Webex WFO-Design- und Installationsleitfaden

Für Bereitstellungen mit neuem WFM

Erstveröffentlichung: 20. Juli 2021
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 9

Lokalisierung und unterstützte Sprachen 11

Übersicht 15

CCaaS-Bereitstellungsmodell 15

Vom Kunden gehostetes ACD Bereitstellungsmodell 15

Authentifizierung – Übersicht 17

Ablauf des Authentifizierungsprozesses 17

Systemanforderungen 19

Browser 19

Netzwerkbandbreite 19

Sonstige Anforderungen 19

Unterstützte Umgebungen 19

Desktop-Software 19

.NET Framework 19

Browser 20

Desktop Analytics Plug-in/Erweiterung 20

Adobe Acrobat Reader 20

Desktop-Software und Audioaufnahme 21

PCI DSS-Konformität 21

Aktivieren Sie die Desktop Analytics-Erweiterung in Ihrem Browser 21

Dateiverschlüsselung 23

Kennwortrichtlinie 23
Business-Continuity-Lösungen 23
Georeplikation 23
Availability Zones 24
Portnutzung 25
CCaaS-Anschlüsse 25
Vom Kunden gehostete ACD Ports 26
Edge-Komponenten 27
Datenserver-Komponenten 28
Informationen zur Speicherung 33
Administratorkonfiguration 33
Speicherebenen 34
Storage-Angebote 35
Massenimport und -Export von Daten 37
Exportieren von Kontakten in großen Mengen 37
Genehmigungsvoraussetzungen für den Export von Massenkontakten 40
Speichern von und Zugreifen auf Bulk-Kontaktdateien 40
Edge-Komponenten 42
Webex WFO-Datenserver 43
Webex WFO ACD Sync-Dienst 45
ACD Synchronisierungsdienst-Konnektivität 45
Webex WFO-Audioaufnahmeservice 46
Verbindung mit dem Audio-Capture-Dienst 46
Webex WFO GIS-Service 46

GIS-Service-Konnektivität 47
Webex WFO-Signalservice 47
Signalservice-Konnektivität 48
Webex WFO-Service für gestaffelten Upload 48
Zweistufige Upload-Komponente 49
Verbindung mit dem gestaffelten Upload-Dienst 49
Webex WFO QM ACD Capture-Service 49
Komponenten QM ACD Capture Service 50
QM ACD Historical Capture-Komponente 50
QM ACD Komponente "Echtzeiterfassung" 50
QM GIS-Erfassungskomponente 50
QM ACD Capture Service-Konnektivität 50
Webex WFO WFM ACD Erfassungsservice 51
Komponenten WFM ACD Capture Service 51
WFM ACD Historical Capture-Komponente 51
WFM ACD Komponente "Echtzeiterfassung" 51
WFM GIS-Erfassungskomponente 51
WFM WHIT-Capture-Komponente 51
WFM ACD Capture-Servicekonnektivität 52
Webex WFO Local Web Services-Dienst 52
Komponenten des lokalen Web-Services-Dienstes 52
Cisco IP Phone Komponente "Services-Steuerungen" 52
Vereinfachte Aufzeichnungssteuerung API Komponente 52
Verbindung mit lokalen Web-Services-Diensten 53

Installieren des Datenservers 53
Voraussetzungen 53
Installieren des Datenservers für einen einzelnen Tenant 54
Datenserver für mehrere Besitzer installieren 54
Cisco Unified Call Manager-Benutzer 55
Webex WFO Smart Desktop 56
Über Webex WFO Smart Desktop 56
Smart Desktop Client-Konnektivität 58
Anforderungen und Überlegungen zu Smart Desktop 58
Desktop-Hardware 61
Verwendung von Smart Desktop-Ports 61
Smart Desktop-Kontaktmetadaten 63
Smart Desktop Capture-Datenflussdiagramme 64
Smart Desktop testen 67
Smart Desktop verwalten 70
Thin Client-Server 73
Installieren des Thin Client-Servers 73
Installation 75
Installieren von Smart Desktop 75
Manuelle Installation 76
Installation mit GPO 77
Replizieren einer Installation mit Desktop-Imaging 77
Rückgabecodes für die Push-Installation 78
Client-Verifizierungstool 79

Steuerelemente für die Aufzeichnung 80
Installieren des Datenservers 81
Voraussetzungen 81
Installieren des Datenservers für einen einzelnen Tenant 82
Datenserver für mehrere Besitzer installieren 82
Cisco Unified Call Manager-Benutzer 83
Entfernung 85
Deinstallieren von Webex WFO Smart Desktop 85
Deinstallieren mit GPO 85
Datenübertragungs-Flussdiagramme 87
Aufzeichnung, Erfassung und Wiedergabe von Datenflussdiagrammen 87
Datenflussdiagramm für die Audiowiedergabe 87
Datenflussdiagramm für die Bildschirmwiedergabe 89
Analytics-Datenflussdiagramm 89
Datenflussdiagramm der Sprachtranskriptionsanalyse 90
Datenflussdiagramme für Cloud-Speicher 90
Cloud-Speicher für CCaaS-Bereitstellungen 91
Cloud-Speicher für vom Kunden gehostete ACD-Bereitstellungen 91
Aufzeichnungsverschlüsselung 92
Cisco Hosted Collaboration Solution (HCS) 93
Plattform-Erfassungsmethoden 94
Unterstützte Erfassungsmethoden nach Plattform 94
Sonus Gateway-Aufzeichnung 98

Einführung

Der *Webex WFO-Design- und Installationsleitfaden* bietet einen allgemeinen Überblick über die Struktur und die Komponenten von Webex WFO in der Cloud und erläutert, wie Webex WFO in einer Cloud-Umgebung installiert wird. Genauere Informationen zu den unterstützten Integrationen finden Sie in den verfügbaren Integrationsleitfäden.

Dieses Handbuch richtet sich an Implementierungs- und Supporttechniker von Cisco, Mitarbeiter der Vertriebstechnik, Partner und Kunden von Cisco. Aber auch für die Entwicklungs-, Marketing-, Vertriebs- und anderen Mitarbeiter von Cisco im gesamten Unternehmen könnte es nützlich sein.

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	x	Begrenzt									
Chinesisch (zh-TW)	x	x	Begrenzt									
Dänisch (da)	x	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	x	Begrenzt	x	x	x		x				
Französisch (fr)	x	x	x	x	x	x		x	x			Begrenzt
Kanadisches Französisch (fr-CA)	x	x		x	x	x		x	x			Begrenzt
Deutsch (de)	x	x	Begrenzt	x	x	x		x	x			Begrenzt
Italienisch (it)	x	x	Begrenzt	x	x	x		x	x			
Japanisch (ja)	x	x	x									
Koreanisch (ko)	x	x	x									
Norwegisch (nb)	x	x	Begrenzt	x	x	x		x	x			
Polnisch (pl)	Begrenzt		Begrenzt	x	x	x		x	x			
Portugiesisch (pt)	x	x	Begrenzt	x	x	x		x	x			
Portugiesisch (Brasilien) (pt-BR)	x	x	x	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	Begrenzt	x										
Spanisch	x	x	x	x	x	x		x	x			Begren
Mexikanisches Spanisch (es-MX)				x	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 technischen Support von Cisco, 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.

Übersicht

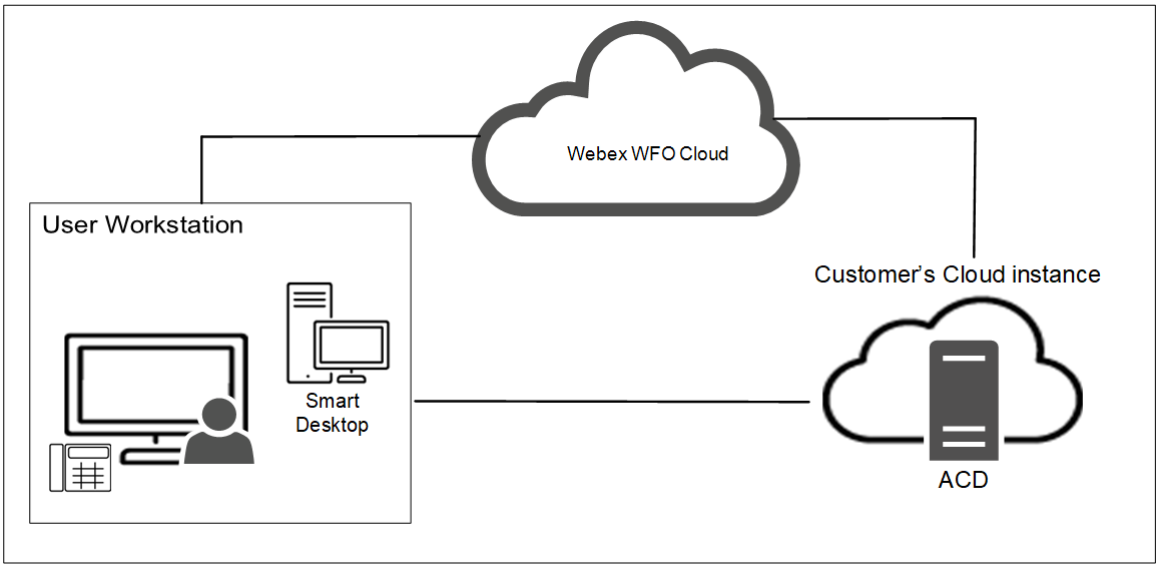
Die gesamte Webex WFO Suite wird in der Cloud gehostet, die von Amazon Web Services und Microsoft Azure betrieben wird. Daten werden zwischen Webex WFO Cloud, Benutzerarbeitsstationen und dem ACD Ihres Unternehmens verschoben.

Webex WFO unterstützt zwei allgemeine Arten von Cloud-Bereitstellungsmodellen. Ihr Cloud ACD-Designmodell kann in eine der beiden unten aufgeführten Kategorien passen, je nachdem, welche ACD Ihre Organisation in Webex WFO integriert hat. Bei diesen beiden Modellen handelt es sich um Contact Center as a Service (CCaaS) und vom Kunden gehostete ACDs.

Die Informationen im *Webex WFO Cloud Design and Installation Guide* gelten für beide Cloud-Modelle, sofern nicht ausdrücklich anders angegeben.

CCaaS-Bereitstellungsmodell

CCaaS-Bereitstellungsmodelle ermöglichen es dem CCaaS-Anbieter, ACD Dienste und Infrastruktur in der Cloud zu hosten. Dadurch können die Kosten für Betriebstechnik und Supportfälle gesenkt werden. Weitere Informationen zu diesem Modell finden Sie in den Themen Portnutzung und Speicher.



Vom Kunden gehostetes ACD Bereitstellungsmodell

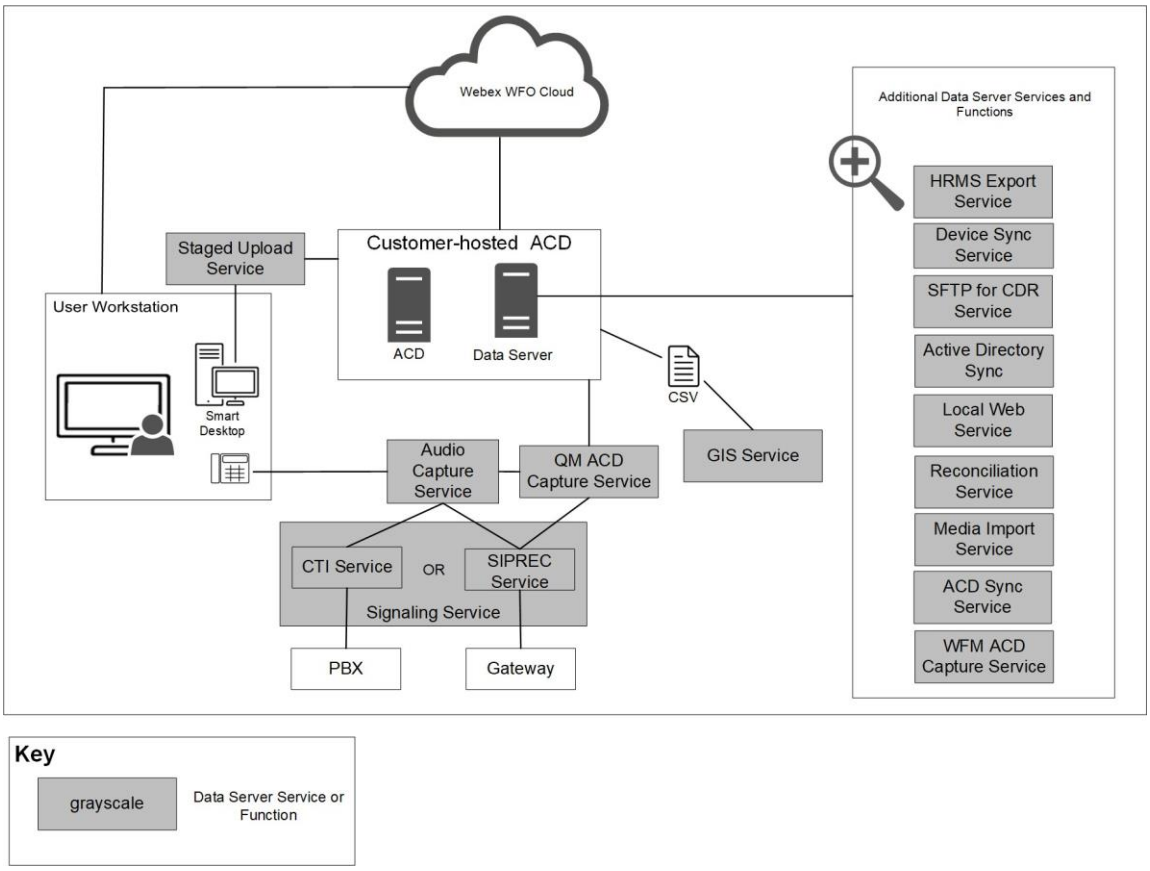
Bei kundengehosteten ACDs befindet sich die ACD Infrastruktur am Kundenstandort zusammen mit einem Webex WFO-Datenserver, der für die Datenübermittlung zum und vom bzw. zum kundengehosteten ACD verwendet wird. Die Webex WFO-Daten

Der Server und die vom Kunden gehostete ACD übergibt diese Daten dann an Webex WFO Cloud. Genauere Details erfahren

Zu diesem Modell in den Themen Portnutzung , Edge-Komponenten und Speicher.

HINWEIS In der folgenden Abbildung werden die ACD-, PBX- und Gateway-Geräte vom Kunden bereitgestellt. Diese Geräte können mit verschiedenen Komponenten des Webex WFO-Produkts verbunden werden, sind aber nicht Teil von

Das Webex WFO-Produkt.



Authentifizierung – Übersicht

Bei der Authentifizierung wird die Identität aller Personen überprüft, die eine Verbindung zu Webex WFO herstellen. Webex WFO erlaubt zwei Methoden zur Authentifizierung von Benutzern im System. Diese Methoden sind die Webex die WFO-Standardauthentifizierung und die einmalige Anmeldung (Single Sign-On mit Security Assertion Markup Language SAML). Wenn sich Benutzer anmelden, durchlaufen sie den Webex WFO Identity and Access Management (IAM)-Authentifizierungsservice. Nachdem Cisco den Benutzer authentifiziert hat, kann der Benutzer auf Grundlage seiner Berechtigungen auf alle Bereiche der Webex WFO Suite zugreifen.

