



Webex WFO Installation Guide for Hybrid Cloud Deployments

First Published: July 10, 2020

Last Updated: April 26, 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2000–2021 Cisco Systems, Inc. All rights reserved.

Contents

- Contents** 3
- Introduction** 9
- Localization and Supported Languages** 10
 - User Interface and Documentation 10
 - Analytics 11
- System Configuration** 13
 - Customer On-Premises Environment 13
 - On- Prem with End Point Recording Configuration 14
 - On Prem with End Point Recording in a Thin Client Configuration 15
 - On Prem with Network Recording Configuration 16
- Supported Environments** 17
 - Supported Phones 17
 - Hard Phones 17
 - Supported Codecs 17
 - Using Multiple Soft Phones 17
 - Supported Mobile Devices 18
- Edge Components** 19
 - Webex WFO Smart Desktop 20
 - Data Server 20
- System Requirements** 23
 - Desktop Hardware 23
 - Desktop Software 24

.NET Framework	24
WebM Media Foundation Components	24
Browsers	24
Adobe Acrobat Reader	25
Desktop Software and Audio Capture	25
Server Software	26
Data Explorer Database	26
Microsoft SQL Server	26
VMWare	27
Tomcat CTI Service Memory Allocation	28
Thin Client Servers	28
Port Usage	29
Core Components	30
Edge Components	39
Data Server Components	39
File Encryption	44
Password Policy	44
Password complexity requirements	44
Authentication	47
Installation Prerequisites	49
Configure a Network Load Balancer	49
Best Practices	50
Apache Load Balancer	50
Using Fully Qualified Domain Names	51

Asian Language or Unicode Font Support	51
Installing Supplemental Language or Unicode Support	51
Supporting Asian Languages or Unicode in PDF Reports	52
Configure Cisco Unified Communications Manager	52
Configure a JTAPI User	53
Configuring Cisco Unified CM Administration	54
Installing the Webex WFO Platform	57
Configuration	59
Configuration and Installation Order	59
Configuring the Web Server	60
Configuring httpd.conf Without Load Balancing	60
Configuring httpd.conf With Load Balancing	61
Configuring the Web Server for Data Explorer	64
Configuring the Application Server	66
Sharing a Folder	66
Installing FFmpeg	66
Configuring Webex WFO Connection Settings	67
Configuring the Grid Server	69
Installing FFmpeg	69
Configuring Grid Server Properties	69
Configuring the Mail Server	70
Installing Applied Analytics Features	71
Installing the Transcription Server	73
Step 1: Download and Source the Installation Script	74

Step 2: Update the Repository and Operating System	75
Step 3: Install the Transcription Server	76
Configuring the Webex WFO Platform for Transcription	78
Configuring the Transcription.json File	78
Installation	79
Java Memory Usage	79
Installing Webex WFO Smart Desktop	82
Manual Installation	83
Installation Using GPO	83
Installation Using SCCM	84
Client Verification Tool	85
Push Installation Return Codes	87
Testing Smart Desktop	90
Recording Controls	91
Installing the Data Server	91
Prerequisites	91
Installing the Data Server for a Single Tenant	92
Installing the Data Server for Multiple Tenants	92
Installing the Thin Client Server	93
Installing Data Explorer	94
1. Prerequisites	94
2. Install and Configure PostgreSQL	96
3. Configure Webex WFO Windows Servers	98
4. Install Data Explorer	100

5. Installing Data Explorer	103
6. Configure Data Explorer in Webex WFO	105
Configuring Citrix Machines for Writing Log Files	106
Managing Certificates	109
Certificate Requirements	109
Creating an SSL Certificate Signing Request	110
Signing a Private CA Certificate	114
Upgrading from Previous Versions	117
Upgrading Applied Analytics Features	118
Validating the Installation	121
Removal	123
Uninstalling Webex WFO	123
Uninstalling Services	123
Removing the Webex WFO Databases	124
Uninstalling Webex WFO Smart Desktop	124
Uninstalling Using GPO	124
Uninstalling the Data Server	125

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 hybrid 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	
French—Canada	X	
French—France	X	
German—Germany	X	

	User Interface	Documentation
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
French—Canada	X			X
Spanish—Mexico	X	X		X
Spanish—United States	X	X		X

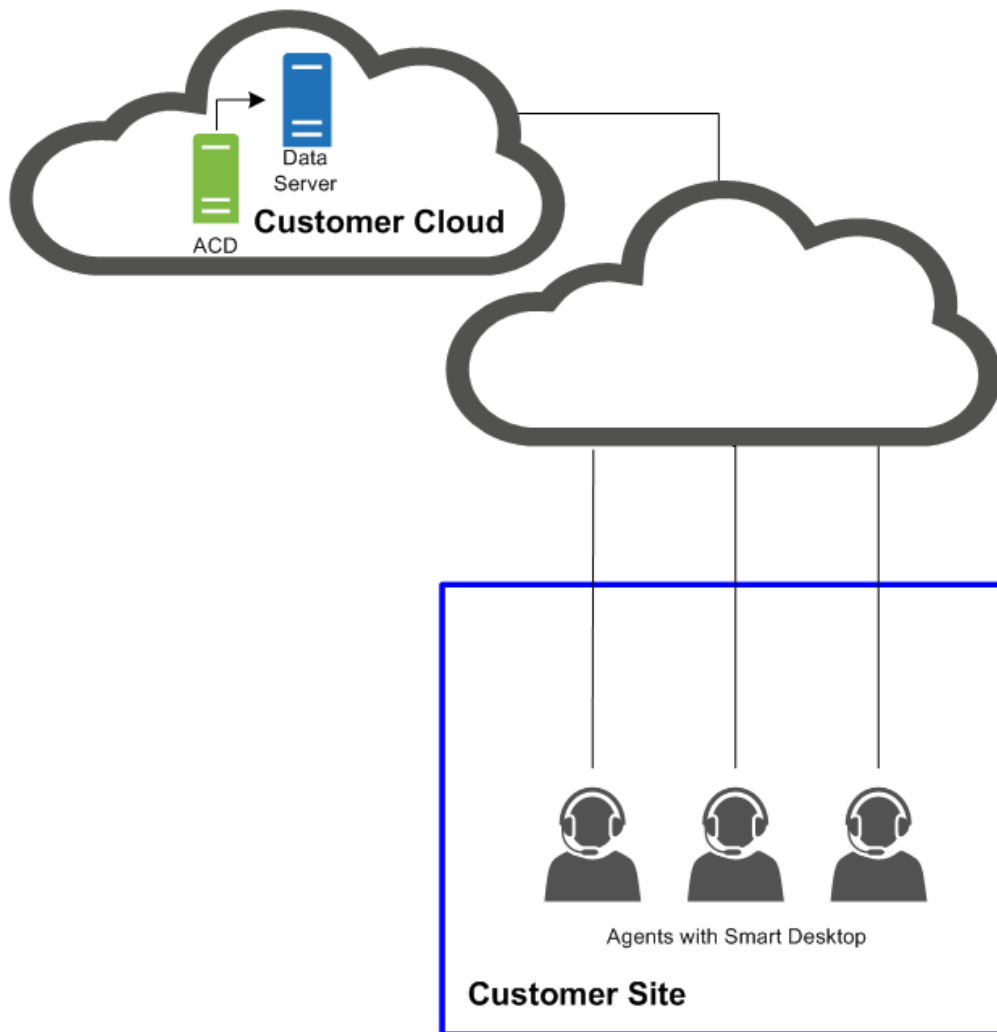
Localization and Supported Languages | Analytics

* 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

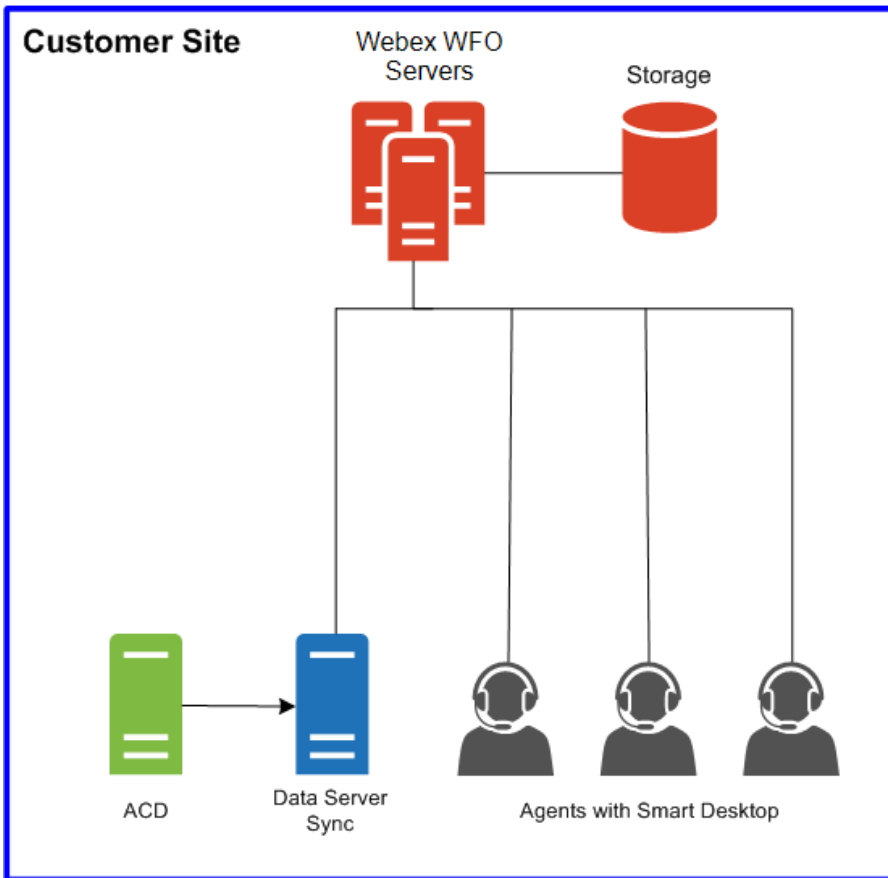
This diagram displays a typical Webex WFO hybrid cloud deployment.



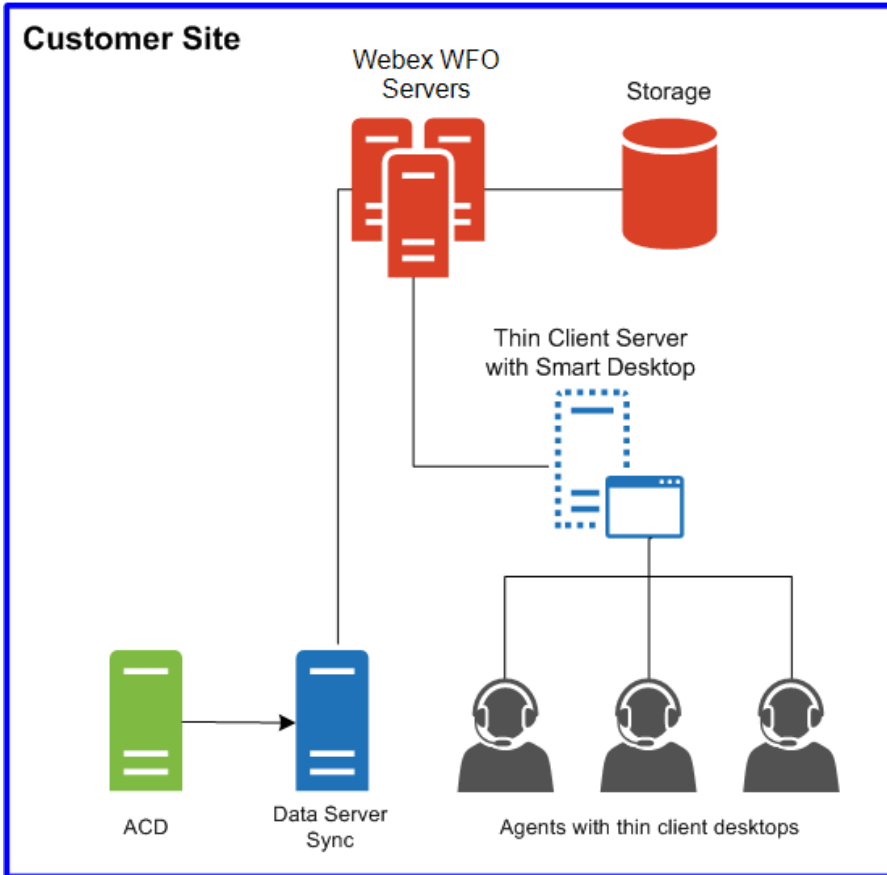
Customer On-Premises Environment

Webex WFO components can be configured in many ways. The following diagrams depict some typical system configurations.

