Webex WFO Installation Guide for Cloud Deployments

First Published: July 10, 2020

Last Updated: May 17, 2021

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

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

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

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

Contents

Introduction

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
- Documentation—online help and PDF guide
- Workforce Optimization (WFM)
- Analytics
  - Phonetics—speech analytics
  - Transcription—speech to text
  - Sentiment—emotion analytics
  - Text—analytics for chat, email, agent notes, and social media

User Interface and Documentation

The user interface and documentation are available in these languages.

	User Interface	Documentation
Chinese (Simplified)	X	
Chinese (Traditional)	X	
Danish—Denmark	X	
Dutch—Netherlands	X	
English—United States	X	X
English—United Kingdom	X	
Finnish—Finland	X	

	User Interface	Documentation
French—Canada	X	
French—France	X	
German—Germany	X	
Italian—Italy	X	
Japanese—Japan	X	
Korean—Korea	X	
Norwegian—Norway	X	
Polish—Poland	X	
Portuguese—Brazil	X	
Portuguese—Portugal	X	
Spanish—United States	X	
Spanish—Spain	X	
Swedish—Sweden	X	

Analytics

Webex WFO offers analytics components for the following languages.

	Transcription / Speech to Text	Phonetics*	Sentiment*	Text‡
English—Australia	X			X
English—Europe	X			X
English—North America	X	X	X	X
English—United Kingdom	X	X	X	X

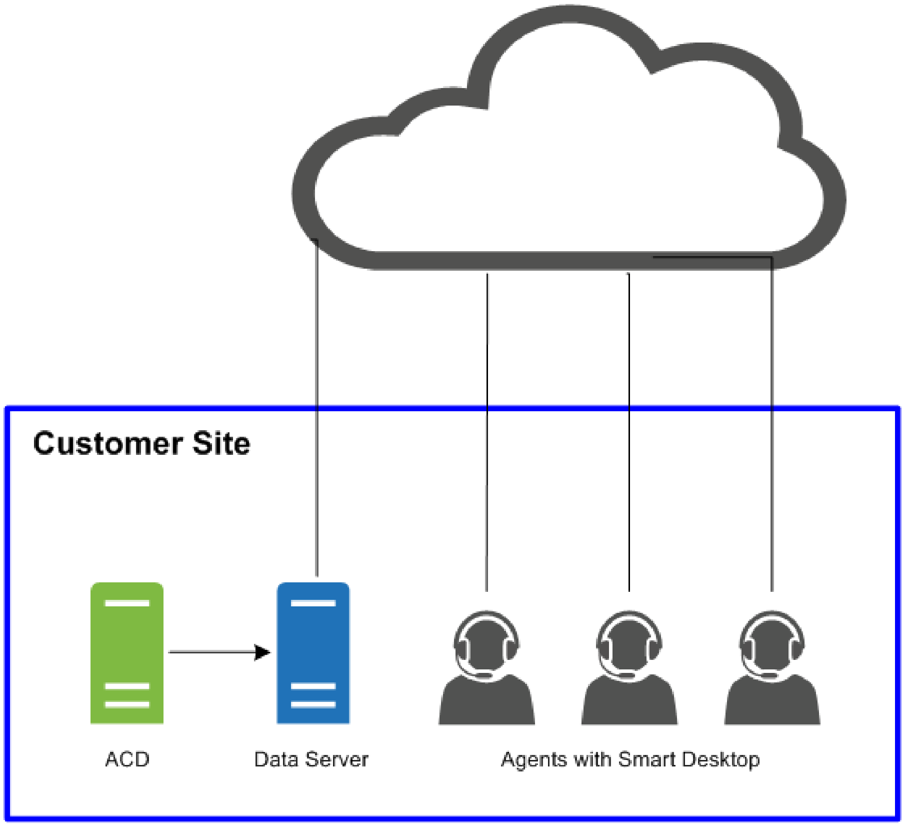
	Transcription / Speech to Text	Phonetics*	Sentiment*	Text‡
French—Canada	X			X
Spanish—Mexico	X	X		X
Spanish—United States	X	X		X

* Adding additional languages for phonetics or transcription requires collaboration with Cisco. Contact your account representative for more information.

