Webex Guide d'installation de WFO Cloud

Pour les déploiements avec WFM classique

Première publication : 10 juillet 2020
Dernière mise à jour : 28 février 2025

Siège social aux États-Unis
Cisco Systems Inc.
170 West Tasman Drive
San José, Californie, 95134-1706 USA
http://www.cisco.com
Tel : 408 526-4000
800 553-NETS(6387)
Télécopie : 408 527-0882

LES SPÉCIFICATIONS ET INFORMATIONS SUR LES PRODUITS PRÉSENTÉS DANS CE MANUEL PEUVENT ÊTRE MODIFIÉES SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS FOURNIES DANS CE MANUEL SONT EXACTES À NOTRE CONNAISSANCE, MAIS SONT PRÉSENTÉES SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. LES UTILISATEURS ASSUMENT L'ENTIÈRE RESPONSABILITÉ DE L'APPLICATION DE TOUT PRODUIT. LA LICENCE DE LOGICIEL ET LA GARANTIE LIMITÉE DU PRODUIT CI-JOINT SONT DÉFINIES DANS LES INFORMATIONS FOURNIES AVEC LE PRODUIT ET SONT INTÉGRÉES AUX PRÉSENTES SOUS CETTE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE LOGICIELLE OU LA LIMITATION DE GARANTIE, DEMANDEZ-EN UN EXEMPLAIRE À VOTRE REPRÉSENTANT CISCO.

La mise en œuvre Cisco de la compression d'en-tête TCP est l'adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB), dans le cadre de la mise au point, par l'UCB, d'une version gratuite du système d'exploitation UNIX. Tous droits réservés. Copyright © 1981, Regents of the University of California.

NONOBSTANT TOUTE AUTRE GARANTIE CONTENUE DANS LES PRÉSENTES, TOUS LES DOSSIERS DE DOCUMENTATION ET LES LOGICIELS PROVENANT DE CES FOURNISSEURS SONT FOURNIS « EN L'ÉTAT », TOUS DÉFAUTS INCLUS. CISCO ET LES FOURNISSEURS SUSMENTIONNÉS DÉCLINENT TOUTE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT CELLES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON, AINSI QUE TOUTE GARANTIE EXPLICITE OU IMPLICITE LIÉE À DES NÉGOCIATIONS, À UN USAGE OU À UNE PRATIQUE COMMERCIALE.

EN AUCUN CAS CISCO OU SES FOURNISSEURS NE SAURAIENT ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES INDIRECTS, SPÉCIAUX, CONSÉQUENTS OU ACCIDENTELS, Y COMPRIS ET SANS LIMITATION, LA PERTE DE PROFITS OU LA PERTE OU LES DOMMAGES DE DONNÉES CONSÉCUTIVES À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Les adresses IP (Internet Protocol) et les numéros de téléphone utilisés dans ce document ne sont pas censés correspondre à des adresses ni à des numéros de téléphone réels. Tous les exemples, résultats d'affichage de commandes, schémas de topologie du réseau et autres illustrations inclus dans ce document sont donnés à titre indicatif uniquement. L'utilisation d'adresses IP ou de numéros de téléphone réels à titre d'exemple est non intentionnelle et fortuite.

Les exemplaires imprimés et les copies numériques de ce document peuvent être obsolètes. La version originale en ligne constitue la version la plus récente.

Cisco compte plus de 200 agences à travers le monde. Les adresses et les numéros de téléphone sont indiqués sur le site Web de Cisco à l'adresse www.cisco.com/go/offices.

Cisco et le logo Cisco sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour voir la liste des marques commerciales Cisco, visitez le site www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. L'utilisation du mot « partenaire » n'implique nullement une relation de partenariat entre Cisco et toute autre entreprise. (1721R)

© 2000-2025 Cisco Systems, Inc. Tous droits réservés.

Table des matières

Contenu 3

Introduction 7

Localisation et langues prises en charge 9

Configuration du système 13

Environnements pris en charge 15

Téléphones pris en charge 15

Téléphones durs 15

Codecs pris en charge 15

Utilisation de plusieurs softphones 15

Appareils mobiles pris en charge 16

Composants Edge 17

Webex Bureau intelligent WFO 18

À propos de Webex WFO Smart Desktop 18

Connectivité Smart Desktop Client 19

Configuration requise et considérations relatives au bureau intelligent 20

Utilisation du port du bureau intelligent 22

Métadonnées de contact Smart Desktop 24

Diagrammes de flux de données Smart Desktop Capture 25

Test du bureau intelligent 28

Gestion de Smart Desktop 31

Application de commandes d'enregistrement 32

Webex serveur de données WFO 34

Configuration système requise **37**

Matériel de bureau 37

Logiciel de bureau 38

.NET Framework 38

Navigateurs 38

Plug-in/extension Desktop Analytics 38

Adobe Acrobat Reader 39

Logiciel de bureau et capture audio 39

Activer l'extension Desktop Analytics dans votre navigateur 39

Serveurs clients légers 40

Installation du serveur client léger 41

Utilisation des ports 42

Composants Edge 43

Composants du serveur de données 43

Chiffrement des fichiers 48

Politique de mot de passe 48

Authentification 51

Méthodes de capture de plate-forme 51

Méthodes de capture prises en charge par plate-forme 51

Enregistrement Sonus Gateway 55

Installation **75**

Installation du serveur de données 75

Prérequis 75

Installer le serveur de données pour un service partagé unique 76

Installer le serveur de données pour plusieurs services partagés 76

Utilisateurs de Cisco Unified Communications Manager 77

Installation de Smart Desktop 78

Installation manuelle 80

Installation à l'aide d'un objet de stratégie de groupe 80

Installer Smart Desktop en utilisant les paramètres de commande silencieuse 81

Réplication d'une installation à l'aide de l'imagerie de bureau 81

Envoyer les codes de retour de l'installation 82

Outil de vérification des clients 83

Commandes d'enregistrement 84

Enlèvement 87

Désinstallation Webex WFO Smart Desktop 87

Désinstallation à l'aide de l'objet de stratégie de groupe 87

Désinstaller Smart Desktop à l'aide des paramètres de commande silencieuse 88

Introduction

Webex WFO est une plateforme hautement évolutive d'optimisation de la main-d’œuvre multi-locataires. Il inclut la possibilité d'effectuer l'enregistrement des appels, la gestion de la qualité, la gestion de la main-d’œuvre et l'analyse.

Ce document explique comment installer Webex WFO dans un environnement cloud.

