Webex WFO Design Guide

For Deployments with Classic WFM

First Published: July 10, 2020
Last Updated: December 27, 2024

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

Contents

Introduction

The *Webex WFO Cloud Platform Design Guide* provides a high-level overview of the structure and components of Webex WFO. The guide details the following:

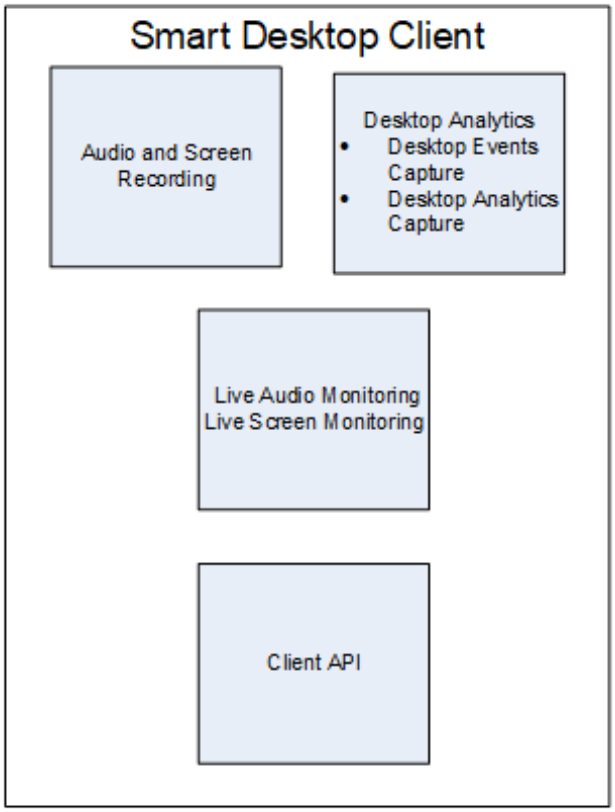
- Edge components
- System requirements
- Platform ACD configurations
- Platform capture configurations
- Data transfer flowcharts

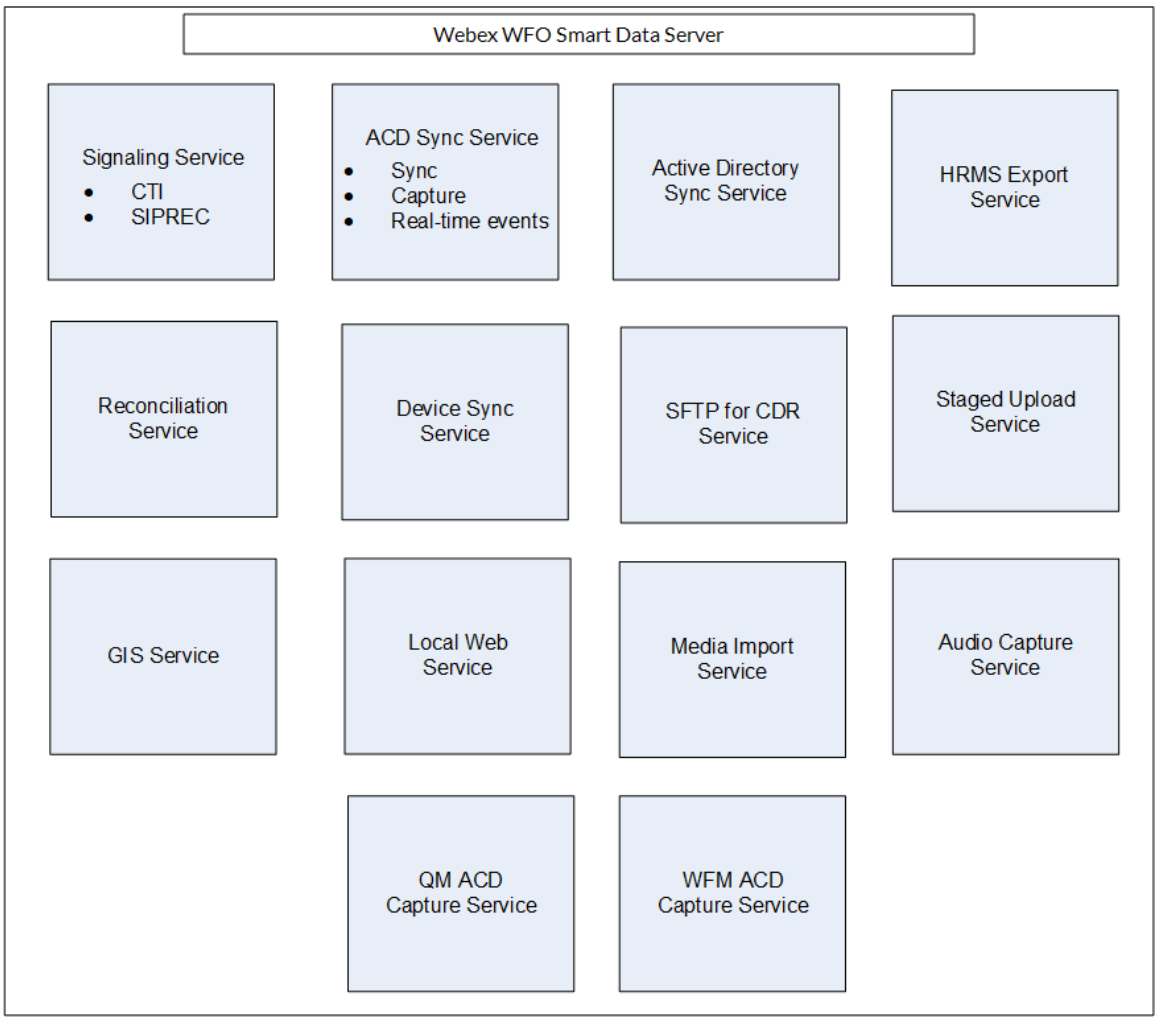
The Cloud Design Guide provides generalized knowledge on the aforementioned details.

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.

Edge components

The Webex WFO Edge components are generally deployed at an on-premises or remote customer site. The components as a whole comprise the Webex WFO Smart Technology Suite. The images below describes the edge components of Webex WFO and the Data Server:





Webex WFO Data Server

The Webex WFO 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. Webex WFO does not support the use of PAC scripts to connect to the internet.

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

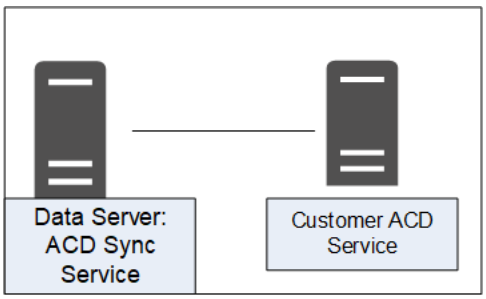
In Webex WFO, the following are functions of the Data Server, their descriptions, and the service they align to.

- 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.



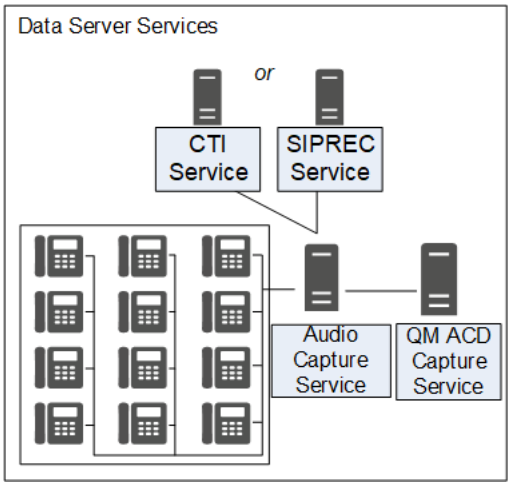
ACD Sync Service connectivity

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.