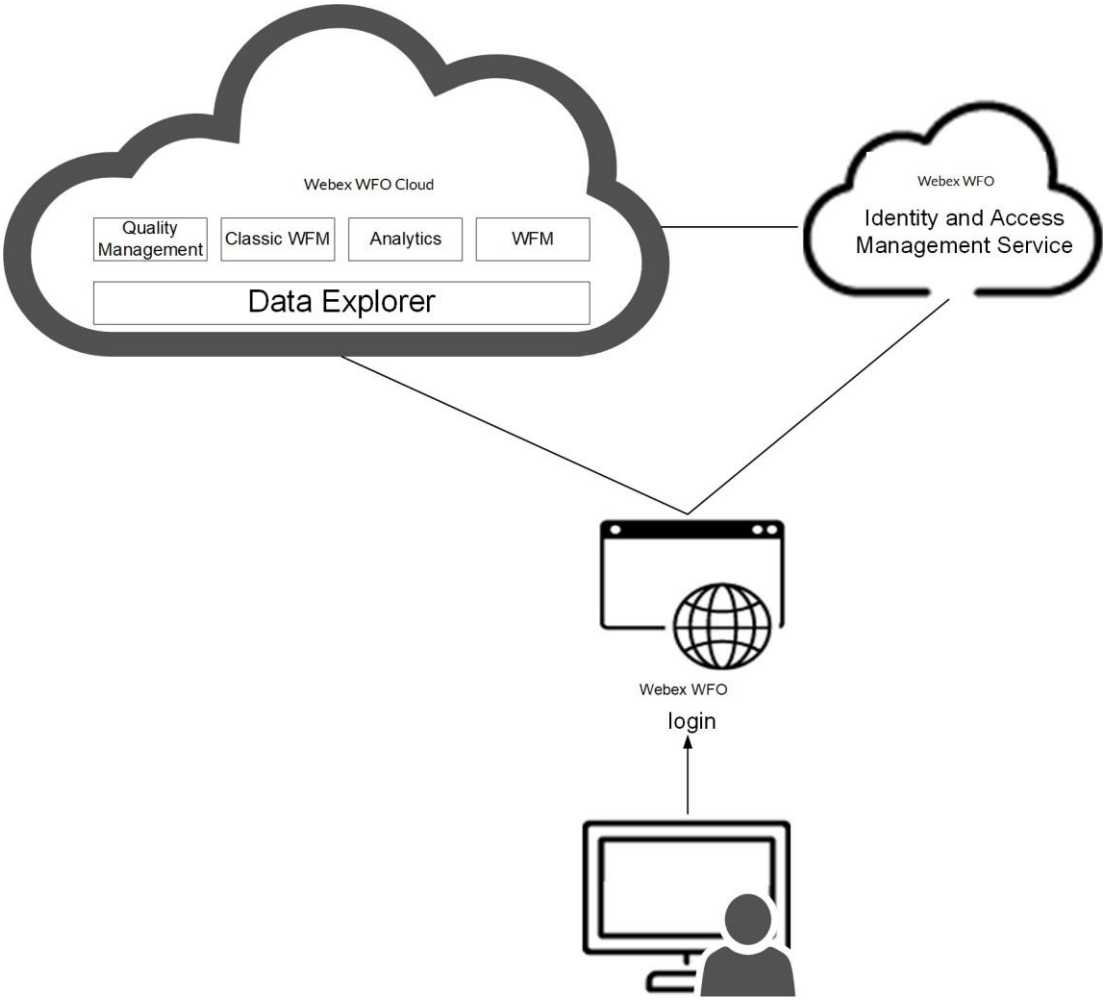
Die gesamte Authentifizierung bekannter Benutzeridentitäten wird vom Webex WFO-Dienst verwaltet. Die Autorisierung erfolgt über Ihre Webex WFO-Produkte. Bei Verwendung von SAML agiert Webex WFO als Service-Provider (Ressourcenserver), und der Identitätsanbieter des Kunden wird verwendet, um den Benutzer mit dem Webex zu verbinden.
WFO-Cloud. Ein Benutzer muss in Webex WFO vorhanden sein, um sich beim Identitätsanbieter des Kunden anzumelden.

Ablauf des Authentifizierungsprozesses

Schritte im Authentifizierungsprozess

1. Ein Benutzer greift auf Webex WFO zu. Wenn sie eine Sitzung haben, fahren sie mit Webex WFO fort. Ist dies nicht der Fall, werden sie an den Webex WFO-Authentifizierungsdienst weitergeleitet.
2. Wenn der Benutzer eine Sitzung im Webex WFO-Authentifizierungsdienst hat, wird er sofort zurück zum Webex WFO geleitet, wo Webex WFO eine Sitzung für den Benutzer einrichtet.
3. Wenn der Benutzer keine Webex WFO-Sitzung hatte, wird er aufgefordert, seine E-Mail-Adresse einzugeben.
4. Wenn die E-Mail-Adresse nur einem Webex WFO-Benutzer gehört, wird der Benutzer entweder über SAML zum IdP des Kunden weitergeleitet oder aufgefordert, sein Kennwort im Webex WFO I am-Authentifizierungsdienst einzugeben, je nachdem, wie die Authentifizierung vom Kunden konfiguriert wurde.
5. Wenn sich der Benutzer erfolgreich authentifiziert hat, wird er aufgefordert, einen Besitzer auszuwählen, wenn er mehreren Tenants angehört, oder er wird sofort zurück zu Webex WFO geleitet, wo eine Sitzung erstellt wird.

Authentifizierung – Übersicht | Ablauf des



Systemanforderungen

Webex WFO-Versionshinweise enthalten die neuesten Informationen zu Änderungen der Systemanforderungen, Kompatibilitäten, Fehlerbehebungen und neuen Funktionen. Archive früherer Versionshinweise sind verfügbar.

Browser

Der Zugriff auf Webex WFO erfolgt über das Internet mit modernen Versionen von Chrome-, Edge- oder Firefox-Webbrowsern und Remote-Desktops. Jeder Benutzer benötigt eine eindeutige E-Mail-Adresse, die zu seinem Benutzernamen wird.

Netzwerkbandbreite

Für generierte Audio-Mediendaten, die zur Verarbeitung und Speicherung in Webex WFO hochgeladen werden, ist die Verfügbarkeit von Netzwerkbandbreite erforderlich. Um sicherzustellen, dass Uploads, Sprachkommunikation oder andere Kundenanwendungen nicht unterbrochen werden, wird dringend empfohlen, dass Sie den geschätzten Bandbreitenverbrauch anhand der folgenden Formeln berechnen und verstehen, wie sich dies auf Ihr Netzwerk auswirkt.

- Aufzeichnungszeit = (# der Benutzer) × (# der Anrufe pro Benutzer und Tag) × (durchschnittliche Anruflänge (Minuten))
- Upload-Bandbreite = Audio-Aufnahmen = 0,48 MB × Aufnahmezeit
- Die Bandbreite für das Hochladen des Bildschirms beträgt 1,5 MB pro Minute pro Monitor.

Sonstige Anforderungen

Unterstützte Umgebungen

Webex WFO unterstützt eine Reihe von Umgebungen und Technologien.

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

Desktop-Software

.NET Framework

Webex WFO Smart Desktop erfordert .NET Framework 4.5 für die Analysefunktion. Wenn Webex WFO nicht installiert ist, kann es keine Browserereignisse als Teil der Desktop Analytics-Daten erfassen. Sie

können die Datei

.NET Framework von http://www.microsoft.com/en-us/download/details.aspx?id=30653.

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 Erweiterung/das Plug-In für den Cisco Analytics-Browser 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 steht unter www.adobe.com zur Verfügung.

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.

PCI DSS-Konformität

HINWEIS Webex WFO v10.3 und höher unterstützt TLS v1.2 und ist TLS v1.1 veraltet.

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*

Dateiverschlüsselung

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

Kennwortrichtlinie

Anforderungen an die Kennwortkomplexität

Kennwörter müssen den folgenden Regeln entsprechen.

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

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

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

HINWEIS: Kennwörter laufen nicht ab.

Business-Continuity-Lösungen

Webex WFO bietet Hochverfügbarkeit und Redundanz in Cloud-Bereitstellungen mit zwei Methoden: Georeplikation für Azure-Teile Webex WFO-Cloud und Verfügbarkeitszonen für AWS-Teile Webex WFO-Cloud.

Georeplikation

Die Georeplikation bietet ein hohes Maß an Geschäftskontinuität, da sie die Wiederherstellungszeit verkürzt und Datenverluste im Zusammenhang mit einer Wiederherstellung im unwahrscheinlichen Fall eines Ausfalls eines ganzen Rechenzentrums begrenzt. Bei der Georeplikation werden Transaktionen, für die ein Commit ausgeführt wurde, in der primären Datenbank in eine sekundäre Datenbank in einem zweiten Rechenzentrum repliziert. Die maximale Menge an aktuellen Datenaktualisierungen, die der Dienst bei der Wiederherstellung nach einem Unterbrechungsereignis (z. B. einem verlorenen Rechenzentrum) verliert, wird als Wiederherstellungspunktziel (Recovery Point Objective, RPO) bezeichnet. Bei der Georeplikation beträgt das RPO 15 Minuten im Vergleich zu einer Woche bei der Standardlösung.

Availability Zones

Eine Region in Amazon Web Services (AWS) verfügt über mehrere Availability Zones. Die Verfügbarkeitszonen, die sich innerhalb einer AWS-Region befinden, sind vollständig unabhängige Rechenzentren. Availability Zones verfügen über redundante Stromversorgung und Netzwerkkonnektivität mit geringer Latenz innerhalb der AWS-Region, in der sie sich befinden. Dies bedeutet, dass Verfügbarkeitszonen vollständig von Ausfällen in anderen Verfügbarkeitszonen isoliert sind. Daher können Verfügbarkeitszonen verwendet werden, um Hochverfügbarkeit zu erreichen, ohne die Region zu verlassen, da in jeder Region Redundanz integriert ist.

Portnutzung

Die Portanforderungen für die Webex WFO-Edge-Komponenten und optionalen Webex WFO-Datenserverkomponenten 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:

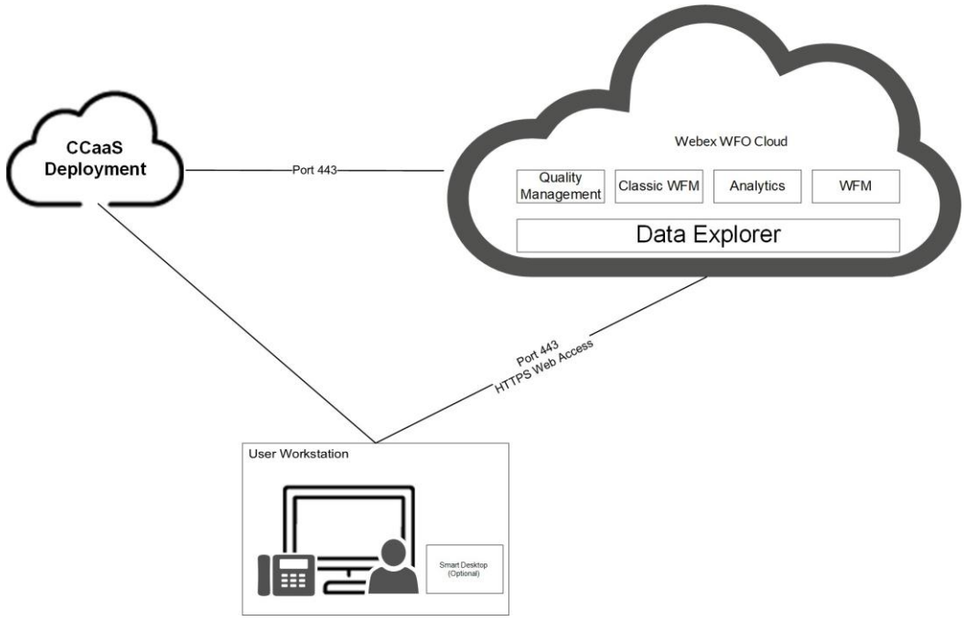
- Intelligenter Desktop

Datenserverkomponenten:

- Datenserver – ACD Sync: 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 Cisco Unified Communications Manager Netzwerkaufzeichnung
- Datenserver – Signalisierung: SIPREC

CCaaS-Anschlüsse

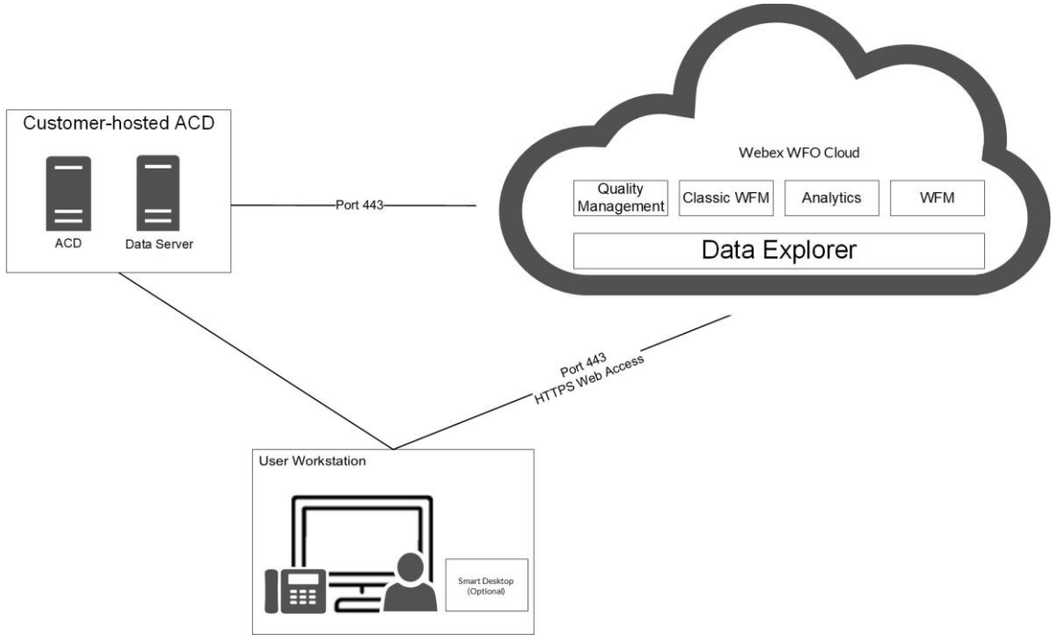
Für die Integration von CCaaS-Bereitstellungsmodellen muss Port 443 geöffnet sein. Anforderungen von Port 80 werden als HTTPS-Anforderungen an 443 umgeleitet.



Vom Kunden gehostete ACD Ports

Für vom Kunden gehostete Integrationen von Bereitstellungsmodellen muss Port 443 geöffnet sein. Anforderungen von Port 80 werden als HTTPS-Anforderungen an 443 umgeleitet.

Zusätzlich zu den Ports 80 und 443 muss für vom Kunden gehostete ACD-Bereitstellungsintegrationen auch Port 1433 geöffnet sein. Port 1433 ermöglicht eine Verbindung zu einer SQL Datenbank.



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 Abrechnungsservic e	—
TCP 8443	Kommunikation zwischen CUCM AXL und dem regionalen Datenserver ACD Synchronisierungseinstellungen auf dem Datenserver	Datenserver	CUCM AXL	—
Datenserver – ACD Synchronisierung: Cisco Unified CCE				
TCP 1433 TCP 1434	Kommunikation zwischen der Cisco Unified CCE AW SQL Server-Datenbank und dem regionalen Datenserver ACD Synchronisierungseinstellungen auf dem Datenserver	Datenserver	Cisco Unified CCE AWDB SQL Serverdatenbank	—
TCP 1433 TCP 1434	Kommunikation zwischen der Cisco Unified CCE HDS SQL Server-Datenbank und den beiden regionalen Datenserver-Abstimmungseinstellungen	Datenserver	Cisco Unified CCE HDS-SQL	—

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
	und die Einstellungen für die Erfassung des regionalen Datenservers ACD für die Daten Server		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 ACD Synchronisierungseinstellungen für den regionalen Datenserver und die regionalen Einstellungen für ACD "Data Server Capture"	Datenserver	Unified CCX 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	Datenserver	Cisco Unified	Seite B Standard. Das ist der RMCM

Port	Gebrauchen	Quelle	Ziel	Anmerkungen
	b) und die Einstellungen des Aufzeichnungs- CTI Signalisierungsservers auf dem Datenserver		CCX CTI Dienst (Seite B)	TCP in Unified CCX Systemparameter konfigurierte Port. Der Port des CTI Servers, der in der Unified CCX ACD Konfiguration konfiguriert ist.
Datenserver – GIS				
—	—	—	—	GIS lauscht zwar nicht direkt auf einen Port, aber die Dateien müssen auf den Datenserver kopiert werden. Erfolgt der Kopiervorgang über FTP, werden die Ports 20 und 21 verwendet.
Datenserver – Aufzeichnen/Erfassen				
UDP 39500–43500	RTP wird aufgezeichnet	Telefon oder Voice-Gateway	Audio-Aufnahme (Aufzeichnungs server)	—
UPD 49152–65535	Live-Audioüberwachung – RTP	Audioaufnahme (Aufzeichnungs server)	Browser des Vorgesetzten	—
Datenserver – Signalisierung: CTI				
TCP 443	Signalisierungsserver	Signalisierungsser ver	Cisco API	—
TCP 52102	Aufzeichnungssignalisierung	Audioaufnahme (Aufzeichnungss erver) oder Smart	Signalisierungsser ver	—

	Desktop

Port	Verwenden	Quelle	Ziel	Anmerkungen
		Kunden		
TCP 52103	Hazelcast	Signalisierungsserver Partner	Signalisierungsserver	—
Datenserver – Signalisierung: CTI, Cisco Unified Communications Manager Netzwerkaufzeichnung				
TCP 2748	JTAPI Signalisierung	Signalisierungsserver	Einheitlich CM Herausgeber und Abonnenten	—
TCP 5060 UDP 5060	SIP-Signalisierung von Unified CM	Jeder Unified CM-Herausgeber oder -Abonnent	Signalisierungsserver	Nicht sicher
TCP 5060	Signalisierungsserver	primärer Signalisierungsserver	sekundärer Signalisierungsserver	Bidirektional
TCP 5061	Sichere SIP-Signalisierung von Unified CM	Jeder Unified CM-Herausgeber oder Abonnent	Signalisierungsserver	Sicher. Wird normalerweise 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	—

Port	Verwenden	Quelle	Ziel	Anmerkungen
TCP 59106	Aufzeichnungssignalisierung	Audioaufnahme (Aufzeichnungsserver)	Signalisierungsserver	—
TCP 59107	Hazelcast	Signaling Server-Partner	Signalisierungsserver	—

Informationen zum Speicher

Es ist wichtig, den Unterschied im erforderlichen Speichertyp in Webex WFO zu beachten.