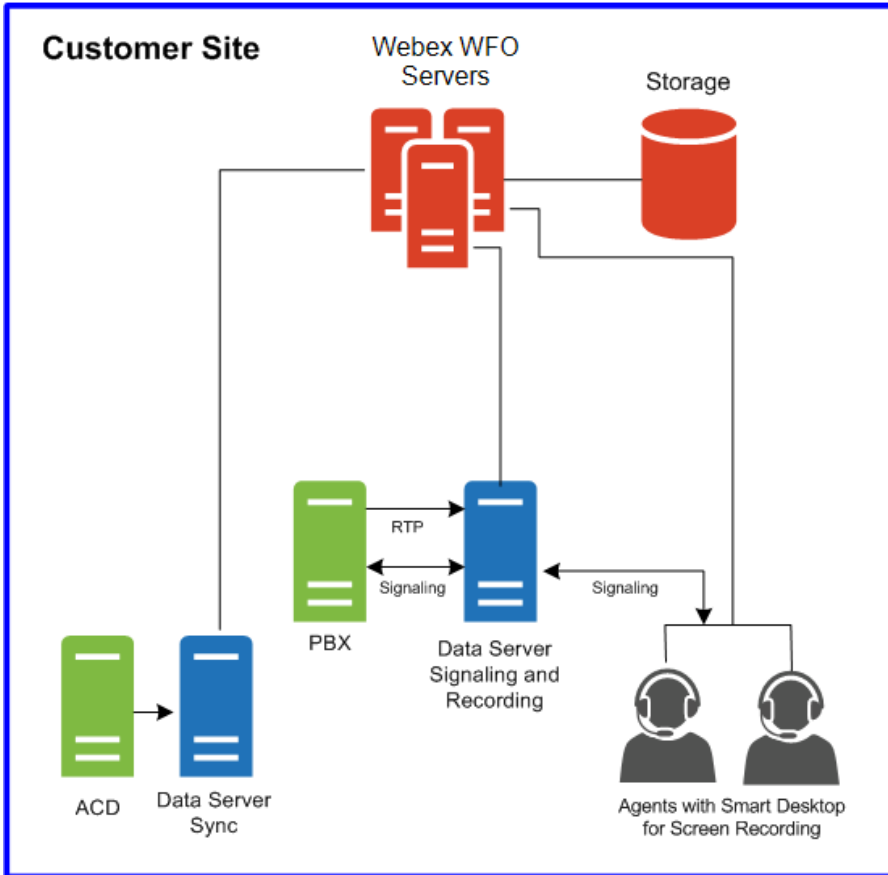
On- Prem with End Point Recording Configuration



On Prem with End Point Recording in a Thin Client Configuration



On Prem with Network Recording Configuration



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.

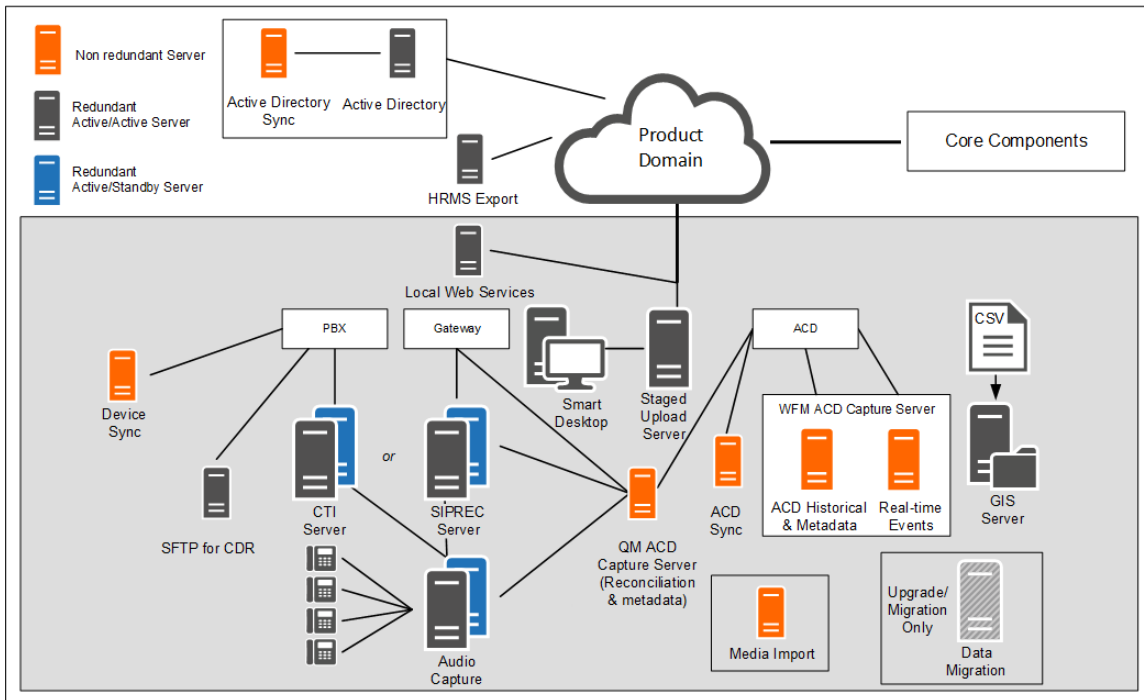
Agents can also view their schedules outside of work through an email client or calendar application on a mobile device or personal computer. The email client or calendar application displays the schedule as it appears in the Webex WFO interface by reading the iCalendar data file from the WFM iCalendar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

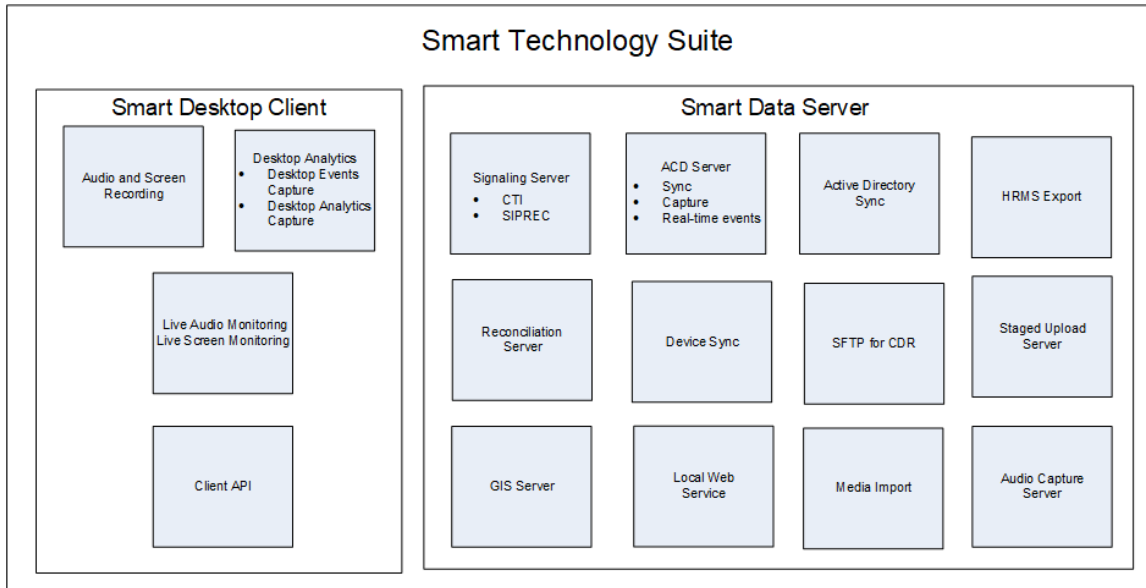
The following clients and devices are supported for viewing a schedule outside of work:

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

NOTE

If the Data Server must connect through a web proxy, all Webex WFO services running on it must run as Windows login accounts with proxy settings.

When configuring the Data Server with a proxy server, the Data Server service must be configured to run as a local administrator.

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

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/hecgknieibccghjmmhhckdfceobjoffdf>

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.

Server Software

The **Webex WFO Supported Product Compatibility List** contains the full list of server operating systems, Microsoft SQL servers, and VMWares supported by Webex WFO.

Data Explorer Database

The required PostgreSQL Version is 9.6.

Microsoft SQL Server

Microsoft SQL server installations must include the latest service pack.

Install SQL Server and verify that Collation is **SQL_Latin1_General_CP1_CI_AS**. Authentication must be set to Mixed Mode.

The latest version of Microsoft ODBC Driver 11 for SQL Server — Windows must be installed on the Webex WFO server.

Microsoft SQL Forced Encryption (TLS) is not supported and needs to be disabled.

The user must be configured in SQL Server Management Studio as follows:

- Choose SQL Server Authentication as the authentication mode.
- When entering the password, clear the Enforce Password Policy check box and choose English as the default language.

The user responsible for configuring the Webex WFO connection settings (see [Configuring the Application Server](#)) must have the dbcreator server role, which gives permission to create a database, and the security admin server role, which gives the ability to create or modify logins and users in Microsoft SQL.

SQL can be deployed stand-alone or within an existing SQL farm or cluster as a dedicated instance, always on availability group for resilience.

NOTE All servers running the Webex WFO Application server services must have SQL Command Line Utilities and PDBC drivers installed for the version of SQL Server they are running.

VMWare

A virtual server environment requires hardware resources equivalent to those required for a physical server. Webex WFO must be installed in its own computing environment that is not shared with multiple hosts.

IMPORTANT VMware Snapshots are only supported for Webex WFO when Webex WFO is not running (that is, when analytic tasks are not running and calls are not being recorded). A snapshot impacts critical server resources. Recording and indexing failures will occur if snapshots are taken while Webex WFO is running. Before you take a snapshot, verify that Webex WFO is not running and stop the Webex WFO services or pause or shut down the server. After you take a snapshot, restart the Webex WFO services.

Recommended VMware Settings

Setting	Description
Shares	Guarantees that VMs are given a percentage of an available resource (CPU, RAM, Storage I/O, Network)
Limits	Guarantees that a VM does not consume more than a specified resource limit
Resource Reservation	Provides an allocated resource for a VM on startup

VMWare Support Statement

will support customers who run Webex WFO products on supported operating systems, irrespective of whether they are running in VMware environments or not. supports operating systems, not specific hardware configurations. Accordingly, VMware operates as a hardware abstraction layer.

VMware supports a set of certified operating systems and hardware, and the customer and VMware will be responsible for any interactions or issues that arise at the hardware or operating system layer as a result of their use of VMware.

will not require clients to recreate and troubleshoot every issue in a non-VMware environment; however, does reserve the right to request our customers to diagnose certain issues in a native certified operating system environment, operating without the virtual environment. will only make this request when there is reason to believe that the virtual environment is a contributing factor to the issue.

Any time spent on investigation of problems that may, in the sole opinion of be related to VMware, will be handled in the following fashion:

- 1) will provide standard support to all Webex WFO products.
- 2) If a problem is encountered while Webex WFO is running in a VMware environment, the client may be required to recreate the problem on a non-VMware server unit, at which time will provide regular support.
- 3) Regardless of the problem type or source, if the problem is determined to be a non VMware related issue, time spent on investigation and resolution will be covered as part of regular maintenance, and support will be provided as usual.

Tomcat CTI Service Memory Allocation

The default memory setting for the Tomcat CTI service is 768 Mb. This allocation will be sufficient for most Webex WFO implementations.

Thin Client Servers

NOTE Webex WFO supports Citrix XenApp installed only on a supported Windows server. See [Server Software](#) for more information.

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.

Core Components:

- [Application Server](#)
- [Broker](#)
- [WFM Grid-Broker](#)
- [Data Explorer](#)
- [Forecast](#)
- [Applied Analytics](#)
- [Scheduler](#)
- [Web Server](#)
- [Miscellaneous Other Ports](#)

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](#)

Core Components

Port	Use	Source	Destination	Notes
Application Server				
UDP 162	Communication between the SNMP server and the Application Server Hazelcast cluster	Application Servers	SNMP server	Used only if SNMP is enabled on the Application Management > Monitoring > Notifications page
TCP 1433	Communication between the	Application Servers	SQL database	Initially configured on the System

Port	Use	Source	Destination	Notes
	Application Server and the SQL database			Configuration page at install and maintained on the Application Management > System Configuration > Database Instance page
TCP 5701	Communication between the Application Servers in the Hazelcast cluster	Application Servers	Application Servers	This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_AppSessions.port=5701
TCP 5801	Communication between the Application Server and the Broker server Hazelcast cluster	Application Servers	Broker server	This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_ComputingGridBroker.port=5801
TCP 8888 UDP 8888	Communication between the Web Server and Application Server	Web Server	Application Servers	—
Broker—Hazelcast Cluster				
TCP 1433	Communication between Broker	Broker server	SQL database	Direction: Inbound/Outbound

Port	Use	Source	Destination	Notes
	cluster servers and the SQL database			Initially configured on the System Configuration page at install and maintained on the Application Management > System Configuration > Database Instance page
TCP 5801	Communication between servers in the Broker Hazelcast cluster with servers in the Application Server Hazelcast cluster	Broker server	Application Server	Direction: Inbound/Outbound This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_ComputingGridBroker.port=5801
TCP 5801	Communication between servers in the Broker Hazelcast cluster with Grid servers	Broker server	Grid server	Direction: Inbound/Outbound This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_ComputingGridBroker.port=5801
Broker—Ignite Cluster				

Port	Use	Source	Destination	Notes
TCP 11211	Server port	—	—	Direction: Inbound/Outbound Used for service administration (for example, connecting to the Ignite cluster via command line tools)
TCP 47100-47200	Communication port range	Application Server, Broker	Broker	Direction: Inbound/Outbound
TCP 47500-47600	Discovery port range	Application Server, Broker	Broker	Direction: Inbound/Outbound
Data Explorer Servers				
TCP 8080	Communication between the Application Web server main port	Client request through a browser	Platform service	—
TCP 8090	Authentication service requests, tokens, sessions	Platform service, Webex WFO Web UI	Authentication service	This port needs to be exposed to complete OAuth2 Flow
TCP 2020	Tenant provisioning requests	Platform service and Data Explorer Application servers	Tenant provisioning service	Ensure Port UDP 53 is not blocked from the containers.
TCP 1433	Communication between the Data Explorer Application servers and the SQL Database	Data Explorer Application servers	SQL database	
Applied Analytics Server				