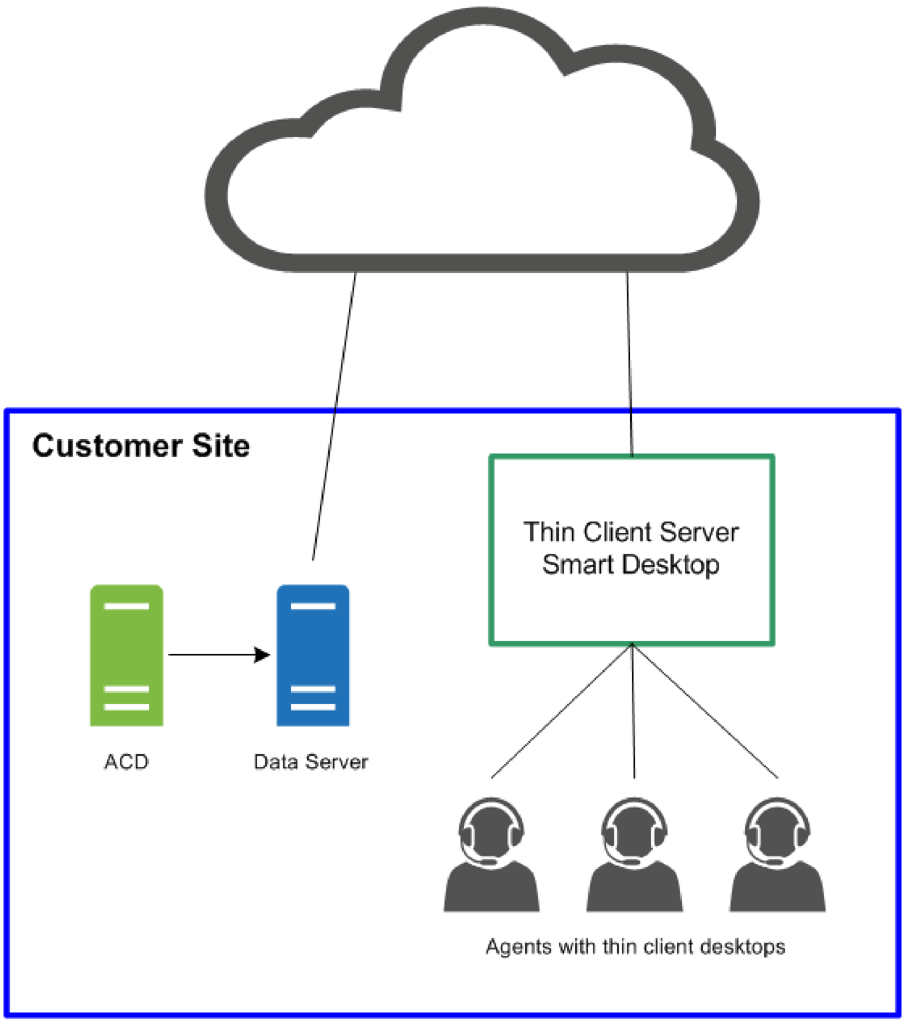
‡ Text analytics is available for all languages that use Western characters.

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.

