Cisco

Webex WFO Cloud-Installationshandbuch

Für Bereitstellungen mit klassisch WFM

Erstveröffentlichung: 10. Juli 2020
Zuletzt aktualisiert: 03. Oktober 2025

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
170 West Tasman
Drive
San Jose, CA 95134-
1706 USA
http://www.cisco.co
m Tel: 408 526-4000
800 553-NETS (6387)
Telefax: 408 527-0882

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE ANGABEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH WURDEN IN DER ANNAHME ZUR VERFÜGUNG GESTELLT, DASS SIE KORREKT SIND. JEDE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG IST JEDOCH AUSGESCHLOSSEN. DIE ALLEINIGE VERANTWORTUNG FÜR DIE ANWENDUNG DER PRODUKTE LIEGT BEI DEN BENUTZERN. DIE SOFTWARELIZENZ UND BESCHRÄNKTE GEWÄHRLEISTUNG FÜR DAS BEILIEGENDE PRODUKT SIND IM INFORMATIONSPAKET FÜR DAS PRODUKT ENTHALTEN UND WERDEN DURCH DIESE BEZUGNAHME IN DIE VORLIEGENDEN BESTIMMUNGEN EINGESCHLOSSEN. WENN SIE DIE SOFTWARELIZENZ ODER BESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN EINEN VERTRETER VON CISCO, UM EINE KOPIE ZU ERHALTEN.

Die Cisco Implementierung der TCP-Headerkomprimierung ist eine Adaption eines Programms, das an der University of California, Berkeley (UCB), als Teil der Public-Domain-Version der UCB für das UNIX-Betriebssystem entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981, Regents of the University of California, USA.

UNGEACHTET ALLER HIERIN ENTHALTENEN GEWÄHRLEISTUNGEN WERDEN ALLE DOKUMENTDATEIEN UND ALLE SOFTWARE DIESER LIEFERANTEN „IM VORLIEGENDEN ZUSTAND” MIT ALLEN FEHLERN GELIEFERT. CISCO UND ALLE ZUVOR GENANNTEN LIEFERANTEN ÜBERNEHMEN KEINERLEI, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIEN, EINSCHLIEßLICH UND OHNE EINSCHRÄNKUNG, DIEJENIGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG ODER DIEJENIGEN, DIE AUS DEM VERLAUF DES HANDELNS, DER VERWENDUNG ODER DES HANDELSBRAUCHS ENTSTEHEN.

UNTER KEINEN UMSTÄNDEN HAFTEN CISCO ODER SEINE ZULIEFERER FÜR JEGLICHE INDIREKTEN, KONKRETEN, ZUFÄLLIGEN ODER FOLGESCHÄDEN, DARUNTER BEISPIELSWEISE ENTGANGENE GEWINNE ODER DATENVERLUSTE, DIE AUS DER VERWENDUNG ODER NICHTVERWENDBARKEIT DIESES HANDBUCHS ERWACHSEN, SELBST FÜR DEN FALL, DASS CISCO ODER SEINE ZULIEFERER AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDEN.

Alle in diesem Dokument verwendeten IP-Adressen (Internet Protocol) und Telefonnummern sind als Beispiele zu verstehen und beziehen sich nicht auf tatsächlich existierende Adressen und Telefonnummern. Die in diesem Dokument enthaltenen Beispiele, Befehlsausgaben, Netzwerktopologie-Diagramme und andere Abbildungen dienen lediglich zur Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

Für gedruckte und kopierte digitale Versionen dieses Dokuments besteht keine Gewährleistung. Die aktuelle Online-Version enthält die neueste Version.

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Adressen und Telefonnummern finden Sie auf der Website Cisco unter www.cisco.com/go/offices.

Cisco und das Cisco-Logo sind Handelsmarken oder eingetragene Marken von Cisco und/oder Tochtergesellschaften in den Vereinigten Staaten und anderen Ländern. Eine Liste der Marken von Cisco finden Sie unter der URL www.cisco.com/go/trademarks. Die genannten Handelsmarken von Drittanbietern sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1721R)

© 2000–2025 Cisco Systems, Inc. Alle Rechte vorbehalten.

Inhalt

Inhalt 3

Einführung 7

Lokalisierung und unterstützte Sprachen 9

Systemkonfiguration 15

Unterstützte Umgebungen 17

Unterstützte Telefone 17

Harte Telefone 17

Unterstützte Codecs 17

Verwenden mehrerer SoftPhones 17

Unterstützte Mobilgeräte 18

Edge-Komponenten 19

Webex WFO Intelligenter Desktop 20

Über Webex WFO Smart Desktop 20

Smart Desktop Client-Konnektivität 21

Anforderungen und Überlegungen zu Smart Desktop 22

Verwendung von Smart Desktop-Ports 24

Smart Desktop-Kontaktmetadaten 26

Smart Desktop Capture-Datenflussdiagramme 27

Smart Desktop testen 30

Smart Desktop verwalten 33

Anwendung "Aufzeichnungssteuerungen" 34

Webex WFO Datenserver 36

Systemvoraussetzungen **39**

Desktop-Hardware 39

Desktop-Software 40

.NET Framework 40

Browser 40

Desktop Analytics-Plug-in/Erweiterung 40

Adobe Acrobat Reader 41

Desktop-Software und Audioaufnahme 41

Aktivieren Sie die Desktop Analytics-Erweiterung in Ihrem Browser 41

Thin Client-Server 42

Installieren des Thin Client-Servers 43

Portnutzung 44

Edge-Komponenten 45

Datenserver-Komponenten 45

Dateiverschlüsselung 50

Kennwortrichtlinie 50

Authentifizierung 51

Plattform-Erfassungsmethoden 51

Unterstützte Erfassungsmethoden nach Plattform 51

Sonus Gateway-Aufzeichnung 55

Installation **75**

Installieren des Datenservers 75

Voraussetzungen 75

Installieren des Datenservers für einen einzelnen Tenant 76

Datenserver für mehrere Besitzer installieren ____ 76

Cisco Unified Call Manager-Benutzer ____ 77

Installieren von Smart Desktop ____ 78

Manuelle Installation ____ 80

Installation mit GPO ____ 80

Installieren Sie Smart Desktop mit den Parametern des unbeaufsichtigten Befehls ____ 81

Replizieren einer Installation mit Desktop-Imaging ____ 81

Rückgabecodes für die Push-Installation ____ 82

Client-Verifizierungstool ____ 83

Steuerelemente für die Aufzeichnung ____ 84

Entfernung ____ 87

Deinstallieren von Webex WFO Smart Desktop ____ 87

Deinstallieren mit GPO ____ 87

Smart Desktop mit den Parametern des unbeaufsichtigten Befehls deinstallieren ____ 88

Einführung

Webex WFO ist eine hochgradig skalierbare, mandantenfähige Workforce-Optimierungsplattform (WFO). Es bietet die Möglichkeit, Anrufaufzeichnungen, Qualitätsmanagement, Workforce Management und Analysen durchzuführen.

In diesem Dokument wird erläutert, wie Sie Webex WFO in einer Cloud-Umgebung installieren.

Lokalisierung und unterstützte Sprachen

Verschiedene Komponenten von Webex WFO unterstützen unterschiedliche Sprachen. Die Sprachunterstützung gilt für die folgenden Elemente:

- Benutzeroberfläche
  - QM, WFM, Analysen und Erkenntnisse
  - Produktinterne Schulungen
- Dokumentation
  - Online-Hilfe
  - PDF Anleitungen
- Analytik
  - Transkription: Sprache-zu-Text und Transkriptionssuche.
  - Transkriptions-Schwärzung: Entfernen Sie personenbezogene Daten aus Transkripten.
  - Interaktionszusammenfassung: Eine Zusammenfassung eines Audiokontakts basierend auf dem Transkript des Kontakts.
  - Phrasentreffer: Identifizierung von vordefinierten Phrasen. Webex WFO identifiziert Ausdruckstreffer basierend auf Sprache-zu-Text-Transkriptionen von Kontakten.
  - Stimmung: Textbasierte Stimmungsanalyse.
  - Vorhersagen: Vorhersagen von Evaluierungsergebnissen und Net Promoter Scores durch maschinelles Lernen.
  - Text: Analysen für Chat, E-Mail, Agentennotizen und Social Media.
  - Trending Topics: Automatische Identifizierung des Kontaktgrundes und Erkennung von aufkommenden Themen.

- Auto QM: Automatische Auswertung von 100% der Kontakte Ihres Unternehmens.
- AI-Tags: Automatisches Anwenden von vordefinierten Labels basierend auf Kontaktzweck und -inhalt.

Komponenten von Webex WFO sind in diesen Sprachen verfügbar.

Sprache	B	Mobil App	Analytik										In-Produkt Ausbildung	
				Transkription Transkription*	Wechselwirkung	Phrase Hits	Vorhersag	Text Analytik	Laufend Themen	Auto QM	Erweitert Gefühl	Künstl iche		
Arabisch (ar-			x		x	x	x		x	x	x	x		
Malaysische Bahasa (ms-MS)			x		x	x	x		x	x	x	x		
Vereinfacht Chinesisch	x						x						Begren	
Traditionelles Chinesisch	x						x						Begren	
Dänisch	x		x		x	x	x		x	x	x	x	Begren	
Niederlän	Begren		x		x	x	x		x	x	x	x	Begren	

Sprache	BENUTZEROBERFLÄCHE	Mobile App	Analytik										In-Produkt Ausbildung	Dokumentation
			Transkription*	Transkription	Interaktio	Phrasentref	Vorhersagen	Textanalyse	Trending Topics	Auto QM	Erweiterte Stimmung	Künstliche Intell		
Englisch (en)	x	x	x		x	x	x	x	x	x	x	x	x	x
Australisches Englisch (en-			x	x	x	x	x	x	x	x	x	x		
Europäisches Englisch (en-			x	x	x	x	x	x	x	x	x	x		
Singapurisches Englisch (en-			x		x	x	x	x	x	x	x	x		
Südafrikanisches Englisch			x	x	x	x	x	x	x	x	x	x		
Englisch (UK) (de-DE)			x	x	x	x	x	x	x	x	x	x		
US-Englisch	x	x	x	x	x	x	x	x	x	x	x	x	x	x

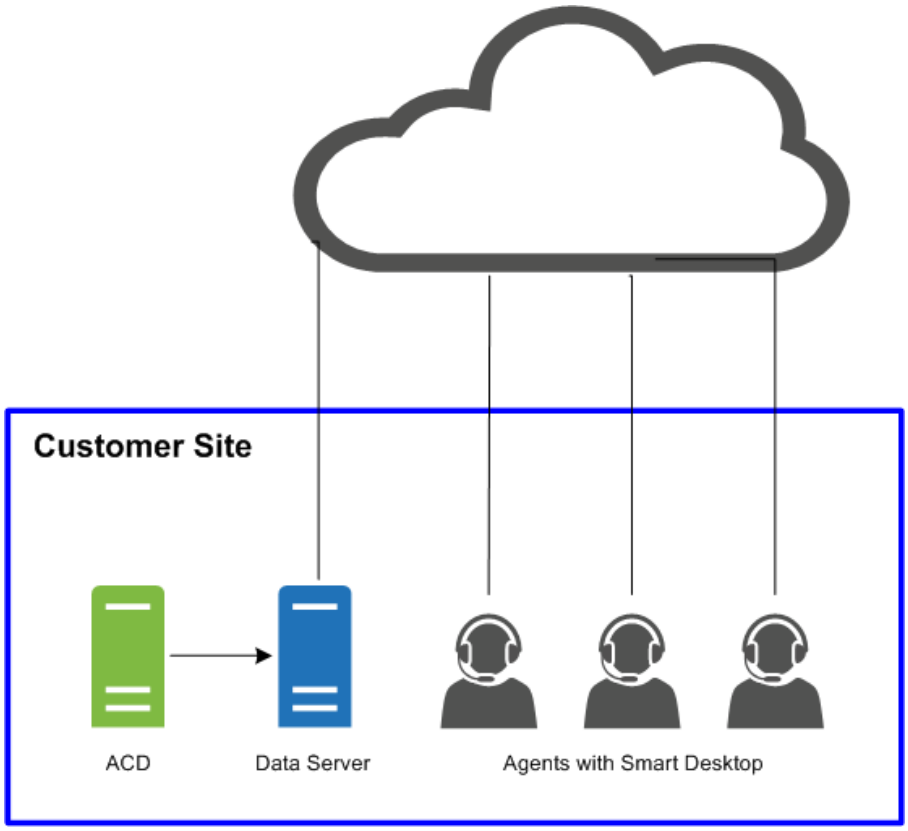
Sprache	BENUTZEROBERFLÄCHE	Mobile App	Analytik										In-Produkt Ausbildung	Dokumentation
			Transkription*	Transkription	Interaktio	Phrasentref	Vorhersagen	Textanalyse	Trending Topics	Auto QM	Erweiterte Stimmung	Künstliche Intell		
(en-US)														
Finnisch (fi)	x		x		x	x	x		x	x	x	x	Begrenzt	
Französisch (fr)	x		x		x	x	x		x	x	x	x	Begrenzt	Begrenzt
Kanadisches Französisch	x		x		x	x	x		x	x	x	x	Begrenzt	Begrenzt
Deutsch (de)	x		x		x	x	x		x	x	x	x	Begrenzt	Begrenzt
Italienisch (it)	x		x		x	x	x		x	x	x	x	Begrenzt	
Japanisch (ja)	x						x						Begrenzt	
Koreanisch (ko)	x						x						Begrenzt	
Norwegisch (nb)	x		x		x	x	x		x	x	x	x	Begrenzt	
Polnisch (pl)	Begrenzt		x		x	x	x		x	x	x	x	Begrenzt	

Sprache	B	Mobil App	Analytik										In-Produkt Ausbildung	
				Transkription Transkription*	Wechselwirkung	Phrase Hits	Vorhersag	Text Analytik	Laufend Themen	Auto QM	Erweitert Gefühl	Künstliche		
Portugiesisch	x		x		x	x	x		x	x	x	x	Begren	
Portugiesisch (Brasilien)	x		x		x	x	x						Begren	
Russisch	Begren						x							
Spanisch	x		x	x	x	x	x		x	x	x	x	Begren	Begren
Mexikanisches Spanisch			x	x	x	x	x		x	x	x	x		
Schwedisch	x		x		x	x	x		x	x	x	x	Begren	

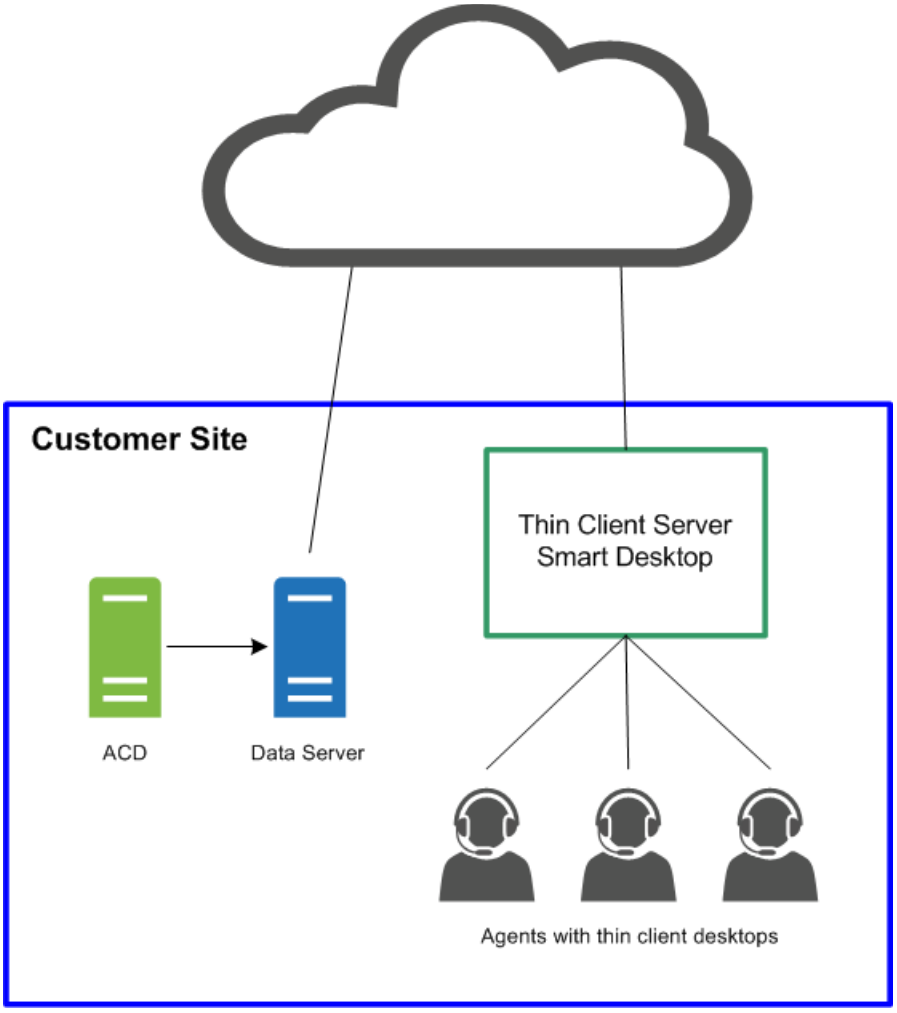
* Einige unterstützte Sprachen erfordern möglicherweise eine zusätzliche Konfiguration für Ihre Webex WFO-Implementierung. Wenden Sie sich an den Support, um sicherzustellen, dass die Sprache, die Sie transkribieren möchten, für Sie konfiguriert ist. Das Hinzufügen weiterer Sprachen oder die Erweiterung des aktuellen Angebots erfordert die Zusammenarbeit mit Cisco. Wenden Sie sich an Ihren Kundenbetreuer, um weitere Informationen zu erhalten.

Systemkonfiguration

Dieses Diagramm zeigt eine typische Webex WFO Cloud-Bereitstellung.



Dieses Diagramm zeigt eine typische Webex WFO Cloudbereitstellung mit einer Thin Client-Umgebung.


Customer Site
Thin Client Server
Smart Desktop
ACD
Data Server
Agents with thin client desktops

Unterstützte Umgebungen

Webex WFO unterstützt eine Reihe von Umgebungen und Technologien.

Für die aktuellsten Informationen zur unterstützten Kompatibilität besuchen Sie www.cisco.com.

Unterstützte Telefone

Webex WFO unterstützt die folgenden Telefone.

Festnetztelefone

Eine Liste der unterstützten Cisco-Handys finden Sie auf der Webseite Unified CM Silent Monitoring/Recording Supported Device Matrix.

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

Unterstützte Codecs

Webex WFO unterstützt die folgenden Codecs:

- g711
- g722
- g729

HINWEIS Die Codec-Paketgröße muss mindestens 20 ms betragen, um eine brauchbare Audioqualität zu gewährleisten.

