by this documentation. For details, see the 'Centralized Media Manager' chapter in the Administering Avaya IP Office™ Platform with Web Manager manual.

3. Click **Update**.

Related links

Media Manager Setup on page 14

Activating an additional hard disk

About this task

If using a local hard disk as the primary call storage for call recordings, you must use a separate hard disk. Storage of call recordings on the same disk used by Voicemail Pro and other IP Office services is not supported.

- For a new server with an addition hard disk already installed, configuration and formatting of the addition drive is part of the new server ignition process.
- For an existing server to which you want to add an additional disk post-ignition, follow the server platform instructions for adding a new drive. Then follow the procedure below to activate the additional hard disk in IP Office.
  - Avaya recommend that where possible, you add two additional drives configured as a RAID pair.

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 and does not contain any existing call recordings, then under **Format Hard Drive** select **Enable**.

   Warning:

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

Next steps

- Check that the Media Manager service is running. See Starting the Media Manager service on page 18.

Related links

Media Manager Setup on page 14

Preparing cloud-based file storage

As an alternative to using an additional local hard drive, external cloud-based storage can be used as the primary storage for Media Manager. If so, ensure you have configured your external cloud storage and it is ready to access:

- Creating a Google Bucket for Media Manager on page 42
- Creating an Azure Blob for Media Manager on page 46
- Creating an Amazon S3 bucket for Media Manager on page 50

Related links

Media Manager Setup on page 14

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 18.

Related links

Media Manager Setup on page 14

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.

Before you begin

Ensure that the primary storage for recordings has been configured:

- If using a local hard drive, see Activating an additional hard disk on page 16.
- If using cloud base storage, see Preparing cloud-based file storage on page 17.

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. Set the **Call Storage Type** as required:
   - If set to **Local Hard Drive**, in the **Call Storage Path**, 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.
   - If set to **Hosted Storage**, set the **Hosted Storage Type** and complete the required details for the cloud-based storage.
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 19.

Related links

Media Manager Setup on page 14

Configuring the IP500 V2 System Address

About this task

IP500 V2 systems support Media Manager by installing an IP Office Application Server to run both Voicemail Pro and Media Manager.

For user to access recordings through User Portal, 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 14

Chapter 3: Media Manager Settings

All the Media Manager configuration settings are accessed through the **Applications** > **Media Manager** menu in IP Office Web Manager.

Using the IP Office security settings, you can configure which IP Office Web Manager service users have access to the Media Manager menus.

Related links

Media Manager Configuration Settings on page 20
Hosted Storage Type Configuration settings on page 22

Media Manager Configuration Settings

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

Name	Description
Profile	Default = Blank The unique name that identifies the configuration profile.
Log Level	Default = INFO The selected log level for the Media Manager service. The options are **INFO**, **DEBUG** and **ERROR**.
Handover Folder	Default = `/opt/vmpro/MM/VRL` The Voicemail Pro path from where Media Manager picks up the recordings. Voicemail Pro writes call recording files to this folder.
Days to Retain Calls	Default = 180 days. Range = 0 to 180 days. The number of days for which the database retains the call details. After this, Media Manager deletes the call recordings. • To disable the deletion, enter 0. • Note: Media Manager also starts deleting 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.

Table continues…

Name	Description
Active Connector	Default = Blank The connector being used for remote archiving copies of recordings. The drop-down menu lists all the available connectors that have been configured. Changing the connector results in a change in the archive destination. However, the recordings from the previous archives are still available.
Call Storage Type	Default = Local Hard Drive Sets the destination that Media Manager use as its primary storage for recordings collected from the **Handover Folder**. • **Local Hard Drive** - Use the local hard drive partition specified by the **Call Storage Path** setting. • **Hosted Storage** - Use the cloud-based storage specified by the **Hosted Storage Type** settings.
Call Storage Path	Default = Blank. This field is available when the **Call Storage Type** is set to **Local Hard Drive**. • 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 in the server's **Platform View** menus. • If you must change the value after you have already started recording, copy all the sub-directories and files from the old directory to the new directory before you resume recording.
Hosted Storage Type	This field is available when the **Call Storage Type** is set to **Hosted Storage**. The supported options are **Amazon S3 Bucket**, **Google Cloud Storage Bucket**, and **Microsoft Azure Blob Storage** Additional fields are shown depending on the selected **Call Storage Type**. For details, see the Administering Avaya IP Office™ Platform Media Manager manual.
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.

Table continues…

Name	Description
SMTP User Name	Default = Blank The user's name for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the user's 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.
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

Media Manager Settings on page 20

Hosted Storage Type Configuration settings

The following additional settings are shown and need to be configured when a **Call Storage Type** is set to **Hosted Storage**.

Google Cloud Storage Bucket

The following options are shown when the **Hosted Storage Type** is set to **Google Cloud Storage Bucket** as primary storage. For details of setting up a Google cloud storage bucket, see Creating a Google Bucket for Media Manager on page 42.

Name	Description
Bucket Name	Enter a unique bucket name that meets the bucket name requirements. See Bucket naming guidelines.
Parent Folder	Enter a unique parent folder name.
Import Service Account Key	Browse and select the and select the `.JSON` file that you downloaded after creating your Google Cloud Bucket. See Service Accounts.

Microsoft Azure Blob Storage

The following options are shown when the **Hosted Storage Type** is set to **Microsoft Azure Blob Storage** as primary storage. For details of setting up Microsoft Azure Blob storage, see Creating an Azure Blob for Media Manager on page 46.

Name	Description
Storage Account Name	A storage account provides allows to specify a unique name. Every media recordings that you store in the external storage has an address that includes the unique storage account name.
Azure Container Name	Enter a container name. See Naming and referencing containers, blobs, and metadata.
Parent Folder	Enter a unique parent folder name.
SAS Token	Enter the generated SAS token. See Authorize access to data in Azure Storage.