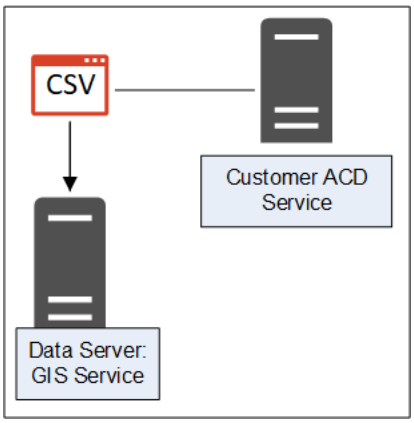
Audio Capture Service connectivity

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

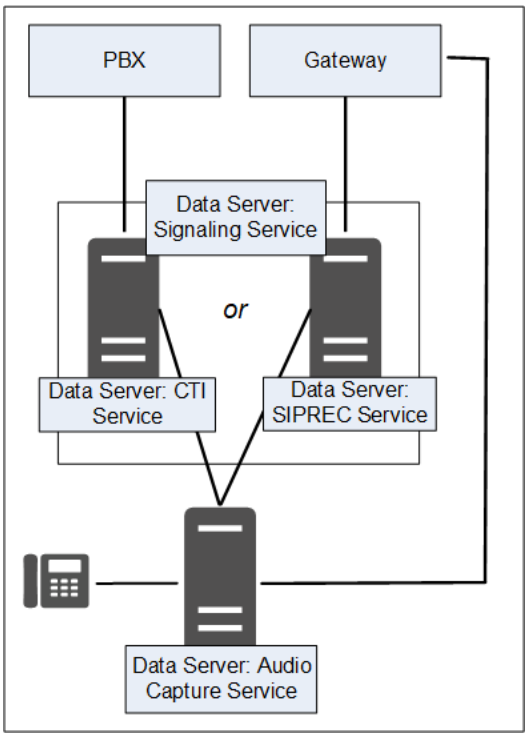
Webex WFO Signaling service

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.



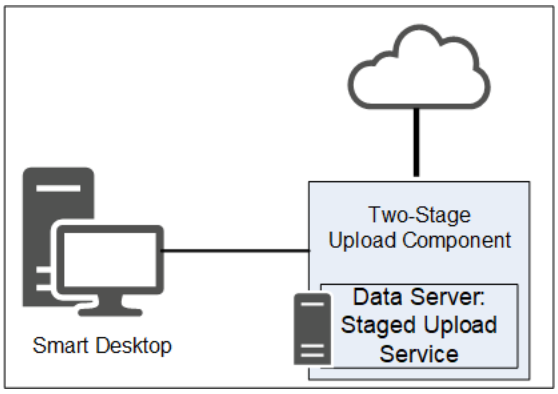
Signaling Service connectivity

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.

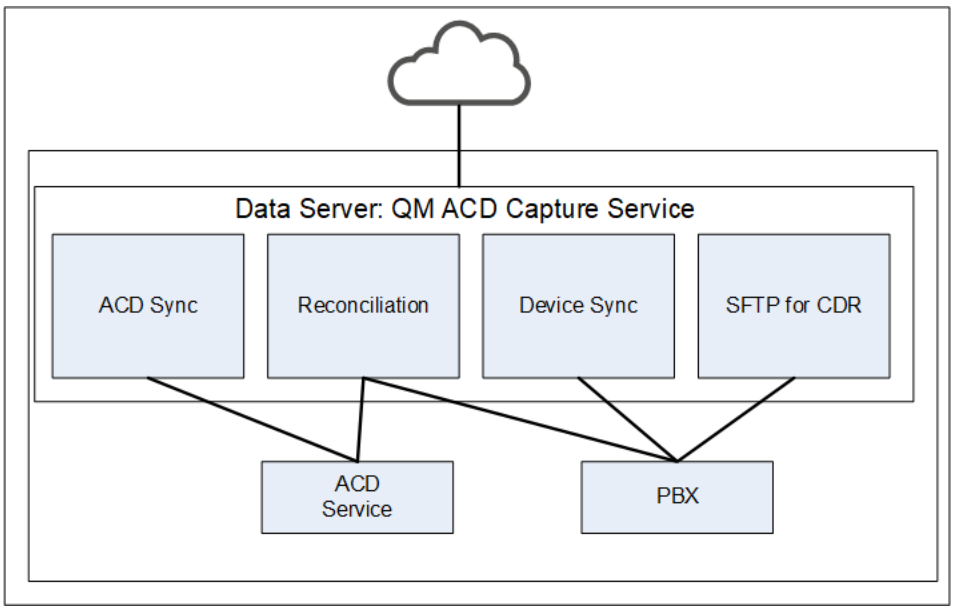
Staged Upload service connectivity

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.

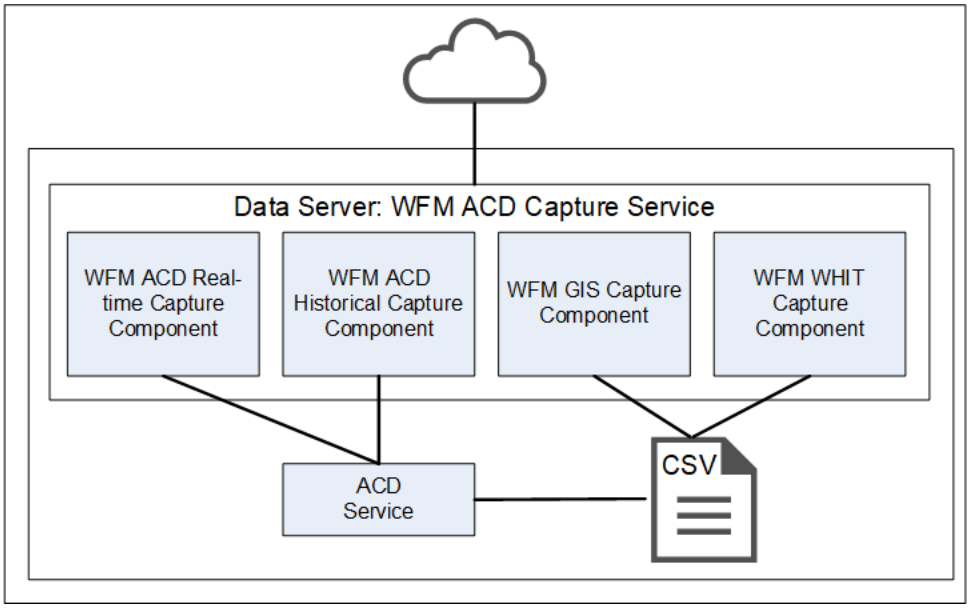
QM ACD Capture Service connectivity

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.