Port	Use	Source	Destination	Notes
TCP 40010	Communication between WFO Machine Learning Sentiment server to accept incoming requests for sentiment tasks	Hazelcast instance	Applied Analytics Server	The port usage is attached to the docker container wfomlsentiment_broker-apply and sends the requests to the functional wfomlsentiment_worker-apply container associated with it. The default port can be changed by modifying the /wfo_ml/wfo_ml_sentiment/.env file: APPLY_PORT=40010
TCP 40000	WFO Machine Learning – Predictive Evaluation Score (PES) Applicator service to run analytics tasks and compare a contact’s data to the PES model built	Hazelcast instance	Applied Analytics Server	The port usage is attached to the docker container wfomlpes_broker-apply and sends the requests to the functional wfomlpes_worker-apply container associated with it. The default port can be changed by modifying the /wfo_ml/wfo_ml_pes/.env file: APPLY_PORT=40000
TCP 40001	WFO Machine Learning – Predictive Evaluation Score (PES) Model Builder analyzes past QM, WFM, and Analytics data to identify what	Hazelcast Instance	Applied Analytics Server	The port usage is attached to the docker container wfomlpes_broker-build and sends the requests to the functional wfomlpes_worker-build

Port	Use	Source	Destination	Notes
	evaluation patterns can be found with the data provided.			container associated with it. The default port can be changed by modifying the /wfo_ml/wfo_ml_pes/.env file: APPLY_PORT=40001
TCP 40100	WFO Machine Learning – Predictive Net Promoter Score (NPS) Applicator service to run analytics tasks and compare a contact’s data to the NPS model built	Hazlecast Instance	Applied Analytics Server	The port usage is attached to the docker container wfomlnps_broker-apply and sends the requests to the functional wfomlnps_worker-apply container associated with it. The default port can be changed by modifying the /wfo_ml/wfo_ml_nps/.env file: APPLY_PORT=40100
TCP 40101	WFO Machine Learning – Predictive Net Promoter Score (NPS) Model Builder analyzes past QM, WFM, and Analytics data to identify what NPS patterns can be found with the data provided.	Hazlecast Instance	Applied Analytics Server	The port usage is attached to the docker container wfomlnps_broker-build and sends the requests to the functional wfomlnps_worker-build container associated with it. The default port can be changed by modifying the /wfo_ml/wfo_ml_nps/.env file: APPLY_PORT=40101
Web Server				

Port	Use	Source	Destination	Notes
TCP 80	Web Server servers listening for HTTP traffic	External clients	Web Server	—
TCP 443	Web Server servers listening for HTTPS traffic	External clients	Web Server	—
WFM Grid-Broker Server - Compile				
TCP 1433	Communication between servers in the Compile Hazelcast cluster and the SQL Database	Compile servers	SQL database	Initially configured on the System Configuration page at install and maintained on the Application Management > System Configuration > Database Instance page
TCP 5901	Communication among servers in the Compile Hazelcast cluster	Compile servers	Compile servers	This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_CompileGrid.port=5901
WFM Grid-Broker Server—Forecast				
TCP 1433	Communication between servers in the Forecast Hazelcast cluster and the SQL Database	Forecast servers	SQL database	Initially configured on the System Configuration page at install and maintained on the Application

Port	Use	Source	Destination	Notes
				Management > System Configuration > Database Instance page
TCP 6001	Communication among servers in the Forecast Hazelcast cluster	Forecast servers	Forecast servers	This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_ForecastGrid.port=6001
WFM Grid-Broker Server—Scheduler				
TCP 1433	Communication between servers in the WFM Forecast Hazelcast cluster and the SQL Database	Scheduler servers	SQL database	Initially configured on the System Configuration page at install and maintained on the Application Management > System Configuration > Database Instance page
TCP 6101	Communication among servers in the Scheduler Hazelcast cluster	Scheduler servers	Scheduler servers	This port is the default. It can be configured in the following line in the hazelcast.properties file (<installation directory>\Config): cluster.WFO_SchedulerGrid.port=6101
Miscellaneous Other Ports				

Port	Use	Source	Destination	Notes
TCP 135–139 UDP 135–139	NetBIOS communication between external storage on a network server (SAN/NAS) and the Application Server	SAN/NAS	Application Server	—
TCP 389 UDP 389	LDAP communication between Active Directory and the Data Server	Active Directory	Data Server	Configured on the Application Management > Tenant Administration > Active Directory Configuration page. This is the default port.
TCP 445	SMB communication between external storage on a network server (SAN/NAS) and the Application server	SAN/NAS	Application Server	—
LDAPS 636 (LDAP over SSL)	LDAP communication between Active Directory and the Data Server	Active Directory	Data Server	Configured on the Application Management > Tenant Administration > Active Directory Configuration page

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				
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	—

Port	Use	Source	Destination	Notes
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 B) and the Recording CTI Signaling Server Settings on the Data Server	Cisco Unified CCE CTI Service (Side B)	Data Server	Side B default if using PG1. Ports will vary based on what PG you are using. The CTI Server Port configured in the Unified CCE ACD Configuration.

Port	Use	Source	Destination	Notes
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 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.

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

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	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.

To prevent unauthorized access to recordings, all Webex WFO servers should be located in a secure location so only authorized personnel have access to the key. To allow other users to have access to the audio files, export them and then move them to a less secure location.

Password Policy

Password complexity requirements

Webex WFO's 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: ! # \$ % & () , . / : ; = ? @ ^ `

Category	Description
----------	-------------

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.

Passwords must conform to the following rules:

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.”

For information on configuring Webex WFO authentication, see the topic, “Authentication” in the *Webex WFO User Guide*.

Installation Prerequisites

The following should be set up and configured before you install Webex WFO.

Configure a Network Load Balancer

Webex WFO supports web server redundancy. The web server includes the Apache Web Server and can be used to load balance.

If you choose to use your own network load balancer, the network load balancer must support the following features:

- Websockets—a protocol that provides full-duplex communication channels over a TCP connection.
- Sticky sessions—the ability to route requests for a particular session to the same machine that serviced the first request for that session. This is used for UI requests.

The Webex WFO Desktop Recording client server requires websockets for client communication and sticky sessions for Alerts. Most load balancers support these features. However, some load balancers (for example, AWS ELB) do not support web sockets natively, and the workaround prevents sticky sessions from being configured.

The network load balancer must point to the IP address or host name of the primary and backup web servers (if applicable).

When configuring the network load balancer, you must:

- Route all URLs that start with “/api” to the application server cluster.
- Route the default route to the UI Server cluster.

Consult your network load balancer documentation for configuration instructions.

NOTE An example of an httpd.conf file that is configured with load balancing is provided in the Web Server topic.

Best Practices

- Use a load balancer (for example, IIS AAR, Apache, or Netscaler) that supports websockets without workarounds.
- Use one load balancer for the Webex WFO user interface and the other load balancers for client connections.
- Use a server with a minimum of 143 IOPS.
- Redirect persistent websocket traffic to a dedicated cluster of web servers.

Apache Load Balancer

The Apache load balancer has a limit of 15,000 concurrent connections. If you have more than 15,000 concurrent connections, you must add one Apache load balancer per every additional 15,000 concurrent connections. Other load balancers will have different capacities and you will have to scale according to the capacity of that load balancer.

Each client desktop uses two connections when a user is logged in (one for the service and one for the logged-in agent). If your agents are using a thin client to connect to Webex WFO, the number of connections used is the number of concurrent agents plus 1 for the service.

NOTE The Apache load balancer can become overloaded and cause performance issues when too many users are using the same environment. To prevent this problem, open more TCP port connections on the Apache load balancer. For more information, see the Microsoft TechNet article located at <https://technet.microsoft.com/en-us/library/cc938196.aspx>.

To open more ports:

1. On the Apache load balancer, navigate to C:\Program Files\Common Files\Webex WFO\Server\config and open the httpd.conf file in a text editor.
2. Add the following statement under #Include conf/extra/httpd-mpm.conf:

```
<IfModule mpm_winnt_module>
    ThreadLimit 15000
    ThreadsPerChild 15000
    MaxConnectionsPerChild 0
</IfModule>
```

3. Save the file.

Using Fully Qualified Domain Names

Webex WFO supports fully qualified domain names (FQDNs) or host names and IP addresses when configuring the system. If you choose to use FQDN, observe the following guidelines:

- The host names specified for Webex WFO must be resolvable by the clients that need to connect to it.

NOTE The clients do not need to be part of the domain.

- The client desktop must be able to connect to the server using the hostname.
- If the client is using desktop recording, the client must be able to connect to the web server.

Asian Language or Unicode Font Support

If you have user-entered data (such as agent or team names) in Asian characters or a Unicode font, you must install the supplemental language support for East Asian languages or a Unicode font. If these are not installed, the characters do not appear in reports when you generate a PDF.

The following languages require supplemental language support.

- Chinese (China and Taiwan)
- Japanese
- Korean
- Russian

Installing Supplemental Language or Unicode Support

1. On the Web Base server, start Control Panel.
2. Open the Clock, Language, and Regions utility and select Language.
3. In the Language window, click Add a Language, select the desired language, and click Add.
4. Restart the Web Base server.
5. After the server has restarted, open Windows Explorer and navigate to C:\Windows\Fonts.
6. Copy the font or fonts you just added:

Batang (Russian and Korean)

MingLiU (Chinese and Japanese)

A Unicode-supported font such as Calibri

7. Navigate to `C:\Program Files\Calabrio\WFO_QM\Java\lib\fonts` and paste the fonts into the fonts folder.
8. Restart the Jetty service.

Supporting Asian Languages or Unicode in PDF Reports

Perform the following steps if you are using a non-Asian locale or a Unicode font, but want to include Asian characters or a Unicode font in your PDF reports. Note that HTML and CVS format reports automatically display Asian characters and Unicode fonts.

1. On the Web Base server, navigate to `.. \Program Files\Cisco\WFO_QM\Jetty\calabrio-solutions\reports` and open the properties file associated with your locale.

EXAMPLE Open `QMReport_zh_CN.properties` if your locale is Chinese.

2. Find “encoding=” and change it to “encoding=UTF-8”.
3. Find “font=Arial” and change Arial to one of the following font names:

- Batang (Russian and Korean)
- MingLiU (Chinese and Japanese)
- A Unicode-supported font such as Calibri

NOTE The font name must match the font name as it appears in the Font name field when you double-click the font in the `C:\Windows\Fonts` folder.

4. Open Windows Explorer and navigate to `C:\Windows\Fonts`.
5. Select and copy the font you just added to the properties file and paste it to this location:

`C:\Program Files\Calabrio\WFO_QM\Java\lib\fonts`

6. Save and close the properties file.
7. Restart the Jetty service.

Configure Cisco Unified Communications Manager

Before you install Webex WFO, configure your Cisco Unified Communications Manager (Unified CM) as follows:

1. Associate phones with the JTAPI user (see [Configure a JTAPI User](#)).
2. Use the Cisco documentation to configure Network Recording or Network Based Recording (optional).
 - Create a recording profile.
 - Create a SIP trunk.
 - Create a route pattern.
 - Assign the recording profile to the DN's to be recorded.
 - Configure DN for a monitoring calling search space.
 - Confirm the DN's monitoring calling search space includes a route pattern.

See [Configuring Cisco Unified CM Administration](#) for more information.

3. Verify the following phone configuration parameters are enabled (Desktop Recording only):
 - PC Port
 - PC Voice VLAN Access
 - Span to PC Port

Configure a JTAPI User

Recording and Quality Management requires that you configure a JTAPI user for Unified CM. This JTAPI user will be used by the Recording CTI service and CUBE SIP CTI service to log into Unified CM. The JTAPI user name and password will be required when you configure Recording and Quality Management for Unified CM.

NOTE If you are configuring Recording and Quality Management for Gateway Recording, you only need a JTAPI user if you intend to record screens.

To add a JTAPI user for Unified CM, see the “Adding a New User” section in the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager*. This document is available on the Cisco website (www.cisco.com).

When you configure the JTAPI user, consider the following guidelines:

- Recording and Quality Management can share the same JTAPI user with other applications.
- Assign all devices that you want to record to the JTAPI user.

- Assign the Standard CTI Enabled group to the JTAPI user. You also need to assign the Standard CTI Allow Call Monitoring group to the JTAPI user. Live Monitoring requires the permissions provided by this group.

Configuring Cisco Unified CM Administration

The following instructions explain how to configure Cisco Unified CM Administrator for Network Recording and Network Based Recording.

Steps	Configuration Steps	Related Procedures and Topics
Step 1	Enable IP phone BIB (Built-in Bridge) to allow monitoring and recording.	See “Cisco Unified IP Phone Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> . NOTE BIB is required to use the silent monitoring and whisper features in the Live Monitoring application.
Step 2	Add a user for the monitoring and recording application.	See “Application User Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 3	Add the user to a access control group that allows monitoring and recording.	See “Application User Setup” and “Access Control Group Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 4	<i>Optional:</i> Configure tones for monitoring and recording.	You can enable a tone to alert parties on the call that they are being monitored or recorded. See “Service Parameter Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 5	Configure DN for a monitoring calling search space.	See “Directory Number Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 6	Enable recording for a line appearance.	See “Directory Number Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 7	Create a recording profile.	See “Recording Profile Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .

Steps	Configuration Steps	Related Procedures and Topics
Step 8	<i>Optional:</i> Create a SIP profile for Recording CTI service.	See “SIP Profile Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
step 9	Disable the Timer Keep Alive Expires setting.	See “SIP Profile Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 10	Create a SIP trunk that points to the Recording CTI service.	See “Trunk Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> . <div style="border-left: 2px solid blue; padding-left: 10px; margin-left: 20px;"> <p>NOTE If you are using Network Based Recording, you must select the This trunk connects to a recording-enabled gateway check box.</p> </div>
Step 11	Create a route pattern for the Recording CTI service.	See “Route Pattern Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Step 12	Configure the recorder for redundancy.	See “Trunk Setup” in the <i>Cisco Unified Communications Manager Administration Guide</i> .

