Webex WFO Cloud Installation Guide

For Deployments with Classic WFM

First Published: July 10, 2020
Last Updated: February 28, 2025

Contents

Introduction

Webex WFO is a highly scalable, multi-tenant workforce optimization (WFO) platform. It includes the ability to perform call recording, quality management, workforce management, and analytics.

This document explains how to install Webex WFO in a cloud environment.

Localization and supported languages

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

- User interface

    - QM, WFM, Analytics, and Insights

    - In-product training

- Documentation

    - Online help

    - PDF guides

- Analytics

    - Transcription: Speech to text and transcription search.

    - Interaction Summary: A summary of an audio contact based on the contact's transcript.

    - Phrase hits: Identification of predefined phrases. Webex WFO identifies phrase hits based on speech-to-text transcriptions of contacts.

    - Sentiment: Text-based sentiment analysis.

    - Predictions: Machine-learning predictions of evaluation scores and net promoter scores.

    - Text: Analytics for chat, email, agent notes, and social media.

Components of Webex WFO are available in these languages.

Language	UI	Mobile App	In-Product Training	Analytics								Documentation
				Transcription*	Interaction Summary	Phrase Hits	Sentiment	Predictions	Text Analytics	Trending Topics	Auto QM	
Arabic (ar-AR)				x	x	x		x				
Simplified Chinese (zh)	x		Limited									
Traditional Chinese (zh-TW)	x		Limited									
Danish (da)	x		Limited	x	x	x		x	x			
Dutch (nl)	Limited		Limited	x	x	x		x	x			
English (en)	x	x	x	x	x	x	x	x	x			x
Australian English (en-AU)				x	x	x	x	x	x			
South African English (en-ZA)				x	x	x	x	x	x			
UK English (en-GB)				x	x	x	x	x	x	x	x	
US English (en-US)	x	x	x	x	x	x	x	x	x	x	x	x

Language	UI	Mobile App	In-Product Training	Analytics							Auto QM	Documentation
				Transcription*	Interaction Summary	Phrase Hits	Sentiment	Predictions	Text Analytics	Trending Topics		
Finnish (fi)	x		Limited	x	x	x		x				
French (fr)	x		Limited	x	x	x		x	x			Limited
Canadian French (fr-CA)	x			x	x	x		x	x			
German (de)	x		Limited	x	x	x		x	x			Limited
Italian (it)	x		Limited	x	x	x		x	x			
Japanese (ja)	x		Limited									
Korean (ko)	x		Limited									
Norwegian (nb)	x		Limited	x	x	x		x	x			
Polish (pl)	Limited		Limited	x	x	x		x	x			
Portuguese (pt)	x		Limited	x	x	x		x	x			
Brazilian Portuguese (pt-BR)	x		Limited	x	x	x		x	x			

Language	UI	Mobile App	In-Product Training	Analytics								Documentation
				Transcription*	Interaction Summary	Phrase Hits	Sentiment	Predictions	Text Analytics	Trending Topics	Auto QM	
Russian (ru)	Limited											
Spanish (es)	x		Limited	x	x	x		x	x			Limited
Mexican Spanish (es-MX)				x	x	x		x	x			
Swedish (sv)	x		Limited	x	x	x		x	x			

* Some supported languages might require additional configuration for your Webex WFO implementation. Consult with Support to ensure the language you want to transcribe is configured for you.

Adding additional languages or expanding current offerings requires collaboration with Cisco. Contact your account representative for more information.

System Configuration

This diagram displays a typical Webex WFO cloud deployment.
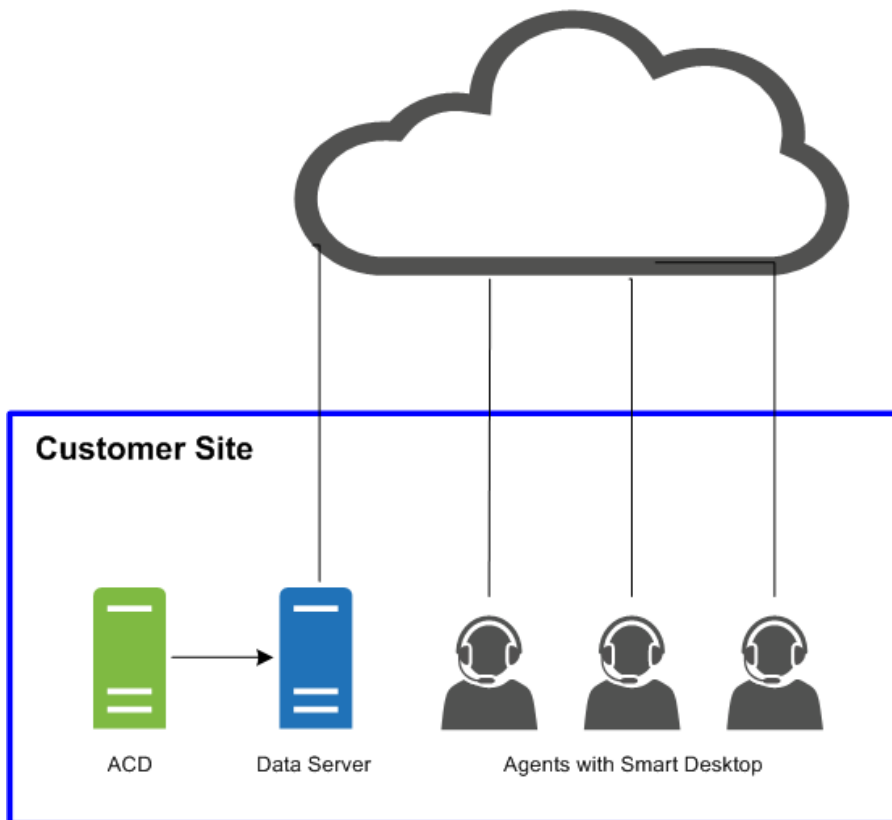
This diagram displays a typical Webex WFO cloud deployment with a thin client environment.

Customer Site

Thin Client Server
Smart Desktop

ACD

Data Server

Agents with thin client desktops
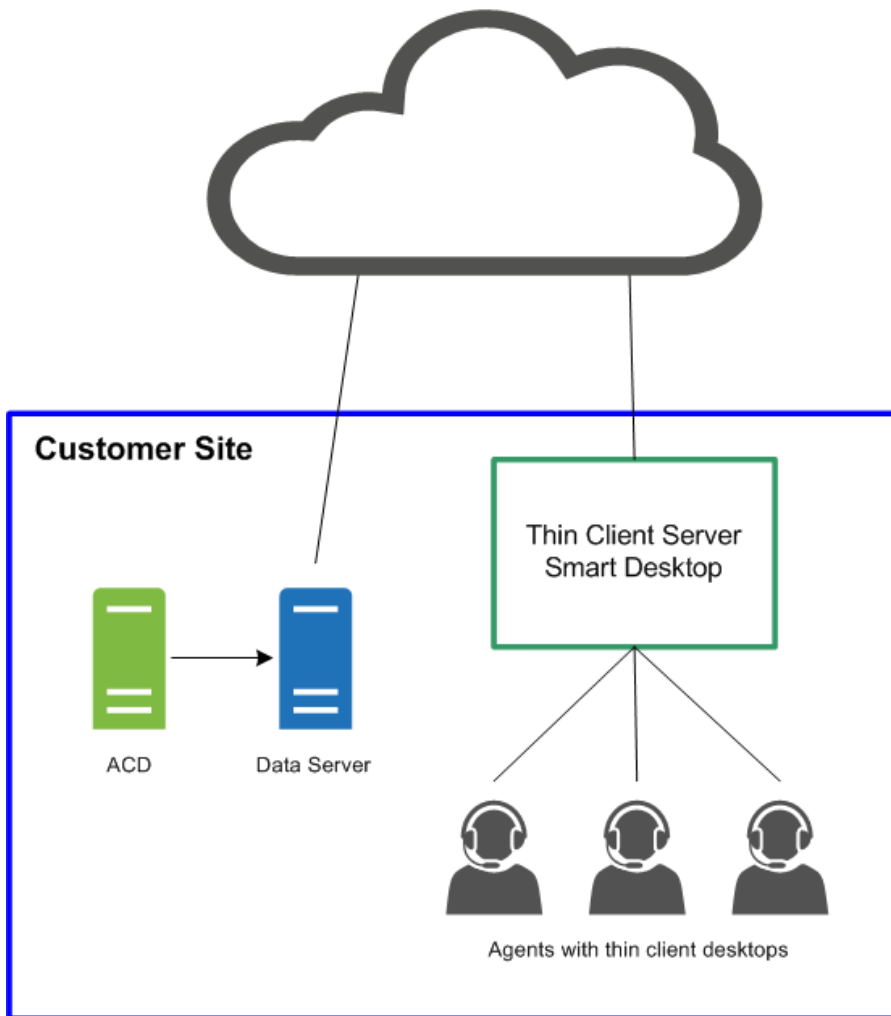
Supported environments

Webex WFO supports a number environments and technologies.