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

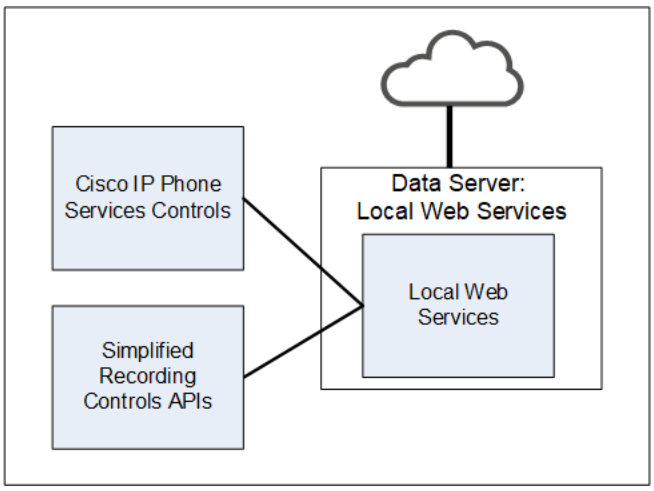
The following table lists the basic connectivity to the WFM ACD Capture service:

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.



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.

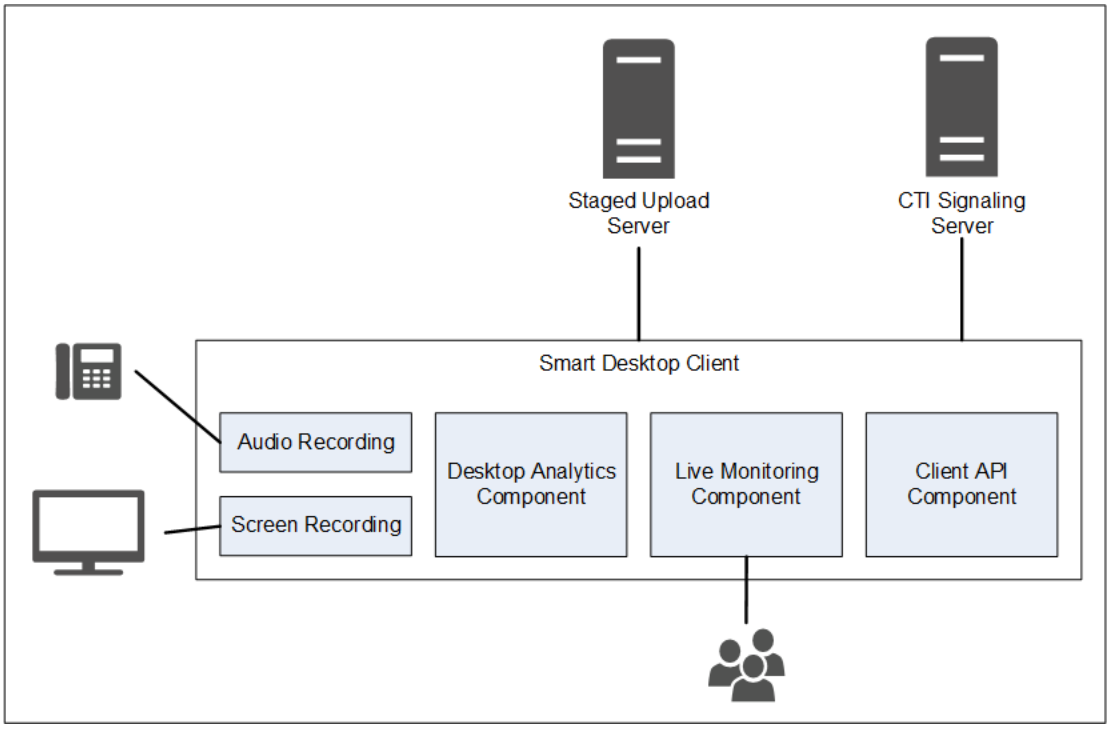
Local Web Services service connectivity

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

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)

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.

Supported environments

Webex WFO supports a number environments and technologies.

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

Desktop hardware

The hardware requirements for Webex WFO desktops are as follows:

Desktop Hardware	
NIC	100 Mbit NIC NICs must support Promiscuous Mode. Configure Windows power settings to disable “Allow the computer to turn off this device to save power” on the network interface cards.
Disk space	20 GB voice recording storage (MB) = number of recordings × average call length × 0.5 MB per minute **NOTE** This formula is based on a 64 kbps (kilobits per second) audio bitrate. [(64 kbps × 60 sec) ÷ 8 bits] ÷ 1024 KB = 0.46875 MB per minute screen recording storage (MB) = number of recordings × average call length × 1.5 MB per minute

Desktop Hardware	
	NOTE The storage requirements for screen recordings depend on three factors: recording length, monitor resolution, and the number of monitors being recorded. The value shown here is based on a single monitor. Each additional monitor is recorded separately, so you must apply this formula for each monitor.
CPU	Intel Core 2 Duo 2.0 GHz, Core i3, AMD Athlon 64 X2 or better
Memory	2 GB

Desktop software

.NET Framework

Webex WFO Smart Desktop requires .NET Framework 4.5 for Webex WFO Analytics features. If .NET Framework is not installed, Webex WFO cannot 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.

Browsers

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

Desktop Analytics plug-in/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 Calabrio Analytics browser extension/plug-in enabled. The plug-in 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 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 plug-in in Microsoft Edge Chromium

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

Enable the Desktop Analytics plug-in in Chrome

The Chrome extension can be downloaded or installed through GPO settings. Download and install the Calabrio Analytics Plug-in, version 0.2.0.4. 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.

Port usage

The port requirements for the Webex WFO 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: Avaya CM with Contact Center Elite
- 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, Avaya Aura Communication Manager Recording
- Data Server—Signaling: CTI, Cisco Unified Communications Manager Network Recording
- Data Server—Signaling: SIPREC

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	SFTP, Data Server	CUCM Billing Service	—

Port	Use	Source	Destination	Notes
TCP 8443	Communication between CUCM AXL and Regional Data Server ACD Sync Settings on the Data Server	Data Server	CUCM AXL	—
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	Data Server	Cisco Unified CCE AWDB SQL Server Database	—
TCP 1433 TCP 1434	Communication between the Cisco Unified CCE HDS SQL Server Database and both the Regional Data Server Reconciliation Settings and the Regional Data Server ACD Capture Settings on the Data Server	Data Server	Cisco Unified CCE HDS SQL 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	Data Server	Cisco Unified CCE CTI Service (Side A)	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	Data Server	Cisco Unified CCE CTI Service (Side B)	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	Data Server	Unified CCX	—

Port	Use	Source	Destination	Notes
	both the Regional Data Server ACD Sync Settings and the Regional Data Server ACD Capture Settings		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	Data Server	Cisco Unified CCX CTI Service (Side A)	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 B) and the Recording CTI Signaling Server Settings on the Data Server	Data Server	Cisco Unified CCX CTI Service (Side B)	Side B Default. This is the RMCM 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	Audio Capture (Record Server)	—

Port	Use	Source	Destination	Notes
UPD 49152–65535	Live audio monitoring—RTP	Audio Capture (Record Server)	Supervisor's browser	—
Data Server—Signaling: CTI				
TCP 443	Signaling Server	Signaling Server	Cisco API	—
TCP 52102	Recording Signaling	Audio Capture (Record Servers) or Smart Desktop clients	Signaling Server	—
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

Port	Use	Source	Destination	Notes
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	—
TCP 59106	Recording signaling	Audio Capture (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.

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. From there, it performs transcoding and streaming.

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.

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.

- Tenants - Use the tenant Storage Location section on the Tenants page to assign and define the storage location for each tenant.

Storage Offerings

Webex WFO Cloud uses intelligent tiering for storage with a single price per GB per month for your total usage. New files and files that have been accessed recently are available immediately. Older files that have not been accessed recently are retrieved from a slightly slower storage tier that they may have been moved to. Older files typically only take a few seconds to be retrieved.

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.
- In WFM, you can import historical data and import forecasts.

NOTE The bulk contact export of root recordings is not supported.

