Webex WFO Cloud-Installationshandbuch

Für Bereitstellungen mit klassischem WFM

Erstveröffentlichung: 10. Juli 2020
Zuletzt aktualisiert: 28. Februar 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 Cisco-Website 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

Einleitung 7

Lokalisierung und unterstützte Sprachen 9

Systemkonfiguration 13

Unterstützte Umgebungen 15

Unterstützte Telefone 15

Harte Telefone 15

Unterstützte Codecs 15

Verwenden mehrerer SoftPhones 15

Unterstützte Mobilgeräte 16

Edge-Komponenten 17

Webex WFO Smart Desktop 18

Über Webex WFO Smart Desktop 18

Smart Desktop Client-Konnektivität 19

Anforderungen und Überlegungen zu Smart Desktop 20

Verwendung von Smart Desktop-Ports 22

Smart Desktop-Kontaktmetadaten 24

Smart Desktop Capture-Datenflussdiagramme 25

Smart Desktop testen 28

Smart Desktop verwalten 31

Anwendung "Aufzeichnungssteuerungen" 32

Webex WFO-Datenserver 34

Systemanforderungen 37

Desktop-Hardware 37

Desktop-Software 38

.NET Framework 38

Browser 38

Desktop Analytics-Plug-in/Erweiterung 38

Adobe Acrobat Reader 39

Desktop-Software und Audioaufnahme 39

Aktivieren Sie die Desktop Analytics-Erweiterung in Ihrem Browser 39

Thin Client-Server 40

Installieren des Thin Client-Servers 41

Portnutzung 42

Edge-Komponenten 43

Datenserver-Komponenten 43

Dateiverschlüsselung 48

Kennwortrichtlinie 48

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 WFO-Plattform (Workforce Optimization). Es umfasst die Möglichkeit, Anrufaufzeichnungen, Qualitätsmanagement, Workforce Management und Analysen durchzuführen.

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

Lokalisierung und unterstützte Sprachen

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

- Benutzeroberfläche
  - QM, WFM, Analysen und Einblicke
  - Produktinterne Schulungen
- Dokumentation
  - Online-Hilfe
  - PDF Leitfäden
- Analysen
  - Transkription: Sprache-zu-Text und Transkriptionssuche.
  - 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.

Komponenten von Webex WFO sind in diesen Sprachen verfügbar.

Sprache	UI	Mobil App	Produktinterne Schulungen	Analysen								Dokumentation
				Transkription*	Zusammenfassung der Interaktion	Phrasentreffer	Gefühl	Vorhersagen	Textanalyse	Trending Topics	Automatische QM	
Arabisch (ar-AR)				x	x	x		x				
Chinesisch (vereinfacht)	x		Begrenzt									
Chinesisch (zh-TW)	x		Begrenzt									
Dänisch (da)	x		Begrenzt	x	x	x		x	x			
Niederländisch (nl)	Begrenzt		Begrenzt	x	x	x		x	x			
Englisch (en)	x	x	x	x	x	x	x	x	x			x
Australisches Englisch (en-AU)				x	x	x	x	x	x			
Südafrikanisches Englisch (de-ZA)				x	x	x	x	x	x			
Englisch (GB) (en-GB)				x	x	x	x	x	x	x	x	
US-Englisch (en-US)	x	x	x	x	x	x	x	x	x	x	x	x

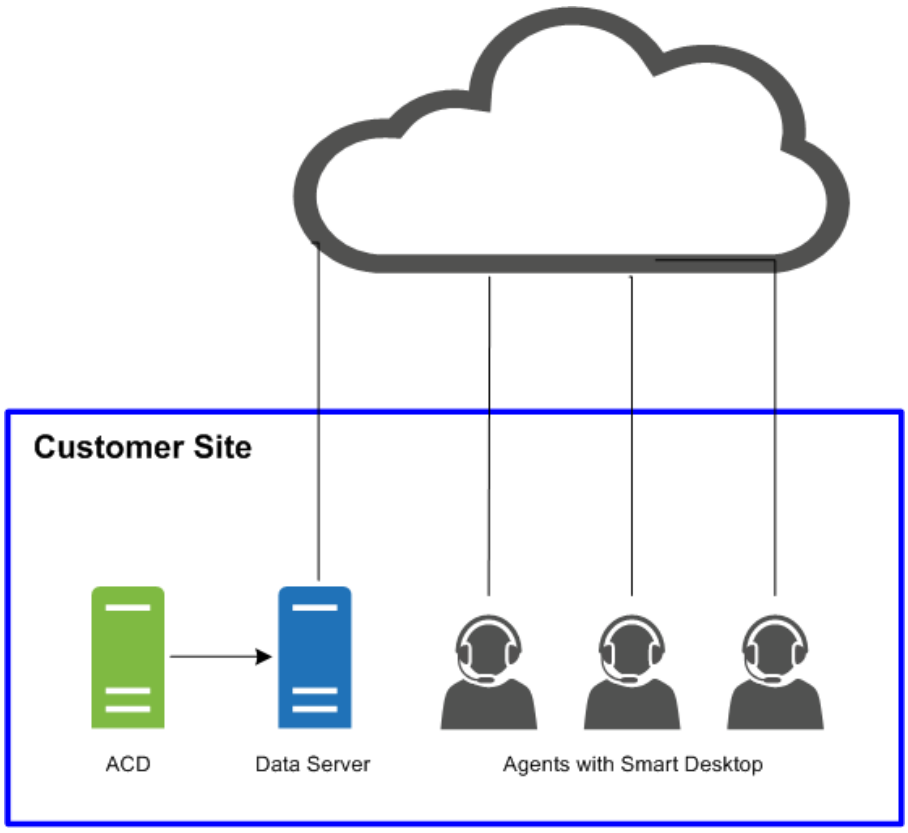
Sprache	UI	Mobil App	Produktinterne Schulungen	Analysen								Dokumentation
				Transkription*	Zusammenfassung der Interaktion	Phrasentreffer	Gefühl	Vorhersagen	Textanalyse	Trending Topics	Automatische QM	
Finnisch (fi)	x		Begrenzt	x	x	x		x				
Französisch (fr)	x		Begrenzt	x	x	x		x	x			Begrenzt
Kanadisches Französisch (fr-CA)	x			x	x	x		x	x			
Deutsch (de)	x		Begrenzt	x	x	x		x	x			Begrenzt
Italienisch (it)	x		Begrenzt	x	x	x		x	x			
Japanisch (ja)	x		Begrenzt									
Koreanisch (ko)	x		Begrenzt									
Norwegisch (nb)	x		Begrenzt	x	x	x		x	x			
Polnisch (pl)	Begrenzt		Begrenzt	x	x	x		x	x			
Portugiesisch (pt)	x		Begrenzt	x	x	x		x	x			
Portugiesisch (Brasilien) (pt-BR)	x		Begrenzt	x	x	x		x	x			

Sprache	UI	Mobil App	Im Produkt	Analysen								Dokumentatio
				Wechselwirkung Transkription*		Phrase Hits	Gefühl	Vorhersag	Text Analysen	Laufend Themen	Automati	
Russisch (ru)	Begrenzt											
	x		Begrenzt	x	x	x		x	x			Begren
Mexikanisches Spanisch (es-MX)				x	x	x		x	x			
	x		Begren	x	x	x		x	x			

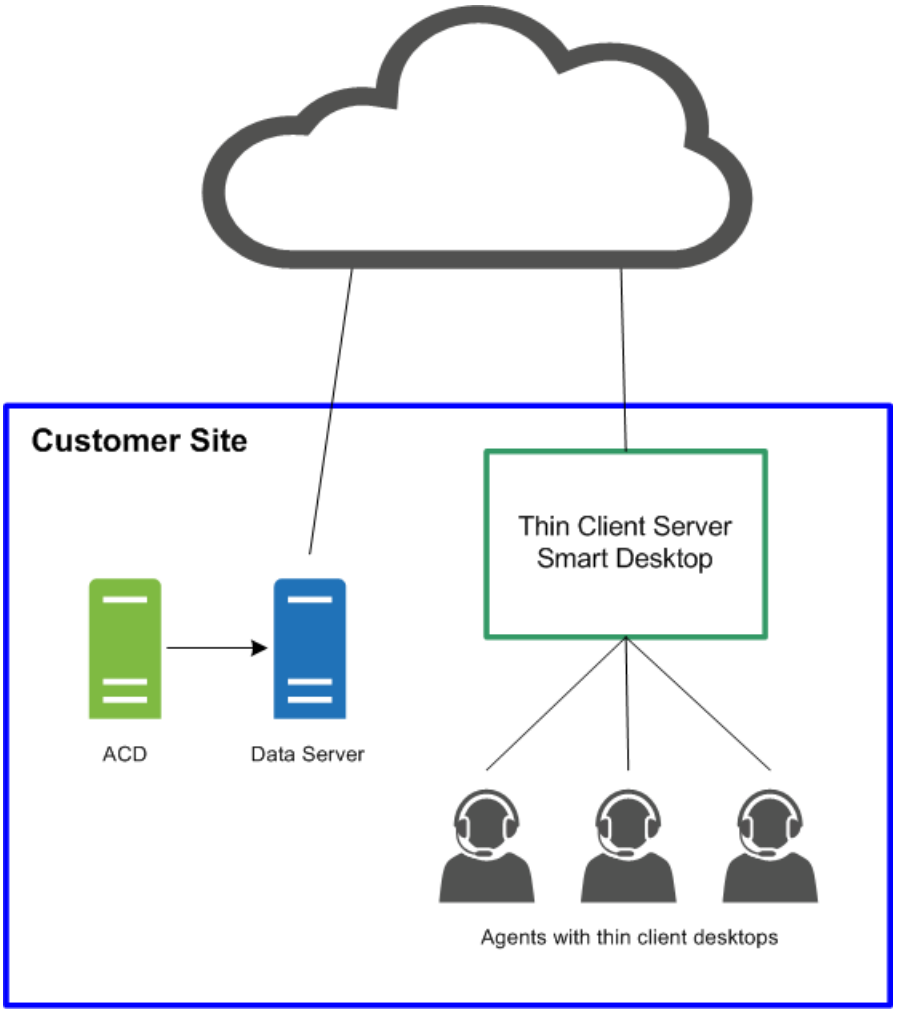
* Einige unterstützte Sprachen erfordern möglicherweise zusätzliche Konfigurationseinstellungen für Ihre Webex WFO-Implementierung. Wenden Sie sich an den Support, um sicherzustellen, dass die Sprache, die Sie transkribieren möchten, für Sie konfiguriert ist. Das Hinzufügen weiterer Sprachen oder die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

Systemkonfigura

Dieses Diagramm zeigt eine typische Webex WFO-Cloudbereitstellung.