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

Supported phones

Webex WFO supports the following phones.

Hard phones

Refer to the Unified CM Silent Monitoring/Recording Supported Device Matrix website for a list of supported Cisco hard phones.

https://developer.cisco.com/site/uc-manager-sip/documents/supported/

Supported codecs

Webex WFO supports the following codecs:

- g711
- g722
- g729

> **NOTE** The codec packet size must be at least 20ms to provide usable audio quality.

Using multiple soft phones

If you are using multiple soft phones at the same time, the soft phones must not bind to a local port number that matches any of the port numbers configured on the Global Settings page (Application Management > QM Configuration > Global Settings > SIP Settings). For example, if the port number entered under SIP Settings is 5060, then none of your soft phones can use a local port bound to port number 5060 if you intend to use multiple soft phones at the same time.

Start the soft phone, log in if necessary, then use one of these tools to view the network connections for that process ID. If any of the network connections show a local port that matches any of the port numbers configured on the Global Settings page, you must do one of the following:

- Use the soft phone alone, with no other soft phones being used at the same time.

- Configure the soft phone so it does not use one of the listed ports.

To confirm port usage, use a tool that monitors network connections such as netstat (at the command line use parameters `-anob`), TCPView, or CurrPorts.

Supported mobile devices

Agents can access a limited version of Webex WFO on a mobile device such as a smart phone or tablet by entering the Webex WFO URL in the device's browser. The agent is automatically redirected to a mobile version of Webex WFO, where the agent logs in as usual.

> **NOTE** The mobile device must be able to access the network where Webex WFO is installed.

Agents can also view their schedules outside of work through an email client or calendar application on a mobile device or personal computer. The email client or calendar application displays the schedule as it appears in the Webex WFO interface by reading the iCalendar data file from the WFM iCalendar service.

The following clients and devices are supported for viewing a schedule outside of work:

- Apple devices such as an iPhone or iPad (in conjunction with the Apple Calendar app)

- Microsoft Outlook

- Android devices such as a tablet or phone (in conjunction with a calendar app that can read an .ics file)

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.
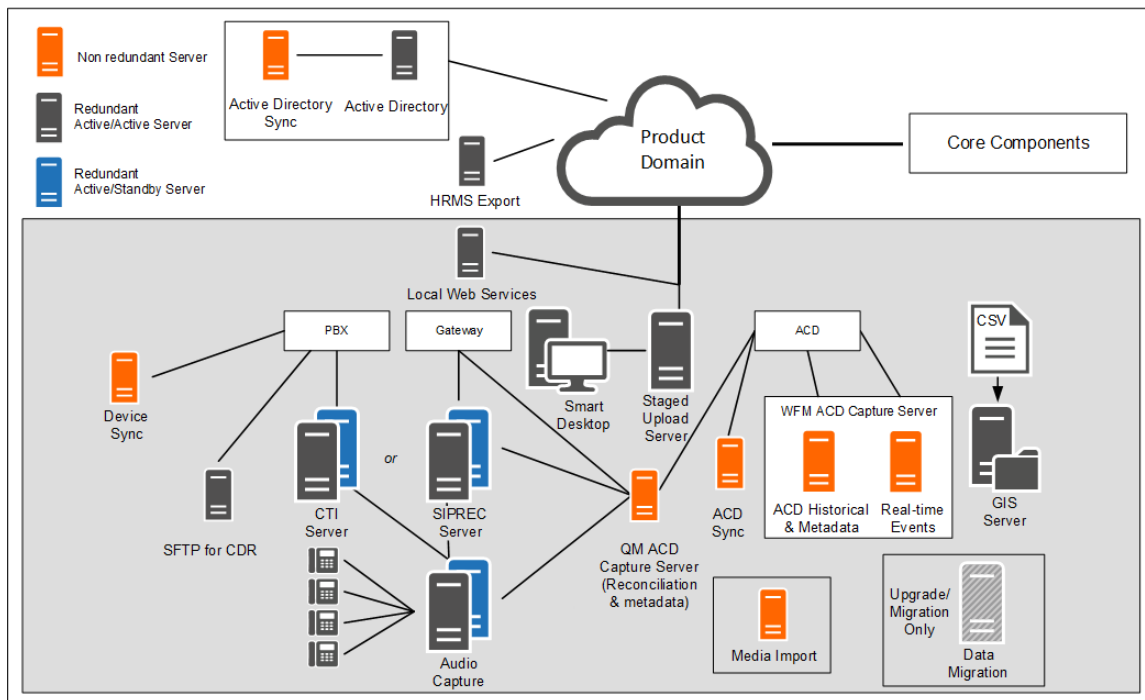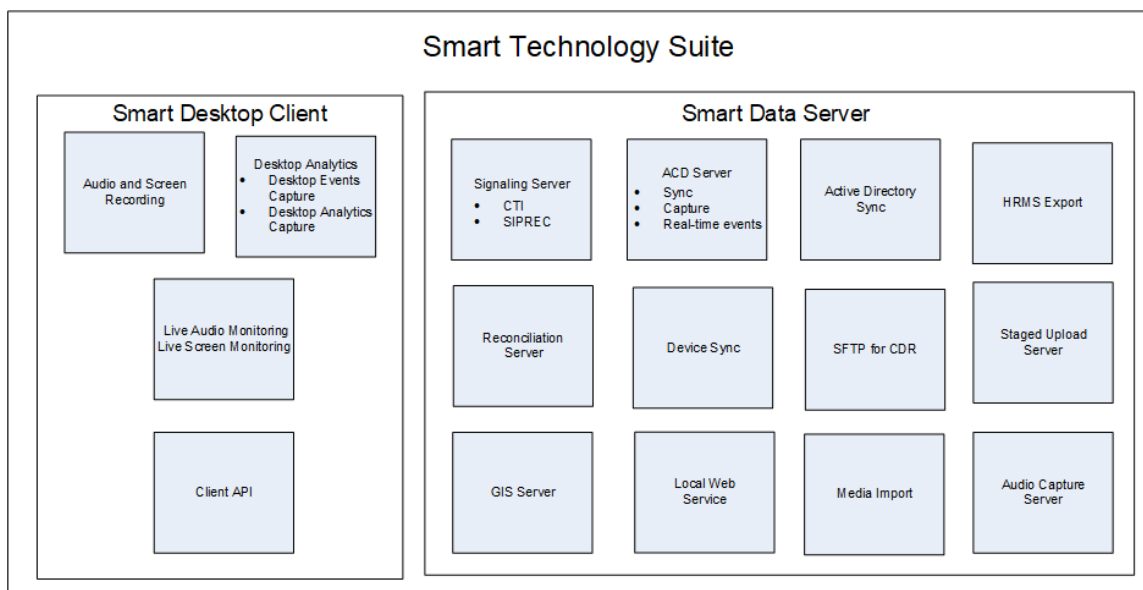
Webex WFO Smart Desktop

Webex WFO Smart Desktop captures all user data (that is, audio recording, screen recording, desktop activity, and call metadata) on an agent's desktop. Webex WFO Smart Desktop is installed on agent desktops in the contact center or on a server that hosts a supported thin client. The Smart Desktop installer must be downloaded from the Webex WFO Application Management > Administration > Downloads page.

About Webex WFO Smart Desktop

The data captured by Smart Desktop can vary depending on your license and permissions enabled in Webex WFO. You need to download the Smart Desktop installer from Application Management > Global > Administration > Downloads (see Download Smart Desktop). You also need the Desktop Analytics extension for your browser.

Audio recording using Smart Desktop depends on recording types. Contact center as a service (CCaaS) solutions record audio and send the file after the contact is completed. Customer-hosted solutions send SIP and RTP protocols because the contact is live. Webex WFO performs screen recordings using the agent desktop and recordings are uploaded after a call is completed.

Smart Desktop has the following components.

- Audio and screen recording — This component records agent calls.

- Desktop Analytics — This component provides analytics data on agent desktop recordings.

- Live Audio Monitoring and Live Screen Monitoring — These components allow supervisors to listen to an agent's audio and view an agent's screen in real time. Agent monitoring and desktop monitoring are the two monitoring types for Smart Desktop.

    Agent Monitoring — A feature for administrators and supervisors that allows them to monitor agents' audio and screens in real time.