Localisation et langues prises en charge

Les différentes composantes de Webex WFO prennent en charge différentes langues. La prise en charge linguistique s'applique aux éléments suivants :

- Interface utilisateur
  - QM, WFM, Analytics et Insights
  - Formation intégrée au produit
- Documentation
  - Aide en ligne
  - PDF guides
- Analyses
  - Transcription : Recherche de conversion de la parole en texte et de transcription.
  - Résumé de l'interaction : résumé d'un contact audio basé sur la transcription du contact.
  - Phrases réussies : identification de phrases prédéfinies. Webex WFO identifie les résultats de phrases en fonction des transcriptions parole-texte des contacts.
  - Sentiment : analyse des sentiments basée sur du texte.
  - Prédictions : prédictions d'apprentissage automatique des scores d'évaluation et des scores nets des promoteurs.
  - Texte : analyses pour le chat, les e-mails, les notes d'agent et les médias sociaux.

Les composants de Webex WFO sont disponibles dans ces langues.

Langue	UI	Mobile Appli	Formation intégrée au produit	Analyses								Documentation
				Transcription*	Résumé de l'interaction	Phrases réussies	Sentiment	Prédictions	Analyse de texte	Sujets tendance	QM automatique	
Arabe (ar-AR)				x	x	x		x				
Chinois simplifié (zh)	x		Limité									
Chinois traditionnel (zh-TW)	x		Limité									
Danois (d bis)	x		Limité	x	x	x		x	x			
Néerlandais (nl)	Limité		Limité	x	x	x		x	x			
Français (fr)	x	x	x	x	x	x	x	x	x			x
Anglais australien (en-AU)				x	x	x	x	x	x			
Anglais sud-africain (fr-ZA)				x	x	x	x	x	x			
Anglais (UK) (en-GB)				x	x	x	x	x	x	x	x	
Anglais (en-US)	x	x	x	x	x	x	x	x	x	x	x	x

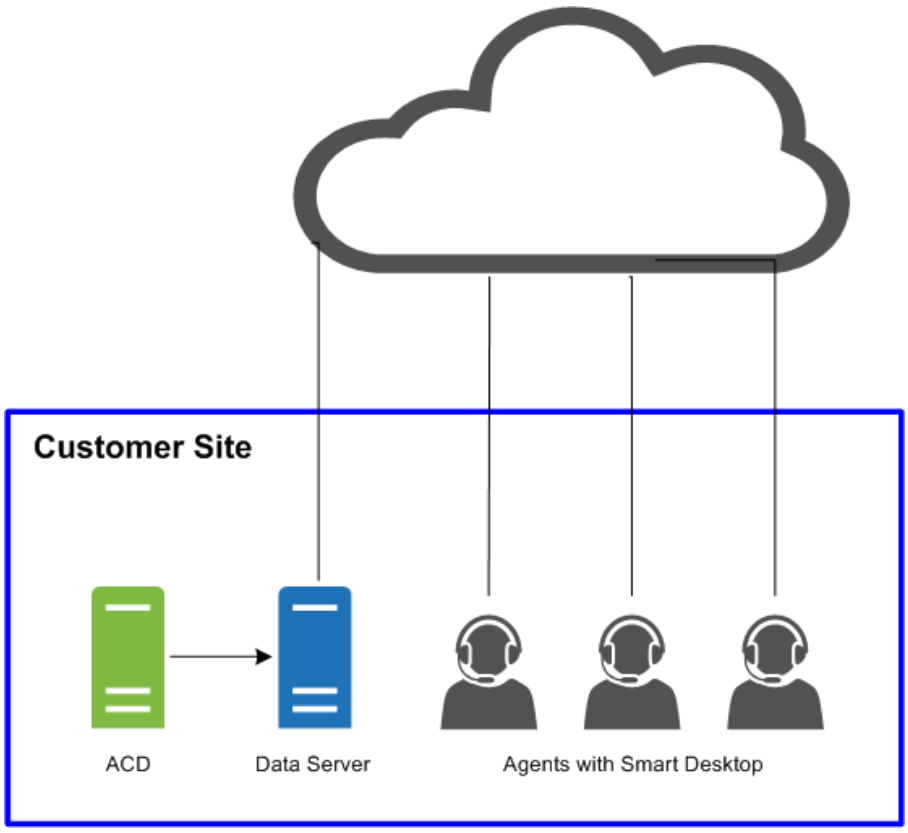
Langue	UI	Mobile Appli	Formation intégrée au produit	Analyses								Documentation
				Transcription*	Résumé de l'interaction	Phrases réussies	Sentiment	Prédictions	Analyse de texte	Sujets tendance	QM automatique	
Finnois (fi)	x		Limité	x	x	x		x				
Français (fr)	x		Limité	x	x	x		x	x			Limité
Français (fr-CA)	x			x	x	x		x	x			
Allemand (de)	x		Limité	x	x	x		x	x			Limité
Italien (it)	x		Limité	x	x	x		x	x			
Japonais (ja)	x		Limité									
Coréen (ko)	x		Limité									
Norvégien (nb)	x		Limité	x	x	x		x	x			
Polonais (pl)	Limité		Limité	x	x	x		x	x			
Portugais (pt)	x		Limité	x	x	x		x	x			
Portugais (Brésil) (pt-BR)	x		Limité	x	x	x		x	x			

Langue	UI	Mobile Appli	Dans le produit	Analyses								Documentation
				Transcription*	Interaction Résumé	Phrase Hits	Sentiment	Prédictions	Texte Analyses	Tendances	QM	
Russe (ru)	Limité											
Espagnol	x		Limité	x	x	x		x	x			Limité
Espagnol mexicain (es-MX)				x	x	x		x	x			
	x		Limité	x	x	x		x	x			