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

Webex WFO unterstützt eine Reihe von Umgebungen und Technologien.

Die neuesten Informationen zur unterstützten Kompatibilität finden Sie unter www.cisco.com.

Unterstützte Telefone

Webex WFO unterstützt die folgenden Telefone.

Harte Telefone

Eine Liste der unterstützten Cisco Festplatten finden Sie auf der Website 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.

Verwenden mehrerer SoftPhones

Wenn Sie mehrere SoftPhones gleichzeitig verwenden, dürfen die SoftPhones nicht mit einer lokalen Portnummer verbunden werden, die mit einer der Portnummern übereinstimmt, die auf der Seite "allgemeine Einstellungen" (Anwendungsverwaltung > QM Konfiguration > allgemeine Einstellungen > SIP-Einstellungen) konfiguriert sind. Wenn beispielsweise die unter SIP-Einstellungen auf 5060 festgelegt ist, 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 ggf. an, und verwenden Sie eines dieser Tools, um die Netzwerkverbindungen für diese Prozess-ID anzuzeigen. Wenn für eine der Netzwerkverbindungen ein lokaler Port angezeigt wird, der mit einer der auf der Seite "allgemeine Einstellungen" konfigurierten

Portnummern übereinstimmt, müssen Sie einen der folgenden Schritte ausführen:

- Verwenden Sie das SoftPhone alleine, ohne dass gleichzeitig andere SoftPhones verwendet werden.
- Konfigurieren Sie das SoftPhone so, dass es keinen der aufgeführten Ports verwendet.

Um die Portverwendung zu bestätigen, verwenden Sie ein Tool, das Netzwerkverbindungen überwacht, z. B. netstat (verwenden Sie in der Befehlszeile Parameters-anob), TCPView oder CurrPorts.

Unterstützte Mobilgeräte

Agenten können auf einer eingeschränkten Version Webex WFO auf einem mobilen Gerät, z. B. einem Smartphone oder Tablet, zugreifen, indem sie die Webex WFO-URL im Browser des Geräts eingeben. Der Agent wird automatisch zu einer mobilen Version von Webex WFO umgeleitet, wo sich der Agent wie üblich anmeldet.

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

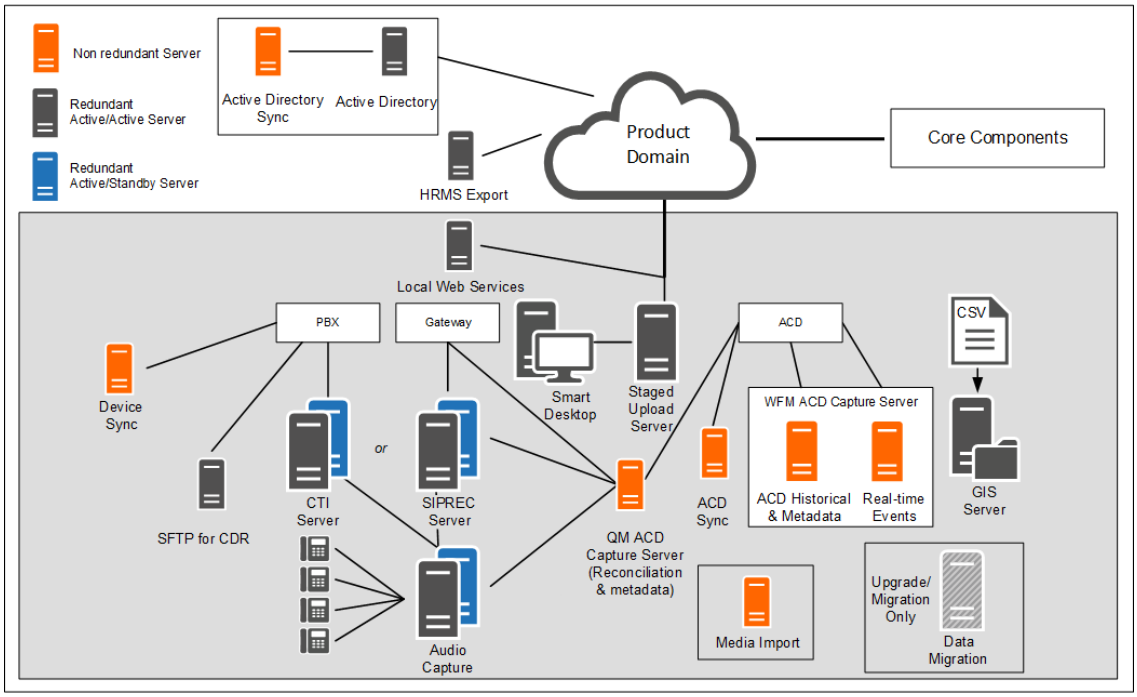
Agenten können ihre Zeitpläne auch außerhalb der Arbeit über einen E-Mail-Client oder eine Kalenderanwendung auf einem mobilen Gerät oder einem PC anzeigen. Der E-Mail-Client bzw. die Kalenderanwendung zeigt den Zeitplan so an, wie er auch in der Webex WFO-Oberfläche dargestellt wird. Dabei wird die iCalendar Datendatei aus dem WFM iCalendar-Service gelesen.

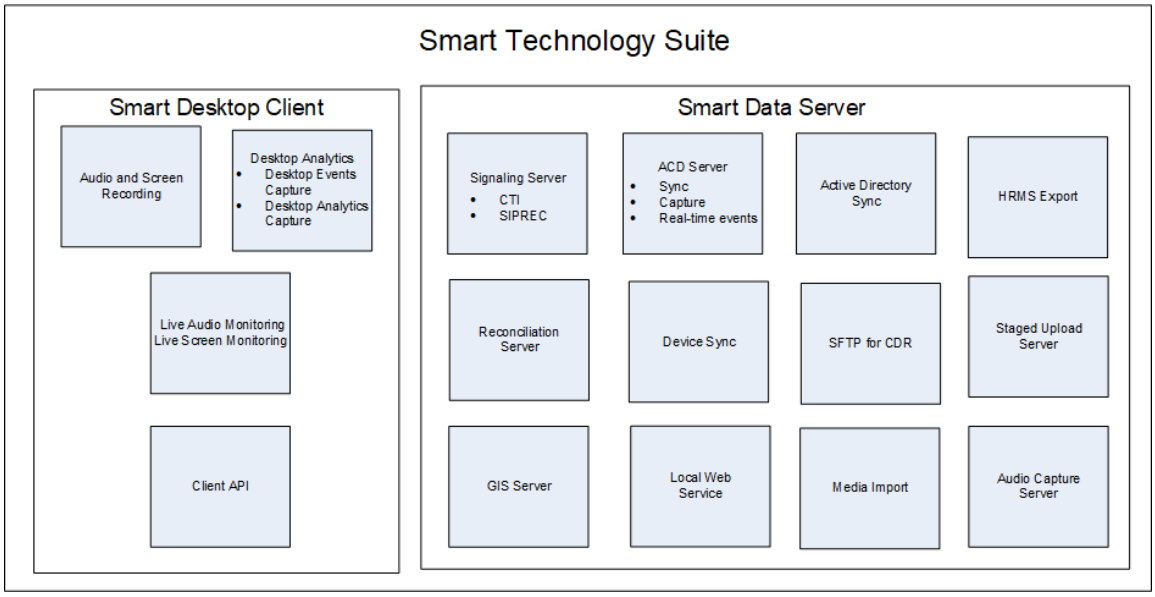
Die folgenden Clients und Geräte werden für die Anzeige eines Zeitplans außerhalb der Arbeit unterstützt:

- Apple-Geräte, z. B. iPhone oder iPad (in Verbindung mit der Apple Calendar-App)
- Microsoft Outlook
- Android-Geräte, z. B. ein Tablet oder Mobiltelefon (in Verbindung mit einer Kalender-App, die .ics Dateien lesen kann)

Edge-Komponenten

Die Webex WFO-Edgekomponenten werden in der Regel an einem lokalen Standort oder an einem Remotekundenstandort bereitgestellt. Die Komponenten als Ganzes bilden die Webex WFO Smart Technology Suite.





Webex WFO Smart Desktop

Webex WFO Smart Desktop erfasst alle Benutzerdaten (d. h. Audioaufzeichnungen, Bildschirmaufzeichnungen, Desktop-Aktivitäten und Anrufmetadaten) auf dem Desktop eines Agenten. Webex WFO-Smartdesktop wird auf Agentendesktops im Contact Center oder auf einem Server installiert, der einen unterstützten Thin Client hostet. Das Smart Desktop-Installationsprogramm 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 Lizenz und Berechtigungen, die in Webex WFO aktiviert sind, variieren. Sie müssen das Smart Desktop-Installationsprogramm von Application Management > Global > Administration > Downloads herunterladen (siehe Herunterladen von Smart Desktop). Außerdem benötigen Sie die Erweiterung "Desktop Analytics" für Ihren Browser.