    Desktop Monitoring — A feature that allows administrators to view users' active and installed versions of Smart Desktop on their PCs, set log levels, and remotely download logs for troubleshooting.
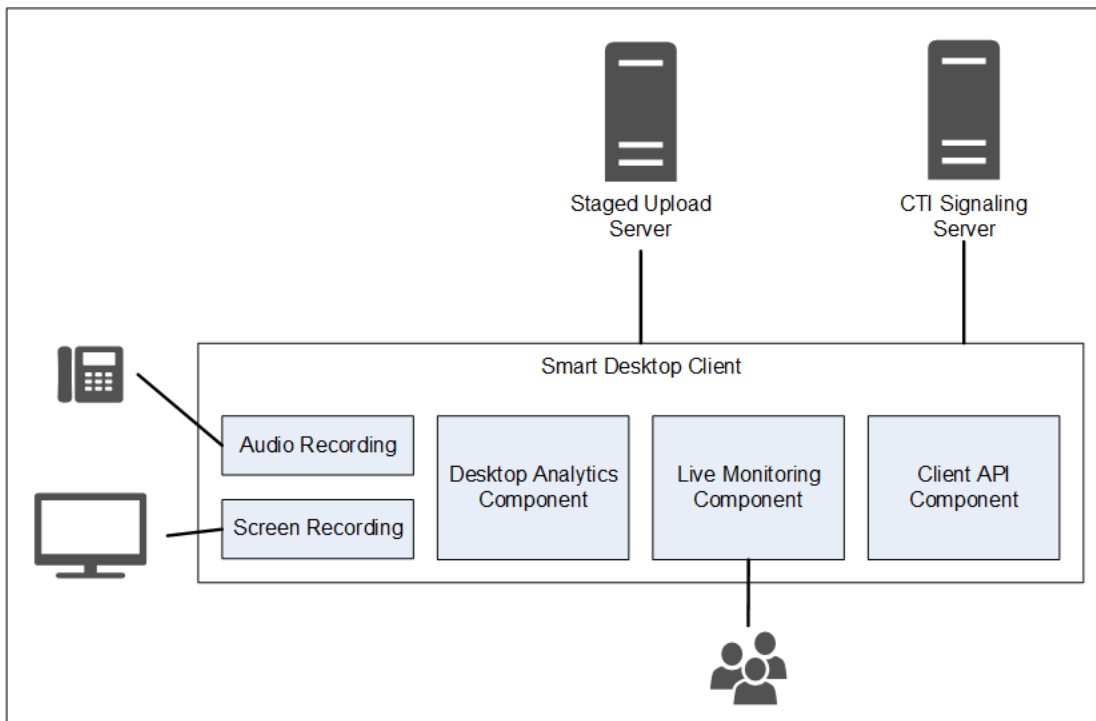
Smart Desktop Client connectivity

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)

Use the links below to navigate to different Smart Desktop topics in this document.

- Smart Desktop Requirements and Considerations

- Desktop hardware

- Smart Desktop Port Usage

- Smart Desktop Contact Metadata

- Smart Desktop Capture Data Flow Diagrams

- Installing Smart Desktop

- Enable the Desktop Analytics extension in your browser

- Test Smart Desktop

- Manage Smart Desktop

- Recording controls application

Smart Desktop Requirements and Considerations

See Thin client servers for more information and considerations when using a thin client server and Smart Desktop.

Refer to the Webex WFO Product Compatibility Matrix for supported Windows desktop operating systems and supported web browsers.

Desktop Capture Bandwidth and Sizing

- Desktop Audio Capture: 0.5 MB/min

- Screen Capture: 1.5 MB/min per monitor

EXAMPLE If one agent takes thirty calls a day with an average talk time of 5 minutes per call, the Desktop audio recording calculation would be: 0.5MB/min x 5 minutes x 30 calls = 75 MB. The Screen capture recording, if the agent has 3 screens, would be: 1.5 MB/min x 5 minutes x 30 calls x 3 screens = 675 MB.

See Desktop hardware for specific requirements on NIC, disk space, CPU, memory, and .NET Framework.

Environments

The following environments are supported in addition to computers that meet the minimum operating system requirements.

- Virtual Desktop Infrastructure (VDI)

- Terminal servers

- Citrix

- Third party agent's environment

- AWS Workspace

NOTE If your organization uses VDIs, terminal servers, or Citrix solutions, share the following information with your Cisco account representative during the installation process: termination time after a contact ends, number of machines, number of servers, and general specifications about your servers.
Terminal servers and Citrix solutions do not support Webex WFO's auto update feature.

.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.

Antivirus Real-time Scanning Exclusions

Cisco recommends excluding the following Cisco directories from antivirus real-time scanning to ensure Smart Desktop features run as expected.

- 64-bit - C:\Program Files (x86)\Calabrio ONE\Desktop*

- 64-bit - C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop*

- 32-bit - C:\Program Files\Calabrio ONE\Desktop*

- 32-bit - C:\Program Files\Common Files\Calabrio ONE\Desktop*

Firewall requirements

Webex WFO must be whitelisted and granted access through your organization's external firewall.

Web browser considerations

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

Browser plugins

See "Desktop Analytics Plug-in/Extension" in System Requirements for more information. Cisco recommends you manage your extensions/plugins through Windows GPO to ensure all dependent features are working as designed.

If users have both Microsoft Edge and Google Chrome browsers, Cisco recommends you install the browser extension on both browsers. Installing it on one browser results in Webex WFO not being able to collect data from the other browser that does not have the extension.

> **IMPORTANT** You must uninstall older browser versions before you install the latest version.

Proxy

- Smart Desktop is proxy-aware. It attempts to use a proxy that it detects.

- If an internet proxy is being used, Smart Desktop requires that the proxy supports secure web socket connections.

- All proxy connections must allow Smart Desktop software to connect to Cisco Cloud on Port 80/443.

Smart Desktop Port Usage

The port information for Webex WFO Smart Desktop components is listed below.

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

Customer-hosted solutions

Refer to the table below for customer-hosted solutions. Examples of customer-hosted solutions include Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Express, Avaya Communication Manager, and more.

Port	Use	Source	Destination	Notes
Smart Desktop				

Port	Use	Source	Destination	Notes
TCP 80, 443	Live audio monitoring (WebRTC)	Audio Capture Server*, Agent's PC	Supervisor's browser	
UDP 39500 - 43500	Recording RTP	Phone, Voice gateway**	Audio Capture Server	
UDP 49152 - 65535	Live audio monitoring (RTP)	Audio Capture Server*, Agent's PC	Supervisor's browser	
TCP 52102	Recording signaling	Audio Capture Server*, Agent's PC	Signaling Server	

*Network recording architecture

**Gateway recording architecture

CCaaS solutions

Refer to the table below for (contact center as a service) CCaaS solutions.

Port	Use	Source	Destination	Notes
Smart Desktop				
TCP 80, 443	Live screen monitoring	Agent's PC	Supervisor's browser	

Cloud STUN/TURN

Refer to the table below for Cloud STUN/TURN ports.

Port	Use	Connections
Smart Desktop		
TCP 80, 443	Via websocket	Signaling Server
TCP 6379	STUN/TURN administration via System Administrator in Webex WFO.	Configuration
UDP 49152 - 65535	Media (audio and video)	SRTP (peer-to-peer)
UDP 49152 - 65535	Media (audio and video)	SRTP (not peer-to-peer)
UDP/TCP 3478	-	IP address discovery

Smart Desktop Contact Metadata

The following table lists available Smart Desktop contact metadata used for each capture mode:

Contact Metadata	SIP Signaling	SCCP Signaling	RTP Logging
Call ID	X	X	Relies on third-party to provide real-time data to DCC API
ANI (Calling)	X	X	Relies on third-party to provide real-time data to DCC API
DNIS (Called)	X	X	Relies on third-party to provide real-time data to DCC API
Line/Extension			Relies on third-party to provide real-time data to DCC API
Call Direction	X	X	Relies on third-party to provide real-time data to DCC API

Contact Metadata	SIP Signaling	SCCP Signaling	RTP Logging
Associated Contact ID	X		Relies on third-party to provide real-time data to DCC API
Recording Type	X	X	X
Duration	X	X	Segment based, unless join_start is used
MAC Address	X	X	
User (by Windows Login ID)	X	X	X
Call Date/Time	X	X	X