Installing the Webex WFO Platform

To install Webex WFO:

1. Copy CalabrioONEServerSetup.exe to the server.
2. Double-click CalabrioONEServerSetup.exe to start the installation wizard and then click **Next**. The Select Destination Location dialog box appears.
3. Enter the path where you want Webex WFO to be installed or use the default path, and then click **Next**.

NOTE The default path is C:\Program Files\Webex WFO. If you need to change the path, do not specify just the root directory (for example, D:\ or E:\). Always include at least one folder in the path (for example, D:\Cisco).

4. Choose one of the following options:
 - a. To install Webex WFO on a single server, select **Full installation** from the drop-down list, and then click **Next**.
 - b. To install Webex WFO on multiple servers, select **Custom installation** from the drop-down list, clear the check boxes for the servers that you do not want to install on this server, and then click **Next**.

The Configuration Files dialog box appears.

5. Enter a shared configuration path in UNC format, and click **Next**.

BEST PRACTICE Webex WFO supports a multiple server environment and it is recommended that the server components share configuration information to simplify installation and reduce system errors. Provide the network location (using UNC) that will contain the shared configuration files. This location can be located on a server where the software is installed, and must be accessible by all other Webex WFO servers.

IMPORTANT In order to use this shared path, the services on the servers must run as a user that has access to this UNC path.

6. Click **Install**.

7. Click **Finish** to complete the installation.
8. Restart the computer if prompted.
9. (Multiple server installation only) Repeat this procedure for each additional server.

NOTE For information on configuring the servers you have installed for a tenant's system, see the "System Configuration" section of the *Webex WFO System Administrator User Guide* and the *Webex WFO User Guide*.

Configuration

This section describes how to configure Webex WFO components.

NOTE The examples provided here assume you are using an Apache server for load balancing. If you are not using an Apache server for load balancing, you must configure the load balancing server according to the requirements for that server.

BEST PRACTICE For regions that adhere to daylight saving time (DST), Cisco recommends setting the timezone on core Webex WFO servers to UTC. This action prevents the timezone from potentially reverting during future upgrades. An alternative approach is to change the Java virtual machine timezone in the registry setting to UTC. However, this action may need to be repeated as part of any future upgrade. Both actions prevent forecast errors on the DST spring forward date.

Configuration and Installation Order

After installing the Webex WFO platform, and running the setup wizard it installs the following components:

- Webex WFO Web Server
- Webex WFO Application Server
- Webex WFO Grid Server
- Webex WFO Mail Server

After the components are installed you must configure the same Webex WFO components contained in the Webex WFO Platform Setup Wizard in the order detailed below:

- Webex WFO Web Server
- Webex WFO Application Server
- Webex WFO Grid Server
- Webex WFO Mail Server

After these components are installed and configured, you can install and configure the optional Analytics components listed below if you have the required licenses.

- Webex WFO Applied Analytics Server
- Webex WFO Transcription Server

Configuring the Web Server

After you open TCP ports 80 and 443 and install the Web Server service, you need to configure the httpd.conf file on the Web Server if you have more than one application server or are also installing Data Explorer. You can do this with or without load balancing.

- If you have one application server and are also installing Data Explorer, configure the httpd.conf file as described in the following sections: [Configuring httpd.conf Without Load Balancing](#) and [Configuring the Web Server for Data Explorer](#).
- If you have more than one application server, configure the httpd.conf file as described in the following section: [Configuring httpd.conf With Load Balancing](#).
- If you have more than one application server and are also installing Data Explorer, configure the httpd.conf file as described in the following sections: [Configuring httpd.conf With Load Balancing](#) and [Configuring the Web Server for Data Explorer](#).

You do not need to configure the httpd.conf file if you only have one application server and are not also installing Data Explorer.

Configuring httpd.conf Without Load Balancing

To configure httpd.conf without load balancing:

1. On the Web Server, open httpd.conf in a text editor. The file is in the following location:

```
C:\Program Files\Common Files\Webex WFO\Server\config
```

2. Locate the following section, and then replace the IP address represented by the variable <application server IP> with the application server's host name or IP address.

NOTE Be sure to replace the entire variable (including the angle brackets) with the IP address.

```
# APP Servers used for web sockets - disablereuse needs to be on
  for websockets: https://issues.apache.org/bugzilla/show_
  bug.cgi?id=55890
<Proxy balancer://wscluster>
```

```

</Proxy>

# Background cluster
<Proxy balancer://bgcluster>
    BalancerMember http://<application server IP>:8888
</Proxy>

# Foreground cluster - needs same sticky session as logi
<Proxy balancer://fgcluster>
    BalancerMember http://<application server IP>:8888 route=fg1
</Proxy>

```

3. Save your changes.
4. Restart the Webex WFO Web Server service.

Configuring httpd.conf With Load Balancing

NOTE Do not copy and paste the config examples in this section directly into your config files.

To configure the httpd.conf file with load balancing:

1. On the Web Server, open httpd.conf in a text editor. The file is located at:


```
C:\Program Files\Common Files\Webex WFO\Server\config
```
2. Enable Apache modules that have been commented out of the file by removing the “#” symbol from the beginning of the following three lines:


```
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
```
3. Scroll to the bottom of the file and apply the following changes:
 - a. Add an IP address for each balance member in a cluster.
 - b. The ProxyPass and ProxyPassReverse paths must point to the appropriate cluster defined in Step a. The following is an example, using a sample IP address.

NOTE Some of the lines shown in these examples have had line breaks added (for example, the line beginning `ProxyPass /api/cometd...`). Do not add these line breaks in your file.

```
#SetEnv force-proxy-request-1.0 1
SetEnv proxy-nokeepalive 1
SetEnv proxy-initial-not-pooled 1
RequestHeader unset Expect early
ErrorLog "|bin/rotatelog.exe -l logs/error.%Y-%m-%d.log 86400"
CustomLog "|bin/rotatelog.exe -l logs/access.%Y-%m-%d.log 86400"
    common

# Disablereuse needs to be on for websockets:
    https://issues.apache.org/bugzilla/show_bug.cgi?id=55890
# APP Servers used for web sockets
<Proxy balancer://wscluster>
BalancerMember ws://172.30.0.43:8888 disablereuse=on
BalancerMember ws://172.30.0.44:8888 disablereuse=on

</Proxy>

Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/"
    env=BALANCER_ROUTE_CHANGED
# Comet. Setup for sticky sessions
<Proxy balancer://cometdcluster>
BalancerMember http://172.30.0.43:8888 route=cometd1
BalancerMember http://172.30.0.44:8888 route=cometd2
</Proxy>

# App cluster
<Proxy balancer://appcluster>
BalancerMember http://10.32.3.22:8888 route=cometd1
BalancerMember http://10.32.3.122:8888 route=cometd2
</Proxy>
```

```
ProxyPass /api/websocket balancer://wscluster/api/websocket
ProxyPassReverse /api/websocket balancer://wscluster/api/websocket
ProxyPass /api/cometd balancer://cometdcluster/api/cometd
    stickysession=ROUTEID
ProxyPassReverse /api/cometd balancer://cometdcluster/api/cometd
    stickysession=ROUTEID
ProxyPass /api balancer://appcluster/api
ProxyPassReverse /api balancer://appcluster/api
ProxyPass /highcharts balancer://appcluster/highcharts
ProxyPassReverse /highcharts balancer://appcluster/highcharts
ProxyPass /calendar balancer://appcluster/api/calendar
ProxyPassReverse /calendar balancer://appcluster/api/calendar
ProxyPass /help balancer://appcluster/help
ProxyPassReverse /help balancer://appcluster/help
ProxyPass /server-status !
ProxyPassReverse /server-status !
ProxyPass /advancedreporting
    balancer://advancedreportingcluster/advanced reporting
    stickysession=ROUTEID
ProxyPassReverse /advancedreporting
    balancer://advancedreportingcluster/advanced reporting
    stickysession=ROUTEID
# Add the following to enable load balancer management. You can now
    access it via http://your.server.name/balancer-manager
<Location /balancer-manager>
SetHandler balancer-manager
Order Deny,Allow
Deny from all
Allow from .example.com
</Location>

# Add the following to enable server status page. You can now
    access it via http://your.server.name/server-status
<Location /server-status>
SetHandler server-status
```

```
Order Deny,Allow
Deny from all
Allow from .example.com
</Location>
```

4. Save your changes.
5. Restart the Webex WFO Web Server service.

Configuring the Web Server for Data Explorer

To configure the httpd.conf file for Data Explorer on existing systems:

1. On the Web server, open httpd.conf in a text editor. The file is in the following location.

```
C:\Program Files\Common Files\Webex WFO\config\httpd.conf
```

Scroll to the bottom of the file and apply the following changes:

```
# Forwarding reverse proxy rules for Advanced Reporting
ProxyPreserveHost On
RequestHeader set X-Forwarded-Proto "https"

# Advanced Reporting cluster
<Proxy balancer://advancedreporting>
BalancerMember http://<IP Address for the Data Explorer Application
server>:8080
</Proxy>

# Advanced Reporting (Keycloak) cluster
<Proxy balancer://keycloak>
BalancerMember http://<IP Address for the Data Explorer Application
server>:8090
</Proxy>

# Advanced Reporting (Tenant Provisioning) cluster
<Proxy balancer://tpscluster>
BalancerMember http://<IP address for the Data Explorer Application
server>:2020
```



```
# Advanced Reporting cluster
ProxyPass /advancedreporting
    balancer://advancedreportingcluster/advancedreporting
ProxyPass /advancedreporting keepalive=On
    balancer://advancedreportingcluster/advancedreporting

# Advanced Reporting (Tenant Provisioning) cluster
ProxyPass /provisioning balancer://tpscluster/provisioning
ProxyPassReverse /provisioning keepalive=On
    balancer://tpscluster/provisioning
```

To configure the httpd.conf file for Data Explorer on new systems:

1. On the Web server, open httpd.conf in a text editor. The file is in the following location.

```
C:\Program Files\Common Files\Webex WFO\Server\config\httpd.conf
```

2. Scroll to the bottom of the file and apply the following changes:

```
# Advanced Reporting cluster
<Proxy balancer://advancedreportingcluster>
BalancerMember http://<IP Address for the Data Explorer Application
    server>:8080
</Proxy>

# Advanced Reporting (Keycloak) cluster
<Proxy balancer://keycloakcluster>
BalancerMember http://<IP Address for the Data Explorer Application
    server>:8090
</Proxy>

# Advanced Reporting (Tenant Provisioning) cluster
<Proxy balancer://tpscluster>
BalancerMember http://<IP Address for the Data Explorer Application
    server>:2020
</Proxy>
```

3. Restart the Web Server service.

Configuring the Application Server

After you install the Webex WFO Application Server, you need to perform the following configuration tasks:

- Create a shared folder where media files will be stored that can be accessed by both the Application Server and the Grid Server.
- Download and install FFmpeg
- Configure the system

Sharing a Folder

To share a folder:

1. Locate the folder on the server.
2. Right-click the folder and choose **Properties**. The Properties dialog box appears.
3. Click the **Sharing** tab, and then click **Share**.
4. Select **Everyone** from the drop-down list and click **Add**.
5. Click the Permission Level field associated with Everyone and select **Read/Write**.
6. Click **Share**, and then click **Done**.

Installing FFmpeg

You must install FFmpeg on both the Application Server and the Grid server. If Webex WFO is removed from a server, all FFmpeg files are also removed from the server. When you reinstall Webex WFO, you must reinstall FFmpeg.

NOTE The maximum size of the converted files produced by FFmpeg is 5 GB. Files larger than this size will be truncated.

Webex WFO supports the following versions of FFmpeg. It is recommended that you install the latest available build.

Build Option	Build Selection
Version	2.6.2, 4.0.2
Architecture	Windows 64-bit
Linking	Static

To download and install FFmpeg Version 4.0.2:

1. In a browser, navigate to the following website:

<https://ffmpeg.zeranoe.com/builds/win64/static/>

2. Download and unzip the following build:

`ffmpeg-4.0.2-win64-static.zip`

3. In the unzipped folder, navigate to the following location:

`..\ffmpeg-4.0.2-win64-static\bin`

4. Copy the **ffmpeg.exe** and **ffprobe.exe** files.

5. On the Application Server, navigate to the following folder:

`C:\Program Files\Webex WFO\Server\AppServer\bin`

6. Paste the **ffmpeg.exe** and **ffprobe.exe** files in this folder.

7. On the Grid Server, navigate to the following folder:

`Program Files\Webex WFO\Server\Grid\bin`

8. Paste the **ffmpeg.exe** and **ffprobe.exe** files in this folder.

To verify FFmpeg is correctly installed:

1. Log in to Webex WFO as a system administrator.
2. Navigate to Application Management > Monitoring > Server Status.
3. Click **Check Media Conversion Service Status**.

If FFmpeg is correctly configured, you receive a Success message.