Amazon S3 Bucket

The following options are shown when the **Hosted Storage Type** is set to **Amazon S3 Bucket** as primary storage. For details of setting up an Amazon S3 storage bucket, see Creating an Amazon S3 bucket for Media Manager on page 50.

Name	Description
Bucket Name	Enter a unique bucket name that meets the bucket name requirements. See Naming rules.
Parent Folder	Enter a unique parent folder name.
User Access key ID	Enter the created access key ID. See Access keys.
User Secret access Key	Enter the created secret access key. See Access keys.

Related links

Media Manager Settings on page 20

Part 2: Recording Calls

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 25
Setting the maximum call recording length on page 26
Configuring the recording display on page 26
Configuring a user's manual call recording destination on page 27
Configuring automatic call recording for a user on page 27
Configuring auto recording for a hunt group on page 28
Configuring automatic call recording for an incoming call route on page 29
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 25

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 25

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 25

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. Configure the recording settings as required:

Name	Description
Destination	Set the destination of the call recordings. The options are: • **Mailbox** Store the recordings in the voicemail mailbox selected. Users can access and manage these recordings using the voicemail mailbox controls. • **Voice Recording Library** Transfer the recordings to Media Manager. • **Voice Recording Library Authenticated** This is a legacy setting. It operates the same as **Voice Recording Library**.

5. Click **OK**.
6. Save the configuration.

Related links

Managing Call Recording 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. Configure the recording settings as required:

Name	Description
Inbound	Sets the frequency of call recording: • **None**: Do not record calls. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls if a recording channel is available. If no recording channel is available, return busy tone to the caller. • **xx%**: Record calls at the set percentage. For example, setting 25% records 1 call in every 4 on average.
Outbound	
Auto Record Calls	Set the type of calls recorded. The options are **Internal**, **External** or **External & Internal**.
Destination	Set the destination of the call recordings. The options are: • **Mailbox** Store the recordings in the voicemail mailbox selected. Users can access and manage these recordings using the voicemail mailbox controls. • **Voice Recording Library** Transfer the recordings to Media Manager. • **Voice Recording Library Authenticated** This is a legacy setting. It operates the same as **Voice Recording Library**.
Time Profile	Optional. Select an existing IP Office time profile to specify when the IP Office uses the automatic call recording settings. If no time profile is selected, the IP Office uses automatic call recording all the time.

5. Click **OK**.
6. Save the configuration.

Related links

Managing Call Recording on page 25

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. Configure the settings as required:

Name	Description
Record Inbound	Sets the frequency of call recording: • **None**: Do not record calls. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls if a recording channel is available. If no recording channel is available, return busy tone to the caller. • **xx%**: Record calls at the set percentage. For example, setting 25% records 1 call in every 4 on average.
Record Time Profile	Optional. Select an existing IP Office time profile to specify when the IP Office uses the automatic call recording settings. If no time profile is selected, the IP Office uses automatic call recording all the time.
Recording (Auto)	Set the destination of the call recordings. The options are: • **Mailbox** Store the recordings in the voicemail mailbox selected. Users can access and manage these recordings using the voicemail mailbox controls. • **Voice Recording Library** Transfer the recordings to Media Manager. • **Voice Recording Library Authenticated** This is a legacy setting. It operates the same as **Voice Recording Library**.
Auto Record Calls	Set the type of calls recorded. The options are **Internal**, **External** or **External & Internal**.

5. Click **OK**.
6. Save the configuration.

Related links

Managing Call Recording on page 25

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. Configure the settings as required:

Name	Description
Record Inbound	Sets the frequency of call recording: • **None**: Do not record calls. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls if a recording channel is available. If no recording channel is available, return busy tone to the caller. • **xx%**: Record calls at the set percentage. For example, setting 25% records 1 call in every 4 on average.
Record Time Profile	Optional. Select an existing IP Office time profile to specify when the IP Office uses the automatic call recording settings. If no time profile is selected, the IP Office uses automatic call recording all the time.
Recording Auto	Set the destination of the call recordings. The options are: • **Mailbox** Store the recordings in the voicemail mailbox selected. Users can access and manage these recordings using the voicemail mailbox controls. • **Voice Recording Library** Transfer the recordings to Media Manager. • **Voice Recording Library Authenticated** This is a legacy setting. It operates the same as **Voice Recording Library**.

5. Click **OK**.
6. Save the configuration.

Related links

Managing Call Recording on page 25

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. Configure the settings as required:

Name	Description
Record Outbound	Sets the frequency of call recording: • **None**: Do not record calls. • **On**: Record calls if a recording channel is available. • **Mandatory**: Record calls if a recording channel is available. If no recording channel is available, return busy tone to the caller. • **xx%**: Record calls at the set percentage. For example, setting 25% records 1 call in every 4 on average.
Record Time Profile	Optional. Select an existing IP Office time profile to specify when the IP Office uses the automatic call recording settings. If no time profile is selected, the IP Office uses automatic call recording all the time.
Recording (Auto)	Set the destination of the call recordings. The options are: • **Mailbox** Store the recordings in the voicemail mailbox selected. Users can access and manage these recordings using the voicemail mailbox controls. • **Voice Recording Library** Transfer the recordings to Media Manager. • **Voice Recording Library Authenticated** This is a legacy setting. It operates the same as **Voice Recording Library**.

5. Click **OK**.
6. Save the configuration.

Related links

Managing Call Recording on page 25

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.

Note:

For configuring NAS archiving, SMB protocol version 2 and 3 is supported. SMB version 3 is more secured protocol and can be used for encryption.

Before you begin

Ensure you have configuration access to Web Manager.