Smart Desktop Capture Data Flow Diagrams

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

Smart Desktop SIP/SCCP Signaling
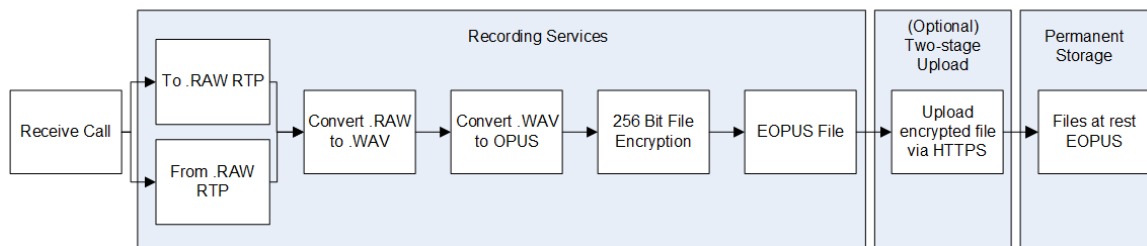
Smart Desktop RTP Logging
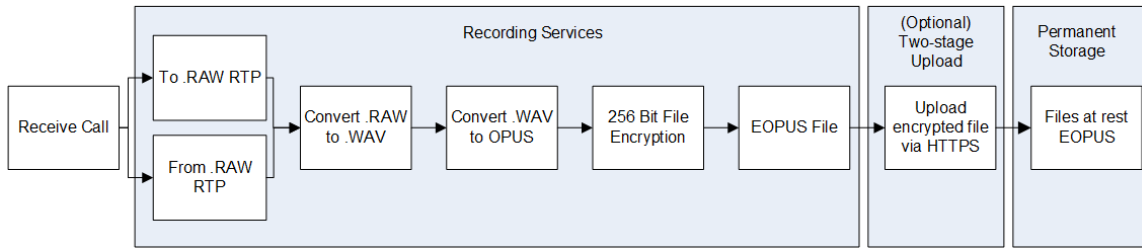
Smart Desktop Live Audio Monitoring
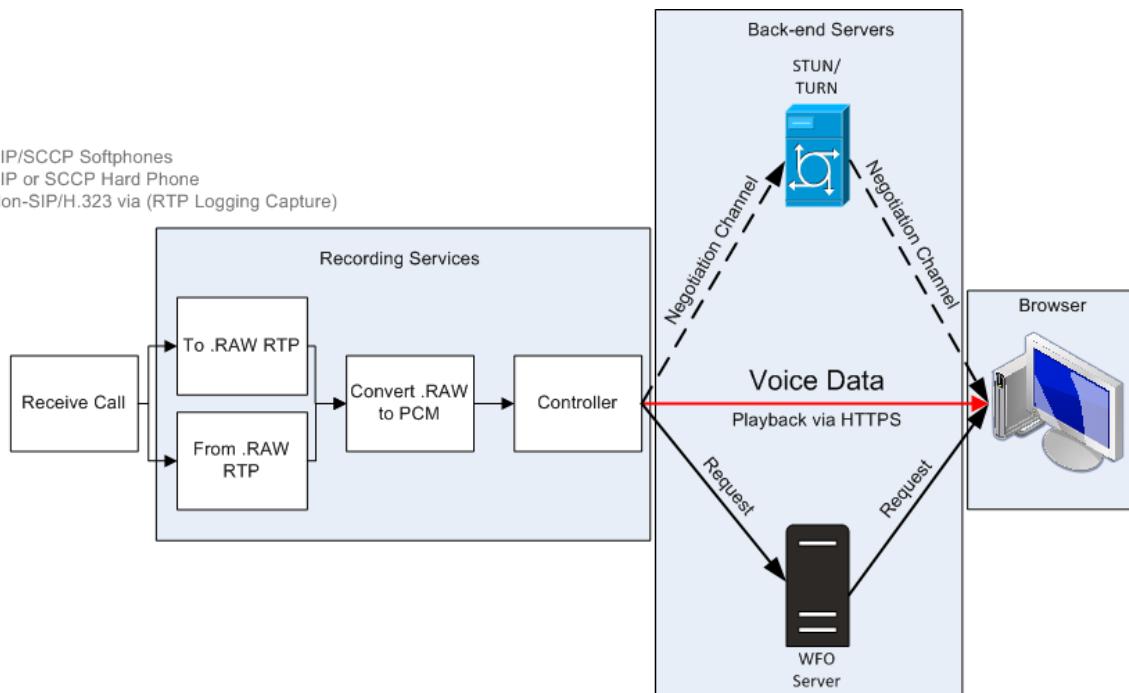
Smart Desktop Live Screen Monitoring
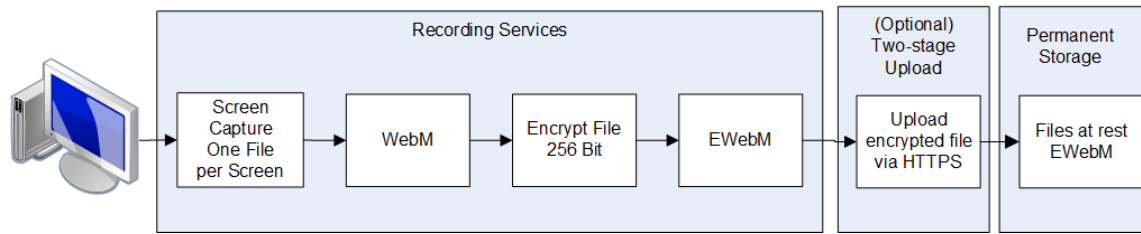
> **NOTE** Smart Desktop screen and audio recording uses AES 256-bit encryption if the recording takes place inside Webex WFO.

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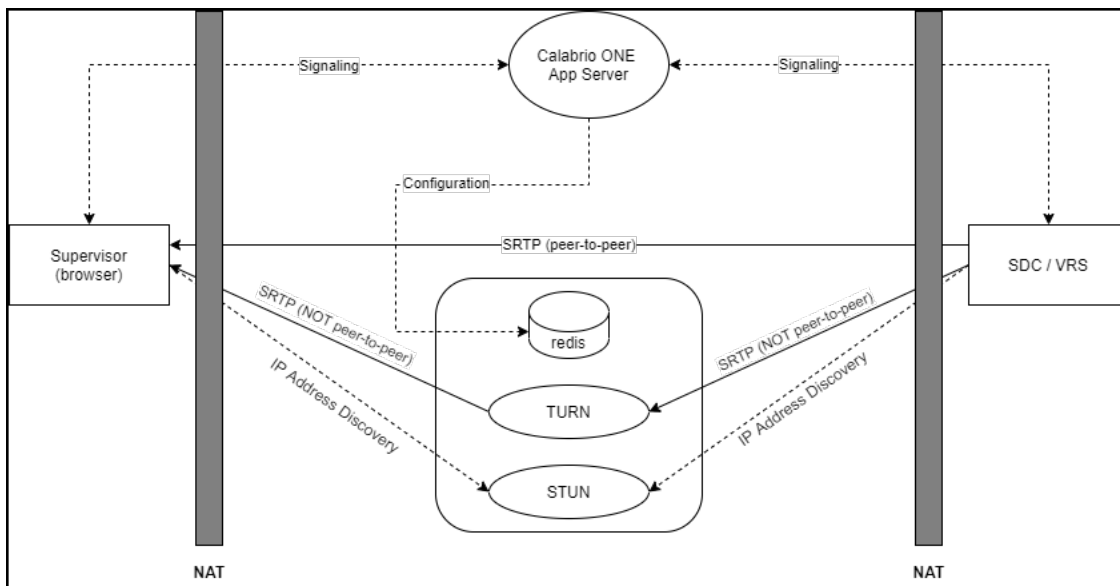
Connection	Ports	Protocol	Notes
Signaling	80, 443	TCP	By websocket
Configuration	6379	TCP	STUN/TURN administration using a System Administrator role in Webex WFO
SRTP (peer-to-peer)	49152–65535	UDP	Audio and visual media

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

Test Smart Desktop

After you have installed Smart Desktop (see Installing Smart Desktop) and desktop analytics (see Enable the Desktop Analytics extension in your browser) follow these steps to make sure your Smart Desktop implementation is working correctly.

Prerequisites

- Your Window's Login (**Application Management** > **User Configuration** > **Users**) must be in [Domain\WindowsNTID] format. If you add your Window's login after installing Smart Desktop, you need to restart Smart Desktop or its desktop services.

- The agent has the following permissions assigned to their role. Permissions are found in **Application Management** > **User Configuration** > **Roles**.

    - Capture Desktop Analytics

    - Capture Contacts

    - Record Screen

    - Record Voice

    - Live Screen Monitoring

    - Live Audio Monitoring

    - Record On Demand (RTP Signaling)

    - Capture Desktop Events

    > **NOTE** Contact center as a service (CCaaS) solutions do not support live audio monitoring.

- The Desktop Analytics extension is running in your browser.

Procedures
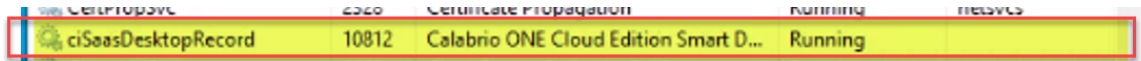
Ensure the correct processes are running on your computer

1. Open **Task Manager**.

2. Confirm the processes `DesktopRecordServer` and `DesktopRecordProcess` are running in **Task Manager**. If `DesktopRecordProcess` is not running, make sure you correctly entered your Window's Login as described in the prerequisites.
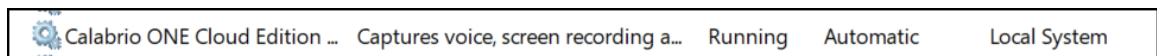
Device Association Framework ...	0%	0.1 MB	0 MB/s	0 Mbps
> DesktopRecordServer (32 bit)	0%	7.2 MB	0 MB/s	0 Mbps
DesktopRecordProcess (32 bit)	0.1%	9.7 MB	0.1 MB/s	0 Mbps
CTF Loader	0%	3.4 MB	0 MB/s	0 Mbps

3. Check that `ciSaasDesktopRecord` is running in **Task Manager**.

CertPropSvc	2328	Certificate Propagation	Running	netsvcs
ciSaasDesktopRecord	10812	Calabrio ONE Cloud Edition Smart D...	Running	

4. Open the **Services** app on your computer and verify that `Calabrio ONE Smart Desktop Record Service` is running.

Calabrio ONE Cloud Edition ...	Captures voice, screen recording a...	Running	Automatic	Local System

Ensure Webex WFO recognizes your computer

Navigate to **Application Management** > **Global** > **Monitoring** > **Desktop Monitoring**. If you see a green circle under the Status column, it means you are connected and the installed version of Smart Desktop is the active version.