Configuring Webex WFO Connection Settings**To configure Webex WFO connection settings:**

1. Open a browser and enter the host name or IP address of your Web Server. You should be automatically redirected to the System Configuration page at:

`https://<web server IP address>/index.html#/sysConfig`

2. Complete the following fields.

Field	Description
Database Server	Enter the IP address or host name for the SQL database server.
Database Port	(Optional) Enter the port number for the SQL database server.
Database Instance	(Optional) Enter the database instance name of the SQL database server. Leave this field blank if you want to use the default instance.
Database User	<p>Enter the user name of the SQL database user. This name is used by Webex WFO to access the system database and is the SQL database owner. This user must be able to create databases and logins.</p> <p>Each tenant will get a new database login with access to only that tenant's data. This system account will be used for system data.</p>
Database Password	Enter the password for the SQL database user.
Web Server Hostname	<p>Enter the IP address or host name for the Webex WFO web server.</p> <p>This host must be accessible to all desktop recording clients and browsers that use the system. All traffic goes through HTTPS.</p>
System Administrator Username	Enter the email address of the system administrator. The system administrator is the service provider administrator and is responsible for creating tenants and configuring system administration settings in Webex WFO.
Change or Set Password	Click to set or change the system administrator's password.
Password/Confirm Password	Create or reset the user's password here. The password must meet minimum requirements for a Good or Strong password to be saved. See Password Policy for more information.
Password Strength	(Display only) Shows the strength of the password as you enter it in the Password field.
Default Media Storage Location	Enter the Uniform Naming Convention (UNC) path to the default

Field	Description
	<p>media storage location where tenant data, such as recordings and schedules, are stored.</p> <p>EXAMPLE \\10.250.235.85\<<path>\<storage-location></p> <p>NOTE This path must exist for Test Connection to validate successfully.</p>
Test Connection	Click Test Connection to verify the connection settings are correct. Resolve any errors and retry the test until you see a Success message.
Save Configuration	Click Save Configuration to save your changes. The Webex WFO Login page will appear. This button is disabled when you save the configuration settings.

NOTE The service account under which the Application Server runs must have access to the Common Files\Webex WFO folder on the web server.

Configuring the Grid Server

After you install the Webex WFO Grid Server, you must configure it by performing the following tasks:

- Download and install FFmpeg
- Configure Grid Server properties

Installing FFmpeg

If you did not install FFmpeg on the Grid Server at the same time that you installed it on the Application Server, you must now install FFmpeg on the Grid Server. See [Configuring the Application Server](#), “Installing FFmpeg.”

Configuring Grid Server Properties

To configure the Grid Server properties file:

1. Navigate to the following location, and open **grid.properties** in a text editor.

C:\Program Files\Common Files\Webex WFO\Server\config\

2. Locate **grid.executor.thread.count**, remove the pound sign (#) from the beginning of the line, and set the value after the equal sign to one less than the number of CPUs on the Grid Server. For example, if there are five CPUs on the Grid Server, the line would read:

```
grid.executor.thread.count=4
```

The grid will use one less than the number of cores. This setting is only needed in the rare event you want something other than the default, such as when other server types are located on the same machine.

Configuring the Mail Server

After you install the Mail Server, configure the mail server in Webex WFO by logging in as System Administrator. Use the Outgoing Mail Server page (Application Management > System Configuration > Mail Server - Outgoing) to configure the Outgoing Mail server to send system notifications and password resets by email.

To configure the Outgoing Mail server:

1. Complete the fields on the Mail Server - Outgoing page.

The fields on the Outgoing Mail Server page are described below.

Field	Description
Protocol	Choose the protocol used by your mail server. Options are: <ul style="list-style-type: none">■ None — No protocol is used.■ Basic — There is authentication with the provided username and password, but network traffic is not encrypted.■ TLS — (Transport Layer Security) Cryptographic protocol that provides encrypted communications security over a computer network.■ SSL — (Secure Sockets Layer) A deprecated predecessor to TLS that provides encrypted communications security over a computer network.

NOTE Webex WFO v10.3 and higher supports TLS v1.2

Field	Description
	and has deprecated TLS v1.1.
Host Name	Enter the host name or IP address for the mail server.
Host Port	Enter the port number for the mail server.
Username	Enter the user name for the mail server.
Password	Enter the password for the mail server.
From Address	Enter the email address that will be used to send notifications.
Test Connection	Validate the current settings. If there is a problem, a server error message will appear with a description of the problem.

2. Click **Test Connection** to verify that the fields were completed correctly.
3. Click **Save**.

Installing Applied Analytics Features

If you have an Analytics license, Speech Analytics, Text Analytics, and Desktop Analytics features are available after installing Webex WFO. In addition to those features, Analytics includes the following added features that either learn and predict future scoring or analyze transcriptions to determine sentiment.

- Predictive Net Promoter Score
- Predictive Evaluation Score
- Sentiment Analysis (requires Speech Analytics for calls and Text Analytics for email or text contacts)

These additional features in Webex WFO must be set up in a Linux environment. To configure the Linux server, install Ubuntu. See the *Webex WFO Product Compatibility Matrix* for information on the latest support version.

You can install and enable these features using the following procedure. Before installing, download `wfo_ml-<version>.tar` and copy it to the machine running Linux, preferably to the `/opt` directory. Each step detailed below is followed by the command or series of commands to execute that step.

To install one of the Applied Analytics features:

1. Connect to the server using SSH.
2. Acquire root privileges on the Linux server.

```
sudo -Es
```

NOTE The `-E` flag is critical to share local administrator environmental variables with the root user.

3. Mount the UNC path to the `hazelcast.properties` file.

```
apt-get update && apt-get install cifs-utils
```

```
mkdir /mnt/config
```

```
nano /etc/fstab
```

Add an entry with the following at the end of the file:

```
//<Shared Config Storage Server>/<config share name> /mnt/config cifs_
netdev, username=<username>,password=<password>,domain=<domain>
```

Where the following variables are used:

- `<Shared Config Storage Server>/<config share name>` — The resolvable name of the server where the shared folder is located, followed by the path to the shared folder containing the `hazelcast.properties` file.
- `<username>` — A name of a user with read and write permissions to that share directory.
- `<password>` — The password of a user with read and write permissions to that share directory.
- `<domain>` — The user's domain.

Save and then close the file.

4. Navigate to the location where the `.tar` package was placed (preferably `/opt`) and extract the package.

```
tar xvf wfo_ml-<version>.tar
```

5. Change directories where the package was just extracted, and install the Docker images.

```
cd wfo_ml-<version>/wfo_ml
```

```
source wfo-ml-install.sh
```


NOTE This command unzips the Docker and Docker Compose binaries and copies them to /usr/bin folder. For upgrades, this command will be ignored.

6. Change directories to the directory of the additional feature that you want to turn on.

```
cd <version>/wfo_ml_install/<feature directory>
```

The additional features and the names are listed below:

- Predictive Net Promoter Score—wfo_ml_nps/
- Predictive Evaluation Score—wfo_ml_pes/
- Sentiment Analysis—wfo_ml_sentiment/

7. Optional: Update the ENV files. The ENV files are in wfo_ml-<version>/wfo_ml/<feature_name>. Predictive Net Promoter Score (NPS) and Predictive Evaluation Score (PES) features have both a build.yml and an apply.yml file. While Sentiment Analysis has only an apply.yml file. For those features with both, run the docker-compose command for the build.yml file first. Then run the apply.yml file.

The following properties might need to be configured in the ENV file.

- Ports
- The number of processes for each feature and task
- The path to the configuration files (for example, hazelcast.properties)

8. Turn on the broker-worker pairs using the Docker-compose files.

```
docker-compose --f <Docker Compose YML file> up -d
```

EXAMPLE To turn on a broker worker pair that builds Predictive Evaluation Score models run the following command:

```
docker-compose --f docker-compose-pes-build.yml up -d
```

The Applied Analytics features are ready to be configured.

Installing the Transcription Server

To install the Transcription Server, you need the following items:

- Installation and license scripts provided by Cisco Professional Services.

- A server running Linux with either CentOS or Red Hat Enterprise Linux 6.10 or 7.x up to 7.8. For hardware requirements and sizing, see the *Webex WFO Design Guide for On-Premises Deployments*.
- A live internet connection: the Transcription Server uses a dynamic license which requires the server to communicate with the site during operation. If a web proxy prevents standard internet connections, you may need to contact Cisco support for a list of public repository mirrors with CentOS to open them up.
- A username and password (provided to you by Webex WFO Support). You must be logged in as a root user or sudoer.
- Open port 17171 on the Transcription Server.

Use the following procedures to install the Transcription Server. Each step is followed by the command or series of commands to execute that step.

IMPORTANT If you are using Red Hat, you must first run the `cat /etc/os-release` prompt and modify the Version ID line to remove the minor release. For example, change the Version ID line from “7.8” to “7.”

Step 1: Download and Source the Installation Script

1. Put the `install.bash` file on the remote host.
2. On the Linux server, log in with the root account.

```
sudo -s
```
3. Install the Screen utility to save your work in the event of network failure.

```
yum -y install screen
```
4. Make an installation directory.

```
mkdir install
```
5. Access the directory.

```
cd install
```
6. Move the `install` file out of the parent folder.

```
mv ../install.bash ./
```
7. Start a Screen session named “install.”

```
screen -S install
```

- Set the username, password, and authentication token provided by Cisco Support as variables.

```
export username=<username>
export password=<password>
export AUTH_TOKEN=<authentication token>
```

EXAMPLE

The username Webex WFO Support provided is **tenant.admin**, and the password is **Tenant1!**. The authentication token is **1234-abdc-5678-efgh**. You enter the following commands:

```
username=tenant.admin
password=Tenant1!
AUTH_TOKEN=1234-abcd-5678-efgh
```

- Save the username and password as part of an authentication string.

```
export VOICI_REPO_AUTH="$username:$password"
```

- Create a license file. Cisco Support provides the license string.

```
echo [requester] > worker.cfg
echo auth_token = ${AUTH_TOKEN} >> worker.cfg
echo "# ASRWorker=ASRWkr-calabrio-28-<license string>" >> worker.cfg
```

NOTE

To confirm all three lines are properly entered, you can run this command:

```
cat worker.cfg
```

- Pull in the functions of the install file.

```
. install.bash
```

Step 2: Update the Repository and Operating System

- Update the Transcription Server repository.

```
voci_install_repo | tee -a voci_install.log | grep VOICI_
```

- Update the Transcription Server operating system. This process might take several minutes to complete.

```
voci_install_osupdate | tee -a voci_install.log | grep VOICI_
```

3. Reboot.

Step 3: Install the Transcription Server

1. Log in with the root account.

```
sudo -s
```

2. Return to the Screen session.

```
screen -S install
```

3. Access the install folder.

```
cd install/
```

4. Source the install file.

```
. install.bash
```

5. Use the next generation repository.

```
export VOICI_YUM_OPTS="=y --enablerepo voci-asr"
```

6. Install the Transcription Server, the language model, and the call center model. This process might take several minutes to complete.

```
voci_install voci-std-gpu9 voci-langpack-<language pack>_callcenter-sw.x86_64  
| tee -a voci_install.log
```

EXAMPLE

You want to install the North American English language model. You run the following command:

```
voci_install voci-std-gpu9 voci-langpack-eng1_callcenter-sw.86_64 |  
tee -a voci_install.log
```

The table below lists the codes for the available language models.

Language Model	Code
English—Australia	eng2
English—Europe	eng3

Language Model	Code
English—North America	eng1
English—United Kingdom	eng3
French—Canada	fre1
Spanish—Mexico	spa3
Spanish—United States	spa1

- Configure the system.

```
voci_install_config | tee -a voci_install.log | grep VOI_
```

- Start the transcription services.

```
systemctl restart vociserver
```

```
systemctl restart vociwebapi
```

- Verify that the service is active and running.

```
systemctl status vociserver
```

- Add a rule to the firewall to keep port 17171 open permanently.

```
firewall-cmd --permanent --add-port=17171/tcp
```

- Reload the firewall.

```
firewall-cmd --reload
```

- Test that transcription is running. You can run this command at any time to test the system.

```
curl -F file=@/opt/voci/server/examples/sample1.wav -X POST
localhost:17171/transcribe
```

NOTE

If you reboot the transcription server and the `vociserver` and `vociwebapi` services do not start automatically, run the following commands to start these services by default.

```
chkconfig vociserver on
```

```
chkconfig vociwebapi on
```

Configuring the Webex WFO Platform for Transcription

After installing the Transcription Server, you need to modify the transcription.json file so that the Transcription Server connects correctly to the Webex WFO Platform:

Configuring the Transcription.json File

After you install the Webex WFO Transcription Server, you need to configure the transcription.json file with the IP address and port of the servers that are to be used for transcription and those that are to be excluded. The IP addresses can be listed individually or as a range in CIDR notation.

To configure the transcription.json file:

1. Navigate to the shared configuration location set up during the installation of Webex WFO. See [Installing the Webex WFO Platform](#).
2. Open **transcription.json** in a text editor.
3. Edit the “servers” and “exclude” lines as illustrated in the below example.
4. Save and close the file.

NOTE The transcription server is only required if Analytics will be used. If Analytics will not be used, these lines can be commented out.

An example of the two lines in the JSON file is as follows:

```
“voci”:[{“ip” : “10.192.0.40”, “port”:17171},{“ip” : “10.192.0.42/60”,  
“port”:17171}],  
“exclude”:[{“ip” : “10.192.0.43”, “port”:17171},{“ip” : “10.192.0.52/54”,  
“port”:17171}]
```

In this example, the servers to include are:

- 10.192.0.40
- 10.192.0.42 through 10.192.0.60 (indicated in CIDR notation by “10.192.0.42/60”)

The servers to exclude are:

- 10.192.0.43
- 10.192.0.52 through 54 (indicated in CIDR notation by “10.192.0.52/54”)

You must configure at least one server to be included. Configuring servers to exclude occurs when you use a range in the inclusion list and is optional.

Installation

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

Java Memory Usage

If your installation of Webex WFO is encountering performance issues because it is consuming too much memory (for example, the application continues to produce `OutOfMemoryError` messages), you can decrease the maximum heap memory size allocated to Webex WFO and Webex WFO services.

The default `JvmMx` is 4096 MB. Webex WFO has the following `-Xmx` defaults for the following services.

Service	-Xmx Default
Broker	4096 MB
Grid	4096 MB
Compile	2048 MB
Forecast	2048 MB
Scheduler	4096 MB

You can change the default `JvmMx` through the Registry Editor. You can change the default `-Xmx` for the services through their properties files.