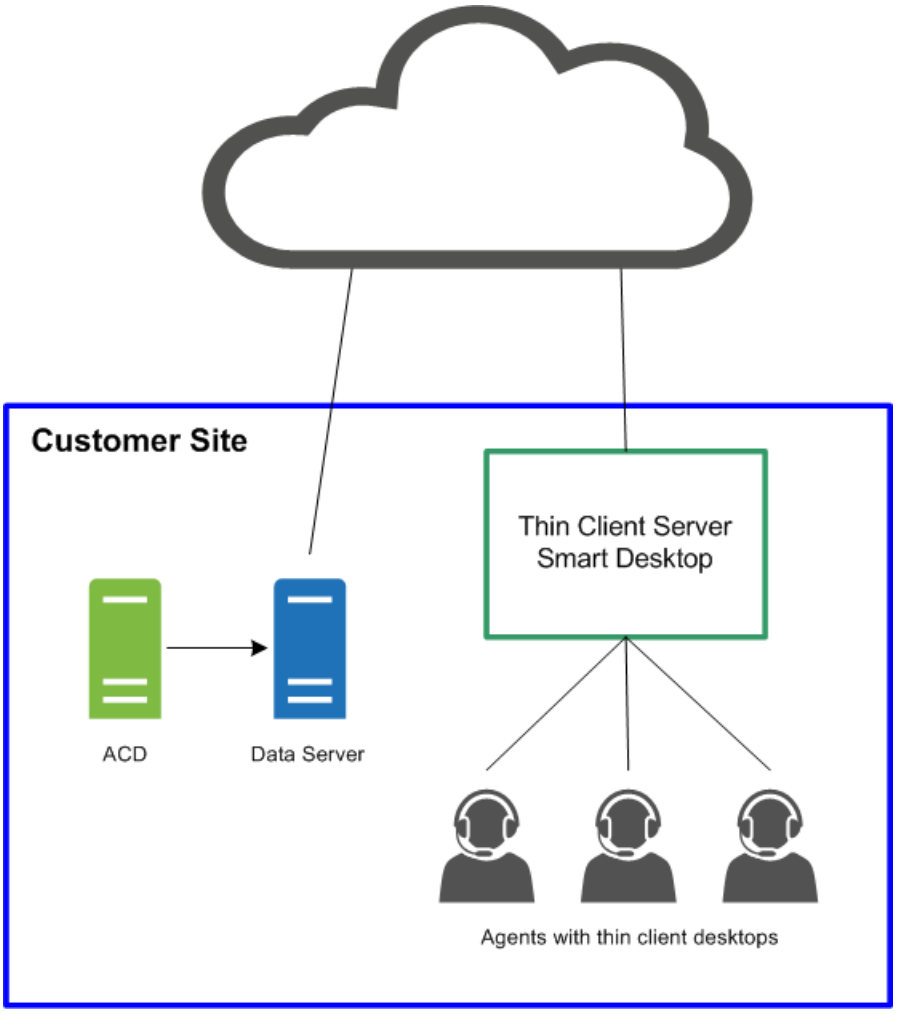
* Certaines langues prises en charge peuvent nécessiter une configuration supplémentaire pour votre implémentation Webex WFO. Consultez le support pour vous assurer que la langue que vous souhaitez transcrire est configurée pour vous. L'ajout de langues supplémentaires ou l'extension de l'offre actuelle nécessite une collaboration avec Cisco. Contactez votre représentant de compte pour plus d'informations.

Configuration du

Ce diagramme illustre un déploiement cloud WFO typique Webex.



Ce diagramme présente un déploiement cloud WFO Webex typique avec un environnement de client léger.


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

Environnements

Webex WFO prend en charge un certain nombre d'environnements et de technologies.

Pour obtenir les dernières informations de compatibilité prises en charge, reportez-vous à # www.cisco.com.

Téléphones pris en charge

Webex WFO prend en charge les téléphones suivants.

Téléphones durs

Reportez-vous au site Web Unified CM Silent Monitoring/Recording Supported Device Matrix (Matrice des périphériques pris en charge) pour obtenir la liste des téléphones matériels Cisco pris en charge.

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

Codecs pris en charge

Webex WFO prend en charge les codecs suivants :

- g711
- g722
- g729

Remarque : La taille du paquet de codec doit être d'au moins 20 ms pour fournir une qualité audio utilisable.

Utilisation de plusieurs softphones

Si vous utilisez plusieurs softphones en même temps, les softphones ne doivent pas se lier à un numéro de port local qui corresponde à l'un des numéros de port configurés dans la page Paramètres généraux (Gestion des applications > QM Configuration > paramètres globaux > paramètres SIP). Par exemple, si le numéro de port saisi sous
Les paramètres SIP sont 5060. Aucun de vos softphones ne peut utiliser un port local lié au numéro de port 5060 si vous avez l'intention d'utiliser plusieurs softphones en même temps.

Démarrez le téléphone logiciel, connectez-vous si nécessaire, puis utilisez l'un de ces outils pour afficher les connexions réseau de cet ID de processus. Si l'une des connexions réseau affiche un port local qui correspond à l'un des numéros de port configurés dans la page Paramètres généraux, vous devez effectuer l'une des actions suivantes :

- Utilisez le softphone seul, sans qu'aucun autre téléphone logiciel ne soit utilisé simultanément.
- Configurez le softphone de sorte qu'il n'utilise pas l'un des ports répertoriés.

Pour confirmer l'utilisation des ports, utilisez un outil qui surveille les connexions réseau tel que netstat (sur la ligne de commande, utilisez parameters-anob), TCPView ou CurrPorts.

Appareils mobiles pris en charge

Les agents peuvent accéder à une version limitée de Webex WFO sur un appareil mobile tel qu'un smartphone ou une tablette, en entrant l'URL WFO Webex dans le navigateur de l'appareil. L'agent est automatiquement redirigé vers une version mobile de Webex WFO, où il se connecte normalement.

Remarque : Le périphérique mobile doit pouvoir accéder au réseau sur lequel Webex WFO est installé.

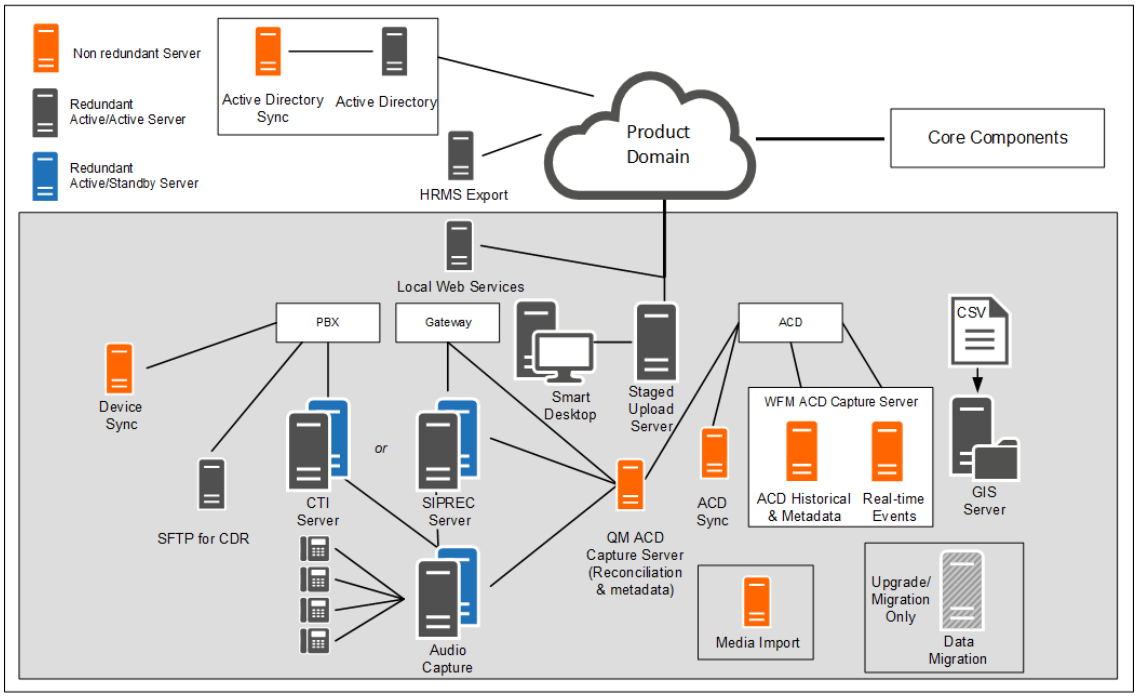
Les agents peuvent également consulter leurs horaires en dehors du travail via un client de messagerie ou l'application de calendrier sur un appareil mobile ou un ordinateur personnel. Le client de messagerie ou l'application de calendrier affiche l'horaire tel qu'il apparaît dans l'interface Webex WFO en lisant le fichier de données iCalendar du service WFM iCalendar.