Verwendung mehrerer Softphones

Wenn Sie mehrere Softphones gleichzeitig verwenden, dürfen die Softphones nicht an eine lokale Portnummer gebunden werden, die mit einer der auf der Seite „globale Einstellungen“ konfigurierten Portnummern übereinstimmt (Anwendungsverwaltung > QM Konfiguration > globale Einstellungen > SIP Einstellungen). Wenn beispielsweise die Portnummer unter
Wenn die Einstellungen SIP auf 5060 gesetzt sind, kann keines Ihrer Softphones einen lokalen Port verwenden, der an die Portnummer 5060 gebunden ist, wenn Sie beabsichtigen, mehrere Softphones gleichzeitig zu verwenden.

Starten Sie das Softphone, melden Sie sich gegebenenfalls an und verwenden Sie dann eines dieser Tools, um die Netzwerkverbindungen für diesen Prozess anzuzeigen ID. Wenn eine der Netzwerkverbindungen einen lokalen Port anzeigt, der mit einer der auf der Seite „globale Einstellungen“ konfigurierten

Portnummern übereinstimmt, müssen Sie eine der folgenden Maßnahmen ergreifen:

- Verwenden Sie ausschließlich das Softphone, und zwar ohne gleichzeitige Nutzung anderer Softphones.
- Konfigurieren Sie das Softphone so, dass es keinen der aufgeführten Ports verwendet.

Um die Portnutzung zu überprüfen, verwenden Sie ein Tool, das Netzwerkverbindungen überwacht, wie z. B. netstat (in der Befehlszeile verwenden Sie die Parameter -anob), TCPView oder CurrPorts.

Unterstützte Mobilgeräte

Agenten können auf eine eingeschränkte Version von Webex WFO auf einem mobilen Gerät wie einem Smartphone oder Tablet zugreifen, indem sie die URL Webex WFO in den Browser des Geräts eingeben. Der Agent wird automatisch auf eine mobile Version von Webex WFO weitergeleitet, wo er sich wie gewohnt einloggt.

HINWEIS Das Mobilgerät muss auf das Netzwerk zugreifen können, in dem Webex WFO installiert ist.

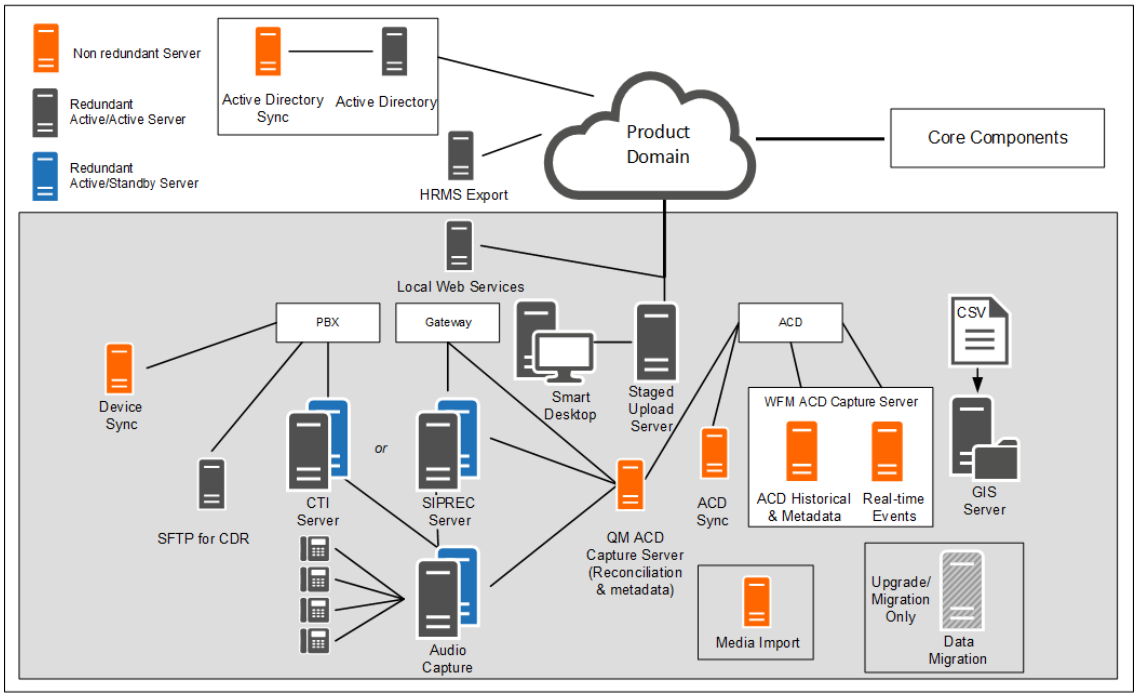
Agenten können ihre Arbeitszeiten auch außerhalb der Arbeitszeit über einen E-Mail-Client oder eine Kalenderanwendung auf einem Mobilgerät oder PC einsehen. Der E-Mail-Client oder die Kalenderanwendung zeigt den Zeitplan so an, wie er in der Webex WFO-Schnittstelle erscheint, indem er die iCalendar-Datendatei vom WFM iCalendar-Dienst liest.

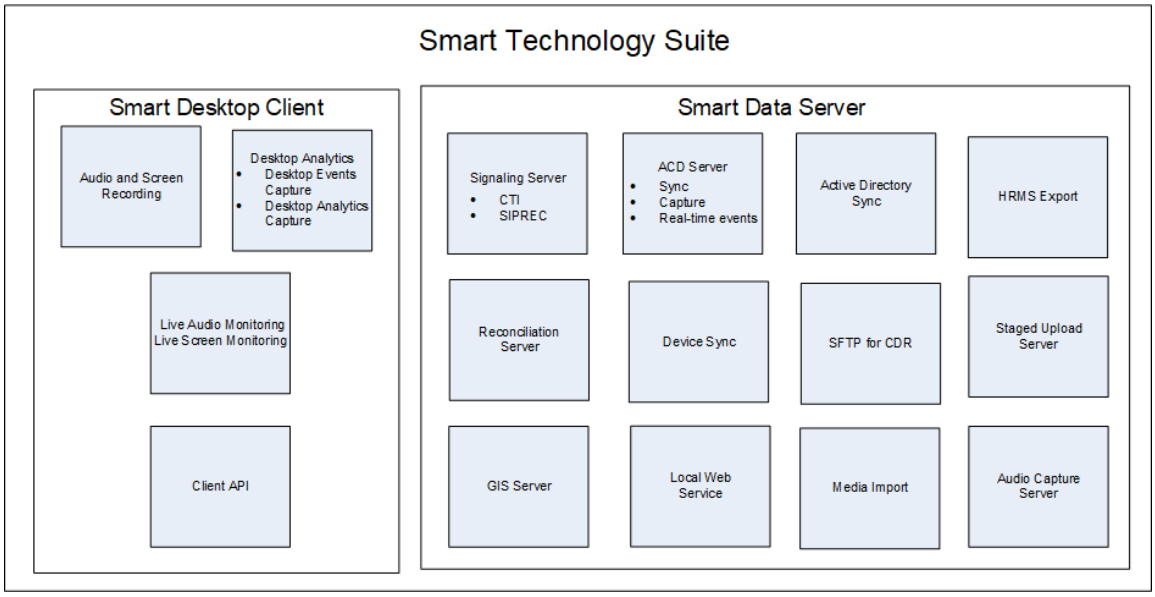
Folgende Clients und Geräte werden für die Anzeige eines Zeitplans außerhalb der Arbeitszeit unterstützt:

- Apple-Geräte wie ein iPhone oder ein iPad (in Verbindung mit der Apple Kalender-App)
- Microsoft Outlook
- Android Geräte wie Tablets oder Smartphones (in Verbindung mit einer Kalender-App, die .ics-Dateien lesen kann)

Edge-Komponenten

Die Webex WFO Edge-Komponenten werden im Allgemeinen bei einem Kunden vor Ort oder an einem entfernten Standort eingesetzt. Die Komponenten als Ganzes bilden die Webex WFO Smart Technology Suite.





Webex WFO Smart Desktop

Webex WFO Smart Desktop erfasst alle Benutzerdaten (d. h. Audioaufzeichnung, Bildschirmaufzeichnung, Desktop-Aktivität und Anrufmetadaten) auf dem Desktop eines Agenten. Webex WFO Smart Desktop wird auf den Agenten-Desktops im Contact Center oder auf einem Server installiert, auf dem ein unterstützter Thin Client gehostet wird. Der Smart Desktop Installer muss von der Seite Webex WFO Application Management > Administration > Downloads heruntergeladen werden.

Über Webex WFO Smart Desktop

Die von Smart Desktop erfassten Daten können je nach Ihrer Lizenz und den in Webex WFO aktivierten Berechtigungen variieren. Sie müssen das Smart Desktop-Installationsprogramm von Anwendungsverwaltung > Global > Administration > Downloads herunterladen (siehe Smart Desktop herunterladen). Sie benötigen außerdem die Desktop Analytics-Erweiterung für Ihren Browser.

Die Audioaufnahme mit Smart Desktop hängt von den Aufnahmetypen ab. Contact Center as a Service (CCaaS)-Lösungen zeichnen Audio auf und senden die Datei nach Abschluss des Kontakts. Kundengehostete Lösungen senden die Protokolle SIP und RTP, weil die Verbindung aktiv ist. Webex WFO führt Bildschirmaufnahmen mit Agent Desktop durch und die Aufnahmen werden nach Beendigung eines Anrufs hochgeladen.

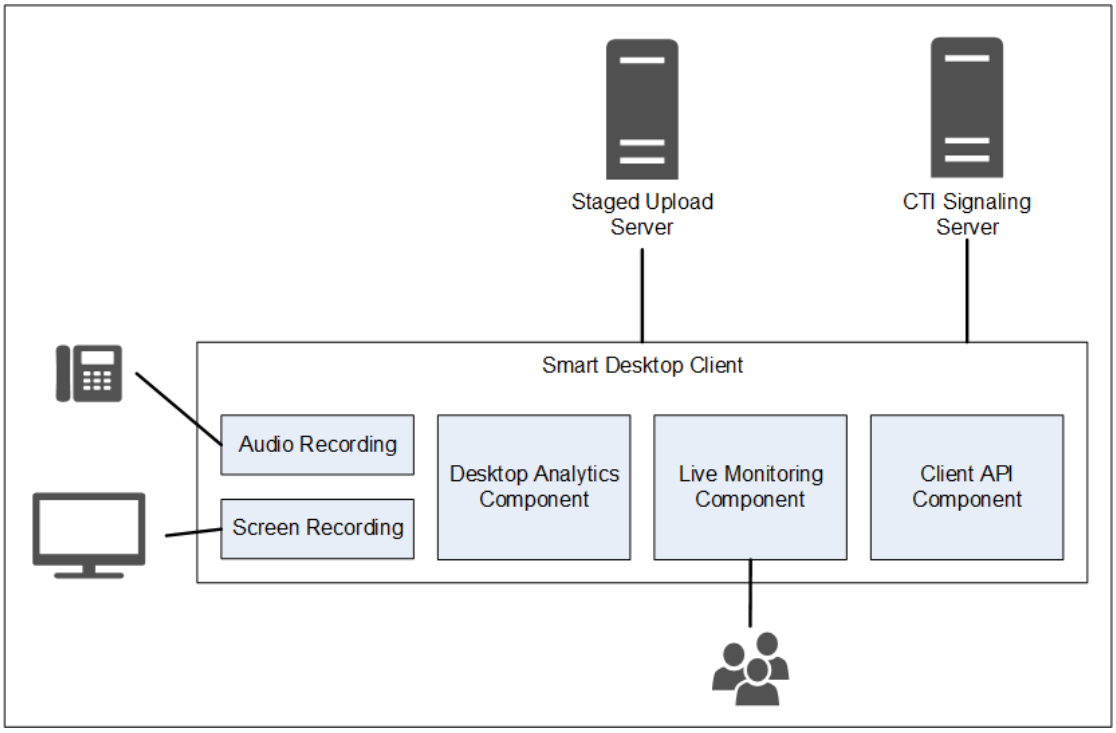
Smart Desktop besteht aus folgenden Komponenten.

- Audio- und Bildschirmaufzeichnung – Diese Komponente zeichnet Agentengespräche auf.
- Desktop Analytics – Diese Komponente liefert Analysedaten zu Agent Desktop-Aufzeichnungen.

- Live-Audioüberwachung und Live-Bildschirmüberwachung – Diese Komponenten ermöglichen es Vorgesetzten, den Ton eines Agenten zu hören und den Bildschirm eines Agenten in Echtzeit zu sehen. Agentenüberwachung und Desktopüberwachung sind die beiden Überwachungsarten für Smart Desktop.

  Agentenüberwachung – Eine Funktion für Administratoren und Vorgesetzte, die es ihnen ermöglicht, Audio und Bildschirme der Agenten in Echtzeit zu überwachen.

  Desktop-Überwachung – Eine Funktion, mit der Administratoren die aktiven und installierten Versionen von Smart Desktop auf den PCs der Benutzer einsehen, Protokollierungsstufen festlegen und Protokolle zur Fehlerbehebung remote herunterladen können.



Smart Desktop Client-Konnektivität

Die folgende Tabelle listet die grundlegenden Verbindungen zum Smart Desktop Client auf:

Komponente	Verbindet sich mit	Eingänge/Ausgänge
Audio- und Bildschirmaufnahme	PC des Agenten	Telefon-Audio- und Bildschirmdaten
Desktop-Analyse	PC des Agenten	Telefon-Audio- und Bildschirmdaten
Live-Überwachung	PCs anderer Agenten	Audio- und Bildschirmdaten anderer Agenten

Verbindung mit Server herstellen	Eingänge/Ausgänge
Gestaffelter Upload	Kontaktinformationen (Audio- und Bildschirmaufzeichnungen

und Metadaten) Verwenden Sie die nachstehenden Links, um zu den verschiedenen Smart

Desktop-Themen in diesem Dokument zu navigieren.

- Anforderungen und Überlegungen zu Smart Desktop
- Desktop-Hardware
- Verwendung von Smart Desktop-Ports
- Smart Desktop-Kontaktmetadaten
- Smart Desktop Capture-Datenflussdiagramme
- Installieren von Smart Desktop
- Aktivieren Sie die Desktop Analytics-Erweiterung in Ihrem Browser
- Smart Desktop testen
- Smart Desktop verwalten
- Anwendung "Aufzeichnungssteuerungen"

Anforderungen und Überlegungen zu Smart Desktop

Weitere Informationen und Überlegungen zur Verwendung eines Thin Client-Servers und Smart Desktop finden Sie unter Thin Client-Server .

In der Webex WFO Produktkompatibilitätsmatrix finden Sie Informationen zu unterstützten Windows-Desktop-Betriebssystemen und unterstützten Webbrowsern.

Bandbreite und Größenanpassung für Desktop-Aufnahmen

- Desktop-Audioaufnahme: 0,5 MB/min
- Screenshot: 1,5 MB/min pro Monitor

BEISPIEL Wenn ein Agent dreißig Anrufe pro Tag mit einer durchschnittlichen Gesprächszeit von 5 Minuten pro Anruf entgegennimmt, würde die Desktop-Audioaufzeichnungsberechnung wie folgt lauten: 0,5 MB/Min. x 5 Minuten x 30 Anrufe = 75 MB.
Wenn der Agent über drei Bildschirme verfügt, sieht die Aufzeichnung eines Screenshots wie folgt aus: 1,5 MB/Min. x 5 Minuten x 30 Anrufe x 3 Bildschirme = 675 MB.

Unter Desktophardware finden Sie Informationen zu spezifischen Anforderungen an Netzwerkkarte, Speicherplatz,

CPU, Arbeitsspeicher und .NET Framework.

Umgebungen

Die folgenden Umgebungen werden zusätzlich zu Computern unterstützt, die die Mindestanforderungen des Betriebssystems erfüllen.

- Virtual Desktop Infrastructure (VDI)
- Terminalserver
- Citrix
- Umgebung des Drittanbieter-Agents
- AWS-Arbeitsbereich

HINWEIS Wenn Ihr Unternehmen VDIs, Terminalserver oder Citrix-Lösungen verwendet, teilen Sie Ihrem Cisco-Kundenbetreuer während des Installationsvorgangs die folgenden Informationen mit: Nachdem ein Kontakt beendet wurde, wird die Anzahl der Computer, die Anzahl der Server und allgemeine Spezifikationen zu Ihren Servern angezeigt.
Terminalserver und Citrix-Lösungen unterstützen die Auto-Update-Funktion von Webex WFO nicht.

.NET Framework

Webex WFO Smart Desktop erfordert .NET Framework 4.5 für Webex WFO Analytics-Features. Wenn .NET Framework nicht installiert ist, kann Webex WFO keine Browserereignisse als Teil der Desktop Analytics-Daten erfassen. Sie können .NET Framework von http://www.microsoft.com/en-us/download/details.aspx?ID=30653 herunterladen.

Ausschlüsse von Antivirus-Echtzeit-Scans

Cisco empfiehlt, die folgenden Cisco-Verzeichnisse von Antiviren-Echtzeitscans auszuschließen, um sicherzustellen, dass die Smart Desktop-Funktionen wie erwartet ausgeführt werden.

- 64-Bit – C:\Program Files (x86)\Calabrio ONE\Desktop*
- 64-Bit – C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop*
- 32-Bit – C:\Program Files\Calabrio ONE\Desktop*
- 32-Bit – C:\Program Files\Common Files\Calabrio ONE\Desktop*

Anforderungen an die Firewall

Webex WFO muss auf die Whitelist gesetzt werden und Zugriff über die externe Firewall Ihrer Organisation erhalten.

Überlegungen zu Webbrowsern

Jeder Browser, den Sie verwenden, muss Dateidownloads zulassen. Popup-Blocker müssen deaktiviert werden.

Browser-Plugins

Weitere Informationen finden Sie unter "Desktop Analytics-Plug-in/-Erweiterung" in den Systemanforderungen . Cisco empfiehlt, dass Sie Ihre Erweiterungen/Plug-Ins über Windows GPO verwalten, um sicherzustellen, dass alle abhängigen Features wie vorgesehen funktionieren.

Wenn Benutzer sowohl über Microsoft Edge- als auch über Google Chrome-Browser verfügen, empfiehlt Cisco, die Browsererweiterung in beiden Browsern zu installieren. Die Installation in einem Browser führt dazu, dass Webex WFO keine Daten aus dem anderen Browser sammeln kann, der nicht über die Erweiterung verfügt.

WICHTIG: Sie müssen ältere Browserversionen deinstallieren, bevor Sie die neueste Version installieren.

Stellvertreter

- Smart Desktop ist Proxy-fähig. Es wird versucht, einen erkannten Proxy zu verwenden.
- Wenn ein Internet-Proxy verwendet wird, erfordert Smart Desktop, dass der Proxy sichere Web-Socket-Verbindungen unterstützt.
- Alle Proxy-Verbindungen müssen es der Smart Desktop-Software ermöglichen, eine Verbindung zur Cisco Cloud auf Port 80/443 herzustellen.

