Webex WFO Design and Installation Guide

For Deployments with New WFM

First Published: July 20, 2021
Last Updated: January 14, 2022

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0882

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Introduction

The *Webex WFO Design and Installation Guide* provides a high-level overview of the structure and components of Webex WFO in the Cloud, and it explains how to install Webex WFO in a cloud environment. For more specific details on supported integrations see the available integration guides.

The guide is designed for Cisco implementation and support engineers, Cisco sales engineering employees, partners, and customers; however, Cisco development, marketing, sales, and other employees across the organization could also find it useful.

Localization and supported languages

Different components of Webex WFO support different languages. Language support applies to these elements:

- User interface
  - QM, WFM, Analytics, and Data Explorer
- Documentation
  - Online help
  - PDF guides
- Analytics
  - Phonetics: speech analytics, predictive evaluation scores, and predictive net promoter scores
  - Transcription: speech to text
  - Sentiment
  - Text: analytics for chat, email, agent notes, and social media

Components of Webex WFO are available in these languages.

			Analytics Transcription		**Analytics Phonetics**			
Language	**UI**	**Mobile App**	**Core**	**Sentiment**	**Core**	**Predictions**	**Text Analytics ***	**Documentation**
Simplified Chinese (zh)	x	x						
Traditional Chinese (zh-TW)	x	x						

Language	UI	Mobile App	Analytics Transcription		Analytics Phonetics		Text Analytics *	Documentation
			Core	Sentiment	Core	Predictions		
Danish (da)	x	x					x	
Dutch (nl)	Limited				x	x	x	
English (en)	x	x	x	x	x	x	x	x
Australian English (en-AU)			x				x	
UK English (en-GB)			x	x	x **	x **	x	
US English (en-US)	x	x	x	x	x	x	x	x
Finnish (fi)	x	x					x	
French (fr)	x	x			x **	x **	x	
Canadian French (fr-CA)	x	x	x		x	x	x	
German (de)	x	x					x	
Italian (it)	x	x					x	
Japanese (ja)	x	x						
Korean (ko)	x	x						
Norwegian (nb)	x	x					x	

Language	UI	Mobile App	Analytics Transcription		Analytics Phonetics		Text Analytics *	Documentation
			Core	Sentiment	Core	Predictions		
Polish (pl)	Limited						x	
Portuguese (pt)	x	x					x	
Brazilian Portuguese (pt-BR)	x	x			x **	x **	x	
Russian (ru)	Limited	x						
Spanish (es)	x	x					x	
Mexican Spanish (es-MX)			x		x	x	x	
Swedish (sv)	x	x					x	

* Text analytics is available for all languages that use Western characters.

** Supported per the capabilities of the current model. No additional model support.

Adding additional languages or expanding current offerings from limited to fully supported requires collaboration with Cisco. Contact your account representative for more information.

Overview

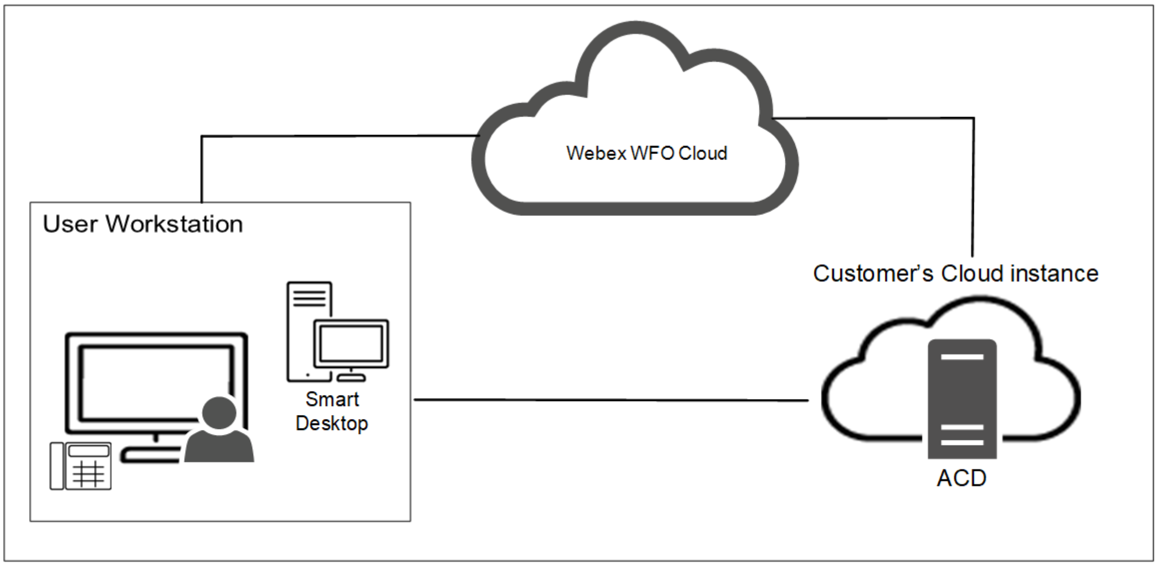
The entire Webex WFO Suite is hosted in the Cloud, which is powered by Amazon Web Services and Microsoft Azure. Data moves between Webex WFO Cloud, user workstations, and your organization's ACD.

Webex WFO supports two general types of Cloud deployment models. Your Cloud ACD design model may fit either of the two categories detailed below depending on the ACD your organization has integrated with Webex WFO. Those two models are Contact Center as a Service (CCaaS) and customer-hosted ACDs.

The information found in the *Webex WFO Cloud Design and Installation Guide* is applicable to both Cloud models unless specifically stated.

CCaaS Deployment Model

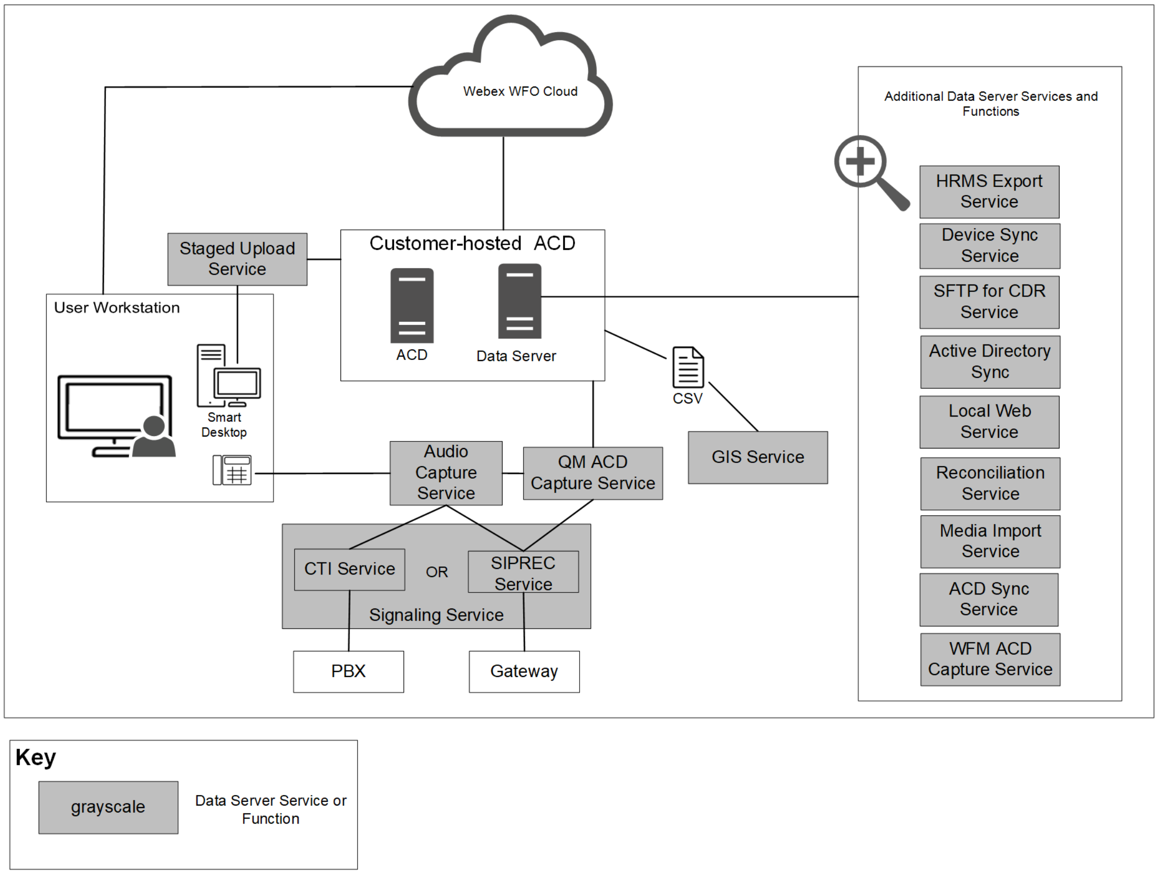
CCaaS deployment models allow for the CCaaS provider to host ACD services and infrastructure in the Cloud. This can reduce the cost of operating technology and support cases. Find out more specific details on this model in the topics on Port Usage and Storage.



Customer-hosted ACD Deployment Model

With customer-hosted ACDs, the ACD infrastructure lives on the customer site along with a Webex WFO Data Server that is used to pass data to and from the customer-hosted ACD. The Webex WFO Data Server and customer-hosted ACD then passes that data to Webex WFO Cloud. Find out more specific details on this model in the topics on Port Usage, Edge Components, and Storage.

> **NOTE** In the diagram below, the ACD, PBX, and Gateway devices are supplied by the customer. These devices connect to different components of the Webex WFO product, but they are not part of the Webex WFO product.



Authentication Overview

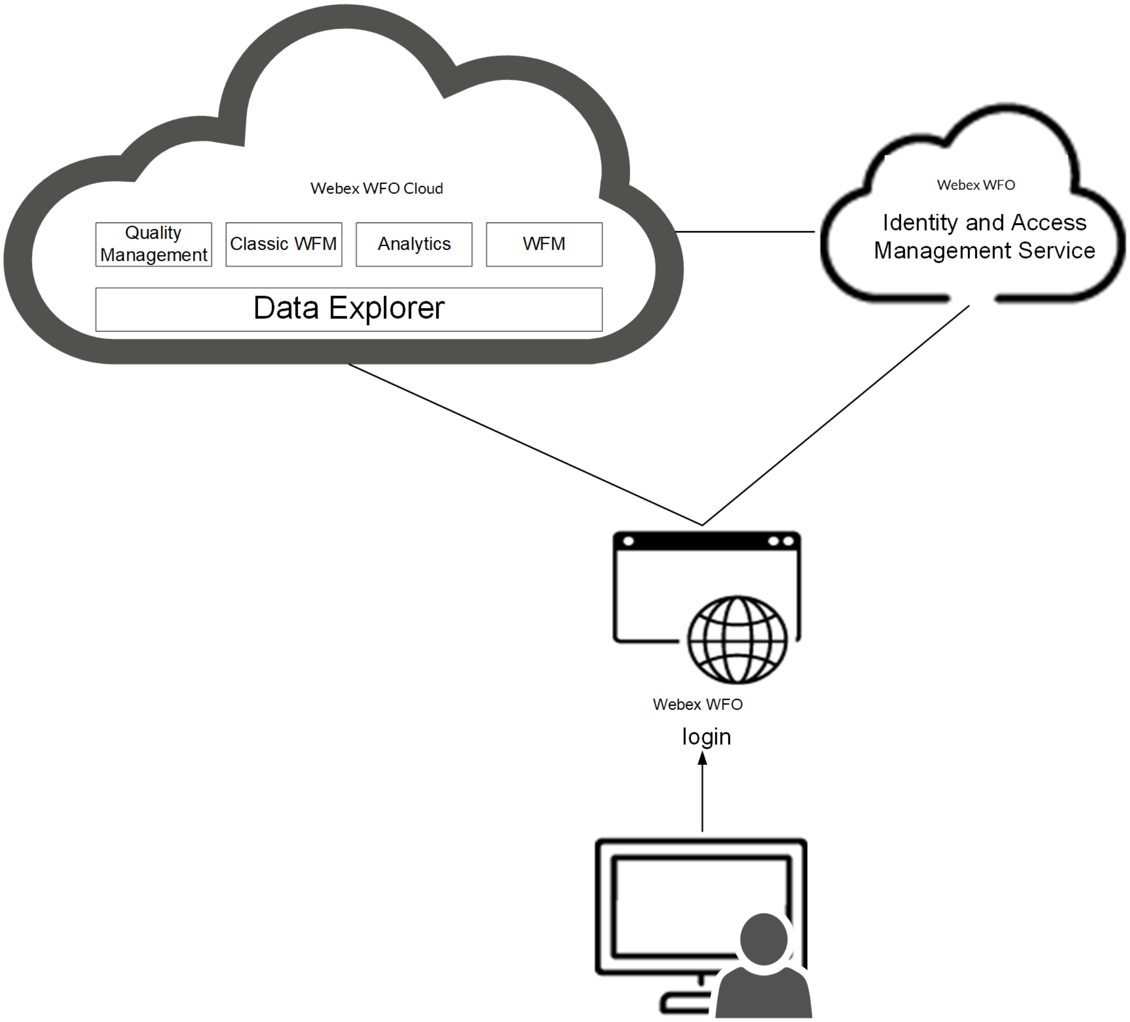
Authentication verifies the identity of anyone who connects to Webex WFO. Webex WFO allows two methods of authenticating users in the system. These methods are the Webex WFO default authentication and single sign-on using Security Assertion Markup Language (SAML). When users login, they go through the Webex WFO Identity and Access Management (IAM) authentication service. After Cisco authenticates the user, the user can access all areas of the Webex WFO Suite based on their permissions.

All authentication of known user identities is managed by the Webex WFO IAM service. Authorization is handled by your Webex WFO products. When using SAML, Webex WFO acts as the service provider (resource server) and the customer’s identity provider (IdP) is used to connect the user to Webex WFO Cloud. A user must exist in Webex WFO to log in with the customer's identity provider.

Authentication Process Flow

Steps in the authentication process

1. A user accesses Webex WFO. If they have a session they proceed to Webex WFO. If not, they are redirected to the Webex WFO IAM authentication service.
2. If the user has a session in the Webex WFO IAM authentication service, they are immediately redirected back to Webex WFO where Webex WFO establishes a session for the user.
3. If the user did not have a Webex WFO IAM authenticated session, they are prompted to enter their email address.
4. Assuming the email address belongs to only one Webex WFO user, the user is either redirected to the customer's IdP via SAML, or the user is prompted to enter their password in the Webex WFO IAM authentication service depending on how authentication has been configured by the customer.
5. When the user has successfully authenticated they are prompted to select a tenant if they belong to more than one, or they are immediately redirected back to Webex WFO where a session is created.


Webex WFO Cloud
Quality Management
Classic WFM
Analytics
WFM
Data Explorer
Webex WFO
Identity and Access Management Service
Webex WFO
login

System Requirements

Webex WFO Release Notes contain the latest information regarding changes to system requirements, compatibilities, bug-fixes, and new features. Archives of past Release Notes are available.

Browsers

Webex WFO is accessed over the internet, using modern versions of Chrome, Edge, or Firefox web browsers and remote desktops. Every user needs a unique email address that becomes their username.

Network bandwidth

Generated audio media data that is uploaded to Webex WFO for processing and storage requires network bandwidth availability. To ensure no interruption to uploads, voice communications, or any other customer applications, it is highly recommended that you calculate your estimated bandwidth consumption based on the formulas below and understand how this will impact your network.

- Recording time = (# of users) × (# of calls per user per day) × (avg call length (minutes))
- Upload bandwidth = audio recordings = 0.48 MB × recording time
- Screen upload bandwidth is 1.5 MB a minute per monitor.

Miscellaneous requirements

Supported Environments

Webex WFO supports a number environments and technologies.

For the latest supported compatibility information, visit www.cisco.com.

Desktop Software

.NET Framework

Webex WFO Smart Desktop requires .NET Framework 4.5 for the Analytics feature. If it is not installed, Webex WFO will not be able to capture browser events as part of the Desktop Analytics data. You can download the .NET Framework from http://www.microsoft.com/en-us/download/details.aspx?id=30653.

WebM Media Foundation Components

Webex WFO requires the WebM Media Foundation Components installed on the desktop. This codec allows you to play back audio and screen recordings in WebM format.

You can download WebM Video from https://tools.google.com/dlpage/webmmf/.

Browsers

Any browser you use must allow file downloads. Popup blockers must be disabled.