Procedure

1. Log in to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Connectors**.
3. Click **Add** and select one of the options as required:
   - **DVD** See Archiving to DVD on page 36.
   - **Google** See Archiving to Google Drive on page 40.
   - **NAS** See Archiving to an External NAS on page 38.
   - **Google Bucket** See Using Google Cloud bucket storage on page 42.
   - **Azure Blob** See Using Azure Blob storage on page 46.

- **Amazon S3 Bucket** See Using Amazon S3 storage on page 50.

Related links

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

Connectors

Applications > **Media Manager** > **Connectors**

For details of adding and editing connectors, see the Administering Avaya IP Office™ Platform Media Manager manual.

Name	Description
Add	The drop-down menu to select a connector. The options are **DVD**, **NAS**, **Google drive**, **Amazon S3 Bucket**, **Google Cloud Storage Bucket** and **Microsoft Azure Blob Storage**.
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.
Last Successful Archive Time	The time the connector was last used successfully.

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+RW drive.

You must monitor the storage capacity and keep a blank DVD+RW available. Insert the blank DVD+RW after a full DVD is ejected. New recordings 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. Use the **Encrypt Recording** setting to select whether recordings should be encrypted. Note, you cannot set **Encrypt Recording** back to **NO** after saving the connector.
   - If encrypted, recordings can only be replayed from IP Office menus. Recordings are unencrypted when downloading from an IP Office menu.
   - If unencrypted, you must ensure that access to recordings in the archive complies with local data protection and privacy requirements.

7. Click **Test Connection**. If connection is successful, click **Create**. Otherwise, check and adjust the settings as required.
8. To start using the connector for archiving, select the connector from the **Active Connector** field and click **Update**.

Result

- Media Manager will regularly copy new recordings from the primary call storage folder to the archive storage.

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

Note:

For configuring NAS archiving, SMB protocol version 2 and 3 is supported. SMB version 3 is more secured protocol and can be used for encryption.

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 username to access file share.
   d. In the **Password For Fileshare** field, enter the password for the username to access file share.
6. Use the **Encrypt Recording** setting to select whether recordings should be encrypted. Note, you cannot set **Encrypt Recording** back to **NO** after saving the connector.
   - If encrypted, recordings can only be replayed from IP Office menus. Recordings are unencrypted when downloading from an IP Office menu.
   - If unencrypted, you must ensure that access to recordings in the archive complies with local data protection and privacy requirements.
7. Click **Test Connection**. If connection is successful, click **Create**. Otherwise, check and adjust the settings as required.
8. To start using the connector for archiving, select the connector from the **Active Connector** field and click **Update**.

Result

- Media Manager will regularly copy new recordings from the primary call storage folder to the archive storage.

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. Use the **Encrypt Recording** setting to select whether recordings should be encrypted. Note, you cannot set **Encrypt Recording** back to **NO** after saving the connector.
   - If encrypted, recordings can only be replayed from IP Office menus. Recordings are unencrypted when downloading from an IP Office menu.
   - If unencrypted, you must ensure that access to recordings in the archive complies with local data protection and privacy requirements.
7. Click **Browse** and select the `JSON` file that you downloaded after creating your Google drive.
8. Click **Upload**.
9. Click **Test Connection**. If connection is successful, click **Create**. Otherwise, check and adjust the settings as required.
10. To start using the connector for archiving, select the connector from the **Active Connector** field and click **Update**.

Result

- Media Manager will regularly copy new recordings from the primary call storage folder to the archive storage.

Related links

Archiving to Google Drive on page 40

Chapter 9: Using Google Cloud bucket storage

Media Manager can use a Google Cloud bucket as storage for recordings. It can use this as its primary storage and/or as archive connector storage.

Related links

Creating a Google Bucket for Media Manager on page 42
Configuring cloud-based storage as primary storage on page 43
Configuring a Google Cloud bucket archiving connector on page 44

Creating a Google Bucket for Media Manager

About this task

This section provides the high-level steps to create a Google Bucket for Media Manager use. It can use this as its primary storage and/or as archive connector storage.

Before you begin

Ensure you have an account, created a project, and enabled it in the Google Cloud console.

Procedure

1. In the Google Cloud Console, go to https://console.cloud.google.com/storage/browser.
2. Click **Create bucket** to open the bucket creation form.
3. Click **Create folder**.
4. Enter the folder name in the following format: `parent-folder <name>`.
5. In the Google Cloud Console, go to the Service Accounts page.
6. Click **Select** your project.
7. Click the email address of the service account to create a key.
8. Click the **Keys** tab.
9. Click **Add key** and select **Create new key**.
10. Select **JSON** as the **Key type** and click **Create**.

Clicking **Create** downloads a service account key file.

11. Go to the browser page and click the Bucket overflow menu.

    Select the bucket associated to which you want to grant a member a role

12. Choose **Edit bucket permissions**.
13. Click **+ Add members**.
14. In the **New members** field, enter service account mail id.
15. Select the following roles from the **Select a role** menu.
    - `Storage Legacy Bucket Writer`
    - `Storage Legacy Object Read`
16. Click **Save**.

Next steps

The external storage can now be used for as either the primary call storage folder for Media Manager or as a connector for archiving recordings:

- Configuring cloud-based storage as primary storage on page 43
- Configuring an Azure Blob Storage archiving connector on page 48

Related links

Using Google Cloud bucket storage on page 42

Configuring cloud-based storage as primary storage

About this task

Use this procedure to configure external cloud-based storage as the primary call storage folder for Media Manager.

Before you begin

Ensure you have configured your external cloud storage and it is ready to access:

- Creating a Google Bucket for Media Manager on page 42
- Creating an Azure Blob for Media Manager on page 46
- Creating an Amazon S3 bucket for Media Manager on page 50

Procedure

1. Go to the **Configuration** view.
2. In **Call Storage Type**, select **Hosted Storage Type**.
3. In **Hosted Storage Type**, select the required external storage.
4. Enter the configuration settings as per the selected type of external storage. See Hosted Storage Type Configuration settings on page 22.