Die Audioaufzeichnung mit Smart Desktop hängt vom Aufzeichnungstyp ab. CCaaS-Lösungen (Contact Center-as-a-Service) zeichnen Audio auf und senden die Datei, nachdem der Kontakt abgeschlossen ist. Vom Kunden gehostete Lösungen senden SIP- und RTP Protokolle, da der Kontakt live ist. Webex WFO führt Bildschirmaufzeichnungen über den Agent Desktop aus. Die Aufzeichnungen werden hochgeladen, nachdem ein Anruf beendet ist.

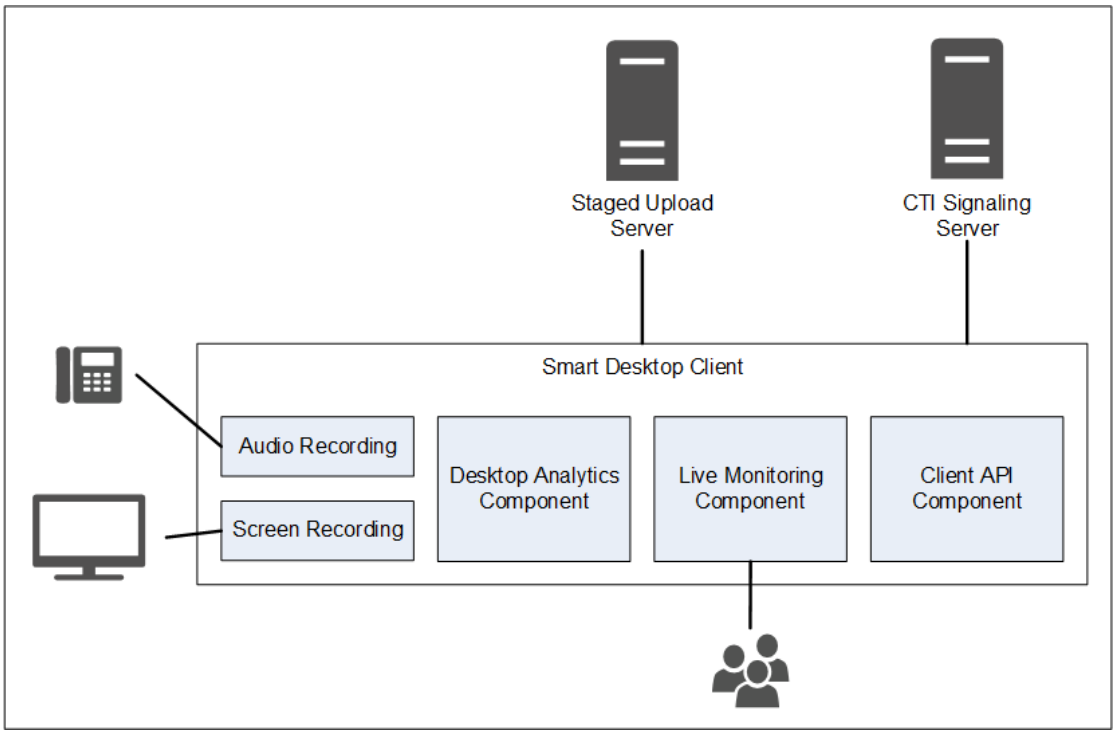
Smart Desktop besteht aus den folgenden Komponenten.

- Audio- und Bildschirmaufzeichnung: Diese Komponente zeichnet Agentenanrufe auf.
- Desktop-Analyse – Diese Komponente stellt Analysedaten zu Agentendesktop-Aufzeichnungen bereit.

- Live-Audioüberwachung und Live-Bildschirmüberwachung – Diese Komponenten ermöglichen es Supervisoren, das Audio eines Agenten anzuhören und den Bildschirm eines Agenten in Echtzeit anzuzeigen. Agentenüberwachung und Desktopüberwachung sind die beiden Überwachungstypen für Smart Desktop.

  Agentenüberwachung – Eine Funktion für Administratoren und Supervisoren, mit der sie den Ton und die Bildschirme von Agenten in Echtzeit überwachen können.

  Desktop-Überwachung – Eine Funktion, mit der Administratoren die aktiven und installierten Versionen von Smart Desktop auf ihren PCs anzeigen, Protokollebenen festlegen und Protokolle zur Fehlerbehebung aus der Ferne herunterladen können.



Smart Desktop Client-Konnektivität

In der folgenden Tabelle sind die grundlegenden Verbindungsmöglichkeiten zum Smart Desktop Client aufgeführt:

Komponente	Verbindet mit	Eingänge/Ausgänge
Audio- und Bildschirmaufzeichnung	PC des Agenten	Audio- und Bildschirmdaten des Telefons
Desktop-Analyse	PC des Agenten	Audio- und Bildschirmdaten des Telefons
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 .

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

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, würde die Aufzeichnung eines Screenshots wie folgt aussehen: 1,5 MB/Min. x 5 Minuten x 30 Anrufe x 3 Bildschirme = 675 MB.

Unter Desktop-Hardware 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 Infrastruktur (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:
Beendigungszeit
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 automatische Updatefunktion 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 unter 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 ein Windows-Gruppenrichtlinienobjekt verwalten, um sicherzustellen, dass alle abhängigen Features wie vorgesehen funktionieren.

Wenn Benutzer sowohl Microsoft Edge- als auch Google Chrome-Browser verwenden, 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 mit der Cisco Cloud über 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 zum 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 u. a. Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Express Avaya Communication Manager.

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	RTP wird aufgezeichnet	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	Gebrauchen	Quelle	Ziel	Anmerkungen
Intelligenter Desktop				
TCP 80, 443	Live-Bildschirmüberwachung	PC des Agenten	Browser des Supervisors	

Cloud 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:

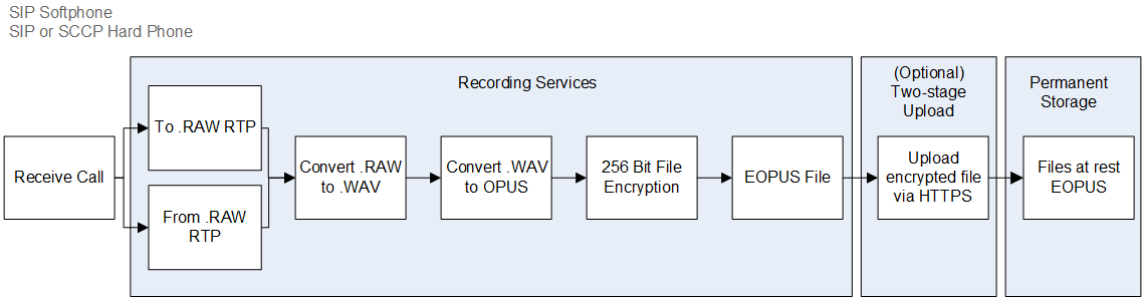
Kontakt-Metadaten	SIP-Signalisierung	SCCP Signalisierung	RTP Protokollierung
Anruf-ID	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC-API
ANI (Anruf)	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC-API
DNIS (angerufen)	X	X	Stützt sich auf Drittanbieter, um 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
Zugehörige Kontakt-ID	X		Verlassen Sie sich auf Drittanbieter, um Echtzeitdaten für DCC-API bereitzustellen
Aufzeichnungstyp	X	X	X
Dauer	X	X	Segmentbasiert, es sei denn, join_start wird verwendet
MAC-Adresse	X	X	
Benutzer (anhand der Windows-Anmelde-ID)	X	X	X
Datum/Uhrzeit des Anrufs	X	X	X

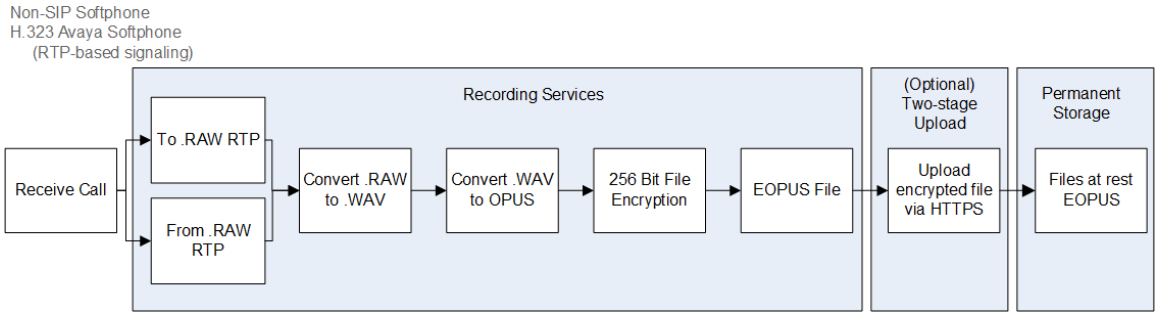
Smart Desktop Capture-Datenflussdiagramme