Der Medienspeicher ist der permanente Speicher für Mediendateien. Es eignet sich für die Langzeitspeicherung und wird nicht zur Wiedergabe verwendet, es sei denn, der Hochgeschwindigkeitsnetzwerkspeicher ist ebenfalls für die Verwendung desselben Speicherorts konfiguriert.

„High Speed Network Storage“ bezieht sich auf das Hochgeschwindigkeitsnetzwerk, das zum Speichern temporärer Dateien, des Ordnerspeicherorts, in dem die gesamte Betriebsverarbeitung stattfindet und in dem Analysedaten (Lucene) gespeichert werden, verwendet wird. Hierzu gehören die Verarbeitung von Massenexporten, die Lokalisierung des Lucene-Index, die Medienkonvertierung, die Medienwiedergabe und Dateien, die mit Ausnahme von Analysen nach 24 Stunden vom System gelöscht werden.

> **HINWEIS** Analysedateien werden in einem Hochgeschwindigkeitsnetzwerkspeicher abgelegt, sind jedoch nicht in der Dateilöschung durch das System im Laufe des Tages enthalten.

Wenn die Wiedergabe eines Anrufs angefordert wird, ruft das System die Datei aus dem permanenten Speicher ab und legt sie für den sofortigen Zugriff im temporären Verzeichnis auf der Ebene des Hochgeschwindigkeitsnetzwerkspeichers ab. Von dort aus führt es Transkodierung und Streaming durch.

Admin-Konfiguration

Bei der Erstkonfiguration des Systems wird der **Standardspeicherort für Medien** auf der Seite „Speicherort“ des Systemadministrators konfiguriert.

> **HINWEIS:** Bei der Ersteinrichtung ist der **Standardspeicherort für Medien** Ihr Hochgeschwindigkeitsnetzwerkspeicher und Medienspeicherort. Weitere Maßnahmen sind erforderlich, um den Hochgeschwindigkeitsnetzwerkspeicher und den Medienspeicher an verschiedenen Standorten aufzuteilen. Netzwerk- und Medienspeicherorte haben sich drastisch verändert
> Unterschiedliche Leistungsmerkmale. Aus diesem Grund wird die Auswahl beider Optionen als Standardspeicherort nicht empfohlen, da dies zu Leistungsproblemen führen kann.

Konfigurieren Sie separate Netzwerk- und Medienspeicherorte

1. Navigieren Sie vor dem Erstellen eines Mandanten zum Systemadministratorportal > Anwendungsverwaltung
   > Systemkonfiguration > Speicherort.
2. Klicken Sie auf **Neuen Speicherort erstellen**.
3. Um einen Hochgeschwindigkeits-Netzwerkspeicherort zu erstellen, geben Sie im Feld **Name** einen

eindeutigen Namen ein.

4. Wählen Sie in der Dropdownliste „Typ“ die Option **Netzwerk (Sofortzugriff)** aus.
5. Aktivieren Sie unter **Standardeinstellungen** das Kontrollkästchen **Netzwerk** .

6. Konfigurieren Sie die verbleibenden **Felder der Netzwerkspeicherkonfiguration** .
7. Klicken Sie auf **Speichern**.
8. Um einen Medienspeicherort zu erstellen, navigieren Sie zurück zu Anwendungsverwaltung > Speicherort.
9. Klicken Sie auf **Neuen Lagerort** anlegen.
10. Um einen Medienspeicherort zu erstellen, geben Sie einen eindeutigen Namen in das **Feld Name** ein.
11. In der Dropdown-Liste Typ ist Netzwerk **(sofortiger Zugriff)** vorausgewählt.
12. Aktivieren Sie unter **"Standardeinstellungen**" das **Kontrollkästchen "Medien** ".
13. Konfigurieren Sie die verbleibenden **Felder der Netzwerkspeicherkonfiguration** .
14. Klicken Sie auf **Speichern**.

BEST PRACTICE : Löschen Sie den ursprünglichen **Standard-Medienspeicherort** , nachdem die neuen Speicherorte für den Netzwerk- und Medienspeicher konfiguriert wurden.

Tenant-Speicher konfigurieren

Führen Sie dieses Verfahren aus, wenn Sie über das Systemadministratorportal einen neuen Mandanten erstellen.

1. Navigieren Sie zu Anwendungsverwaltung > Mandantenverwaltung > Mandanten.
2. Suchen Sie im Abschnitt Speicherort den standardmäßigen Hochgeschwindigkeitsnetzwerkspeicherort, und aktivieren Sie das Kontrollkästchen **Verfügbar** .
3. Suchen Sie den Standard-Medienspeicherort, und aktivieren Sie die Kontrollkästchen "Verfügbar **" und** " **Standard** ".
4. Klicken Sie auf **Speichern**.
5. Melden Sie sich zum Überprüfen beim Mandanten an, und navigieren Sie zu Anwendungsverwaltung > Systemkonfiguration > Speicherprofile.
6. Klicken Sie auf die **Dropdown-Liste Speicherort** . Die Netzwerk- und Medienspeicherorte werden in der Dropdown-Liste angezeigt.

   HINWEIS: Wählen Sie Netzwerkspeicher nicht als Speicherprofil aus.

Speicherebenen

Es gibt drei Speicherebenen für Kontaktdaten:

- Amazon S3 (sofortiger Zugriff) – Amazon S3-Speicher (Standard) wird für die kurzfristige Speicherung (12 bis 24 Monate) von alltäglichen Betriebsinhalten verwendet, z. B. Mediendateien (Sprache und Bildschirm) und Verlaufsdaten für Berichte, Prognosen und Planung. Die Antwortraten auf Benutzeranfragen können wie folgt lauten:

Nahezu sofort in Sekundenschnelle, kann jedoch je nach Datenmenge oder Datentyp leicht variieren.

- Amazon S3 Shared (Immediate Access) – Ähnlich wie die Amazon S3-Speicherebene, mit der Ausnahme, dass mehrere Mandanten ihre Daten innerhalb desselben Amazon S3-Speicher-Buckets in einem mandantenspezifischen Ordner speichern.
- Netzwerk (sofortiger Zugriff) – Netzwerkspeicher (Leistung) wird für benutzergesteuerte Medieninhalte, Analysen und Datamart-Inhalte verwendet. Hierbei handelt es sich um ein SAN (Storage Area Network) oder einen Dateiserver. Es bietet eine nahezu sofortige Antwortrate auf Benutzeranfragen. Diese Daten befinden sich für einen im Workflow definierten Zeitraum und werden anschließend gelöscht. Optional können Administratoren einen gestaffelten Uploadspeicherort angeben, an dem Daten gespeichert werden, bevor sie an den langfristigen Echtzeit-Datenspeicherort hochgeladen werden.

Sie können sich auch dafür entscheiden, Ihre Daten nach Ablauf der Aufbewahrungsfrist von einem Drittanbieter speichern zu lassen. Nachdem die Daten gespeichert wurden, werden sie aus Webex WFO gelöscht. Wenn Sie gespeicherte Daten abrufen, müssen Sie andere Anwendungen als Webex WFO verwenden, um sie zu überprüfen.

- Mandanten: Verwenden Sie den Abschnitt "Mandantenspeicherort" auf der Seite "Mandanten", um den Speicherort für jeden Mandanten zuzuweisen und zu definieren.

Storage-Angebote

Webex WFO Cloud verwendet intelligentes Tiering für den Speicher mit einem einzigen Preis pro GB und Monat für Ihre Gesamtnutzung. Neue Dateien und Dateien, auf die kürzlich zugegriffen wurde, sind sofort verfügbar. Ältere Dateien, auf die in letzter Zeit nicht zugegriffen wurde, werden von einer etwas langsameren Speicherebene abgerufen, auf die sie möglicherweise verschoben wurden. Das Abrufen älterer Dateien dauert in der Regel nur wenige Sekunden.

Massenimport und -Export von Daten

In diesem Thema werden Methoden zum Importieren und Exportieren von Daten in Webex WFO beschrieben.

Massenimport und -Export von Daten über Webex WFO

Webex WFO können Sie verschiedene Datentypen importieren und exportieren. Im Folgenden wird beschrieben, welche Daten importiert und exportiert werden können und wie sie importiert und exportiert werden können. Datendateien, die importiert oder exportiert werden, weisen CSV Format auf. Folgende Datentypen können importiert und exportiert werden:

- Sie können Benutzer, Teams und Gruppen global importieren und exportieren.
- In Analytics können Sie Phrasen und Anwendungen importieren und exportieren.
- In Quality Management können Sie Evaluierungsformulare importieren und exportieren sowie Kontaktdaten exportieren.

HINWEIS Der Massenexport von Stammaufzeichnungen durch Kontakte wird nicht unterstützt.

Import- und Export-APIs

Diese APIs stellen REST-ähnliche Endpunkte zum Importieren und Exportieren von Daten zur Verfügung:

- Importieren API: Ermöglicht das Abrufen von Informationen zu den Back-End-Objektmodellen (die Back-End-Modellfelder und die diesen Feldern zugeordneten Typen) und das Importieren dieser Daten aus CSV-Dateien in diese Back-End-Modelle
- Export API: Ermöglicht das Abrufen von Daten aus den Back-End-Modellen in einem CSV Format.

Weitere Informationen finden Sie im WFO API Reference Guide Webex.

Exportieren von Kontakten in großen Mengen

Sie können Daten für mehrere Kontakte exportieren, indem Sie die Option "Massen-Kontaktexport" in der Dropdown-Liste der Optionen der Seite "Interaktionen" verwenden. Exportierte Dateien werden in entsprechend benannten Ordnern an einem externen Speicherort gespeichert. Der externe Speicher kann so konfiguriert werden, dass er sofortigen oder sofortigen Zugriff ermöglicht. Weitere Informationen zu externem Speicher finden Sie unter "Konfigurieren von Speicherprofilen" im Webex WFO-Benutzerhandbuch.

HINWEIS: Kontakte und Metadaten werden als CSV Dateien exportiert.

Planen eines wiederkehrenden Massenkontaktexports

1. Erstellen und speichern Sie auf der Seite Interaktionen einen Filtersatz.

   WICHTIG: Sie müssen alle Filter, die Sie Ihrem Filtersatz hinzufügen, vollständig konfigurieren. Wenn Sie nicht alle Filter vollständig konfigurieren, schlägt der Massen-Kontextexport fehl.

   BEISPIEL Sie fügen den **Filter "Predictive Net Promoter Score** " zu Ihrem Filtersatz hinzu. Sie wählen **"Ist gleich"** aus der **Dropdown-Liste "Operator** ", geben aber im Feld "Ergebnis **" keine Zahl** ein. Wenn dieser Filter nicht vollständig konfiguriert ist, schlägt der Export von Massenkontakten fehl.

2. Klicken Sie auf das **Symbol Optionen** und anschließend auf Massenexport **von**Kontakten.
3. Klicken Sie auf die **Registerkarte Neuer Export** .
4. Konfigurieren Sie den Export entsprechend der Definition in den unten beschriebenen Feldern.

   Exportname – Geben Sie einen Namen für die Exportdatei für Massenkontakte ein.

   Gespeicherte Suche : Wählen Sie Ihren gespeicherten Filtersatz aus.

   Speicherort – Wählen Sie den externen Speicherort aus, in den Sie die Kontakte exportieren möchten.

   Medientyp – Wählen Sie das Dateiformat aus, in das Webex WFO Audio- und Videodateien exportiert.

   - **Audio-/Videoformate – Wählen Sie das Dateiformat** aus, in das die Audio-/Videomedien exportiert werden sollen. Nur für Kontakte mit Audio- und Bildschirmaufzeichnungen verfügbar.
   - **Nur-Audio-Formate** : Wählen Sie das Dateiformat aus, in das die reinen Audiomedien exportiert werden sollen. Nur für Kontakte mit Audioaufzeichnungen verfügbar.
   - **Keine** : Wählen Sie Nur **Transkriptionen aus** , um nur Transkripts zu exportieren.

   Analytics-Ausgabeformat : Wählen Sie das Dateiformat aus, in das Sie Analytics-Transkriptionsdaten exportieren möchten: JSON oder XML. Wenn Sie "Kein" **auswählen**, exportiert Webex WFO keine Analytics-Transkriptionsdaten. Wählen Sie **"Keine** ", um nur eine CSV Datei mit Metadaten zu exportieren.

5. Wählen Sie Geplante Ausfuhr **senden aus, und planen Sie**den Export wie unten beschrieben.

   Wöchentlich – Wählen Sie einen oder mehrere Wochentage aus, und wählen Sie dann die Uhrzeit aus, zu der Webex Kontakte von WFO exportiert werden sollen.

   Monatlich – Wählen Sie den Tag des Monats und dann die Uhrzeit aus, an der Webex WFO die Kontakte exportieren soll.

6. Klicken Sie auf **Erstellen**.

Wenn Sie einen geplanten Massenkontaktexport erstellen, wird der Export Webex WFO gespeichert. Um den Export zu bearbeiten, klicken Sie auf die **Registerkarte "Export** gespeicherter Kontakte" und wählen Sie den Export aus der **Dropdown-Liste "Dateiname** des gespeicherten Exports" aus.

HINWEIS: Der erste geplante Export (wöchentlich oder monatlich) muss nach der nächsten geplanten Ausführung der Aufgabe "dynamische App-Aktualisierung" erfolgen. Andernfalls findet der erste geplante Export nicht statt.
Obwohl zukünftige Exporte dies tun werden. Standardmäßig wird die Aufgabe "dynamische App-Aktualisierung" alle fünfzehn Minuten ausgeführt. Wenden Sie sich an den Systemverwalter, um diesen Zeitplan zu überprüfen.

Sofortiges Exportieren von Kontakten

1. Erstellen und speichern Sie auf der Seite Interaktionen einen Filtersatz.

   WICHTIG: Sie müssen alle Filter, die Sie Ihrem Filtersatz hinzufügen, vollständig konfigurieren. Wenn Sie nicht alle Filter vollständig konfigurieren, schlägt der Massen-Kontextexport fehl.

   BEISPIEL Sie fügen den **Filter "Predictive Net Promoter Score** " zu Ihrem Filtersatz hinzu. Sie wählen **"Ist gleich"** aus der **Dropdown-Liste "Operator** ", geben aber im Feld "Ergebnis **" keine Zahl** ein. Wenn dieser Filter nicht vollständig konfiguriert ist, schlägt der Export von Massenkontakten fehl.

2. Klicken Sie auf das **Symbol Optionen** und anschließend auf Massenexport **von**Kontakten.
3. Klicken Sie auf die **Registerkarte Neuer Export** .
4. Konfigurieren Sie den Export wie unten beschrieben.

   Exportname – Geben Sie einen Namen für die Exportdatei für Massenkontakte ein.

   Gespeicherte Suche : Wählen Sie Ihren gespeicherten Filtersatz aus.

   Speicherort – Wählen Sie den externen Speicherort aus, in den Sie die Kontakte exportieren möchten.

   Medientyp – Wählen Sie das Dateiformat aus, in das Webex WFO Audio- und Videodateien exportiert.

   - **Audio-/Videoformate – Wählen Sie das Dateiformat** aus, in das die Audio-/Videomedien exportiert werden sollen. Nur für Kontakte mit Audio- und Bildschirmaufzeichnungen verfügbar.
   - **Nur-Audio-Formate**: Wählen Sie das Dateiformat aus, in das die reinen Audiomedien exportiert werden sollen. Nur für Kontakte mit Audioaufzeichnungen verfügbar.
   - **Keine** : Wählen Sie Nur **Transkriptionen aus** , um nur Transkripts zu exportieren.

   Analytics-Ausgabeformat : Wählen Sie das Dateiformat aus, in das Sie Analytics-Transkriptionsdaten exportieren möchten: JSON oder XML. Wenn Sie "Kein" **auswählen**,

exportiert Webex WFO keine Analytics-Transkriptionsdaten. Wählen Sie **"Keine** ", um nur eine CSV Datei mit Metadaten zu exportieren.

5. Wählen Sie "Export sofort **senden" aus**.
6. Klicken Sie auf **Erstellen**.

Genehmigungsvoraussetzungen für den Export von Massenkontakten

Cisco fordert Sie auf, einen Lizenztyp für den Massenexport von Kontakten auszuwählen.

- **Standardlizenz** – Exportieren Sie täglich bis zu 1.000 Kontakte über die Benutzeroberfläche.
- **Leistungslizenz**: Exportieren Sie Kontakte in großen Mengen, indem Sie in regelmäßigen Abständen jeden Tag mehrere Kontaktexportaufträge konfigurieren.