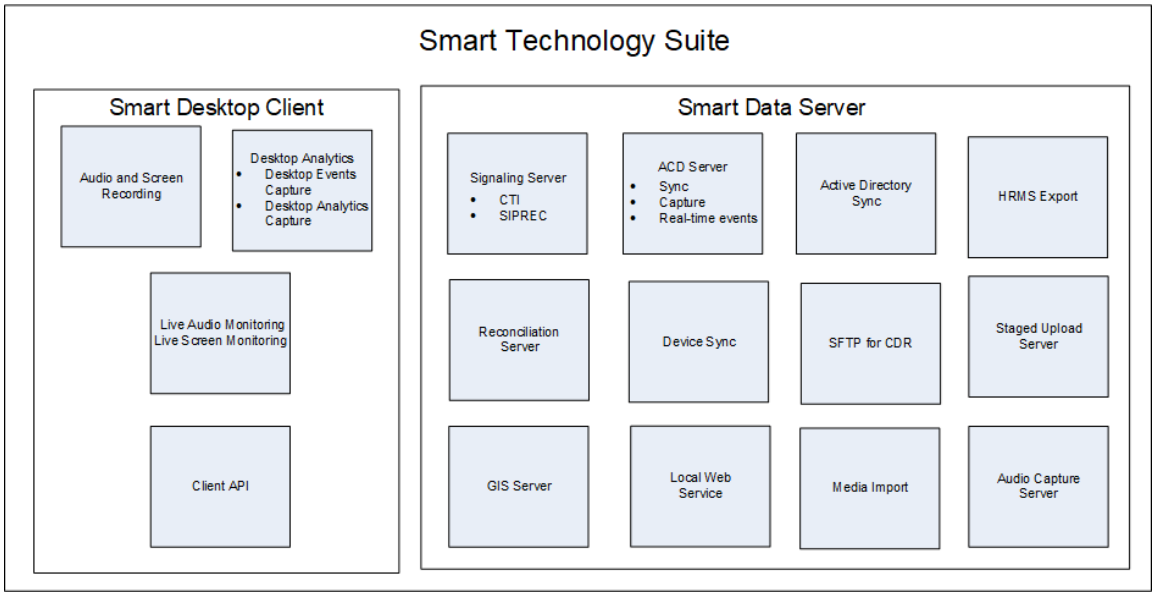
Les clients et les périphériques suivants sont pris en charge pour l'affichage d'un horaire en dehors du travail :

- Les appareils Apple tels que l'iPhone ou l'iPad (en conjonction avec l'application Apple Calendrier)
- Microsoft Outlook
- Les appareils Android comme les tablettes ou les téléphones (en conjonction avec une application de calendrier qui peut lire un fichier de .ics)

Composants Edge

Les composants WFO Edge Webex sont généralement déployés sur site sur site ou à distance. L'ensemble des composants constitue la Webex WFO Smart Technology Suite.





Webex Bureau intelligent WFO

Webex WFO Smart Desktop capture toutes les données utilisateur (c'est-à-dire l'enregistrement audio, l'enregistrement d'écran, l'activité du bureau et les métadonnées d'appel) sur le bureau d'un agent. Webex WFO Smart Desktop est installé sur les bureaux d'agents du centre d'appels ou sur un serveur qui héberge un client léger pris en charge. Le programme d'installation de Smart Desktop doit être téléchargé à partir de la page Webex WFO Application Management > administration > downloads.

À propos de Webex WFO Smart Desktop

Les données capturées par Smart Desktop peuvent varier en fonction de votre licence et des autorisations activées dans Webex WFO. Vous devez télécharger le programme d'installation de Smart Desktop à partir de Gestion des applications > administration > global > téléchargements (voir Télécharger Smart Desktop). Vous avez également besoin de l'extension Desktop Analytics pour votre navigateur.

L'enregistrement audio à l'aide de Smart Desktop dépend des types d'enregistrement. Les solutions de centre de contact en tant que service (CCaaS) enregistrent l'audio et envoient le fichier une fois le contact terminé. Les solutions hébergées par le client envoient les protocoles SIP et RTP car le contact est actif. Webex WFO effectue des enregistrements d'écran à l'aide du bureau d'agent et les enregistrements sont téléchargés une fois l'appel terminé.

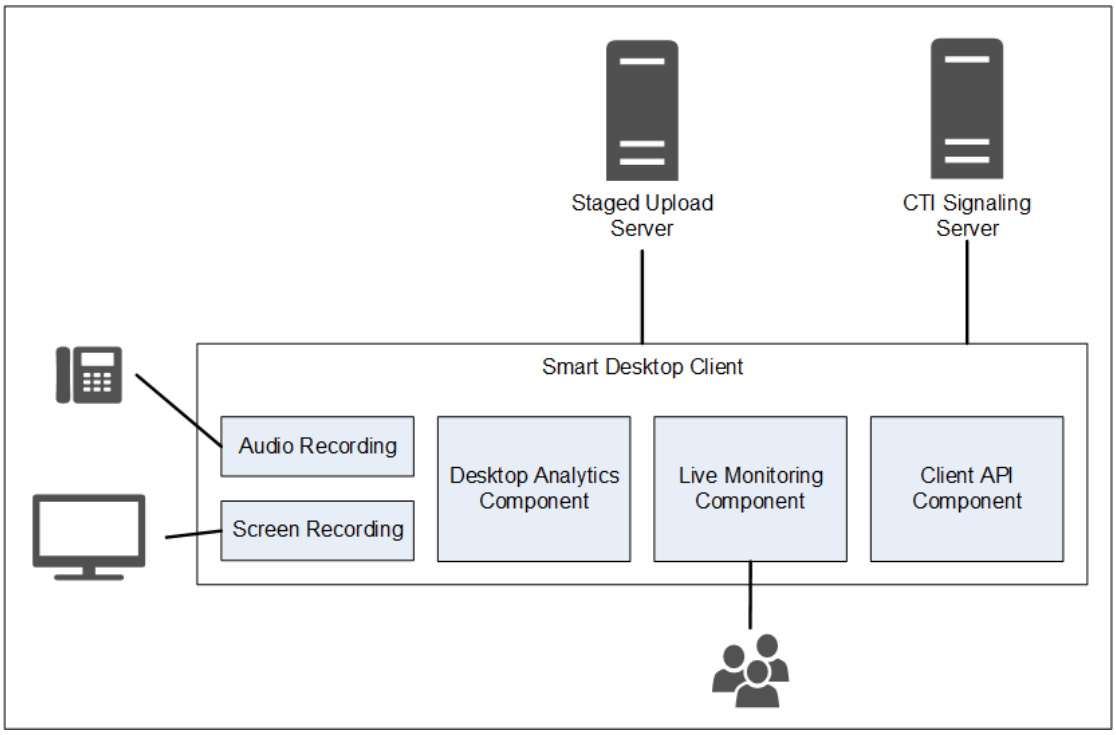
Le bureau intelligent comporte les composants suivants.