Ensure Webex WFO recognizes agents using Smart Desktop

1. Navigate to **Application Management** > **Global** > **Monitoring** > **Agent Monitoring**.

2. You can monitor an agent's screen if the agent's screen monitoring icon ⬤ is black. If the icon is black, the agent has Smart Desktop Client running on their PC with the correct permissions.

3. You can monitor an agent's audio if the agent's audio monitoring icon 📞 is black. If the icon is black, the agent is configured for desktop recording, has Smart Client running on their PC with the correct permissions, is configured for server recording, and is assigned to a monitored device on the Device Associations page.

4. Click the agent's screen monitoring icon 👁 to open the live screen monitoring window.

5. From the live screen monitoring window, click **Screen** to start the monitoring session. Click **Audio** to monitor the agent's call. You can only hear audio if the agent is on an active call.

Make a test call

1. Make a phone call from an agent's desktop.

2. In Webex WFO, click **Interactions**.

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 the Screen Recording panel does not appear or is blank, verify that the pop-up blocker on the browser is disabled.

Review the upload status of video and audio recorded contacts

1. Navigate to **Interactions**.

2. Click the **Lists Options** icon in the top-right corner of the page.

3. Click **Show/Hide columns**. The Show/Hide columns window appears.
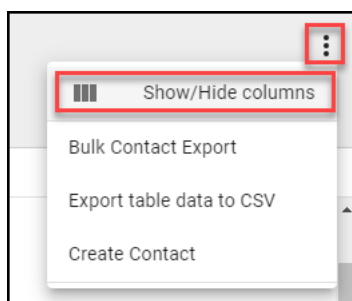
4. Click **Audio File Upload State** and **Video File Upload State** if they are listed under **Hidden columns**.

5. Click **Apply**. Now you can easily see if video and audio files are pending upload or have successfully uploaded.

6. Double-click on a contact to review the audio and screen recordings associated with the call.

Manage Smart Desktop

Cisco recommends you update Smart Desktop quarterly. Webex WFO supports a non-interruptive update process.

Whether you choose to auto update or do customer-managed updates, updates run silently and without interruption to recordings or contacts. Both the existing version and the updated version of Smart Desktop run side-by-side until a Windows login process takes place. Desktop monitoring allows administrators to view users' active and installed versions of Smart Desktop on their PCs, set logging levels, and remotely download logs for troubleshooting.

> **BEST PRACTICE** Administrators should familiarize themselves with desktop monitoring to verify the status and versions of Smart Desktop across your organization.

Auto update

Webex WFO has an auto-update feature that can be enabled or disabled at any time by navigating to **Application Management** > **Administration** > **Global Settings**. From the Global Settings page, use the **Enable Client Auto Update** button to enable or disable the auto-update feature.

If enabled, when a user logs in to a computer running Smart Desktop, the computer checks to see if there is a new update available to download.

Customer-managed update

You can push updates using a managed software push (for example, GPO or LANDesk).

> **BEST PRACTICE** Your organization's policy should require agents to log off their PC at the end of their shift. This action can be automated using GPO settings.

Best practices for uploading recordings to Webex WFO

Getting audio and screen recordings from a user's desktop as soon as possible ensures that the recordings are available for playback after the call has been recorded. There are options for moving the recordings off the user's desktop immediately or at a set time. The decision on when to upload recordings is a collaboration between business and IT personnel by considering account audio and screen accessibility needs, bandwidth, and storage. Cisco recommends the upload processes listed below.

- Immediate upload using QM workflows—This process ensures that the recording is available for playback after the call has been recorded and storage space is not overly consumed on the agent PC. Cisco recommends that you configure recordings to immediately upload from the agent's PC to

Webex WFO if WAN and LAN bandwidth are sufficient. Use the **Workflow Administration** page in **Application Management** to perform immediate uploads.

- Delayed upload using QM workflows—You can configure this process to take place after business hours. Audio and/or screen recordings are uploaded at a specified time. After your recordings are uploaded, you can download them on demand. Use the **Workflow Administration** page in **Application Management** to perform delayed uploads.

- Immediate upload using the Webex WFO Data Server's regional staged upload settings—If internet bandwidth is a concern, a staged-upload approach can mitigate external WAN traffic during business hours. This option requires you to configure the Cisco Data Server's staged upload settings (see Configure the Data Server and Configure staged upload for more). This process ensures calls are moved from a PC to local storage during the day. At a specified time after hours, the recordings are uploaded. After your recordings are uploaded, you can download them on demand. Configure "Regional Data Server Staged Upload Settings" on the Data Server Configuration page in Application Management to perform staged uploads.

Recording controls application

Webex WFO Recording Controls is a standalone web application that allows you to start, pause, resume, and stop audio, screen, and keystroke recording for active calls. You can also tag calls and add metadata to them.

To start Recording Controls, choose **Calabrio ONE Recording Controls** from your Start menu. To close Recording Controls, click **Quit**.

Agents can use the Smart Desktop recording controls application, also known as the Desktop Capture and Controller (DCC) application, to control recordings and insert metadata from their desktops. The recording controls application is installed with Smart Desktop. It appears in the Program list under Cisco on the agent's desktop after Smart Desktop is installed.

The recording controls application is shown below:
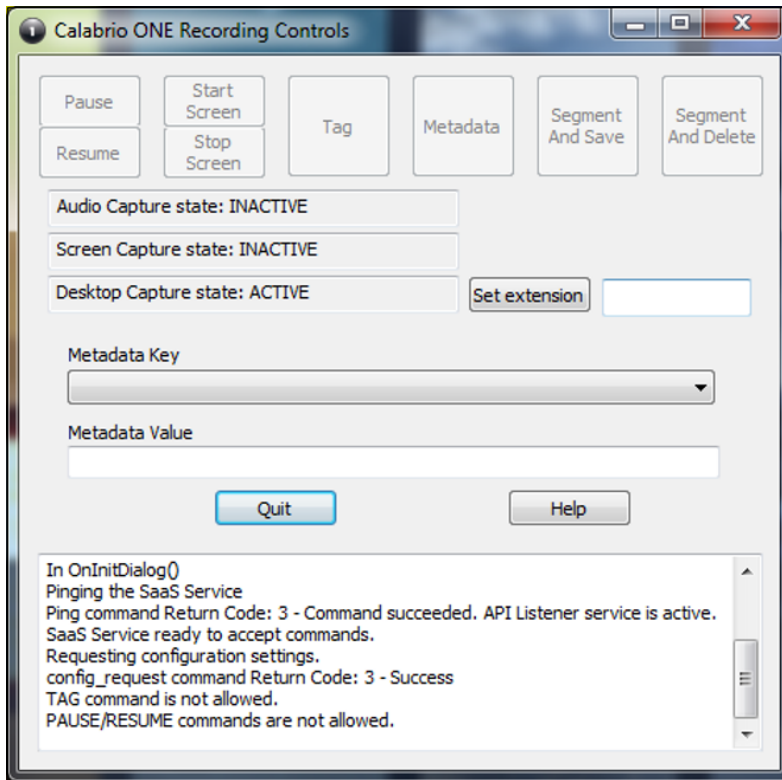
The correct roles and permissions must be granted to agents by a tenant administrator before agents can use the recording controls application.

The recording controls application allows users to do the following:

- Tag an active call or the most recent call recording

- Record calls

- Pause and resume the recording of audio

- Start the recording of a call

- Discard previously recorded audio and screen for a call

- Delete the recording for the active call—once a call is over you cannot delete the recording

- Log in or log out for hoteling recording

- Add metadata to an active call or the most recent call

- Start or stop the audio and screen recording of an active call

- Start or stop the screen recording

The recording controls application supports the following recording types:

- Desktop Recording

- Network Recording

See "Recording Controls API" in the *API Reference Guide* for information on DCC commands.

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).

System requirements

The following sections list the minimum system requirements for Webex WFO.

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
	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

Desktop Hardware	
	▌ 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.

Enable the Desktop Analytics extension in your browser

Smart Desktop must be installed on your computer and activated before you can mark fields. Users who have permission to administer fields for Desktop Analytics using the Field Manager page and on the agents' desktops where Smart Desktop is installed must have the appropriate Desktop Analytics browser plug-in configured for the browser they use.

Prerequisites

- Your organization has one of the following licenses:
    - Analytics Essentials
    - Analytics Enterprise

- Desktop Analytics
- Smart Desktop is installed and activated on your computer.

Procedures

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.