Desktop Analytics Plugin/Extension

Users who administer fields for Desktop Analytics via the Field Manager page in Webex WFO and agent desktops that have Smart Desktop installed must have the Cisco Analytics browser extension/plugin enabled. The plugin is required not only for marking fields in the browser but also for monitoring agent web activity within the browser.

Enable the Desktop Analytics extension in Internet Explorer

The Desktop Analytics plugin is automatically installed and enabled when Smart Desktop is installed. No further action is required.

> **NOTE** When agents are using Internet Explorer, the Desktop Analytics Plugin/Extension will not capture field-level events on pages that render in document modes before Internet Explorer 8.

Enable the Desktop Analytics extension in Firefox

The first time you log in to Webex WFO using Firefox, you see a dialog box telling you to install the Calabrio Browser Extension. Select **Allow this installation** and click **Continue**. No further action is required.

Enable the Desktop Analytics plugin in Microsoft Edge Chromium

In Edge Chromium, go to https://chrome.google.com/webstore/detail/calabrio-analytics-plugin/hecgknieibccghjmmhhckdfeobjoffdf and click **Add to Chrome**.

> **NOTE** The plugin does not support Internet Explorer compatibility mode.

Enable the Desktop Analytics plugin in Chrome

Download and install the Calabrio Analytics Plugin, version 0.2.0.2. The plug-in is located at:

https://chrome.google.com/webstore/detail/calabrio-analytics-plugin/hecgknieibccghjmmhhckdfeobjoffdf

> **NOTE** If clicking the link does not work, copy the URL and paste it into your browser.

Adobe Acrobat Reader

The Adobe Reader is required to open exported PDF files and user documentation. A free Acrobat Reader download is available at www.adobe.com.

> **IMPORTANT** There are known issues with Adobe Reader versions that use the Security (Enhanced) feature. If you plan to use the Desktop Analytics feature, you must navigate to **Security (Enhanced)** under **Preferences** in Adobe Reader, clear the **Enable Protected Mode at startup** and **Enhanced Security** check boxes, click **Yes** for any warning messages, and then click **OK** to save your changes. When finished, restart Adobe Reader for the changes to take effect. If Adobe Reader is not configured correctly, Desktop Analytics will not be able capture events related to Adobe Reader.

Desktop Software and Audio Capture

In order for Smart Desktop to perform proper phone detection and audio capture, the ability to detect and capture certain network protocols (such as SIP, SCCP and RTP) is required. Any software running on the PC that interferes with, redirects, or otherwise hides network traffic will cause Smart Desktop to fail to function correctly.

> **EXAMPLE** The SonicWall VPN client with the Deterministic Network Enhancer (DNE) lightweight filter enabled causes outgoing network traffic to be redirected from the network adapter that Smart Desktop uses. In this case the DNE lightweight filter must be disabled to allow Smart Desktop to function correctly.

PCI DSS Compliance

> **NOTE** Webex WFO v10.3 and higher supports TLS v1.2 and has deprecated TLS v1.1.

File encryption

Media and data are encrypted for security purposes. Webex WFO uses a key to decrypt the recorded customer conversations. The encryption key is located in the database. Each tenant has its own encryption key. Encryption keys can be updated.

Password policy

Password complexity requirements

Passwords must conform to the following rules.

- Must be a minimum of 8 characters.
- Must contain at least one of each of the following.

  Uppercase letters
  Lowercase letters
  Numbers 0-9
  Special characters ! # $ % & ( ) , . / : ; = ? @ ^ ` |

- Cannot contain your name or email address.

NOTE Passwords do not expire.

Port usage

The port requirements for the Webex WFO edge components and optional Webex WFO Data Server components are listed below.

Generally, port 80 and port 443 to a web server need to be open to connect to Webex WFO for all cloud integrations with Webex WFO. Exact port requirements vary depending on your cloud deployment model.

Edge components:

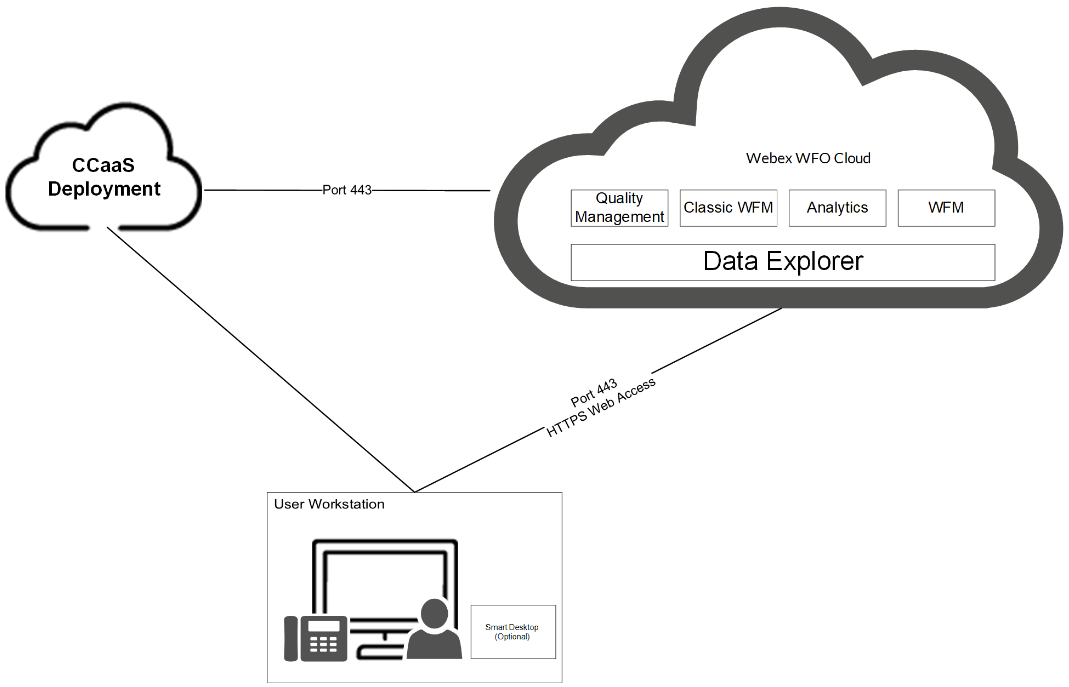
- Smart Desktop

Data Server components:

- Data Server—ACD Sync: CCaaS Integrations
- Data Server—ACD Sync: CUCM Network Recording
- Data Server—ACD Sync: Cisco Unified Contact Center Enterprise (Unified CCE)
- Data Server—ACD Sync: Cisco Unified Contact Center Express (Unified CCX)
- Data Server—GIS
- Data Server—Record/Capture
- Data Server—Signaling: CTI
- Data Server—Signaling: CTI, Cisco Unified Communications Manager Network Recording
- Data Server—Signaling: SIPREC

CCaaS ports

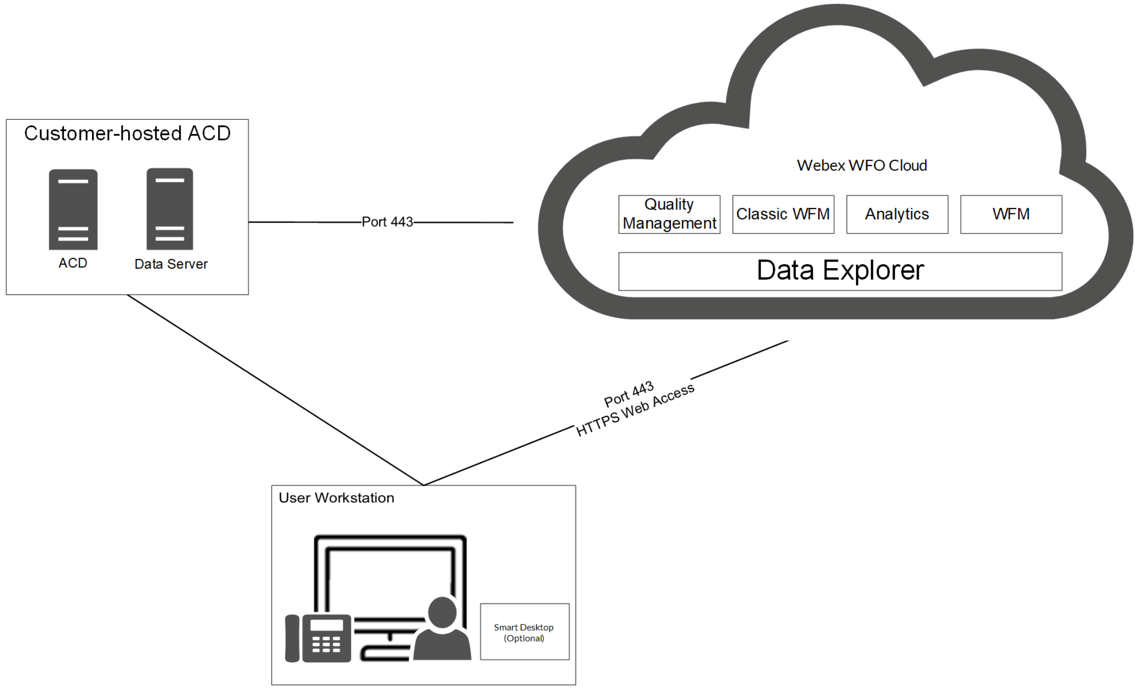
CCaaS deployment model integrations require port 443 to be open. Port 80 requests are redirected to 443 as HTTPS requests.



Customer-hosted ACD ports

Customer-hosted deployment model integrations require port 443 to be open. Port 80 requests are redirected to 443 as HTTPS requests.

In addition to ports 80 and 443, customer-hosted ACD deployment integrations also require port 1433 to be open. Port 1433 allows for a connection to a SQL database.



Edge components

Port	Use	Source	Destination	Notes
Smart Desktop				
UDP 49152–65535	Live audio monitoring—RTP Live screen monitoring—RDP stream	Agent's PC	Supervisor's browser	—
TCP 52102	Communication between Cisco CTI data servers and SDC	Smart Desktop	Data Server	

Data Server components

Port	Use	Source	Destination	Notes
Data Server—ACD Sync: CCaaS Integrations				
TCP 443	Communication between CCaaS integrations and the following settings on the Data Server: Regional Data Server ACD Capture Settings, Recording CTI Signaling Server Settings, and Regional Data Server ACD Capture Settings	—	—	—
Data Server—ACD Sync: CUCM Network Recording				
TCP 22	Communication between both the SFTP Configuration and the Regional Data Server Reconciliation Settings on the Data Server and the CUCM Billing Service	CUCM Billing Service	SFTP, Data Server	—
TCP 8443	Communication between CUCM AXL and Regional Data Server ACD Sync Settings on the Data Server	CUCM AXL	Data Server	—
Data Server—ACD Sync: Cisco Unified CCE				
TCP 1433 TCP 1434	Communication between the Cisco Unified CCE AW SQL Server Database and the Regional Data Server ACD Sync Settings on the Data Server	Cisco Unified CCE AWDB SQL Server Database	Data Server	—
TCP 1433 TCP 1434	Communication between the Cisco Unified CCE HDS SQL Server Database and both the Regional Data Server Reconciliation Settings	Cisco Unified CCE HDS SQL	Data Server	—

Port	Use	Source	Destination	Notes
	and the Regional Data Server ACD Capture Settings on the Data Server	Server Database		
TCP 42027	Communication between the Cisco Unified CCE CTI Service (Side A) and the Recording CTI Signaling Server Settings on the Data Server	Cisco Unified CCE CTI Service (Side A)	Data Server	Side A default if using PG1. Ports will vary based on what PG you are using. The CTI Server Port configured in the Unified CCE ACD Configuration.
TCP 43027	Communication between the Cisco Unified CCE CTI Service (Side B) and the Recording CTI Signaling Server Settings on the Data Server	Cisco Unified CCE CTI Service (Side B)	Data Server	Side B default if using PG1. Ports will vary based on what PG you are using. The CTI Server Port configured in the Unified CCE ACD Configuration.
Data Server—ACD Sync: Cisco Unified CCX				
TCP 1504	Communication between the Unified CCX Informix Database and both the Regional Data Server ACD Sync Settings and the Regional Data Server ACD Capture Settings	Data Server	Unified CCX Informix Database	—
TCP 12028	Communication between the Cisco Unified CCX CTI Service (Side A) and the Recording CTI Signaling Server Settings on the Data Server	Cisco Unified CCX CTI Service (Side A)	Data Server	Side A Default. This is the RMCM TCP port configured in Unified CCX System Parameters. The CTI Server Port configured in the Unified CCX ACD Configuration.
TCP 12028	Communication between the Cisco Unified CCX CTI Service (Side	Cisco Unified	Data Server	Side B Default. This is the RMCM

Port	Use	Source	Destination	Notes
	B) and the Recording CTI Signaling Server Settings on the Data Server	CCX CTI Service (Side B)		TCP port configured in Unified CCX System Parameters. The CTI Server Port configured in the Unified CCX ACD Configuration.
Data Server—GIS				
—	—	—	—	While GIS does not directly listen on a port, the files need to be copied over to the Data Server. If the copying is done via FTP, port 20 and 21 are used.
Data Server—Record/Capture				
UDP 39500–43500	Recording RTP	Phone or voice gateway	Record Server	—
UPD 49152–65535	Live audio monitoring—RTP	Record Server	Supervisor's browser	—
Data Server—Signaling: CTI				
TCP 443	Signaling Server	Signaling Server	Cisco API	—
TCP 52102	Recording Signaling	Record Servers or Smart Desktop clients	Signaling Server	—

Port	Use	Source	Destination	Notes
TCP 52103	Hazelcast	Signaling Server partner	Signaling Server	—
Data Server—Signaling: CTI, Cisco Unified Communications Manager Network Recording				
TCP 2748	JTAPI signaling	Signaling Server	Unified CM publishers and subscribers	—
TCP 5060 UDP 5060	SIP signaling from Unified CM	Any Unified CM publisher or subscriber	Signaling Server	Not secure
TCP 5060	Signaling Server	primary Signaling Server	secondary Signaling Server	Bidirectional
TCP 5061	Secure SIP signaling from Unified CM	Any Unified CM publisher or subscriber	Signaling Server	Secure. Typically used only when system is configured for SRTP.
Data Server—Signaling: SIPREC				
TCP 443	Cisco API queries	Signaling Server	Cisco API	—
TCP 5060 UDP 5060	SIP signaling from gateway	Gateway	Signaling Server	—

Port	Use	Source	Destination	Notes
TCP 59106	Recording signaling	Record Servers	Signaling Server	—
TCP 59107	Hazelcast	Signaling Server partner	Signaling Server	—

About Storage

It’s important to note the difference in required storage type in Webex WFO.

Media storage is the permanent storage for media files. It is suitable for long-term storage, and it is not used for playback unless high speed network storage is also configured to use the same location. See Media File — Standard Storage and Media File — Archival Storage to learn more.

High Speed Network Storage refers to the high speed network used for storage of temporary files, folder location where all operational processing takes place, and where analytics (Lucene) data is stored. This includes bulk export processing, the Lucene index location, media conversion, media playback, and files that are deleted after 24 hours by the system throughout the day with the exception of analytics.

> **NOTE** Analytics files are stored in high speed network storage but are not included in the deletion of files by the system throughout the day.

When a call is requested for playback, the system pulls the file from permanent storage and places it in the temporary directory within the High Speed Network Storage level for instant access (see High Speed Network Storage). From there, it performs transcoding and streaming.

Storage Types

One consideration your organization should make prior to installing Webex WFO is whether to use network-attached storage (NAS), storage area network (SAN), or a file server as your storage type.

> **BEST PRACTICE** Before any tenants are created, ensure you have a SAN or a file server that is to be used for high speed network storage. NAS devices should not be used. NAS devices are not intended for fast delivery of data and likely have more traffic on the device. Customers should use a SAN, but a file server in close proximity to platform servers, as in the same data center, is also acceptable as the high speed network storage location.

High speed network storage ideally should be a SAN or other device intended for fast access.

NAS and SAN were developed to solve the problem of making stored data available to many users at once. Each provides dedicated storage for a group of users, but they use different approaches to achieving their mission.

NAS is a single storage device that serves files over an Ethernet connection and is relatively inexpensive and easy to set up.

SAN is a tightly coupled network of multiple devices that work with block-based data and is more expensive and complex to set up and manage. From a user perspective, the biggest difference between NAS and SAN is that NAS devices look like volumes on a file server and use protocols like NFS and SMB/CIFS, while SAN-connected disks appear to the user as local drives.