HINWEIS Standardmäßig ist jeder Exportbatch auf 10.000 pro Auftrag beschränkt, wobei die maximale Anzahl der Gesamtkontakte pro Tag bei 40.000 mit der Performance-Lizenz liegt. Wenn eine Erhöhung dieser

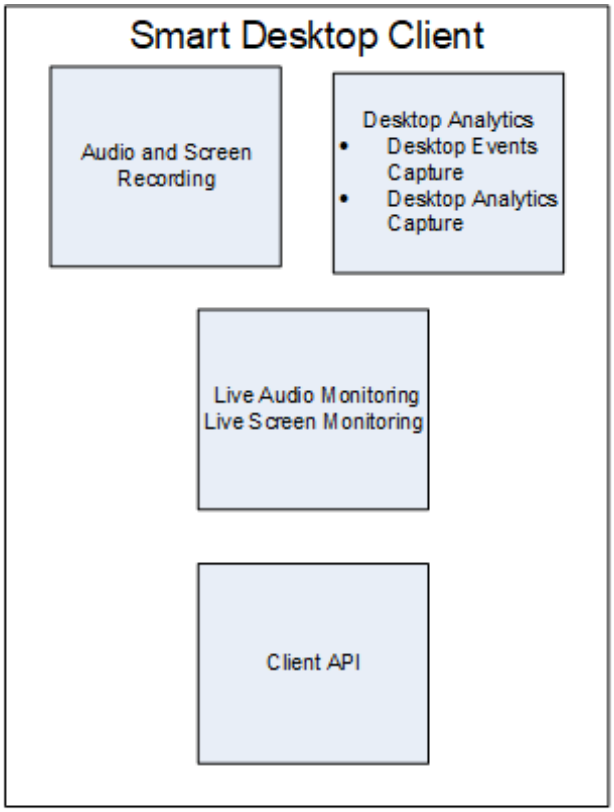
Wenden Sie sich an Cisco Professional Services oder den Cisco Support Services.

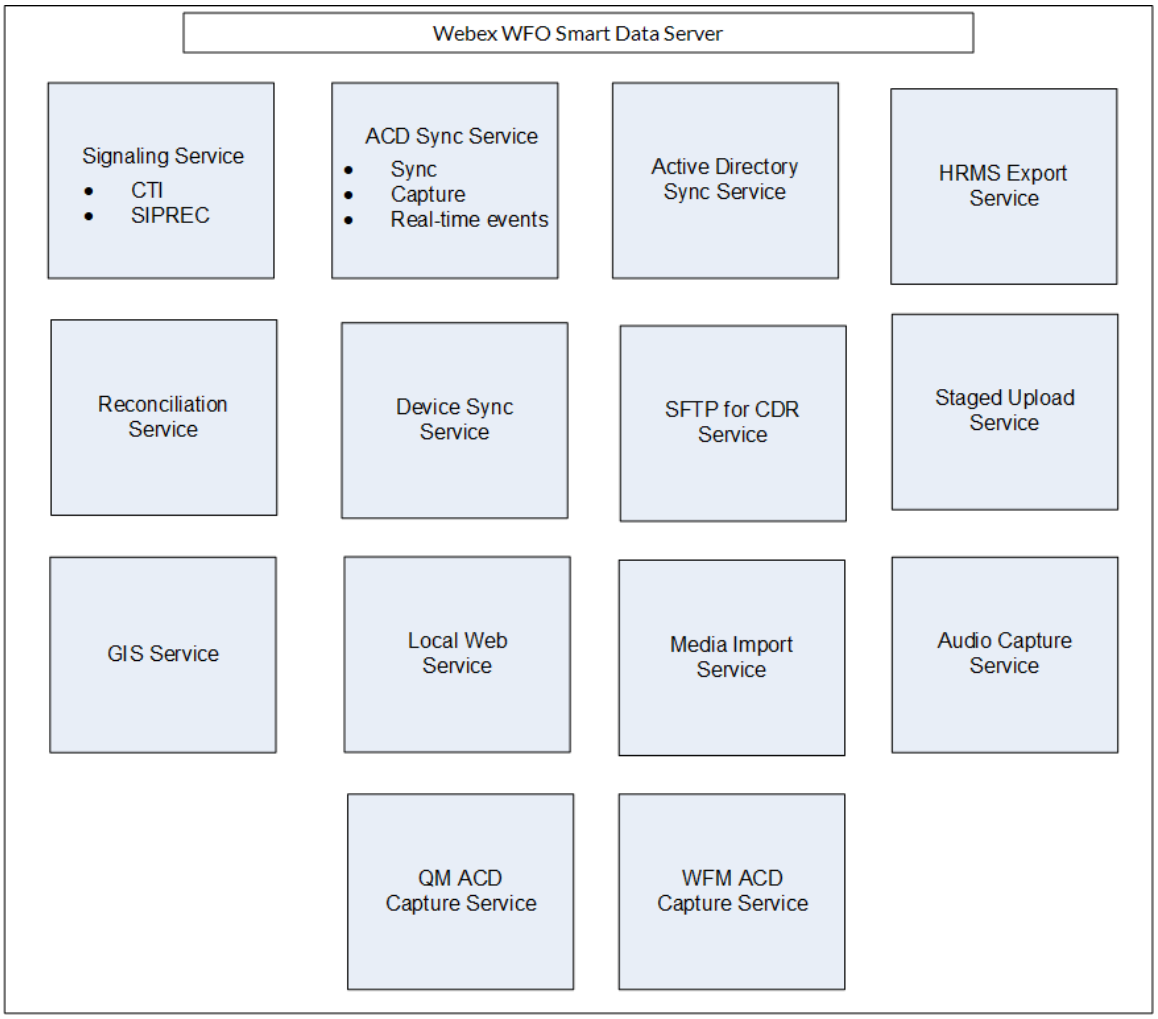
Speichern von und Zugreifen auf Bulk-Kontaktdateien

Webex WFO exportiert und speichert Massen-Kontaktdateien im Ordner "Exporte" an dem von Ihnen konfigurierten externen Speicherort (siehe "Anwendungsverwaltung> globale >Systemkonfiguration > Externer Speicher").

Edge-Komponenten

Die Webex WFO-Edge-Komponenten bestehen aus dem Webex WFO Smart Desktop Client. Webex WFO Smart Desktop können Sie den Status eines Agenten anzeigen, einen Anruf mithören und den Bildschirm des Agenten in Echtzeit anzeigen. Der Webex WFO-Datenserver ist eine optionale Komponente, die von Ihrem Cloud-Integrationsmodell abhängt.





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

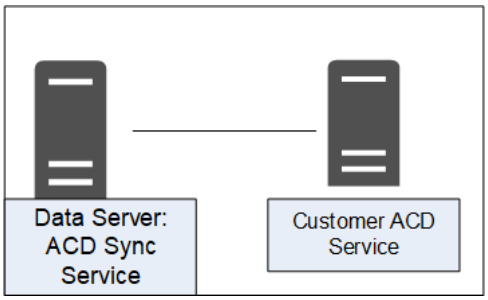
In Webex WFO sind die folgenden Funktionen des Datenservers, ihre Beschreibungen und der Service, an dem sie ausgerichtet sind, aufgeführt.

- 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).

Webex WFO ACD Sync-Dienst

Der ACD Sync-Dienst wird verwendet, um Benutzer- und Teaminformationen von einem unterstützten ACD zu synchronisieren. Der Synchronisierungsprozess wird alle zehn Minuten ausgeführt, um alle im ACD vorgenommenen Änderungen in Webex WFO zu aktualisieren.



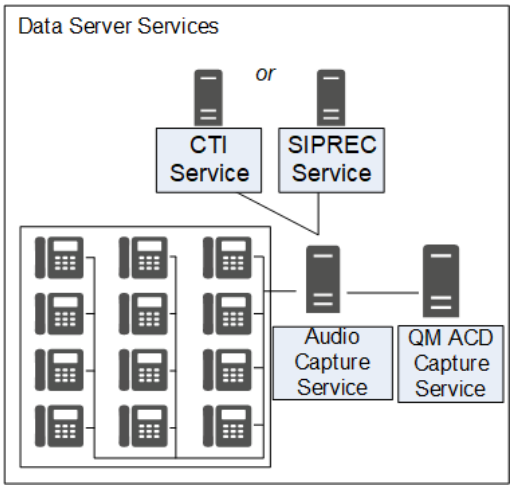
ACD Synchronisierungsdienst-Konnektivität

In der folgenden Tabelle sind die grundlegenden Verbindungsfunktionen zum ACD Sync-Dienst aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
ACD Service für Mieter	Aktualisierungen ACD Agenten- oder Teaminformationen

Webex WFO-Audioaufnahmeservice

Webex WFO verwendet den Audio Capture-Dienst für Audioaufzeichnungsumgebungen mit Edgeservern oder Gateways (SBC). Er kann Clustern zugewiesen werden. Der primäre Signalisierungsdienst (CTI oder SIPREC) weist Anrufe den Erfassungsservern in einem Round-Robin-Algorithmus zu. Audioaufnahmedienste können als aktiv/aktiv oder aktiv/Standby konfiguriert werden.



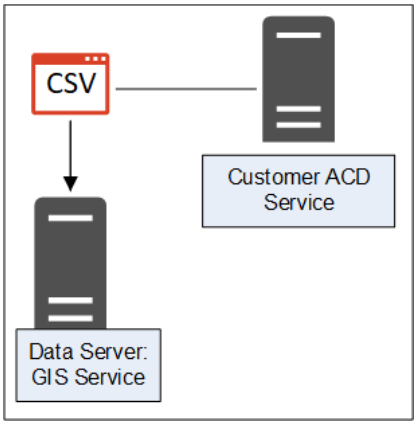
Verbindung mit dem Audio-Capture-Dienst

In der folgenden Tabelle sind die grundlegenden Verbindungsmöglichkeiten zum Audio Capture-Service aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
CTI-Dienst	Empfängt Signale für Audioaufnahmen
SIPREC-Dienst	Empfängt Signale für Audioaufnahmen

Webex WFO GIS-Service

Mithilfe des GIS-Service (Generic Interface Service) können Sie Metadaten für externe Kontakte aus einer . CSV Datei in Webex WFO ein.



GIS-Service-Konnektivität

In der folgenden Tabelle sind die grundlegenden Verbindungen zum GIS-Service aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
ACD Service für Mieter	Aktualisierungen ACD Agenten- oder Teaminformationen
Äußerlich. CSV Datei	Externe Flatfile-Quelle für Aktualisierungen von Agenten- oder Teaminformationen Kann eine oder mehrere Dateien sein

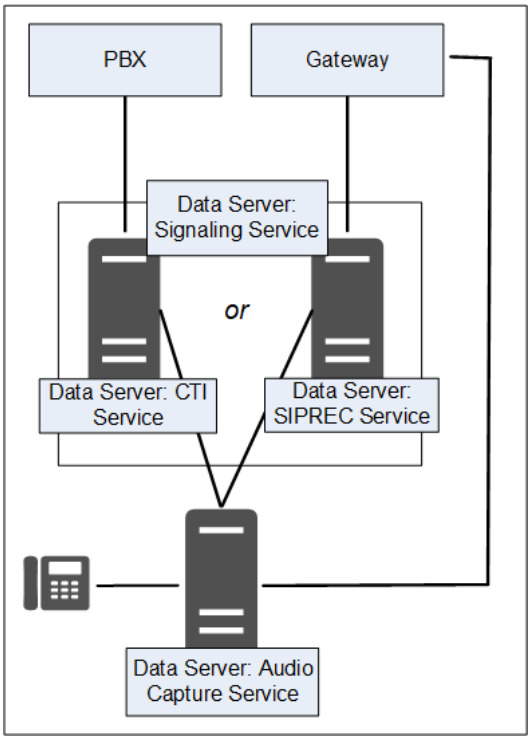
Webex WFO-Signalservice

Ihr Signalisierungsservice kann entweder CTI oder SIPREC sein:

- Ein CTI Signaldienst wird für Edgeserver-Aufzeichnungsumgebungen verwendet, um Start- und Stoppereignisse nachzuverfolgen und CTI Metadaten für Anrufaufzeichnungen zu erfassen.
- Ein SIPREC-Signalisierungsdienst wird für Edge-Gateway-Aufzeichnungsumgebungen (SBC) verwendet, um Start- und Stoppereignisse zu verfolgen und SIPREC-Metadaten für Anrufaufzeichnungen zu erfassen.

Sie können entweder den CTI- oder den SIPREC-Dienst für Redundanz konfigurieren.

HINWEIS Der Audioaufnahmedienst kann nur mit einer Telefoniegruppe verknüpft werden, die einen CTI- oder SIPREC-Dienst enthält.



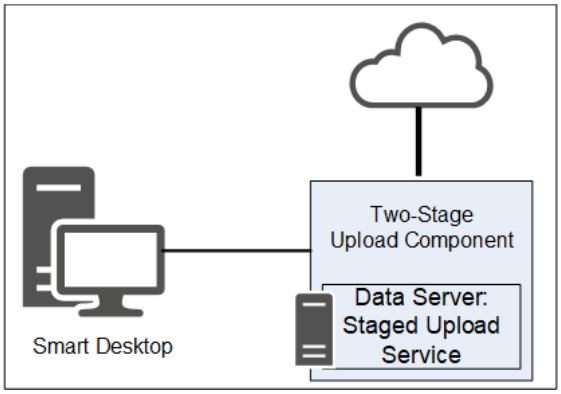
Signalservice-Konnektivität

In der folgenden Tabelle sind die grundlegenden Verbindungsmöglichkeiten zum Signalservice aufgeführt:

Typ	Verbindung mit Service herstellen
CTI	PBX-Dienst
	Audio-Capture-Service
SIPREC	Gateway-/SBC-Service
	Audio-Capture-Service
	QM ACD-Capture-Service

Webex WFO-Service für gestaffelten Upload

Der Webex WFO-Dienst sammelt lokal Kontaktdaten von Smart Desktop Client-Benutzern und lädt die Dateien in regelmäßigen Abständen in die Webex WFO-Komponenten in der Cloud hoch.



Zweistufige Upload-Komponente

Mit der zweistufigen Upload-Komponente können Sie in regelmäßigen Abständen Daten vom Datenserver an die Webex WFO-Kernkomponenten senden.

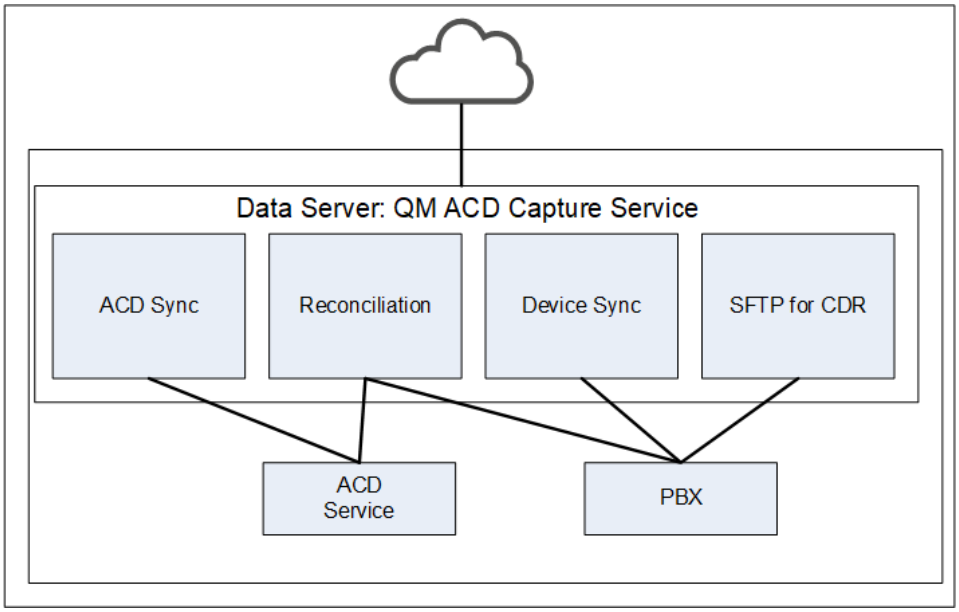
Verbindung mit dem gestaffelten Upload-Dienst

In der folgenden Tabelle sind die grundlegenden Verbindungsmöglichkeiten zum Service für den gestaffelten Upload aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
ACD Service für Mieter	Aktualisierungen ACD Agenten- oder Teaminformationen

Webex WFO QM ACD Capture-Service

Webex WFO verwendet den QM ACD Capture-Service, um benutzerdefinierte Metadaten zu erfassen und über ein Gateway eingehende Anrufe abzugleichen.



Komponenten QM ACD Capture Service

Der QM ACD Capture-Service besteht aus vier Komponenten:

- QM ACD Verlaufserfassungskomponente
- QM ACD Echtzeiterfassungskomponente
- QM GIS-Erfassungskomponente

QM ACD Historical Capture-Komponente

Die QM ACD Historical Capture-Komponente erfasst benutzerdefinierte Metadaten und Abstimmungsdaten aus dem ACD.

QM ACD Komponente "Echtzeiterfassung"

Die QM ACD Echtzeiterfassungskomponente erfasst Kontaktdaten.

QM GIS-Erfassungskomponente

Die QM GIS-Erfassungskomponente importiert Metadaten aus externen QM Kontakten.