Verwendung von Smart Desktop-Ports

Die Portinformationen für Webex WFO Smart Desktop-Komponenten sind unten aufgeführt.

Im Allgemeinen müssen Port 80 und Port 443 zu einem Webserver geöffnet sein, um eine Verbindung zu Webex WFO für alle Cloud-Integrationen mit Webex WFO herzustellen. Die genauen Portanforderungen variieren je nach Cloud-Bereitstellungsmodell.

Vom Kunden gehostete Lösungen

In der folgenden Tabelle finden Sie Informationen zu vom Kunden gehosteten Lösungen. Beispiele für vom Kunden gehostete Lösungen sind Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Express, Avaya Communication Manager und mehr.

Port	Ge	Quelle	Ziel
Intelligenter Desktop			

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
TCP 80, 443	Live-Audioüberwachung (WebRTC)	Audio Gefangennahme Server* PC des Agenten	Supervisor Browser	
UDP 39500 – 43500	Aufnahme RTP	Telefon Voice Tor**	Audio Gefangennahme Server	
UDP 49152 – 65535	Live-Audioüberwachung (RTP)	Audio Gefangennahme Server* PC des Agenten	Supervisor Browser	
TCP 52102	Signalisierung wird aufgezeichnet	Audio Gefangennahme Server* PC des Agenten	Signalisierung Server	

*Netzwerk-Recording-Architektur

**Gateway-Aufzeichnungsarchitektur

CCaaS-Lösungen

In der folgenden Tabelle finden Sie CCaaS-Lösungen (Contact Center as a Service).

Port	Ge	Quelle	Ziel
Intelligenter Desktop			
TCP 80, 443	Live-Bildschirmüberwachung Agenten	PC	Browser des Supervisors

Wolken-STUN/TURN

In der folgenden Tabelle finden Sie Cloud STUN/TURN-Ports.

Port	Gebrauchen	Verbindungen
Intelligenter Desktop		
TCP 80, 443	Per Websocket	Signalisierungsserver
TCP 6379	STUN/TURN Administration über den Systemadministrator in Webex WFO.	Konfiguration
UDP 49152 – 65535	Medien (Audio und Video)	SRTP (Peer-to-Peer)
UDP 49152 – 65535	Medien (Audio und Video)	SRTP (nicht Peer-to-Peer)
UDP/TCP 3478	-	IP Adressenerkennung

Smart Desktop-Kontaktmetadaten

In der folgenden Tabelle sind die verfügbaren Smart Desktop-Kontaktmetadaten aufgeführt, die für jeden Erfassungsmodus verwendet werden:

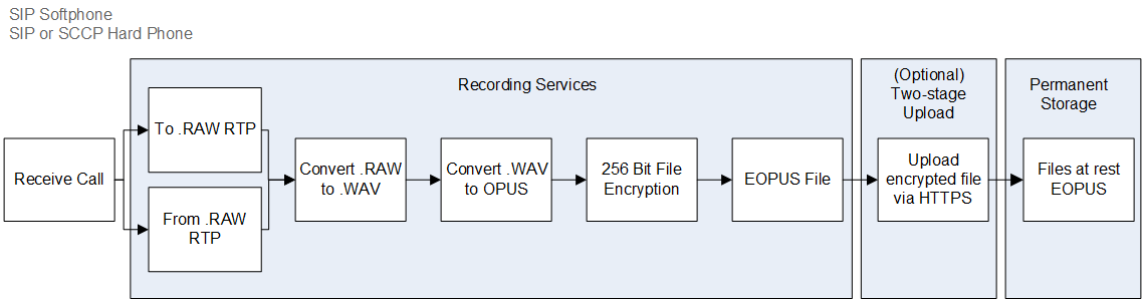
Kontakt-Metadaten	SIP Signalisierung	SCCP Signalisierung	RTP Protokollierung
Anruf-ID	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC API
ANI (Anruf)	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC API
DNIS (angerufen)	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC API
Leitung/Nebenstelle			Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC API
Anrufrichtung	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen

Kontakt-Metadaten	SIP Signalisierung	SCCP Signalisierung	RTP Protokollierung
Zugehöriger Kontakt ID	X		Verlassen Sie sich auf Drittanbieter, um DCC Echtzeitdaten zur Verfügung zu stellen API
Aufzeichnungstyp	X	X	X
Dauer	X	X	Segmentbasiert, es sei denn, join_start wird verwendet
MAC-Adresse	X	X	
Benutzer (mit Windows Login ID)	X	X	X
Datum/Uhrzeit des Anrufs	X	X	X

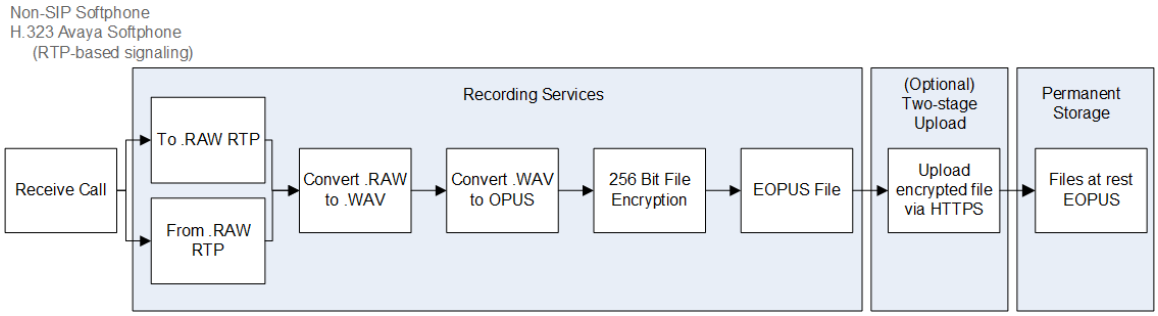
Smart Desktop Capture-Datenflussdiagramme

Dieses Thema enthält Diagramme, die den Smart Desktop-Datenfluss beschreiben.

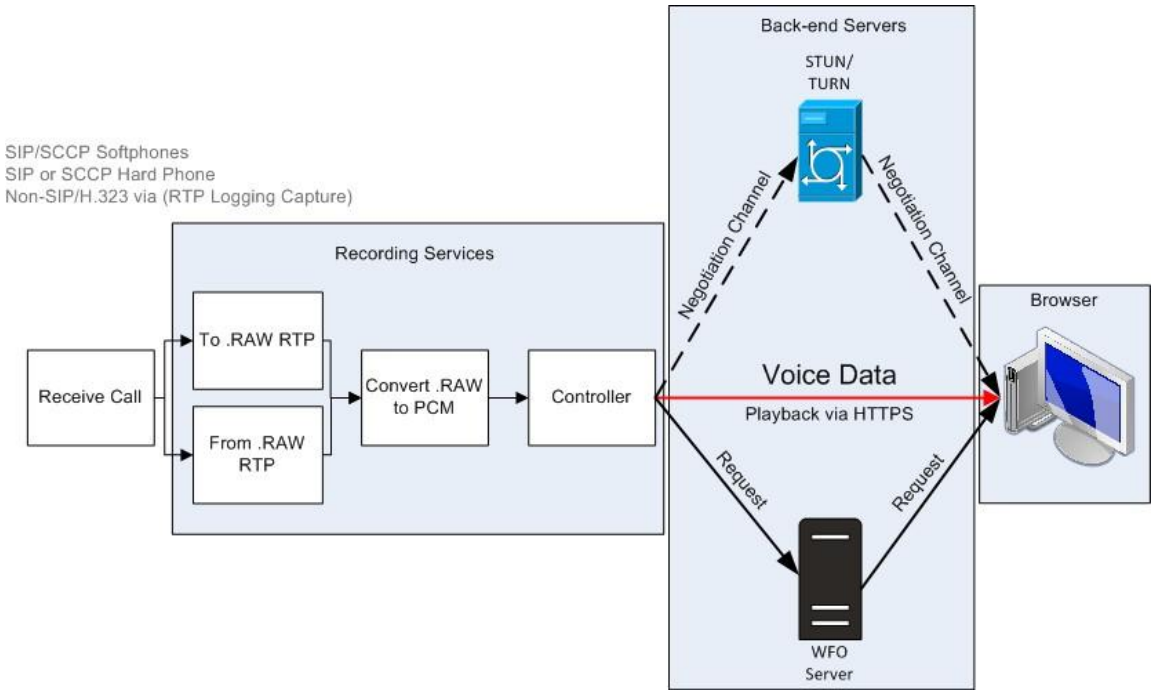
Smart Desktop SIP/SCCP Signalisierung



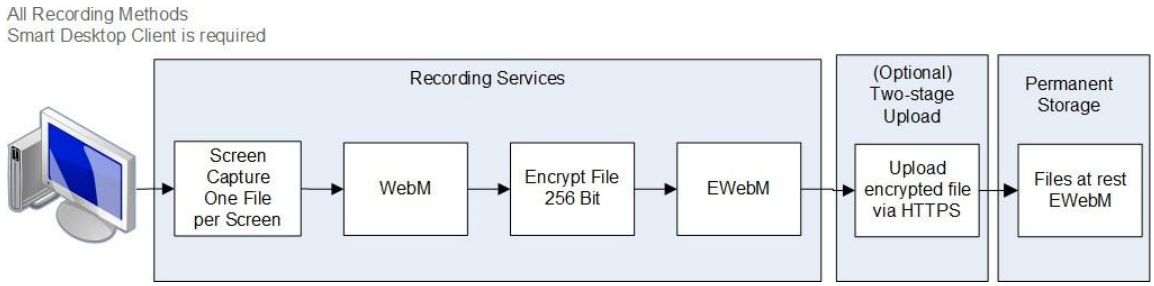
Smart Desktop RTP Protokollierung



Smart Desktop Live-Audioüberwachung

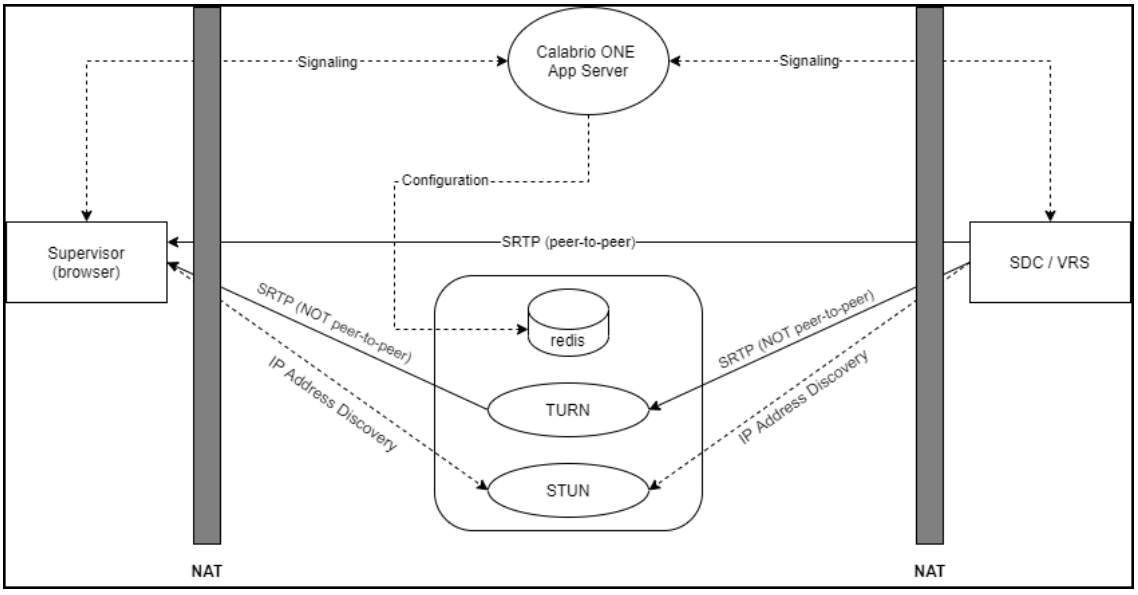


Smart Desktop Live-Bildschirmüberwachung



HINWEIS Die Smartdesktop-Bildschirm- und Audioaufzeichnung verwendet AES 256-Bit-Verschlüsselung, wenn die Aufzeichnung innerhalb von Webex WFO stattfindet.

Smart Desktop Live Monitor-Verbindungen



Verbindung	Anschlüsse	Protokoll	Anmerkungen
Signalisierung	80, 443	TCP	Per Websocket
Konfiguration	6379	TCP	STUN/TURN-Verwaltung mit einer Systemadministratorrolle in Webex WFO
SRTP (Peer-to-Peer)	49152–65535	UDP	Audio- und Bildmedien

Verbindung	Anschlüsse	Protokoll	Anmerkungen
SRTP (nicht Peer-to-Peer)	49152–65535	UDP	Audio- und Bildmedien
IP Adressenerkennung	3478	UDP und TCP	—

Smart Desktop testen

Führen Sie nach der Installation von Smart Desktop (siehe Installieren von Smart Desktop) und der Desktopanalyse (siehe Aktivieren der Desktop Analytics-Erweiterung in Ihrem Browser) die folgenden Schritte aus, um sicherzustellen, dass Ihre Smart Desktop-Implementierung ordnungsgemäß funktioniert.

Voraussetzungen

- Die Windows-Anmeldung (Anwendungsverwaltung> Benutzerkonfiguration > Benutzer **) muss das Format [**Domäne\WindowsNTID**]** haben. Wenn Sie die Windows-Anmeldung nach der Installation von Smart Desktop hinzufügen, müssen Sie Smart Desktop oder seine Desktop-Dienste neu starten.
- Dem Agenten sind die folgenden Berechtigungen zugewiesen: Berechtigungen befinden sich unter Anwendungsverwaltung > Benutzerkonfiguration > Rollen **.**
  - Capture Desktop Analytics
  - Kontakte erfassen
  - Bildschirm aufzeichnen
  - Stimme aufzeichnen
  - Live-Bildschirmüberwachung
  - Live-Audioüberwachung
  - Auf Anforderung aufzeichnen (RTP Signalisierung)
  - Desktop-Ereignisse erfassen

  HINWEIS CCaaS-Lösungen (Contact Center as a Service) unterstützen keine Live-Audioüberwachung.
- Die Erweiterung "Desktop Analytics" wird in Ihrem Browser ausgeführt.

Prozeduren

Stellen Sie sicher, dass auf Ihrem Computer die richtigen Prozesse ausgeführt werden

1. Öffnen Sie **den Task-Manager**.
2. Bestätigen Sie die Prozesse , die DesktopRecordServer und DesktopRecordProcess im **Task-Manager** ausführen. Wenn DesktopRecordProcess nicht ausgeführt wird, stellen Sie sicher, dass Sie die Windows-Anmeldung korrekt eingegeben haben, wie in den Voraussetzungen beschrieben.

3. Überprüfen Sie, ob ciSaasDesktopRecord im **Task-Manager** ausgeführt wird.

4. Öffnen Sie die **Services-App** auf Ihrem Computer und überprüfen Sie, ob der Calabrio ONE Smart Desktop Record Service ausgeführt wird.

Stellen Sie sicher, dass Webex WFO Ihren Computer erkennt

Navigieren Sie zu **Anwendungsverwaltung** > **Global** > **Überwachung** > **Desktop-Überwachung**. Wenn Sie einen grünen Kreis unter der Statusspalte sehen, bedeutet dies, dass Sie verbunden sind und die installierte Version von Smart Desktop die aktive Version ist.

Stellen Sie sicher, dass Webex WFO Agenten erkennt, die Smart Desktop verwenden

1. Navigieren Sie zu **Anwendungsverwaltung** > **Global** > **Überwachung** > **Agentenüberwachung**.
2. Sie können den Bildschirm eines Agenten überwachen, wenn das Symbol für die Bildschirmüberwachung des Agenten schwarz ist. Wenn das Symbol schwarz ist, wird der Smart Desktop Client des Agenten auf seinem PC mit den entsprechenden Berechtigungen ausgeführt.
3. Sie können die Audioüberwachung eines Agenten überwachen, wenn das Symbol für die Audioüberwachung Ist schwarz. Ist das Symbol schwarz, ist der Agent für die Desktop-Aufzeichnung konfiguriert, der Smart Client wird auf seinem PC mit den richtigen Berechtigungen ausgeführt, er ist für die Serveraufzeichnung konfiguriert und der Agent wird auf der Seite "Gerätezuordnungen" einem überwachten Gerät zugewiesen.

4. Klicken Sie auf das Symbol für die Bildschirmüberwachung des Agenten, um das Fenster "Live-Bildschirmüberwachung" zu öffnen.

5. Klicken Sie im Fenster "Live-Bildschirmüberwachung" auf " **Bildschirm** ", um die Überwachungssitzung zu starten. Klicken Sie auf **Audio**

   , um den Anruf des Agenten zu überwachen. Die Audiowiedergabe ist nur möglich, wenn der Agent sich in einem aktiven Gespräch befindet.

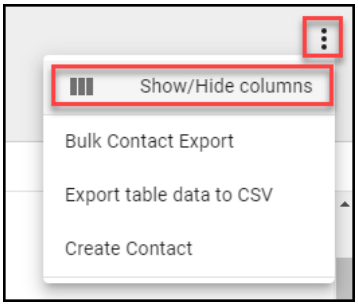
Führen Sie einen Testanruf durch

1. Sie tätigen einen Anruf vom Desktop eines Agenten aus.
2. Klicken Sie in Webex WFO auf **Interaktionen**.
3. Vergewissern Sie sich, dass Sie die Aufzeichnung des Anrufs finden können.
4. Doppelklicken Sie auf die Aufzeichnung, um den Anruf und ggf. die Bildschirmaufzeichnung wiederzugeben.

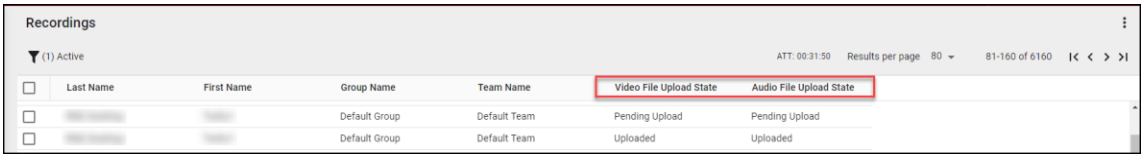
   Wenn das Bedienfeld "Bildschirmaufzeichnung" nicht angezeigt wird oder leer ist, überprüfen Sie, ob der Popup-Blocker im Browser deaktiviert ist.

Überprüfen des Upload-Status von mit Video und Audio aufgezeichneten Kontakten

1. Navigieren Sie zu **Interaktionen**.
2. Klicken Sie auf das **Symbol "Listenoptionen** " in der oberen rechten Ecke der Seite.
3. Klicken Sie auf **Spalten ein-/ausblenden**. Das Fenster Spalten ein-/ausblenden wird angezeigt.