- Enregistrement audio et d'écran : ce composant enregistre les appels de l'agent.
- Desktop Analytics — Ce composant fournit des données d'analyse sur les enregistrements du bureau de l'agent.

- Surveillance dynamique vocale et surveillance dynamique de l'écran : ces composants permettent aux superviseurs d'écouter le son d'un agent et de visualiser l'écran d'un agent en temps réel. La surveillance de l'agent et la surveillance du poste de travail sont les deux types de surveillance de Smart Desktop.

  Surveillance des agents — Fonction destinée aux administrateurs et aux superviseurs qui leur permet de surveiller le son et les écrans des agents en temps réel.

  Desktop Monitoring — Une fonctionnalité qui permet aux administrateurs d'afficher les versions actives et installées de Smart Desktop des utilisateurs sur leurs PC, de définir des niveaux de journalisation et de télécharger à distance les journaux pour le dépannage.



Connectivité Smart Desktop Client

Le tableau suivant répertorie la connectivité de base au client Smart Desktop :

Composant	Se connecte à	Entrées/Sorties
Enregistrement audio et d'écran	PC de l'agent	Audio du téléphone et données d'écran
Analyse du bureau.	PC de l'agent	Audio du téléphone et données d'écran
Surveillance dynamique	PC d'autres agents	Données audio et d'écran du téléphone des autres agents

Connexion au serveur	Entrées/Sorties
Téléchargement intermédiaire	Informations sur le contact (enregistrements audio et d'écran et

métadonnées) Utilisez les liens ci-dessous pour accéder aux différentes rubriques Bureau

intelligent de ce document.

- Configuration requise et considérations relatives au bureau intelligent
- Matériel de bureau
- Utilisation du port du bureau intelligent
- Métadonnées de contact Smart Desktop
- Diagrammes de flux de données Smart Desktop Capture
- Installation de Smart Desktop
- Activer l'extension Desktop Analytics dans votre navigateur
- Test du bureau intelligent
- Gestion de Smart Desktop
- Application de commandes d'enregistrement

Configuration requise et considérations relatives au bureau intelligent

Voir Serveurs clients légers pour plus d'informations et de considérations lors de l'utilisation d'un serveur client léger et de Smart Desktop.

Reportez-vous à la Webex Matrice de compatibilité des produits WFO pour connaître les systèmes d'exploitation de bureau Windows et les navigateurs Web pris en charge.

Capture de la bande passante et dimensionnement du bureau

- Capture audio de bureau : 0,5 MB/min
- Capture d'écran : 1,5 MB/min par moniteur

EXEMPLE : Si un agent prend trente appels par jour avec un temps de conversation moyen de 5 minutes par appel, le calcul d'enregistrement audio du bureau sera de : 0,5 Mo/min x 5 minutes x 30 appels = 75 MB.
L'enregistrement de capture d'écran, si l'agent dispose de 3 écrans, serait de : 1,5 MB/min x 5 minutes x 30 appels x 3 écrans = 675 MB.

Voir Matériel de bureau pour connaître les exigences spécifiques relatives à la carte réseau, à l'espace disque, au

CPU, à la mémoire et au .NET Framework.

Environnements

Les environnements suivants sont pris en charge en plus des ordinateurs qui répondent à la configuration minimale requise du système d'exploitation.

- Architecture VDI (virtualisation des postes de travail)
- Serveurs Terminal Server
- Citrix
- Environnement de l'agent tiers
- Espace de travail AWS

Remarque : Si votre organisation utilise des VDI, des serveurs Terminal Server ou des solutions Citrix, partagez les informations suivantes avec votre représentant de compte Cisco pendant le processus d'installation : Heure de fin

À la fin d'un contact, nombre de machines, nombre de serveurs et spécifications générales de vos serveurs.

Les serveurs Terminal Server et les solutions Citrix ne prennent pas en charge Webex fonctionnalité de mise à jour automatique de WFO.

.NET Framework

Webex WFO Smart Desktop nécessite .NET Framework 4.5 pour Webex les fonctionnalités de WFO Analytics. Si .NET Framework n'est pas installé, Webex WFO ne peut pas capturer les événements du navigateur dans le cadre des données Desktop Analytics. Vous pouvez télécharger le .NET Framework à partir de http://www.microsoft.com/en- us/download/details.aspx ?id=30653.

Exclusions de l'analyse antivirus en temps réel

Cisco recommande d'exclure les répertoires Cisco suivants de l'analyse antivirus en temps réel afin de s'assurer que les fonctionnalités du Bureau intelligent s'exécutent comme prévu.

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

Configuration requise pour le pare-feu

Webex WFO doit être mis sur liste blanche et son accès via le pare-feu externe de votre organisation.

Considérations relatives aux navigateurs Web

Tout navigateur que vous utilisez doit autoriser le téléchargement de fichiers. Les bloqueurs de fenêtres publicitaires intempestives doivent être désactivés.

Modules logiciels du navigateur

Voir "Desktop Analytics Plug-in/Extension" dans Configuration requise pour plus d'informations. Cisco vous recommande de gérer vos extensions/plug-ins via l'objet de stratégie de groupe Windows pour vous assurer que toutes les fonctionnalités dépendantes fonctionnent comme prévu.

Si les utilisateurs utilisent à la fois les navigateurs Microsoft Edge et Google Chrome, Cisco vous recommande d'installer l'extension de navigateur sur les deux navigateurs. En l'installant sur un navigateur, Webex WFO ne peut pas collecter les données de l'autre navigateur qui n'a pas l'extension.

IMPORTANT Vous devez désinstaller les anciennes versions du navigateur avant d'installer la dernière version.

Procuration

- Smart Desktop prend en charge les proxys. Il tente d'utiliser un proxy qu'il détecte.
- Si un proxy Internet est utilisé, Smart Desktop nécessite que le proxy prenne en charge les connexions Web sécurisées.
- Toutes les connexions proxy doivent permettre au logiciel Smart Desktop de se connecter au Cloud Cisco sur le port 80/443.