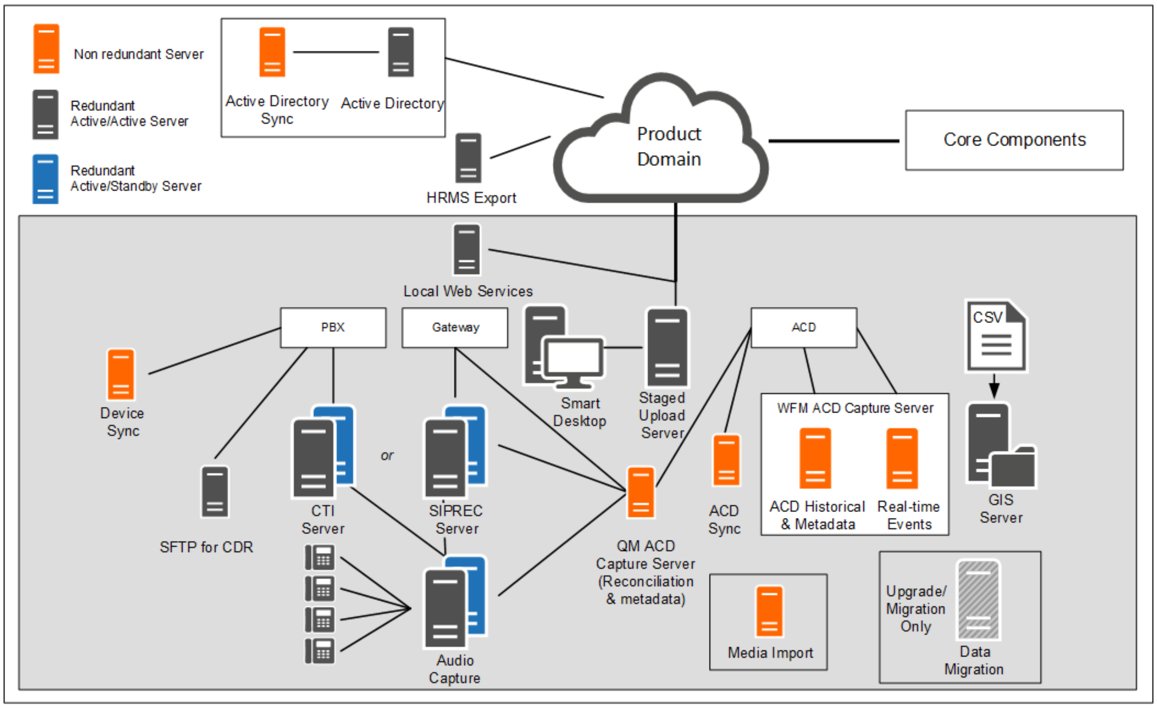
Agents can also view their schedules outside of work through an email client or calendar application on a mobile device or personal computer. The email client or calendar application displays the schedule as it appears in the Webex WFO interface by reading the iCalendar data file from the WFM iCalendar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

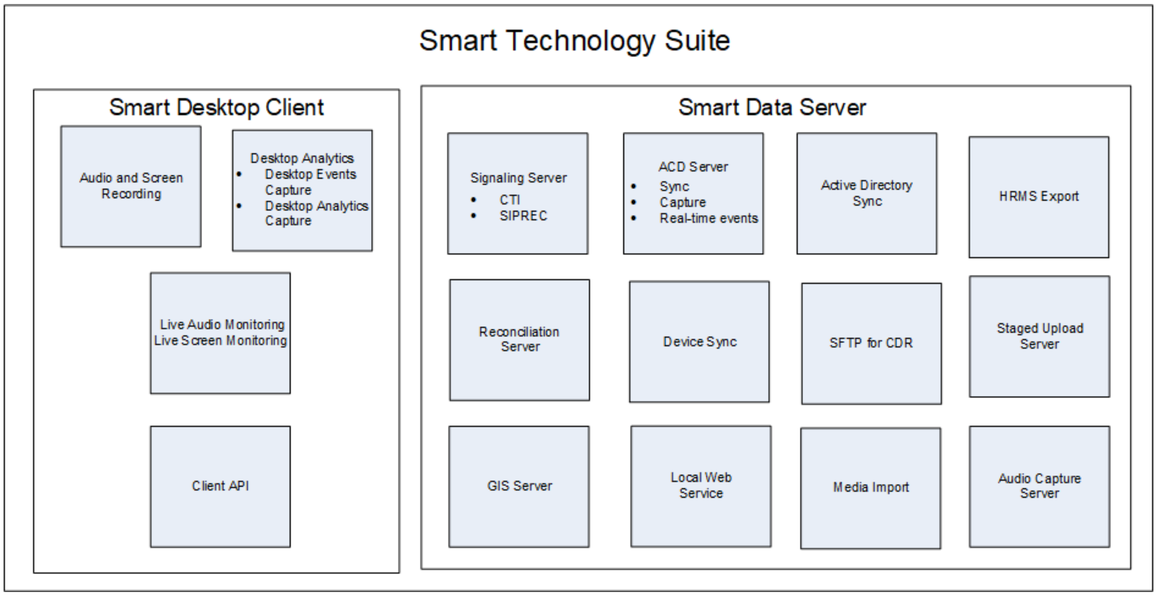
The following clients and devices are supported for viewing a schedule outside of work:

- 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

The Smart Desktop is installed on agent desktops in the contact center or on a server that hosts a supported thin client. It captures all user data (that is, call recording, screen, and desktop activity) on an agent desktop. The installer must be added to the Downloads page so that it can be accessed by the tenant administrator.