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.

Export contacts in bulk

You can export data for multiple contacts using the Bulk Contact Export option on the Interactions page 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.

NOTE Contacts and metadata are exported as CSV files.

Schedule a recurring bulk contact export

1. On the Interactions page, create and save a filter set.

   IMPORTANT You must fully configure all the filters you add to your filter set. If you do not fully configure all the filters, the bulk context export will fail.

   EXAMPLE You add the **Predictive Net Promoter Score** filter to your filter set. You select **Equals** from the **Operator** drop-down list but do not enter a number in the **Score** field. Not fully configuring this filter will cause the bulk contact export to fail.

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 Interactions page, create and save a filter set.

   > **IMPORTANT** You must fully configure all the filters you add to your filter set. If you do not fully configure all the filters, the bulk context export will fail.

   > **EXAMPLE** You add the **Predictive Net Promoter Score** filter to your filter set. You select **Equals** from the **Operator** drop-down list but do not enter a number in the **Score** field. Not fully configuring this filter will cause the bulk contact export to fail.

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 1,000 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.

Storing and accessing Bulk Contact Files

Webex WFO exports and stores bulk contact files in the Exports folder in the external storage location you configure (see Application Management > Global > System Configuration > External Storage).

Data Transfer Flow Diagrams

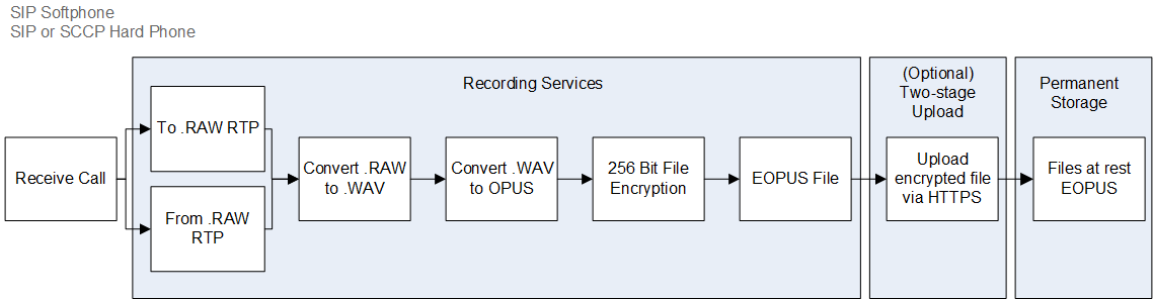
This topic includes diagrams illustrating the following:

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

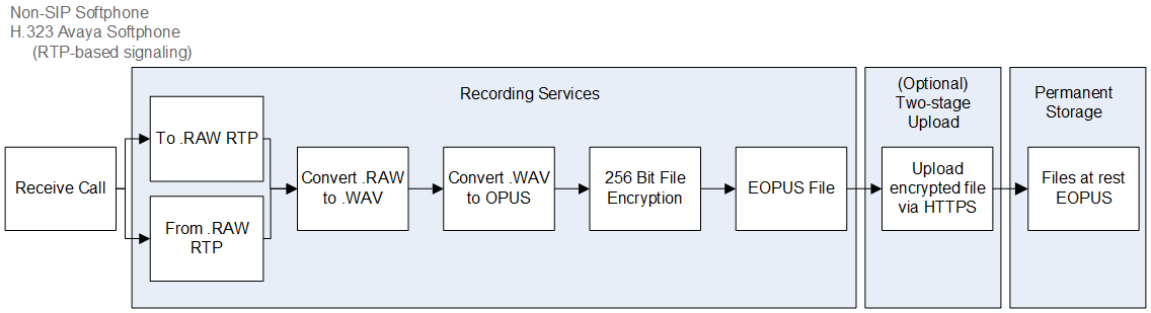
Smart Desktop Capture Data Flow Diagrams

This topic includes diagrams that describe the Smart Desktop data flow.