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

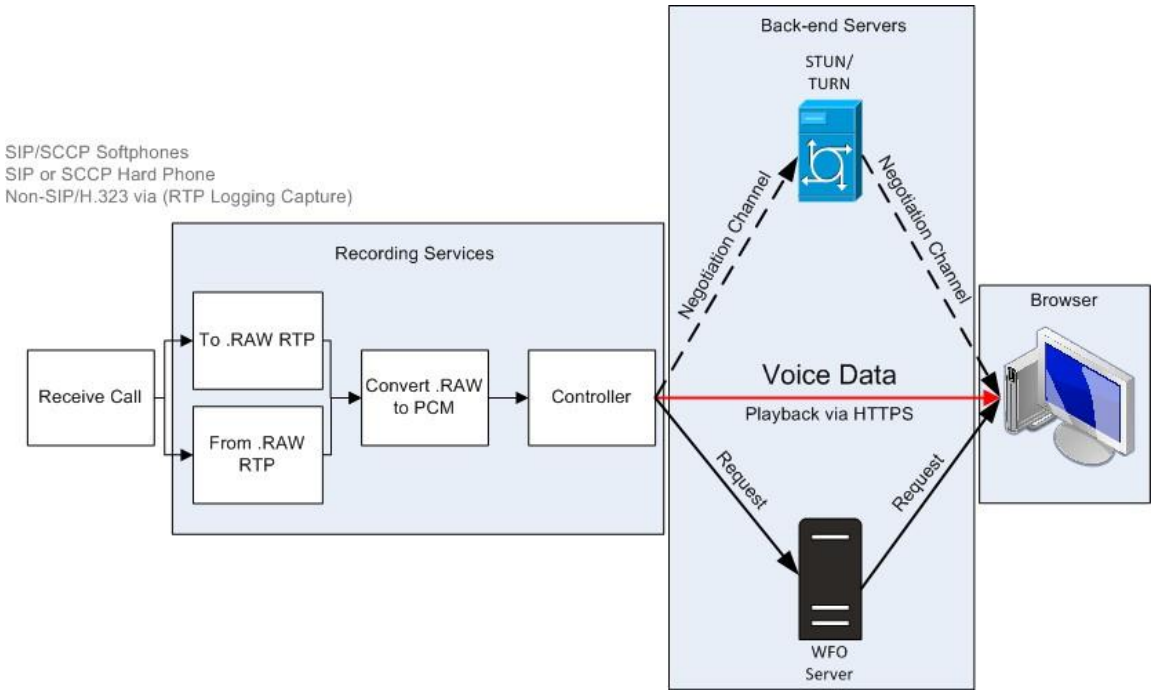
Smart Desktop SIP/SCCP Signalisierung



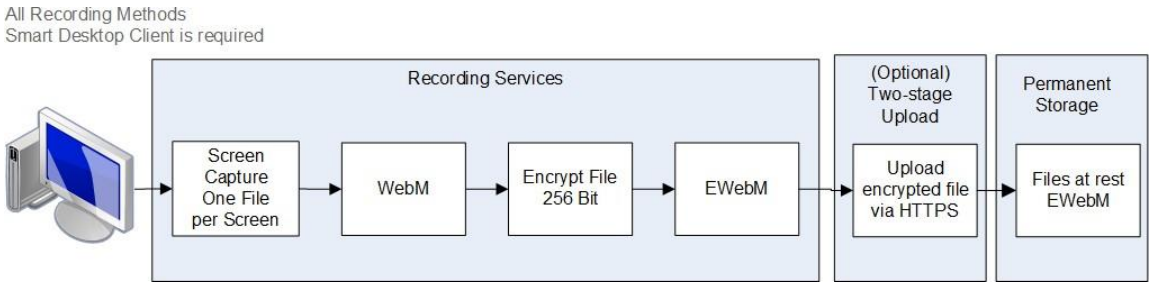
Protokollierung von Smart Desktop-RTP



Smart Desktop Live-Audioüberwachung

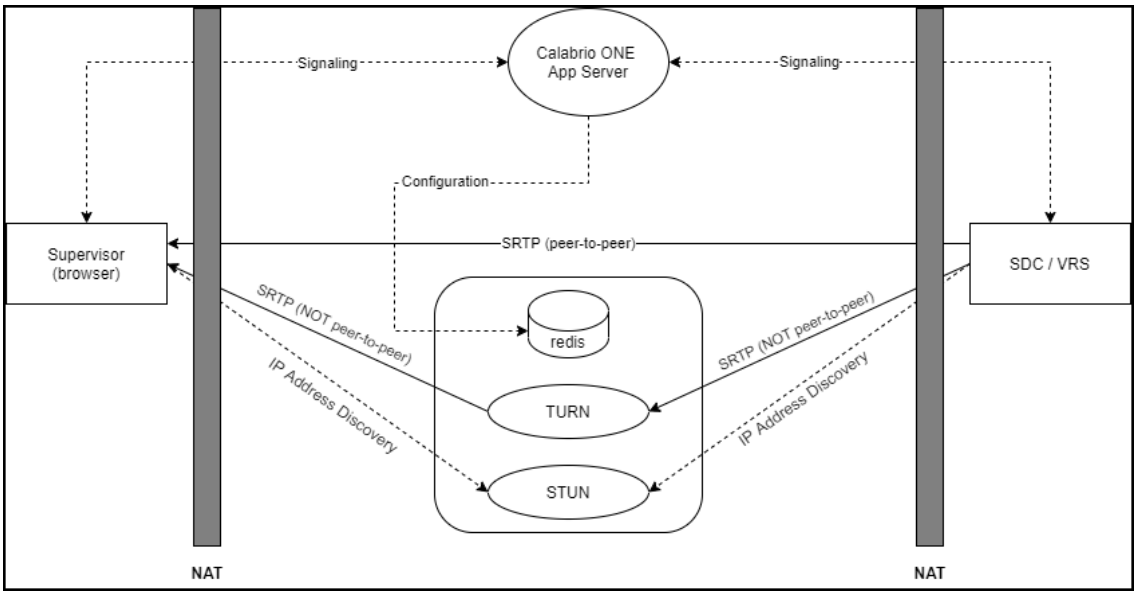


Smart Desktop Live-Bildschirmüberwachung



HINWEIS Die Smartdesktop-Bildschirm- und Audioaufzeichnung verwendet AES 256-Bit-Verschlüsselung, wenn die Aufzeichnung innerhalb 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

Nachdem Sie Smart Desktop (siehe Smart Desktop installieren) und Desktop Analytics (siehe Desktop Analytics-Erweiterung in Ihrem Browser aktivieren) installiert haben, führen Sie diese Schritte aus, um sicherzustellen, dass Ihre Smart Desktop-Implementierung ordnungsgemäß funktioniert.

Voraussetzungen

- Ihre Windows-Anmeldung (**Anwendungsverwaltung** > **Benutzerkonfiguration** > **Benutzer**) muss im Format [Domäne\WindowsNTID] vorliegen. Wenn Sie Ihre Windows-Anmeldung nach der Installation von Smart Desktop hinzufügen, müssen Sie Smart Desktop oder seine Desktopdienste neu starten.
- Dem Agenten sind seiner Rolle die folgenden Berechtigungen zugewiesen. Berechtigungen finden Sie unter **Anwendungsverwaltung** > **Benutzerkonfiguration** > **Rollen**.
  - Desktopanalysen erfassen
  - Kontakte erfassen
  - Bildschirmaufnahme
  - Stimme aufnehmen
  - Live-Bildschirmüberwachung
  - Live-Audioüberwachung
  - Aufzeichnen auf Anfrage (RTP Signalisierung)
  - Desktop-Ereignisse erfassen

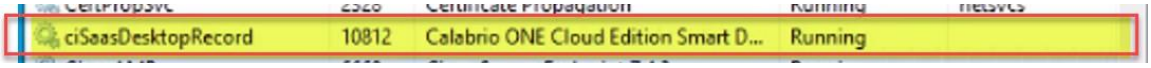
  HINWEIS Contact Center as a Service (CCaaS)-Lösungen unterstützen keine Live-Audioüberwachung.
- Die Desktop Analytics-Erweiterung wird in Ihrem Browser ausgeführt.

Prozeduren

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

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

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



4. Öffnen Sie die App **Dienste** auf Ihrem Computer und vergewissern Sie sich, dass der Calabrio ONE Smart Desktop Record Service ausgeführt wird.

Stellen Sie sicher, dass Webex WFO Ihren Computer erkennt

Navigieren Sie zu **Anwendungsverwaltung** > **Global** > **Überwachung** > **Desktopüberwachung**. Wenn Sie unter der Spalte „Status“ einen grünen Kreis 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 Bildschirmüberwachungssymbol des Agenten schwarz ist. Wenn das Symbol schwarz ist, läuft auf dem PC des Agenten der Smart Desktop Client mit den richtigen Berechtigungen.
3. Sie können die Audiodaten eines Agenten überwachen, wenn das Symbol für die Audioüberwachung des Agenten Ist schwarz. Wenn das Symbol schwarz ist, ist der Agent für die Desktop-Aufzeichnung konfiguriert, hat Smart Client mit den richtigen Berechtigungen auf seinem PC ausgeführt, ist für die Server-Aufzeichnung konfiguriert und ist auf der Seite „Gerätezuordnungen“ einem überwachten Gerät zugewiesen.

4. Klicken Sie auf das Bildschirmüberwachungssymbol des Agenten , um das Fenster zur Live-Bildschirmüberwachung zu öffnen.

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

   Um den Anruf des Agenten zu überwachen. Sie können den Ton nur hören, wenn der Agent ein aktives Gespräch führt.

Tätigen Sie einen Testanruf

1. Tätigen Sie 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.

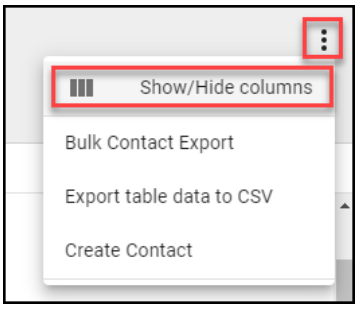
   Wenn das Bedienfeld "Bildschirmaufzeichnung" nicht angezeigt wird oder leer ist, überprüfen Sie, ob der Popup-Blocker im Browser deaktiviert ist.