4. Klicken Sie auf "Upload-Status von **Audiodateien" und** "Upload-Status **von Videodateien",**
   wenn diese unter "Ausgeblendet" **aufgeführt**sind.
5. Klicken Sie auf **Übernehmen**. Jetzt können Sie leicht sehen, ob Video- und Audiodateien hochgeladen wurden oder erfolgreich hochgeladen wurden.



6. Doppelklicken Sie auf einen Kontakt, um die Audio- und Bildschirmaufzeichnungen anzuzeigen, die mit dem Anruf verbunden sind.

Smart Desktop verwalten

Cisco empfiehlt, Smart Desktop vierteljährlich zu aktualisieren. Webex WFO unterstützt einen unterbrechungsfreien Aktualisierungsvorgang.

Unabhängig davon, ob Sie sich für eine automatische Aktualisierung oder für vom Kunden verwaltete Aktualisierungen entscheiden, werden Aktualisierungen automatisch und ohne Unterbrechung von Aufzeichnungen oder Kontakten ausgeführt. Sowohl die vorhandene Version als auch die aktualisierte Version von Smart Desktop werden parallel ausgeführt, bis ein Windows-Anmeldevorgang stattfindet. Die Desktop-Überwachung ermöglicht es Administratoren, die aktiven und installierten Versionen von Smart Desktop auf ihren PCs anzuzeigen, Protokollierungsebenen festzulegen und Protokolle zur Fehlerbehebung aus der Ferne herunterzuladen.

BEST PRACTICE Administratoren sollten sich mit der Desktop-Überwachung vertraut machen, um den Status und die Versionen von Smart Desktop in Ihrem Unternehmen zu überprüfen.

Automatische Aktualisierung

Webex WFO verfügt über eine automatische Aktualisierungsfunktion, die jederzeit aktiviert oder deaktiviert werden kann, indem Sie zu **Anwendungsverwaltung** > **Verwaltung** > **Globale Einstellungen** navigieren. Aktivieren oder deaktivieren Sie auf der Seite "allgemeine Einstellungen" die **Schaltfläche "Automatische Clientaktualisierung** aktivieren", um die automatische Aktualisierungsfunktion zu aktivieren oder zu deaktivieren.

Wenn diese Option aktiviert ist und sich ein Benutzer bei einem Computer anmeldet, auf dem Smart Desktop ausgeführt wird, prüft der Computer, ob ein neues Update zum Download verfügbar ist.

Vom Kunden verwaltetes Update

Sie können Updates mit einem verwalteten Software-Push (z. B. GPO oder LANDesk) per Push übertragen.

BEST PRACTICE Die Richtlinie Ihres Unternehmens sollte vorschreiben, dass sich Agenten am Ende ihrer Schicht von ihrem PC abmelden müssen. Dieser Vorgang kann mithilfe der GPO-Einstellungen automatisiert werden.

Best Practices für das Hochladen von Aufzeichnungen auf Webex WFO

Wenn Sie Audio- und Bildschirmaufzeichnungen so schnell wie möglich vom Desktop eines Benutzers abrufen, stellen Sie sicher, dass die Aufzeichnungen nach der Aufzeichnung des Anrufs wiedergegeben werden können. Es gibt Optionen, um die Aufzeichnungen sofort oder zu einem festgelegten Zeitpunkt vom Desktop des Benutzers zu entfernen. Die Entscheidung, wann Aufzeichnungen hochgeladen werden sollen, ist eine Zusammenarbeit zwischen Geschäfts- und IT-Mitarbeitern unter Berücksichtigung der Anforderungen an die Audio- und Bildschirmzugänglichkeit, die Bandbreite und den Speicherplatz des Kontos. Cisco empfiehlt die unten aufgeführten Upload-Prozesse.

- Sofortiges Hochladen mit QM-Workflows – Mit diesem Vorgang wird sichergestellt, dass die

Aufzeichnung nach der Aufzeichnung des Anrufs für die Wiedergabe zur Verfügung steht und der Speicherplatz auf dem Agenten-PC nicht übermäßig belegt wird. Cisco empfiehlt, Aufzeichnungen so zu konfigurieren, dass sie sofort vom PC des Agenten auf

Webex WFO, wenn WAN und LAN-Bandbreite ausreichend sind. Auf der **Seite "Workflow-Verwaltung** " in **der Anwendungsverwaltung** können Sie sofortige Uploads durchführen.

- Verzögerter Upload mithilfe von QM-Workflows: Sie können diesen Vorgang so konfigurieren, dass er außerhalb der Geschäftszeiten stattfindet. Audio- und/oder Bildschirmaufzeichnungen werden zu einem bestimmten Zeitpunkt hochgeladen. Nachdem Ihre Aufzeichnungen hochgeladen wurden, können Sie sie bei Bedarf herunterladen. Auf der Seite "Workflow-Verwaltung **" in** der **Anwendungsverwaltung** können Sie verzögerte Uploads durchführen.
- Sofortiger Upload mit den regionalen Einstellungen für gestaffelten Upload des Webex WFO-Datenservers: Wenn die Internetbandbreite ein Problem darstellt, kann ein Ansatz mit gestaffeltem Upload den externen WAN-Datenverkehr während der Geschäftszeiten verringern. Für diese Option müssen Sie die Einstellungen für den gestaffelten Upload des Cisco Datenservers konfigurieren (weitere Informationen finden Sie unter Konfigurieren des Datenservers und Konfigurieren des gestaffelten Uploads). Auf diese Weise wird sichergestellt, dass Anrufe tagsüber von einem PC in den lokalen Speicher verschoben werden. Nach Feierabend werden die Aufzeichnungen zu einem bestimmten Zeitpunkt hochgeladen. Nachdem Ihre Aufzeichnungen hochgeladen wurden, können Sie sie bei Bedarf herunterladen. Konfigurieren Sie auf der Seite "Datenserverkonfiguration" in der Anwendungsverwaltung die Option "Einstellungen für gestaffelte Uploads für regionale Datenserver", um gestaffelte Uploads auszuführen.

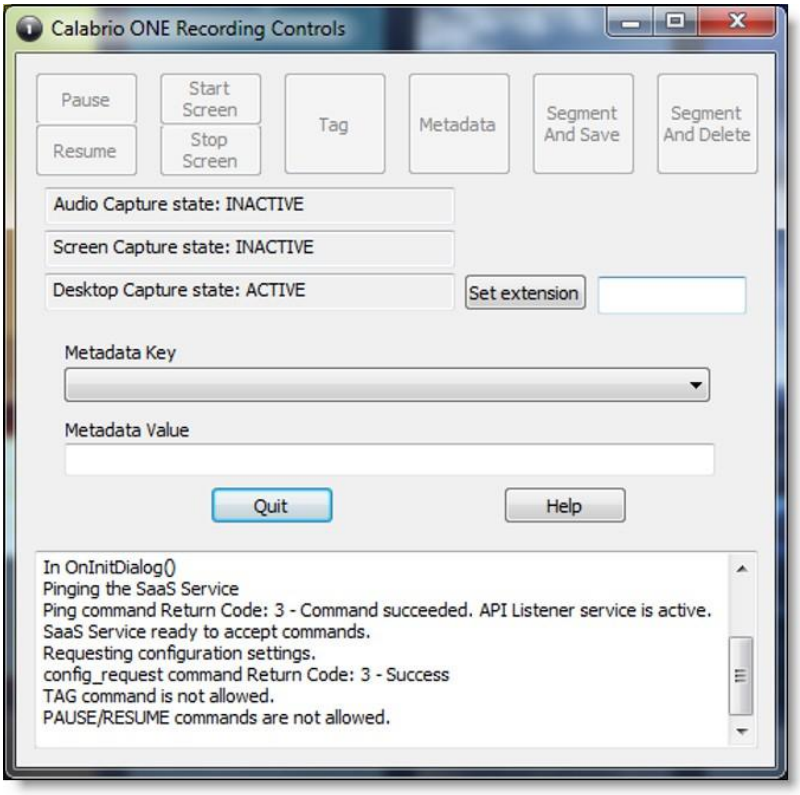
Anwendung "Aufzeichnungssteuerungen"

Webex WFO Recording Controls ist eine eigenständige Webanwendung, mit der Sie Audio-, Bildschirm- und Tastenanschlagaufzeichnungen für aktive Anrufe starten, anhalten, fortsetzen und beenden können. Sie können Anrufe auch mit Tags versehen und ihnen Metadaten hinzufügen.

Um Recording Controls zu starten, wählen Sie **Calabrio ONE Recording Controls** aus dem Start-Menü. Um die Aufzeichnungssteuerung zu schließen, klicken Sie auf " **Beenden**".

Agenten können die Smart Desktop Recording Controls application, auch bekannt als Desktop Capture and Controller (DCC)-Anwendung, verwenden, um Aufzeichnungen und Insert Metadaten von ihren Desktops aus zu steuern. Die Anwendung "Aufzeichnungssteuerung" wird mit Smart Desktop installiert. Es wird in der Programmliste unter Cisco auf dem Desktop des Agenten angezeigt, nachdem Smart Desktop installiert wurde.

Die Anwendung "Aufzeichnungssteuerung" ist unten dargestellt:



Die richtigen Rollen und Berechtigungen müssen Agenten von einem Tenant-Administrator zugewiesen werden, damit Agenten die Anwendung "Aufzeichnungssteuerung" verwenden können.

Mit der Anwendung "Aufzeichnungssteuerung" können Benutzer folgende Aufgaben ausführen:

- Markieren eines aktiven Anrufs oder der neuesten Anrufaufzeichnung
- Anrufe aufzeichnen
- Audioaufnahme anhalten und fortsetzen
- Aufzeichnung eines Anrufs starten
- Zuvor aufgezeichnete Audiodaten und den Bildschirm für einen Anruf verwerfen
- Die Aufzeichnung des aktiven Anrufs löschen. Sobald ein Anruf beendet wurde, können Sie die Aufzeichnung nicht mehr löschen.
- Für Hoteling-Aufzeichnung an- oder abmelden
- Hinzufügen von Metadaten zu einem aktiven Anruf oder zum letzten Anruf
- Audio- und Bildschirmaufzeichnung eines aktiven Anrufs starten oder anhalten
- Bildschirmaufzeichnung starten oder stoppen

Die Anwendung "Aufzeichnungssteuerung" unterstützt die folgenden Aufzeichnungstypen:

- Desktopaufzeichnung
- Netzwerkaufzeichnung

Weitere Informationen zu DCC-Befehlen finden Sie unter "Recording Controls API" im *Referenzhandbuch* API.

Webex WFO Datenserver

Der Webex WFO Datenserver ist für Funktionen wie die ACD Synchronisierung und gestaffelte Uploads zuständig. Ein Mandantenadministrator kann den Datenserver für einen einzelnen Mandanten installieren, oder ein Systemadministrator kann einen Basisdatenserver installieren und ihn als gemeinsam genutzten Datenserver für mehrere Mandanten konfigurieren.

HINWEIS Wenn der Datenserver eine Verbindung über einen Webproxy herstellen muss, müssen alle Webex WFO-Dienste, die darauf ausgeführt werden, als Windows-Anmeldekonten mit Proxyeinstellungen ausgeführt werden. Bei der Konfiguration des Datenservers mit einem Proxyserver muss der Datenserverdienst so konfiguriert sein, dass er als lokaler Administrator ausgeführt wird. Webex WFO unterstützt nicht die Verwendung von PAC-Skripts zur Herstellung einer Verbindung mit dem Internet.

Mit der Data Server-Software werden folgende Dienste installiert.

- CTI Signalisierungsdienst
- Datenserver
- Datenserver-Webdienste
- Netzwerkaufzeichnungsservice
- SIPREC Service

In Webex WFO sind die folgenden Funktionen des Datenservers, ihre Beschreibungen und der Dienst, an dem sie ausgerichtet sind, aufgeführt.

- Regional Data Server ACD Sync Settings (Synchronisierungseinstellungen für regionale Datenserver) – Wird verwendet, um Benutzer- und Teaminformationen von einem unterstützten ACD (Webex WFO Data Server) zu synchronisieren.
- Recording Capture Server Settings (Aufzeichnungserfassungsserver-Einstellungen): Wird für Audioaufzeichnungsumgebungen mit Edge-Servern oder Gateways (SBC) verwendet. Der primäre Signalisierungsdienst (CTI oder SIPREC) weist Anrufe den Erfassungsservern in einem Roundrobin-Algorithmus (Webex WFO Network Recording Service) zu.
- Speicherort der GIS-Datei des regionalen Datenservers – Wird verwendet, um Metadaten externer Kontakte aus einer CSV-Datei in Webex WFO (Webex WFO Data Server) zu importieren.

- Aufzeichnungs-SIPREC-Signalservereinstellungen – Wird verwendet, um Start- und Stoppereignisse zu verfolgen und Metadaten für Anrufaufzeichnungen zu erfassen. Ein SIPREC-Signalisierungsdienst wird für Edge-Gateway-Aufzeichnungsumgebungen (Session Border Controller) verwendet (Webex WFO SIPREC Service).
- Recording CTI Signaling Server Settings (Aufzeichnungsserver-Einstellungen): Wird verwendet, um Start- und Stoppereignisse zu verfolgen und Metadaten für Anrufaufzeichnungen zu erfassen. Ein CTI-Signalisierungsdienst wird für Edgeserver-Aufzeichnungsumgebungen verwendet (Webex WFO CTI Signaling Service).
- Gestaffelte Upload-Einstellungen für regionale Datenserver – Wird verwendet, um Kontaktdaten lokal von Smart Desktop-Benutzern zu sammeln und die Dateien regelmäßig auf die Webex WFO-Komponenten in der Cloud hochzuladen (Webex WFO Datenserver).
- Regional Data Server ACD Capture Settings (Erfassungseinstellungen) – Wird verwendet, um benutzerdefinierte Metadaten zu erfassen und Anrufe abzugleichen, die über ein Gateway (Webex WFO Datenserver) empfangen wurden.
- Regionale Datenserver-Echtzeit-Ereigniseinstellungen – Verwendet zum Erfassen von Verlaufs- und Echtzeit-ACD-Daten für WFM- und ACD-Metadaten, die als benutzerdefinierte Metadaten an Anrufkontakte angehängt werden (Webex WFO Datenserver).
- Regionale Datenserver-Abstimmungseinstellungen – Der Abgleich ist ein Prozess, bei dem Gateway-Stammaufzeichnungen mit begrenzten Anrufdaten mit zusätzlichen Anrufdaten verbunden werden, die dem richtigen Agenten (Webex WFO Datenserver) zugeordnet sind.
- Active Directory Sync – Ermöglicht Webex WFO den Abgleich und die Synchronisierung von Webex WFO Benutzern mit Active Directory Benutzern (Webex WFO Data Server).
- Einstellungen für die Gerätesynchronisierung des Datenservers – Ermöglicht die Synchronisierung von Geräten über den Datenserver. Diese Geräte können dann über die Seite "Gerätezuordnungen" in der Anwendungsverwaltung (Webex WFO Datenserver) Benutzern, Aufzeichnungsgruppen und Aufzeichnungstypen zugeordnet werden.
- Lokale Webdiensteinstellungen – Aktiviert die API-Integration auf diesem Datenserver. Wenn diese Option aktiviert ist, können Sie Folgendes aktivieren:
    - Cisco IP Phone Services Controls – Ermöglicht Cisco-fähige Aufzeichnungssteuerungen von unterstützten Cisco-Geräten.
    - Simplified Recording Controls API – Ermöglicht die Verwendung der nativen Datenserverauthentifizierung für Cisco Aufzeichnungssteuerelemente.
- HRMS-Konfiguration – Ermöglicht dem Datenserver den Export von Daten in ein Human Resource Management System (HRMS) (SFTP Datenserver).
- TURN Konfiguration – Ermöglicht Ihnen die Konfiguration Ihres SFTP Servers (Webex WFO Datenservers).

- Einstellungen für den Medienimportserver – Aktiviert den Import von Aufnahmedateien von einem externen Speicherort (Webex WFO Datenserver).

Systemvoraussetzungen

In den folgenden Abschnitten werden die Mindestsystemanforderungen für Webex

WFO aufgeführt. Für die aktuellsten Informationen zur unterstützten

Kompatibilität besuchen Sie www.cisco.com.

Desktop-Hardware

Die Hardwareanforderungen für Webex WFO-Desktops sind wie folgt:

Desktop-Hardware	
NIC	100-Mbit-Netzwerkkarte Netzwerkkarten müssen den Promiscuous-Modus unterstützen. Konfigurieren Sie die Windows-Energieeinstellungen so, dass die Option "Computer darf dieses Gerät ausschalten, um Energie zu sparen" für die Netzwerkschnittstellenkarten deaktiviert wird.
Speicherplatz	20 GB Speicherkapazität für Sprachaufzeichnungen (MB) = Anzahl der Aufzeichnungen × durchschnittliche Gesprächsdauer × 0,5 MB pro Minute **NOTIZ** Diese Formel basiert auf einer Audio-Bitrate von 64 kbps (Kilobit pro Sekunde). [(64 kbps × 60 s) ÷ 8 Bit] ÷ 1024 KB = 0.46875 MB pro Minute Speicherplatz für Bildschirmaufnahmen (MB) = Anzahl der Aufnahmen × durchschnittliche Gesprächsdauer × 1,5 MB pro Minute **HINWEIS: Der Speicherbedarf für Bildschirmaufnahmen hängt von drei Faktoren ab: Aufnahmelänge, Monitorauflösung und Anzahl der**

	Aufnahmen. von Monitoren, die aufgezeichnet werden. Der hier angegebene Wert basiert auf einem einzelnen Monitor. Jeder zusätzliche Monitor wird separat aufgezeichnet,

Desktop-Hardware	
	Sie müssen diese Formel für jeden Monitor anwenden.
CPU	Intel Core 2 Duo 2,0 GHz, Core i3, AMD Athlon 64 X2 oder besser
Erinnerung	2 GB

Desktop-Software

.NET Framework

Webex WFO Smart Desktop benötigt .NET Framework 4.5 für die Webex WFO Analysefunktionen. Wenn .NET Framework nicht installiert ist, kann Webex WFO keine Browserereignisse als Teil der Desktop Analytics-Daten erfassen. Sie können das .NET Framework von http://www.microsoft.com/en-us/download/details.aspx?ID=30653 herunterladen.

Browser

Jeder von Ihnen verwendete Browser muss das Herunterladen von Dateien ermöglichen. Popup-Blocker müssen deaktiviert werden.

Desktop-Analytics-Plug-in/Erweiterung

Benutzer, die Felder für Desktop Analytics über die Seite „Field Manager“ in Webex WFO verwalten, und Agenten-Desktops, auf denen Smart Desktop installiert ist, müssen die Browsererweiterung/das Plug-in Calabrio Analytics aktiviert haben. Das Plug-in wird nicht nur zum Markieren von Feldern im Browser benötigt, sondern auch zur Überwachung der Webaktivitäten des Agenten innerhalb des Browsers.