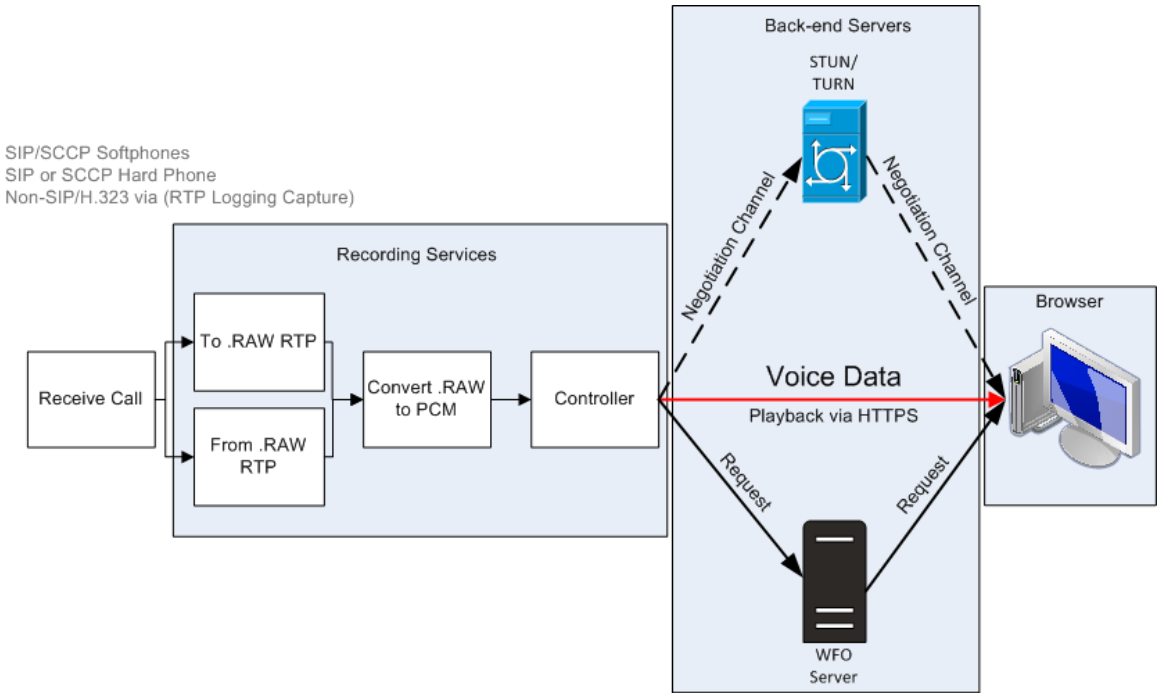
Smart Desktop SIP/SCCP Signaling



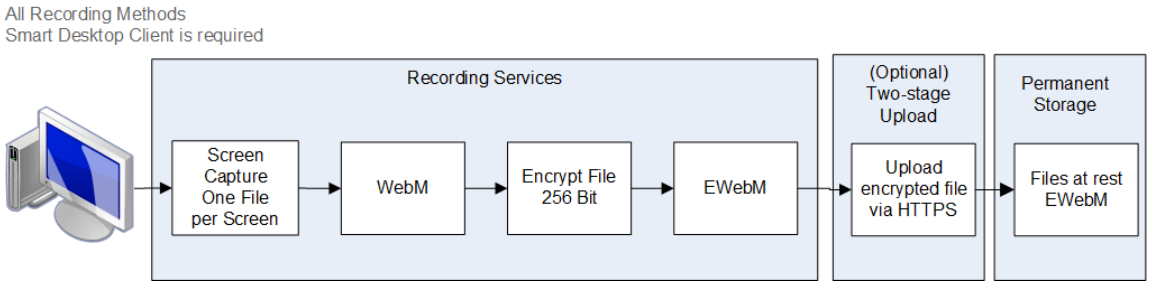
Smart Desktop RTP Logging



Smart Desktop Live Audio Monitoring

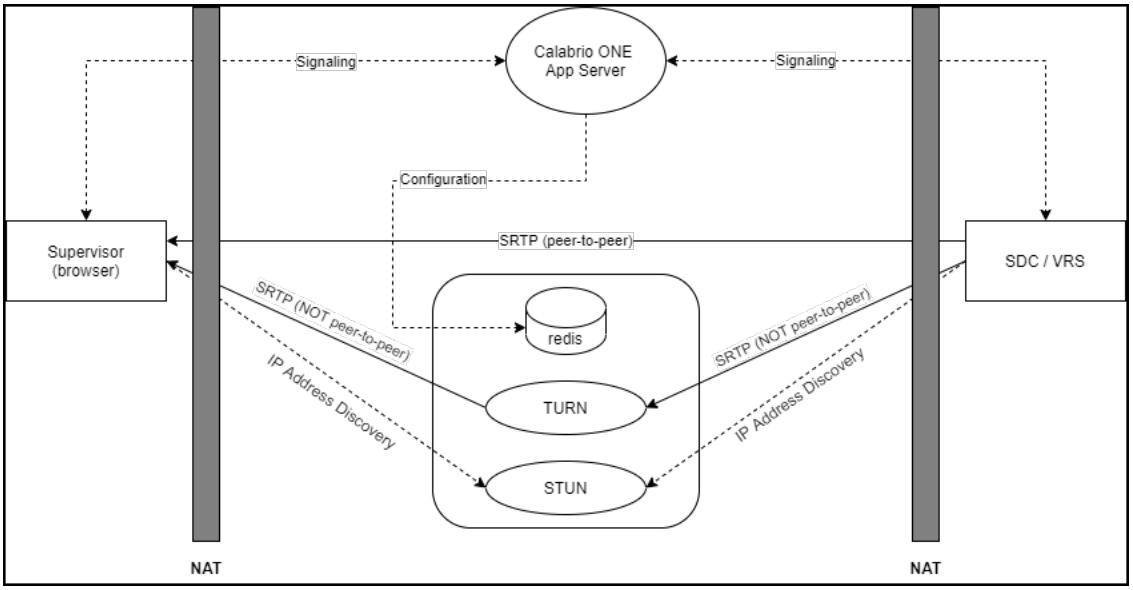


Smart Desktop Live Screen Monitoring



NOTE Smart Desktop screen and audio recording uses AES 256-bit encryption if the recording takes place inside Webex WFO.

Smart Desktop Live Monitoring Connections



Connection	Ports	Protocol	Notes
Signaling	80, 443	TCP	By websocket
Configuration	6379	TCP	STUN/TURN administration using a System Administrator role in Webex WFO
SRTP (peer-to-peer)	49152–65535	UDP	Audio and visual media

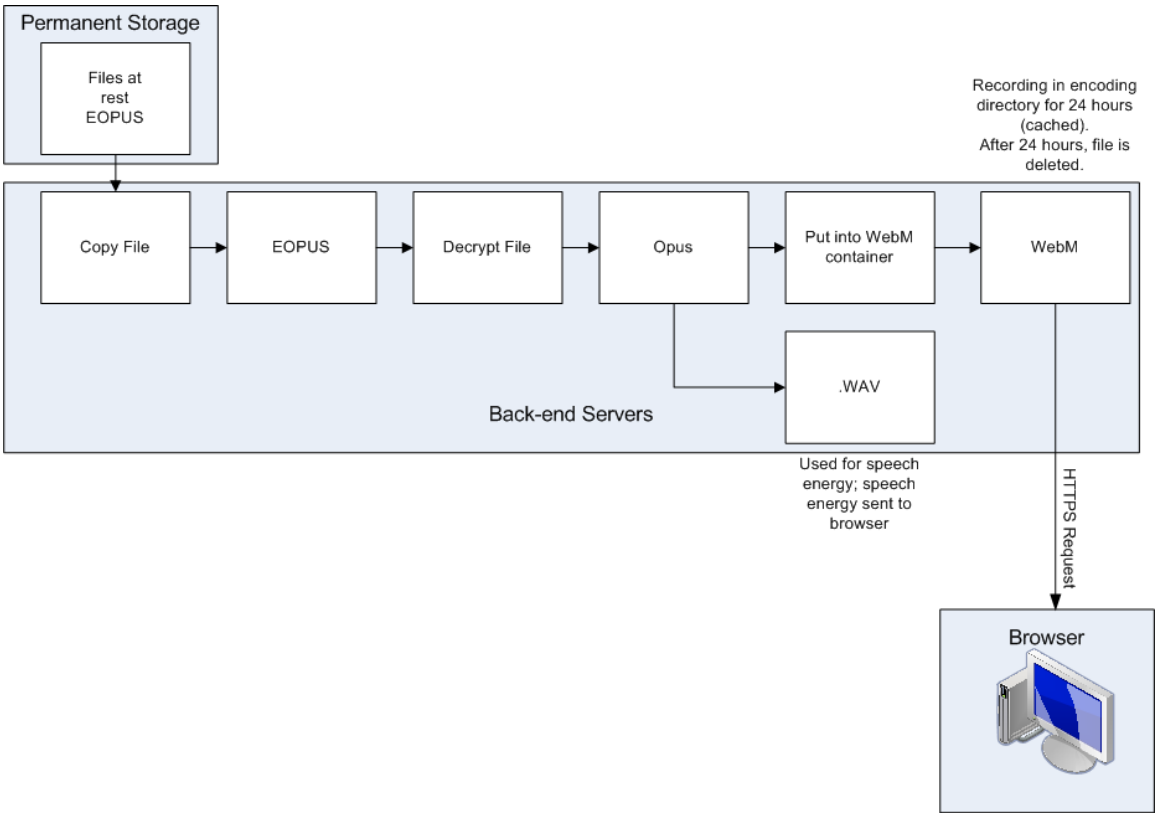
Connection	Ports	Protocol	Notes
SRTP (not peer-to-peer)	49152–65535	UDP	Audio and visual media
IP Address Discovery	3478	UDP and TCP	—