Utilisation du port du bureau intelligent

Les informations de port pour Webex composants WFO Smart Desktop sont répertoriées ci-dessous.

En règle générale, les ports 80 et 443 vers un serveur Web doivent être ouverts pour se connecter à Webex WFO pour toutes les intégrations cloud avec Webex WFO. Les exigences exactes en matière de port varient en fonction de votre modèle de déploiement cloud.

Solutions hébergées par le client

Reportez-vous au tableau ci-dessous pour les solutions hébergées par le client. Parmi les exemples de solutions hébergées par le client, citons Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Express, Avaya Communication Manager, etc.

Port	Util	Source	Destination
Bureau intelligent			

Port	Utiliser	Source	Destination	Remarques
TCP 80, 443	Surveillance dynamique audio (WebRTC)	Audio Capturer Serveur* PC de l'agent	du superviseur Navigateur	
UDP 39500 - 43500	RTP d'enregistrement	Téléphone Voix passerelle**	Audio Capturer Serveur	
UDP 49152 - 65535	Surveillance dynamique audio (RTP)	Audio Capturer Serveur* PC de l'agent	du superviseur Navigateur	
TCP 52102	Signalisation d'enregistrement	Audio Capturer Serveur* PC de l'agent	Signalisation Serveur	

*Architecture d'enregistrement réseau

**Architecture d'enregistrement de la passerelle

Solutions CCaaS

Reportez-vous au tableau ci-dessous pour connaître les solutions CCaaS (centre de contact en tant que service).

Port	Utiliser	Source	Destination	Remarques
Bureau intelligent				
TCP 80, 443	Surveillance dynamique de l'écran	PC de l'agent	Navigateur du superviseur	

STUN/TURN Cloud

Reportez-vous au tableau ci-dessous pour connaître les ports Cloud STUN/TURN.

Port	Utiliser	Connexions
Bureau intelligent		
TCP 80, 443	Via websocket	Serveur de signalisation
TCP 6379	Administration STUN/TURN via l'administrateur système dans Webex WFO.	Configuration
UDP 49152 - 65535	Médias (audio et vidéo)	SRTP (peer-to-peer)
UDP 49152 - 65535	Médias (audio et vidéo)	SRTP (et non peer-to-peer)
UDP/TCP 3478	-	Détection d'adresses IP

Métadonnées de contact Smart Desktop

Le tableau suivant répertorie les métadonnées de contact Smart Desktop disponibles utilisées pour chaque mode de capture :

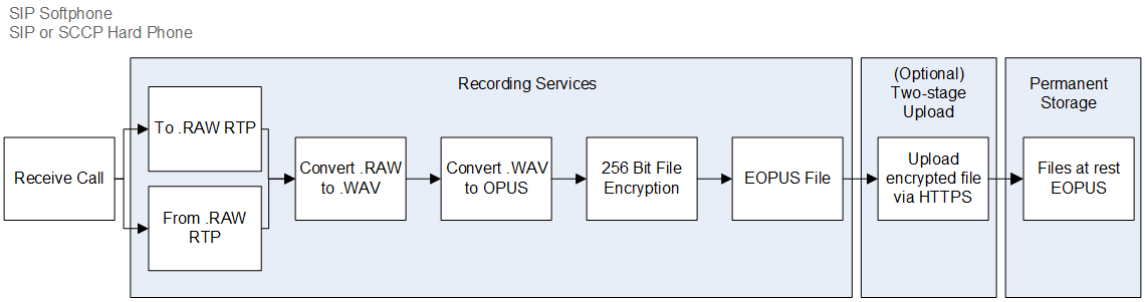
Métadonnées de contact	Signalisation SIP	Signalisation SCCP	Journalisation RTP
ID de l'appel	X	X	S'appuie sur des tiers pour fournir des données en temps réel aux CDC API
ANI (appel)	X	X	S'appuie sur des tiers pour fournir des données en temps réel aux CDC API
DNIS (appelé)	X	X	S'appuie sur des tiers pour fournir des données en temps réel aux CDC API
Ligne/Poste			S'appuie sur des tiers pour fournir des données en temps réel aux CDC API
Direction de l'appel	X	X	S'appuie sur des tiers pour fournir des données en temps réel aux CDC API

Métadonnées de contact	Signalisation SIP	Signalisation SCCP	Journalisation RTP
ID contact associé	X		S'appuie sur des tiers pour fournir des données en temps réel à CDC API
Type d'enregistrement	X	X	X
Duration	X	X	Basé sur un segment, sauf si join_start est utilisé
Adresse MAC	X	X	
Utilisateur (par ID de connexion Windows)	X	X	X
Date/Heure des appels	X	X	X

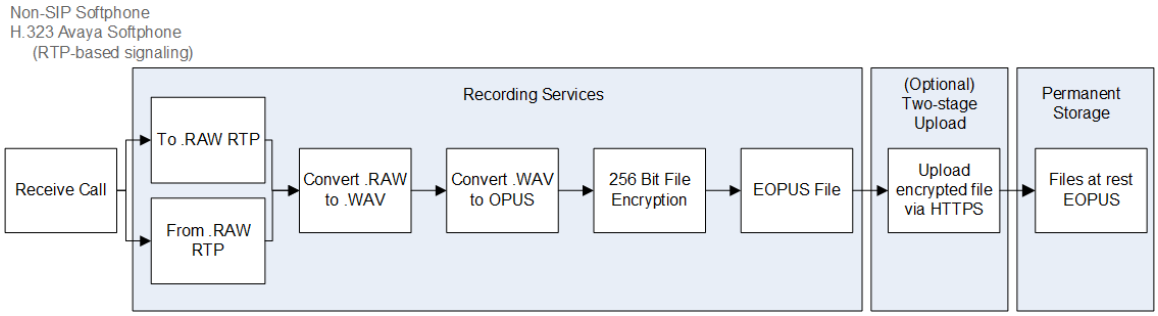
Diagrammes de flux de données Smart Desktop Capture

Cette rubrique inclut des diagrammes qui décrivent le flux de données Smart Desktop.