Aktivieren Sie die Desktop-Analytics-Erweiterung in Firefox.

Wenn Sie sich zum ersten Mal mit Firefox bei Webex WFO anmelden, erscheint ein Dialogfeld, in dem Sie aufgefordert werden, die Calabrio-Browsererweiterung zu installieren. Wählen Sie **Diese Installation zulassen** und klicken Sie auf **Weiter**. Es sind keine weiteren Maßnahmen erforderlich.

Aktivieren Sie das Desktop-Analytics-Plug-in in Webex WFO Edge Chromium

In Edge Chromium gehen Sie zu https://chrome.google.com/webstore/detail/calabrio-Analytics-plugin/hecgknieibccghjmmhhckdfeobjoffdf und klicken Sie auf **Zu Chrome hinzufügen**.

Aktivieren Sie das Desktop-Analytics-Plug-in in Chrome.

Die Chrome-Erweiterung kann heruntergeladen oder über Gruppenrichtlinieneinstellungen installiert werden. Laden Sie das Calabrio Analytics Plug-in, Version 0.2.0.4, herunter und installieren Sie es. Das Plug-in befindet sich hier:

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

HINWEIS: Falls das Klicken auf den Link nicht funktioniert, kopieren Sie die URL und fügen Sie sie in Ihren Browser ein.

Adobe Acrobat Reader

Zum Öffnen exportierter PDF-Dateien und der Benutzerdokumentation wird der Adobe Reader benötigt. Ein kostenloser Download von Acrobat Reader ist unter www.adobe.com verfügbar.

WICHTIG Es gibt bekannte Probleme mit Adobe Reader-Versionen, die die Sicherheitsfunktion (Erweitert) verwenden. Wenn Sie die Desktop-Analysefunktion nutzen möchten, müssen Sie in Adobe Reader unter „Einstellungen“ zu „Sicherheit (Erweitert)“ navigieren und die Option „Geschützten Modus beim Start aktivieren“ deaktivieren.
Und aktivieren Sie die Kontrollkästchen für **Erweiterte Sicherheit** , klicken Sie bei Warnmeldungen auf **Ja** und anschließend auf **OK** , um Ihre Änderungen zu speichern. Nach Abschluss der Bearbeitung müssen Sie Adobe Reader neu starten, damit die Änderungen wirksam werden. Wenn Adobe Reader nicht korrekt konfiguriert ist, kann Desktop Analytics keine Ereignisse im Zusammenhang mit Adobe Reader erfassen.

Desktop-Software und Audioaufnahme

Damit Smart Desktop eine ordnungsgemäße Telefonerkennung und Audioaufzeichnung durchführen kann, ist die Fähigkeit erforderlich, bestimmte Netzwerkprotokolle (wie SIP, SCCP und RTP) zu erkennen und aufzuzeichnen. Jegliche Software, die auf dem PC ausgeführt wird und den Netzwerkverkehr stört, umleitet oder auf andere Weise verbirgt, führt dazu, dass Smart Desktop nicht ordnungsgemäß funktioniert.

BEISPIEL Der SonicWall-Client VPN mit aktiviertem DNE-Lightweight-Filter (Deterministic Network Enhancer) bewirkt, dass ausgehender Netzwerkverkehr vom Netzwerkadapter umgeleitet wird.
Das Smart Desktop verwendet. In diesem Fall muss der DNE Lightweight-Filter deaktiviert werden, damit Smart Desktop ordnungsgemäß funktioniert.

Aktivieren Sie die Desktop Analytics-Erweiterung in Ihrem Browser.

Smart Desktop muss auf Ihrem Computer installiert und aktiviert sein, bevor Sie Felder markieren können. Benutzer, die über die Berechtigung verfügen, Felder für Desktop Analytics mithilfe der Seite „Field Manager“ und auf den Desktops der Agenten, auf denen Smart Desktop installiert ist, zu verwalten, müssen das entsprechende Desktop Analytics-Browser-Plug-in für den von ihnen verwendeten Browser konfiguriert haben.

Voraussetzungen

- Ihre Organisation besitzt eine der folgenden Lizenzen:
  - Grundlagen der Analytik

- Analytics Enterprise

  - Desktop-Analyse
- Smart Desktop ist auf Ihrem Computer installiert und aktiviert.

Verfahren

Aktivieren Sie die Desktop-Analytics-Erweiterung in Firefox.

Wenn Sie sich zum ersten Mal mit Firefox bei Webex WFO anmelden, erscheint ein Dialogfeld, das Sie zur Installation der Calabrio-Browsererweiterung auffordert. Wählen Sie **Diese Installation zulassen** und klicken Sie auf **Weiter**. Es sind keine weiteren Maßnahmen erforderlich.

Aktivieren Sie das Desktop-Analytics-Plug-in in Microsoft Edge Chromium

In Edge Chromium gehen Sie zu https://chrome.google.com/webstore/detail/calabrio-Analytics-plugin/hecgknieibccghjmmhhckdfeobjoffdf und klicken Sie auf **Zu Chrome hinzufügen**.

Aktivieren Sie das Desktop-Analytics-Plug-in in Chrome.

Die Chrome-Erweiterung kann heruntergeladen oder über Gruppenrichtlinieneinstellungen installiert werden. Laden Sie das Calabrio Analytics Plug-in, Version 0.2.0.4, herunter und installieren Sie es. Das Plug-in befindet sich hier:

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

HINWEIS: Falls das Klicken auf den Link nicht funktioniert, kopieren Sie die URL und fügen Sie sie in Ihren Browser ein.

Verwandte Themen

„Installation von Webex WFO Smart Desktop“ in der *Webex WFO Installationsanleitung*

Thin-Client-Server

NOTIZ Citrix XenApp wird nur auf unterstützten Windows-Servern unterstützt.

Bei Verwendung eines Thin-Client-Servers ist Folgendes zu beachten:

- Für Thin Clients, die Smart Desktop verwenden, ist eine Remote-Desktop-Sitzung erforderlich, um alle Benutzerdaten (Audio, Bildschirm und Desktop-Aufzeichnung) zu erfassen. Falls keine Remote-Desktop-Sitzung vorhanden ist, installieren Sie Smart Desktop auf den Agenten-Desktops, um alle Benutzerdaten auf dem Desktop zu erfassen, während der Benutzer angemeldet ist.
- Konfigurieren Sie Arbeitsabläufe so, dass sowohl für Bildschirm- als auch für Sprachaufnahmen die Funktion „Sofortiger Upload“ verwendet wird, um sicherzustellen, dass alle Aufnahmen zugänglich sind.

- Wenn Sie Smart Desktop für Aufzeichnungszwecke verwenden, benötigt der Thin-Client-Server zusätzliche Serverressourcen für Bildschirmaufzeichnungen. Der Ressourcenbedarf variiert je nach konkretem Design und erfordert möglicherweise detaillierte Hardware-Designs, die vor der Bereitstellung von Cisco geprüft werden sollten.
- Wenn Sie ein virtuelles Image verwenden und dieses Zugriff auf Ihre lokale Netzwerkkarte hat, können Sie Smart Desktop für die agentenseitige Aufzeichnung nutzen.

Installation des Thin-Client-Servers

Installieren Sie Citrix XenApp oder Windows Terminal Services gemäß der Produktdokumentation.

Verwenden Sie die folgenden Einstellungen, die für die Unterstützung der Audio- und Bildschirmaufnahme- sowie der Wiedergabefunktionen in Webex WFO erforderlich sind:

Bereich	Rücksichtnahme
Browser	▪ Bei Thin-Client-Server-Bereitstellungen sollte ein unterstützter Browser integriert werden. Thin-Client-Server müssen einen unterstützten Browser enthalten, um auf Webex WFO zugreifen zu können. ▪ Veröffentlichen Sie den Browser lokal auf jedem Server. ▪ Stellen Sie sicher, dass die Browser-Sicherheitseinstellungen es Endbenutzern ermöglichen, Aufnahmen über den Thin Client abzuspielen.
Sitzungen beschränkt.	Die Anzahl gleichzeitiger Sitzungen pro Benutzer ist auf eine einzige Sitzung
Intelligenter Desktop-Client	▪ Für Citrix-Clientdienste müssen Sie außerdem Smart Desktop installieren. Der Client auf dem Thin-Client-Server zeichnet die Desktop-Aktivitäten der Benutzer (Desktop-Analyse) und Telefongespräche mit Hilfe eines unterstützten Softphones auf. ▪ Der Smart Desktop Client verbindet sich mit der Webex WFO-Plattform über den eindeutigen Domänen-/Windows-Login des Benutzers.

Portnutzung

Die Portanforderungen für die Webex WFO-Komponenten sind unten aufgeführt.

Im Allgemeinen müssen die Ports 80 und 443 eines Webservers geöffnet sein, um eine Verbindung zu Webex WFO für alle Cloud-Integrationen mit Webex WFO herzustellen. Die genauen Portanforderungen variieren je nach Ihrem Cloud-Bereitstellungsmodell.

Kantenkomponenten:

- Smart Desktop

Datenserverkomponenten:

- Datenserver – ACD Synchronisierung: Avaya CM mit Contact Center Elite
- Datenserver – ACD Synchronisierung: CCaaS-Integrationen
- Datenserver – ACD Synchronisierung: CUCM Netzwerkaufzeichnung
- Datenserver – ACD Synchronisierung: Cisco Unified Contact Center Enterprise (Unified CCE)
- Datenserver – ACD Synchronisierung: Cisco Unified Contact Center Express (Unified CCX)
- Datenserver – GIS
- Datenserver – Aufzeichnung/Erfassung
- Datenserver – Signalisierung: CTI
- Datenserver – Signalisierung: CTI, Avaya Aura Communication Manager Aufzeichnung
- Datenserver – Signalisierung: CTI, Cisco Unified Communications Manager Netzwerkaufzeichnung
- Datenserver – Signalisierung: SIPREC

Edge-Komponenten

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
Smart Desktop				
UDP 49152–65535	Live-Audioüberwachung – RTP Live-Bildschirmüberwachung – RDP-Stream	PC des Agenten	Browser des Vorgesetzten	—
TCP 52102	Kommunikation zwischen den Cisco CTI-Datenservern und SDC	Smart Desktop	Datenserver	

Datenserverkomponenten

Port	Ge	Quelle	Ziel	Anm
Datenserver – ACD Synchronisierung: CCaaS-Integrationen				
TCP 443	Kommunikation zwischen CCaaS-Integrationen und den folgenden Einstellungen auf dem Datenserver: Regionaler Datenserver ACD Erfassungseinstellungen, Aufzeichnung CTI Signalisierungsservereinstellungen und regionale Daten Server ACD Aufnahmeeinstellungen	—	—	—
Datenserver – ACD Synchronisierung: CUCM Netzwerkaufzeichnung				
TCP 22	Kommunikation zwischen der SFTP-Konfiguration und den regionalen Datenserver-Abgleichseinstellungen auf dem Datenserver und dem CUCM-Abrechnungsdienst	SFTP, Datenserver	CUCM Abrechnung - Service	

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
TCP 8443	Kommunikation zwischen CUCM AXL und dem regionalen Datenserver ACD Synchronisierungseinstellungen auf dem Datenserver	Datenserver	CUCM AXL	—
Datenserver – ACD Synchronisierung: Cisco Unified CCE				
TCP 1433 TCP 1434	Kommunikation zwischen dem Cisco Unified CCE AW SQL Server Datenbank und regionaler Datenserver ACD Synchronisierungseinstellungen auf dem Datenserver	Datenserver	Cisco Unified CCE AWDB SQL Serverdatenbank	—
TCP 1433 TCP 1434	Kommunikation zwischen dem Cisco Unified CCE HDS SQL Server Datenbank- und regionale Datenserver-Abgleichseinstellungen und die Erfassungseinstellungen des regionalen Datenservers ACD für die Daten Server	Datenserver	Cisco Unified CCE HDS SQL Serverdatenbank	—
TCP 42027	Kommunikation zwischen dem Cisco Unified CCE CTI-Dienst (Seite A) und die Aufzeichnung CTI Signalisierungsservereinstellungen auf den Daten Server	Datenserver	Cisco Unified CCE CTI Service (Seite A)	Seite A ist Standard, wenn PG1 verwendet wird. Häfen werden variieren je nachdem, welche PG Sie verwenden. Der Server-Port CTI ist konfiguriert in Unified CCE ACD Konfiguration.
TCP 43027	Kommunikation zwischen dem Cisco Unified CCE CTI-Dienst (Seite b) und die Einstellungen des Aufzeichnungsservers CTI Signalisierungsserver auf den Daten Server	Datenserver	Cisco Unified CCE CTI Service (Seite B)	Seite B ist Standard, wenn PG1 verwendet wird. Häfen werden variieren je nachdem, welches PG Sie verwenden. Der CTI Serverport, der im Unified CCE ACD Konfiguration.
Datenserver – ACD Synchronisierung: Cisco Unified CCX				

TCP 1504	Kommunikation zwischen der Unified CCX Informix-Datenbank und	Datenserver	Unified CCX	—

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
	sowohl die Einstellungen für die Synchronisierung des regionalen Datenservers ACD als auch die regionalen Datenserver ACD Erfassungseinstellungen		Informix-Datenbank	
TCP 12028	Kommunikation zwischen dem Cisco Unified CCX CTI Service (Seite a) und die Einstellungen des Aufzeichnungsservers CTI Signalisierungsserver für die Daten Server	Datenserver	Cisco Unified CCX CTI Dienst (Seite A)	Seite A Standardeinstellung. Das ist der RMCM TCP Port konfiguriert in Unified CCX Systemparameter. Der Server CTI Port konfiguriert im Unified CCX ACD Konfiguration.
TCP 12028	Kommunikation zwischen dem Cisco Unified CCX CTI Service (Seite b) und die Einstellungen des Aufzeichnungsservers CTI Signalisierungsservers auf den Daten Server	Datenserver	Cisco Unified CCX CTI Dienst (Seite B)	Seite B Standard. Das ist der RMCM TCP in Unified CCX konfigurierter Port Systemparameter. Der Server CTI Port konfiguriert im Unified CCX ACD Konfiguration.
Datenserver – GIS				
—	—	—	—	Während GIS nicht direkt auf einem müssen die Dateien kopiert werden nach dem Datenserver. Wenn der Kopiervorgang abgeschlossen ist Über FTP werden die Ports 20 und 21 verwendet.
Datenserver – Aufzeichnen/Erfassen				
UDP 39500–43500	Aufnahme RTP	Telefon oder Sprachanruf Tor	Audio-Aufnahme (Aufzeichnungsserver)	—

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
UPD 49152–65535	Live-Audioüberwachung – RTP	Audio-Aufnahme (Aufzeichnungsserver)	Browser des Supervisors	—
Datenserver – Signalisierung: CTI				
TCP 443	Signalisierungsserver	Signalisierungsserver	Cisco API	—
TCP 52102	Signalisierung wird aufgezeichnet	Audio-Capture (Aufzeichnungsserver) oder Smartdesktop-Clients	Signalisierungsserver	—
TCP 52103	Hazelcast (Haselnussguss)	Signalserver-Partner	Signalisierungsserver	—
Datenserver – Signalisierung: CTI, Cisco Unified Communications Manager Netzwerkaufzeichnung				
TCP 2748	JTAPI Signalisierung	Signalisierungsserver	Vereinheitlicht CM Herausgeber und Abonnenten	—
TCP 5060 UDP 5060	SIP Signalisierung von Unified CM	Ein beliebiger Unified CM Publisher oder Abonnent	Signalisierungsserver	Nicht sicher
TCP 5060	Signalisierungsserver	primärer Signalisierserver	sekundärer Signalisierserver	Bidirektional

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
TCP 5061	Sichere SIP Signalisierung von Unified CM	Ein beliebiger Unified CM Publisher oder Abonnent	Signalisierungsserver	Sicher. Wird in der Regel nur verwendet, wenn das System für SRTP konfiguriert ist.
Datenserver – Signalisierung: SIPREC				
TCP 443	Cisco API Abfragen	Signalisierungsserver	Cisco API	—
TCP 5060 UDP 5060	SIP Signalisierung vom Gateway	Gateway	Signalisierungsserver	—
TCP 59106	Signalisierung wird aufgezeichnet	Audio-Aufnahme (Aufzeichnungsserver)	Signalisierungsserver	—
TCP 59107	Hazelcast (Haselnussguss)	Signalserver-Partner	Signalisierungsserver	—

Dateiverschlüsselung

Medien und Daten werden aus Sicherheitsgründen verschlüsselt. Webex WFO verwendet einen Schlüssel, um die aufgezeichneten Kundengespräche zu entschlüsseln. Der Verschlüsselungsschlüssel befindet sich in der Datenbank. Jeder Mandant verfügt über einen eigenen Verschlüsselungsschlüssel. Die Verschlüsselungsschlüssel können aktualisiert werden.

Kennwortrichtlinie

Anforderungen an die Kennwortkomplexität

Kennwörter müssen den folgenden Regeln entsprechen.

- Muss mindestens 8 Zeichen lang sein.
- Muss mindestens eines der folgenden Elemente enthalten.

  Großbuchstaben
  Kleinbuchstaben
  Zahlen 0-9
  Besondere Charaktere ! # $ % & ( ), . / : ; = ? @ ^ ` |

- Es darf weder Ihren Namen noch Ihre E-Mail-Adresse enthalten.

HINWEIS: Kennwörter laufen nicht ab.

Authentifizierung

Standardmäßig werden die Benutzerauthentifizierung und Kennwörter mit Webex WFO verwaltet. Bei Systemen, die mit einem ACD synchronisiert sind, werden Benutzer im ACD erstellt und verwaltet, obwohl Sie auch in Webex WFO Benutzer erstellen können.

Sie können die Authentifizierung SAML (Security Assertion Markup Language) verwenden. SAML ermöglicht es Ihnen, einen externen Identitätsanbieter (IdP) zu verwenden, um Benutzernamen und Kennwörter zu authentifizieren. Diese Methode der Benutzerauthentifizierung und Kennwortverwaltung wird allgemein als "Single Sign-On" bezeichnet.

Plattform-Erfassungsmethoden

In diesem Thema wird beschrieben, wie Sie Webex WFO mit verschiedenen Contact Center-Plattformen konfigurieren können.

Unterstützte Erfassungsmethoden nach Plattform

In der folgenden Tabelle wird beschrieben, wie Contact Center-Plattformen die Aufzeichnungserfassung unterstützen.