Related topics
"Installing Webex WFO Smart Desktop" in the *Webex WFO Installation Guide*

Thin client servers

> **NOTE**   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.
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.

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	—

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

Password complexity requirements are based on Microsoft's password policy: https://technet.microsoft.com/en-us/library/hh994562.aspx.

The following rules apply when you create or edit a user, or when you change or reset a password.

- Passwords cannot contain any white spaces (blanks).

- Passwords must be at least eight characters long. Minimum length can be configured by an administrator.

- Passwords must contain characters from three of the following four categories:

Category	Description
Uppercase letters	A–Z Uppercase unicode characters: http://www.fileformat.info/info/unicode/category/Lu/list.htm
Lowercase letters	a–z Lowercase unicode characters: http://www.fileformat.info/info/unicode/category/Lu/list.htm
Numbers	0–9
Special characters	The following characters are allowed for a tenant database password: ! # $ % & ( ) , . / : ; = ? @ ^ ` | The following characters are allowed for all other passwords: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

These rules apply only where you configure a password that is controlled by Webex WFO. If a user enters a password for an external system that is not controlled by Webex WFO, Webex WFO will not validate the password (for example, ACD configuration).

> **NOTE**   A user can be created without a password (manually or automatically via ACD sync). A user without a password cannot log in. That user must use the "Forgot Password" link and set up a password.

Authentication

By default, user authentication and passwords are managed using Webex WFO. In systems that sync with an ACD, users are created and managed in the ACD, although you can still create users in Webex WFO.

You can opt to use Security Assertion Markup Language (SAML) authentication. SAML allows you to use an external identity provider (IdP) to authenticate user names and passwords. This method of user authentication and password management is commonly referred to as "single sign-on."

Platform Capture Methods

This topic describes how you can configure Webex WFO with various contact center platforms.

Supported Capture Methods by Platform

The following table describes how contact center platforms support recording capture.

> **NOTE**
> Webex WFO supports SRTP with the following capture methods only:
>
> - Acme packet
>
> - Cisco Unified CM

Platform	Capture Method	Signaling	Signaling Description
Cisco	Built-in bridge network recording	JTAPI	Registers with call manager for JTAPI events
Cisco	Desktop recording	JTAPI	Registers with call manager for JTAPI events
Cisco	Gateway (Cisco Unified Border Element—CUBE)	SIPREC	Registers with CUBE for SIPREC signaling
Cisco	Smart Desktop Client	IP Communicator (SIP/SCCP)	SCCP messages off desktop

Platform	Capture Method	Signaling	Signaling Description
Cisco	Smart Desktop Client	Jabber (SIP/SCCP)	Sniffs SIP/SCCP messages off desktop
Cisco	Smart Desktop Client	Cisco IP HardPhone (SIP/SCCP)	Sniffs SIP/SCCP messages off desktop
Cisco Webex Contact Center (CWCC)	Automated import	CWCC Analyzer API	Poll CWCC Analyzer for post-call CDR and post-call processing
ACME	Gateway (ACME packets)	SIPREC	Registers with ACME for SIPREC signaling
SONUS	Gateway (SONUS)	SIPREC	Registers with SONUS for SIPREC signaling

Cisco Voice Capture Methods

The following table provides information on integrating Cisco-supported and -tested capture types and signaling:

Capture Method	Signaling	Description	Media Stream	Smart Desktop Screen Capture	Live Audio Monitor
Network Recording— Built-in Bridge (BIB)	JTAPI	Registers with CUCM/JTAPI Events	BIB—Media Streamed from Phone	Yes (Smart Desktop Client Requires CTI Connection)	Yes (Smart Desktop Client) via WebRTC
Smart Desktop Client – IP Communicator	SIP/SCCP	Monitor SIP/SCCP messages off Desktop/Softphone	Media Stream captured directly on desktop	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via WebRTC
Smart Desktop Client – Jabber	SIP/SCCP	Monitors SIP/SCCP Messages off Desktop	Media Stream captured directly on	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via

Capture Method	Signaling	Description	Media Stream	Smart Desktop Screen Capture	Live Audio Monitor
			desktop		WebRTC
Smart Desktop Client – Cisco IP Phone (Daisy Chained)	SIP/SCCP	Monitors SIP/SCCP Messages off Desktop	Media Stream captured directly on desktop	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via WebRTC
Gateway (CUBE)	SIPREC	Registers with CUBE for SIPREC Signaling	SIPREC – Media Forking from Cisco CUBE	Yes (Smart Desktop Client)	No
Bulk Contact Import	API Based	Registers with CUBE for SIPREC Signaling	Automated import of unencrypted .WAV and associated contact metadata files in bulk	N/A – Files Encrypted and Imported	No

Legacy Five9 Voice Capture Integrations

The following table provides information on integrating Five9-supported and -tested capture types and signaling. It specifically refers to the legacy Five9integration, not Five9 ARU or Five9 VCC with VoiceStream.

Capture Type	Signaling	Description	Media Stream	Smart Desktop Screen Capture	Live Audio Monitor
Smart Desktop Client	Kafka CTI	Webex WFO Platform Registers with Five9 Kafka Events API	Media Stream captured directly on	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via WebRTC

Capture Type	Signaling	Description	Media Stream	Smart Desktop Screen Capture	Live Audio Monitor
			desktop – Post call CDR and Reconciliation processing redacts and inserts events based on Kafka call events		
Smart Desktop Client	Five9 Agent Desktop Plus (ADP) - Kafka CTI	Monitor SIP/SCCP messages off Desktop/Softphone	Media Stream captured directly on desktop – Post call CDR and Reconciliation processing redacts and inserts events based on Kafka call events	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via WebRTC
Smart Desktop Client	Five9 Agent Desktop Toolkit (ADT) - Kafka CTI	Monitors SIP/SCCP Messages off Desktop	Media Stream captured directly on desktop – Post call CDR and Reconciliation processing redacts and inserts events based on Kafka call events	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via WebRTC

Capture Type	Signaling	Description	Media Stream	Smart Desktop Screen Capture	Live Audio Monitor
Smart Desktop Client	Five9 Java Agent Desktop - Kafka CTI	Monitors SIP/SCCP Messages off Desktop	Media Stream captured directly on desktop – Post call CDR and Reconciliation processing redacts and inserts events based on Kafka call events	Yes (Smart Desktop Client)	Yes (Smart Desktop Client) via WebRTC
Smart Desktop Client	Five9 VCC Import	Five9/Webex WFO Cloud Integration to Import Five9 VCC audio recordings into Webex WFO Cloud	N/A – Import Only	Yes (Smart Desktop Client)	No

Sonus Gateway Recording

Cisco supports resiliency for Sonus Gateway Recording.

You need to add Sonus SIP Message Manipulation (SMM) rules to the SIP and SIPREC INVITE headers in Cisco-Guid for Sonus SBC to work with QM. This allows QM to reconcile calls against the Cisco Unified CM CDR records. The rules will do the following:

- For calls that come into the SBC without a "Cisco-Guid" header, the SMM will create a Cisco-Guid by using the 4 hex tuples from the exiting Call-ID. Each tuple will be converted to a 10 digit 0 padded decimal number that will be separated by dashes to form the Cisco-Guid.

- For calls that already contain a Cisco-Guid header, the header will remain as is.

    NOTE **Note:** The Cisco_Guid will NOT be overwritten by a new Call-ID created Cisco-Guid.

- The SIPREC Invite to the recorder will contain a Cisco-Guid header that matches the Cisco-Guid above.

The rules must be associated with your recorded trunk and the Unified CM trunk that is being used by your Unified CM. You only need to create these rules once. If you create new zones and trunks, you can reuse these rules.

To configure Sonus Session Border Controllers for use with QM:

1. From the Sonus command line interface (CLI), create and enable the SMM rules

   a. Create and enable the Unified CM inbound SMM rules. See Example of Inbound SMM Rules for Unified CM for more information.

   b. Add the Unified CM outbound SMM rules. See Example of Outbound SMM Rules for Unified CM for more information.

   c. Add the recorder outbound SMM rules. See Example of Outbound SMM Rules for the Recorder for more information.

2. Use the Sonus CLI to enable SIPREC for the SIp Sig Port in the zone that contains your Unified CM trunk.

3. Use the Sonus CLI or Navigator to create a Sip Trunk Group for QM's Sonus SIPREC Server. Assign the Ingress IP Prefix to the IP address of the QM machine that is running the "Monitoring and Recording Sonus SIPREC Service."

4. Use the Sonus CLI/Navigation to assign SMM rules to your trunks as follows:

   a. Assign UCM_INBOUND SMM to the Signaling Message Manipulation adapter input profile of your Unified CM trunk.

   b. Assign UCM_OUTBOUND SMM to the Signaling Message Manipulation adapter output profile of your Unified CM trunk.

   c. Assign RECORDER_OUTBOUND SMM to the Signaling Message Manipulation adapter output profile for QM's Sonus SIPREC trunk.