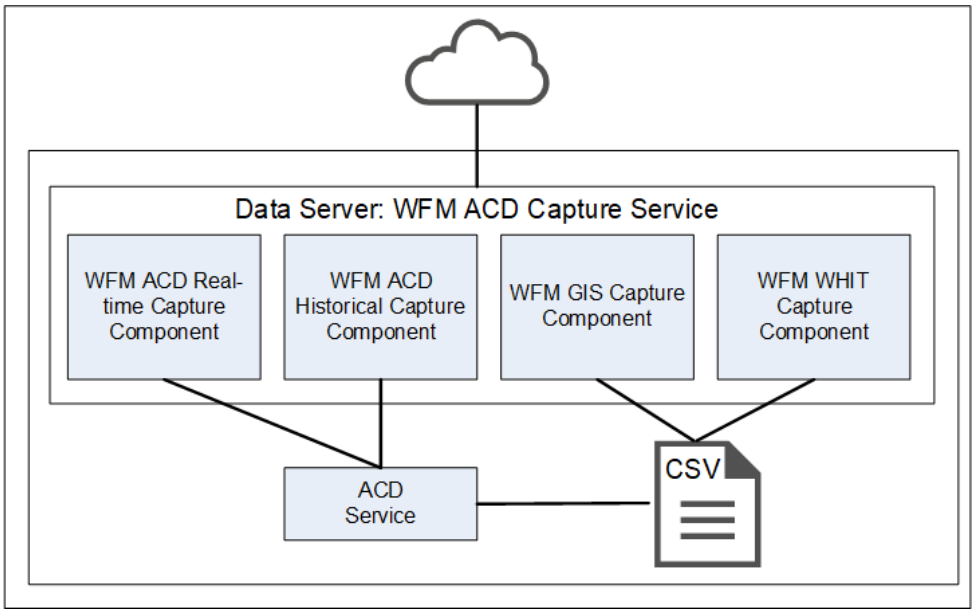
QM ACD Capture Service-Konnektivität

In der folgenden Tabelle sind die grundlegenden Verbindungsmöglichkeiten zum QM ACD Capture-Service aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
ACD Service für Mieter	Aktualisierungen ACD Agenten- oder Teaminformationen

Webex WFO WFM ACD Erfassungsservice

Der Webex WFO WFM ACD Capture-Service erfasst ACD Verlaufs- und Echtzeitdaten für WFM und ACD Metadaten, die als benutzerdefinierte Metadaten an Anrufkontakte angehängt werden.



Komponenten WFM ACD Capture Service

Der WFM ACD Capture-Service besteht aus vier Komponenten:

- WFM ACD Verlaufserfassungskomponente
- WFM ACD Echtzeiterfassungskomponente
- WFM GIS-Erfassungskomponente
- WFM WHIT-Erfassungskomponente

WFM ACD Historical Capture-Komponente

Die WFM ACD Historical Capture-Komponente erfasst historische und Echtzeit-ACD-Daten für WFM sowie Metadaten zur ACD, die als benutzerdefinierte Metadaten an Anrufkontakte angehängt werden können.

WFM ACD Komponente "Echtzeiterfassung"

Die WFM ACD Echtzeiterfassungskomponente erfasst Kontaktdaten.

WFM GIS-Erfassungskomponente

Die WFM GIS-Erfassungskomponente erfasst ACD Daten von nicht direkten ACDs.

WFM WHIT-Capture-Komponente

Mit der WFM WHIT-Erfassungskomponente können Sie historische ACD Daten importieren.

WFM ACD Capture-Servicekonnektivität

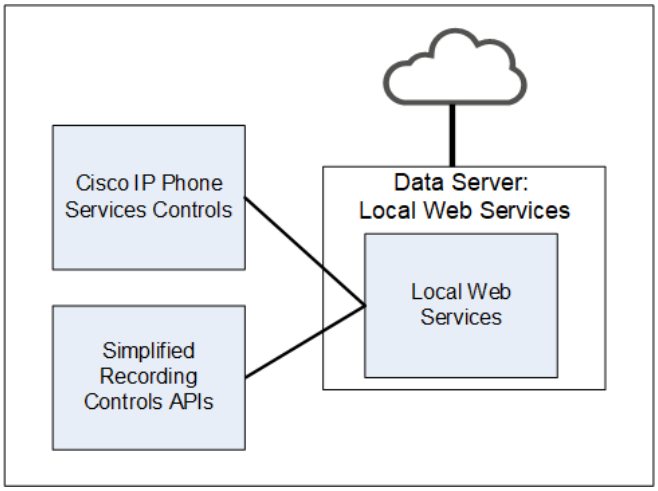
In der folgenden Tabelle sind die grundlegenden Verbindungsfunktionen zum WFM ACD Capture-Service aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
ACD Service für Mieter	Aktualisierungen ACD Agenten- oder Teaminformationen

Webex WFO Local Web Services-Dienst

Der Webex WFO Local Web Services Data Server-Service ermöglicht Aufzeichnungssteuerungen und die systemeigene Datenserver-Authentifizierung.

HINWEIS: Der Local Web Services-Service wird bei Bereitstellungen von CCaaS-Anbietern nicht unterstützt.



Komponenten des lokalen Web-Services-Dienstes

Der Local Web Services-Service besteht aus zwei Komponenten:

- Cisco IP Phone Komponente "Services-Steuerungen"
- Vereinfachte Aufzeichnungssteuerung API Komponente

Cisco IP Phone Komponente "Services-Steuerungen"

Die Komponente "Cisco IP Phone Dienststeuerung" ermöglicht die Aufzeichnungssteuerung von Cisco unterstützten Cisco-Geräten.

Vereinfachte Aufzeichnungssteuerung API Komponente

Die Komponente "Vereinfachte Aufzeichnungssteuerungen API" ermöglicht die Verwendung der nativen Datenserver-Authentifizierung für die Aufzeichnungssteuerungen von Cisco.

Verbindung mit lokalen Web-Services-Diensten

In der folgenden Tabelle sind die grundlegenden Verbindungen zum lokalen Web-Services-Service aufgeführt:

Verbindung mit Service herstellen	Eingänge/Ausgänge
Vereinfachte Aufzeichnungssteuerung API	Datenserver-Authentifizierung für Cisco-Aufzeichnungssteuerungen
Cisco IP Phone Services-Steuerelemente	Ermöglicht die native Datenserver-Authentifizierung für Cisco-Aufzeichnungssteuerungen

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 Portnutzung.

Installieren des Datenservers für einen einzelnen Tenant

Ein Besitzeradministrator kann den Datenserver für einen einzelnen Besitzer installieren.

Installieren des Datenservers für einen einzelnen Tenant

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

Den Datenserver testen

1. Melden Sie sich bei Webex WFO als 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.

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.

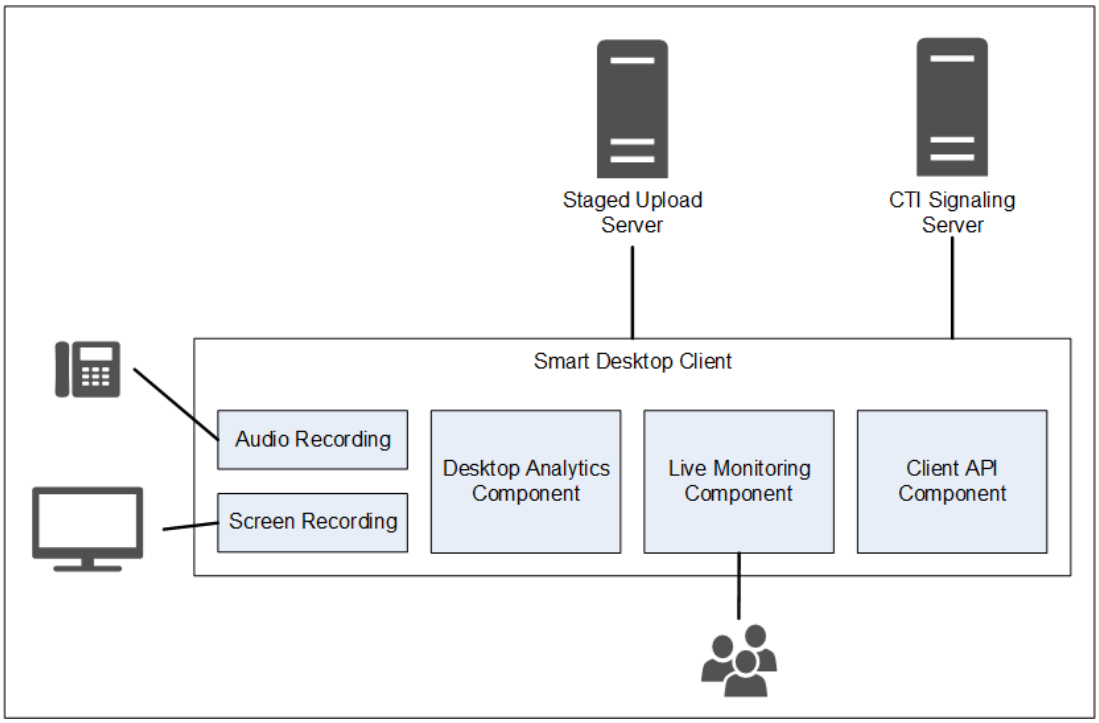
Die Audioaufzeichnung mit Smart Desktop hängt vom Aufzeichnungstyp ab. CCaaS-Lösungen (Contact Center-as-a-Service) zeichnen Audio auf und senden die Datei, nachdem der Kontakt abgeschlossen ist. Vom Kunden gehostete Lösungen senden SIP- und RTP Protokolle, da der Kontakt live ist. Webex WFO führt Bildschirmaufzeichnungen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

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. Da jeder weitere Monitor separat aufgezeichnet wird, müssen Sie 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

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	Gebrauchen	Quelle	Ziel	Anmerkungen
Intelligenter Desktop				
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:

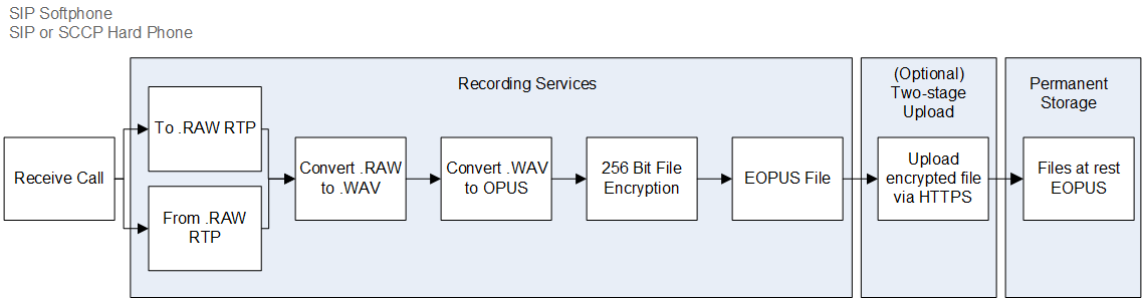
Kontakt-Metadaten	SIP-Signalisierung	SCCP Signalisierung	RTP Protokollierung
Anruf-ID	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC-API
ANI (Anruf)	X	X	Stützt sich auf Drittanbieter, um Echtzeitdaten bereitstellen DCC-API
DNIS (angerufen)	X	X	Stützt sich auf Drittanbieter, um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

Kontakt-Metadaten	SIP-Signalisierung	SCCP Signalisierung	RTP Protokollierung
Anrufrichtung	X	X	Verlassen Sie sich auf Drittanbieter, um Echtzeitdaten für DCC-API bereitzustellen
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

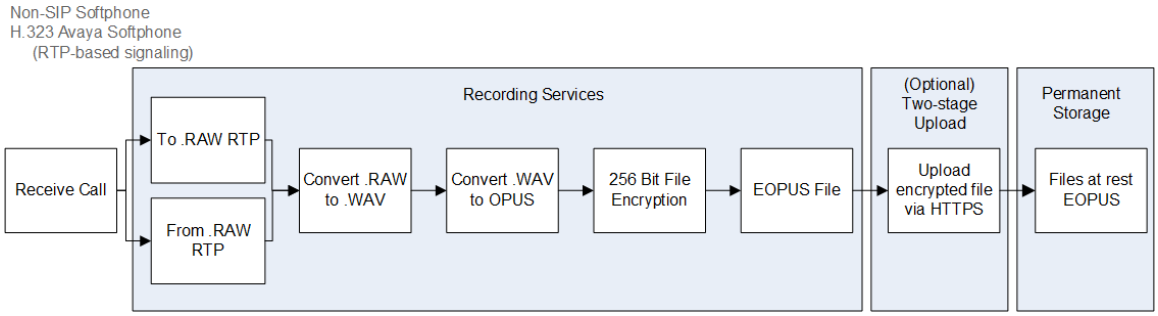
Smart Desktop Capture-Datenflussdiagramme