Admin Configuration

When configuring the system for the first time, the **Default Media Storage Location** is configured on the System Administrator Storage Location page.

> **NOTE** During initial setup the **Default Media Storage Location** is your high speed network storage and media storage location. Further action is needed to separate high speed network storage and media storage to different locations. Network and media storage locations have drastically different performance characteristics. This is why selecting both options as the default storage location is not recommended because it can lead to performance issues.

Configure Separate Network and Media Storage Locations

1. Before creating any tenant, navigate to the System Administrator portal > Application Management > System Configuration > Storage Location.
2. Click **Create a new storage location**.
3. To create a high speed network storage location, enter a unique name in the **Name** field.
4. In the Type drop-down list, select **Network (Instant Access)**.
5. Under **Defaults**, select the **Network** check box.
6. Configure the remaining **Network Storage Configuration** fields.
7. Click **Save**.
8. To create a media storage location navigate back to Application Management > Storage Location.
9. Click **Create a new storage location**.
10. To create a media storage location, enter a unique name in the **Name** field.
11. In the Type drop-down list, **Network (Instant Access)** is pre-selected.
12. Under **Defaults**, select the **Media** check box.
13. Configure the remaining **Network Storage Configuration** fields.
14. Click **Save**.

BEST PRACTICE Delete the initial **Default Media Storage Location** after the new locations for Network and Media storage are configured.

Configure Tenant Storage

Conduct this procedure when creating a new tenant from the System Administrator portal.

1. Navigate to Application Management > Tenant Administration > Tenants.
2. Within the Storage Location section, find the default high speed network storage location and select the **Available** check box.
3. Find the default media storage location and select the **Available** check box and **Default** check box.
4. Click **Save**.
5. To validate, log in to the tenant and navigate to Application Management > System Configuration > Storage Profiles.
6. Click the **Storage Location** drop-down list. The network and media storage locations appear in the drop-down list.

   NOTE Do not choose Network storage for a storage profile.

Storage levels

There are three levels of storage for contact data:

- Amazon S3 (Immediate Access) — Amazon S3 storage (standard) is used for shorter-term storage (12–24 months) of day-to-day operational content, such as media files (voice and screen) and historical data for reporting, forecasting, and scheduling. The response rates to user requests can be near immediate in seconds, yet can vary slightly depending on the amount of data or the type of data being requested.
- Amazon S3 Shared (Immediate Access) — Similar to the Amazon S3 storage level except multiple tenants store their data within the same Amazon S3 storage bucket in a tenant specific folder.
- Network (Instant Access) — Network storage (performance) is used for user-driven media content, Analytics, and Datamart content. This is a storage area network (SAN) or a file server. It provides a near-immediate response rate to user requests. This data is resident for a workflow-defined period of time, after which it is purged. Optionally, administrators can specify a staged upload location, which holds data before uploading it to the long-term real-time data storage location.

NOTE Amazon S3 storage is not recommended for on-premise deployments of Webex WFO.

You can also choose to have a third party store your data after it has reached the end of its retention period. After the data is stored, it is purged from Webex WFO. When you retrieve stored data, you must use applications other than Webex WFO to review it.

High Speed Network Storage and Media Storage

Comparison

The following table describes the main differences between High Speed Network Storage and Media Storage. NAS has many similarities to Webex WFO Media Storage. SAN has many similarities to Webex WFO High Speed Network Storage.

NAS	SAN
Typically used in homes and small to medium sized businesses.	Typically used in professional and enterprise environments.
Less expensive	More expensive
Easier to manage	Requires more administration
Data accessed as if it were a network-attached drive (files)	Servers access data as if it were a local hard drive (blocks)
Speed dependent on local TCP/IP usually Ethernet network, typically 100 megabits to one gigabit per second. Generally slower throughput and higher latency due to slower file system layer.	High speed using Fibre Channel, 2 gigabits to 128 gigabits per second. Some SANs use iSCSI as a less expensive but slower alternative to Fibre Channel.
I/O protocols: NFS, SMB/CIFS, HTTP	SCSI, iSCSI, FCoE
Lower-end not highly scalable; high-end NAS scale to petabytes using clusters or scale-out nodes	Network architecture enables admins to scale both performance and capacity as needed
Does not work with virtualization	Works with virtualization
Requires no architectural changes	Requires architectural changes
Entry level systems often have a single point of failure, e.g. power supply	Fault tolerant network with redundant functionality
Susceptible to network bottlenecks	Not affected by network traffic bottlenecks.

NAS	SAN
	Simultaneous access to cache, benefiting applications such as video editing.
File backups and snapshots economical and schedulable.	Block backups and mirrors require more storage.

The main differentiators between NAS and SAN are that NAS is slower, has a lower throughput, and higher latency. NAS is generally less expensive and simpler. NAS is also used for simple file storage and media retrieval, and it is connected via HTTP, LAN/WAN, etc.

Compared to NAS, SAN is faster and based on a network of pooled storage devices. SAN is generally more expensive, and is used for high transaction areas such as databases and web servers/processing. Unlike NAS, SAN is connected via iSCSI.

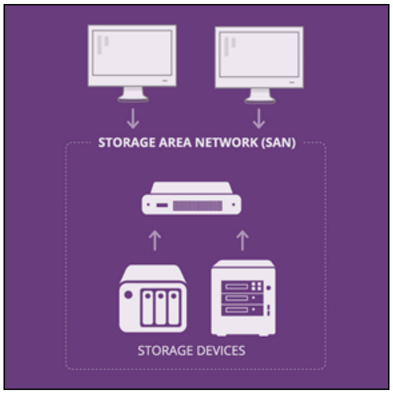
Webex WFO Storage Types

High Speed Network Storage

High Speed Network Storage characteristics are very similar to a Storage Area Network (SAN).

- High IOPS
- Low Latency
- High Performance Drives
- High Transactions and Response Rates required

In Webex WFO High Speed Network Storage is used for the Microsoft SQL database and Analytics Lucene database.

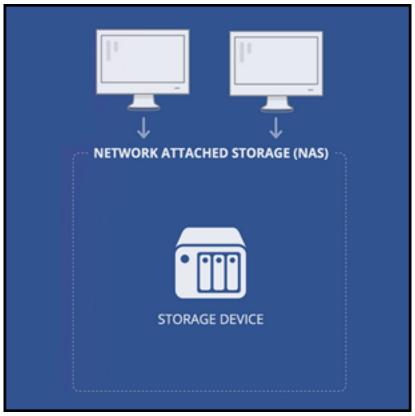


Media Storage

Media file standard storage characteristics are very similar to network attached storage (NAS).

- Simple to Setup
- Less Expensive
- Looks like a standard local drive to the user
- Similar to a File Server for files and media

In Webex WFO Media Storage is used for audio and screen files.



Storage Diagrams

Use Cases for Diagram Process Flows

1. Process flow to record and upload a recording from a client.

   The client can be a server or an agent PC.

2. Process flow to playback files.

3. Process flow to export files.

4. Process flow to analyze files.

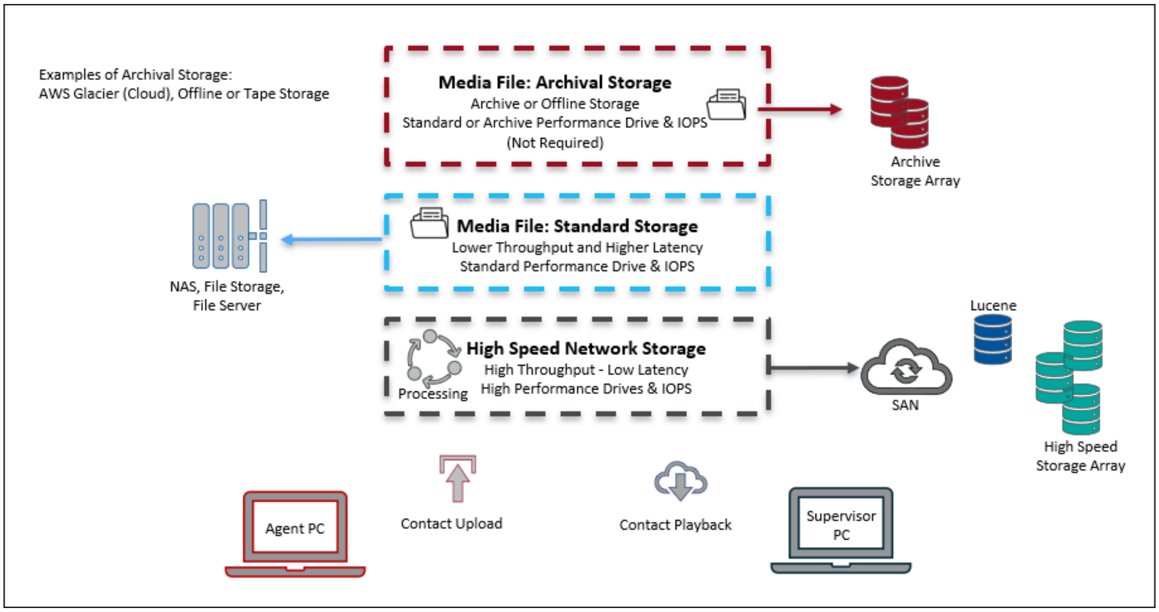
5. Temporary file characteristics (Self-Cleaning).

   Files are stored for 24 hours on high speed network storage and then they are deleted.

Webex WFO Storage Types

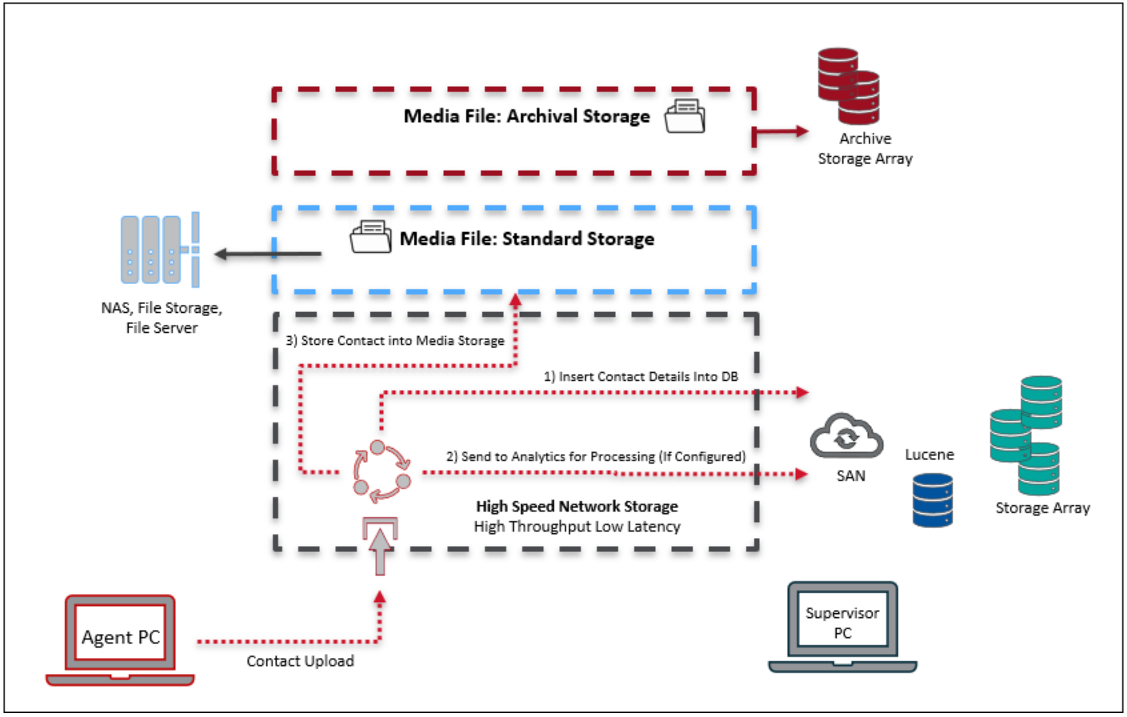
The following diagram depicts recommended storage by data type.

IMPORTANT High Speed Network Storage and Media File Storage locations require different types of storage performance and should never be configured on the same storage drive.

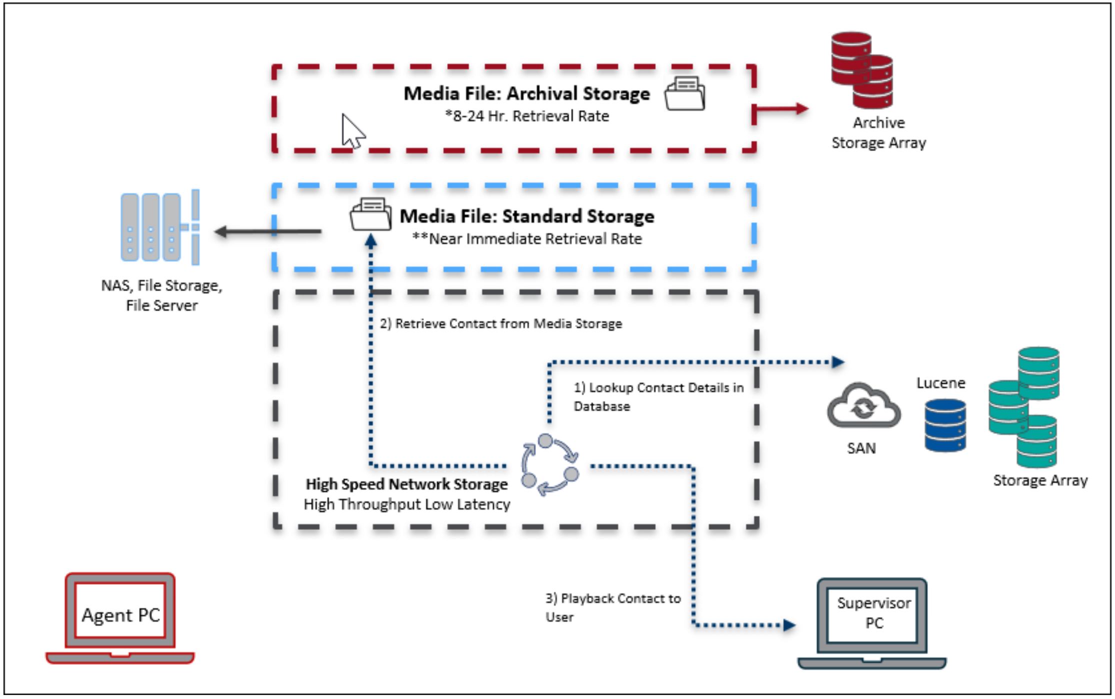

Examples of Archival Storage:
AWS Glacier (Cloud), Offline or Tape Storage
Media File: Archival Storage
Archive or Offline Storage
Standard or Archive Performance Drive & IOPS
(Not Required)
Archive
Storage Array
Media File: Standard Storage
Lower Throughput and Higher Latency
Standard Performance Drive & IOPS
NAS, File Storage,
File Server
Lucene
High Speed Network Storage
High Throughput - Low Latency
High Performance Drives & IOPS
Processing
SAN
High Speed
Storage Array
Agent PC
Contact Upload
Contact Playback
Supervisor
PC

Webex WFO Storage Process Flow

Contact Upload Processing


Media File: Archival Storage
Archive
Storage Array
Media File: Standard Storage
NAS, File Storage,
File Server
3) Store Contact into Media Storage
1) Insert Contact Details Into DB
2) Send to Analytics for Processing (If Configured)
SAN
Lucene
Storage Array
High Speed Network Storage
High Throughput Low Latency
Agent PC
Contact Upload
Supervisor
PC

Contact Playback Processing Diagram


Media File: Archival Storage
*8-24 Hr. Retrieval Rate
Archive
Storage Array
Media File: Standard Storage
**Near Immediate Retrieval Rate
NAS, File Storage,
File Server
2) Retrieve Contact from Media Storage
1) Lookup Contact Details in
Database
Lucene
SAN
Storage Array
High Speed Network Storage
High Throughput Low Latency
3) Playback Contact to
User
Agent PC
Supervisor
PC

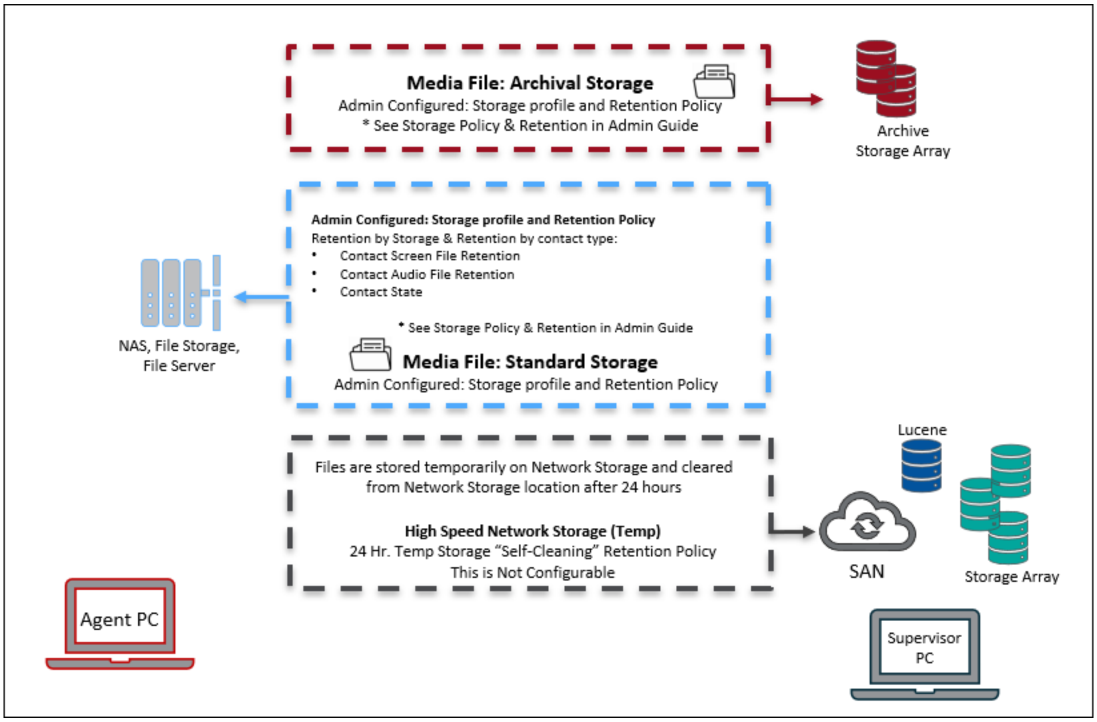
* If an offline storage option is used to store Media Files it can take an extended amount of time to retrieve files for playback (8-24hrs). The system will alert the user when the file is downloaded and ready.