Data Server

The Data Server is responsible for ACD synchronization and two-stage uploads. 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.

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

The Data Server installation includes the following servers:

- Webex WFO ACD Sync Server—Used to sync user and team information from a supported ACD.
- Webex WFO Audio Capture Server—Used for Edge Server or Gateway (SBC) audio recording environments. The primary Signaling server (CTI or SIPREC) assigns calls to capture servers in a round-robin algorithm.
- Webex WFO GIS (Generic Interface Service) Server—Used to import external contact metadata from a CSV file into Webex WFO.
- Webex WFO Signaling Server—Can be either an CTI Signaling server or SIPREC Signaling server, used to track start and stop events and capture metadata for call recordings.
    - A CTI Signaling Server is used for Edge Server recording environments.
    - A SIPREC Signaling Server is used for Edge Gateway (SBC) recording environments.
- Webex WFO Staged Upload Server—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 QM ACD Capture Server—Used to capture custom metadata and reconcile calls received through a gateway.
- Webex WFO WFM ACD Capture Server—Used to capture historical and real-time ACD data for WFM and ACD metadata to attach to call contacts as custom metadata.

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

Desktop Hardware	
	separately, so you must apply this formula for each monitor.
CPU	Intel Core 2 Duo 2.0 GHz, Core i3, AMD Athlon 64 X2 or better
Memory	2 GB

Desktop Software

.NET Framework

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

WebM Media Foundation Components

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

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

Browsers

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

> **NOTE** It is recommended that you disable the Internet Explorer browser’s smooth scrolling option to prevent “screen bounce” when working with Webex WFO. To do this, open Internet Options. On the Advanced tab, locate Browsing > Use smooth scrolling and clear the check box.

Internet Explorer and Windows

By default, Windows 8.1 opens Internet Explorer 11 in the Metro mode. This mode is not supported with Smart Desktop’s capture feature. Desktop capture requires that Internet Explorer be run in Desktop mode.

To run Internet Explorer in Desktop mode, pin it to the Windows taskbar and launch it from there.

Desktop Analytics Plugin/Extension

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

Enable the Desktop Analytics extension in Internet Explorer

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

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

Enable the Desktop Analytics extension in Firefox

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

Enable the Desktop Analytics plugin in Chrome

Download and install the Calabrio Analytics Plugin, version 0.1.5. 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 past 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.

Thin Client Servers

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

When using a thin client server, note:

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

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: Avaya IP Office with ACCS
- 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: Genesys
- 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 Calabrio 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				

Port	Use	Source	Destination	Notes
TCP 22	Communication between both the SFTP Configuration and the Regional Data Server Reconciliation Settings on the Data Server and the CUCM Billing Service	CUCM Billing Service	SFTP, Data Server	—
TCP 8443	Communication between CUCM AXL and Regional Data Server ACD Sync Settings on the Data Server	CUCM AXL	Data Server	—
Data Server—ACD Sync: Cisco Unified CCE				
TCP 1433 TCP 1434	Communication between the Cisco Unified CCE AW SQL Server Database and the Regional Data Server ACD Sync Settings on the Data Server	Cisco Unified CCE AWDB SQL Server Database	Data Server	—
TCP 1433 TCP 1434	Communication between the Cisco Unified CCE HDS SQL Server Database and both the Regional Data Server Reconciliation Settings and the Regional Data Server ACD Capture Settings on the Data Server	Cisco Unified CCE HDS SQL Server Database	Data Server	—
TCP 42027	Communication between the Cisco Unified CCE CTI Service (Side A) and the Recording CTI Signaling Server Settings on the Data Server	Cisco Unified CCE CTI Service (Side A)	Data Server	Side A default if using PG1. Ports will vary based on what PG you are using. The CTI Server Port configured in the Unified CCE ACD Configuration.
TCP 43027	Communication between the Cisco Unified CCE CTI Service (Side	Cisco Unified	Data Server	Side B default if using PG1. Ports