Recording Capture and Playback Data Flow Diagrams

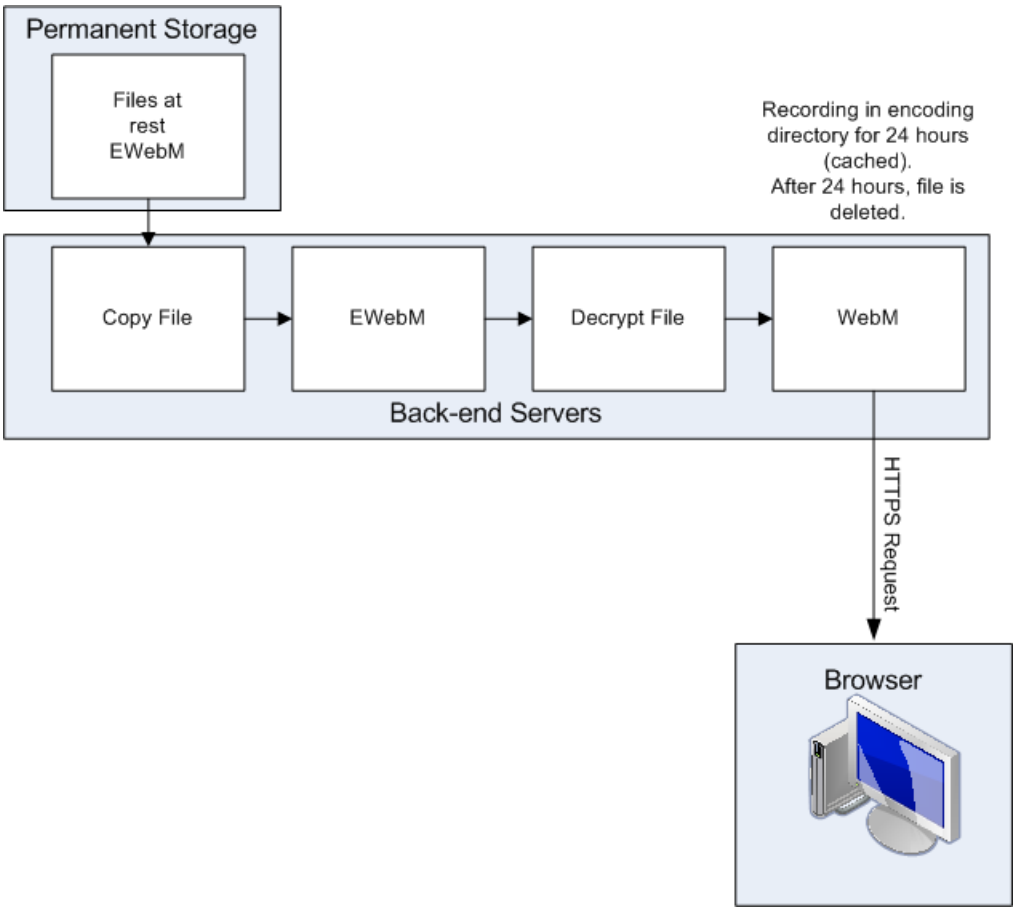
This topic describes the process of playing back contact recordings.

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.



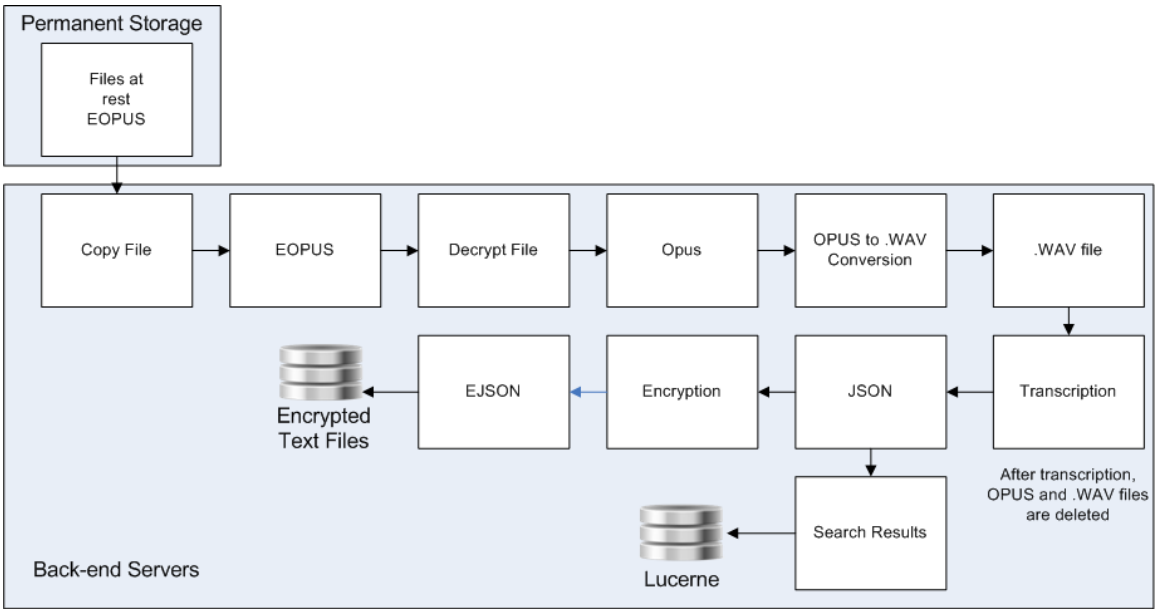
Screen Playback Data Flow Diagram



Analytics Data Flow Diagram

This topic describes the data flow for processing Analytics data.

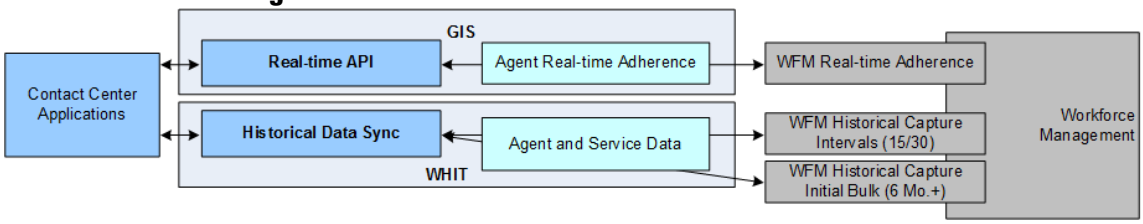
Speech Transcription Analytics Data Flow Diagram



WFM Data Flow Diagram

This topic describes the data flow for precessing WFM real-time adherence and historical data.