ANMERKUNG

Webex WFO unterstützt SRTP nur mit den folgenden Erfassungsmethoden:

- ACME-Paket
- Cisco Unified CM

Bahnsteig	Erfassungsmethode	Signalisierung	Beschreibung der Signalisierung
Cisco	Integrierte Bridge-Netzwerkaufzeichnung	JTAPI	Registriert sich mit dem Call Manager für JTAPI-Ereignisse
Cisco	Desktop-Aufzeichnung	JTAPI	Registrierung beim Call Manager für JTAPI-Ereignisse
Cisco	Gateway (Cisco Unified Border Element – CUBE)	SIPREC	Registrierung bei CUBE für SIPREC-Signalisierung
Cisco	Smartdesktop-Client	IP Communicator (SIP/SCCP)	SCCP Nachrichten vom Desktop

Bahnsteig	Erfassungsmethode	Signalisierung	Beschreibung der Signalisierung
Cisco	Smartdesktop-Client	Jabber (SIP/SCCP)	Schnüffelt SIP/SCCP Nachrichten vom Desktop
Cisco	Smartdesktop-Client	Cisco IP TelefonTelefon: (SIP/SCCP)	Schnüffelt SIP/SCCP Nachrichten vom Desktop
Cisco Webex Contact Center (CWCC)	Automatisierter Import	CWCC Analysator API	Umfrage CWCC Analyzer für die Verarbeitung nach Anruf CDR und Anruf
ACME	Gateway (ACME Pakete)	SIPREC	Registriert mit ACME für SIPREC-Signalisierung
SONUS	Gateway (SONUS)	SIPREC	Registriert sich bei SONUS für die SIPREC-Signalisierung

Cisco Spracherfassungsmethoden

Die folgende Tabelle enthält Informationen zur Integration der von Cisco unterstützten und getesteten Erfassungstypen und Signale:

Erfassungsmethode	Signalisierung	Beschreibung	Medien Bach	Intelligenter Desktop Screenshot	Live-Audio Monitor
Netzwerk Aufzeichnung—Integrierte Brücke (BIB)	JTAPI	Registriert bei CUCM/JTAPI Ereignisse	BIB – Medien Gestreamt von Telefonnummer	Ja (Smart) Desktop-Client Erfordert CTI Anschluss)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Auftraggeber – IP Mitteilende	SIP/SCCP	Monitor SIP/SCCP Nachrichten aus Desktop/Softphone	Medienstrom eingefangen direkt auf Desktop	Ja (Smart) Desktop-Client)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Auftraggeber – Jabber	SIP/SCCP	Monitore SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf	Ja (Smart) Desktop-Client)	Ja (Smart) Desktop Client) über

Erfassungsmethode	Signalisierung	Beschreibung	Medien Bach	Intelligenter Desktop Screenshot	Live-Audio Monitor
			Desktop		WebRTC
Intelligenter Desktop Auftraggeber – Cisco IP Telefon (Gänseblümchen Verkettet)	SIP/SCCP	Monitore SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Desktop	Ja (Smart) Desktop-Client)	Ja (Smart) Desktop Client) über WebRTC
Gateway (CUBE)	SIPREC	Registriert bei CUBE für SIPREC Signalisierung	SIPREC – Medien-Forking ab Cisco WÜRFEL	Ja (Smart) Desktop-Client)	Nein
Massenkontakt Importieren	API basiert	Registriert bei CUBE für SIPREC Signalisierung	Automatisiert Import von unverschlüsselt . WAV und assoziiert Kontakt Metadaten-Dateien en gros	N/A – Dateien Verschlüsselt und Eingeführt	Nein

Legacy-Spracherfassungsintegrationen von Five9

Die folgende Tabelle enthält Informationen zur Integration von Five9-unterstützten und -getesteten Erfassungstypen und Signalen. Es bezieht sich speziell auf die ältere Five9-Integration, nicht auf Five9 ARU oder Five9 VCC mit VoiceStream.

Erfassungstyp	Signalisierung	Beschreibung	Medienstrom	Intelligenter Desktop - Bildschirm Gefangennahme	Live-Audio Monitor

| **Plattform-**

Smartdesktop-Client	Kafka CTI	Webex WFO Plattform registriert sich bei Five9 Kafka-Veranstaltungen API	Medien-Stream, der direkt auf	Ja (Smart Desktop Client)	Ja (Smart Desktop Client) über WebRTC

Erfassungstyp	Signalisierung	Beschreibung	Medienstrom	Intelligenter Desktop - Bildschirm Gefangennahme	Live-Audio Monitor
			Schreibtisch – POST Aufruf CDR und Versöhnung Verarbeitung Schwärzungen und Fügt Ereignisse ein nach Kafka Anrufereignisse		
Intelligenter Desktop Client	Five9-Agent Desktop Plus (ADP) - Kafka CTI	Monitor SIP/SCCP Nachrichten aus Desktop/Softphone	Medienstrom eingefangen direkt auf Schreibtisch – POST Aufruf CDR und Versöhnung Verarbeitung Schwärzungen und Fügt Ereignisse ein nach Kafka Anrufereignisse	Ja (Smart) Desktop Auftraggeber)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Client	Five9-Agent Desktop Werkzeugsatz (ADT) - Kafka CTI	Monitore SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Schreibtisch – POST Aufruf CDR und Versöhnung Verarbeitung Schwärzungen	Ja (Smart) Desktop Auftraggeber)	Ja (Smart) Desktop Client) über WebRTC

| **Plattform-**

	und
	Fügt Ereignisse ein
	nach Kafka
	Anrufereignisse

Erfassungstyp	Signalisierung	Beschreibung	Medienstrom	Intelligenter Desktop - Bildschirm Gefangennahme	Live-Audio Monitor
Intelligenter Desktop Client	Five9 Java Agent Desktop-Kafka CTI	Monitore SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Schreibtisch – POST Aufruf CDR und Versöhnung Verarbeitung Schwärzungen und Fügt Ereignisse ein nach Kafka Anrufereignisse	Ja (Smart) Desktop Auftraggeber)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Client	Five9 VCC Importieren	Fünf9/Webex WFO Cloud-Integration in Five9 VCC importieren Audioaufnahmen in Webex WFO Wolke	N/A – Importieren Nur	Ja (Smart) Desktop Auftraggeber)	Nein

Sonus Gateway-Aufzeichnung

Cisco unterstützt die Ausfallsicherheit für Sonus Gateway Recording.

Sie müssen den Headern SIP und SIPREC INVITE in Cisco-Guid Sonus SIP SMM-Regeln (Message Manipulation) hinzufügen, damit Sonus SBC mit QM funktioniert. Dadurch kann QM Aufrufe mit den Cisco Unified CM CDR-Datensätzen abgleichen. Die Regeln bewirken Folgendes:

- Für Anrufe, die ohne "Cisco-Guid"-Header in den SBC eingehen, erstellt der SMM eine Cisco-Guid unter Verwendung der 4 Hexadezimal-Tupel der Ausgangs-Anruf-ID. Jedes Tupel wird in eine mit 0 aufgefüllte Dezimalzahl konvertiert, die durch Bindestriche von der Cisco-Guid getrennt wird.
- Bei Anrufen, die bereits einen Cisco-Guid-Header enthalten, bleibt der Header unverändert.

HINWEIS **Hinweis:** Die Cisco_Guid wird NICHT durch eine neu erstellte Cisco-Guid

überschrieben.

- Die SIPREC-Einladung zum Recorder enthält einen Cisco-Guid-Header, der mit dem obigen Cisco-Guid übereinstimmt.

Die Regeln müssen mit Ihrem aufgezeichneten Trunk und dem Unified CM-Trunk verknüpft sein, der von Ihrem Unified CM verwendet wird. Sie müssen diese Regeln nur einmal erstellen. Wenn Sie neue Zonen und Trunks erstellen, können Sie diese Regeln wiederverwenden.

So konfigurieren Sie Sonus Session Border Controller für die Verwendung mit QM:

1. Erstellen und aktivieren Sie die SMM-Regeln über die Sonus-Befehlszeilenschnittstelle (CLI)
    a. Erstellen und aktivieren Sie die Unified CM SMM-Regeln für eingehende Anrufe. Weitere Informationen finden Sie im Beispiel für SMM-Regeln für eingehenden Datenverkehr für Unified CM .
    b. Fügen Sie die Unified CM Outbound SMM-Regeln hinzu. Weitere Informationen finden Sie im Beispiel für ausgehende SMM-Regeln für Unified CM .
    c. Fügen Sie die SMM-Regeln für ausgehende Recorder-Anrufe hinzu. Weitere Informationen finden Sie im Beispiel für ausgehende SMM-Regeln für den Recorder .
2. Verwenden Sie die Sonus-CLI, um SIPREC für den SIP Sig-Port in der Zone zu aktivieren, in der sich Ihr Unified CM-Trunk befindet.
3. Verwenden Sie die Sonus CLI oder den Navigator, um eine SIP-Trunk-Gruppe für den Sonus SIPREC-Server von QM zu erstellen. Weisen Sie der IP Adresse des QM Rechners, auf dem der "Monitoring and Recording Sonus SIPREC Service" ausgeführt wird, das Präfix IP Ingress zu.
4. Verwenden Sie die Sonus CLI/Navigation, um Ihren Trunks SMM-Regeln wie folgt zuzuweisen:
    a. Weisen Sie UCM_INBOUND SMM dem Eingabeprofil des Signalnachrichtenbearbeitungsadapters Ihres Unified CM-Trunks zu.
    b. Weisen Sie UCM_OUTBOUND SMM dem Ausgabeprofil des Signaling Message Manipulation-Adapters Ihres Unified CM-Trunks zu.
    c. Weisen Sie RECORDER_OUTBOUND SMM dem Ausgangsprofil des Signaling Message Manipulation-Adapters für den Sonus SIPREC-Trunk von QM zu.
5. Verwenden Sie den Sonus PSX, um eine IP Signaling Peer Group für den Sonus SIPREC Server des QM zu erstellen. Weisen Sie der IP Adresse des QM Rechners, auf dem der "Monitoring and Recording Sonus SIPREC Service" ausgeführt wird, das Präfix IP Ingress zu.
6. Verwenden Sie den Sonus PSX, um eine Trunk-Gruppe für den Sonus SIPREC-Server des QM zu erstellen. Verwenden Sie exakt den gleichen Namen wie in Schritt 3.

7. Verwenden Sie den Sonus PSX, um ein Recorder-Profil für Ihren QM Sonus SIPREC Server zu erstellen. Weisen Sie die IP4-Adresse dem QM-Computer zu, auf dem der "Monitoring and Recording Sonus SIPREC Service" ausgeführt wird, und legen Sie die Portnummer auf 5060 fest.
8. Verwenden Sie den Sonus PSX, um Kriterien für die Anrufaufzeichnung zu erstellen.

Beispiel für eingehende SSM-Regeln für Unified CM

konfigurieren

set profiles signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 applyMatchHeader all

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Kriterium 1 Typ Nachricht

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Kriterium 1 Nachricht messageTypes all

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Kriterium 2 Typ Header

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Kriterium 2 Headername Cisco-Guid

set-Profile , die sipAdaptorProfile signalisieren, UCM_INBOUND Regel 1, Kriterium 2, Header-Bedingung vorhanden

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Aktion 1 Typ Header

Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_INBOUND Regel 1 Aktion 1 Vorgang speichern

set profiles signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Aktion 1 headerInfo fieldValue

profile festlegen , die sipAdaptorProfile signalisieren UCM_INBOUND Regel 1 Aktion 1 vom Typ header

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 1 Aktion 1 von Wert Cisco-Guid

Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_INBOUND Regel 1 Aktion 1 auf den Typ variable

Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_INBOUND Regel 1 Aktion 1 auf variableValue var1

Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_INBOUND Regel 2 applyMatchHeader eins

profile signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 1 Typ

| **Plattform-**

Nachricht						
set profiles signalisieren sipAdaptorProfile messageTypes request		UCM_INBOUND	Regel 2	Kriterium	1	
set-profile , die sipAdaptorProfile-Nachrichtenmethode-Typen invite signalisieren		UCM_INBOUND	Regel 2	Kriterium	1	
set profiles, die sipAdaptorProfile-Nachrichtenbedingung vorhanden signalisieren		UCM_INBOUND	Regel 2	Kriterium	1	
Festlegen von Profilen, die sipAdaptorProfile-Header signalisieren		UCM_INBOUND	Regel 2	Kriterium	2	Art
profile festlegen , die sipAdapterorProfile-Headername signalisieren Von		UCM_INBOUND	Regel 2	Kriterium	2	
set profiles, die signalisieren, dass die Header-Bedingung sipAdaptorProfile vorhanden ist		UCM_INBOUND	Regel 2	Kriterium	2	
set-Profile-Signalisierung sipAdaptorProfile-Variable		UCM_INBOUND	Regel 2	Kriterium	3	Art
set profiles, die signalisieren, dass die sipAdaptorProfile-Variable vorhanden ist		UCM_INBOUND	Regel 2	Kriterium	3	
set-Profile-Signalisierung sipAdaptorProfile-Variablen-Variablen-ID var1		UCM_INBOUND	Regel 2	Kriterium	3	
Signalisierungsparameter für Profile festlegen	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	Art
Festlegen von Profilen Signalisierungsvorgang	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	
Hinzufügen	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	
set profiles signalisieren paramType generic	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	Von
Festlegen von Profilen Signalisierungstyp Variable	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	Von
set-profile-signalisierungsvariableWert var1	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	zum Eingeben von
Signalisierungsparameter für Profile festlegen						
Profile festlegen , die Cisco-GUID signalisieren						
begehen						

set-Profile , die sipAdaptorProfile-UCM_INBOUND-Status aktiviert Commit signalisieren

Beispiel für ausgehende SMM-Regeln für Unified CM

konfigurieren

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Kriterium 1 Typ Nachricht

set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Kriterium 1 message messageTypes request

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Kriterium 1 NachrichtenmethodeTypen invite

profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Kriterium 2 Typ Header

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Kriterium 2 Headername cisco-guid

profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Kriterium 2 Header-Bedingung fehlt

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Aktion 1 Typ Variable

Festlegen von Profilen, die sipAdaptorProfile UCM_OUTBOUND Regel 1 Aktion 1 Vorgangsspeicher

set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Aktion 1 vom Typ Wert

profile festlegen, die sipAdaptorProfile UCM_OUTBOUND Regel 1 Aktion 1 aus dem Wert cisco-guid signalisieren

Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 1 Aktion 1 auf den Typ variable

profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 1 Aktion 1 auf variableValue var1 festlegen

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 1 Typ Nachricht

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 1 message messageTypes request

profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 1 NachrichtenmethodeTypen invite

profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 2 Typ Variable

set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 2 Variable Bedingung vorhanden

profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 2

variable variableID var1
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 3 Typ Header
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 3 Headername Anruf-ID
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Kriterium 3 Header-Bedingung vorhanden
profile festlegen, die sipAdaptorProfile signalisieren UCM_OUTBOUND Regel 2 Aktion 1 Typ Header
Festlegen von Profilen, die sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 1 Vorgang speichern
profile festlegen, die sipAdaptorProfile signalisieren UCM_OUTBOUND Regel 2 Aktion 1 headerInfo-FeldWert
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 , Aktion 1 vom Typ header
profile festlegen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 , Aktion 1 aus dem Wert call-id
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 1 auf den Typ variable
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 1 auf variableValue var2 setzen
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 2 Typ Variable
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 2 Operation regdel
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 2 auf den Typ variable
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 2 auf variableValue var2 festlegen
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 2 regulärer Ausdruck string @.*
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 2 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 3 Typ Variable
profile festlegen, die sipAdaptorProfile signalisieren UCM_OUTBOUND Regel 2 Aktion 3 Vorgang speichern
Festlegen von Profilen, die sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 3 von

Typ Variable
profile festlegen, die sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 3 von variableValue var2 signalisieren
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 3 auf den Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 3 auf variableValue var3
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 4 Typ Variable
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 4 Operation regdel
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 4 auf den Typ variable festlegen
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 4 auf variableValue var2
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 4 regexp string _.*
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 4 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 5 Typ Variable
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 5 Operation regdel
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 5 auf den Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 5 auf variableValue var3
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 5 Regexp String .*_
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 5 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 Typ Variable
profile festlegen, die sipAdaptorProfile signalisieren UCM_OUTBOUND Regel 2 Aktion 6 Vorgang regappend
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 vom Typ value
Festlegen von Profilen, die sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 von

Wert 000000000
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 6 auf den Typ variable
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 auf variableValue var2 setzen
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 reguläre Ausdruckszeichenfolge ^
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 7 Typ Variable
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 7 Vorgang regappend
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 7 vom Typ Wert
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 7 aus Wert 000000000
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 7 auf den Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 , Aktion 7 auf variableValue var3
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 7 reguläre Ausdruckszeichenfolge ^
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 7 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 8 Typ Variable
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 8 Operation regpredel
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 8 auf den Typ variable
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 8 auf variableValue var2 setzen
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 8 reguläre Ausdruckszeichenfolge $
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 8 regexp matchInstanz eins
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 9 Typ

Variable
profile festlegen signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 9
Operation regpredel
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 9
auf den Typ variable
profile signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 9 auf variableValue var3
setzen
set-profile-signalisierung sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 9 reguläre
Ausdruckszeichenfolge $
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 9 regexp matchInstance
one

Signalisierungsvariable "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	10	Art
Festlegen von Profilen Signalisierungsvorgang	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	10	
Anhängen Wert für den	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	10	Von
Signalisierungstyp "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	10	Von
Festlegen des Signalisierungswerts für	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	10	An
Profile - Festlegen von Profilen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	10	An
Signalisierungstyp Variable Setze Profile	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	11	Art
SignalisierungsvariableWert var2	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	11	
Signalisierungsvariable "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	11	Von
Festlegen von Profilen Signalisierungsvorgang	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	11	Von
Anhängen Festlegen von Profilen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	11	An
Signalisierungstyp Variable set-profile-signalisierungsvariableWert var3	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	11	An
	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	12	Art
Festlegen von Profilen Signalisierungstyp Variable Setze Profile	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	12	

| **Plattform-**

SignalisierungsvariableWe
rt var2
Signalisierungsvariable
"Profile" festlegen
Signalisierung von Profilen festlegen

Vorgangsspeicher							
Festlegen von Profilen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	12	Von
Signalisierungstyp Variable							
Setze Profile	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	12	Von
SignalisierungsvariableWert var2	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	12	An
Festlegen von Profilen							
Signalisierungstyp Variable	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	12	An
set-profile-signalisierungsvariableWert var3	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	13	Art
Signalisierungsvariable "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	13	
Festlegen von Profilen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	13	Von
Signalisierungsvorgang Anhängen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	13	Von
Wert für den							
Signalisierungstyp "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	13	An
Festlegen des	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	13	An
Signalisierungswerts für Profile -	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	14	Art
Festlegen von Profilen							
Signalisierungstyp Variable	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	14	
Setze Profile							
SignalisierungsvariableWert var2	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	14	Von
Signalisierungsvariable "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	14	Von
Festlegen von Profilen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	14	An
Signalisierungsvorgang Anhängen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	14	An
Festlegen von Profilen							
Signalisierungstyp Variable	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	15	Art
set-profile-signalisierungsvariableWert var3	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	15	
Festlegen von Profilen	sipAdapterProfil	UCM_OUTBOUND	Regel	2	Aktion	15	
Signalisierungstyp Variable							
Setze Profile							