Port	Use	Source	Destination	Notes
	B) and the Recording CTI Signaling Server Settings on the Data Server	CCE CTI Service (Side B)		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 UCCX				
TCP 1504	Communication between the UCCX Informix Database and both the Regional Data Server ACD Sync Settings and the Regional Data Server ACD Capture Settings	Data Server	UCCX Informix Database	—
TCP 12028	Communication between the Cisco UCCX CTI Service (Side A) and the Recording CTI Signaling Server Settings on the Data Server	Cisco UCCX CTI Service (Side A)	Data Server	Side A Default. This is the RMCM TCP port configured in UCCX System Parameters. The CTI Server Port configured in the UCCX ACD Configuration.
TCP 12028	Communication between the Cisco UCCX CTI Service (Side B) and the Recording CTI Signaling Server Settings on the Data Server	Cisco UCCX CTI Service (Side B)	Data Server	Side B Default. This is the RMCM TCP port configured in UCCX System Parameters. The CTI Server Port configured in the UCCX ACD Configuration.
Data Server—GIS				
—	—	—	—	While GIS does not directly listen on

Port	Use	Source	Destination	Notes
				a port, the files need to be copied over to the Data Server. If the copying is done via FTP, port 20 and 21 are used.
Data Server—Record/Capture				
UDP 39500–43500	Recording RTP	Phone or voice gateway	Record Server	—
UPD 49152–65535	Live audio monitoring—RTP	Record Server	Supervisor’s browser	—
Data Server—Signaling: CTI				
TCP 443	Signaling Server	Signaling Server	Cisco API	—
TCP 52102	Recording Signaling	Record Servers or Smart Desktop clients	Signaling Server	—
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	—

Port	**Use**	**Source**	**Destination**	**Notes**
			and subscribers	
TCP 5060 UDP 5060	SIP signaling from Unified CM	Any Unified CM publisher or subscriber	Signaling Server	Not secure
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	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.”

Installation

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

Installing Webex WFO Smart Desktop

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

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

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

Manual Installation

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

To 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 **Webex WFO Smart Desktop** installer link. Webex WFO provides a .exe file for manual installation. The available .msi file is for the SCCM push only.
3. Accept the End User License Agreement (EULA) when prompted.
4. Run the installer and follow the prompts in the installation wizard.
5. Select the **Activate** checkbox if prompted and click **Finish**.
6. After running the Smart Desktop installer, restart your system.
7. Run the Client Verification tool. See Client Verification Tool for more information.
8. Test Smart Desktop. See Testing Smart Desktop for more information.

Installation Using GPO

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

To 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 **Webex WFO Smart Desktop** installer link. Webex WFO provides a .exe file for manual installation.
3. Accept the End User License Agreement (EULA) when prompted.
4. Copy **CalabrioONEDesktopSetup_<TenantName>.exe** from your Downloads folder and paste it in the server share location.
5. Create a batch script to run the installer that contains the following script:

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

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

Installation Using SCCM

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

To install Smart Desktop using SCCM:

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

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

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

     and click **Next**.

     > **NOTE** See Installation Using GPO to understand the implications of using these arguments.
9. Click **Next** and then click **Close**.

The /ACTIVATE and /NORESTART Arguments

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

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

The NPCAP ARGUMENTS

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

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

Push Installation Return Codes

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

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

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

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

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

Testing Smart Desktop

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

To test Smart Desktop:

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

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

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

Client Verification Tool

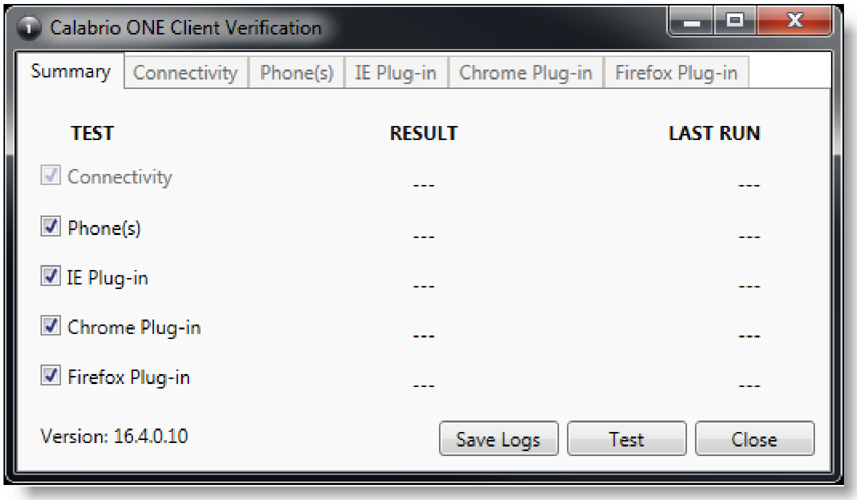
The Client Verification tool tests the client PC to ensure that the connectivity with servers and the phone are suitable for running Smart Desktop. It is installed when Smart Desktop is installed. The tool runs various tests and reports results as either a pass or fail.