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

1. Navigieren Sie zu **Interaktionen**.

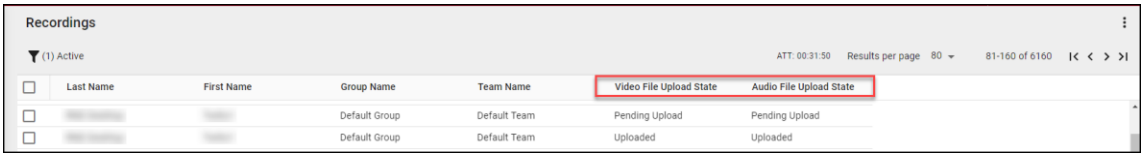
2. Klicken Sie auf das **Symbol "Listenoptionen** " in der oberen rechten Ecke der Seite.

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**. 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 beim Hochladen von Aufzeichnungen in 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-Verfahren.

- Sofortiges Hochladen mithilfe von 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 Mitarbeiters auf

Webex WFO, wenn die WAN- und LAN-Bandbreite ausreicht. 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.

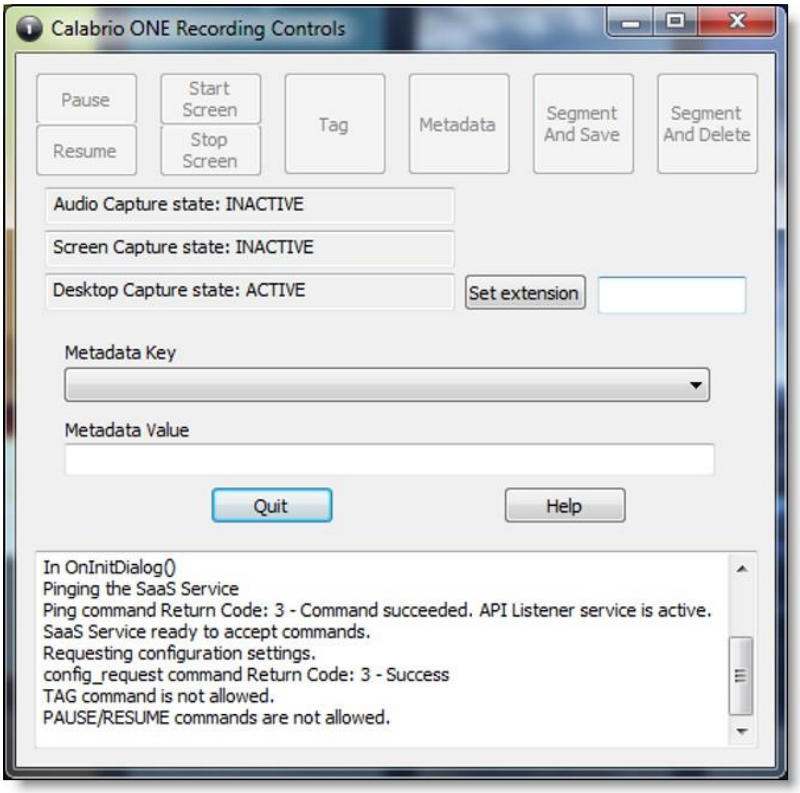
Anwendung "Aufzeichnungssteuerungen"

Webex WFO Recording Controls ist eine eigenständige Webanwendung, mit der Sie die Aufzeichnung von Audio-, Bildschirm- und Tastenanschlägen 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 mit der Smart Desktop Recording Controls Application (DCC), auch bekannt als Desktop Capture and Controller (DCC)-Anwendung, die verwendet, um Aufzeichnungen zu steuern und Metadaten von ihren Desktops einzufügen. 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 *API Referenzhandbuch* .

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 darauf ausgeführten WFO-Dienste 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 die Verwendung von PAC-Skripts nicht, um Verbindungen mit dem Internet herzustellen.

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 Service, an dem sie ausgerichtet sind, aufgeführt.

- Einstellungen für die ACD Synchronisierung des regionalen Datenservers – Wird verwendet, um Benutzer- und Teaminformationen von einem unterstützten ACD (Webex WFO-Datenserver) zu synchronisieren.
- Recording Capture Server Settings (Aufzeichnungserfassungsserver-Einstellungen): Wird für Audioaufzeichnungsumgebungen mit Edge-Servern oder Gateways (SBC) verwendet. Der primäre Signalservice (CTI oder SIPREC) weist Anrufe den Erfassungsservern in einem Round-Robin-Algorithmus (Webex WFO Network Recording Service) zu.
- Regionaler Datenserver GIS-Dateispeicherort – Wird verwendet, um externe Kontaktmetadaten aus einer CSV-Datei in Webex WFO (Webex WFO-Datenserver) 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) (Webex WFO SIPREC Service) verwendet.
- Aufzeichnungs- CTI Signalservereinstellungen – Wird verwendet, um Start- und Stoppereignisse zu verfolgen und Metadaten für Anrufaufzeichnungen zu erfassen. Für Edgeserver-Aufzeichnungsumgebungen wird ein CTI Signalservice verwendet (Webex WFO CTI Signaling Service).
- Einstellungen für den gestaffelten Upload des regionalen Datenservers – Wird verwendet, um Kontaktdaten lokal von Smart Desktop-Benutzern zu sammeln und die Dateien regelmäßig in die Webex WFO-Komponenten in der Cloud (Webex WFO-Datenserver) hochzuladen.
- Regional Data Server ACD Capture Settings (Einstellungen für die Erfassung von regionalen Datenservern): Wird verwendet, um benutzerdefinierte Metadaten zu erfassen und Anrufe abzugleichen, die über ein Gateway (Webex WFO-Datenserver) empfangen wurden.
- Regionale Datenserver-Echtzeit-Ereigniseinstellungen – Dient zum Erfassen von Verlaufs- und Echtzeit-ACD Daten für WFM und ACD Metadaten, die als benutzerdefinierte Metadaten an Anrufkontakte angehängt werden sollen (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 (Active Directory-Synchronisierung): Ermöglicht Webex WFO, Webex WFO-Benutzer mit Active Directory-Benutzern (Webex WFO-Datenserver) abzugleichen und zu synchronisieren.
- 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 API Integration auf diesem Datenserver. Wenn diese Option aktiviert ist, können Sie Folgendes aktivieren:
    - Cisco IP Phone Services Controls (Steuerelemente für Dienste) – Ermöglicht Cisco-fähige Aufzeichnungssteuerungen von unterstützten Cisco-Geräten.
    - Simplified Recording Controls API – Ermöglicht die Verwendung der nativen Datenserver-Authentifizierung für die Aufzeichnungssteuerelemente von Cisco.
- HRMS-Konfiguration: Ermöglicht dem Datenserver das Exportieren von Daten in ein Personalmanagementsystem (Human Resource Management System, HRMS) (Webex WFO-Datenserver).
- SFTP Konfiguration – Ermöglicht die Konfiguration Ihres SFTP Servers (Webex WFO-Datenserver).

- Media Import Server Settings (Medienimport-Servereinstellungen): Ermöglicht den Import von Aufzeichnungsdateien von einem externen Speicherort (Webex WFO-Datenserver).

Systemanforderungen

In den folgenden Abschnitten werden die Mindestsystemanforderungen für Webex

WFO aufgeführt. Die neuesten Informationen zur unterstützten Kompatibilität

finden Sie unter www.cisco.com.

Desktop-Hardware

Die Hardwareanforderungen für Webex WFO-Desktops lauten wie folgt:

Desktop-Hardware	
NIC	100 Mbit Netzwerkkarte Netzwerkkarten müssen den Promiscuous-Modus unterstützen. Konfigurieren Sie die Windows-Energieeinstellungen, um "Dem Computer erlauben, dieses Gerät auszuschalten, um Strom zu sparen" auf den Netzwerkkarten zu deaktivieren.
Festplattenspeicher	20 GB Sprachaufzeichnungsspeicher (MB) = Anzahl der Aufzeichnungen × durchschnittliche Anruflänge × 0,5 MB pro Minute **ANMERKUNG** Diese Formel basiert auf einer Audiobitrate von 64 KBit/s (Kilobits pro Sekunde). [(64 KBit/s × 60 Sek.) ÷ 8 Bit] ÷ 1024 KB = 0.46875 MB pro Minute Bildschirmaufzeichnungsspeicher (MB) = Anzahl der Aufzeichnungen × durchschnittlicher Anruflänge × 1,5 MB pro Minute **HINWEIS** Die Speicheranforderungen für Bildschirmaufzeichnungen hängen von drei Faktoren ab: Aufzeichnungslänge, Monitorauflösung und Anzahl der Monitore, die aufgezeichnet werden. Der hier angezeigte Wert bezieht sich auf einen einzelnen Monitor. Jeder weitere Monitor

wird separat aufgezeichnet, sodass

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
Gedächtnis	2 GB

Desktop-Software

.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 unter http://www.microsoft.com/en-us/download/details.aspx?id=30653 herunterladen.

Browser

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

Desktop Analytics-Plug-in/Erweiterung

Benutzer, die Felder für die Desktop-Analyse über die Seite "Feldmanager" in Webex WFO verwalten, sowie Agentendesktops, auf denen Smart Desktop installiert ist, müssen die Calabrio Analytics-Browsererweiterung/das Plug-In aktiviert haben. Das Plug-in wird nicht nur zum Markieren von Feldern im Browser benötigt, sondern auch zum Überwachen der Webaktivität von Agenten innerhalb des Browsers.