To change the default `JvmMx`:

1. Open the Registry Editor.
2. In the Registry Editor, navigate to the following location.

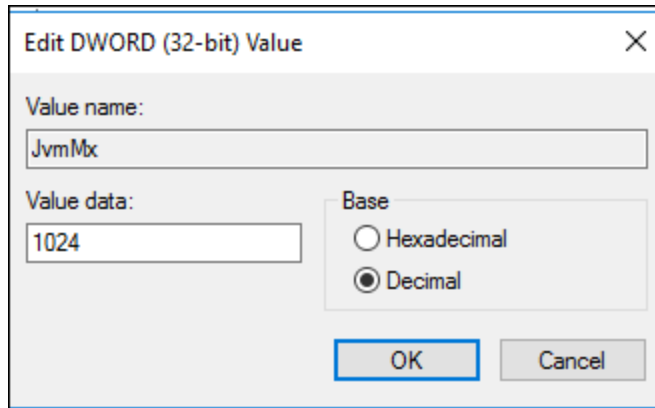
```
HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432NODE > Apache Software Foundation >  
Procrun 2.0 > ciWFOTomcat > Parameters > Java
```

3. Right-click **JvmMx**, and then click **Modify**.
4. In the **Base** section, select the base that you want to use.

5. In the **Value data** field, enter a new value for the maximum heap memory size written in the base that you selected. The unit of this value is megabytes.

EXAMPLE

In the following image, Decimal is selected as the base, and 1024 is entered in the “Value data” field. This means that the new maximum heap memory size is 1024 MB.



6. Click **OK**.

To change the default -Xmx for the Broker, Grid, Compile, Forecast, or Scheduler service:

1. On the server where the service is running, navigate to the location of the service's properties file.

Service	File	Location
Broker	WfoGridBrokerService.properties	C:\Program Files\Common Program Files\Calabrio ONE\Server\config
Grid	WfoGridService.properties	C:\Program Files\Common Program Files\Calabrio ONE\Server\config
Compile	wfocompile.properties	C:\Program Files\Common Program Files\Calabrio ONE\Server\WFM\config
Forecast	wforecast.properties	C:\Program Files\Common Program Files\Calabrio ONE\Server\WFM\config
Scheduler	wfoscheduler.properties	C:\Program Files\Common Program Files\Calabrio ONE\Server\WFM\config

2. Open the properties file with a text editor (for example, Notepad).
3. Locate the following line.

```
# This is a Service4J configuration override file.
# Options defined in this file will be added to the service configuration

# This value specifies additional arguments to be passed to the JVM, such
# as -Xmx512m, etc. Delimited with pipe '|'
# Do not repeat options already included in the default config file.
service4j.jvmOptions=-Xmx<Default>M
```

4. Delete the default value for the maximum heap memory size.

EXAMPLE In the following image, the default value for the maximum heap memory size is represented by the highlighted <Default> variable.

EXAMPLE

```
# This is a Service4J configuration override file.  
# Options defined in this file will be added to the service configuration  
  
# This value specifies additional arguments to be passed to the JVM, such  
# as -Xmx512m, etc. Delimited with pipe '|'   
# Do not repeat options already included in the default config file.  
service4j.jvmOptions=-Xmx<Default>M
```

5. Enter a new value for the maximum heap memory size as a number. Do not change the unit, add spaces, or enter manual line breaks.

EXAMPLE

In the following image, the default value for the maximum heap memory size has been replaced with a new maximum memory pool size of 1024 MB.

```
# This is a Service4J configuration override file.  
# Options defined in this file will be added to the service configuration  
  
# This value specifies additional arguments to be passed to the JVM, such  
# as -Xmx512m, etc. Delimited with pipe '|'   
# Do not repeat options already included in the default config file.  
service4j.jvmOptions=-Xmx1024M
```

6. Save your changes.

NOTE If you receive an “Access is denied” error message when you try to save your changes, run your text editor as the administrator, and then open the properties file with the text editor.

After you save your changes, restart the service.

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

NPCAP 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.

Client Verification Tool

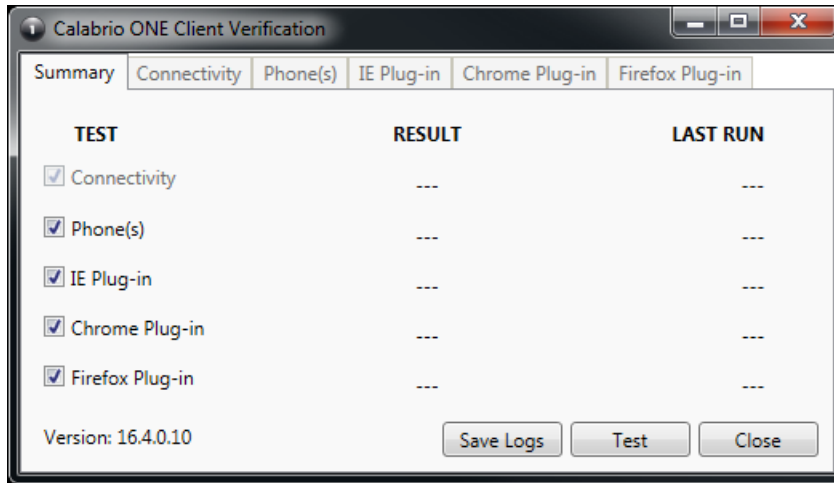
The Client Verification tool tests the client PC to ensure that the connectivity with servers and the phone are suitable for running Smart Desktop. It is installed when Smart Desktop is installed. The tool runs various tests and reports results as either a pass or fail.

To run the Client Verification tool:

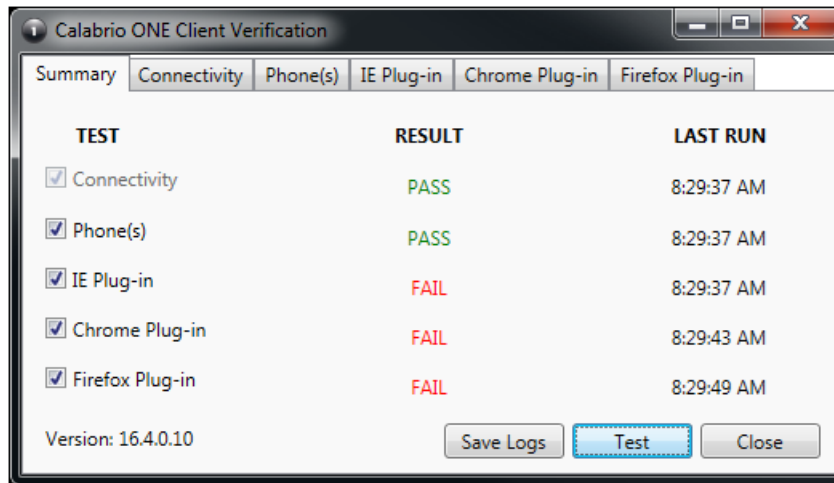
1. After installing Smart Desktop, navigate to the following folder on the client PC:

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

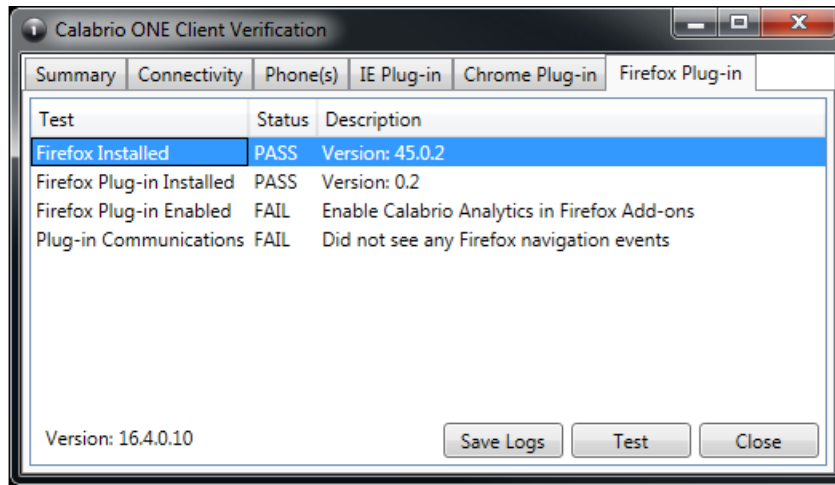
2. Double-click **ClientDiag.exe**. The Client Verification tool starts.



3. By default, all tests are selected. Click **Test**.
4. The tool reports the results of the test as either a pass or fail.



- 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.



- 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.

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.

Return Code	Description
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.
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	Microsoft 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

Return Code	Description
	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 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.

Return Code	Description
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.
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/>.

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.

Installing the Data Server

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.

Prerequisites

The server must have Microsoft Windows Update KB2999226 installed in order to install the Data Server. If the Data Server is installed on the same server as the Webex WFO Platform, you must install it in the Webex WFO Platform installation directory.

NOTE While on Step 3 of [Installing the Webex WFO Platform](#), you decide to use the default installation directory: C:\Program Files\Webex WFO. If you install the Data Server on the same server as Webex WFO, you must also install the Data Server in C:\Program Files\Webex WFO. If you use a different directory (for example, E:\Webex WFO), the installation will fail.

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](#).

Installing the Data Server for a Single Tenant


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

To 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.

To test the Data Server:

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

 **NOTE** This might take a few minutes to complete.

Installing the Data Server for Multiple Tenants

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

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

Install the Base Data Server

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

To install a Base Data Server:

1. In the **Download Base Data Server** section, click the **Webex WFO Data Server** link. This downloads the file CalabrioONEDataServerSetup.exe to your computer.

2. Double-click the executable to start the Data Server Setup Wizard.
3. Follow the instructions in the wizard to complete the installation.

Configure the Base Data Server

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

To configure the base Data Server:

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

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

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

Field	Description
Server Name	Enter a name for the Data Server.
Webex WFO 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.

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	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none">■ 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.

Installing Data Explorer

Webex WFO offers an installer to add Data Explorer.

1. Prerequisites

To install Data Explorer, you need an application server, a database server, and access to certain other items. The following sections describe these requirements.

1a. Hardware Requirements for the Application and Database Servers

While the database and application servers can reside on the same machine, this is not recommended for performance and scalability reasons. They should be on different servers with appropriate connection rules. See [Data Explorer Implementation Sizing](#) to determine the hardware requirements for Data Explorer.

1b. OS Requirements for the Application and Database Servers

The application and database servers need to be running CentOS 7. The installer was developed on CentOS 7 kernel version 3.10.0-693.21.1.el7.x86_64. You can get minimal CentOS 7 ISO images for virtualization software on the CentOS website: <https://www.centos.org/download/>.

The following images have been tested with Data Explorer:

- CentOS-7-x86_64-Minimal-1708.iso
- CentOS-7-x86_64-Minimal-1804.iso
- CentOS-7-x86_64-Minimal-1810.iso

IMPORTANT Do not upgrade CentOS 7 before the installation.

1c. Software Requirements for the Database Server

The required PostgreSQL Version is 9.6. You will need credentials for the database to allow database and user creation.

1d. Software Requirements for the Application Server

To perform some of the pre-installation steps, you will need the following CentOS packages installed on the application server:

- cifs-utils: To support CIFS file system for external mounts
- java: To use Java truststore

You also need to install a text editor such as Vim or Nano.

To install the packages:

1. Connect to the server running CentOS via SSH.
2. Run the following commands to install the packages:

```
yum install cifs-utils
yum install java
```

1e. Software Files for Data Explorer

You will need access to the software files described in the following table.

File	Description
OnPrem-packages-<release version>.tar.gz	Contains all the packages and dependencies for an air-gapped installation of Data Explorer.
OnPrem-images-<release version>.tar.gz	Contains all the images for the services needed for Data Explorer and an image for the local registry.
OnPrem-installer-<release version>.tar.gz	(Optional) Contains the installer code. Also used for updates.
Version	Keeps the version number for the data contribution service.

1f. (Optional) Additional Hosts

An extra host and credentials within the same subnet to support the addition of extra nodes.

BEST PRACTICE If you are using virtualization software, it is recommended that you take a snapshot of the system before attempting to install Data Explorer.

2. Install and Configure PostgreSQL

2a. Install PostgreSQL 9.6

Before continuing, you need to install PostgreSQL 9.6 on the database server. You can download this version of PostgreSQL from <https://postgresql.org>.

2b. Configure the PostgreSQL Host Configuration

On the database server, run the following commands to make it allow connections from Data Explorer.

```
echo kernel.shmmax=17179869184 >> /etc/sysctl.conf
echo kernel.shmall=4194304 >> /etc/sysctl.conf
sysctl -p

export PG_DATA=/var/lib/pgsql/<PostgreSQL version>/data
echo "host all all 0.0.0.0/0 md5" >> ${PG_DATA}/pg_hba.conf
sed -i 's/^\(local.*peer\)$/\1 map=indicee/' ${PG_DATA}/pg_hba.conf
echo "listen_addresses = '*' " >> ${PG_DATA}/postgresql.conf
```



```
echo "indicee postgres indicee" >> ${PG_DATA}/pg_ident.conf
echo "indicee postgres postgres" >> ${PG_DATA}/pg_ident.conf
```

```
systemctl enable postgresql-<PostgreSQL version>.service
systemctl start postgresql-<PostgreSQL version>.service
systemctl status postgresql-<PostgreSQL version>.service
```

```
firewall-cmd --zone=public --add-port=<PostgreSQL port number>/tcp --permanent
firewall-cmd --reload
```

2c. Set PostgreSQL Database Credentials

To set database credentials:

1. Connect to the database VM via SSH if you are performing an upgrade on a database that is still using a database OVA.
2. Change login session owner to the postgres user. (This user's username is "postgres.") Make sure the prompt changes to **bash**:

```
su - postgres
```

3. Connect to the database engine as the PostgreSQL user:

```
psql
```

4. Change the password.

```
\password
```

Set a new password for the postgres user.