NOTE For On-Premises deployments using an offline archival storage is non-typical.

** Retrieval and playback rates for Media Files stored on standard storage are available nearly immediately depending on file size, quality, and network latency.

Webex WFO Storage Retention

The following diagram depicts contact retention processing.


Media File: Archival Storage
Admin Configured: Storage profile and Retention Policy
* See Storage Policy & Retention in Admin Guide
Archive
Storage Array
Admin Configured: Storage profile and Retention Policy
Retention by Storage & Retention by contact type:
• Contact Screen File Retention
• Contact Audio File Retention
• Contact State
* See Storage Policy & Retention in Admin Guide
Media File: Standard Storage
Admin Configured: Storage profile and Retention Policy
NAS, File Storage,
File Server
Lucene
Files are stored temporarily on Network Storage and cleared from Network Storage location after 24 hours
High Speed Network Storage (Temp)
24 Hr. Temp Storage "Self-Cleaning" Retention Policy
This is Not Configurable
SAN
Storage Array
Agent PC
Supervisor
PC

*See the *System Administrator User Guide* for full details on storage policies and contact retention policies.

Storage Offerings

Webex WFO offers two types of storage that are detailed below.

Storage	Description
Webex WFO Short-Term Storage	Short-term storage used for files that incur a higher number of requests including additional processing or tasks.

Storage	Description
Webex WFO Long-Term Storage	Long-term storage used for files that no longer require processing and receive a very low number of real-time file requests.

Bulk Import and Export of Data

This topic describes methods for importing data into and exporting data out of Webex WFO.

Bulk Import and Export of Data Through Webex WFO

Webex WFO allows you to import and export several types of data. Described below is what data can be imported and exported, and how it can be imported and exported. Data files that are imported or exported are in CSV format. The following types of data can be imported and exported:

- Globally, you can import and export users, teams, and groups.
- In Analytics, you can import and export phrases and applications.
- In Quality Management, you can import and export evaluation forms, and export contact data.

Import and Export APIs

These APIs expose REST-like endpoints for importing and exporting data:

- Import API—Allows you to retrieve information about the back-end object models (the back-end model fields and the types associated with those fields) and import that data from CSV files into those back-end models
- Export API—Allows you to retrieve data from the back-end models in a CSV format.

See the *Webex WFO API Reference Guide* for more information.

Exporting Contacts in Bulk

You can export data for multiple contacts using the Bulk Contact Export button on the Recordings Lists options drop-down list. Exported files are stored in appropriately named folders in an external storage location. External storage can be configured to allow immediate or instant access. For more on External Storage see “Configure Storage Profiles” in the Webex WFO User Guide.

IMPORTANT Contacts and metadata are exported as CSV files.

Schedule a recurring bulk contact export

1. On the Recordings page, create and save a filter set.
2. Click the **Options** icon, and then click **Bulk Contact Export**.
3. Click the **New Export** tab.
4. Configure the export as defined in the described fields below.

   Export Name — Enter a name for the bulk contact export file.

   Saved Search — Select your saved filter set.

   Storage Location — Select the external storage location to which you want to export the contacts.

   Media Type — Select the file format in which Webex WFO exports audio and video files.

   - **Audio/Video Formats** — Select the file format in which the audio/video media should be exported. Only available for contacts with both audio and screen recordings.
   - **Audio-only Formats** — Select the file format in which the audio-only media should be exported. Only available for contacts with audio recordings.
   - **None** — Select **Transcriptions Only** to export transcriptions only.

   Analytics Output Format — Select the file format in which you want to export Analytics transcription data: JSON or XML. If you select **None**, Webex WFO does not export any Analytics transcription data. Select **None** to export only a CSV file with metadata.

5. Select **Send Scheduled Export**, and then schedule the export as described below.

   Weekly — Select one or more days of the week, and then select the time on those days that Webex WFO will export the contacts.

   Monthly — Select the day of the month, and then select the time on that day that Webex WFO will export the contacts.

6. Click **Create**.

   When you create a scheduled bulk contact export, Webex WFO saves the export. To edit the export, click the **Saved Contact Export** tab and select the export from the **Saved Export File Name** drop-down list.

> **NOTE** The first scheduled export (weekly or monthly) must occur after the next scheduled run of the App Dynamic Refresher task. Otherwise, the first scheduled export will not happen, although future exports will. By default, the App Dynamic Refresher task runs every fifteen minutes. Contact your system administrator to verify this schedule.

Export contacts immediately

1. On the Recordings page, create and save a filter set.
2. Click the **Options** icon, and then click **Bulk Contact Export**.
3. Click the **New Export** tab.
4. Configure the export as described below.

   Export Name — Enter a name for the bulk contact export file.

   Saved Search — Select your saved filter set.

   Storage Location — Select the external storage location to which you want to export the contacts.

   Media Type — Select the file format in which Webex WFO exports audio and video files.

   - **Audio/Video Formats** — Select the file format in which the audio/video media should be exported. Only available for contacts with both audio and screen recordings.
   - **Audio-only Formats**—Select the file format in which the audio-only media should be exported. Only available for contacts with audio recordings.
   - **None** — Select **Transcriptions Only** to export transcriptions only.

   Analytics Output Format — Select the file format in which you want to export Analytics transcription data: JSON or XML. If you select **None**, Webex WFO does not export any Analytics transcription data. Select **None** to export only a CSV file with metadata.

5. Select **Send Export Immediately**.
6. Click **Create**.

Licensing Requirements for Bulk Contact Export

Cisco requires you to select a license type for bulk contact export.

- **Standard license**—Export up to 500 contacts daily through the UI.
- **Performance license**—Export contacts in bulk by configuring multiple contact export jobs periodically throughout each day.

NOTE By default, each export batch is limited to 10,000 per job with the max amount of total contacts per day at 40,000 with the Performance license. If there is a need for an increase in these limits please contact Cisco Professional Services or Cisco Support Services.

Bulk Contact File Storage

Webex WFO stores bulk contact files in the location you select (see Application Management > System Configuration> External Storage). The default Storage Location is Network (Instant Access) storage. You can also select other storage options. If you configure network storage on a local drive, you do not need to specify SFTP .

BEST PRACTICE We recommend specifying SFTP. If you do not specify SFTP, your storage defaults to your system's Network Storage location. If users want to access files locally, they will need to have access to the Network Storage location.

Accessing Exported Files

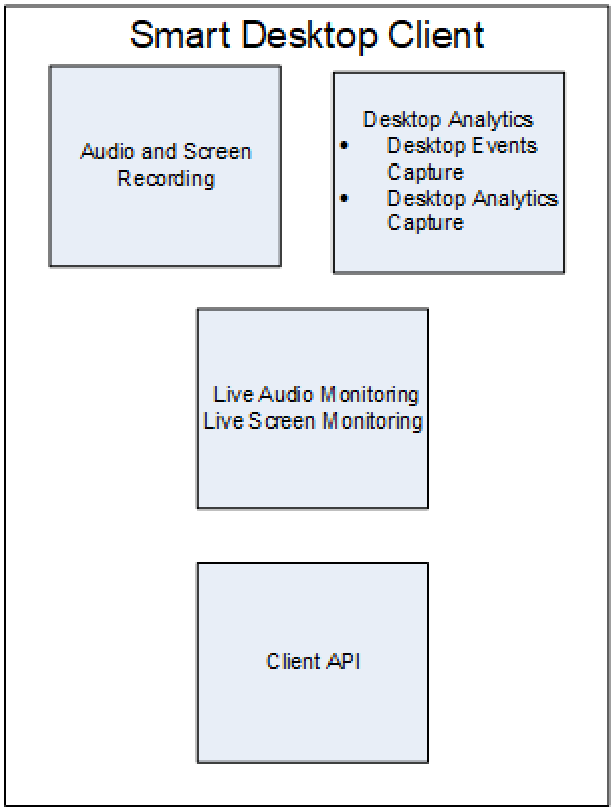
Your media and contact files are located in the Exports folder on your configured Storage Location:

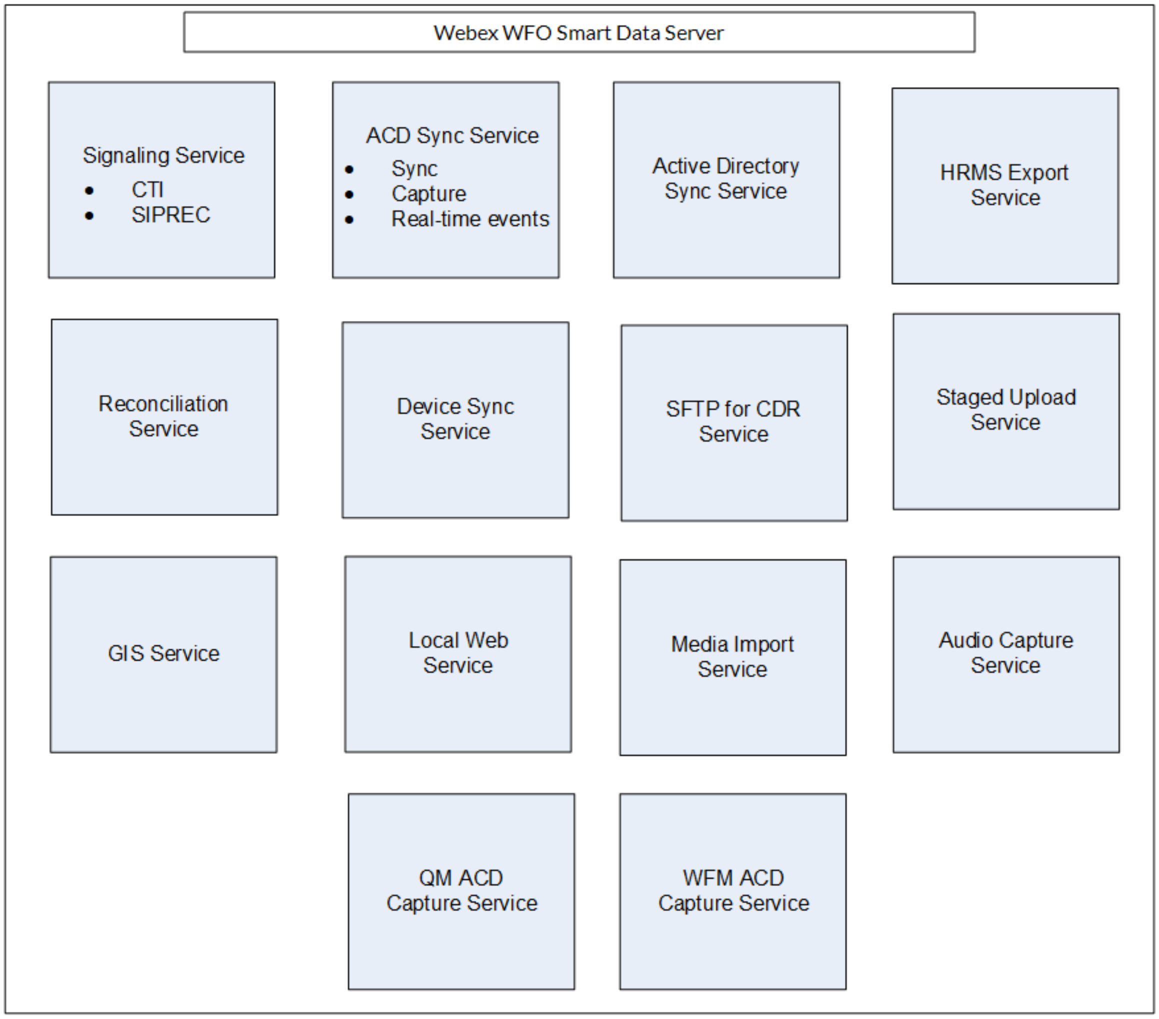
- If you have configured SFTP in your Archive Configuration, the files are stored there.
- If you have not configured SFTP in your Archive Configuration, the files are stored on your Network Storage location.

Network Storage can be configured in System Administration > External Storage.

Edge components

The Webex WFO edge components are comprised of the Webex WFO Smart Desktop Client. Webex WFO Smart Desktop enables you to view an agent's status, listen in on a call, and view the agent's screen in real time. The Webex WFO Data Server is an optional component depending on your Cloud integration model.





Webex WFO Smart Data Server

The Webex WFO Smart Data Server is responsible for functions such as ACD synchronization and staged uploads. A tenant administrator can install the Data Server for a single tenant, or a system administrator can install a base Data Server and configure it as a shared Data Server for multiple tenants.

> **NOTE** If the Data Server must connect through a web proxy, all Webex WFO services running on it must run as Windows login accounts with proxy settings. When configuring the Data Server with a proxy server, the Data Server service must be configured to run as a local administrator.

The services installed with the Data Server software are as follows.

- CTI Signaling Service
- Data Server

- Data Server Web Services
- Network Recording Service
- SIPREC Service

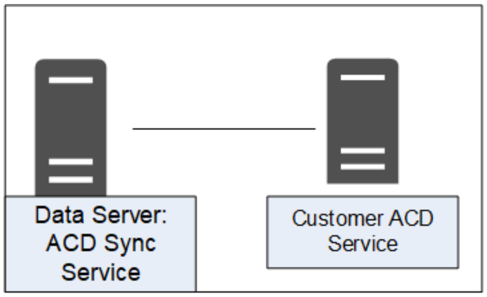
In Webex WFO, the following are functions of the Data Server, their descriptions, and the service they align to.

- Regional Data Server ACD Sync Settings — Used to sync user and team information from a supported ACD (Webex WFO Data Server).
- Recording Capture Server Settings — Used for edge server or gateway (SBC) audio recording environments. The primary Signaling service (CTI or SIPREC) assigns calls to capture servers in a round-robin algorithm (Webex WFO Network Recording Service).
- Regional Data Server GIS File Location — Used to import external contact metadata from a CSV file into Webex WFO (Webex WFO Data Server).
- Recording SIPREC Signaling Server Settings — Used to track start and stop events and capture metadata for call recordings. A SIPREC Signaling service is used for edge gateway (session border controller) recording environments (Webex WFO SIPREC Service).
- Recording CTI Signaling Server Settings — Used to track start and stop events and capture metadata for call recordings. A CTI Signaling service is used for edge server recording environments (Webex WFO CTI Signaling Service).
- Regional Data Server Staged Upload Settings — Used to gather contact data locally from Smart Desktop users and periodically upload the files to the Webex WFO components in the Cloud (Webex WFO Data Server).
- Regional Data Server ACD Capture Settings — Used to capture custom metadata and reconcile calls received through a gateway (Webex WFO Data Server).
- Regional Data Server Real-Time Event Settings— Used to capture historical and real-time ACD data for WFM and ACD metadata to attach to call contacts as custom metadata (Webex WFO Data Server).
- Regional Data Server Reconciliation Settings — Reconciliation is a process that connects gateway root recordings, which have limited call data, with additional call data that includes association with the correct agent (Webex WFO Data Server).
- Active Directory Sync — Enables Webex WFO to match and sync Webex WFO users with Active Directory users (Webex WFO Data Server).