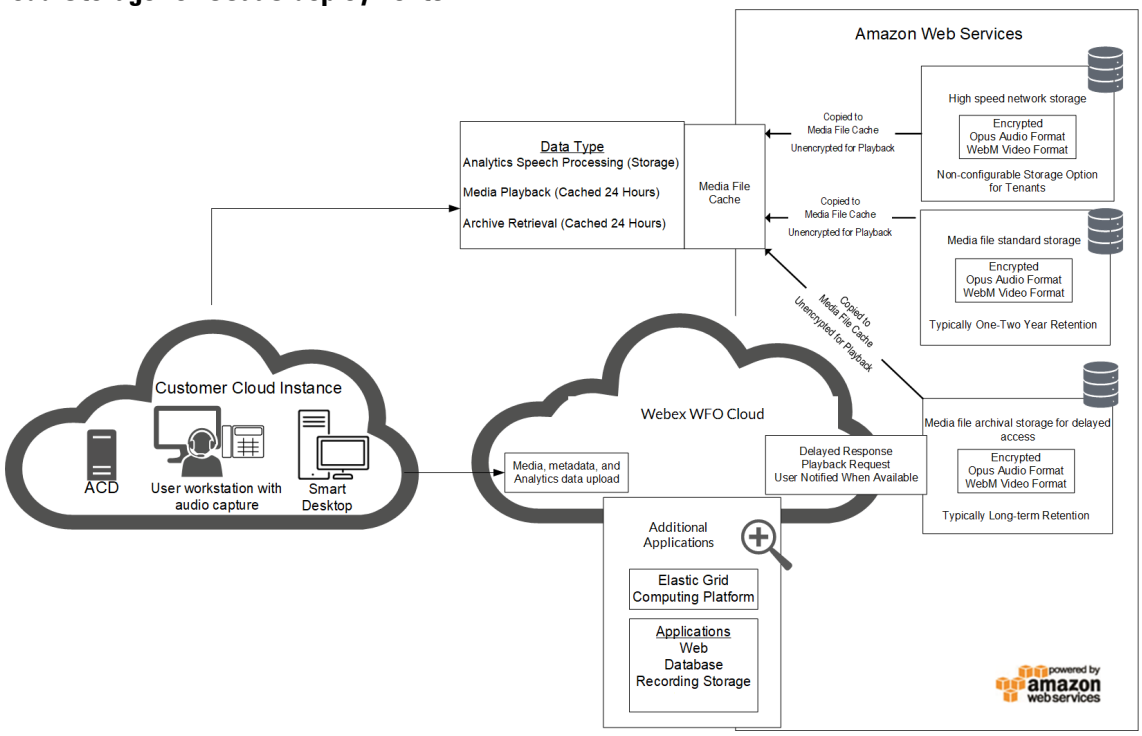
WFM Data Flow Diagram



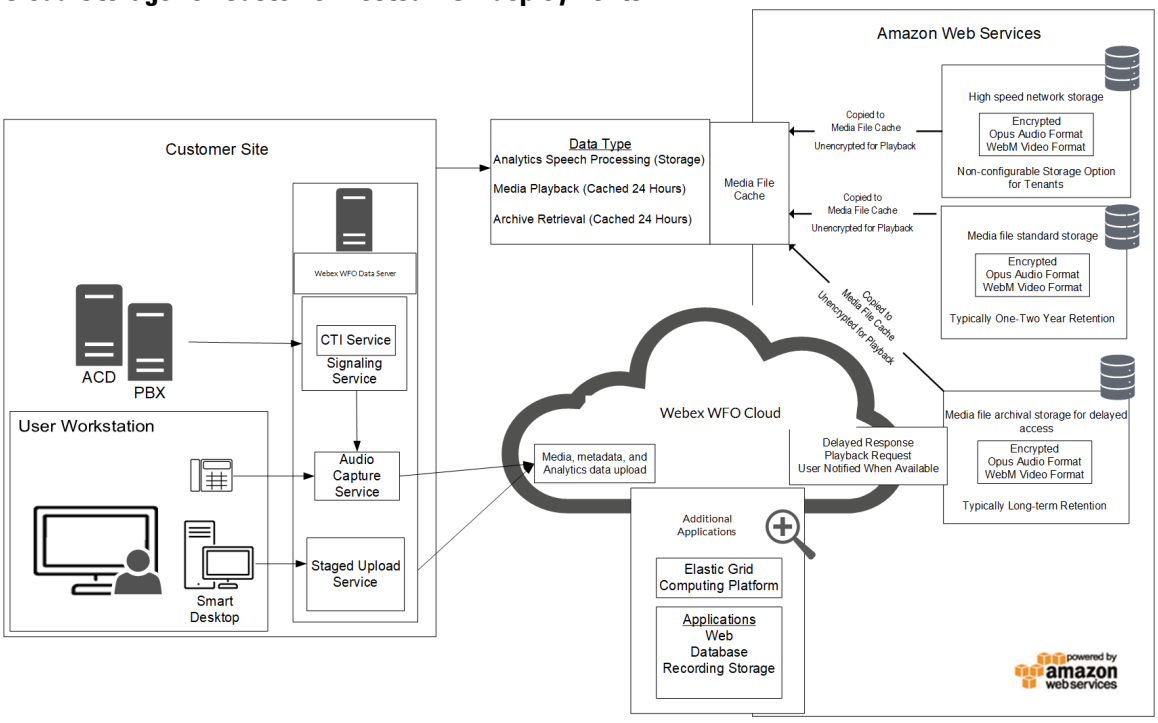
Cloud Storage Data Flow Diagrams

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

Cloud Storage for CCaaS deployments



Cloud Storage for Customer-hosted ACD deployments

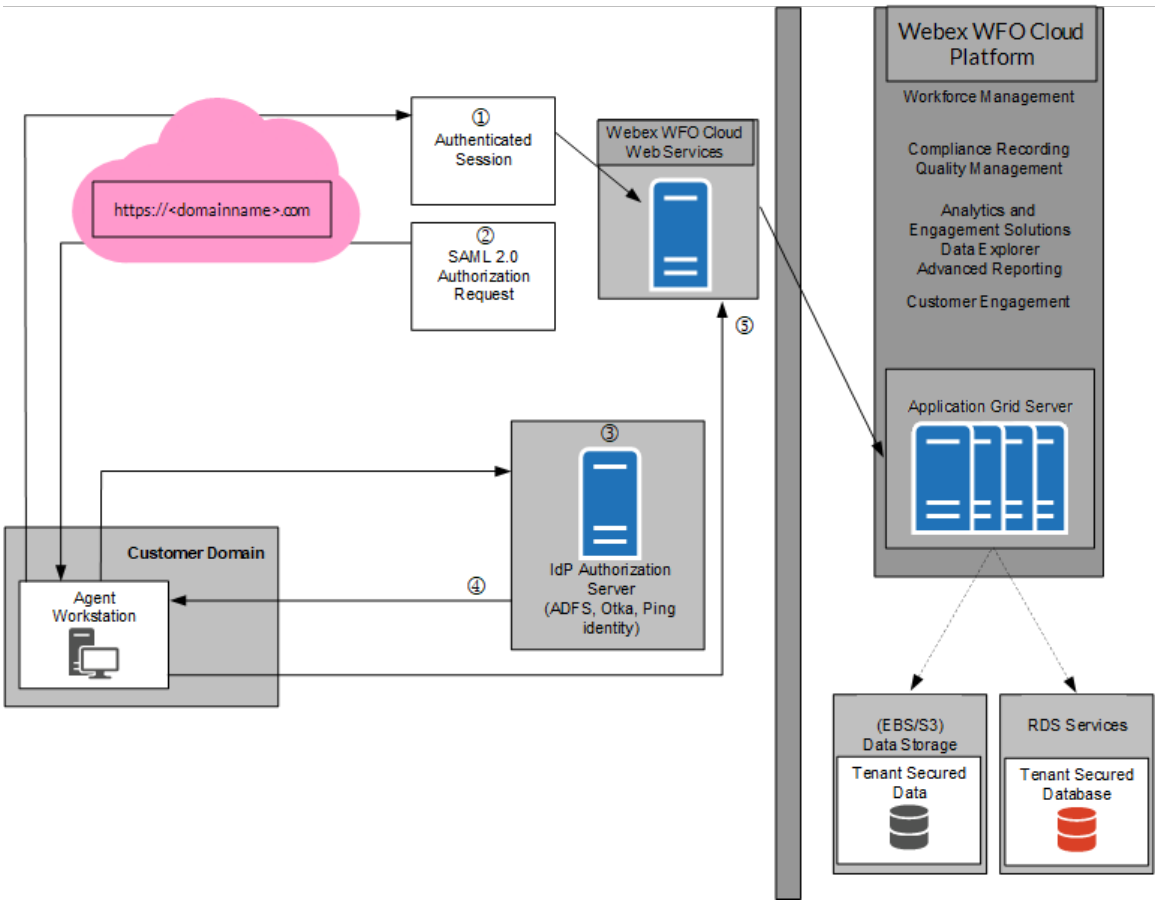


SAML Authentication Process Flow Diagram

This topic describes the process for SAML authentication.

All authorization and authentication of known user identities is managed by the customer within the Identity Provider (Authorization Server) and outside of Webex WFO Cloud. Webex WFO acts as the service provider (resource server) and consumes all user identities from the customer's identity provider (IdP). Known user identities that are active within the customer's IdP are provided proper authorization to access your organization's URL (for example, `https://Ciscocloud.com`) through a SAML authorization communication between the customer's IdP and Webex WFO's Resource Server.