IMPORTANT Take note of this password. It must be used during installation.

5. Enter the following commands to leave the database:

```
\q
```

```
exit
```

3. Configure Webex WFO Windows Servers

Before you begin installing Data Explorer services on the Data Explorer platform server, you need to prepare the Webex WFO Windows servers so that Data Explorer can connect to it during the installation process.

3a. Create a Shared Data Contribution Folder

You need to create a shared folder that all Data Explorer and Webex WFO services can access. It is recommended that you place this folder in the same location as the shared media folder that Webex WFO uses.

You need to know the username, password, and domain of an account with read and write permissions to this share. Since all data loaded into the system is copied to this share, it would be best if the share had several gigabytes of available space. It might need more available space depending on the amount of customer data.

3b. Add a Self-Signed Certificate to the Web Server

If you have not already added a self-signed certificate, create one and add it to the Webex WFO Web Server. See [Managing Certificates](#).

NOTE Data Explorer does not support localhost as a deployment option.

3c. Connect the Webex WFO Web Server to the Data Explorer Application Server

You must configure the Webex WFO Web Server to connect to the Data Explorer application server. You can do this by editing the HTTPD configuration file (httpd.conf) on the Web Server.

On the Web Server, open httpd.conf in a text editor. The file is in the following location.

```
C:\Program Files\Common Files\Webex WFO\server\config\
```

Ensure that the following sections exist in the file. If they do not exist, locate the comment that includes the words “#Foreground cluster” and add the following text after that section. Replace “[Application Server IP address]” with the IP address of the Data Explorer Application Server.

NOTE If you are upgrading from an older version of Webex WFO that used Logi, remove sections that reference Logi and add the following sections to the end of the file.

IMPORTANT If you copy text from a PDF version of this document, be aware that indented lines are continuations of the preceding line. Make sure that the indented text is added to the preceding line, with a space added before it. To avoid this issue, access this documentation as HTML help for lines that do not wrap.

```
# Forwarding reverse proxy rules for Advanced Reporting
ProxyPreserveHost On
RequestHeader set X-Forwarded-Proto "https"

# Advanced Reporting cluster
<Proxy balancer://advancedreportingcluster>
BalancerMember http://[Application server IP address]:8080
</Proxy>

# Advanced Reporting (Keycloak) cluster
<Proxy balancer://keycloakcluster>
BalancerMember http://[Application server IP address]:8090
</Proxy>

# Advanced Reporting (Tenant Provisioning) cluster
<Proxy balancer://tpscluster>
BalancerMember http://[Application server IP address]:2020
</Proxy>
```

Locate the section of the configuration file that includes the word “ProxyPass”. Add the following text to the end of the that section.

```
# Advanced Reporting cluster
ProxyPass /advancedreporting
    balancer://advancedreportingcluster/advancedreporting
ProxyPassReverse /advancedreporting keepalive=0n
    balancer://advancedreportingcluster/advancedreporting

# Advanced Reporting (Keycloak) cluster
ProxyPass /auth balancer://keycloakcluster/auth
ProxyPassReverse /auth keepalive=0n balancer://keycloakcluster/auth

# Advanced Reporting (Tenant Provisioning) cluster
ProxyPass /provisioning balancer://tpscluster/provisioning
ProxyPassReverse /provisioning keepalive=0n
    balancer://tpscluster/provisioning
```

After making these changes, save the file and restart the Apache service on the Webex WFO Web server.

NOTE If you are using multiple Webex WFO Web server services, you must restart each Apache service.

4. Install Data Explorer

4a. Transfer the Installer Files to the Application Server

To standardize your Data Explorer environment, it is recommended that you create a directory named `dx` within the `opt` directory and transfer the files to that location.

The location of these files (called the “installation directory for Data Explorer” throughout the rest of this document) is then as follows:

```
/opt/dx
```

4b. Set File Structure

Unpack the **Installer TAR** file and organize the files.

To unpack the TAR file and organize the files:

1. Navigate to the installation directory for Data Explorer (where you placed your software files).
2. Run the following command.

```
tar xfz OnPrem-installer-<release version>.tar.gz --no-same-owner
```

This creates the `onprem-installer` directory within the installation directory for Data Explorer.

3. Move the following files from the installation directory into the `onprem-installer` directory: `OnPrem-packages-<release version>.tar.gz`, `OnPrem-images-<release version>.tar.gz`, and `version`.

```
mv OnPrem-images-<release version>.tar.gz OnPrem-packages-<release
version>.tar.gz version ./onprem-installer/
```

4c. Set Data Contribution Service Storage Location

The Data Contribution Service in Data Explorer saves a copy of all data that is uploaded to the system. This copy might be needed later if the data needs to be reloaded. Since the upgrade path sometimes requires replacing the Data Explorer Application Server, it is important that these data contribution files are stored in a different location. To do this, use the common internet file system (CIFS) to mount the `contribution-data` directory to an external store.

This external source is the shared data contribution folder that you created in [3a. Create a Shared Data Contribution Folder](#).

To set a Data Contribution Service Storage location:

1. Connect to the Data Explorer Application server, and then enter the password for the server.
2. Edit the `FSTAB` file.

```
nano /etc/fstab
```

3. Set a symbolic link to the shared Windows folder on the Linux directory. Add the following line at the bottom of the file (there are spaces before and after `cifs` and between the `<server>/<shared directory>` and the `<installation directory for Data Explorer variables>`):

```
//<server>/<shared directory> <installation directory for Data
Explorer>/onprem-installer/config/contribution-data
cifs _netdev,username=<username>,password=<password>,domain=<domain>
```

In this example, the following variables are used:

- `<server>/<shared data contribution directory>`—The resolvable name of the server where the share is located and the name of the shared directory. Ensure that no other applications write to the shared directory.

- <installation directory for Data Explorer>—The directory where the installation files are located on the application server.
 - <username>—A name of a user with read and write permissions to the shared directory.
 - <password>—The password of a user with read and write permissions to the shared directory.
 - <domain>—The user’s domain.
4. Save and exit the file.
 5. Mount the volume.

```
mount -a
```

NOTE You can confirm that the volume is mounted by typing `mount` and verifying that the volume is listed. If you see a mount error that says, “Host is down,” your Samba version is incorrect. To fix this issue, add “, vers=2.0” to the end of the command in step 3 as seen in the following text:

```
//<server>/<share> <path>/onprem-installer/config/contribution-data  
cifs _netdev,username=<username>,password=<password>,domain=<domain>,  
vers=2.0
```

To test the Data Contribution Service Storage location:

1. Change directories to the Contribution Data directory with the following command.

```
cd ../onprem-installer/config/contribution-data
```
2. Enter the following text to create a file.

```
touch hello
```
3. Confirm you see the file on the shared drive by looking at the shared directory from another machine on the network.

4d. (Data Explorer Version 10.3.9 and earlier) Add Your Self-Signed Certificate to the Trust Store

If you are installing Data Explorer version 10.3.9 and earlier, you must add a self-signed SSL certificate to the Trust Store on the Data Explorer Application server. Make sure that the common name (CN) for your certificate matches your domain, the server name in the HTTPD configuration file on the Webex WFO Web server, and the public host set up on initial install. This CN is case sensitive.

NOTE Data Explorer does not support localhost as a deployment option.

To add an SSL certificate to the Trust Store:

1. Connect to the Data Explorer Application server, and then enter the password for the server.
2. Secure copy (SCP) your Webex WFO certificate to the Data Explorer Application server.
3. Change directories to the /onprem-installer/config/certs/ directory:

```
cd ../onprem-installer/config/certs/
```

4. Place the certificate.

```
keytool -import -alias C1cert -file <cert_file> -keystore truststore_cacerts
```

5. Enter the following password:

```
changeit
```

5. Installing Data Explorer

Once you have unpacked the installer TAR file, you can begin the installation process on the application server.

To install Data Explorer:

1. In the installation directory for Data Explorer, run the following commands:

```
chmod +x *.sh
./menu.sh
```

The installer will pick up the release version from the image file and Data Contribution from the version file and the Data Explorer installer will open the Menu.

2. Enter “1” to select the “Configure and Install Platform” option and complete the prompts.

Prompt	Description
Webex WFO Web server name	If the fully qualified domain name (FQDN) is resolvable, it should be used here. If the FQDN is not resolvable, you must make a DNS server available before continuing to install the application.
DB host	The IP address of the PostgreSQL host.
DB port	The port on which the PostgreSQL is listening for connections.

Prompt	Description
	(Default is 5432.)
Credentials for DB	<p>The postgres user credentials for the database engine, not the database VM. This prompt requires the following credentials. These credentials were set during the PostgreSQL database configuration. See 2c. Set PostgreSQL Database Credentials.</p> <p>Username—For the root user configured on the PostgreSQL database</p> <p>Password—For the root user configured on the PostgreSQL database</p>
Credentials for Keycloak Admin	<p>Must be in email syntax.</p> <p>NOTE These credentials are for the super administrative user for the authentication service. Create a secure password, and store it safely.</p> <p>Username—(Email) For the user with administrator permissions to be configured in Keycloak master realm</p> <p>Password—For the user with administrator permission to be configured in Keycloak master realm</p>

After the initial configuration, the installer should verify the connectivity and proceed with the installation if everything checks out. If an error occurs, no configuration is kept and the installer returns to the main menu.

The installation process includes the following steps:

1. Installing packages
2. Loading Docker images
3. Setting up a Docker registry
4. Pushing images to the registry
5. Starting the services.

The installation might take several minutes to complete. If the installation completes with no errors, you can verify that Data Explorer is running by entering the following address in your browser:

<https://<Calabrio ONE Web server>/advancedreporting>

6. Configure Data Explorer in Webex WFO

6a. Get Credentials for Authorization

Authorization for Data Explorer is handled in Keycloak. The installation process creates and configures a Keycloak client. Once a client has been created and configured, you can identify the Client Secret, which must be entered on the Data Explorer Credentials page. (See “Data Explorer Credentials” in the *System Administrator User Guide*.)

NOTE Once a Keycloak client is created and configured through the installation process, the Client ID is **advanced_reporting_apis**.

To access the Keycloak Console, enter the following URL in your browser’s address bar:

<http://<IP of Data Explorer Application Server>:8090/auth/admin>

Login with the Keycloak credentials.

To locate the Client Secret in the Keycloak Console:

1. Select Clients from navigation pane on the left side of the Keycloak page. The Clients page opens.
2. Click **Edit** beside **advanced_reporting_apis**. The configuration page for that client opens.
3. Select **Installation** to open the Installation tab.
4. Select either format from the **Format Option** drop-down list. A code sample appears beneath the list. The Client Secret is a string that appears in the code.
 - If you chose **Keycloak OIDC JSON** option, the secret will appear in the JSON file as a value following the “**secret**” key.
 - If you choose **Keycloak OIDC JBoss Subsystem XML** option, the secret will appear in the XML file as text within the **credential name=“secret”** tags.

6b. Add Credentials to Webex WFO

After the installation is complete, you need to enter the API credentials in Webex WFO so it can make calls to Data Explorer. This involves retrieving the Client ID and Secret from Keycloak and adding them to Webex WFO. See [Getting Credentials for Authorization](#) to retrieve the Client ID and Secret.

To add credentials to Webex WFO:

1. Log in to Webex WFO as a system administrator.
2. Open the Data Explorer Credentials page from the System Administration section of Application Management.
3. Enter the Client ID.
4. Enter the Client Secret.
5. Click **Save**.

BEST PRACTICE After adding your credentials, verify that the Keycloak integration is working. Using a system administrator account, go to the Tenants page (Application Management > Tenants), and make sure that the Data Explorer Job Statuses section indicates that the integration is working and that the Force Tenant Update check box is available.

6c. Provision the Tenant

To provision the tenant:

1. Log in to Webex WFO as a system administrator.
2. Navigate to Application Management > Tenants.
3. Select **Edit an existing tenant**, and then select the tenant.
4. In the Data Explorer >Reporting Password section, enter and confirm a password.
5. Select **Force update**.
6. Click **Save**.

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" />

Managing Certificates

Webex WFO supports both self-signed and certificate authority (CA) signed certificates. Cisco recommends using CA signed certificates. The steps below pertain to generating signing requests and signing certificates for CA signed certificates. The self-signed certificate is sufficient to encrypt the communication path between the Webex WFO server and the client browsers. However, it has the following limitations:

- Agents see a certificate error or security alert the first time they access Webex WFO.
- User security is not complete. Users are vulnerable to a man-in-the-middle attack (an active form of eavesdropping where private communication is controlled by a hacker).

You can update the certificate so that users are not required to accept self-signed certificates. This prevents the possibility of man-in-the-middle attacks.

IMPORTANT Follow the instructions in this section to replace Webex WFO's provided self-signed certificate with a CA signed certificate in order to maintain HTTPS access.

If you are using the Web server redundancy feature in Webex WFO, you must configure a unique certificate for both the primary and backup Web server.

Certificate Requirements

The following are the minimum requirements for creating a certificate:

- A common name to include the server's FQDN. The common name must be the Webex WFO URL that was configured during installation.
- SAN entries must include the Webex WFO Web URL hostname. Optionally, short names, web server hostnames, and IP addresses can also be included in the SAN.
- 2048-bit key size
- SHA2 algorithm
- Key usage of digital signature and key encipherment
- Enhanced key usage of server authentication

- The Cisco Implementation team must receive the certification in base64 format as a CRT or CER file and the private key of the certificate

Creating an SSL Certificate Signing Request

To create an SSL certificate signing request:

1. Navigate to the folder where the Webex WFO Web server service configuration file is located:

```
C://Program Files/Common Files/Webex WFO/Server/Config
```

2. Back up the `httpd.conf` file, `localhost` public certificate file, and `localhost.key` private key files by copying and saving the files to a preferred location.
3. Download and install OpenSSL for Windows (any version).