- Data Server Device Sync Settings — Enables you to sync devices through the Data Server. These devices can then be associated to users, recording groups, and recording types using the Device Associations page in Application Management (Webex WFO Data Server).
- Local Web Service Settings — Enables API integration on this data server. If enabled, you have the option to enable the following:
  - Cisco IP Phone Services Controls — Allows Cisco-enabled recording controls from supported Cisco devices.
  - Simplified Recording Controls API — Enables you to use the native data server authentication for Cisco recording controls.
- HRMS Configuration — Enables the Data Server to export data to a human resource management system (HRMS) (Webex WFO Data Server).
- SFTP Configuration — Enables you to configure your SFTP server (Webex WFO Data Server).
- Media Import Server Settings — Enables the import of recording files from an external location (Webex WFO Data Server).

Webex WFO ACD Sync service

The ACD Sync service is used to sync user and team information from a supported ACD. The Sync process runs every ten minutes to update any changes made in the ACD into Webex WFO.



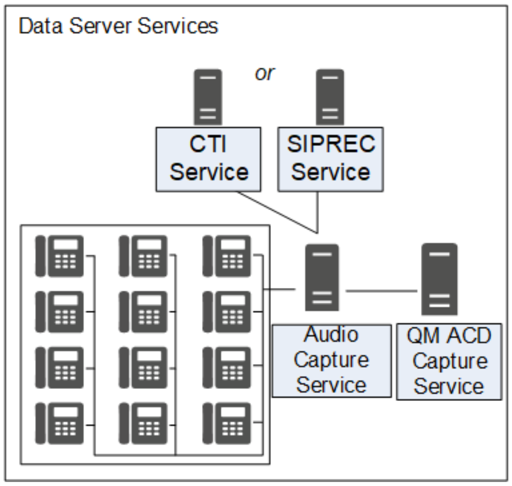
ACD Sync Service connectivity

The following table lists the basic connectivity to the ACD Sync service:

Connect to Service	Inputs/Outputs
Tenant’s ACD Service	Updates to ACD agent or team information

Webex WFO Audio Capture service

Webex WFO uses the Audio Capture service for edge server or gateway (SBC) audio recording environments. It can be assigned to clusters. The primary Signaling service (CTI or SIPREC) assigns calls to capture servers in a round-robin algorithm. Audio Capture services can be configured as active/active or active/standby.



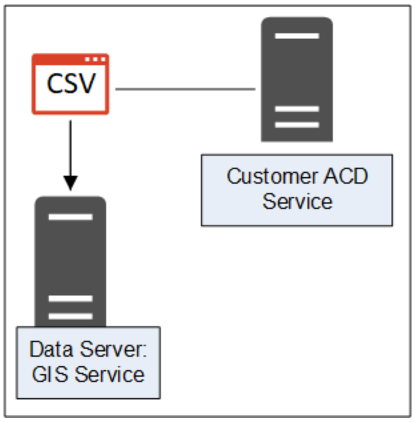
Audio Capture Service connectivity

The following table lists the basic connectivity to the Audio Capture service:

Connect to Service	Inputs/Outputs
CTI service	Receives signaling for audio capture
SIPREC service	Receives signaling for audio capture

Webex WFO GIS Service

Use the Generic Interface Service (GIS) service to import external contact metadata from a .CSV file into Webex WFO.



GIS Service connectivity

The following table lists the basic connectivity to the GIS service:

Connect to Service	Inputs/Outputs
Tenant’s ACD Service	Updates to ACD agent or team information
External .CSV file	External flat-file source for agent or team information updates Can be single or multiple files

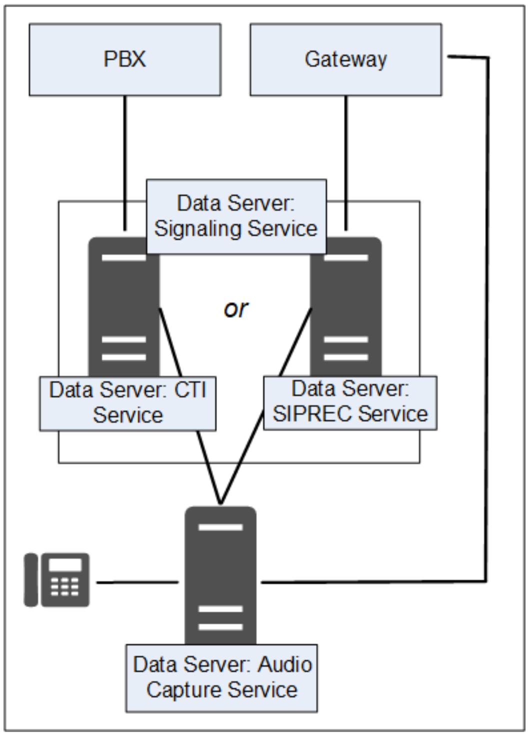
Webex WFO Signaling service

Your Signaling service can be either CTI or SIPREC:

- A CTI Signaling service is used for edge server recording environments, to track start and stop events and capture CTI metadata for call recordings.
- A SIPREC Signaling service is used for edge gateway (SBC) recording environments to track start and stop events and capture SIPREC metadata for call recordings.

You can configure either the CTI or SIPREC services for redundancy.

> **NOTE** The Audio Capture service can only be linked to one telephony group that includes a CTI or SIPREC service.


PBX
Gateway
Data Server: Signaling Service
or
Data Server: CTI Service
Data Server: SIPREC Service
Data Server: Audio Capture Service

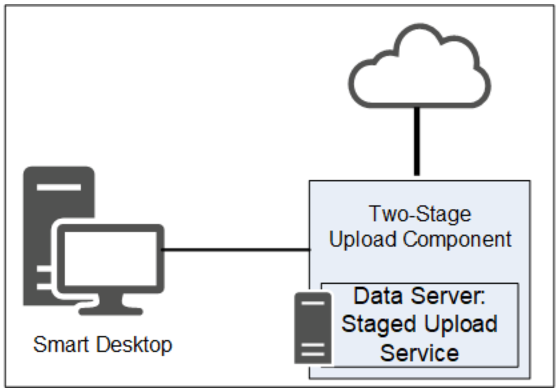
Signaling Service connectivity

The following table lists the basic connectivity to the Signaling service:

Type	Connect to Service
CTI	PBX service
	Audio Capture service
SIPREC	Gateway/SBC Service
	Audio Capture service
	QM ACD Capture service

Webex WFO Staged Upload service

The Webex WFO Staged Upload service gathers contact data locally from Smart Desktop Client users and periodically uploads the files to the Webex WFO components in the cloud.



Two-stage Upload component

The Two-stage Upload component enables you to periodically send data from the Data Server to the Webex WFO core components.

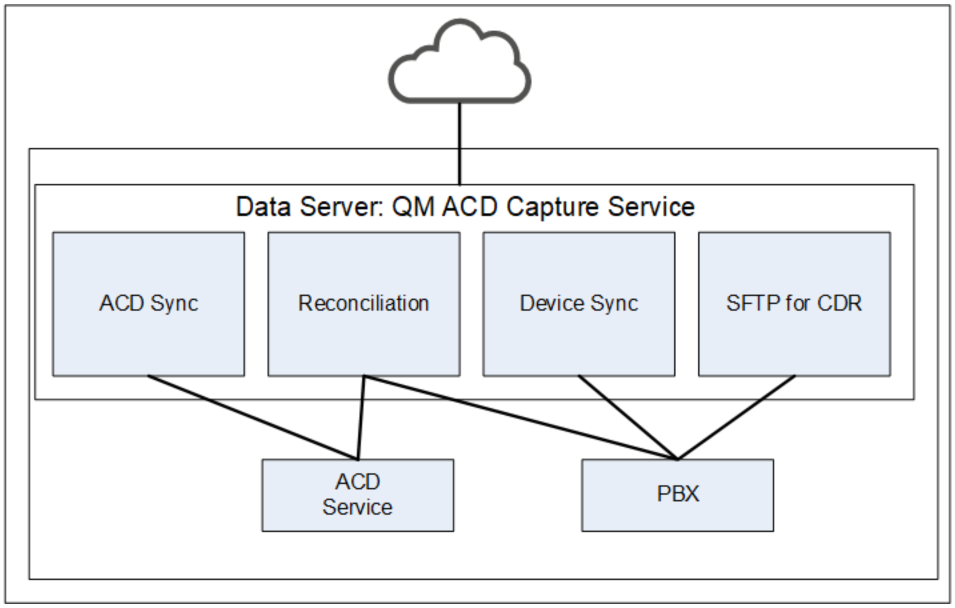
Staged Upload service connectivity

The following table lists the basic connectivity to the Staged Upload service:

Connect to Service	Inputs/Outputs
Tenant’s ACD Service	Updates to ACD agent or team information

Webex WFO QM ACD Capture service

Webex WFO uses the QM ACD Capture service to capture custom metadata and reconcile calls received through a gateway.



QM ACD Capture Service components

The QM ACD Capture service is composed of four components:

- QM ACD Historical Capture Component
- QM ACD Real-Time Capture Component
- QM GIS Capture Component

QM ACD Historical Capture component

The QM ACD Historical Capture component captures custom metadata and reconciliation data from the ACD.

QM ACD Real-Time Capture component

The QM ACD Real-Time Capture component captures contact data.

QM GIS Capture component

The QM GIS Capture component imports external QM contact metadata.

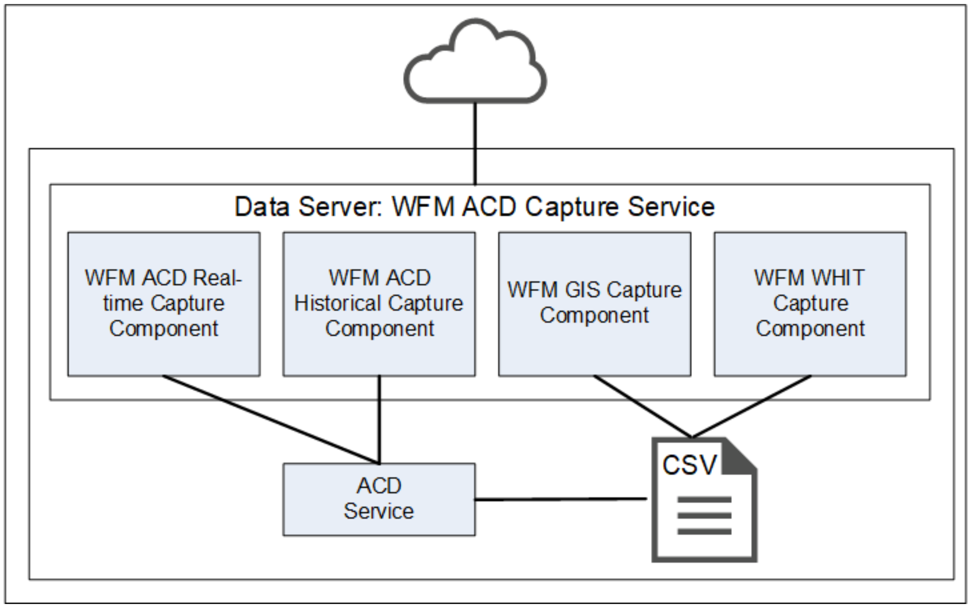
QM ACD Capture Service connectivity

The following table lists the basic connectivity to the QM ACD Capture service:

Connect to Service	Inputs/Outputs
Tenant's ACD Service	Updates to ACD agent or team information

Webex WFO WFM ACD Capture service

The Webex WFO WFM ACD Capture service captures historical and real-time ACD data for WFM and ACD metadata to attach to call contacts as custom metadata.


Data Server: WFM ACD Capture Service
WFM ACD Real-time Capture Component
WFM ACD Historical Capture Component
WFM GIS Capture Component
WFM WHIT Capture Component
ACD Service
CSV

WFM ACD Capture Service components

The WFM ACD Capture service is composed of four components:

- WFM ACD Historical Capture Component
- WFM ACD Real-Time Capture Component
- WFM GIS Capture Component
- WFM WHIT Capture Component

WFM ACD Historical Capture component

The WFM ACD Historical Capture component captures historical and real-time ACD data for WFM as well as ACD metadata to attach to call contacts as custom metadata.

WFM ACD Real-Time Capture component

The WFM ACD Real-Time Capture component captures contact data.

WFM GIS Capture component

The WFM GIS Capture component captures ACD data from non-direct ACDs.

WFM WHIT Capture component

The WFM WHIT Capture component allows you to import historical ACD data.

WFM ACD Capture service connectivity

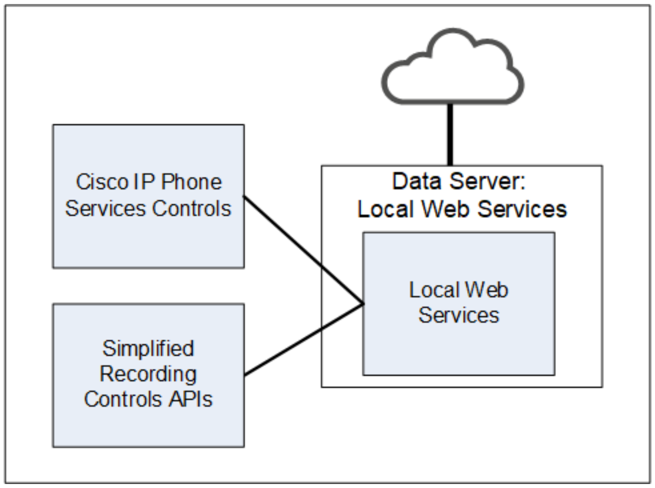
The following table lists the basic connectivity to the WFM ACD Capture service:

Connect to Service	Inputs/Outputs
Tenant’s ACD Service	Updates to ACD agent or team information

Webex WFO Local Web Services service

The Webex WFO Local Web Services Data Server service enables recording controls and native Data Server authentication.

NOTE The Local Web Services service is not supported with CCaaS vendor deployments.


Cisco IP Phone Services Controls
Simplified Recording Controls APIs
Data Server: Local Web Services
Local Web Services

Local Web Services Service components

The Local Web Services service is composed of two components:

- Cisco IP Phone Services Controls component
- Simplified Recording Controls API component

Cisco IP Phone Services Controls component

The Cisco IP Phone Services Controls component enables Cisco recording controls from supported Cisco devices.

Simplified Recording Controls API component

The Simplified Recording Controls API component allows for use of native Data Server authentication for Cisco recording controls.

Local Web Services service connectivity

The following table lists the basic connectivity to the Local Web Services service:

Connect to Service	Inputs/Outputs
Simplified Recording Controls API	Data Server authentication for Cisco recording controls
Cisco IP Phone Services Controls	Allows native Data Server authentication for Cisco recording controls

Installing the Data Server

A tenant administrator can install the Data Server for a singe tenant, or a system administrator can install a Base Data Server and configure it as a Shared Data Server for multiple tenants.

Prerequisites

If a Data Server must connect through a Web Proxy, each Data Server service must be configured to use a service account. This affects the following Windows services:

- Calabrio ONE CTI Signaling Service
- Calabrio ONE Data Server
- Calabrio ONE Network Recording Service
- Calabrio ONE SIPREC Service
- Calabrio ONE Data Server Web Services

For port usage requirements, see Port usage.

Installing the Data Server for a single tenant

A tenant administrator can install the Data Server for a single tenant.

Install the Data Server for a single tenant:

1. From the server where you want to install the Data Server, open a browser and log in to Webex WFO using tenant administrator credentials.
2. On the **Downloads** page (Application Management > Administration > Downloads), click the appropriate link to download the Data Server installer.
3. Follow the prompts.

Test the Data Server:

1. Log into Webex WFO as a tenant administrator.
2. On the **Agent Monitoring** page (Application Management > Monitoring > Agent Monitoring) select the Data Server from the Data Server Logs section and click **Retrieve Logs**. If the log request is successful, the Data Server is connected.

   NOTE This might take a few minutes to complete.