SignalisierungsvariableWe
rt var2
Signalisierungsheader für
Profile festlegen
Festlegen von Profilen
Signalisierungsvorgang
Hinzufügen
Signalisierung von Profilen festlegen

headerPosition zuletzt
Setzen Sie Profile, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 15 vom Typ Variable
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 15 von variableValue var2
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 15 auf den Typ header
Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 , Aktion 15 , auf Wert Cisco-Guid
begehen
set profiles, die sipAdaptorProfile UCM_OUTBOUND Status aktiviert Commit
signalisieren

Beispiel für ausgehende SMM-Regeln für den Rekorder

konfigurieren

set profiles signalisieren sipAdaptorProfile applyMatchHeader all	RECORDER_OUTBOUND	Regel 1		
set-Profile-Signalisierung sipAdaptorProfile-Typmeldung	RECORDER_OUTBOUND	Regel 1	Kriterium	1
set profiles signalisieren sipAdapterorProfile message messageTypes all	RECORDER_OUTBOUND	Regel 1	Kriterium	1
set-Profile , die sipAdaptorProfile-Typ messageBody signalisieren	RECORDER_OUTBOUND	Regel 1	Kriterium	2
set-profile-signalisierung sipAdaptorProfile-NachrichtKörperbedingung regex-match	RECORDER_OUTBOUND	Regel 1	Kriterium	2
set profiles signaling sipAdaptorProfile messageBody regexp string cisco-guid=.* set	RECORDER_OUTBOUND	Regel 1	Kriterium	2
profiles signaling sipAdaptorProfile messageBody regexp numMatch match	RECORDER_OUTBOUND	Regel 1	Kriterium	2

profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1 type messageBody
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1 Vorgang regstore
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1 vom Typ messageBody
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1

from messageBodyValue all
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 1 Aktion 1 auf den Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 1 Aktion 1 auf variableValue var1
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1 regulärer Ausdruck Zeichenfolge "cisco-guid=.*?(? =; -Tag)"
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1 regulärer Ausdruck matchInstance last
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 2 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 2 Vorgang regdel
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 2 vom Typ variable
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 2 von variableValue var1
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 1 Aktion 2 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 2 auf variableValue var1 festlegen
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 2 reguläre Ausdruckszeichenfolge cisco-guid=
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 4 Typ Header
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 4 Vorgang hinzufügen
profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 1 Aktion 4 headerLetzte Position
profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 1 Aktion 4 vom Typ variable
profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 1 Aktion 4 von variableValue var1
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 1 Aktion 4 auf den Typ header
Profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 4 auf Wert Cisco-Guid festlegen
Festlegen von Profilen, die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 2 Kriterium 1

Nachricht eingeben

set profiles signalisieren sipAdaptorProfile messageTypes request | RECORDER_OUTBOUND | Regel 2 | Kriterium 1

set-profile , die sipAdaptorProfile-Nachrichtenmethode-Typen invite signalisieren | RECORDER_OUTBOUND | Regel 2 | Kriterium 1

set-Profile-Signalisierung sipAdapterprofile-Typ-Header | RECORDER_OUTBOUND | Regel 2 | Kriterium 2

profile signalisieren sipAdaptorProfile-Headername cisco-guid | RECORDER_OUTBOUND | Regel 2 | Kriterium 2

set-Profile-Signalisierung sipAdapterorProfile-Header-Bedingung fehlt | RECORDER_OUTBOUND | Regel 2 | Kriterium 2

profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Aktion 1 Typ Variable

Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 2 Aktion 1 Vorgang speichern

set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Aktion 1 vom Typ value

profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 2 Aktion 1 aus dem Wert cisco-guid

Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 2 Aktion 1 auf den Typ variable

Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 2, Aktion 1 auf variableValue var1

Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 3 applyMatchHeader all

profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Kriterium 1 Typ Nachricht

set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Kriterium 1 Nachricht messageTypes all

profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Kriterium 2 Typ messageBody

Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Kriterium 2 messageKörperbedingung regex-match

set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Kriterium 2 messageBody regexp string cisco-guid=.*

Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 3 Kriterium 2 messageBody regexp numMatch Match

profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Aktion 1

Typ Variable
profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 3 Aktion 1 Vorgang speichern
Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Aktion 1 vom Typ Wert
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 3 Aktion 1 aus dem Wert cisco-guid
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 3 Aktion 1 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Aktion 1 auf variableValue var10 setzen
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Kriterium 1 Typ Variable gesetzte Profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Kriterium 1 variable Bedingung fehlt
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Kriterium 1 Variable variableID var10
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 1 type messageBody
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 1 Vorgang regstore
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 1 vom Typ messageBody
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 1 von messageBodyValue all
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 1 auf den Typ variable
Setzen Sie Profile, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 1 auf variableValue var2
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 1 Regexp-Zeichenfolge <callid>.*</callid>
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 1 regulärer Ausdruck matchInstance eins
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 2 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 2 Operation regdel
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 2 auf

Typ Variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4, Aktion 2 auf variableValue var2
Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 2 Regexp-Zeichenfolge <callid>
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 2 regulärer Ausdruck matchInstance eins
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 3 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 3 Operation regdel
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 3 auf den Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 3 auf variableValue var2
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 3 regulärer Ausdruck Zeichenfolge @.*
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 3 regexp matchInstance one
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 4 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 4 Vorgang speichern
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 4 vom Typ Variable
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 4 aus variableValue var2
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 4 auf den Typ variable festlegen
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 4 auf variableValue var3 setzen
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 5 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 5 Operation regdel
Setzen Sie Profile, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 5 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 5 auf

variableValue var2
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 5 reguläre Ausdruckszeichenfolge _.*
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 5 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 6 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 6 Operation regdel
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 6 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 6 auf variableValue var3 setzen
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 6 reguläre Ausdruckszeichenfolge .*_
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 6 regulärer Ausdruck matchInstance one
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 7 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 7 Operation regappend
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 7 vom Typ Wert
Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 7 ab Wert 000000000
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 7 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 7 auf variableValue var2 setzen
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 7 reguläre Ausdruckszeichenfolge ^
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 7 regexp matchInstance one
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8 Operation regappend
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8

Von Typ Wert
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8 ab Wert 000000000
Setzen Sie Profile, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 8 auf den Typ Variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4, Aktion 8 auf variableValue var3
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8 reguläre Ausdruckszeichenfolge ^
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8 regexp matchInstanz eins
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 9 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 9 Operation regpredel
Legen Sie Profile fest , die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 9 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 9 auf variableValue var2 setzen
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 9 reguläre Ausdruckszeichenfolge $
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 9 regulärer Ausdruck matchInstance eins
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 10 Typ Variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 10 Operation regpredel
Setzen Sie Profile, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 10 auf den Typ Variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 10 auf variableValue var3 setzen
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 10 reguläre Ausdruckszeichenfolge $
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 10 regexp matchInstance one
set profiles signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 11 Typ Variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 11

Operation anhängen
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 11 vom Typ Wert
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 11 von Wert -
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 11 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 11 auf variableValue var2 setzen
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 12 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 12 Vorgang anhängen
Setzen Sie Profile, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 12 vom Typ Variable
Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 12 von variableValue var3
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 12 auf den Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 12 auf variableValue var2
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 13 Typ Variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 13 Vorgangsspeicher
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 13 vom Typvariable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 13 von variableValue var2
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 13 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 13 auf variableValue var3 setzen
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 14 Typ Variable
profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 4 Aktion 14 Vorgang anhängen
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 14

Von Typ Wert
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 14 aus Wert
-
Setzen Sie Profile, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 14 auf den Typvariable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 14 auf variableValue var2 festlegen
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 15 Typ Variable
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 15 Vorgang anhängen
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 15 vom Typ variable
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 15 von variableValue var3
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 15 auf den Typ variable
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 15 auf variableValue var2 setzen
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 16 Typ Header
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 16 Vorgang hinzufügen
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 16 headerLetzte Position
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 16 vom Typ Variable
profile festlegen , die sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 16 von variableValue var2 signalisieren
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 16 auf den Typ header
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 16 auf Wert Cisco-Guid
begehen
set profiles, die signalisieren, dass sipAdaptorProfile RECORDER_OUTBOUND Status aktiviert ist Commit aktiviert

| **Plattform-**

Installation

In diesem Abschnitt wird beschrieben, wie die verschiedenen Komponenten von Webex WFO installiert werden.

Installieren des Datenservers

Ein Mandantenadministrator kann den Datenserver für einen einzelnen Besitzer installieren, oder ein Systemadministrator kann einen Basisdatenserver installieren und ihn als gemeinsam genutzten Datenserver für mehrere Besitzer konfigurieren. Nachdem Sie den Webex WFO Datenserver installiert haben, können Sie ihn auf der Seite "Datenserverkonfiguration" unter "Anwendungsverwaltung" > "globale >Systemkonfiguration" > "Datenserverkonfiguration" weiter konfigurieren.

BEST PRACTICE Benutzer mit Edge-Geräten sollten einen regelmäßigen Zeitplan für den Download und das Upgrade ihrer Webex WFO-Datenserver auf die neueste Version der Webex WFO-Software festlegen. In der Regel wird jede Cloud
Enthält eine neue Version der Webex WFO Data Server-Software, die Benutzer von ihrem Mandanten herunterladen können.

Wenn Ihre Organisation über eine der folgenden Integrationen verfügt, finden Sie im Integrationsleitfaden dieser ACD zusätzliche Datenserverkonfigurationen, die für die ACD spezifisch sind.

- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express (Unified CCX)
- Cisco Webex Contact Center

Voraussetzungen

Wenn ein Datenserver eine Verbindung über einen Web-Proxy herstellen muss, muss jeder Datenserverdienst für die Verwendung eines Dienstkontos konfiguriert sein. Dies betrifft die folgenden Windows-Dienste:

- Webex WFO CTI Signalisierungsdienst
- Webex WFOData-Server
- Webex WFO Netzwerkaufzeichnungsdienst
- Webex WFO SIPREC Service
- Webex WFO Datenserver-Webdienste

Informationen zu den Anforderungen an die

Portnutzung finden Sie unter Portnutzung.

Installieren des Datenservers für einen einzelnen Tenant

Ein Besitzeradministrator kann den Datenserver für einen einzelnen Besitzer installieren.

Installieren des Datenservers für einen einzelnen Tenant

1. Öffnen Sie auf dem Server, auf dem Sie den Datenserver installieren möchten, einen Browser, und melden Sie sich mit den Anmeldeinformationen des Mandantenadministrators bei Webex WFO an.
2. Klicken Sie auf der **Seite "Downloads** " (Anwendungsverwaltung > -verwaltung > "Downloads") auf den entsprechenden Link, um das Data Server-Installationsprogramm herunterzuladen.
3. Folgen Sie den Ansagen.

Den Datenserver testen

1. Melden Sie sich bei Webex WFO als Mandantenadministrator an.
2. Wählen Sie auf der **Seite "Agentenüberwachung** " (Anwendungsverwaltung > "Überwachung" > "Agentenüberwachung") im Abschnitt "Datenserverprotokolle" den Datenserver aus, und klicken Sie auf **"Protokolle** abrufen". Wenn die Protokollanforderung erfolgreich ist, wird eine Verbindung mit dem Datenserver hergestellt.

   HINWEIS Dies kann einige Minuten dauern.

Datenserver für mehrere Besitzer installieren

Ein Systemadministrator kann einen Datenserver so konfigurieren, dass er von mehreren Tenants gemeinsam genutzt wird. Jedes Mal, wenn ein gemeinsam genutzter Datenserver aktualisiert wird (z. B. wenn ein neuer Besitzer hinzugefügt wird), müssen Sie seine Konfiguration aktualisieren. Dies erfolgt über die Data Server Updater-Datei, die generiert wird, wenn Sie Ihre Änderungen speichern und sich für den Download der Konfiguration entscheiden.

Um einen Datenserver für mehrere Besitzer zu konfigurieren, muss ein Systemadministrator einen Basisdatenserver installieren und anschließend den Basisdatenserver als gemeinsam genutzten Datenserver konfigurieren. Systemadministratoren können einen Basisdatenserver über die Seite "Anwendungsverwaltung > -Downloads" oder "Anwendungsverwaltung > gemeinsam genutzten Datenserver" herunterladen.

Installieren des Basisdatenservers

Als Erstes müssen Sie den Base Data Server herunterladen und installieren. Dieser Basisdatenserver wird nach seiner Konfiguration zu einem gemeinsam genutzten Datenserver. Sie können mehrere Basisdatenserver installieren.

1. Klicken Sie im **Abschnitt Download Base Data Server** auf **Calabrio ONE Data Server**. Dadurch wird die CalabrioONEDataServerSetup.exe Datei auf Ihren Computer heruntergeladen.
2. Doppelklicken Sie auf die ausführbare Datei, um den Assistenten für das Datenserver-Setup zu starten.

3. Befolgen Sie die Anweisungen des Assistenten, um die Installation abzuschließen.

Konfigurieren des Basisdatenservers

Als Nächstes konfigurieren Sie den Basisdatenserver als gemeinsam genutzten Datenserver.

1. Wählen Sie Neue Konfiguration zum Datenserver **hinzufügen aus**.

   HINWEIS Um eine vorhandene Konfiguration zu bearbeiten, wählen Sie **vorhandene Datenserverkonfiguration** bearbeiten und wählen Sie den Datenserver aus, den Sie bearbeiten möchten.

2. Füllen Sie die Felder gemäß der Definition in der folgenden Tabelle aus.

Feld	Beschreibung
Servername	Geben Sie einen Namen für den Datenserver ein.
Calabrio ONE-Server ein, der	Geben Sie die IP Adresse oder den Hostnamen des Webex WFO-Servers Hostet den Datenserverdienst.
Port	Geben Sie die Portnummer des Servers ein, auf dem der Datenserver-Service gehostet wird. Der Standardport ist 443.
Verfügbar	Eine Liste der verfügbaren Besitzer.
Zugewiesen	Eine Liste der Besitzer, die diesem Data Server-Service zugewiesen sind.

3. Klicken Sie auf " **Konfiguration** speichern/herunterladen", um die Konfiguration zu speichern und das Konfigurationsprogramm (CalabrioONEDataServerUpdaterSetup.exe) auf Ihren Computer herunterzuladen.

   HINWEIS: Sie können auch auf Speichern **klicken** , um die Konfiguration zu speichern, ohne das Konfigurationsprogramm herunterzuladen. Sie können diese Option wählen, wenn Sie die Konfiguration des Datenservers noch nicht abgeschlossen haben, aber die unvollständige Konfiguration speichern möchten.

4. Doppelklicken Sie auf die ausführbare Datei des Konfigurationsprogramms, um den Setup-Assistenten für Data Server Updater zu starten.

5. Befolgen Sie die Anweisungen des Assistenten, um die Konfiguration des gemeinsam genutzten Datenservers abzuschließen.

Cisco Unified Call Manager-Benutzer

Wenn Sie Cisco Unified Call Manager (UCM) verwenden, um CDRs über SFTP zu erfassen, müssen Sie möglicherweise die Systemeigenschaft Data Server Service festlegen, um die Schlüsselaustauschalgorithmen (KEX) zwischen Webex WFO und unterstützten Versionen von Cisco UCM abzugleichen.

Diese Kex-Algorithmen erfordern keine zusätzliche Konfiguration:

- ECDH-SHA2-NISTP521
- ECDH-SHA2-NISTP384
- diffie-hellman-group-exchange-sha256

Diese Algorithmen erfordern eine zusätzliche

Konfiguration:

- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha1

Legen Sie die Systemeigenschaft Data Server Service fest, um die zulässigen KEX-Algorithmen anzugeben

1. Navigieren Sie auf dem Server CDR SFTP zu
   C:\Program Files\Common Files\Calabrio ONE\Data Server\config
2. Öffnen Sie die Datei dataGatheringService.properties.
3. Suchen Sie die Zeile, die mit **service4j.jvmOptions** beginnt, und fügen Sie den folgenden Text am Ende der Zeile hinzu: **| -Dsftp.KexAlgorithms=diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1**
4. Speichern Sie die Datei, und starten Sie den Datenserverdienst Webex WFO neu.

HINWEIS Wenn Sie ein Upgrade auf eine neuere Version von Cisco UCM durchführen, die keinen dieser Kex-Algorithmen unterstützt, müssen Sie diese Systemeigenschaft neu konfigurieren, um die neuen unterstützten Algorithmen anzugeben.

Installieren von Smart Desktop

Webex WFO Smart Desktop kann auf drei Arten auf dem Computer eines Agenten installiert werden:

- Manuell auf den Computern der einzelnen Agenten
- Verwenden von Gruppenrichtlinienobjektskripts (Group Policy Object, GPO)
- Parameter für unbeaufsichtigte Befehle verwenden

HINWEIS Wenn Sie möchten, dass Smart Desktop Desktop-Analysen erfasst, muss für die Agentenrolle die Berechtigung "Desktop-Analysen erfassen" aktiviert sein, bevor Smart Desktop installiert wird. Wenn die Berechtigung
Nicht aktiviert sind, sind die Capture-Plug-Ins nicht auf dem Client-Desktop installiert.

Weitere Überlegungen

- Sie benötigen ein Desktop Analytics-Plug-in/eine Desktop-Analyse-Erweiterung, wenn Sie die Desktop Analytics-Funktion verwenden oder anhalten und fortsetzen möchten.
- Browsererweiterungen für Chrome und Edge müssen über ein Gruppenrichtlinienobjekt oder einen anderen Prozess bereitgestellt werden, den die lokale IT-Abteilung verwendet. Browsererweiterungen werden für Analysen sowie für das Anhalten und Fortsetzen benötigt.
- Cisco stellt die exe-Basisdatei bereit. Es liegt in der Verantwortung des Kunden, die Datei in eine MSI-Datei zu konvertieren.
- Bei der Installation über SCCM oder Microsoft Endpoint Configuration Manager sind Sie als Kunde für die Erstellung des Pakets für die Bereitstellung verantwortlich.
- Cisco bietet die Möglichkeit, die Software automatisch zu aktualisieren. Wenn Ihr Paketierungsteam Desktopversionen oder Microsoft Endpoint Configuration Manager verwaltet und diese die automatischen Updates stören, kann Cisco das Feature für automatische Updates TURN, und Ihr Team kann alle drei bis sechs Monate eine neue Version der Software herunterladen und über einen Paket-Push bereitstellen.
- Ihr Team kann die Abfragen in der Microsoft-Software so ändern, dass Versionsnummern oder eindeutige Bezeichner nicht verwaltet werden, wenn die Gruppe automatische Aktualisierungen beibehalten möchte.