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

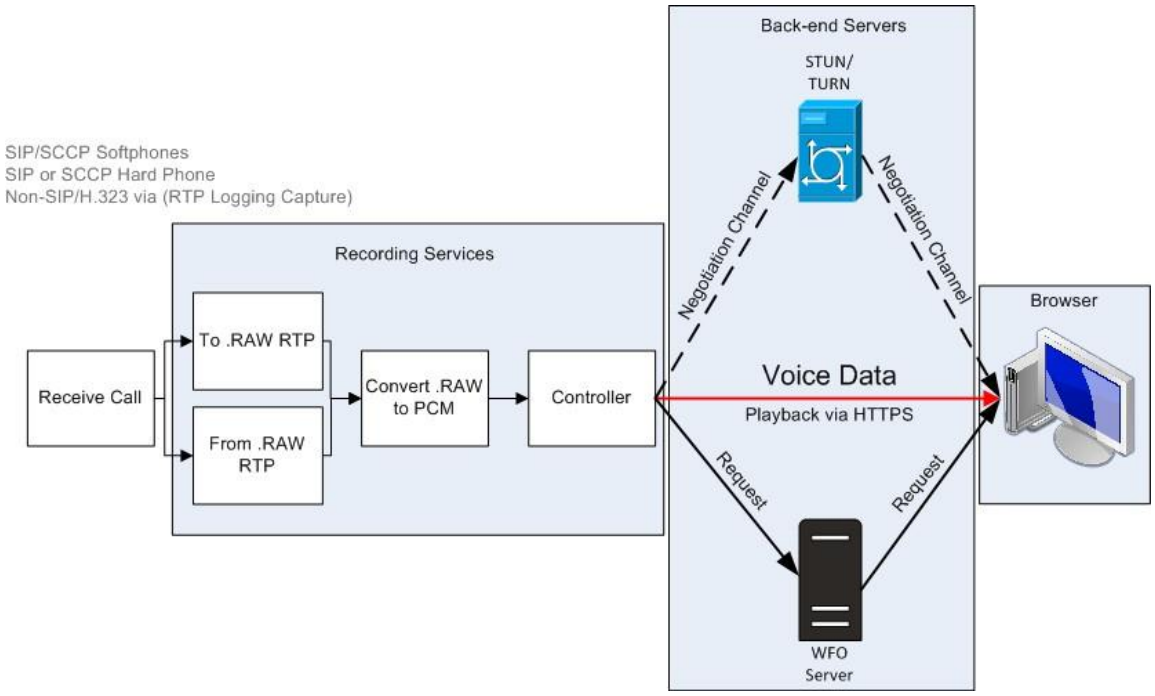
Smart Desktop SIP/SCCP Signalisierung



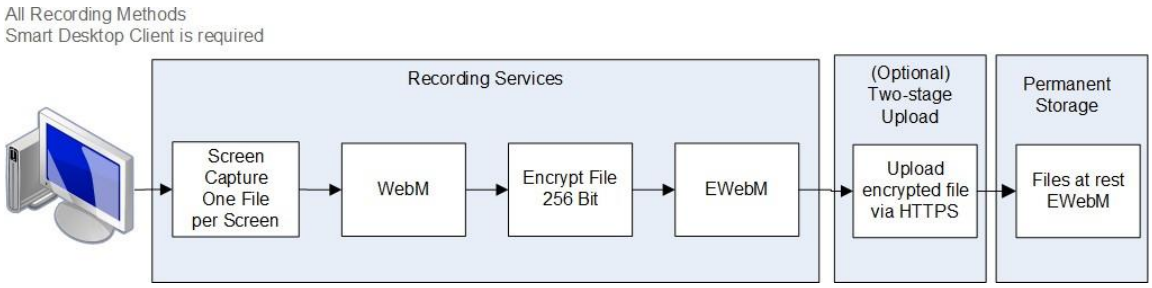
Protokollierung von Smart Desktop-RTP



Smart Desktop Live-Audioüberwachung

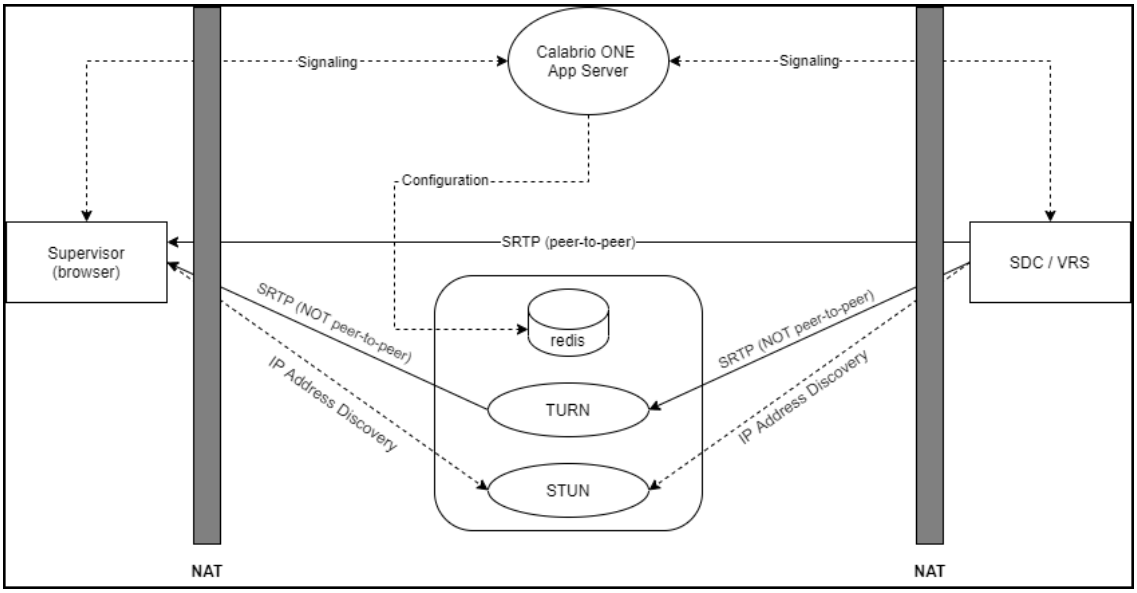


Smart Desktop Live-Bildschirmüberwachung



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

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

Voraussetzungen

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

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

Prozeduren

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

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

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

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

Stellen Sie sicher Webex WFO Ihren Computer erkennt

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

Stellen Sie sicher Webex WFO Agenten mithilfe von Smart Desktop erkennt

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

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

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

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

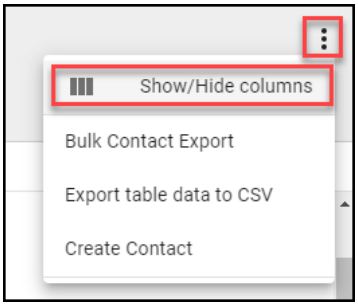
Führen Sie einen Testanruf durch

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

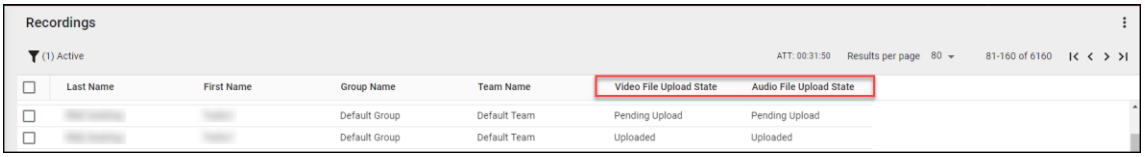
   Wenn das Bedienfeld "Bildschirmaufzeichnung" nicht angezeigt wird oder leer ist, überprüfen Sie, ob der Popup-Blocker im Browser deaktiviert ist.

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

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



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



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

Smart Desktop verwalten

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

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

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

Automatische Aktualisierung

Webex WFO verfügt über eine automatische Update-Funktion, die jederzeit aktiviert oder deaktiviert werden kann, indem Sie zu **Anwendungsverwaltung** > **Verwaltung** > **Globale Einstellungen navigieren**. Aktivieren oder deaktivieren Sie die Funktion für automatische Updates auf der Seite „globale Einstellungen“ mit der Schaltfläche **Automatische Clientaktualisierung aktivieren** .

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 mithilfe eines verwalteten Software-Pushs (z. B. GPO oder LANDesk) pushen.

BEST PRACTICE Die Richtlinien Ihres Unternehmens sollten von den Agenten verlangen, sich am Ende ihrer Schicht von ihrem PC abzumelden. Diese Aktion kann mithilfe von GPO-Einstellungen automatisiert werden.

Best Practices zum Hochladen von Aufnahmen auf Webex WFO

Durch das schnellstmögliche Abrufen von Audio- und Bildschirmaufzeichnungen vom Desktop eines Benutzers wird sichergestellt, dass die Aufzeichnungen nach der Aufzeichnung des Anrufs zur Wiedergabe verfügbar sind. Es gibt Optionen zum sofortigen oder zum Festlegen einer Zeit, mit denen die Aufzeichnungen vom Desktop des Benutzers entfernt werden können. Die Entscheidung darüber, wann Aufzeichnungen hochgeladen werden, erfolgt in Zusammenarbeit zwischen dem Geschäfts- und dem IT-Personal unter Berücksichtigung der Audio- und Bildschirmzugänglichkeitsanforderungen des Kontos, der Bandbreite und des Speicherplatzes. Cisco empfiehlt die unten aufgeführten Upload-Prozesse.

- Sofortiger Upload mithilfe von QM-Workflows – Dieser Prozess stellt sicher, dass die Aufzeichnung nach der Aufzeichnung des Anrufs zur Wiedergabe verfügbar ist und der Speicherplatz auf dem

Agenten-PC nicht übermäßig belegt wird. Cisco empfiehlt, Aufzeichnungen so zu konfigurieren, dass sie sofort vom PC des Agenten hochgeladen werden auf

Webex WFO, wenn WAN- und LAN-Bandbreite ausreichend sind. Verwenden Sie die Seite **Workflow-Verwaltung** in der **Anwendungsverwaltung** , um sofortige Uploads durchzuführen.

- Verzögerter Upload mithilfe von QM-Workflows – Sie können diesen Vorgang so konfigurieren, dass er nach den Geschäftszeiten stattfindet. Audio- und/oder Bildschirmaufnahmen werden zu einem festgelegten Zeitpunkt hochgeladen. Nachdem Ihre Aufnahmen hochgeladen wurden, können Sie sie bei Bedarf herunterladen. Verwenden Sie die Seite **Workflow-Verwaltung** in der **Anwendungsverwaltung** , um verzögerte Uploads durchzuführen.

- Sofortiger Upload mithilfe der regionalen Einstellungen für stufenweises Hochladen des WFO-Datenservers Webex – Wenn die Internetbandbreite ein Problem darstellt, kann ein stufenweises Hochladen den externen WAN-Verkehr während der Geschäftszeiten verringern. Für diese Option müssen Sie die Einstellungen für den stufenweisen Upload des Cisco-Datenservers konfigurieren (weitere Informationen finden Sie unter Datenserver konfigurieren und Stufenweisen Upload konfigurieren). Dieser Vorgang stellt sicher, dass Anrufe im Laufe des Tages von einem PC in den lokalen Speicher verschoben werden. Zu einem festgelegten Zeitpunkt nach Feierabend werden die Aufnahmen hochgeladen. Nachdem Ihre Aufnahmen hochgeladen wurden, können Sie sie bei Bedarf herunterladen. Konfigurieren Sie „Einstellungen für stufenweise Uploads des regionalen Datenservers“ auf der Seite „Datenserverkonfiguration“ in der Anwendungsverwaltung, um stufenweise Uploads durchzuführen.

Thin-Client-Server

NOTIZ unterstützt Citrix XenApp nur auf einem unterstützten Windows-Server installiert.

Beachten Sie bei der Verwendung eines Thin-Client-Servers:

- Thin Clients, die den Smart Desktop verwenden, erfordern eine Remote-Desktop-Sitzung, um alle Benutzerdaten (Audio-, Bildschirm- und Desktop-Aufzeichnung) zu erfassen. Wenn keine Remote-Desktop-Sitzung vorhanden ist, installieren Sie Smart Desktop auf den Agent-Desktops, um alle Benutzerdaten auf dem Desktop zu erfassen, während der Benutzer angemeldet ist.
- Konfigurieren Sie Workflows zur Verwendung des sofortigen Uploads sowohl für Bildschirm als auch Sprache, um sicherzustellen, dass auf alle Aufzeichnungen zugegriffen werden kann.
- Wenn Sie Smart Desktop für Aufzeichnungszwecke verwenden, benötigt der Thin Client-Server zusätzliche Serverressourcen für Bildschirmaufzeichnungen. Der Ressourcenbedarf variiert je nach tatsächlichem Design und erfordert möglicherweise einige detaillierte Hardwaredesigns, die vor der Bereitstellung von Cisco überprüft werden sollten.
- Wenn Sie ein virtuelles Image verwenden und es 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, die zur Unterstützung der Audio- und Bildschirmaufzeichnungs- und Aufzeichnungswiedergabefunktionen in Webex WFO erforderlich sind:

Bereich	Rücksichtnahme
Browser	▪ Integrieren Sie einen unterstützten Browser in Thin-Client-Serverbereitstellungen. 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 es Endbenutzern ermöglichen, Aufzeichnungen über den Thin Client wiederzugeben.
Sitzungen	Begrenzen Sie die Anzahl gleichzeitiger Sitzungen pro Benutzer auf eine einzige Sitzung.

Bereich	Rücksichtnahme
Smart Desktop Client	▪ Für Citrix-Clientdienste müssen Sie auch den Smart Desktop installieren Client auf dem Thin-Client-Server, um die Desktop-Aktivität des Benutzers (Desktop Analytics) und Telefonanrufe mithilfe eines unterstützten Softphones aufzuzeichnen. ▪ Der Smart Desktop Client stellt mithilfe der eindeutigen Domänen-/Windows-Anmeldung des Benutzers eine Verbindung zur Webex WFO-Plattform her.

Installation

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

Smart Desktop installieren

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

- Manuell auf dem Computer jedes Agenten
- Verwenden von GPO-Skripts (Group Policy Object)
- Verwenden von Parametern für stille Befehle

NOTIZ Wenn Sie möchten, dass Smart Desktop Desktopanalysen erfasst, muss für die Agentenrolle vor der Installation von Smart Desktop die Berechtigung „Desktopanalysen erfassen“ aktiviert sein. 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.

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.

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
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

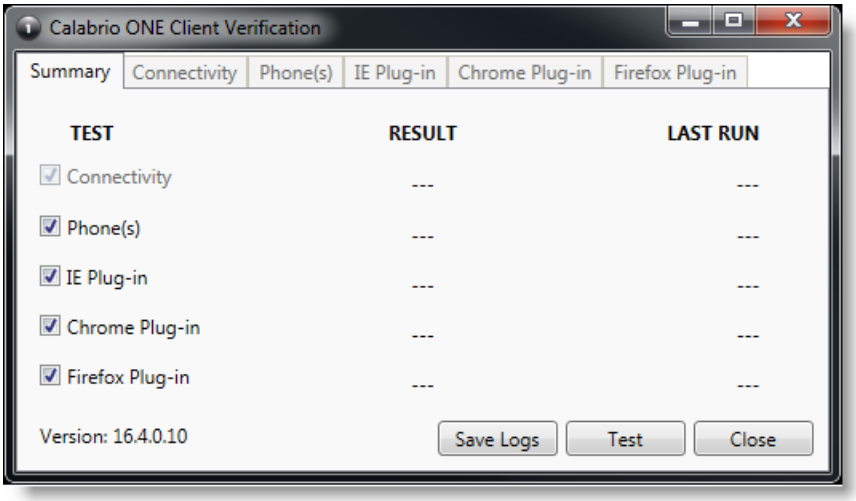
Das Clientüberprüfungstool testet den Client-PC, um sicherzustellen, dass die Konnektivität mit den Servern und dem Telefon für die Ausführung von Smart Desktop geeignet ist. Es wird installiert, wenn Smart Desktop installiert ist. Das Tool führt verschiedene Tests durch und meldet die Ergebnisse entweder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

Ausführen des Clientüberprüfungstools

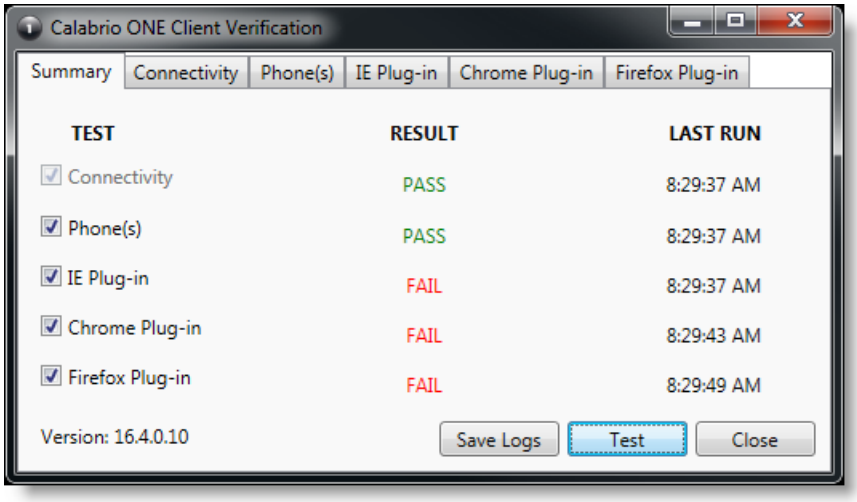
1. Navigieren Sie nach der Installation von Smart Desktop zum folgenden Ordner auf dem Client-PC:

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

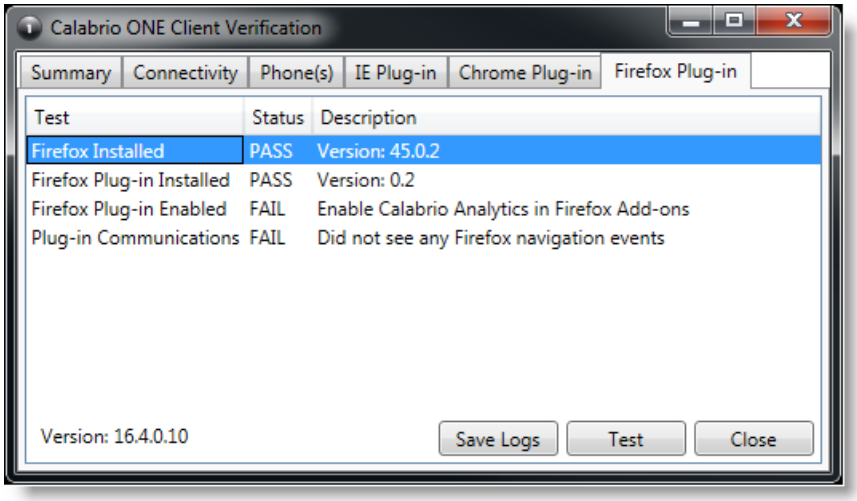
2. Doppelklicken Sie auf **ClientDiag.exe**. Das Clientüberprüfungstool wird gestartet.



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.

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.

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.