5. Click **Test Connection**.
6. Click **Save**.

Result

- All new recordings are stored in the configured external storage.

Related links

Using Google Cloud bucket storage on page 42
Using Azure Blob storage on page 46
Using Amazon S3 storage on page 50

Configuring a Google Cloud bucket archiving connector

About this task

You can use the following process to use a Google Cloud bucket as a connector for archiving call recordings from the primary call storage folder.

Before you begin

- Create a Google project and download the JSON file. See Creating a Google Bucket for Media Manager on page 42.

Procedure

1. Log in to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Connectors**.
3. Click **Add**.
4. Select **Google Cloud Storage Bucket**.
5. On the Add Google Cloud Bucket Connector window, in the **Name** field, type the name of the connector.
6. Add the **Bucket Name**.
7. Enter the **Parent Folder** name.
8. In Service Accounts, browse and select the `.JSON` file downloaded after creating your Google Cloud bucket.
9. Click **Upload**.
10. Use the **Encrypt Recording** setting to select whether recordings should be encrypted. Note, you cannot set **Encrypt Recording** back to **NO** after saving the connector.
    - If encrypted, recordings can only be replayed from IP Office menus. Recordings are unencrypted when downloading from an IP Office menu.
    - If unencrypted, you must ensure that access to recordings in the archive complies with local data protection and privacy requirements.

11. Click **Test Connection**. If connection is successful, click **Create**. Otherwise, check and adjust the settings as required.
12. To start using the connector for archiving, select the connector from the **Active Connector** field and click **Update**.

Result

- Media Manager will regularly copy new recordings from the primary call storage folder to the archive storage.

Related links

Using Google Cloud bucket storage on page 42

Chapter 10: Using Azure Blob storage

Media Manager can use an Azure Blob as storage for recordings. It can use this as its primary storage and/or as archive connector storage.

Related links

Creating an Azure Blob for Media Manager on page 46
Configuring cloud-based storage as primary storage on page 43
Configuring an Azure Blob Storage archiving connector on page 48

Creating an Azure Blob for Media Manager

About this task

This section provides the high-level steps to create Azure Blob storage for Media Manager use. It can use this as its primary storage and/or as archive connector storage.

Before you begin

Ensure you have an active Azure subscription to access the Azure Blob storage account.

Procedure

1. Go to Azure portal https://portal.azure.com/#home.
2. Select **Storage accounts** to display a list of your storage accounts.
3. On the **Create a storage account** page in fill in the required information.
4. Select **Review + create**. Azure runs validation on the storage account settings that you select.
   - If validation passes, you can proceed to create the storage account.
   - If validation fails, modify the settings indicated by the portal.
5. On the **Storage accounts** page, select **Create**.
6. Navigate to your new storage account in the Azure portal.
7. Go to **Data storage** > **Blob containers**.
8. Select the **+ Container** button. For more information about creating container, see create containers.

9. Type a name for your new container.

   Ensure the name of the new container follows the valid DNS name. See Naming and referencing containers, blobs, and metadata for more information.
10. Set the level of public access to the container.
11. Select **OK** to create the container.
12. Add a parent folder inside the container.
13. Go to your blob and select **Generate SAS**. See Authorize access to data in Azure Storage.
14. Select **Signing method** > **Account key**.
15. To define **Permissions**, select the following permissions:
    - `Blob Read`
    - `Blob Write`
    - `Blob List`
    - `Blob Update`
    - `Blob Delete`
16. Review and select **Generate SAS token and URL**.

    The **Blob SAS token** query string and **Blob SAS URL** are displayed in the lower area of the window.
17. Copy and paste the **Blob SAS token** and URL values in a secure location.

    Note:

    The **Blob SAS token** is displayed once and cannot be retrieved after the window is closed.

Next steps

The external storage can now be used for as either the primary call storage folder for Media Manager or as a connector for archiving recordings:

- Configuring cloud-based storage as primary storage on page 43
- Configuring an Azure Blob Storage archiving connector on page 48

Related links

Using Azure Blob storage on page 46

Configuring cloud-based storage as primary storage

About this task

Use this procedure to configure external cloud-based storage as the primary call storage folder for Media Manager.

Before you begin

Ensure you have configured your external cloud storage and it is ready to access:

- Creating a Google Bucket for Media Manager on page 42
- Creating an Azure Blob for Media Manager on page 46
- Creating an Amazon S3 bucket for Media Manager on page 50

Procedure

1. Go to the **Configuration** view.
2. In **Call Storage Type**, select **Hosted Storage Type**.
3. In **Hosted Storage Type**, select the required external storage.
4. Enter the configuration settings as per the selected type of external storage. See Hosted Storage Type Configuration settings on page 22.
5. Click **Test Connection**.
6. Click **Save**.

Result

- All new recordings are stored in the configured external storage.

Related links

Using Google Cloud bucket storage on page 42
Using Azure Blob storage on page 46
Using Amazon S3 storage on page 50

Configuring an Azure Blob Storage archiving connector

About this task

After configuring an Azure Blob, you can use the following process to use it as a connector for archiving call recordings from the primary call storage folder.

Before you begin

Ensure you have a Blob container details and SAS token. See Creating an Azure Blob for Media Manager on page 46.

Procedure

1. Log in to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Connectors**.
3. Click **Add**.
4. Select **Microsoft Azure Blob Storage**.