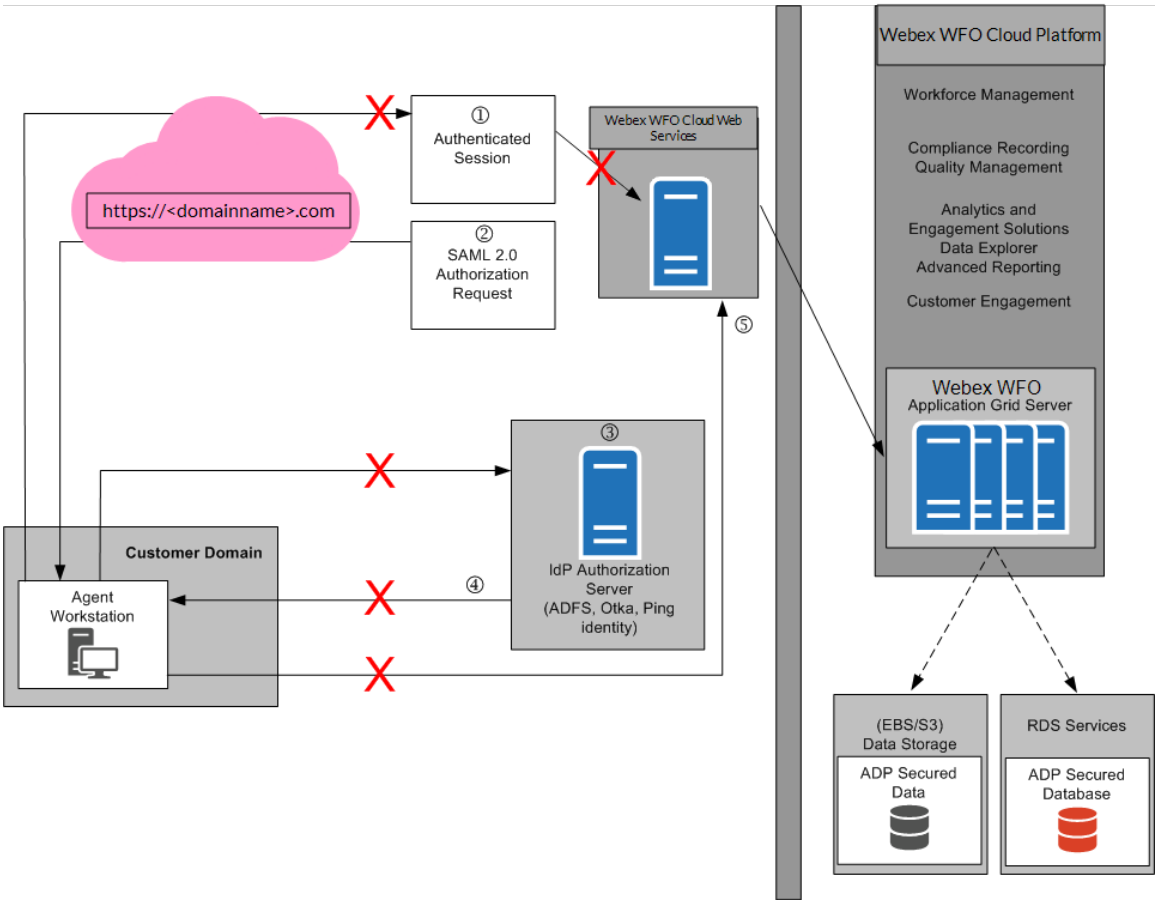
SAML Approval process



Steps for SAML authentication:

1. The user accesses the Webex WFO URL (for example, `https://Ciscocloud.com`); if the user has an authenticated session with the IdP (Authorization Server), the user is allowed access.
2. If the user does not have an authenticated session, create a SAML Authentication Request and redirect back to browser to the IdP (Authorization Server).
3. If the user is not already authenticated with the IdP (Authorization Server), the user is asked to log in.
4. After the user successfully logs into the IdP, or if they were already logged in, the IdP sends a redirect back to the browser with a SAML response.
5. Webex WFO validates the SAML response, receives the user's information from the SAML response, creates an authenticated session, and allows access.

SAML Denial Process

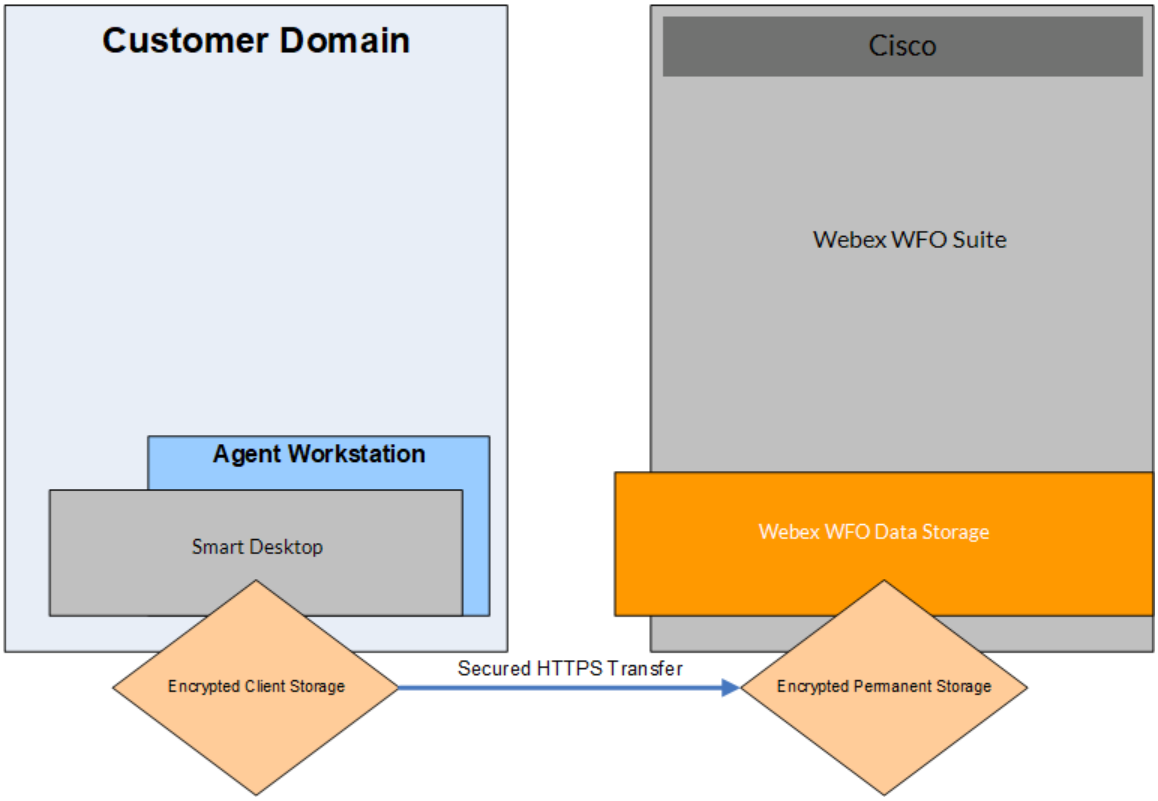


Steps for SAML authentication denial:

1. The user's authentication access has been terminated in the IdP.
2. If the user does not have an authenticated session, create a SAML Authentication Request and redirect back to browser to the IdP (Authorization Server).
3. Because the user is not authenticated with the IdP (Authorization Server), the user is asked to log in.
4. The user is unable to authenticate with the IdP (Authentication Server), and is not authorized.
5. The user is denied access.

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.