Installing the Data Server for multiple tenants

A system administrator can configure a Data Server to be shared by multiple tenants. Any time a Shared Data Server is updated (for example, when a new tenant is added to it) you must update its configuration. This is done by the Data Server Updater file that is generated when you save your changes and opt to download the configuration.

To configure a Data Server for multiple tenants, a system administrator must install a Base Data Server, and then configure the Base Data Server as a Shared Data Server. System administrators can download a Base Data Server on the Application Management > Downloads page or the Application Management > Shared Data Server page.

Install the Base Data Server

The first thing you must do is download and install the Base Data Server. This Base Data Server becomes a Shared Data Server when it is configured. You can install multiple Base Data Servers.

1. In the **Download Base Data Server** section, click the **Calabrio ONE Data Server** link. This downloads the file CalabrioONEDataServerSetup.exe to your computer.
2. Double-click the executable to start the Data Server Setup Wizard.
3. Follow the instructions in the wizard to complete the installation.

Configure the Base Data Server

Next, configure the Base Data Server to become a Shared Data Server.

1. Select the **Add a new configuration to the data server** option.

   > NOTE To edit an existing configuration, select the **Edit an existing data server configuration** option and select the Data Server you want to edit.

2. Complete the fields as defined in the following table.

Field	Description
Server Name	Enter a name for the Data Server.
Calabrio ONE Server	Enter the IP address or host name of the Calabrio ONE server that hosts the Data Server service.
Port	Enter the port number of the server that hosts the Data Server service. The default port is 443.

Field	Description
Available	A list of available tenants.
Assigned	A list of tenants assigned to this Data Server service.

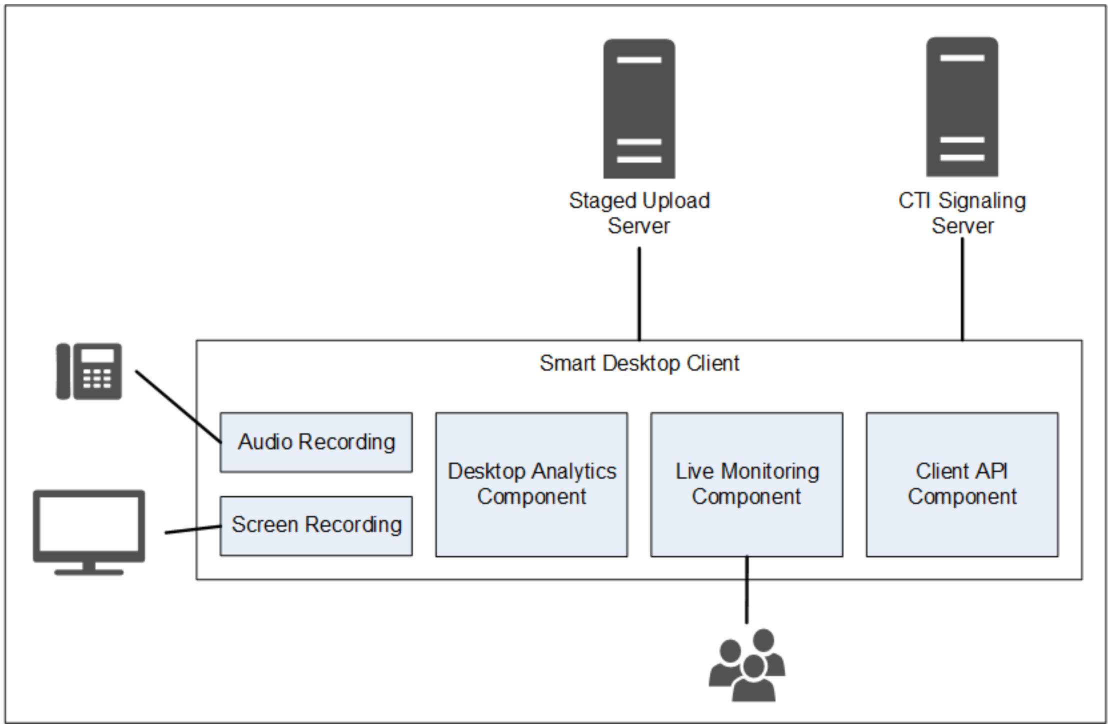
3. Click **Save/Download Configuration** to save the configuration and download the Configuration utility (CalabrioONEDataServerUpdaterSetup.exe) to your computer.

   > **NOTE** You can also click **Save** to save the configuration without downloading the configuration utility. You might choose to do this if you have not finished configuring the Data Server but want to save the incomplete configuration.

4. Double-click the configuration utility executable to start the Data Server Updater Setup Wizard.
5. Follow the instructions in the wizard to complete the configuration of the Shared Data Server.

Webex WFO Smart Desktop Client

The Smart Desktop Client is installed on agent desktops or on a server that hosts a supported thin client. (See Thin client servers for more information.) It captures all user data (including call recording, screen, and desktop activity) on an agent's desktop. You must add the installer on the Downloads page in Application Management, so that it can be accessed by the tenant administrator.



Users with Smart Desktop Client installed who are configured with the required permissions can perform Live Audio and Live Screen monitoring.

Smart Desktop Client components

The Smart Desktop Client contains four components:

- Audio and Screen Recording component
- Desktop Analytics component
- Live Audio Monitoring and Live Screen Monitoring component
- Client API component

Audio and Screen Recording component

The Audio and Screen Recording component records agents’ calls.

Desktop Analytics component

The Desktop Analytics component provides analytical analysis of the agent’s desktop recordings.

Live Audio Monitoring and Live Screen Monitoring component

The Live Audio and Live Screen Monitoring component allows users with the appropriate permissions set to perform Live Audio and Live Screen monitoring.

NOTE Live Audio Monitoring is not supported with CCaaS vendor deployments.

Smart Desktop Client connectivity

The following table lists the basic connectivity to the Smart Desktop Client:

Component	Connects To	Inputs/Outputs
Audio and Screen Recording	Agent’s PC	Phone audio and screen data
Desktop Analytics	Agent’s PC	Phone audio and screen data
Live Monitoring	Other agents’ PCs	Other agents’ phone audio and screen data

Connect to Server	Inputs/Outputs
Staged Upload	Contact information (audio and screen recordings and metadata)

Thin client servers

NOTE Webex WFO supports Citrix XenApp installed only on a supported Windows server.

When using a thin client server, note:

- Thin clients using the Smart Desktop require a remote desktop session to capture all user data (audio, screen, and desktop recording). If no remote desktop session is present, install Smart Desktop on the agent desktops to capture all user data on the desktop while the user is logged in.
- Configure workflows to use Immediate Upload for both screen and voice to assure all recordings are accessible.
- If you are using Smart Desktop for recording purposes, the thin client server requires additional server resources for screen recordings. The resource requirements will vary depending on the actual design and might require some detailed hardware designs that should be reviewed by Cisco before deployment.
- If you are using a virtual image and it has access to your local NIC, you can use Smart Desktop for agent-side recording.

Installing the Thin Client Server

Install Citrix XenApp or Windows Terminal Services per the product documentation.

Use the following settings required to support audio and screen recording and recording playback functions in Webex WFO:

Area	Consideration
Browser	■ Include a supported browser on thin client server deployments. Thin client servers must include a supported browser to access Webex WFO. ■ Publish the browser locally to each server. ■ Ensure that the browser security settings allow end users to play back recordings through the thin client.
Sessions	Limit the number of simultaneous sessions per user to a single session.

Area	Consideration
Smart Desktop Client	■ For Citrix client services, you must also install the Smart Desktop Client on the thin client server, in order to record user desktop activity (Desktop Analytics) and phone calls, using a supported soft phone. ■ The Smart Desktop Client connects to the Webex WFO platform using the unique Domain\Windows Login of the user.

Installation

This section describes how to install the various components of Webex WFO.

Installing Smart Desktop

Webex WFO Smart Desktop can be installed to an agent's computer in any one of three ways:

- Manually on each agent's computer
- Using Group Policy Object (GPO) scripts
- Using Microsoft System Center Configuration Manager (SCCM)

> **NOTE** If you want Smart Desktop to capture desktop analytics, the agent role must have the "Capture Desktop Analytics" permission enabled before installing Smart Desktop. If the permission is not enabled, the capture plugins are not installed on the client desktop.

Manual installation

Use this procedure to install Smart Desktop manually on an agent's computer or on a thin client server.

Install Smart Desktop manually:

1. From the agent's computer or the thin client server, log in to Webex WFO using administrator credentials.
2. On the Downloads page (Application Management > Global > Administration > Downloads), click the **Calabrio ONE Smart Desktop** installer link. Webex WFO provides a .exe file for manual installation. The available .msi file is for the SCCM push only.
3. Accept the End User License Agreement (EULA) when prompted.
4. Run the installer and follow the prompts in the installation wizard.
5. Select the **Activate** checkbox if prompted and click **Finish**.
6. After running the Smart Desktop installer, restart your system.
7. Run the Client Verification tool. See Client Verification tool for more information.
8. Test Smart Desktop. See Testing Smart Desktop for more information.

Installation using GPO

A Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users. Microsoft provides a program snap-in that allows you to use the Group Policy Microsoft Management Console to define various options, including scripts options. Refer to Push Installation Return Codes as needed after pushing the client.

Deploy Smart Desktop using GPO:

1. Log in to Webex WFO using administrator credentials.
2. On the Downloads page (Application Management > Global > Administration > Downloads), click the **Calabrio ONE Smart Desktop** installer link. Webex WFO provides a .exe file for manual installation.
3. Accept the End User License Agreement (EULA) when prompted.
4. Copy **CalabrioONEDesktopSetup_<TenantName>.exe** from your Downloads folder and paste it in the server share location.
5. Create a batch script to run the installer that contains the following script:

   ```
   <host name or IP address of server share location>\CalabrioONEDesktopSetup_
      <TenantName>.exe /LOG /VERYSILENT /ACTIVATE /NORESTART
   ```

6. Start the Group Policy Management Editor and navigate to Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown) and add the batch script.

Installation using SCCM

You can use Microsoft System Center Configuration Manager (SCCM) to push Smart Desktop to multiple agent computers. Refer to Push Installation Return Codes as needed after pushing the client.

Install Smart Desktop using SCCM:

1. Copy the following files to the server share location:
   - SCCM_Support.msi
   - CalabrioONEDesktopSetup_<TenantName>.exe
2. Start SCCM and create an application.
3. Select the “Automatically detect information about this application from installation files” option.
4. In the **Type** field, select Windows Installer (*.msi file)
5. In the **Location** field, browse to the location of the SCCM_Support.msi file.

6. Click **Yes** if a warning appears that the publisher cannot be identified.
7. Click **Next** after the application is successfully imported.
8. Choose one of the following options:
   - MSI-based installs: Click **Next**.
   - EXE-based installs: Change the Installation Program field to:

     ```
     CalabrioONEDesktopSetup_<TenantName>.exe/LOG /VERYSILENT /ACTIVATE
        /NORESTART
     ```

     and click **Next**.

     > **NOTE** See Installation using GPO to understand the implications of using these arguments.

9. Click **Next** and then click **Close**.

The /ACTIVATE and /NORESTART arguments

It is important that you understand the implications of using the /ACTIVATE and /NORESTART arguments in the batch script.

- The /ACTIVATE argument activates Smart Desktop as soon as it is installed. Call recording is stopped until the installation and activation process is completed. If you push a new version of Smart Desktop during a work period, it is recommended that you do not include the /ACTIVATE argument. In that case, the new version will activate automatically the next time the agent logs in.
- The /NORESTART argument prevents a sudden reboot that can interrupt and lose call recordings.
- Adding the /FORCENPCAP argument forces the NPCAP installer to run when executing the Smart Desktop Client installation. The NPCAP installer is included with the Smart Desktop Client.
- Adding the /NONPCAP argument prevents the NPCAP installer from being installed on the target machine when executing the Smart Desktop Client installation.

  > **NOTE** Use the /FORCENPCAP and /NONPCAP arguments independently from each other. Do not use them within the same command.

The NPCAP arguments

NPACP arguments are optional and can be used to control the installation of NPCAP on client devices. It’s important to note that the arguments are independent from each other and only one of the arguments should be used during installation.

- The /FORCENPCAP argument forces the NPCAP installer to run when executing the Smart Desktop Client installation.
- The /NONPCAP argument prevents the NPCAP installer from being run when executing the Smart Desktop Client installation.

Replicating an installation using desktop imaging

After you have installed the Smart Desktop Record Service on one PC using one of the previous installation methods (see Manual installation, Installation using GPO, or Installation using SCCM), you can replicate that installation on multiple PCs by creating a generic system image that can be used across multiple hardware designs. When Smart Desktop is installed on a PC for imaging, some information must be removed that will allow the image to run on different PCs without causing issues.

Recommended method: Cisco’s System Preparation hook

To remove PC-specific information from a Windows installation and “generalize” it so that it can be installed on different PCs, we strongly recommend that you use Cisco’s System Preparation (sysprep) hook. Sysprep is Microsoft’s system preparation tool used to prepare a system image for deploying to multiple PCs. Sysprep prepares a Windows installation (Windows client and Windows Server) for imaging, allowing you to capture a customized installation. The sysprep hook is installed with Smart Desktop and registers with the system automatically. When you run sysprep, it automatically calls all the hooks registered with the system.

Secondary method: Configure the image manually

If you cannot use sysprep, you must perform the following steps manually for any image where the Smart Desktop Record Service is installed before deploying that image to additional PCs.

> **IMPORTANT** If you choose to perform these steps, check back to this document frequently to keep current with any changes to these steps.

1. Stop the Smart Desktop Record Service.
2. Open the “log” folder where the Smart Desktop Record Service is installed (by default, this is C:\Program Files (x86)\Calabrio ONE\Desktop\Active\log) and remove all files that do not contain the word “postinstall.”
3. Remove all sub-folders (including their contents) from the “log” folder.
4. Open “C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop\config” and remove all files except for “Install.ini” and “sysproperties.cfg.”
5. Remove all sub-folders (including their contents) from the “config” folder.

6. Open “C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop\recordings” and delete all files and sub-folders (including their contents). The “recordings” folder must be empty.
7. Open “C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop\chunks” and delete all files and sub-folders (including their contents). The “chunks” folder must be empty.

> **NOTE** The “chunks” folder might not exist. If the “chunks” folder does not exist, you can skip this step.

Push installation return codes

When you use a push installation method (such as GPO or SCCM) you will receive return codes indicating install success or failure. The possible return codes are described below.

Return Code	Description
0	Setup was successfully run to completion or the /HELP or /? command line parameter was used.
1	Setup failed to initialize.
2	The user clicked Cancel in the wizard before the actual installation started, or chose “No” on the opening “This will install…” message box.
3	A fatal error occurred while preparing to move to the next installation phase (for example, from displaying the pre-installation wizard pages to the actual installation process). This should never happen except under the most unusual of circumstances, such as running out of memory or Windows resources.
4	A fatal error occurred during the actual installation process. **NOTE** Errors that cause an Abort-Retry-Ignore box to be displayed are not fatal errors. If the user chooses Abort at such a message box, exit code 5 will be returned.
5	The user clicked Cancel during the actual installation process, or chose Abort at an Abort-Retry-Ignore box.
6	The Setup process was forcefully terminated by the debugger (Run | Terminate was used in the IDE).
7	The “Preparing to Install” stage determined that Setup cannot proceed

Return Code	Description
	with installation.
8	The “Preparing to Install” stage determined that Setup cannot proceed with installation, and that the system needs to be restarted in order to correct the problem.
501	Microsoft redistributable installed successfully. MSI return code could not be detected.
502	Microsoft redistributable installed successfully. MSI returned a fatal error.
503	Microsoft redistributable installed successfully. MSI returned a Mutex error.
504	Microsfot redistributable installed successfully. MSI requires a reboot.
505	Microsoft redistributable installed successfully. MSI returned an unexpected return code.
520	Could not determine Microsoft redistributable return code. MSI installed successfully.
521	Could not determine Microsoft redistributable return code. MSI return code could not be detected.
522	Could not determine Microsoft redistributable return code. MSI returned a fatal error.
523	Could not determine Microsoft redistributable return code. MSI returned a Mutex error.
524	Could not determine Microsoft redistributable return code. MSI requires a reboot.
525	Could not determine Microsoft redistributable return code. MSI returned an unexpected return code.
540	Microsoft redistributable returned a Mutex error. MSI installed successfully.