5. On the Add Azure Blob Storage Connector window, in the **Name** field, type the name of the connector.
6. Add the **Name**.
7. Enter **Storage Account Name**.
8. Enter **Container Name**.
9. Enter the **Parent Folder** name.
10. Enter **SAS Token**.
11. Use the **Encrypt Recording** setting to select whether recordings should be encrypted. Note, you cannot set **Encrypt Recording** back to **NO** after saving the connector.
    - If encrypted, recordings can only be replayed from IP Office menus. Recordings are unencrypted when downloading from an IP Office menu.
    - If unencrypted, you must ensure that access to recordings in the archive complies with local data protection and privacy requirements.
12. Click **Test Connection**. If connection is successful, click **Create**. Otherwise, check and adjust the settings as required.
13. To start using the connector for archiving, select the connector from the **Active Connector** field and click **Update**.

Result

- Media Manager will regularly copy new recordings from the primary call storage folder to the archive storage.

Related links

Using Azure Blob storage on page 46

Chapter 11: Using Amazon S3 storage

Media Manager can use Amazon Simple Storage Service (Amazon S3) as storage for recordings. It can use this as its primary storage and/or as archive connector storage.

Related links

Creating an Amazon S3 bucket for Media Manager on page 50
Configuring cloud-based storage as primary storage on page 43
Configuring an Amazon S3 archiving connector on page 52

Creating an Amazon S3 bucket for Media Manager

About this task

This section provides the high-level steps to create an Amazon S3 bucket storage for Media Manager use. It can use this as its primary storage and/or as archive connector storage.

Procedure

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Select **Create bucket**.
3. In **Bucket Name**, enter a DNS compliant name for your bucket.

   Note:

   After you create the bucket, you cannot change its name. For information about naming buckets, see Bucket naming rules.
4. In **Region**, choose the AWS Region where you want the bucket to reside.
5. In **Bucket settings for Block Public Access**, select **Block Public Access** to apply to the bucket.
6. Select **Create bucket** see Creating a bucket.
7. Add resource bucket **Name** and set **Object** to **Any**.
8. Navigate to your new Amazon S3 bucket.
9. Add a parent folder in the container.

10. Create and configure IAM user policies for controlling user access to the Amazon S3 bucket. For more information, see Creating an IAM User in Your AWS account.
11. Grant group-level permissions for the Amazon S3 bucket.

    Provide access to the following bucket operations for accessing the bucket:

    - `GetObject`
    - `PutObject`
    - `DeleteObject`
    - `GetBucketLocation`
12. Use your AWS account ID or account alias, IAM username, and password to sign in to the IAM console.
13. In the navigation bar on the upper right, choose your username, and select **My Security Credentials**.
14. Expand the **Access keys (access key ID and secret access key)** section. See Managing access keys (console).
15. Click **Create New Access Key**.

    The access key includes access key IDs and secret access keys. Save the keys for configuring the Amazon S3 bucket in Media Manager.

Next steps

The external storage can now be used for as either the primary call storage folder for Media Manager or as a connector for archiving recordings:

- Configuring cloud-based storage as primary storage on page 43
- Configuring an Amazon S3 archiving connector on page 52

Related links

Using Amazon S3 storage on page 50

Configuring cloud-based storage as primary storage

About this task

Use this procedure to configure external cloud-based storage as the primary call storage folder for Media Manager.

Before you begin

Ensure you have configured your external cloud storage and it is ready to access:

- Creating a Google Bucket for Media Manager on page 42
- Creating an Azure Blob for Media Manager on page 46

- Creating an Amazon S3 bucket for Media Manager on page 50

Procedure

1. Go to the **Configuration** view.
2. In **Call Storage Type**, select **Hosted Storage Type**.
3. In **Hosted Storage Type**, select the required external storage.
4. Enter the configuration settings as per the selected type of external storage. See Hosted Storage Type Configuration settings on page 22.
5. Click **Test Connection**.
6. Click **Save**.

Result

- All new recordings are stored in the configured external storage.

Related links

Using Google Cloud bucket storage on page 42
Using Azure Blob storage on page 46
Using Amazon S3 storage on page 50

Configuring an Amazon S3 archiving connector

About this task

After configuring an Amazon S3 storage folder, you can use the following process to use it as a connector for archiving call recordings from the primary call storage folder.

Before you begin

Ensure you have an Amazon S3 container, access key, and secret key. See Creating an Amazon S3 bucket for Media Manager on page 50.

Procedure

1. Log in to **Web Manager** on the server hosting Media Manager.
2. Click **Applications** > **Media Manager** > **Connectors**.
3. Click **Add**.
4. Select **Amazon S3 Bucket**.
5. On the Add Amazon S3 Storage Connector window, in the **Name** field, type the name of the connector.
6. Enter **Bucket Name**.
7. Enter the **Parent Folder** name.
8. Enter **User Access key ID**.

9. Enter **User Secret access Key**.
10. Use the **Encrypt Recording** setting to select whether recordings should be encrypted. Note, you cannot set **Encrypt Recording** back to **NO** after saving the connector.
    - If encrypted, recordings can only be replayed from IP Office menus. Recordings are unencrypted when downloading from an IP Office menu.
    - If unencrypted, you must ensure that access to recordings in the archive complies with local data protection and privacy requirements.
11. Click **Test Connection**. If connection is successful, click **Create**. Otherwise, check and adjust the settings as required.
12. To start using the connector for archiving, select the connector from the **Active Connector** field and click **Update**.

Result

- Media Manager will regularly copy new recordings from the primary call storage folder to the archive storage.

Related links

Using Amazon S3 storage on page 50

Part 4: Recordings and Alarms

Chapter 12: Administering Recordings

The following processes can be performed by administrators who have access to Media Manager (see Configuring Media Manager Access on page 55).