Aktivieren Sie die Erweiterung Desktop Analytics in Firefox

Wenn Sie sich das erste Mal mit Firefox bei Webex WFO anmelden, wird ein Dialogfeld angezeigt, 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 des Desktop Analytics-Plug-Ins in Microsoft Edge Chromium

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

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

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

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

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

Adobe Acrobat Reader

Der Adobe Reader wird benötigt, um exportierte PDF Dateien und Benutzerdokumentationen zu öffnen. Ein kostenloser Download von Acrobat Reader ist unter www.adobe.com verfügbar.

WICHTIG Es gibt bekannte Probleme mit Adobe Reader-Versionen, die die Funktion Sicherheit (Erweitert) verwenden. Wenn Sie die Funktion "Desktop Analytics" verwenden möchten, müssen Sie in Adobe Reader unter **"Voreinstellungen** " zu "Sicherheit (Erweitert)" **navigieren** und die **Option "Geschützten Modus beim Start aktivieren" deaktivieren** und **Erhöhte Sicherheit** , klicken Sie bei Warnmeldungen auf **Ja** und anschließend auf **OK** , um die Änderungen zu speichern. Wenn Sie fertig sind, starten Sie Adobe Reader neu, damit die Änderungen wirksam werden. Wenn Adobe Reader nicht korrekt konfiguriert ist, kann Desktop Analytics keine Ereignisse erfassen, die sich auf Adobe Reader beziehen.

Desktop-Software und Audioaufnahme

Damit Smart Desktop eine ordnungsgemäße Telefonerkennung und Audioaufnahme durchführen kann, ist die Fähigkeit erforderlich, bestimmte Netzwerkprotokolle (z. B. SIP, SCCP und RTP) zu erkennen und zu erfassen. Jede auf dem PC ausgeführte Software, die den Netzwerkverkehr stört, umleitet oder anderweitig verbirgt, führt dazu, dass Smart Desktop nicht richtig funktioniert.

BEISPIEL Der SonicWall VPN-Client mit aktiviertem DNE-Filter (Deterministic Network Enhancer) bewirkt, dass ausgehender Netzwerkverkehr vom Netzwerkadapter umgeleitet wird Die von Smart Desktop verwendet wird. In diesem Fall muss der Lightweight-DNE-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. Bei Benutzern, die über die Berechtigung verfügen, Felder für Desktop Analytics über die Seite "Field Manager" und auf den Desktops der Agenten, auf denen Smart Desktop installiert ist, zu verwalten, muss das entsprechende Desktop Analytics-Browser-Plug-in für den von ihnen verwendeten Browser konfiguriert haben.

Voraussetzungen

- Ihre Organisation verfügt über eine der folgenden Lizenzen:
  - Analytics-Grundlagen
  - Analytics Enterprise

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

Prozeduren

Aktivieren Sie die Erweiterung Desktop Analytics in Firefox

Wenn Sie sich das erste Mal mit Firefox bei Webex WFO anmelden, wird ein Dialogfeld angezeigt, 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 des Desktop Analytics-Plug-Ins in Microsoft Edge Chromium

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

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

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

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

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

Ähnliche Themen

"Installieren von Webex WFO Smart Desktop" im *Webex WFO-Installationshandbuch*

Thin Client-Server

ANMERKUNG unterstützt Citrix XenApp, das nur auf einem unterstützten Windows-Server installiert ist.

Beachten Sie bei Verwendung eines Thin Client-Servers Folgendes:

- Thin Clients, die den Smart Desktop verwenden, benötigen eine Remote-Desktop-Sitzung, um alle Benutzerdaten (Audio-, Bildschirm- und Desktopaufzeichnung) zu erfassen. Wenn keine Remote-Desktop-Sitzung vorhanden ist, installieren Sie Smart Desktop auf den Agentendesktops, um alle Benutzerdaten auf dem Desktop zu erfassen, während der Benutzer angemeldet ist.
- Konfigurieren Sie Workflows so, dass die Funktion "Sofortiger Upload" sowohl für den Bildschirm als auch für die Sprachübertragung verwendet wird, um sicherzustellen, dass auf alle Aufzeichnungen zugegriffen werden kann.

- Wenn Sie Smart Desktop für Aufzeichnungen verwenden, benötigt der Thin Client-Server zusätzliche Serverressourcen für Bildschirmaufzeichnungen. Die Ressourcenanforderungen variieren je nach tatsächlichem Design und erfordern möglicherweise einige detaillierte Hardwaredesigns, 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 verwenden.

Installieren des Thin Client-Servers

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

Verwenden Sie die folgenden Einstellungen, um Audio-, Bildschirmaufzeichnungs- und Aufzeichnungswiedergabefunktionen in Webex WFO zu unterstützen:

Fläche	Überlegung
Browser	▪ Einen unterstützten Browser in Thin-Client-Server-Bereitstellungen einbinden. 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 Sicherheitseinstellungen des Browsers die Wiedergabe von Aufzeichnungen über den Thin Client zulassen.
Sitzungen	Beschränken Sie die Anzahl der gleichzeitigen Sitzungen pro Benutzer auf eine einzige Sitzung.
Smartdesktop-Client	▪ Für Citrix-Clientdienste müssen Sie auch den Smart Desktop installieren Client auf dem Thin Client-Server, um Desktop-Aktivitäten (Desktop Analytics) und Telefonanrufe unter Verwendung eines unterstützten Softphones aufzuzeichnen. ▪ Der Smart Desktop Client stellt über die eindeutige Domain\Windows-Anmeldung des Benutzers eine Verbindung mit der Webex WFO-Plattform her.

Portnutzung

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

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

Edge-Komponenten:

- Intelligenter Desktop

Datenserverkomponenten:

- Datenserver – ACD Sync: Avaya CM mit Contact Center Elite
- Datenserver – ACD Sync: 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 – Aufzeichnen/Erfassen
- 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
Intelligenter Desktop				
UDP 49152–65535	Live-Audioüberwachung – RTP Live-Bildschirmüberwachung – RDP-Stream	PC des Agenten	Browser des Supervisors	—
TCP 52102	Kommunikation zwischen Cisco CTI Datenservern und SDC	Intelligenter Desktop	Datenserver	

Datenserver-Komponenten

Port	Ge	Quelle	Ziel	Anm
Datenserver – ACD Sync: CCaaS-Integrationen				
TCP 443	Kommunikation zwischen CCaaS-Integrationen und den folgenden Einstellungen auf dem Datenserver: Regionale Datenserver-ACD-Erfassungseinstellungen, Aufzeichnungs- CTI Signalisierungsservereinstellungen und Regionale Datenserver-ACD-Erfassungseinstellungen	—	—	—
Datenserver – ACD Synchronisierung: CUCM Netzwerkaufzeichnung				
TCP 22	Kommunikation zwischen der SFTP-Konfiguration und den regionalen Datenserver-Abstimmungseinstellungen auf dem Datenserver und dem CUCM Abrechnungsservice	SFTP, Datenserver	CUCM Abrechnung Dienstleistung	—

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
TCP 8443	Kommunikation zwischen CUCM AXL und regionalem 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 die Einstellungen für die ACD Synchronisierung des regionalen Datenservers auf der 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-Abstimmungseinstellungen und die Einstellungen für die Erfassung des regionalen Datenservers ACD für die Daten Server	Datenserver	Cisco Unified CCE HDS-SQL Serverdatenbank	—
TCP 42027	Kommunikation zwischen dem Cisco Unified CCE CTI Service (Seite a) und die Einstellungen des Aufzeichnungs- CTI Signalisierungsservers für die Daten Server	Datenserver	Cisco Unified CCE CTI Service (Seite A)	Seite A Standard, wenn PG1 verwendet wird. Ports werden variieren je nachdem, welches PG Sie verwenden. Der CTI Serverport, der im Unified CCE ACD Konfiguration.
TCP 43027	Kommunikation zwischen dem Cisco Unified CCE CTI Service (Seite b) und die Einstellungen des Aufzeichnungs- CTI Signalisierungsservers auf den Daten Server	Datenserver	Cisco Unified CCE CTI Service (Seite B)	Seite B Standardeinstellung, wenn PG1 verwendet wird. Ports 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
	ACD Synchronisierungseinstellungen für den regionalen Datenserver und die regionalen Einstellungen für ACD "Data Server Capture"		Informix-Datenbank	
TCP 12028	Kommunikation zwischen dem Cisco Unified CCX CTI Service (Seite a) und die Einstellungen des Aufzeichnungs- CTI Signalisierungsservers für die Daten Server	Datenserver	Cisco Unified CCX CTI Dienst (Seite A)	Seite A Standardeinstellung. Das ist der RMCM TCP in Unified CCX konfigurierter Port Systemparameter. Der CTI Server Im Unified CCX konfigurierter Port ACD Konfiguration.
TCP 12028	Kommunikation zwischen dem Cisco Unified CCX CTI Service (Seite b) und die Einstellungen des Aufzeichnungs- 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 CTI Server Im Unified CCX konfigurierter Port 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 genutzt.
Datenserver – Aufzeichnen/Erfassen				
UDP 39500–43500	RTP wird aufgezeichnet	Telefon oder Sprachanruf Tor	Audio-Aufnahme (Aufzeichnungsserver)	—

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
UPD 49152–65535	Live-Audioüberwachung – RTP	Audio-Aufnahme (Aufzeichnungs server)	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	Beliebiger Unified CM Herausgeber 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	Beliebiger Unified CM Herausgeber 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

Die Anforderungen an die Kennwortkomplexität basieren auf der Kennwortrichtlinie von Microsoft: https://technet.microsoft.com/en-us/library/hh994562.aspx.