5. Use the Sonus PSX to create an IP Signaling Peer Group for the QM's Sonus SIPREC Server. Assign the Ingress IP Prefix to the IP address of the QM machine that is running the "Monitoring and Recording Sonus SIPREC Service."

6. Use the Sonus PSX to create a Trunk Group for the QM's Sonus SIPREC Server. Use the exact same name that you used in step 3.

7. Use the Sonus PSX to create a Recorder Profile for your QM Sonus SIPREC Server. Assign the IP4 address to the QM machine that is running the "Monitoring and Recording Sonus SIPREC Service," set the Port Number to 5060.

8. Use the Sonus PSX to Create Call Recording Criteria.

Example of Inbound SSM Rules for Unified CM

```
configure
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 applyMatchHeader
    all
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 criterion 1 type
    message
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 criterion 1
    message messageTypes all
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 criterion 2 type
    header
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 criterion 2
    header name Cisco-Guid
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 criterion 2
    header condition exist
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1 type
    header
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1
    operation store
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1
    headerInfo fieldValue
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1 from
    type header
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1 from
    value Cisco-Guid
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1 to type
    variable
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 1 action 1 to
    variableValue var1
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 applyMatchHeader
    one
    set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 1 type
```

```
message
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 1
message messageTypes request
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 1
message methodTypes invite
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 1
message condition exist
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 2 type
header
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 2
header name From
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 2
header condition exist
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 3 type
variable
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 3
variable condition exist
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 criterion 3
variable variableID var1
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1 type
parameter
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1
operation add
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1
paramType generic
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1 from
type variable
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1 from
variableValue var1
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1 to type
parameter
set profiles signaling sipAdaptorProfile UCM_INBOUND rule 2 action 1 to value
cisco-guid
commit
set profiles signaling sipAdaptorProfile UCM_INBOUND state enabled
commit
```

Example of Outbound SMM Rules for Unified CM

```
configure
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 criterion 1 type
    message
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 criterion 1
    message messageTypes request
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 criterion 1
    message methodTypes invite
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 criterion 2 type
    header
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 criterion 2
    header name cisco-guid
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 criterion 2
    header condition absent
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 action 1 type
    variable
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 action 1
    operation store
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 action 1 from
    type value
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 action 1 from
    value cisco-guid
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 action 1 to type
    variable
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 1 action 1 to
    variableValue var1
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 1 type
    message
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 1
    message messageTypes request
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 1
    message methodTypes invite
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 2 type
    variable
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 2
    variable condition exist
    set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 2
```

```
variable variableID var1
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 3 type
header
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 3
header name call-id
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 criterion 3
header condition exist
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1 type
header
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1
operation store
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1
headerInfo fieldValue
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1 from
type header
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1 from
value call-id
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 1 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 2 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 2
operation regdel
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 2 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 2 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 2 regexp
string @.*
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 2 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 3 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 3
operation store
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 3 from
```

```
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 3 from
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 3 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 3 to
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 4 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 4
operation regdel
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 4 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 4 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 4 regexp
string _.*
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 4 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 5 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 5
operation regdel
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 5 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 5 to
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 5 regexp
string .*_
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 5 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6
operation regappend
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 from
type value
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 from
```

```
value 000000000
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 regexp
string ^
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 6 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7
operation regappend
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 from
type value
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 from
value 000000000
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 to
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 regexp
string ^
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 7 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 8 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 8
operation regpredel
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 8 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 8 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 8 regexp
string ..........$
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 8 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 9 type
```

```
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 9
operation regpredel
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 9 to type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 9 to
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 9 regexp
string ..........$
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 9 regexp
matchInstance one
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 10 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 10
operation append
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 10 from
type value
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 10 from
value -
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 10 to
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 10 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 11 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 11
operation append
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 11 from
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 11 from
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 11 to
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 11 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 12 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 12
```

```
operation store
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 12 from
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 12 from
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 12 to
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 12 to
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 13 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 13
operation append
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 13 from
type value
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 13 from
value -
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 13 to
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 13 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 14 type
variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 14
operation append
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 14 from
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 14 from
variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 14 to
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 14 to
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15 type
header
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15
operation add
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15
```

```
headerPosition last
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15 from
type variable
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15 from
variableValue var2
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15 to
type header
set profiles signaling sipAdaptorProfile UCM_OUTBOUND rule 2 action 15 to
value Cisco-Guid
commit
set profiles signaling sipAdaptorProfile UCM_OUTBOUND state enabled
commit
```

Example of Outbound SMM Rules for the Recorder

```
configure
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1
    applyMatchHeader all
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 criterion 1
    type message
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 criterion 1
    message messageTypes all
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 criterion 2
    type messageBody
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 criterion 2
    messageBody condition regex-match
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 criterion 2
    messageBody regexp string cisco-guid=.*
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 criterion 2
    messageBody regexp numMatch match
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1
    type messageBody
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1
    operation regstore
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1
    from type messageBody
    set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1
```

```
from messageBodyValue all
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1 to
variableValue var1
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1
regexp string "cisco-guid=.*?(?=;tag)"
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 1
regexp matchInstance last
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2
operation regdel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2
from type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2
from variableValue var1
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2 to
variableValue var1
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 2
regexp string cisco-guid=
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4
type header
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4
operation add
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4
headerPosition last
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4
from type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4
from variableValue var1
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4 to
type header
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 1 action 4 to
value Cisco-Guid
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 criterion 1
```

```
type message
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 criterion 1
message messageTypes request
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 criterion 1
message methodTypes invite
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 criterion 2
type header
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 criterion 2
header name cisco-guid
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 criterion 2
header condition absent
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 action 1
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 action 1
operation store
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 action 1
from type value
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 action 1
from value cisco-guid
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 action 1 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 2 action 1 to
variableValue var1
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3
applyMatchHeader all
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 criterion 1
type message
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 criterion 1
message messageTypes all
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 criterion 2
type messageBody
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 criterion 2
messageBody condition regex-match
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 criterion 2
messageBody regexp string cisco-guid=.*
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 criterion 2
messageBody regexp numMatch match
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 action 1
```

```
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 action 1
operation store
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 action 1
from type value
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 action 1
from value cisco-guid
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 action 1 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 3 action 1 to
variableValue var10
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 criterion 1
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 criterion 1
variable condition absent
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 criterion 1
variable variableID var10
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1
type messageBody
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1
operation regstore
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1
from type messageBody
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1
from messageBodyValue all
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1 to
variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1
regexp string <callid>.*</callid>
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 1
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 2
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 2
operation regdel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 2 to
```

```
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 2 to
variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 2
regexp string <callid>
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 2
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 3
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 3
operation regdel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 3 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 3 to
variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 3
regexp string @.*
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 3
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 4
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 4
operation store
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 4
from type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 4
from variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 4 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 4 to
variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 5
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 5
operation regdel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 5 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 5 to
```

```
variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 5
regexp string _.*
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 5
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 6
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 6
operation regdel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 6 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 6 to
variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 6
regexp string .*_
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 6
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7
operation regappend
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7
from type value
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7
from value 000000000
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7 to
variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7
regexp string ^
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 7
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8
operation regappend
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8
```

```
from type value
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8
from value 000000000
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8 to
variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8
regexp string ^
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 8
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 9
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 9
operation regpredel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 9 to
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 9 to
variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 9
regexp string ..........$
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 9
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 10
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 10
operation regpredel
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 10
to type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 10
to variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 10
regexp string ..........$
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 10
regexp matchInstance one
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 11
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 11
```

```
operation append
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 11
from type value
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 11
from value -
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 11
to type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 11
to variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 12
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 12
operation append
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 12
from type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 12
from variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 12
to type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 12
to variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 13
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 13
operation store
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 13
from typevariable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 13
from variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 13
to type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 13
to variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 14
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 14
operation append
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 14
```

```
from type value
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 14
from value -
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 14
to typevariable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 14
to variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 15
type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 15
operation append
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 15
from type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 15
from variableValue var3
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 15
to type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 15
to variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
type header
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
operation add
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
headerPosition last
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
from type variable
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
from variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
to type header
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND rule 4 action 16
to value Cisco-Guid
commit
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND state enabled
commit
```

Installation

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

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. After you install the Webex WFO Data Server, you can further configure it on the Data Server Configuration page in Application Management > Global > System Configuration > Data Server Configuration.

> **BEST PRACTICE** Users with edge devices should set a regular schedule to download and upgrade their Webex WFO Data Servers to the latest version of Webex WFO software. Typically, each Cloud deployment includes a new version of the Webex WFO Data Server software that users can download from their tenant.

If your organization has any of the following integrations, consult that ACD's integration guide for additional data server configurations specific to the ACD.

- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco Webex Contact Center

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:

- Webex WFO CTI Signaling Service
- Webex WFO Data Server
- Webex WFO Network Recording Service
- Webex WFO SIPREC Service
- Webex WFO Data Server Web Services

For port usage requirements, see Port usage.

Install 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.

Install 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 **Calabrio ONE Data Server**. 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 **Add a new configuration to the data server**.