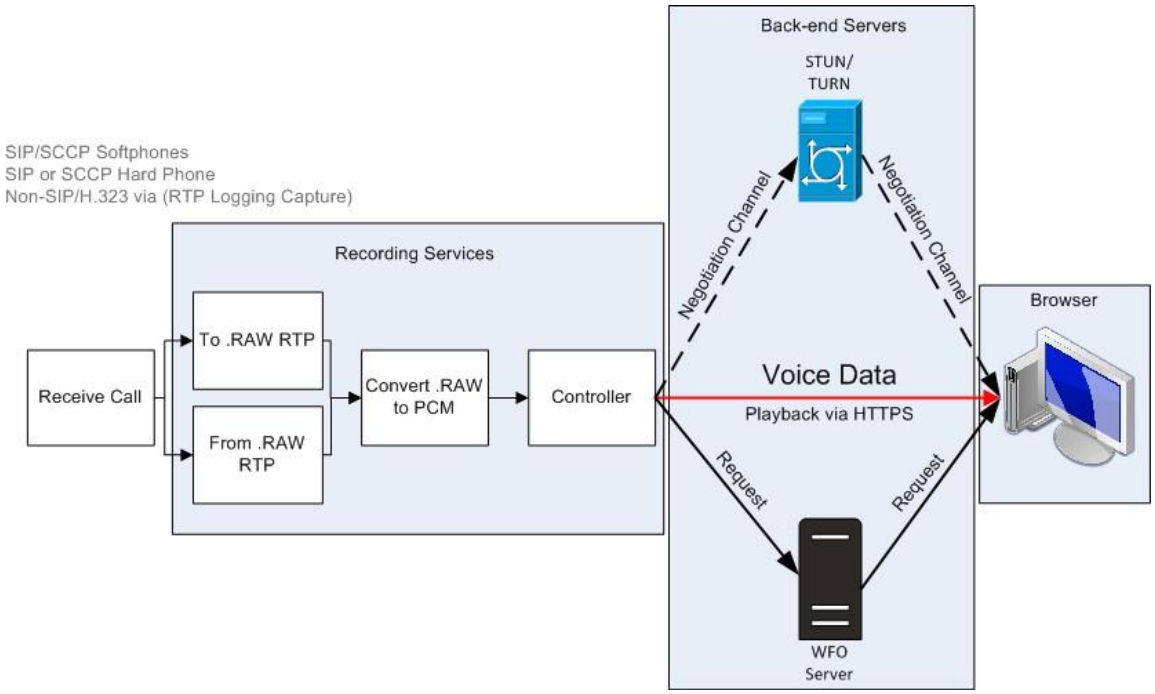
Signalisation SIP/SCCP de bureau intelligent



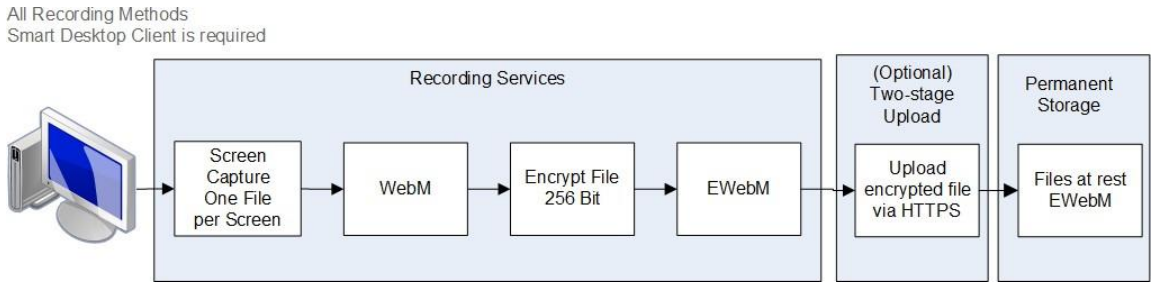
Journalisation des RTP des postes de travail intelligents



Surveillance dynamique Smart Desktop

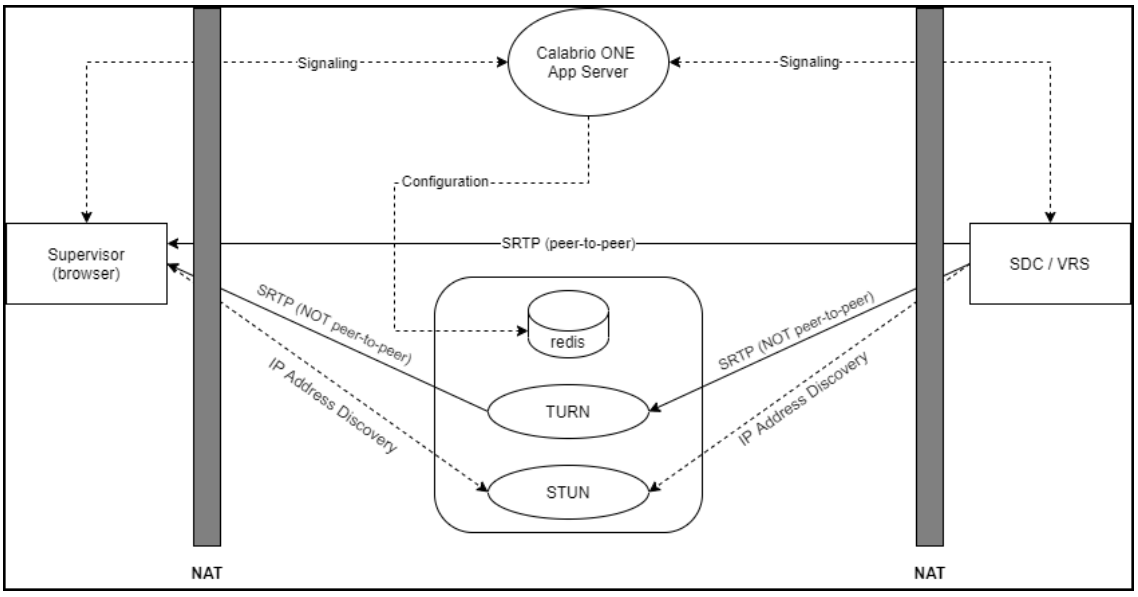


Surveillance dynamique de l'écran Smart Desktop



REMARQUE L'écran Smart Desktop et l'enregistrement audio utilisent AES cryptage 256 bits si l'enregistrement a lieu à l'intérieur Webex WFO.

Connexions de surveillance dynamique Smart Desktop



Connexion	Ports	Protocole	Remarques
Signalisation	80, 443	TCP	Par websocket
Configuration	6379	TCP	Administration STUN/TURN utilisant un rôle Administrateur système dans Webex WFO
SRTP (poste à poste)	49152–65535	UDP	Médias audio et visuels

Connexion	Ports	Protocole	Remarques
SRTP (et non d'égal à égal)	49152–65535	UDP	Médias audio et visuels
Détection d'adresses IP	3478	UDP TCP	—

Test du bureau intelligent

Après avoir installé Smart Desktop (voir Installation de Smart Desktop) et Desktop Analytics (voir Activer l'extension Desktop Analytics dans votre navigateur), procédez comme suit pour vous assurer que votre implémentation Smart Desktop fonctionne correctement.