BEST PRACTICE It is recommended that you download the latest non-experimental version of OpenSSL Light for Windows from the following link:

<https://slproweb.com/products/Win32OpenSSL.html>

4. Chrome release 58 and newer require subject alternate names (SANs) that you configure for validation and no longer validates by common name only. To resolve this, generate a new certificate with a SAN value. Note that Internet Explorer and Firefox are not affected by this. To configure SAN values, edit the `openssl.cnf` file. Navigate to the following location and open the CNF file in a text editor:

```
..\OpenSSL\bin\openssl.cnf
```

If the `..\OpenSSL\bin` folder does not contain an `openssl.cnf` file, create one using a text editor.

5. Replace the existing file content with the content below. Only update the `[alt_names]` entries, and then run the command.

where:

- `DNS.1 = <ServerHostname_FQDN>` is the server FQDN
- `DNS.2 = <WebServerAlias>` is the web server alias

IMPORTANT You must replace the existing file content with the below text exactly. You cannot alter any text except for the [alt_names] values for DNS.1 and DNS.2. The values for DNS.1 and DNS. 2 must be manually updated before running the certificate signing request command. You only enter your own information in the other response fields during a later step in the procedure.

```
[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
req_extensions = v3_req
x509_extensions = v3_ca

# The extensions to add to a certificate request

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = AU
countryName_min = 2
countryName_max = 2

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Some-State

localityName = Locality Name (eg, city)

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Internet Widgits Pty Ltd

organizationalUnitName = Organizational Unit Name (eg, section)
```

Managing Certificates | Creating an SSL Certificate Signing Request

```
commonName = Common Name (Webex WFO One URL hostname)
```

```
commonName_max = 64
```

```
emailAddress = Email Address
```

```
emailAddress_max = 64
```

```
[ req_attributes ]
```

```
challengePassword = A challenge password
```

```
challengePassword_min = 4
```

```
challengePassword_max = 20
```

```
unstructuredName = An optional company name
```

```
[ v3_req ]
```

```
# Extensions to add to a certificate request
```

```
basicConstraints = CA:FALSE
```

```
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

```
subjectAltName = @alt_names
```

```
[ alt_names ]
```

```
DNS.1 = <ServerHostname_FQDN>
```

```
DNS.2 = <WebServerAlias>
```

6. OpenSSL for Windows tries to use the default OpenSSL configuration file normally used in Linux deployments. This will fail in the Webex WFO environment with the error message, "Unable to load config info from /usr/local/ssl/openssl.cnf." To prevent this, set an environment variable OPENSSL_CONF to point to the correct configuration file. In the command prompt, enter the following:

```
set OPENSSL_CONFIG=<installation path>\bin\openssl.cnf
```


7. Reboot the server for the environment variable change to take effect.
8. Open OpenSSL located in the following folder:

```
..\OpenSSL\bin
```

9. Enter the following command to generate a new private key and a certificate signing request (CSR) for the server certificate, where <ServerNamePrivate> is the private key name and <ServerNameCSR> is the name of your CSR.

```
openssl req -out <ServerNameCSR>.CSR -new -newkey rsa:2048 -nodes -keyout
    <ServerNamePrivate>.key -config openssl.cnf -extensions v3_req
```

10. Enter the requested information in the fields named below to configure the certificate.

- Country Name <2 letter code>
 - See <https://www.digicert.com/ssl-certificate-country-codes.htm> for a list of country codes.
- State or Province Name <full name>
- Locality Name <eg, city>
- Organizational Name <eg, company>
- Organizational Unit Name <eg, section>
- Common Name <Webex WFO URL hostname>
- Email Address

NOTE “Common Name” refers to the name of your Webex WFO URL. Do not use a challenge password or optional company name.

The generated CSR file is located in the ..\OpenSSL\bin folder.

11. Send the ServerNameCSR.CSR file generated to an SSL service provider to get it signed. The certificate authority can be public or private. It must be signed with base64 encoding. Your SSL provider will give you a CER or CRT file.
12. **BEST PRACTICE** Once you receive the signed certificate and key file, store the files to the configuration share path location.
13. Move the key file into the ..\Webex WFO\Server\config folder.
14. Update the SSL certificates for each Web server. See [To update SSL certificates for each Web server](#).

Signing a Private CA Certificate

To sign a certificate when using a private CA:

1. Ensure that your private certificate authority certificate, certificate authority private key, server certificate's CSR, and server certificate's private key are in the `..\OpenSSL\bin` folder.
2. Run the following command.

```
openssl x509 -req -days <1825> -in <ServerNameCSR>.CSR -signkey  
  <ServerNamePrivate>.key -CA <myCA>.pem -CAkey <myCA>.key -out  
  servername.crt -extensions v3_req -extfile openssl.cnf
```

where:

- `<ServerNameCSR>` is the server CSR
- `<ServerNamePrivate>` is the server CA key file name
- `<myCA>.pem` is the CA certification
- `<myCA>.key` is the CA private key file name
- `<1825>` is the number of days until the certificate expires.

The CRT file is the generated certificate.

3. Depending on your version of OpenSSL, you might receive an error message asking for an SRL file. This is a serial file that OpenSSL uses to keep track of certificates. You can add the `<-CAcreateserial>` parameter to the command to generate the SRL file, see below:

```
openssl x509 -req -days 1825 -in ServerNameCSR.CSR -signkey  
  ServerNamePrivate.key -CA myCA.pem -CAkey myCA.key -out servername.crt -  
  extensions v3_req -extfile openssl.cnf <-CAcreateserial>
```

The `<-CAcreateserial>` entry is only needed for the first certificate you sign with your CA. For subsequent certificates, use `<-CAserial>`, where `<-CAserial>` is the name of your generated serial file. This ensures the same serial file is updated with the newly generated certificates. It should adhere to the format below:

```
openssl x509 -req -days 1825 -in ServerNameCSR.CSR -signkey  
  ServerNamePrivate.key -CA myCA.pem -CAkey myCA.key -out servername.crt -  
  extensions v3_req -extfile openssl.cnf <-CAserial> CA.srl
```

The customer is responsible for generating and maintaining SSL certificates. Certificates expire after a period of time and must be maintained. Most public SSL providers do not allow SSL certificates to be generated via IP address or internal domain name. For this, Microsoft AD Certificate Services or a customer's private certificate authority is required.

To update SSL certificates for each Web server:

1. Copy the signed certificate and its private key to the configuration share path.
2. Using administrator credentials, open the `httpd.conf` file located in the `config` folder in a text editor. Search for the line that begins with `<SSLCertificateFile>`. At the `<SSLCertificateFile>` line, replace the existing public certificate folder path, filename, and extension with the SSL certificate file detailed below:

```
C:/Program Files/Common Files/Webex WFO/Server/config/<ServerName>.crt
```

Where `<ServerName>` is the name of the CRT file.

3. Find the line that begins with `<SSLCertificateKeyFile>`. Update the lines to use the new certificate and private key.

```
EXAMPLE SSLCertificateFile "//<configSharePath>/<customer>.crt"  
SSLCertificateKeyFile "//<configSharePath>/<customer>.key"
```

4. Update the `<ServerName>` entry to match the `<CommonName>` entry in the certificate. By default, this is set to `Localhost`. Unless the certificate has a SAN entry for `localhost`, the Web server service will fail to restart.
5. Save and close the file.
6. Restart the Webex WFO Web server service.
7. Repeat steps 1–6 for all Webex WFO servers.

You can now access Webex WFO without receiving the certificate error message. Use either the common name or one of the SAN entries in the URL.

Upgrading from Previous Versions

The Webex WFO Platform supports over-the-top upgrades from previous versions.

Webex WFO components should be upgraded in the following order:

1. Back up your database. See [Backup and Restore](#) for more information.
2. Stop all Webex WFO services.

IMPORTANT You must stop the Application Server, Broker, and Grid Server at the same time for the upgrade to complete successfully.

3. Upgrade Webex WFO services by running CalabrioONEServerSetup.exe.

NOTE If you change the installation directory when you perform an over-the-top upgrade of the Webex WFO Platform, the installation will fail. If you want to change the installation directory, uninstall and then reinstall the Webex WFO Platform.

NOTE If you have mapped custom metadata to the disVdn reconciliation field in your database, you must remap the metadata to a different field.

4. Upgrade the Webex WFO Database by running the [Admin Utility Tool](#).
5. Restart Webex WFO services, beginning with the Broker.
6. Download and upgrade the Data Server.

NOTE If you change the installation directory when you perform an over-the-top upgrade of the Data Server, the installation will fail. If you want to change the installation directory, uninstall and then reinstall the Data Server.

7. Download and upgrade the Smart Desktop on agent PCs.

NOTE

- If you have Thin Smart Desktop 2016.7 or earlier installed on the Thin Client server, it must be removed before you upgrade to the current version of Smart Desktop. Thin Smart Desktop is no longer supported; it has been replaced with the new version of Smart Desktop.

- Auto update of Webex WFO Smart Desktop in Citrix/Terminal environments is not supported. For these installations, new versions of the Webex WFO Smart Desktop must be manually installed on the Citrix/Terminal server.

Upgrading Applied Analytics Features

Upgrading the Predictive Net Promoter Score, Predictive Evaluation Score, and Sentiment Analysis features includes stopping all of the brokers in all of the additional features, turning the Docker containers off, and performing an install of the new version.

To upgrade Analytics additional features:

1. Use a POST call to the /stop endpoint to turn each broker off, so it will stop sending new jobs to the workers. Enter the following command to turn off a broker.

```
curl -X POST http://<IP of Linux server running additional feature>:<feature port>/stop
```

- Sentiment Analysis — Port 40010
- Predictive Evaluation Score — Port 40001
- Predictive Net Promoter Score — Port 40101

NOTE You can find the port number in the ENV file in the feature directory.

Repeat this command for every broker for each of the additional features that are running.

2. Look in the worker log files to verify that the worker is no longer processing a job.

NOTE Worker log files are located at /var/log/ and follow the following file naming format:

```
worker-MLGRID_<FEATURE>  
broker-MLGRID_<FEATURE>.
```

3. Once all the in-progress jobs are complete, turn the docker containers off. Go to each of the feature directories and turn off the broker-worker pairs using the docker-compose file.

```
docker-compose --f <Docker Compose YAML file> down
```

The additional features and names are as follows.

```
cd <version>/wfo_ml_install/<feature directory>
```

- Predictive Net Promoter Score—wfo_ml_nps/
- Predictive Evaluation Score—wfo_ml_pes/
- Sentiment Analysis—wfo_ml_sentiment/

Predictive Net Promoter Score (NPS) and Predictive Evaluation Score (PES) features have both a build.yml and an apply.yml file, while Sentiment Analysis only has an apply.yml file. For those features, run the docker-compose command for the build.yml file first, then the apply.yml file afterwards.

EXAMPLE To turn off a broker-worker pair that builds Predictive Evaluation Score models run the following command:

```
docker-compose --f docker-compose-pes-build.yml down
```

4. Run the following command to verify that everything in the Docker container is down.

```
docker ps
```

There should be no running containers.

5. Install the upgrade. See [Installing Applied Analytics Features](#).

Validating the Installation

After you install and configure the servers, verify that the services are connected.

To verify that the Platform services are connected:

1. From a browser, enter the URL or IP address of the Webex WFO web server hostname you configured during installation.
2. Log in to Webex WFO with system administrator credentials. This is the email and password initially entered on the System Configuration page.
3. Open the Server Status page (Application Management > Monitoring > Server Status).
4. Verify all the service types listed in the Services section have green check marks next to them.

To verify that the Data Servers are connected:

1. From a browser, enter the URL or IP address of the Webex WFO Web Server hostname you configured during installation.
2. Log into Webex WFO with tenant administrator credentials.
3. Navigate to **Data Server Status** (Application Management > Global > Monitoring > Data Server Status).
4. Verify all Data Servers show as Connected.

Removal

The following topics describe how to uninstall Webex WFO components.

Uninstalling Webex WFO

To uninstall Webex WFO you must uninstall the Webex WFO services.

Recordings are not uploaded from agent desktops or servers when you uninstall Webex WFO. They are maintained in the Recordings folder located at

```
..\Program Files\Common Files\Webex WFO\Desktop\recordings
```

on the same drive where you installed the Webex WFO services.

If you did not use the default location, you specify the custom location you used when you installed Webex WFO.

NOTE A user must log in as an administrator in order to remove any Webex WFO applications.

Uninstalling Services

When you uninstall Webex WFO services, the software is completely removed except for the Webex WFO database. The services can be uninstalled in any order.

To uninstall Webex WFO services:

1. Log into the Webex WFO server as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.
3. Select Calabrio ONE Server, right-click Uninstall, and follow the prompts.
4. After the uninstall is completed, you might be prompted to reboot. You are given the option to reboot now or later.

BEST PRACTICE Reboot immediately to complete the uninstallation process.

Removing the Webex WFO Databases

Using the Windows Control Panel on the Webex WFO server to remove services does not remove the Webex WFO database.

IMPORTANT If you intend to reinstall or upgrade Webex WFO, and you want to retain historical data, you must not remove the Webex WFO database.

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.

Uninstalling the Data Server

NOTE You must log in as an administrator in order to uninstall the Data Server.

To uninstall the Data Server:

1. Log into the Data Server as the local machine administrator.
2. Start the Programs and Features utility in Control Panel.
3. Select **Calabrio ONE Smart Data Server**, click **Uninstall**, and follow the prompts. You might be prompted to restart the machine.