To run the Client Verification tool:

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

   ```
   C:\Program Files (x86)\Webex WFO\Desktop\Active\bin\
   ```

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

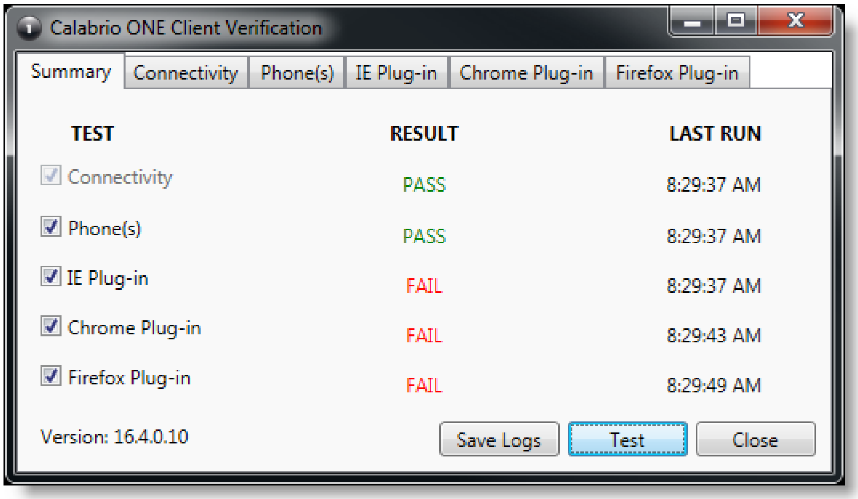


TEST	RESULT	LAST RUN
☑ Connectivity	---	---
☑ Phone(s)	---	---
☑ IE Plug-in	---	---
☑ Chrome Plug-in	---	---
☑ Firefox Plug-in	---	---

Version: 16.4.0.10

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

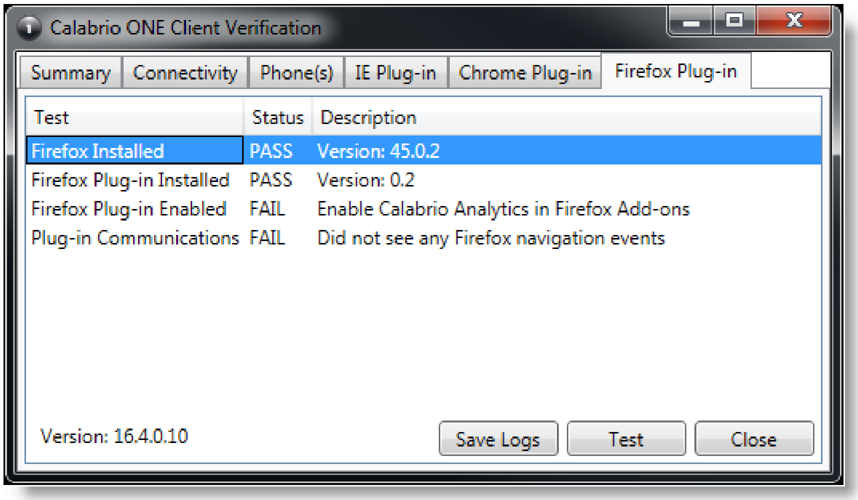
4. The tool reports the results of the test as either a pass or fail.



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

Version: 16.4.0.10

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



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

Version: 16.4.0.10

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

Recording Controls

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

Using Recording Controls is optional.

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

The Recording Controls executable is installed here:

```
C:\Program Files (x86)\Webex WFO\Desktop\Active\bin\DCC.exe
```

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

Configuring Citrix Machines for Writing Log Files

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

To configure Citrix machines to write log files:

1. Create a directory to store IE logs.

   EXAMPLE C:\log_files

2. Give the directory you created Low Integrity access.

   a. Navigate to the Administrator command prompt.

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

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

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

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

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

Removal

The following topics describe how to uninstall Webex WFO components.

Uninstalling Webex WFO Smart Desktop

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

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.

To uninstall Smart Desktop using GPO:

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.