  HINWEIS Automatische Updates müssen deaktiviert werden, wenn Ihr Unternehmen Citrix- oder Terminalserver verwendet. Es gibt keine Möglichkeit, verschiedene Umgebungen zu trennen.

- Wenn Sie ein Upgrade von Webex WFO Version 11.5 On-Premise auf Webex WFO Cloud durchführen, benötigen Sie drei Testcomputer. Eine Maschine ist für eine manuelle Installation vorgesehen. Die zweite Maschine ist für eine automatische Installation auf einer sauberen Maschine. Der dritte Computer ist für die vorhandene Version 11.5 von Webex WFO vorgesehen, um das von Ihrem IT-Team erstellte Deinstallationspaket und das Installationspaket für Webex WFO Cloud zu testen. Stellen Sie dem Implementierungsingenieur eine Liste aller auf dem Computer installierten Pakete einschließlich Browsererweiterungen zur Verfügung. Arbeiten Sie mit Ihrem IT-Team zusammen, um die gesamte Webex WFO Version 11.5-Software zu entfernen, bevor Sie Webex WFO Cloud installieren.
    - Wenn Ihr Unternehmen den Anbieter von einer anderen Workforce Engagement Management (WEM)-Lösung (z. B. Verint oder Nice) auf Webex WFO umstellt, arbeiten Sie mit Ihrem IT-Team zusammen, um die Originalsoftware auf einem dritten Testcomputer zu deinstallieren und das von Ihrem Team erstellte automatisierte Paket bereitzustellen.
- Wenn Sie eine Version von 11.5 On-Premise auf eine neuere Version von 11.5 aktualisieren,

müssen Sie eine neue Version von Smart Desktop erneut herunterladen und erneut bereitstellen.

Manuelle Installation

Gehen Sie wie folgt vor, um Smart Desktop manuell auf dem Computer eines Agenten oder auf einem Thin Client-Server zu installieren. Stellen Sie sicher, dass alle Browser vor der Installation geschlossen sind, und verwenden Sie den Task-Manager, um sicherzustellen, dass Ihre Browser nicht im Hintergrund ausgeführt werden.

Smart Desktop manuell installieren

1. Melden Sie sich am Computer des Agenten oder auf dem Thin Client-Server mit Administratoranmeldeinformationen bei Webex WFO an.
2. Klicken Sie auf der Seite "Downloads" (Application Management > Global > Administration > Downloads) auf den Link für das **Calabrio ONE Smart Desktop-Installationsprogramm** . Webex WFO stellt eine .exe Datei für die manuelle Installation bereit.
3. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), wenn Sie dazu aufgefordert werden.
4. Führen Sie das Installationsprogramm aus und befolgen Sie die Anweisungen des Installationsassistenten.
5. Aktivieren Sie das **Kontrollkästchen "Aktivieren** ", wenn Sie dazu aufgefordert werden, und klicken Sie auf **"Fertig stellen**".
6. Nachdem Sie das Smart Desktop-Installationsprogramm ausgeführt haben, starten Sie Ihr System neu.
7. Führen Sie das Clientüberprüfungstool aus. Weitere Informationen finden Sie unter Clientüberprüfungstool .
8. Testen Sie Smart Desktop. Weitere Informationen finden Sie unter Testen von Smart Desktop .

Installation mit GPO

Ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) ist eine Sammlung von Einstellungen, die definieren, wie ein System aussieht und wie es sich für eine definierte Benutzergruppe verhält. Microsoft stellt ein Programm-Snap-In bereit, mit dem Sie die Gruppenrichtlinie Microsoft Management Console verwenden können, um verschiedene Optionen, einschließlich Skriptoptionen, zu definieren. Weitere Informationen finden Sie unter Rückgabecodes für die Push-Installation, die nach dem Pushen des Clients erforderlich sind.

Bereitstellen von Smart Desktop mithilfe von GPO

1. Melden Sie sich mit Ihren Administratoranmeldeinformationen bei Webex WFO an.
2. Klicken Sie auf der Seite "Downloads" (Application Management > Global > Administration > Downloads) auf den Link für das **Calabrio ONE Smart Desktop-Installationsprogramm** . Webex WFO stellt eine .exe Datei für die manuelle Installation bereit.
3. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), wenn Sie dazu aufgefordert werden.
4. Kopieren Sie **CalabrioONEDesktopSetup_<TenantName>.exe aus dem Ordner "Downloads",** und fügen Sie ihn in den Speicherort für die Serverfreigabe ein.

5. Erstellen Sie zum Ausführen des Installationsprogramms ein Batchskript, das das folgende Skript enthält:

   <Hostname oder IP Adresse des Freigabeorts des Servers>\CalabrioONEDesktopSetup_<TenantName>.exe /LOG /VERYSILENT /ACTIVATE /NORESTART/NONPCAP

6. Starten Sie den Gruppenrichtlinienverwaltungs-Editor, navigieren Sie zu Computerkonfiguration > Richtlinien > Windows-Einstellungen >-Skripts (Starten/Herunterfahren), und fügen Sie das Batchskript hinzu.

Installieren Sie Smart Desktop mit den Parametern des unbeaufsichtigten Befehls

Mit unbeaufsichtigten Parametern können Sie Webex WFO über Ihre Befehlszeilenschnittstelle installieren. Siehe "Einrichten von Befehlszeilenparametern" in https://jrsoftware.org/ishelp/index.php?topic=setupcmdline für Optionen. Zu den häufig verwendeten Befehlen gehören die folgenden.

- /LOG
- /SEHRSILENT
- /AKTIVIEREN
- /NORESTART
- /NONPCAP

Replizieren einer Installation mit Desktop-Imaging

Nachdem Sie den Smart Desktop Record Service mit einer der vorherigen Installationsmethoden (siehe Manuelle Installation oder Installation mit GPO) auf einem PC installiert haben, können Sie diese Installation auf mehreren PCs replizieren, indem Sie ein generisches Systemabbild erstellen, das über mehrere Hardwaredesigns hinweg verwendet werden kann. Wenn Smart Desktop auf einem PC für das Imaging installiert wird, müssen einige Informationen entfernt werden, damit das Image auf verschiedenen PCs ausgeführt werden kann, ohne Probleme zu verursachen.

empfohlene Methode: Cisco's System Preparation Hook

Um PC-spezifische Informationen aus einer Windows-Installation zu entfernen und zu "verallgemeinern", damit sie auf verschiedenen PCs installiert werden können, empfehlen wir dringend, den Systemvorbereitungs-Hook (sysprep) von Cisco zu verwenden. Sysprep ist das Systemvorbereitungstool von Microsoft, mit dem ein Systemabbild für die Bereitstellung auf mehreren PCs vorbereitet wird.
Sysprep bereitet eine Windows-Installation (Windows-Client und Windows Server) für das Image vor, sodass Sie eine benutzerdefinierte Installation erfassen können. Der Sysprep-Hook wird mit Smart Desktop installiert und automatisch beim System registriert. Wenn Sie sysprep ausführen, werden automatisch alle im System registrierten Hooks aufgerufen.

Sekundäre Methode: Manuelles Konfigurieren des Bildes

Wenn Sie Sysprep nicht verwenden können, müssen Sie die folgenden Schritte manuell für jedes Image ausführen, in dem der Smart Desktop Record Service installiert ist, bevor Sie dieses Image auf zusätzlichen PCs bereitstellen.

WICHTIG Wenn Sie diese Schritte ausführen möchten, lesen Sie dieses Dokument regelmäßig, um sich über Änderungen an diesen Schritten auf dem Laufenden zu halten.

1. Beenden Sie den Smart Desktop Record-Dienst.
2. Öffnen Sie den Ordner "log", in dem der Smart Desktop Record Service installiert ist (standardmäßig C:\Program Files (x86)\Calabrio ONE\Desktop\Active\log), und entfernen Sie alle Dateien, die nicht das Wort "postinstall" enthalten.
3. Entfernen Sie alle Unterordner (einschließlich ihres Inhalts) aus dem Ordner "log".
4. Öffnen Sie "C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop\config" und entfernen Sie alle Dateien außer "Install.ini" und "sysproperties.cfg".
5. Entfernen Sie alle Unterordner (einschließlich ihres Inhalts) aus dem Ordner "config".
6. Öffnen Sie "C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop\recordings" und löschen Sie alle Dateien und Unterordner (einschließlich ihres Inhalts). Der Ordner "Aufzeichnungen" muss leer sein.
7. Öffnen Sie "C:\Program Files (x86)\Common Files\Calabrio ONE\Desktop\chunks" und löschen Sie alle Dateien und Unterordner (einschließlich ihres Inhalts). Der Ordner "chunks" muss leer sein.

   HINWEIS Der Ordner "chunks" ist möglicherweise nicht vorhanden. Wenn der Ordner "chunks" nicht vorhanden ist, können Sie diesen Schritt überspringen.

Rückgabecodes für die Push-Installation

Wenn Sie eine Push-Installationsmethode (z. B. GPO) verwenden, erhalten Sie Rückgabecodes, die den Erfolg oder Fehler der Installation angeben. Die möglichen Rückgabecodes werden im Folgenden beschrieben.

Rückgabecode	Beschreibung
0	Erfolgreiche Installation
1	Fehlgeschlagene Installation

Darüber hinaus werden Ereignisse in das Windows-Ereignisprotokoll geschrieben. Das Ereignisdetail enthält eine Beschreibung des Geschehens. Es werden drei verschiedene Ereignis-IDs geschrieben. Das Ereignis selbst enthält mehr Details, aber im Allgemeinen geben die IDs Folgendes an:

Veranstaltung ID	Beschreibung
8080	Erfolgreiche Installation

Veranstaltung ID	Beschreibung
8081	Fehlgeschlagene Installation
8084	Informationsmeldung

Die Details für eine erfolgreiche oder fehlgeschlagene Installation werden sowohl in das Windows-Ereignisprotokoll als auch in die Protokolle geschrieben, die im Wrapper-Ordner unter dem Smart Desktop Client-Installationsordner enthalten sind.

Client-Verifizierungstool

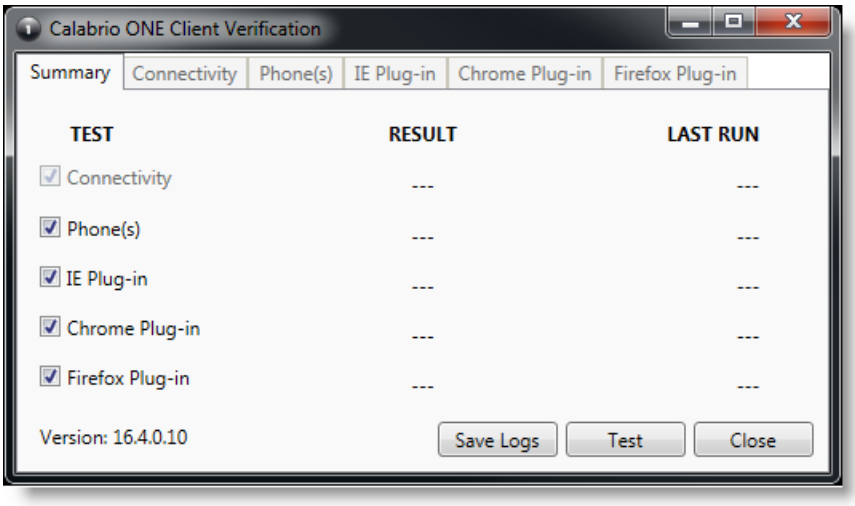
Das Clientüberprüfungstool testet den Client-PC, um sicherzustellen, dass die Konnektivität mit den Servern und dem Telefon für die Ausführung von Smart Desktop geeignet ist. Es wird installiert, wenn Smart Desktop installiert ist. Das Tool führt verschiedene Tests durch und meldet die Ergebnisse entweder als bestanden oder nicht bestanden.

Ausführen des Clientüberprüfungstools

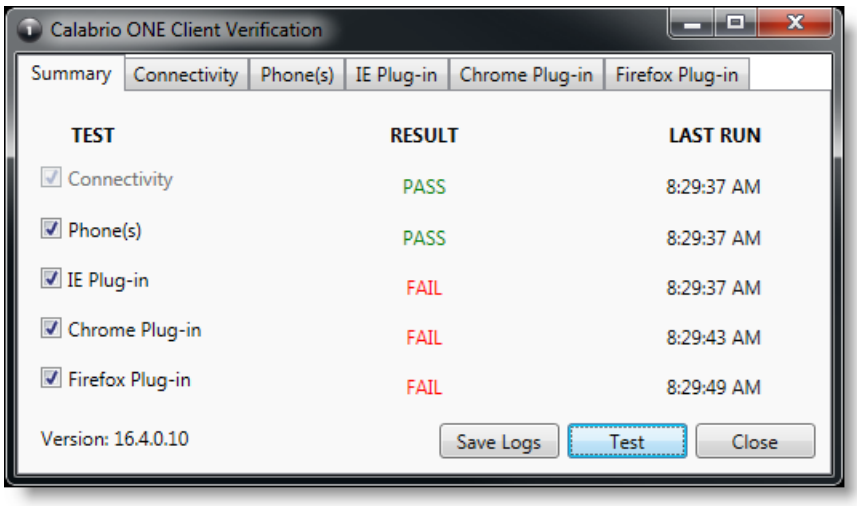
1. Navigieren Sie nach der Installation von Smart Desktop zum folgenden Ordner auf dem Client-PC:

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

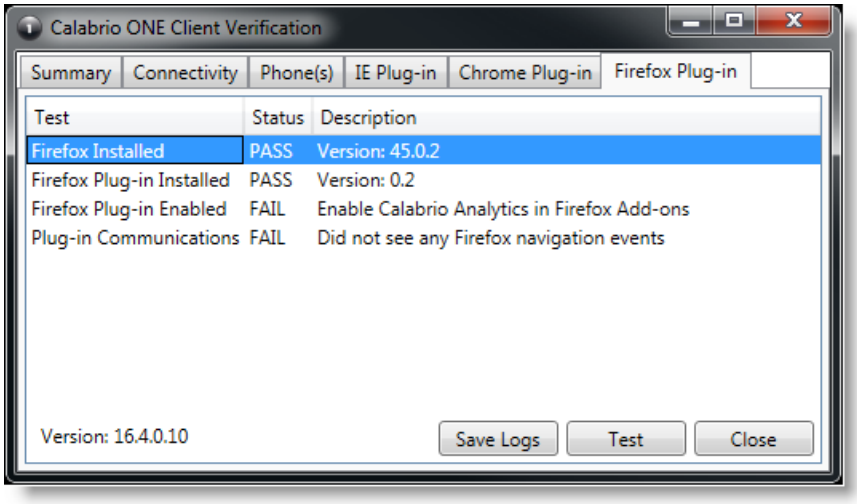
2. Doppelklicken Sie auf **ClientDiag.exe**. Das Clientüberprüfungstool wird gestartet.



3. Standardmäßig sind alle Tests ausgewählt. Klicken Sie auf Test .
4. Das Tool meldet die Ergebnisse des Tests als bestanden oder nicht bestanden.



5. Für jeden Test gibt es eine Tab, in der Details zum Test angezeigt werden. Wenn der Test fehlschlägt, geben die Details auf der Tab Hinweise darauf, was falsch ist.



6. Bei Bedarf können Sie auf Protokolle **speichern klicken** , um die Protokolle für Postinstall und Smart Desktop zu komprimieren und Probleme zu identifizieren. Die Protokolle werden automatisch in eine Datei mit dem Namen Clientlogs.zip komprimiert.

Steuerelemente für die Aufzeichnung

Die eigenständige Anwendung "Recording Controls" wird automatisch mit Smart Desktop installiert. Mit der Aufzeichnungssteuerung kann ein Agent die Aufzeichnung von Audio-, Bildschirm- und Tastenanschlägen für aktive Anrufe starten, anhalten, fortsetzen und beenden sowie Anrufe markieren und ihnen Metadaten hinzufügen.

Die Verwendung der Steuerelemente für die Aufzeichnung ist optional.

HINWEIS Die Anwendung "Aufzeichnungssteuerungen" wird von bestimmten Bereitstellungen von CCaaS-Anbietern nicht unterstützt.

Die ausführbare Datei von Recording Controls wird hier installiert:

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

Im Startmenü heißt die Anwendung Webex WFORecording Controls und befindet sich standardmäßig unter Webex WFO.

Entfernung

In den folgenden Themen wird beschrieben, wie Sie Webex WFO-Komponenten deinstallieren.

Deinstallieren von Webex WFO Smart Desktop

HINWEIS: Sie müssen sich als Administrator anmelden, um Smart Desktop deinstallieren zu können.

1. Öffnen Sie auf dem Desktop oder dem Thin Client-Server, auf dem Smart Desktop installiert ist, die Windows-Systemsteuerung.
2. Starten Sie das Dienstprogramm zum Hinzufügen oder Entfernen von Programmen .
3. Wählen Sie in der Liste die Anwendung aus, die Sie entfernen möchten, und klicken Sie auf Deinstallieren .

   Wenn Sie beabsichtigen, Smart Desktop neu zu installieren, nachdem Sie eine ältere Version vollständig entfernt haben (eine Neuinstallation), stellen Sie sicher, dass die Aufzeichnungsspeicherordnerstrukturen entfernt wurden, bevor Sie die neue Version installieren.

4. Starten Sie den Desktop oder den Thin Client-Server neu.

Deinstallieren mit GPO

Ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) ist eine Sammlung von Einstellungen, die definieren, wie ein System aussieht und wie es sich für eine definierte Benutzergruppe verhält. Microsoft stellt ein Programm-Snap-In bereit, mit dem Sie die Gruppenrichtlinie Microsoft Management Console verwenden können, um verschiedene Optionen, einschließlich Skriptoptionen, zu definieren.

1. Erstellen Sie zum Ausführen des Installationsprogramms ein Batchskript, das das folgende Skript enthält:

   ```
   <C:\Program Files (x86)\Calabrio ONE\Desktop\Wrapper\unins000.exe /LOG
       /VERYSILENT /NORESTART>
   ```

2. Starten Sie den Gruppenrichtlinienverwaltungs-Editor, navigieren Sie zu Computerkonfiguration > Richtlinien > Windows-Einstellungen >-Skripts (Starten/Herunterfahren), und fügen Sie das Batchskript hinzu.

WICHTIG: Dadurch wird das Schließen aller geöffneten Browser erzwungen. Wenn Browser erneut geöffnet werden, bevor die Deinstallation abgeschlossen ist, schlägt die Deinstallation möglicherweise fehl und muss neu gestartet werden.

Smart Desktop mit den Parametern des unbeaufsichtigten Befehls deinstallieren

Mit unbeaufsichtigten Parametern können Sie Webex WFO über Ihre Befehlszeilenschnittstelle deinstallieren.

Weitere Optionen finden Sie unter "Deinstallations-Befehlszeilenparameter" in https://jrsoftware.org/ishelp/index.php?topic=setupcmdline .