Datenübertragungs-Flussdiagramme

Dieses Thema enthält Diagramme zur Veranschaulichung folgender Informationen:

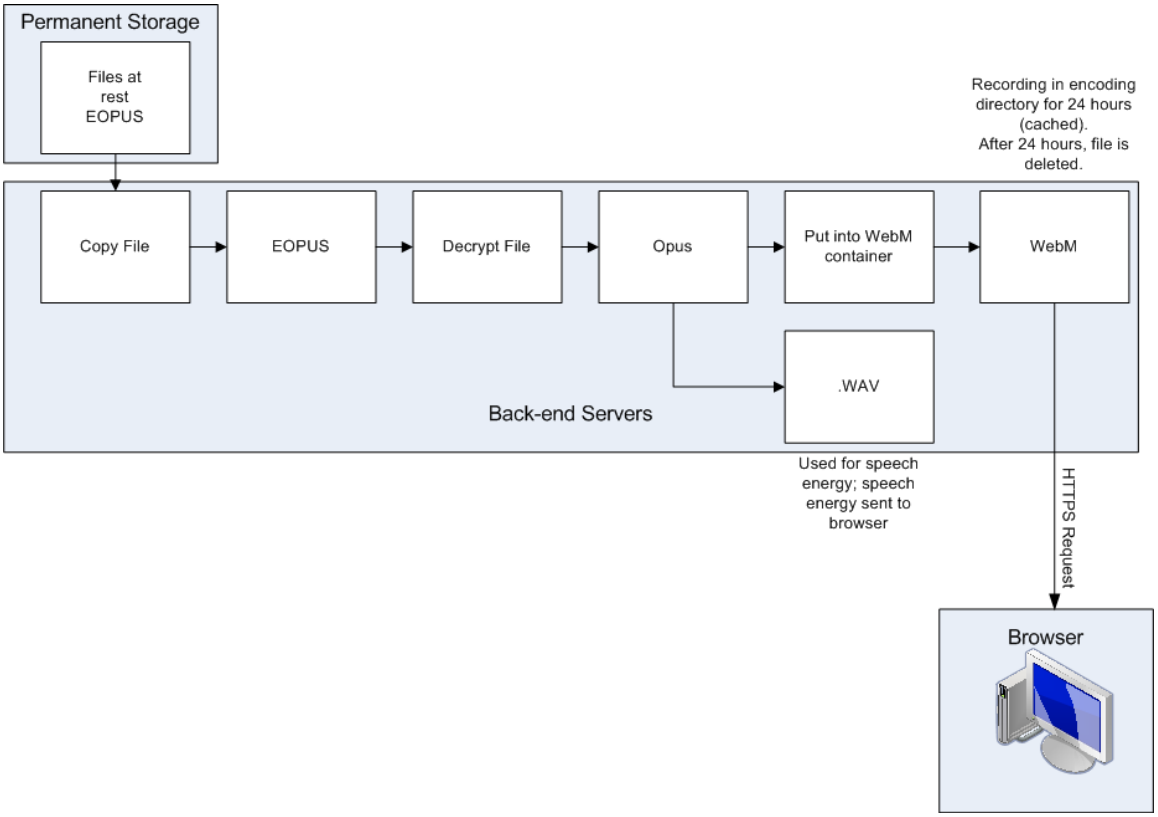
- Webex WFO-Aufzeichnung – Aufnahme und Wiedergabe
- Webex WFO Analytics-Datenfluss
- Webex WFO-Speicherdatenfluss
- Webex WFO-Aufzeichnungsverschlüsselung
- Cisco Hosted Collaboration Solution (HCS)

Aufzeichnung, Erfassung und Wiedergabe von Datenflussdiagrammen

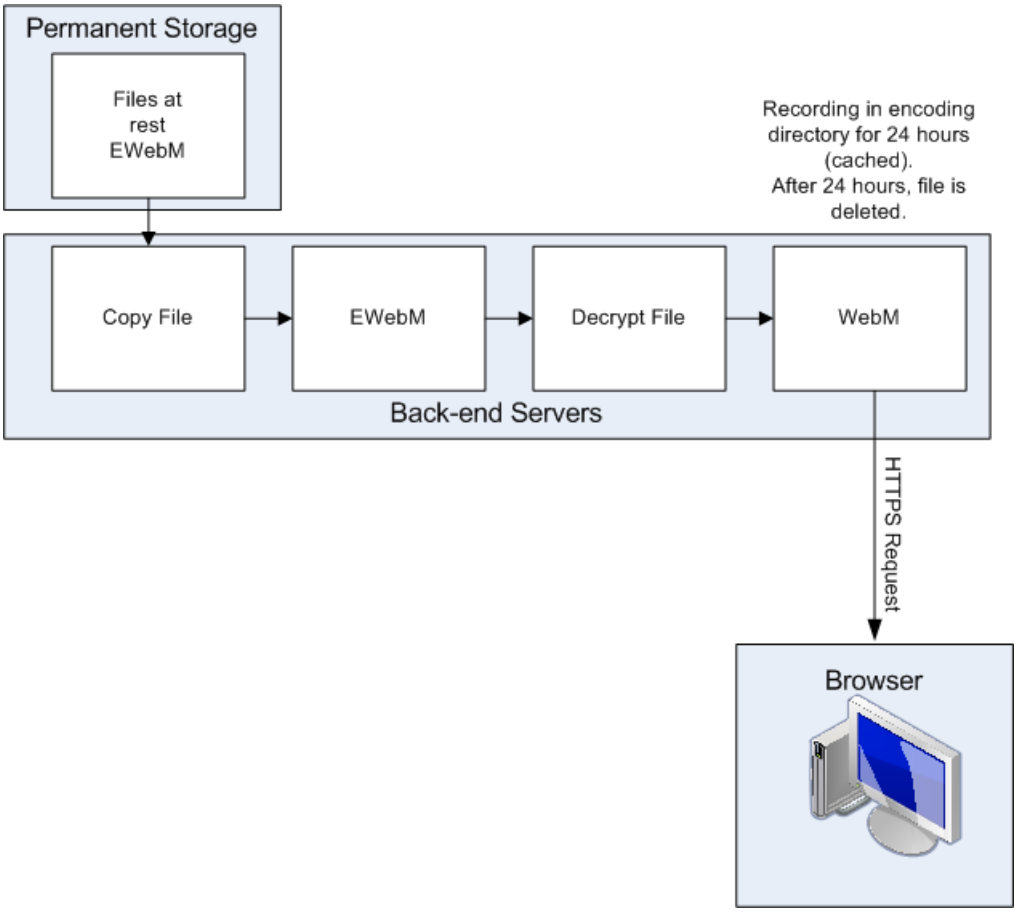
In diesem Thema wird das Wiedergeben von Kontaktaufzeichnungen beschrieben.

Datenflussdiagramm für die Audiowiedergabe

Während der Wiedergabe werden Audio- und Bildschirmaufzeichnungsdateien aus dem permanenten Speicher kopiert und in einem sicheren Cloud-Netzwerkspeicher abgelegt, entschlüsselt und für die Wiedergabe verarbeitet. Die Dateien werden gleichzeitig entschlüsselt und durch Netzwerkspeicher und HTTPS gesichert.


Permanent Storage
Files at rest EOPUS
Recording in encoding directory for 24 hours (cached). After 24 hours, file is deleted.
Copy File
EOPUS
Decrypt File
Opus
Put into WebM container
WebM
.WAV
Back-end Servers
Used for speech energy; speech energy sent to browser
HTTPS Request
Browser

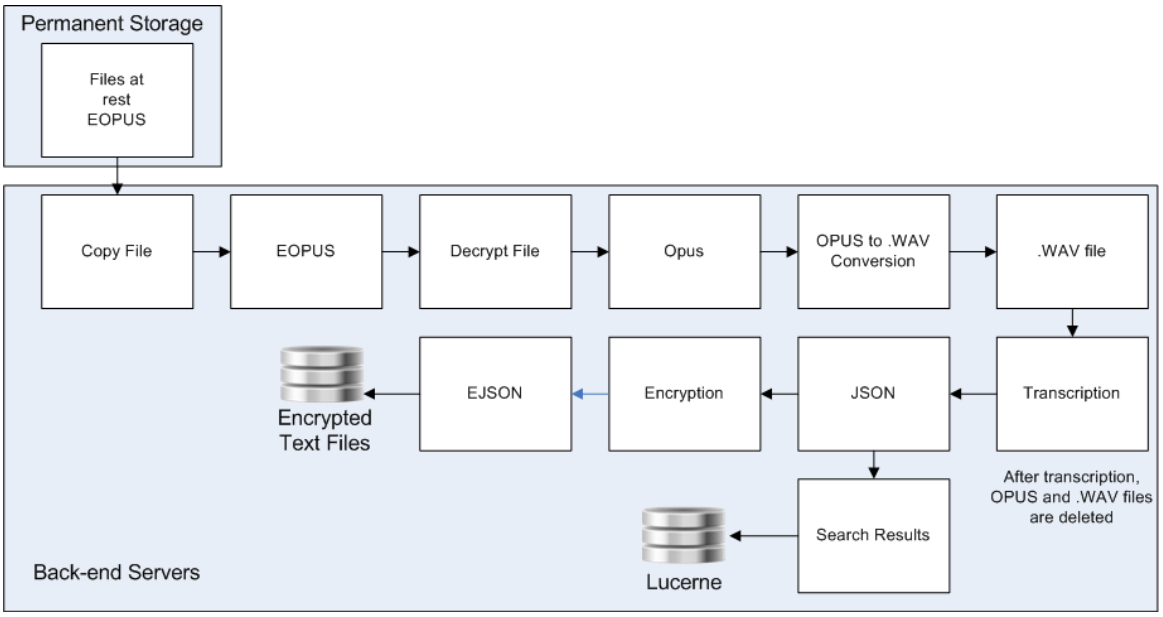
Datenflussdiagramm für die Bildschirmwiedergabe



Analytics-Datenflussdiagramm

In diesem Thema wird der Datenfluss für die Verarbeitung von Analytics-Daten beschrieben.

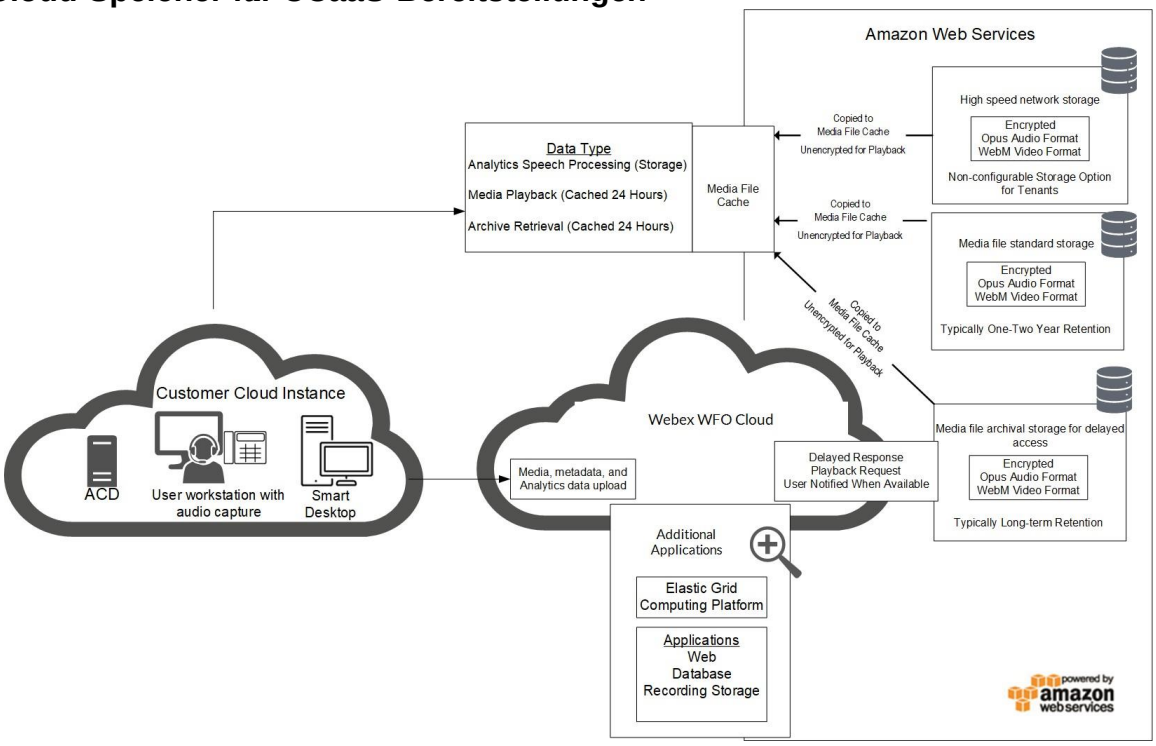
Datenflussdiagramm der Sprachtranskriptionsanalyse



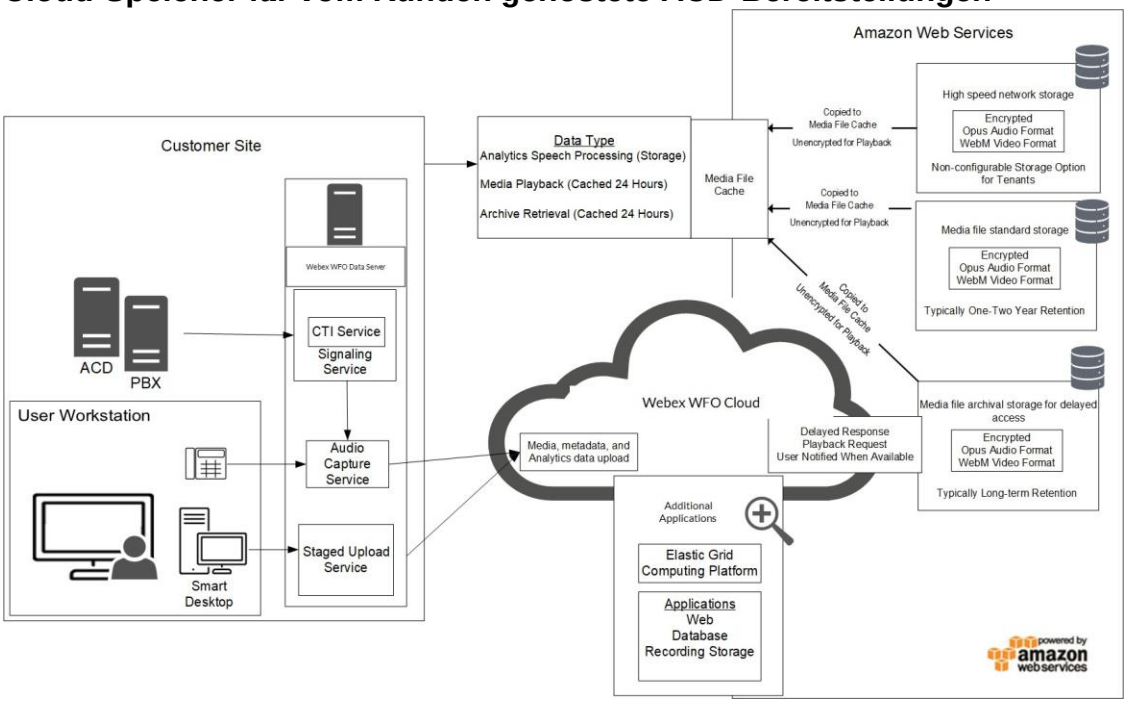
Datenflussdiagramme für Cloud-Speicher

In diesem Thema wird der Datenfluss für die Kontaktdatenspeicherung in Webex WFO für CCaaS- und vom Kunden gehostete Bereitstellungen beschrieben.

Cloud-Speicher für CCaaS-Bereitstellungen

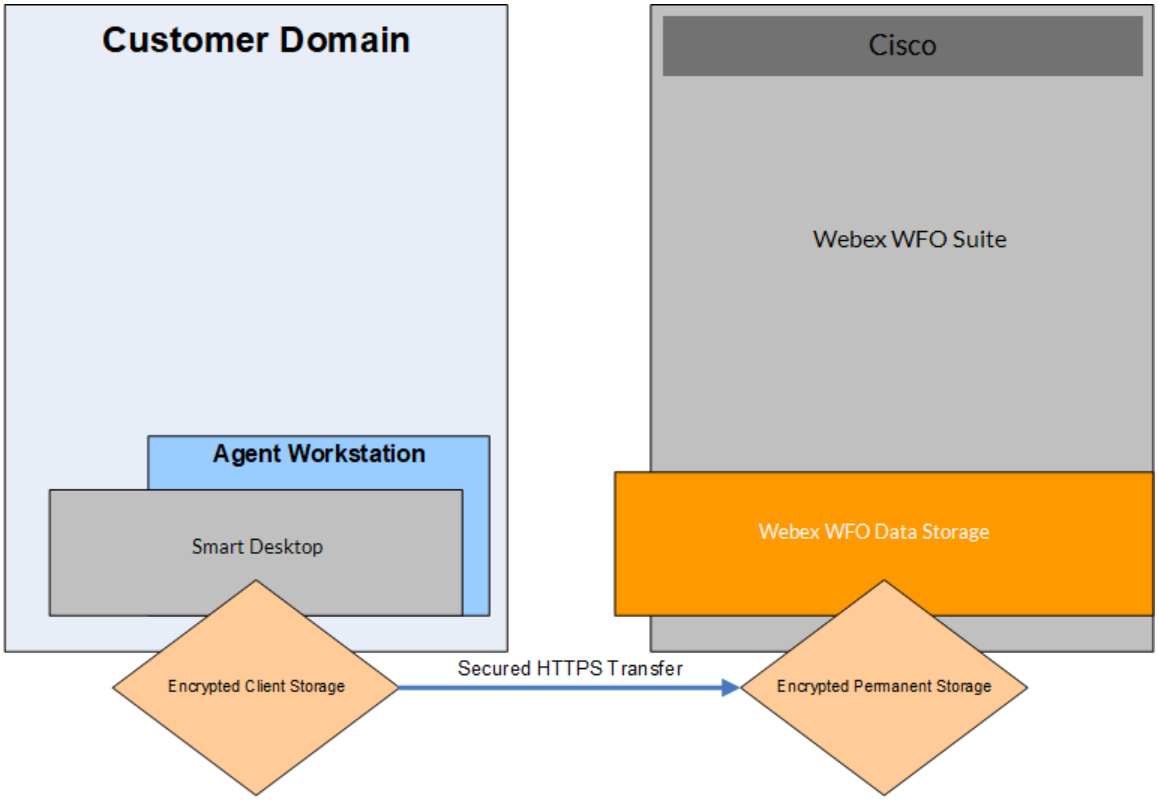


Cloud-Speicher für vom Kunden gehostete ACD-Bereitstellungen



Aufzeichnungsverschlüsselung

Das folgende Diagramm beschreibt die Verschlüsselung von Aufzeichnungen in Webex WFO.