Return Code	Description
541	Microsoft redistributable returned a Mutex error. MSI return code could not be detected.
542	Microsoft redistributable returned a Mutex error. MSI returned a fatal error.
543	Microsoft redistributable returned a Mutex error. MSI returned a Mutex error.
544	Microsoft redistributable returned a Mutex error. MSI requires a reboot.
545	Microsoft redistributable returned a Mutex error. MSI returned an unexpected return code.
560	Microsoft redistributable requires a reboot. MSI installed successfully.
561	Microsoft redistributable requires a reboot. MSI return code could not be detected.
562	Microsoft redistributable requires a reboot. MSI returned a fatal error.
563	Microsoft redistributable requires a reboot. MSI returned a Mutex error.
564	Microsoft redistributable requires a reboot. MSI requires a reboot.
565	Microsoft redistributable requires a reboot. MSI returned an unexpected return code.
580	Microsoft redistributable returned an unexpected return code. MSI installed successfully.
581	Microsoft redistributable returned an unexpected return code. MSI return code could not be detected.
582	Microsoft redistributable returned an unexpected return code. MSI returned a fatal error.
583	Microsoft redistributable returned an unexpected return code. MSI returned a Mutex error.
584	Microsoft redistributable returned an unexpected return code. MSI

Return Code	Description
	requires a reboot.
585	Microsoft redistributable returned an unexpected return code. MSI returned an unexpected return code.
599	There was an error processing return codes.
3010	A reboot is required to ensure the product runs properly.

Testing Smart Desktop

After you have installed Smart Desktop and properly configured the browser, follow these steps to make sure everything is working correctly.

1. Make a phone call from an agent's desktop.
2. In Webex WFO, click **Recordings**.
3. Verify that you can find the recording for the call.
4. Double-click the recording to play back the call and the screen recording, if applicable.

   If you are expecting the screen window to appear and it does not, verify that the pop-up blocker on the browser is disabled.

   If a Playback Error message appears, WebM is not installed on the Internet Explorer browser. Download WebM from http://tools.google.com/dlpage/webmmf/.

Client Verification tool

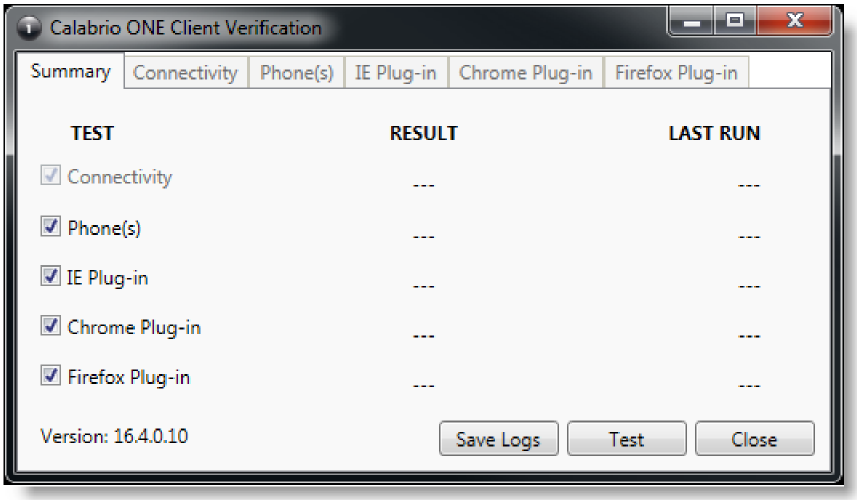
The Client Verification tool tests the client PC to ensure that the connectivity with servers and the phone are suitable for running Smart Desktop. It is installed when Smart Desktop is installed. The tool runs various tests and reports results as either a pass or fail.

Run the Client Verification tool:

1. After installing Smart Desktop, navigate to the following folder on the client PC:

   ```
   C:\Program Files (x86)\Calabrio ONE\Desktop\Active\bin\
   ```

2. Double-click **ClientDiag.exe**. The Client Verification tool starts.

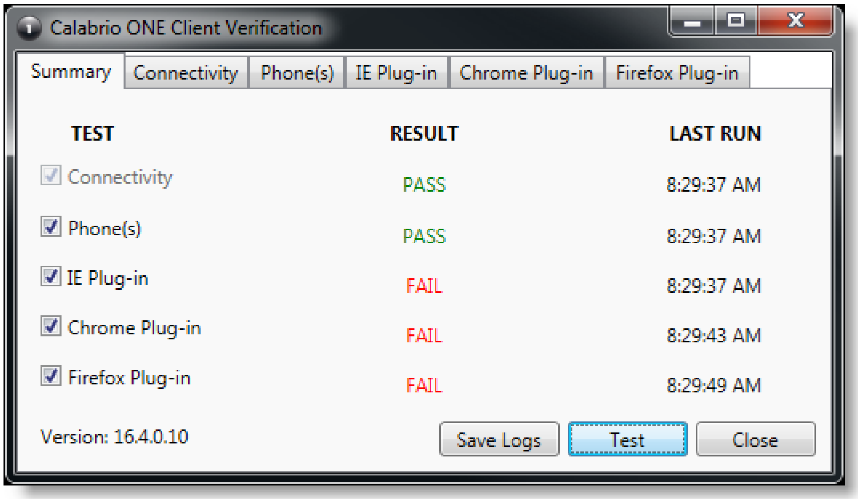


TEST	RESULT	LAST RUN
☑ Connectivity	---	---
☑ Phone(s)	---	---
☑ IE Plug-in	---	---
☑ Chrome Plug-in	---	---
☑ Firefox Plug-in	---	---

Version: 16.4.0.10

3. By default, all tests are selected. Click **Test**.

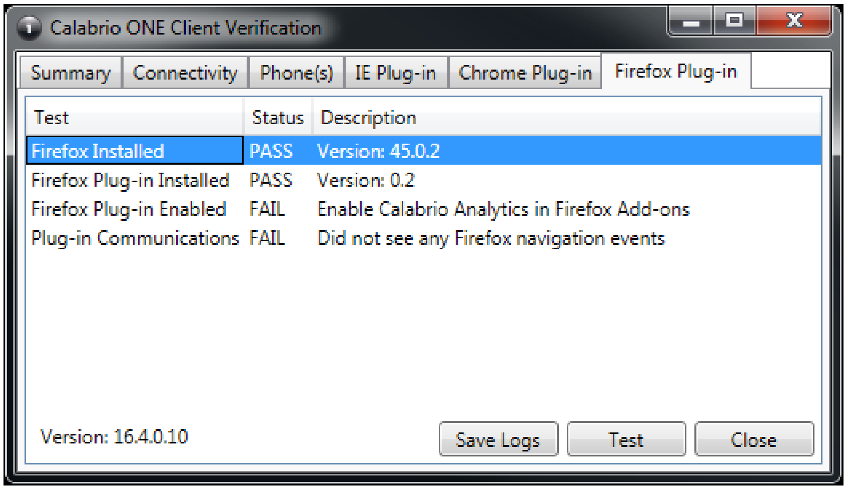
4. The tool reports the results of the test as either a pass or fail.



TEST	RESULT	LAST RUN
☑ Connectivity	PASS	8:29:37 AM
☑ Phone(s)	PASS	8:29:37 AM
☑ IE Plug-in	FAIL	8:29:37 AM
☑ Chrome Plug-in	FAIL	8:29:43 AM
☑ Firefox Plug-in	FAIL	8:29:49 AM

Version: 16.4.0.10

5. There is a tab for each test where details of the test are displayed. If the test fails, the details on the tab will provide guidance about what is wrong.



Test	Status	Description
Firefox Installed	PASS	Version: 45.0.2
Firefox Plug-in Installed	PASS	Version: 0.2
Firefox Plug-in Enabled	FAIL	Enable Calabrio Analytics in Firefox Add-ons
Plug-in Communications	FAIL	Did not see any Firefox navigation events

Version: 16.4.0.10

6. If needed, you can click **Save Logs** to zip up the logs for Postinstall and Smart Desktop to help identify issues. The logs are automatically zipped to a file named Clientlogs.zip.

Recording Controls

The Recording Controls standalone application is automatically installed with Smart Desktop. Recording Controls enables an agent to start, pause, resume, and stop audio, screen, and keystroke recording for active calls, as well as tag calls and add metadata to them.

Using Recording Controls is optional.

NOTE The Recording Controls application is not supported with CCaaS vendor deployments.

The Recording Controls executable is installed here:

```
C:\Program Files (x86)\Calabrio ONE\Desktop\Active\bin\DCC.exe
```

In the Start menu, the application is named Webex WFO Recording Controls and by default is under Webex WFO.

Configuring Citrix machines for writing log files

In Citrix environments running Internet Explorer, the IEplugin log configuration needs to be adjusted. Use the steps below to configure Citrix environments to write log files.

1. Create a directory to store IE logs.

   EXAMPLE C:\log_files

2. Give the directory you created Low Integrity access.

   a. Navigate to the Administrator command prompt.

   b. Run `‘icacis C:\<`IE log directory`> /setintegritylevel L’`

3. Set IE Browser Helper Object (BHO) logging to use the IE logs directory:

   a. Navigate to `C:\Program Files (x86)\Calabrio ONE\Desktop\Active\config\IEPlugin.config`

   b. Find `<file value="C:\Users\<user directory>\AppData\LocalLow\calabrio\IEPlugin.txt" />`

   c. Modify it to `<file value="C:\<IE log directory>\${`userdomain`}=${`username`}\IEPlugin.txt" />`

Removal

The following topics describe how to uninstall Webex WFO components.

Uninstalling Webex WFO Smart Desktop

NOTE You must log in as an administrator in order to uninstall Smart Desktop.

1. On the desktop or the thin client server where Smart Desktop is installed, open the Windows Control Panel.
2. Start the Add or Remove Programs utility.
3. From the list, select the application you want to remove and click **Uninstall**.

   If you intend to reinstall Smart Desktop after completely removing an older version (a clean install), verify that the recording storage folder structures are removed before installing the new version.
4. Restart the desktop or the Thin Client server.

Uninstalling using GPO

A Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users. Microsoft provides a program snap-in that allows you to use the Group Policy Microsoft Management Console to define various options, including scripts options.

1. Create a batch script to run the installer that contains the following script:

   ```
   <C:\Program Files (x86)\Calabrio ONE\Desktop\Wrapper\unins000.exe /LOG
      /VERYSILENT /NORESTART>
   ```
2. Start the Group Policy Management Editor and navigate to Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown) and add the batch script.

IMPORTANT This will force all open browsers to close. If browsers are re-opened before uninstallation is complete, the uninstall may fail and need to be restarted.

Data Transfer Flow Diagrams

This topic includes diagrams illustrating the following:

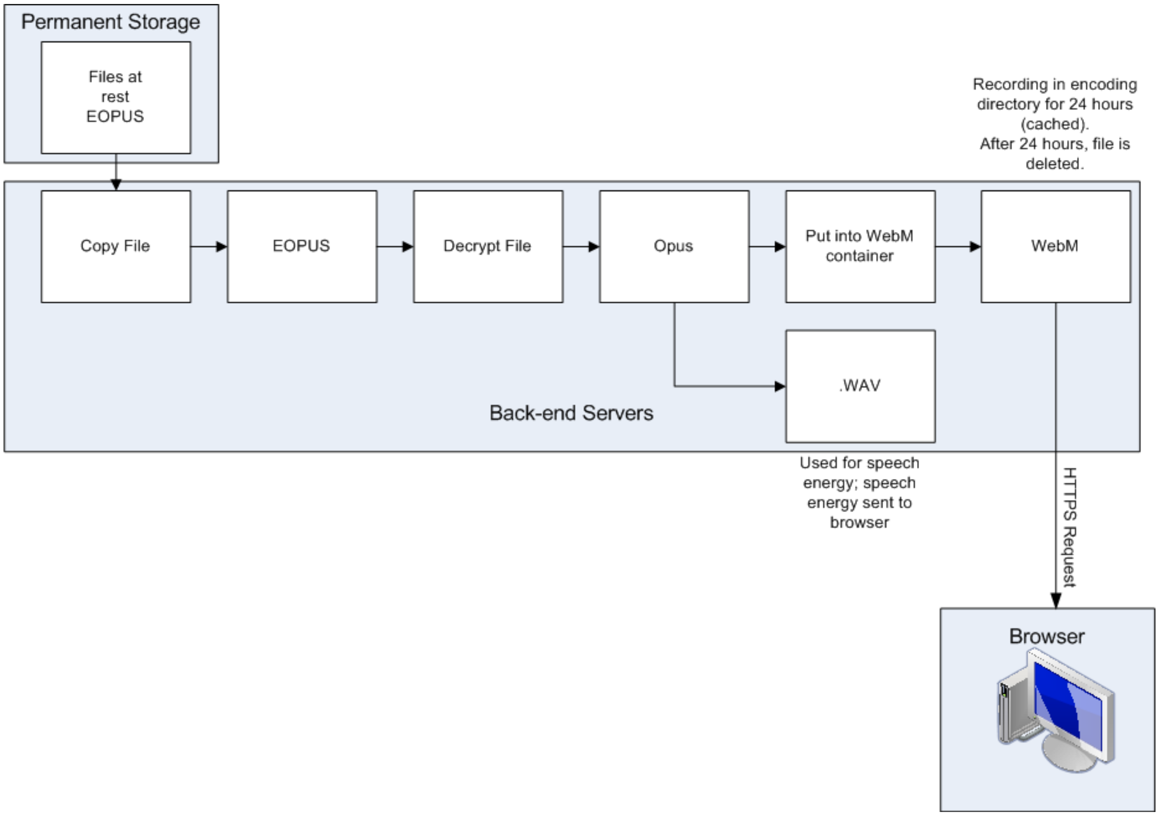
- Webex WFO recording capture and playback
- Webex WFO Analytics data flow
- Webex WFO storage data flow
- Webex WFO recording encryption

Recording Capture and Playback Data Flow Diagrams

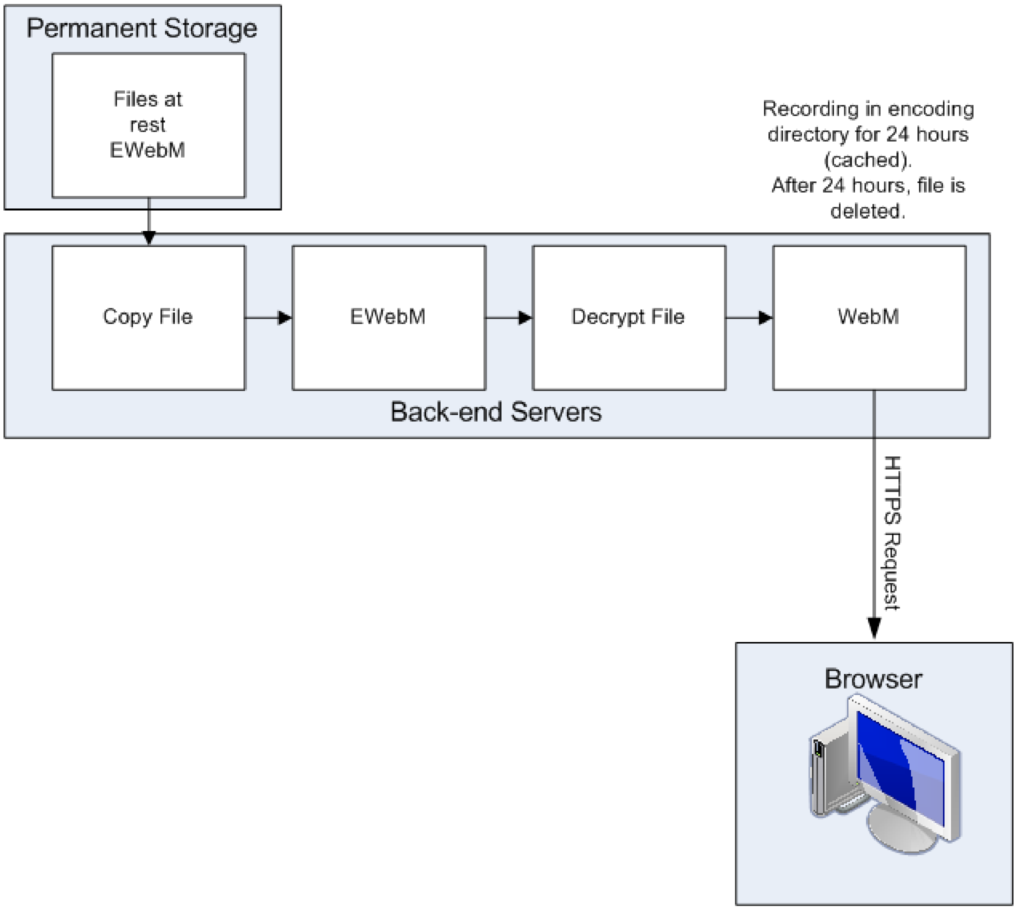
This topic describes the process of playing back contact recordings.