Related links

Configuring Media Manager Access on page 55
Accessing the recordings on page 57
Recordings Details on page 58
Searching recordings using the search text box on page 59
Filtering the recordings displayed on page 60
Playing a call recording on page 61
Downloading recordings on page 61
Verifying authentication of call recordings on page 62
Deleting recordings on page 63

Configuring Media Manager Access

Recordings can be access at 2 levels:

Access Level	Description
System Administrators	Administrators can access and manage all recordings. They do so through the IP Office Web Manager application. • Administrators can be given access recordings and Media Manager configuration settings or to recordings only. See Providing administrator access to Media Manager on page 56.
Extension Users	Individual users can be allowed to access recordings using the User Portal application. User configuration includes setting what recordings the user can access and whether they can download recordings. See Configuring user access through the user portal on page 56.

Related links

Administering Recordings on page 55
Providing administrator access to Media Manager on page 56
Configuring user access through the user portal on page 56

Providing administrator access to Media Manager

About this task

Use this procedure to control administrator access to Media Manager. The settings are applied by the security **Rights Group** to which the administrator belongs.

Note that the settings can include permissions to access other settings and services. This section only covers the minimum necessary for Media Manager access.

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 55

Configuring user access through the user portal

About this task

Administrators can provide end users with access to recordings using the User Portal application. Refer to the Using the IP Office User Portal user guide.

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 **User Portal**.
5. Click **Enable User Portal** 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.
     - **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 unencrypted and outside the control of the Media Manager application including the audit trail. Therefore, you must on download recordings if assured that their storage and usage will continue to comply with local data protection and privacy requirements.
9. Click **Update**.

Related links

Configuring Media Manager Access on page 55

Accessing the recordings

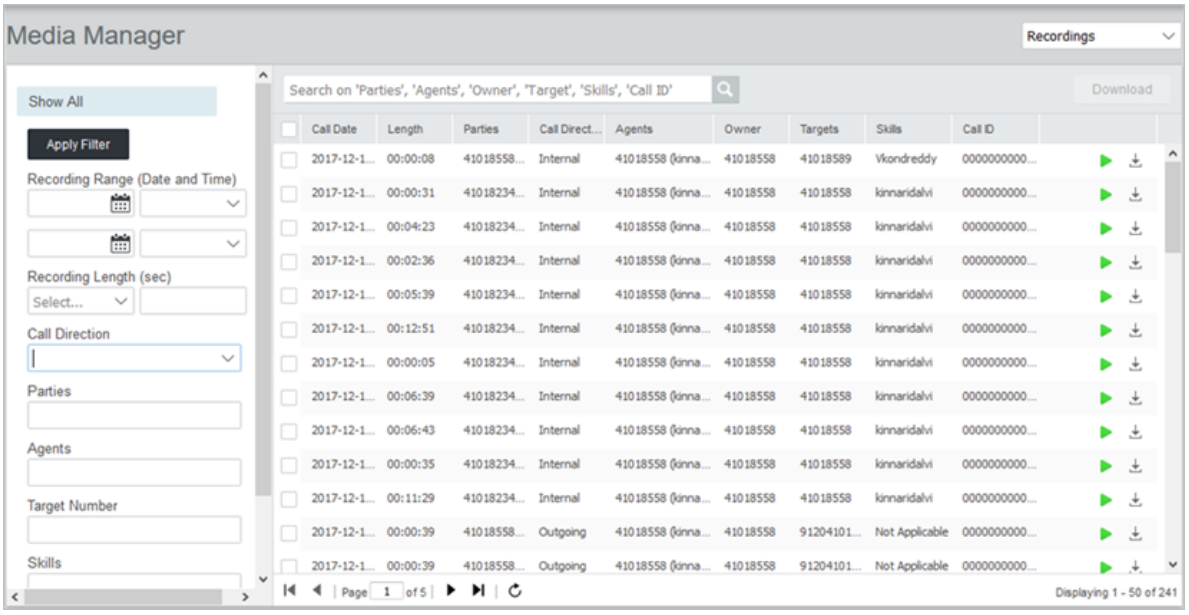
About this task

Media Manager allows administrators to use IP Office Web Manager to view details, play, delete and download.

- The recordings 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, Google Chrome and Safari browser (iOS 11 and macOS).
- Non-administrator users can access recordings using

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 58 for details.



Related links

[Administering Recordings](#) on page 55

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 62.
	Play the individual recording.
	Download the individual recording. See Downloading recordings on page 61.

Related links

Administering Recordings on page 55

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 55

Filtering the recordings displayed

About this task

When displaying recordings, you can use the search filters shown on the left to display only recordings that match your criteria.

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 60.
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 55
Filter Options on page 60

Filter Options

This following options can be used when applying a filter (see Filtering the recordings displayed on page 60) 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.
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 60

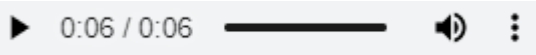
Playing a call recording

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 59 and Filtering the recordings displayed on page 60).
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 55

Downloading recordings

About this task

You can download recordings from Media Manager.

- You can only download up to 50 recordings at a time.
- The files are downloaded in `OPUS` file format.

⚠ Warning:

- Downloaded recordings are unencrypted and outside the control of the Media Manager application including the audit trail. Therefore, you must on download recordings if assured that their storage and usage will continue to comply with local 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 59 and Filtering the recordings displayed on page 60).
4. Do any one of the following:
   - To download a single recording, click the icon next to the recording.
   - 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 file includes a HTML file containing call details for each recording. When the zip file is unpacked to a folder, you can open the HTML file in a browser to see file details and playback the downloaded recordings.

Related links

Administering Recordings on page 55

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 59 and Filtering the recordings displayed on page 60).
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 55

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 59 and Filtering the recordings displayed on page 60).
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 55

Chapter 13: 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 username, date, time, and 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 64
Exporting the Audit Trail on page 65

Viewing the Audit Trail

About this task

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

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 64
Audit field descriptions on page 65

Audit field descriptions

Name	Description
Search on "User Name"	The text box to search the audit records of users. Type the username 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** and **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 64

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 64

Chapter 14: 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 18).