Die folgenden Regeln gelten, wenn Sie einen Benutzer erstellen oder bearbeiten sowie ein Kennwort ändern oder zurücksetzen.

- Kennwörter dürfen keine Leerzeichen (Leerzeichen) enthalten.
- Kennwörter müssen mindestens acht Zeichen lang sein. Die Mindestlänge kann von einem Administrator konfiguriert werden.
- Kennwörter müssen Zeichen aus drei der folgenden vier Kategorien enthalten:

Kategorie	Beschreibung
Großbuchstaben	A–Z Unicode-Zeichen in Großbuchstaben: http://www.fileformat.Info/Info/unicode/category/Lu/list.htm
Kleinbuchstaben	A–Z Unicode-Zeichen in Kleinbuchstaben: http://www.fileformat.Info/Info/unicode/category/Lu/list.htm
Zahlen	0–9
Sonderzeichen	Für ein Mandantendatenbankkennwort sind die folgenden Zeichen zulässig: ! # $ % & ( ), . / : ; = ? @ ^ ` | Für alle anderen Passwörter sind folgende Zeichen erlaubt: ! " # $ % & ' ( ) * +, – . / : ; < = >? @ [ ] ^ _ ` { | } ~

Diese Regeln gelten nur, wenn Sie ein Kennwort konfigurieren, das von Webex WFO gesteuert wird. Wenn ein Benutzer ein Kennwort für ein externes System eingibt, das nicht von Webex WFO gesteuert wird, validiert Webex WFO das Kennwort nicht (z. B. ACD-Konfiguration).

HINWEIS Ein Benutzer kann ohne Passwort erstellt werden (manuell oder automatisch über die ACD-Synchronisierung). Ein Benutzer ohne Passwort kann sich nicht anmelden. Dieser Benutzer muss den Link "Passwort vergessen" verwenden und ein
Passwort.

Authentifizierung

Standardmäßig werden Benutzerauthentifizierung und Passwörter mit Webex WFO verwaltet. In Systemen, die mit einem ACD synchronisiert werden, werden Benutzer im ACD erstellt und verwaltet, Sie können jedoch weiterhin Benutzer im Webex WFO erstellen.

Sie können sich für die Verwendung der Security Assertion Markup Language (SAML)-Authentifizierung entscheiden. SAML ermöglicht Ihnen die Verwendung eines externen Identitätsanbieters (IdP) zur Authentifizierung von Benutzernamen und Passwörtern. Diese Methode der Benutzerauthentifizierung und Kennwortverwaltung wird allgemein als „Single Sign-On“ bezeichnet.

Methoden zur Plattformerfassung

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.

NOTIZ

Webex WFO unterstützt SRTP nur mit den folgenden Erfassungsmethoden:

- Acme-Paket
- Cisco Unified CM

Plattform	Erfassungsmethode	Signalisierung	Signalisierungsbeschreibung
Cisco	Integrierte Bridge-Netzwerkaufzeichnung	JTAPI	Registriert sich beim Callmanager für JTAPI-Events
Cisco	Desktop-Aufzeichnung	JTAPI	Registriert sich beim Callmanager für JTAPI-Events
Cisco	Gateway (Cisco Unified Border Element – CUBE)	SIPREC	Registriert sich bei CUBE für SIPREC-Signalisierung
Cisco	Smart Desktop Client	IP Kommunikator (SIP/SCCP)	SCCP-Nachrichten vom Desktop

Plattform	Erfassungsmethode	Signalisierung	Signalisierungsbeschreibung
Cisco	Smart Desktop Client	Jabber (SIP/SCCP)	Erschnüffelt SIP/SCCP-Nachrichten vom Desktop
Cisco	Smart Desktop Client	Cisco IP HardPhone (SIP/SCCP)	Erschnüffelt SIP/SCCP-Nachrichten vom Desktop
Cisco Webex Contact Center (CWCC)	Automatisierter Import	CWCC-Analysator API	Poll CWCC Analyzer für Post-Call-CDR und Post-Call-Verarbeitung
ACME	Gateway (ACME-Pakete)	SIPREC	Registriert sich bei ACME für SIPREC-Signalisierung
SONUS	Gateway (SONUS)	SIPREC	Registriert sich bei SONUS für SIPREC-Signalisierung

Cisco-Spracherfassungsmethoden

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

Erfassungsmethode	Signalisierung	Beschreibung	Medien Strom	Intelligenter Desktop Bildschirmaufnahme	Live-Audio Überwachung
Netzwerk Aufnahme-Eingebaute Brücke (LÄTZCHEN)	JTAPI	Registriert bei CUCM/JTAPI Veranstaltungen	BIB—Medien Gestreamt von Telefonnummer	Ja (Smart Desktop-Client Erfordert CTI Verbindung)	Ja (Smart Desktop Client) über WebRTC
Intelligenter Desktop Kunde – IP Kommunikator	SIP/SCCP	Monitor SIP/SCCP Nachrichten aus Desktop/Softphone	Medienstream gefangen direkt auf Desktop	Ja (Smart Desktop-Client)	Ja (Smart Desktop Client) über WebRTC
Intelligenter Desktop Kunde – Jabber	SIP/SCCP	Überwacht SIP/SCCP Nachrichten aus Desktop	Medienstream gefangen direkt auf	Ja (Smart Desktop-Client)	Ja (Smart Desktop Client) über

Erfassungsmethode	Signalisierung	Beschreibung	Medien Strom	Intelligenter Desktop Bildschirmaufnahme	Live-Audio Überwachung
			Desktop		WebRTC
Intelligenter Desktop Kunde – Cisco IP Telefon (Daisy Angekettet)	SIP/SCCP	Überwacht SIP/SCCP Nachrichten aus Desktop	Medienstream gefangen 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 von Cisco WÜRFEL	Ja (Smart Desktop-Client)	Nein
Massenkontakt Importieren	API-basiert	Registriert bei CUBE für SIPREC Signalisierung	Automatisiert Import von unverschlüsselt .WAV und verbunden Kontakt Metadatendateien in großen Mengen	N/A – Dateien Verschlüsselt und Importiert	Nein

Legacy Five9 Voice Capture-Integrationen

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

Erfassungstyp	Signalisierung	Beschreibung	Medienstream	Intelligenter Desktop - Bildschirm Erfassen	Live-Audio Überwachung

Plattform-					
Smart Desktop Client	Kafka CTI	Webex WFO-Plattform registriert sich bei Five9 Kafka Events API	Medienstream direkt erfasst auf	Ja (Smart Desktop Client)	Ja (Smart Desktop Client) über WebRTC

Erfassungstyp	Signalisierung	Beschreibung	Medienstream	Intelligenter Desktop - Bildschirm Erfassen	Live-Audio Überwachung
			Desktop – Beitrag Rufen Sie CDR an und Versöhnung Verarbeitung redigiert und fügt Ereignisse ein basierend auf Kafka Anrufereignisse		
Intelligenter Desktop Client	Five9-Agent Desktop Plus (ADP) - Kafka CTI	Monitor SIP/SCCP Nachrichten aus Desktop/Softphone	Medienstream gefangen direkt auf Desktop – Beitrag Rufen Sie CDR an und Versöhnung Verarbeitung redigiert und fügt Ereignisse ein basierend auf Kafka Anrufereignisse	Ja (Smart Desktop Kunde)	Ja (Smart Desktop Client) über WebRTC
Intelligenter Desktop Client	Five9-Agent Desktop Werkzeugkasten (ADT) - Kafka CTI	Überwacht SIP/SCCP Nachrichten aus Desktop	Medienstream gefangen direkt auf Desktop – Beitrag Rufen Sie CDR an und	Ja (Smart Desktop Kunde)	Ja (Smart Desktop Client) über WebRTC

Plattform-
Versöhnung
Verarbeitung
redigiert und
fügt Ereignisse ein
basierend auf Kafka
Anrufereignisse

Erfassungstyp	Signalisierung	Beschreibung	Medienstream	Intelligenter Desktop - Bildschirm Erfassen	Live-Audio Überwachung
Intelligenter Desktop Client	Five9 Java Agent Desktop - Kafka CTI	Überwacht SIP/SCCP Nachrichten aus Desktop	Medienstream gefangen direkt auf Desktop – Beitrag Rufen Sie CDR an und Versöhnung Verarbeitung redigiert und fügt Ereignisse ein basierend auf Kafka Anrufereignisse	Ja (Smart Desktop Kunde)	Ja (Smart Desktop Client) über WebRTC
Intelligenter Desktop Client	Five9 VCC Importieren	Five9/Webex WFO Cloud-Integration für Five9 VCC importieren Audioaufnahmen in Webex WFO Cloud	N/A – Import Nur	Ja (Smart Desktop Kunde)	Nein

Sonus Gateway-Aufzeichnung

Cisco unterstützt die Ausfallsicherheit für Sonus Gateway Recording.

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

- Für Anrufe, die ohne „Cisco-Guid“-Header beim SBC eingehen, erstellt das SMM eine Cisco-Guid, indem es die 4 Hex-Tupel aus der vorhandenen Anruf-ID verwendet. Jedes Tupel wird in eine 10-stellige, mit Nullen aufgefüllte Dezimalzahl umgewandelt, die durch Bindestriche von der Cisco-Guid getrennt wird.
- Bei Anrufen, die bereits einen Cisco-Guid-Header enthalten, bleibt der Header unverändert.

NOTIZ **Notiz:** Die Cisco_Guid wird NICHT durch eine neue, mit der Call-ID erstellte Cisco-Guid überschrieben.