Audio Playback Data Flow Diagram

During playback, audio and screen recording files are copied from permanent storage and placed into a secured cloud network storage, decrypted, and processed for playback .The files are simultaneously decrypted and secured through network storage and HTTPS.


Permanent Storage
Files at rest EOPUS
Copy File
EOPUS
Decrypt File
Opus
Put into WebM container
WebM
Recording in encoding directory for 24 hours (cached).
After 24 hours, file is deleted.
.WAV
Back-end Servers
Used for speech energy; speech energy sent to browser
HTTPS Request
Browser

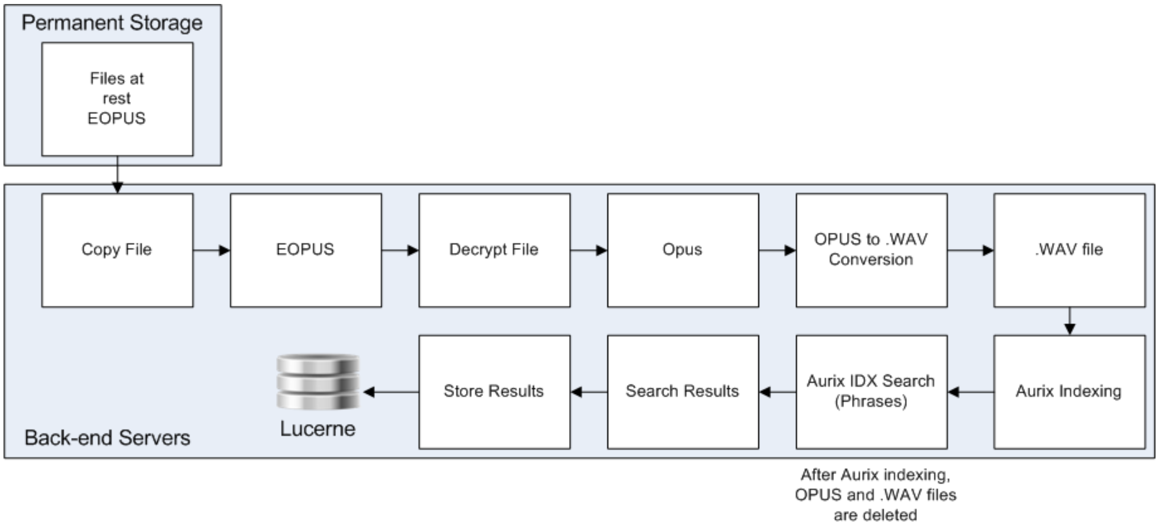
Screen Playback Data Flow Diagram



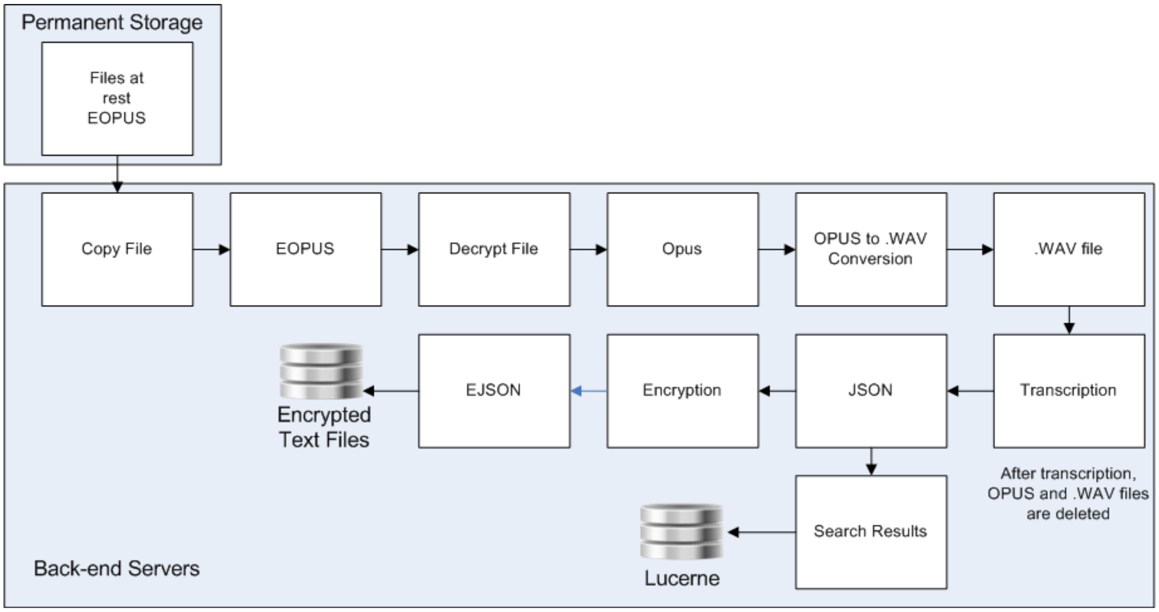
Analytics Data Flow Diagrams

This topic describes the data flow for processing Analytics data.

Phonetic Speech Analytics Data Flow Diagram



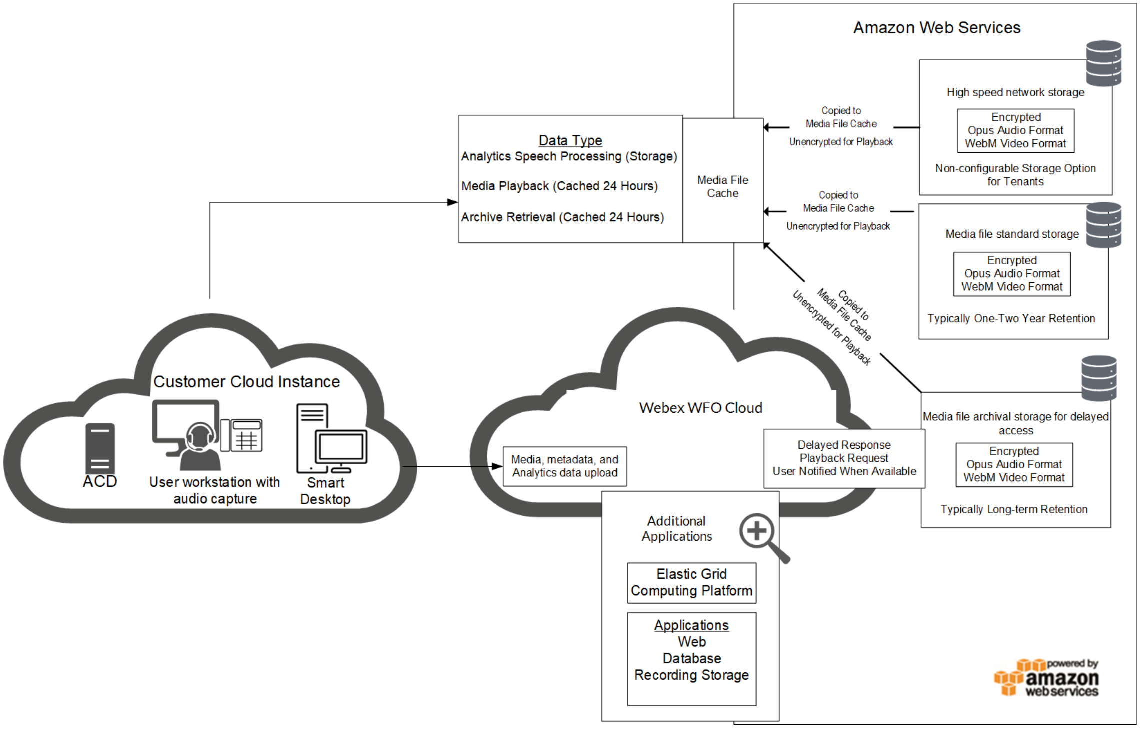
Speech Transcription Analytics Data Flow Diagram



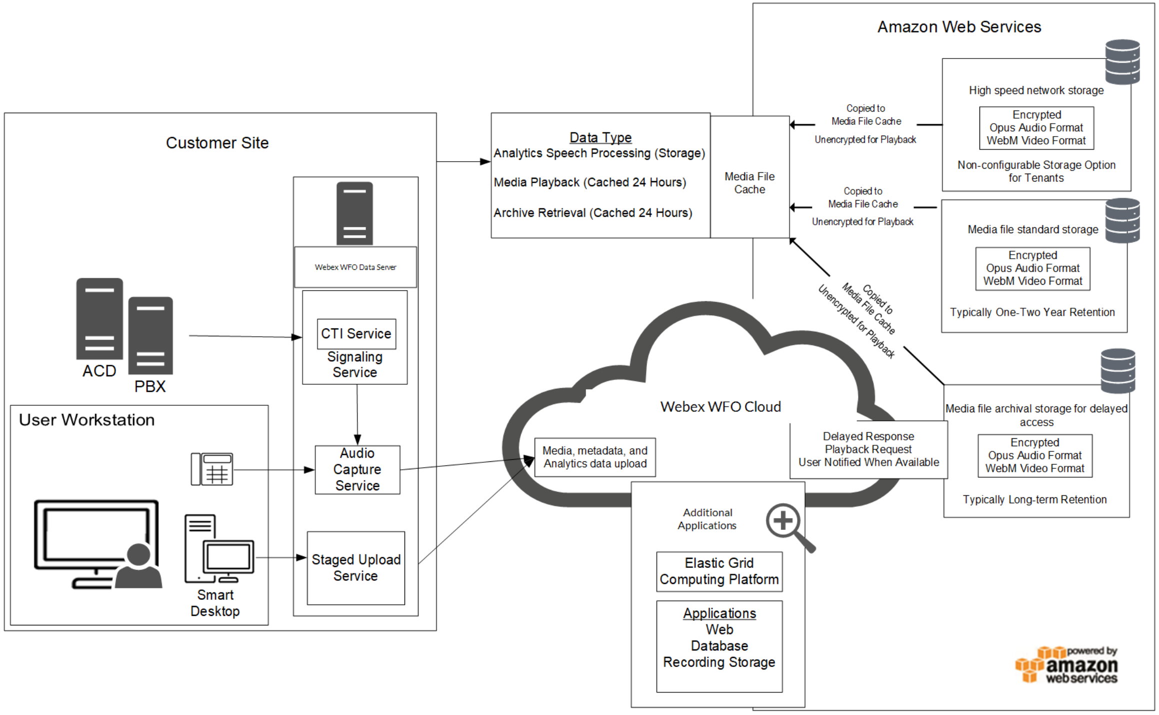
Cloud Storage Data Flow Diagrams

This topic describes the data flow for contact data storage in Webex WFO for CCaaS and customer-hosted deployments.

Cloud Storage for CCaaS deployments

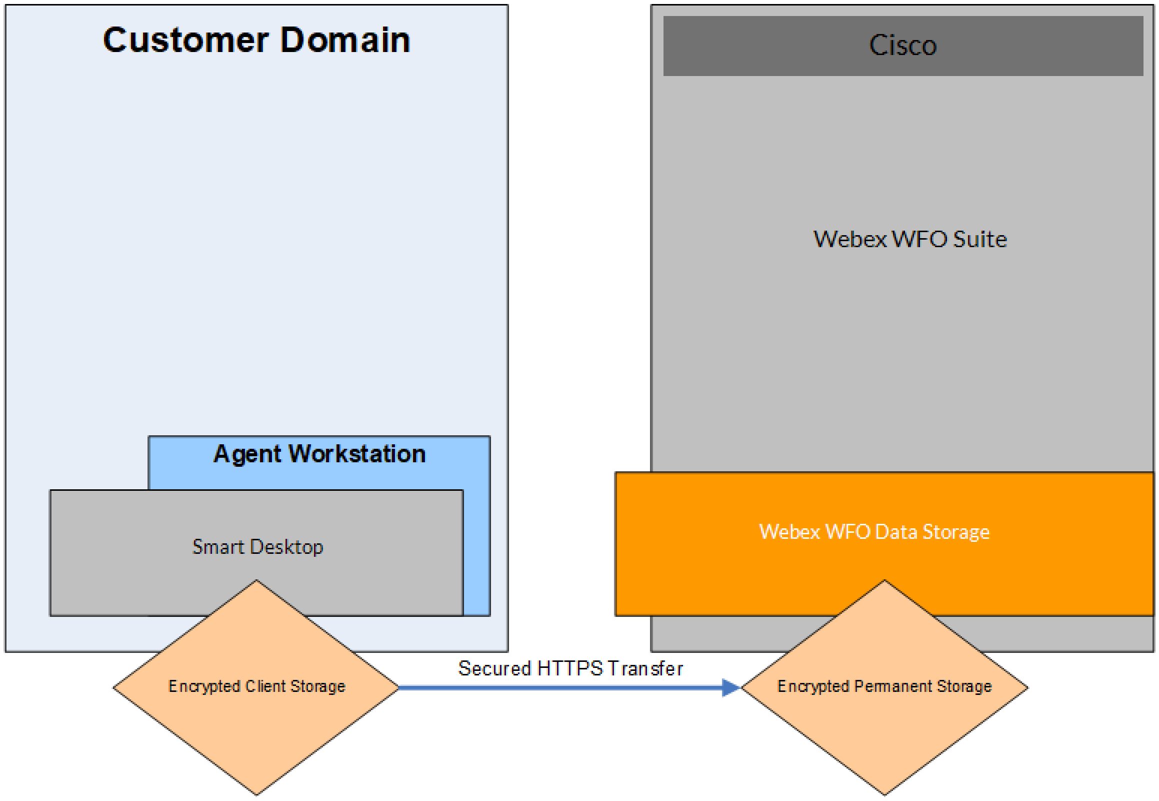

Amazon Web Services
High speed network storage
Encrypted
Opus Audio Format
WebM Video Format
Non-configurable Storage Option for Tenants
Copied to Media File Cache
Unencrypted for Playback
Data Type
Analytics Speech Processing (Storage)
Media Playback (Cached 24 Hours)
Archive Retrieval (Cached 24 Hours)
Media File Cache
Copied to Media File Cache
Unencrypted for Playback
Media file standard storage
Encrypted
Opus Audio Format
WebM Video Format
Typically One-Two Year Retention
Copied to Media File Cache
Unencrypted for Playback
Customer Cloud Instance
ACD
User workstation with audio capture
Smart Desktop
Webex WFO Cloud
Media, metadata, and Analytics data upload
Delayed Response
Playback Request
User Notified When Available
Media file archival storage for delayed access
Encrypted
Opus Audio Format
WebM Video Format
Typically Long-term Retention
Additional Applications
Elastic Grid Computing Platform
Applications
Web
Database
Recording Storage
powered by amazon web services

Cloud Storage for Customer-hosted ACD deployments


Amazon Web Services
High speed network storage
Encrypted
Opus Audio Format
WebM Video Format
Non-configurable Storage Option for Tenants
Customer Site
Data Type
Analytics Speech Processing (Storage)
Media Playback (Cached 24 Hours)
Archive Retrieval (Cached 24 Hours)
Media File Cache
Copied to Media File Cache
Unencrypted for Playback
Copied to Media File Cache
Unencrypted for Playback
Media file standard storage
Encrypted
Opus Audio Format
WebM Video Format
Typically One-Two Year Retention
Webex WFO Data Server
CTI Service
Signaling Service
ACD
PBX
Copied to Media File Cache
Unencrypted for Playback
User Workstation
Audio Capture Service
Webex WFO Cloud
Media, metadata, and Analytics data upload
Delayed Response
Playback Request
User Notified When Available
Media file archival storage for delayed access
Encrypted
Opus Audio Format
WebM Video Format
Typically Long-term Retention
Additional Applications
Elastic Grid Computing Platform
Applications
Web
Database
Recording Storage
Smart Desktop
Staged Upload Service
powered by amazon web services

Recording Encryption

The following diagram describes the encryption of recordings in Webex WFO.



All data is encrypted and transported via secured HTTPS/SSL from customer premise to Webex WFO for processing and storage.

In cloud deployments, the available encryption method is RSA-2048 (with asymmetric keys) and AES-256 for media recorded by Webex WFO.

In cloud deployments of Webex WFO, only the tenant (not Webex WFO Cloud Operations) controls the keys used to encrypt recordings, and these keys are stored in the tenant’s database. In addition, a second layer of encryption is embedded into Webex WFO, which Webex WFO Cloud Operations also does not have access to.