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 68

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

Alarms and notifications on page 67
Alarms on page 68

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**, and **Critical Alarms**.
Description	A brief description about the alarm.

Related links

Viewing alarms on page 68

Part 5: Miscellaneous

Chapter 15: Migrating recordings to different storage

You can now manually transfer the media recordings from between different primary storage options.

- You must ensure that the new storage has the same folder structure as the original storage.
- After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings from HDD to Google Cloud Bucket on page 70
Migrating recordings from HDD to Amazon S3 Bucket on page 71
Migrating recordings from HDD to Azure Blob on page 71
Migrating recordings from Google Cloud to HDD on page 71
Migrating recordings from Google Cloud to Azure Blob on page 72
Migrating recordings from Google Cloud to Amazon on page 72
Migrating recordings from Azure to HDD on page 72
Migrating recordings from Azure to Google on page 73
Migrating recordings from Azure to Amazon on page 73
Migrating recordings from Amazon to HDD on page 73
Migrating recordings from Amazon to Google on page 74
Migrating recordings from Amazon to Azure on page 74

Migrating recordings from HDD to Google Cloud Bucket

Use the following process to migrate the primary storage from HDD to Google.

1. Upload the folder to the parent folder in the bucket using Google Cloud Platform (GCP) **Upload Folder** feature.
2. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from HDD to Amazon S3 Bucket

Use the following process to migrate the primary storage from HDD to Amazon.

1. Upload <call-storage-path> folder to AWS bucket using s3 console. See Uploading objects.
2. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from HDD to Azure Blob

Use the following process to migrate the primary storage from HDD to Azure.

1. Download and set up azcopy tool to linux system to which HDD is connected. See Get started with AzCopy.
2. Copy all the media files from NAS to Azure Blob use command.**`/azcopy copy "/additional-hdd#1/*" "`**. Add your container name and SAS token to the web address for the path to work.https://byosstorage123.blob.core.windows.net/mycontainer?<SAS-Token>. For more details, see Upload files to Azure Blob storage by using AzCopy
3. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Google Cloud to HDD

Use the following process to migrate the primary storage from Google to HDD.

1. Download the folder from the bucket and add it to the desired location in the HDD
2. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Google Cloud to Azure Blob

Use the following process to migrate the primary storage from Google to Azure.

1. Follow the steps given in the documentation to authorize GCP and Azure. See Copy data from Google Cloud Storage to Azure Storage by using AzCopy
2. Copy folders inside the parent folder in Azure Blob storage container.
   - https://storage.cloud.google.com/<bucket-name>/<parent-folder-name>
   - https://<storage-account-name>.blob.core.windows.net/<container-name>
3. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Google Cloud to Amazon

Use the following process to migrate the primary storage from Google to Amazon.

1. Install AWS CLI and configure your AWS credentials in your GCP. See Installing, updating, and uninstalling the AWS CLI for installing AWS CLI and Configuring the AWS CLI to configure AWS CLI
2. Go to any instance or cloud shell in GCP.
3. Use gsutil tool and type your storage name and bucket name the following command: **`gsutil -m rsync -rd gs://<storagename> s3://<bucketname>`**.
4. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Azure to HDD

Use the following process to migrate the primary storage from Azure to HDD.

1. Download the folder from the blob and add it to the desired location in the HDD
2. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Azure to Google

Use the following process to migrate the primary storage from Azure to Google.

1. Create a SAS token for Azure Storage Account, see Use GCP Data Transfer Service import data from Azure Blob
2. Use the GCP Data transfer Service.
3. Select the source as Azure container
4. Add Storage Account Name, Container Name and SAS token.
5. Select the destination bucket.
6. Start the transfer.
7. Set the parent folder name in Media Manager configuration to the folder where the azure files are copied.
8. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Azure to Amazon

Use the following process to migrate the primary storage from Azure to Amazon.

1. Using azcopy, download the blob from azure storage to a local folder. See SAS token in the following web address for the path to work.https://mmbyos.blob.core.windows.net/mm-recording-primary?<SAS-token>.
2. Upload the folder to the AWS bucket using the S3 console.
3. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Amazon to HDD

Use the following process to migrate the primary storage from Amazon to HDD.

1. Download the folder from the bucket and add it to the desired location in the HDD
2. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Amazon to Google

Use the following process to migrate the primary storage from Amazon to Google.

1. Create a SAS token for Azure Storage Account, see Use GCP Data Transfer Service import data from Azure Blob.
2. Use the GCP Data transfer Service.
3. Select the source as Azure container
4. Add Storage Account Name, Container Name and SAS token.
5. Select the destination Bucket.
6. Start the transfer.
7. Set the parent folder name in Media Manager configuration to the folder in which the azure files are copied.
8. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Migrating recordings from Amazon to Azure

Use the following process to migrate the primary storage from Amazon to Azure.

1. Download and set up azcopy tool of Microsoft and add the command **`azcopy cp`**. See Migrate AWS S3 buckets to Azure blob storage.
2. After migrating, you must configure the new storage settings to access the recordings. See Configuring Media Manager on page 18.

Related links

Migrating recordings to different storage on page 70

Chapter 16: 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. 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. 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 the 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 connectors, Media Manager adds a time stamped name to the migrated connectors. The name is in the format `MigratedX-Timestamp`.

Migrating multiple times

Normally, migration is 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 can perform 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. Migrated connectors are deleted unless they have already been renamed.