    > **NOTE** To edit an existing configuration, select **Edit an existing data server configuration** 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 Webex WFO 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.
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.

Cisco Unified Call Manager users

If you use Cisco Unified Call Manager (UCM) to gather CDRs via SFTP, you might need to set the Data Server Service system property to reconcile the key exchange (kex) algorithms between Webex WFO and supported versions of Cisco UCM.

These kex algorithms do not require additional configuration:

- ecdh-sha2-nistp521

- ecdh-sha2-nistp384

- diffie-hellman-group-exchange-sha256

These algorithms require additional configuration:

- diffie-hellman-group14-sha1

- diffie-hellman-group1-sha1

- diffie-hellman-group-exchange-sha1

Set the Data Server Service system property to specify the allowed kex algorithms

1. On the CDR SFTP server, navigate to
   `C:\Program Files\Common Files\Calabrio ONE\Data Server\config`

2. Open the dataGatheringService.properties file.

3. Find the line beginning with **service4j.jvmOptions** and add the following text to the end of the line: **| -Dsftp.KexAlgorithms=diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1**

4. Save the file and restart the Webex WFO Data Server Service.

NOTE If you upgrade to a newer version of Cisco UCM that does not support any of these kex algorithms, you must reconfigure this system property to specify the new supported algorithms.

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 silent commands parameters

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 plug-ins are not installed on the client desktop.

Additional considerations

- You need a Desktop Analytics plug-in/extension if you wish to use the Desktop Analytics feature or pause and resume.

- Browser extensions for Chrome and Edge need to be deployed via GPO or any other process the local IT department uses. Browser extensions are needed for analytics and pause and resume.

- Cisco provides the base exe file. It is the customers responsibility to convert the file to an MSI.

- If installing via SCCM or Microsoft Endpoint Configuration Manager, you, the customer, are responsible for building the package for deployment.

- Cisco offers the option to auto-update the software. If your packaging team manages desktop versions or Microsoft Endpoint Configuration Manager and they interfere with the auto-updates, Cisco can turn the auto-update feature off and your team can download a new version of the software every three to six months and deploy it via a package push.

- Your team can change the queries in the Microsoft software to not manage version numbers or unique identifiers if the group wishes to maintain auto updates.

  > **NOTE** Auto-updates have to be turned off if your organization uses Citrix or Terminal servers. There is no way to segregate different environments.

- If you are upgrading from Webex WFO version 11.5 on-premise to Webex WFO Cloud, then you need three test machines. One machine is for a manual install. The second machine is for an automatic install on a clean machine. The third machine is for the existing version 11.5 of Webex WFO to test the uninstall package built by your IT team and the install package for Webex WFO Cloud. Supply the implementation engineer with a list of all the packages installed on the machine, including browser extensions. Work with your IT team to remove all Webex WFO version 11.5 software prior to installing Webex WFO Cloud.

  - If your organization is changing vendors from another workforce engagement management (WEM) solution (such as Verint or Nice) to Webex WFO, then work with your IT team to uninstall the original software on a third test machine and deploy the automated package built by your team.

- If you are upgrading a version of 11.5 on-premise to a newer version of 11.5, then you have to redownload a new version of Smart Desktop and redeploy it.

Manual installation

Use this procedure to install Smart Desktop manually on an agent's computer or on a thin client server. Ensure that all browsers are closed before you install, and use Task Manager ensure your browsers are not running in the background.

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.

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 Test 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/NONPCAP
```

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

Install Smart Desktop using silent command parameters

Silent parameters allow you to install Webex WFO using your command-line interface. See "Setup Command Line Parameters" in https://jrsoftware.org/ishelp/index.php?topic=setupcmdline for options. Commonly used commands include the following.

- /LOG

- /VERYSILENT

- /ACTIVATE

- /NORESTART

- /NONPCAP

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 or Installation using GPO), 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), you will receive return codes indicating install success or failure. The possible return codes are described below.

Return Code	Description
0	Successful installation
1	Failed installation

Additionally, events will be written to the Windows event log. The event detail will list a description of what occurred. Three different event IDs will be written. The event itself will contain more detail, but in general the IDs indicate the following:

Event ID	Description
8080	Successful installation

Event ID	Description
8081	Failed installation
8084	Informational message

The detail for a successful or failed installation will be written to both the Windows event log and within the logs contained in the wrapper folder under the Smart Desktop Client installation folder.

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.
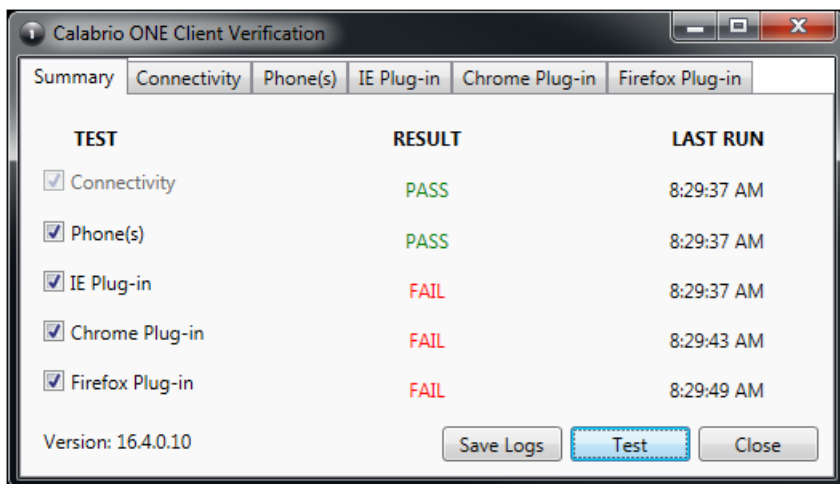
Run the Client Verification tool

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

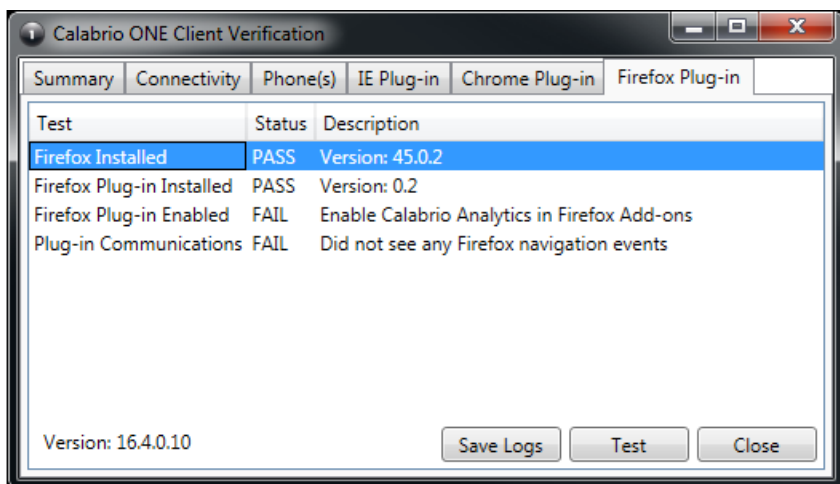   `C:\Program Files (x86)\Calabrio ONE\Desktop\Active\bin\`

2. Double-click **ClientDiag.exe**. The Client Verification tool starts.
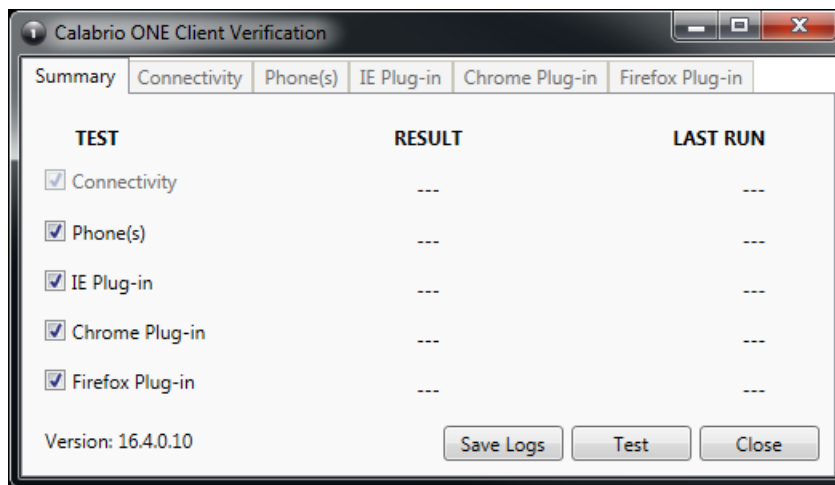
3. By default, all tests are selected. Click **Test**.

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

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.

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 certain 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 WFORecording Controls and by default is under Webex WFO.

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.

Uninstall Smart Desktop using silent command parameters

Silent parameters allow you to uninstall Webex WFO using your command-line interface. See "Uninstaller Command Line Parameters" in https://jrsoftware.org/ishelp/index.php?topic=setupcmdline for options.