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

Die Regeln müssen mit Ihrem aufgezeichneten Trunk und dem von Ihrem Unified CM verwendeten Trunk verknüpft sein. 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 über die Sonus-Befehlszeilenschnittstelle (CLI) die SMM-Regeln
    a. Erstellen und aktivieren Sie die eingehenden SMM-Regeln Unified CM. Sehen Beispiel für Inbound-SMM-Regeln für Unified CM für weitere Informationen.
    b. Fügen Sie die ausgehenden SMM-Regeln Unified CM hinzu. Sehen Beispiel für ausgehende SMM-Regeln für Unified CM für weitere Informationen.
    c. Fügen Sie die ausgehenden SMM-Regeln des Rekorders hinzu. Sehen Beispiel für ausgehende SMM-Regeln für die Recorder für weitere Informationen.
2. Verwenden Sie die Sonus CLI, um SIPREC für den SIp-Sig-Port in der Zone zu aktivieren, die Ihr Unified CM enthält Stamm.
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 das Ingress-Präfix IP der Adresse IP der Maschine QM zu, auf der der „Monitoring and Recording Sonus SIPREC Service“ ausgeführt wird.
4. Verwenden Sie die Sonus CLI/Navigation, um Ihren Trunks SMM-Regeln wie folgt zuzuweisen:
    a. Weisen Sie UCM_INBOUND SMM dem Signaling Message Manipulation-Adapter-Eingabeprofil 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 Ausgabeprofil des Signaling Message Manipulation-Adapters für den Sonus SIPREC-Trunk von QM zu.
5. Verwenden Sie Sonus PSX, um eine IP-Signalisierungs-Peer-Gruppe für den Sonus SIPREC-Server von QM zu erstellen. Weisen Sie das Ingress-Präfix IP der Adresse IP der Maschine QM zu, auf der der „Monitoring and Recording Sonus SIPREC Service“ ausgeführt wird.
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 Rekorderprofil 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 SSM-Regeln für eingehende Anrufe 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

Nachricht						
set profiles signalisieren sipAdaptorProfile message 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 set profiles signalisieren	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	
paramType generic Festlegen von Profilen	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	Von
Signalisierungstyp Variable	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	Von
set-profile-signalisierungsvariableWert var1 Signalisierungsparameter für Profile festlegen Profile festlegen , die Cisco-GUID signalisieren begehen	sipAdapterProfil	UCM_INBOUND	Regel 2	Aktion	1	zum Eingeben von
set-Profile , die sipAdaptorProfile-UCM_INBOUND-Status aktiviert Commit signalisieren						

Beispiel für Outbound 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-	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	11	An
signalisierungsvariableWert var3	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	12	Art
Festlegen von Profilen Signalisierungstyp Variable Setze Profile	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	12	

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

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

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 applyMatchOrder 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=.* RECORDER_OUTBOUND Regel 1 Kriterium 2

set 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 messageRECORDER_OUTBOUND Regel 2 Kriterium 1 messageTypes request

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

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" in "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 Webex WFO-Software festlegen. In der Regel wird jede Cloud
> Enthält eine neue Version der Webex WFO-Datenserversoftware, die Benutzer von ihrem Mandanten herunterladen können.

Wenn Ihr Unternehmen 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 WFO-Datenserver
- Webex WFO-Netzwerkaufzeichnungsservice
- Webex WFO SIPREC-Dienst
- Webex WFO-Datenserver-Webdienste

Informationen zu den Anforderungen an die

Portnutzung finden Sie unter Port-Nutzung.

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 Tenant-Administrator 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,	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 KEX-Algorithmen (Key Exchange, 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 CDR SFTP Server 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 Webex WFO-Datenserverdienst 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 des 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 zur Verfügung. Es liegt in der Verantwortung des Kunden, die Datei in eine MSI-Datei zu konvertieren.
- Wenn die Installation über SCCM oder Microsoft Endpoint Configuration Manager erfolgt, 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 die automatische Aktualisierungsfunktion deaktivieren, 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 Updates verwalten 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 WFO-Software der Version 11.5 zu entfernen Webex 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 zu definieren, einschließlich Skriptoptionen. 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 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 Verzeichnisses der Serverfreigabe>\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 die 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: Ciscos Systemvorbereitungs-Hook

Um PC-spezifische Informationen aus einer Windows-Installation zu entfernen und zu "verallgemeinern", sodass sie auf verschiedenen PCs installiert werden kann, empfehlen wir Ihnen dringend, den Sysprep-Hook (System Preparation Hook) 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:

Ereignis-ID	Beschreibung
8080	Erfolgreiche Installation

Ereignis-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

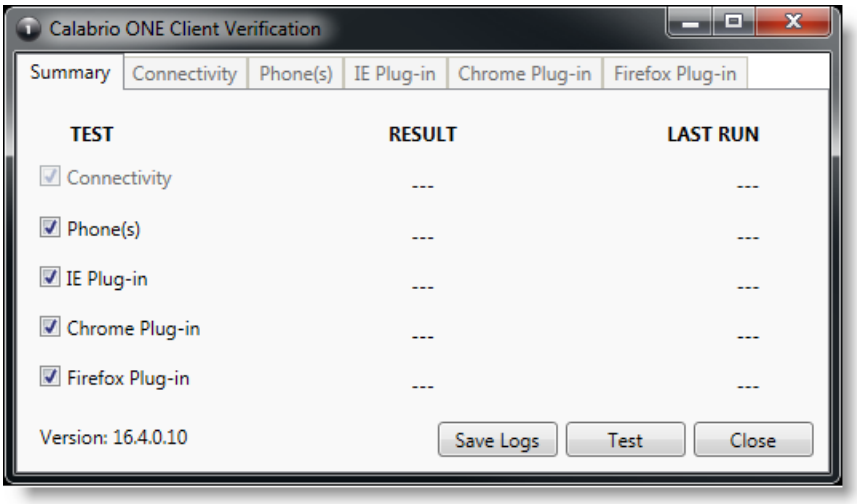
Das Clientüberprüfungstool testet den Client-PC, um sicherzustellen, dass die Konnektivität mit den Servern und dem Telefon für die Ausführung von Smart Desktop geeignet ist. Es wird installiert, wenn Smart Desktop installiert ist. Das Tool führt verschiedene Tests durch und meldet die Ergebnisse entweder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

Ausführen des Clientüberprüfungstools

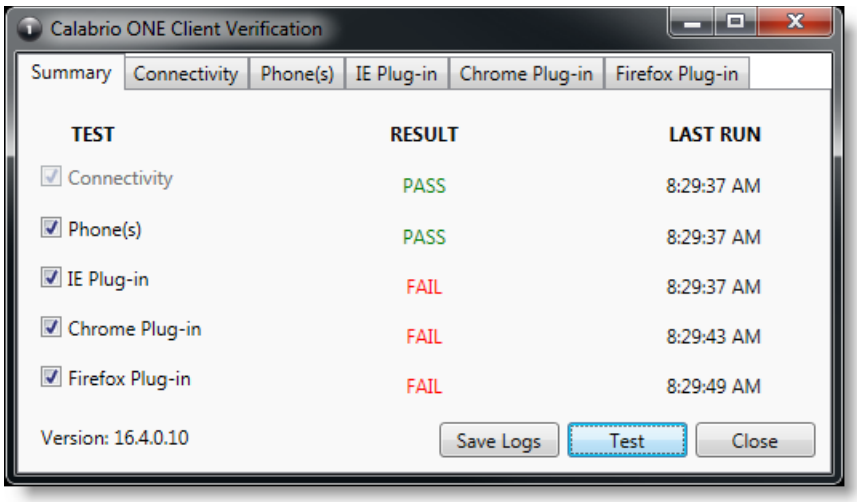
1. Navigieren Sie nach der Installation von Smart Desktop zum folgenden Ordner auf dem Client-PC:

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

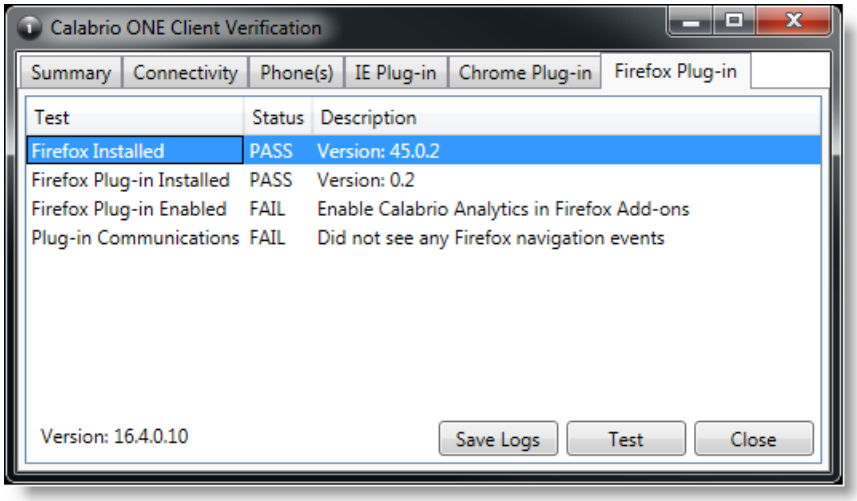
2. Doppelklicken Sie auf **ClientDiag.exe**. Das Clientüberprüfungstool wird gestartet.



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 Registerkarte, auf der Details zum Test angezeigt werden. Wenn der Test fehlschlägt, geben die Details auf der Registerkarte 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 Webex WFO-Komponenten deinstalliert werden.

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 zu definieren, einschließlich Skriptoptionen.

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 die Befehlszeilenschnittstelle deinstallieren.

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