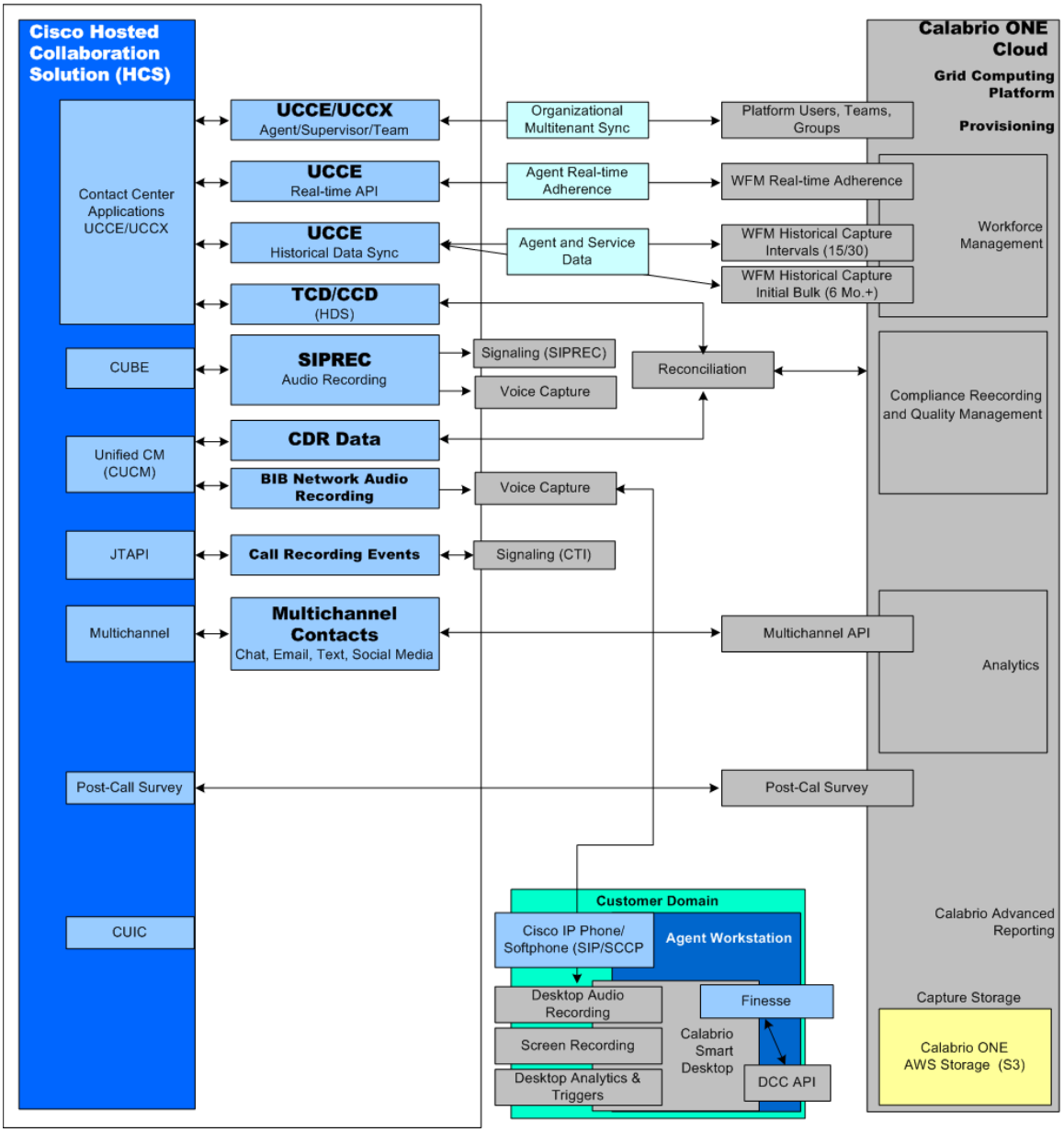
Alle Daten werden verschlüsselt und über gesichertes HTTPS/SSL vom Kundenstandort zur Verarbeitung und Speicherung Webex WFO transportiert.

In Cloud-Bereitstellungen ist die verfügbare Verschlüsselungsmethode RSA-2048 (mit asymmetrischen Schlüsseln) und AES-256 für Medien, die von Webex WFO aufgezeichnet wurden.

In Cloud-Bereitstellungen von Webex WFO steuert nur der Mandant (nicht Webex WFO Cloud Operations) die Schlüssel, die zum Verschlüsseln von Aufzeichnungen verwendet werden, und diese Schlüssel werden in der Datenbank des Mandanten gespeichert. Darüber hinaus ist eine zweite Verschlüsselungsebene in Webex WFO eingebettet, auf die Webex WFO Cloud Operations ebenfalls keinen Zugriff hat.

Cisco Hosted Collaboration Solution (HCS)

Die Webex WFO-Plattform lässt sich in ein Cisco Hosted Collaboration Solution (HCS) für Unified CCE auf die gleiche Weise wie eine einzelne Cisco Unified CCE-Lösung integrieren. Webex WFO kann eine Verbindung mit einzelnen Instanzen von Cisco HCS Unified CCE herstellen, um eine mehrinstanzenfähige Lösung zu erstellen. Jede Verbindung ist spezifisch für den beabsichtigten Kunden und segmentiert von anderen Mandanten. Der Webex WFO-Datenserver kann eine Verbindung zu mehreren Instanzen von Cisco Unified CCE herstellen, um Agenten-, Supervisor- und Teaminformationen unabhängig vom Kunden zu synchronisieren.



Plattform-Erfassungsmethoden

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

Unterstützte Erfassungsmethoden nach Plattform

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

ANMERKUNG

Webex WFO unterstützt SRTP nur mit den folgenden Erfassungsmethoden:

- Acme-Paket
- Cisco Unified CM

Plattform	Erfassungsmethode	Signalisierung	Beschreibung der Signalisierung
Cisco	Integrierte Bridge-Netzwerkaufzeichnung	JTAPI	Registrierung bei Call Manager für JTAPI Ereignisse
Cisco	Desktop-Aufzeichnung	JTAPI	Registrierung bei Call Manager für JTAPI Ereignisse
Cisco	Gateway (Cisco Unified Border Element—CUBE)	SIPREC	Registrierung bei CUBE für SIPREC-Signalisierung
Cisco	Smartdesktop-Client	IP Communicator (SIP/SCCP)	SCCP Nachrichten außerhalb des Desktops
Cisco	Smartdesktop-Client	Jabber (SIP/SCCP)	Schnüffelt SIP/SCCP-Nachrichten außerhalb des Desktops
Cisco	Smartdesktop-Client	Cisco IP HardPhone (SIP/SCCP)	Schnüffelt SIP/SCCP-Nachrichten außerhalb des Desktops
Cisco Webex Contact Center (CWCC)	Automatisierter Import	CWCC Analyzer API	CWCC-Analysator für Anruf-CDR und Anruf-Nachbereitung abfragen
ACME	Gateway	SIPREC	Registriert sich bei ACME für SIPREC

Plattform	Erfassungsmethode	Signalisierung	Beschreibung der Signalisierung
	(ACME Pakete)		signalisierung
SONUS	Gateway (SONUS)	SIPREC	Registriert sich bei SONUS für die SIPREC-Signalisierung

Cisco-Spracherfassungsmethoden

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

Erfassungsmethode	Signalisierung	Beschreibung	Medien Bach	Intelligenter Desktop Screenshot	Live-Audio Überwachung
Netzwerk Aufzeichnung— Integrierte Brücke (BIB)	JTAPI	Registriert bei CUCM/JTAPI Ereignisse	BIB – Medien Gestreamt von Telefonnummer	Ja (Smart) Desktop-Client Erfordert CTI Anschluss)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Auftraggeber – IP Mitteilende	SIP/SCCP	SIP/SCCP überwachen Nachrichten aus Desktop/Softphone	Medienstrom eingefangen direkt auf Desktop	Ja (Smart) Desktop-Client)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Auftraggeber – Jabber	SIP/SCCP	Überwachung von SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Desktop	Ja (Smart) Desktop-Client)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Auftraggeber – Cisco IP Telefon (Gänseblümchen Verkettet)	SIP/SCCP	Überwachung von SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Desktop	Ja (Smart) Desktop-Client)	Ja (Smart) Desktop Client) über WebRTC
Gateway (CUBE)	SIPREC	Registriert bei CUBE für SIPREC Signalisierung	SIPREC – Medien-Forking von Cisco WÜRFEL	Ja (Smart) Desktop-Client)	Nein

Erfassungsmethode	Signalisierung	Beschreibung	Medien Bach	Intelligenter Desktop Screenshot	Live-Audio Überwachung
Massenkontakt Importieren	API-basiert	Registriert bei CUBE für SIPREC Signalisierung	Automatisiert Import von unverschlüsselt. WAV und assoziiert Kontakt Metadaten-Dateien en gros	N/A – Dateien Verschlüsselt und Eingeführt	Nein

Legacy-Spracherfassungsintegrationen von Five9

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

Erfassungstyp	Signalisierung	Beschreibung	Medienstrom	Intelligenter Desktop - Bildschirm Gefangennahme	Live-Audio Überwachung
Intelligenter Desktop Client	Kafka-CTI	Webex WFO Plattform-Register mit Five9 Kafka Veranstaltungen API	Medienstrom eingefangen direkt auf Desktop – Post Anruf-CDR und Versöhnung Verarbeitung Schwärzungen und Fügt Ereignisse ein nach Kafka Anrufereignisse	Ja (Smart) Desktop Auftraggeber)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter	Five9-Agent	SIP/SCCP	Medienstrom	Ja (Smart)	Ja (Smart)

Desktop		überwachen			
Client	Desktop Plus (ADP) -	Nachrichten aus Desktop/Softphone	eingefangen	Desktop Auftraggeber)	Desktop Client) über

Erfassungstyp	Signalisierung	Beschreibung	Medienstrom	Intelligenter Desktop - Bildschirm Gefangennahme	Live-Audio Überwachung
	Kafka-CTI		direkt auf Desktop – Post Anruf-CDR und Versöhnung Verarbeitung Schwärzungen und Fügt Ereignisse ein nach Kafka Anrufereignisse		WebRTC
Intelligenter Desktop Client	Five9-Agent Desktop Werkzeugsatz (ADT) - Kafka-CTI	Überwachung von SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Desktop – Post Anruf-CDR und Versöhnung Verarbeitung Schwärzungen und Fügt Ereignisse ein nach Kafka Anrufereignisse	Ja (Smart) Desktop Auftraggeber)	Ja (Smart) Desktop Client) über WebRTC
Intelligenter Desktop Client	Fünf9 Java Agent Desktop- Kafka-CTI	Überwachung von SIP/SCCP Nachrichten aus Desktop	Medienstrom eingefangen direkt auf Desktop – Post Anruf-CDR und Versöhnung Verarbeitung Schwärzungen	Ja (Smart) Desktop Auftraggeber)	Ja (Smart) Desktop Client) über WebRTC

	und
	Fügt Ereignisse ein nach Kafka

Erfassungstyp		Beschreibu		Intelligenter Desktop-	Live-Audio Überwach
			Anrufereignisse		
Smartdesktop-Client	Five9 VCC-Import	Five9/Webex WFO-Cloud-Integration zum Importieren von Five9 VCC-Audioaufnahmen in Webex WFO-Cloud	N/A – Nur Import	Ja (Smart) in Desktop Auftraggeber)	Ke

Sonus Gateway-Aufzeichnung

Cisco unterstützt 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 können QM Anrufe mit den Cisco Unified CM CDR-Datensätzen abgleichen. Die Regeln bewirken Folgendes:

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

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

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

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

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

1. Erstellen und aktivieren Sie die SMM-Regeln über die Sonus-Befehlszeilenschnittstelle (CLI)

    a. Erstellen und aktivieren Sie die Unified CM SMM-Regeln für eingehenden Anruf. Weitere Informationen finden Sie im Beispiel für SMM-Regeln für eingehenden Unified CM .

    b. Fügen Sie die Unified CM ausgehenden SMM-Regeln hinzu. Weitere Informationen finden Sie im Beispiel für ausgehende SMM-Regeln Unified CM .

    c. Fügen Sie die SMM-Regeln für ausgehende Recorder-Anrufe hinzu. Weitere Informationen finden Sie im Beispiel für ausgehende SMM-Regeln für den Recorder .

2. Verwenden Sie die Sonus CLI, um SIPREC für den SIp Sig-Port in der Zone zu aktivieren, in der sich Ihr Unified CM Trunk befindet.

3. Verwenden Sie die Sonus CLI oder den Navigator, um eine SIP-Trunk-Gruppe für den Sonus SIPREC-Server von QM zu erstellen. Weisen Sie das Präfix "Ingress IP Präfix der IP des QM Rechners zu, auf dem 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 Eingabeprofil des Adapters zur Bearbeitung von Signalnachrichten Ihres Unified CM Trunks zu.

    b. Weisen Sie UCM_OUTBOUND SMM dem Ausgangsprofil des Signalisierungsadapters für die Bearbeitung von Nachrichten Ihres Unified CM Trunks zu.

    c. Weisen Sie RECORDER_OUTBOUND SMM dem Ausgangsprofil des Signaling Message Manipulation-Adapters für den Sonus SIPREC-Trunk von QM zu.

5. Verwenden Sie den Sonus PSX, um eine IP Signaling Peer Group für den Sonus SIPREC Server des QM zu erstellen. Weisen Sie das Präfix "Ingress IP Präfix der IP des QM Rechners zu, auf dem 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 festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 1 Typ Nachricht

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

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 1 NachrichtenmethodeTypen invite

profile signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 1

Nachrichtenbedingung vorhanden

profile signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 2 Typ Header

profile festlegen , die sipAdaptorProfile signalisieren UCM_INBOUND Regel 2 Kriterium 2 Headername Von

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

profile festlegen signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 3 Typ Variable

set profiles signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 3 Variable Bedingung vorhanden

profile signalisieren sipAdaptorProfile UCM_INBOUND Regel 2 Kriterium 3 variable variableID var1

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

Profile festlegen, die sipAdapterProfile signalisieren UCM_OUTBOUND Regel 1 Kriterium 1

message messageTypes-Anforderung

set-profile, die sipAdaptorProfile- UCM_OUTBOUND Regel 1 Kriterium 1 Nachrichtenmethode-Typen invite signalisieren

Festlegen von Profilen, die sipAdaptorProfile- UCM_OUTBOUND Regel 1 Kriterium 2 Typ Header signalisieren

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

set-Profile-Signalisierung sipAdapterorProfile- 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 festlegen 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

Festlegen von Profilen 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
set-Profile, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 Aktion 3 vom 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
set profiles signalisieren sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 aus 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
Festlegen von Profilen, die sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 6 regulärer Ausdruck

Schnur^
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
Festlegen von Profilen, die sipAdaptorProfile UCM_OUTBOUND Regel 2 Aktion 9 auf

variableValue var3

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	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	12	
Setze Profile SignalisierungsvariableWert var2	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	12	Von
Signalisierungsvariable "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	12	Von
Speicher für den Signalisierungsvorgang	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	12	An

von Profilen festlegen

Festlegen von Profilen

Signalisierungstyp Variable

Setze Profile

SignalisierungsvariableWe

rt var2

Signalisierung von Profilen festlegen

Typ 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	Von
Festlegen von Profilen Signalisierungstyp Variable	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	13	An
Setze Profile SignalisierungsvariableWert var2	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	14	Art
Signalisierungsvariable "Profile" festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	14	
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	Von
set-profile-signalisierungsvariableWert var3	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	14	An
Festlegen von Profilen Signalisierungstyp Variable	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	14	An
Setze Profile SignalisierungsvariableWert var2	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	15	Art
Signalisierungsheader für Profile festlegen	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	15	
Festlegen von Profilen Signalisierungsvorgang Hinzufügen	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	15	
	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	15	Von
	sipAdapterProfil	UCM_OUTBOUND	Regel 2	Aktion	15	An

set profiles signalisierung
headerposition last set
profiles signalisierungstyp
variable
Setze Profile
SignalisierungsvariableWe
rt var2
Signalisierung von Profilen festlegen

Kopfzeile eingeben

Festlegen von Profilen, die sipAdaptorProfile signalisieren, UCM_OUTBOUND Regel 2 , Aktion 15 , auf Wert Cisco-Guid

begehen

set profiles, die sipAdaptorProfile UCM_OUTBOUND Status aktiviert Commit signalisieren

Beispiel für ausgehende SMM-Regeln für den Rekorder

konfigurieren

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

Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1 von 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 signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 1 Aktion 1

regexp-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
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Kriterium 1 Typ Nachricht
profile festlegen , die sipAdaptorProfile signalisieren RECORDER_OUTBOUND Regel 2 Kriterium 1 message messageTypes request
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Kriterium 1 NachrichtenmethodeTypen invite
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Kriterium 2

Kopfzeile eingeben
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Kriterium 2 Headername cisco-guid
profile festlegen signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 2 Kriterium 2 Header-Bedingung fehlt
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 festlegen 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
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 3 Aktion 1

Von-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
Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 2 auf den 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>
profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 2

regexp 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 setzen

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

Festlegen von Profilen, die sipAdaptorProfile signalisieren, 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
Festlegen von Profilen, die sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 8 vom 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 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

Festlegen von Profilen, die 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 -

profile signalisieren sipAdaptorProfile RECORDER_OUTBOUND Regel 4 Aktion 11

Variable eingeben

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 RECORDER_OUTBOUND Regel 4 Aktion 14 vom Typ value signalisieren

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

Festlegen von Profilen, die sipAdaptorProfile signalisieren, RECORDER_OUTBOUND Regel 4 Aktion 14

zu variableValue var2
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