Availability of Contact Recorder features in Media Manager

Feature	Description	Contact Recorder	Media Manager
Search by administrator	Search by administrators using Target Number, Skills, Agent, and Call ID	✓	✓
Search through Web Self-Admin	Search by users using the search filters Target Number, Skills, Agent, and Call ID	✓	✓
Web Self-Admin search results	A maximum of 100 results are displayed.	✓	✓

Table continues…

Feature	Description	Contact Recorder	Media Manager
Call sets	Facility to save search results for retrieving in the future.	✓	×
Email	Attaching recordings to emails.	✓	×
Bulk Export	Exporting multiple recordings and the related details	✓	✓ Maximum 50 calls at a time.
Owner	Available as a search option.	×	✓
Audit Trail	Available for tracking the use of recordings.	✓	✓
Windows Domain Authentication	-	✓	×

Related links

Migration limitations on page 76
Migration prerequisites on page 77
Initiating Contact Recorder migration on page 77

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 75

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 16.
- 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 75

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

- The **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 75

Part 6: Further Help

Chapter 17: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 80
Getting Help on page 80
Finding an Avaya Business Partner on page 81
Additional IP Office resources on page 81
Training on page 82

Additional Manuals and User Guides

The Avaya Documentation Center website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the Avaya IP Office™ Platform Manuals and User Guides document.
- The Avaya IP Office Knowledgebase and Avaya Support websites also provide access to the IP Office technical manuals and users guides.
  - Note that where possible these sites redirect users to the version of the document hosted by the Avaya Documentation Center.

For other types of documents and other resources, visit the various Avaya websites (see Additional IP Office resources on page 81).

Related links

Additional Help and Documentation on page 80

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See Finding an Avaya Business Partner on page 81.

Related links

Additional Help and Documentation on page 80

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the Avaya Website at https://www.avaya.com
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

Additional Help and Documentation on page 80

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 80), there are a range of website that provide information about Avaya products and services including IP Office.

- Avaya Website (https://www.avaya.com)

  This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- **Avaya Sales & Partner Portal** *(*https://sales.avaya.com*)*

  This is the official website for all Avaya business partners. The site requires registration for a user name and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- **Avaya IP Office Knowledgebase** *(*https://ipofficekb.avaya.com*)*

  This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- **Avaya Support** *(*https://support.avaya.com*)*

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

- **Avaya Support Forums** *(*https://support.avaya.com/forums/index.php*)*

  This site provides forums for discussing product issues.

- **International Avaya User Group** *(*https://www.iuag.org*)*

  This is the organization for Avaya customers. It provides discussion groups and forums.

- **Avaya DevConnect** *(*https://www.devconnectprogram.com/*)*

  This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

- **Avaya Learning** *(*https://www.avaya-learning.com/*)*

  This site provides access to training courses and accreditation programs for Avaya products.

Related links

Additional Help and Documentation on page 80

Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website.

Related links

Additional Help and Documentation on page 80

Index

A

account code 30
additional hard drive 16
administrative access
providing 56
Administrator 80
alarms 68
about 67
viewing 68
Amazon
Migrate to Azure 74
Migrate to Google 74
Migrate to HDD 73
amazon S3
archiving 52
Amazon S3 Bucket 12
APIs 81
Application Notes 81
architecture 9
Archival Solution 16
archiving
Amazon S3 50
azure blob 46
BYOS 46, 50
dvd 36
Google cloud bucket 42
google drive 40
nas 38
audit
field descriptions 65
audit trail 64
exporting 65
viewing 64
Azure
Migrate to Amazon 73
Migrate to Google 73
Migrate to HDD 72
azure blob
archiving 48
Azure Blob 12

B

business partner locator 81
BYOS 12
archival storage 44

C

call storage
configuration 22
Capacity 10
Centralized Media Manager 16
changing 26
Cloud-based storage 12
configuration 20
settings 22
configure
account code recording 30
hunt group recording 28
incoming call route recording 29
user auto recording 27
user manual recording 27
configuring 25
amazon blob 52
archival storage 44
azure blob 48
recording display 26
connector 34
adding 33
adding NAS 38
delete 35
modifying 34
contact recorder 75, 77
Contact Recorder 13
contact recorder database 75
courses 81
creating
amazon S3 bucket 50
azure blob 46
Google bucket 42

D

database
about backup and restore 12

E

encryption 12
external calls 29

F

filter 60
filters 60
forums 81

G

Google
Migrate to Amazon 72
Migrate to Azure 72
Migrate to HDD 71

Google bucket 42
google drive
adding as a connector 41
creating 40
group 28

H

HDD
Migrate to Amazon 71
Migrate to Azure 71
Migrate to Google 70
Help 80
hunt group 28

I

incoming call route 29

L

license
verify 15
verifying through web manager 15
voicemail pro 15
licensing 14
limitation 76
Local Media Manager 16

M

Manuals 80
Media Archival Solution 16
media manager 14, 20, 58, 60, 68
accessing 11
configuration 18
configuring the application server 19
overview 8
starting the service 18
Media Manager 34
Centralize 16
Local 16
migrate
Amazon to Azure 74
Amazon to Google 74
Amazon to HDd 73
Azure to Amazon 73
Azure to Google 73
Google to Amazon 72
Google to Azure 72
HDD to Amazon 71
HDD to Azure 71
HDD to Google 70
primary storage 70
migrating 77
migration 75–77
migration *(continued)*
Azure to HDD 72
Google to HDD 71

P

prerequisites 77
primary storage
cloud-base storage 43, 47, 51

Q

Quick Reference Guides 80

R

Recording size 10
recording time 26
recording warning 25
recordings 58
accessing 57
deleting 63
downloading 61
play 56
playing 61
searching using search box 59
verifying authentication 62
vrla 62
Reseller 80
resilience 11

S

sales 81
SDKs 81
self-administration 56
support 81
System Administrator 80

T

Technical Bulletins 81
training 81, 82

U

user
auto record 27
manual recording 27
User Guides 80
user portal 56

V

viewing

viewing *(continued)*
audit trail 64

W

websites 81