Prérequis

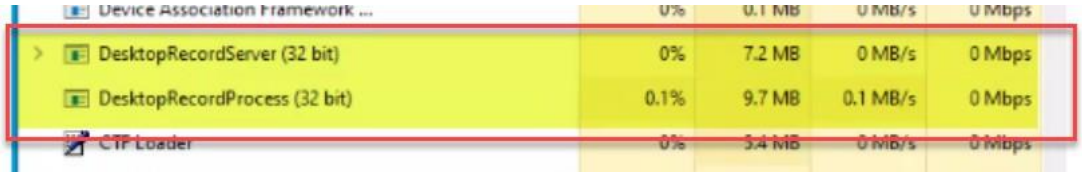
- La connexion de votre fenêtre (**Gestion des** applications> **Configuration** utilisateur> **Utilisateurs**) doit être au format [Domaine\WindowsNTID]. Si vous ajoutez la connexion de votre Windows après avoir installé Smart Desktop, vous devez redémarrer Smart Desktop ou ses services de bureau.
- L'agent dispose des autorisations suivantes affectées à son rôle. Les autorisations se trouvent dans **Gestion des** applications> **Configuration** utilisateur> **Rôles**.
  - Capture Desktop Analytics
  - Capturer les contacts
  - Écran d'enregistrement
  - Enregistrement de la voix
  - Surveillance dynamique de l'écran
  - Surveillance dynamique vocale
  - Enregistrement à la demande (signalisation RTP)
  - Capturer les événements du bureau

  REMARQUE Les solutions de centre de contact en tant que service (CCaaS) ne prennent pas en charge la surveillance audio dynamique.
- L'extension Desktop Analytics est en cours d'exécution dans votre navigateur.

Procédures

Assurez-vous que les processus corrects sont en cours d'exécution sur votre ordinateur

1. Ouvrez le **Gestionnaire des** tâches.
2. Vérifiez que les processus DesktopRecordServer et DesktopRecordProcess sont en cours d'exécution dans le Gestionnaire des tâches. Si DesktopRecordProcess n'est pas en cours d'exécution, assurez-vous que vous avez correctement saisi la connexion de votre fenêtre, comme décrit dans les conditions préalables.



3. Vérifiez que ciSaasDesktopRecord est en cours d'exécution dans **le Gestionnaire des** tâches.

4. Ouvrez l'application **Services** sur votre ordinateur et vérifiez que Calabrio ONE Smart Desktop Record Service est en cours d'exécution.

Assurez-vous Webex WFO reconnaît votre ordinateur

Accédez à **Gestion des** applications> **Global** > **Monitoring** > **Desktop Monitoring**. Si vous voyez un cercle vert sous la colonne État, cela signifie que vous êtes connecté et que la version installée de Smart Desktop est la version active.

S'assurer Webex WFO reconnaît les agents qui utilisent Smart Desktop

1. Accédez à **Gestion des** applications> **Surveillance>** Globale > **Surveillance de** l'agent.
2. Vous pouvez surveiller l'écran d'un agent si l'icône de surveillance de l'écran de l'agent est noire. Si l'icône est noire, cela signifie que Smart Desktop Client est en cours d'exécution sur le PC de l'agent avec les autorisations appropriées.
3. Vous pouvez surveiller l'audio d'un agent si l'icône de surveillance audio de l'agent Est noir. Si l'icône est noire, cela signifie que l'agent est configuré pour l'enregistrement de bureau, que Smart Client s'exécute sur son PC avec les autorisations appropriées, qu'il est configuré pour l'enregistrement de serveur et qu'il est affecté à un périphérique surveillé sur la page Device Associations (Associations de périphériques).

4. Cliquez sur l'icône de surveillance de l'écran de l'agent pour ouvrir la fenêtre de surveillance dynamique de l'écran.

5. Dans la fenêtre de surveillance dynamique de l'écran, cliquez sur **Écran** pour démarrer la session de surveillance. Cliquez sur **Audio**

   Pour surveiller l'appel de l'agent. Vous ne pouvez entendre le son que si l'agent est en communication.

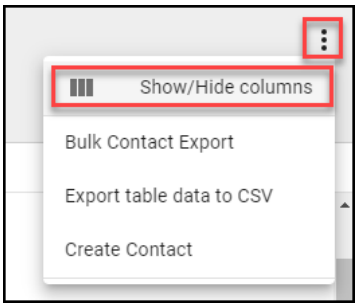
Effectuer un appel de test

1. Passer un appel téléphonique depuis le bureau d'un agent.
2. Dans Webex WFO, cliquez sur **Interactions**.
3. Vérifiez que vous pouvez trouver l'enregistrement de l'appel.
4. Double-cliquez sur l'enregistrement pour lire l'appel et l'enregistrement d'écran, le cas échéant.

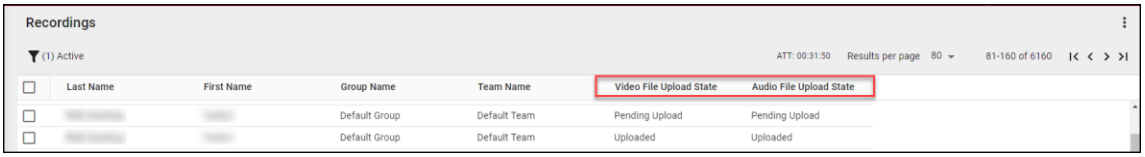
   Si le panneau Enregistrement d'écran n'apparaît pas ou est vide, vérifiez que le bloqueur de fenêtres publicitaires intempestives du navigateur est désactivé.

Consulter l'état de téléchargement des contacts enregistrés vidéo et audio

1. Accédez à **Interactions**.
2. Cliquez sur l'icône **Options de listes** dans le coin supérieur droit de la page.
3. Cliquez sur **Afficher/Masquer les colonnes**. La fenêtre Afficher/Masquer les colonnes s'affiche.



4. Cliquez sur **État** de téléchargement de fichier audio et **État de téléchargement** de fichier vidéo s'ils sont répertoriés sous **Colonnes masquées**.
5. Cliquez sur **Appliquer**. Maintenant, vous pouvez facilement voir si les fichiers vidéo et audio sont en attente de téléchargement ou ont été téléchargés avec succès.



6. Double-cliquez sur un contact pour visualiser les enregistrements audio et d'écran associés à l'appel.

Gestion de Smart Desktop

Cisco recommande de mettre à jour Smart Desktop tous les trimestres. Webex WFO prend en charge un processus de mise à jour non interruptif.

Que vous choisissiez de mettre à jour automatiquement ou d'effectuer des mises à jour gérées par le client, les mises à jour s'exécutent silencieusement et sans interruption des enregistrements ou des contacts. La version existante et la version mise à jour de Smart Desktop s'exécutent côte à côte jusqu'à ce qu'un processus de connexion Windows ait lieu. La surveillance du bureau permet aux administrateurs d'afficher les versions actives et installées de Smart Desktop des utilisateurs sur leurs PC, de définir des niveaux de journalisation et de télécharger à distance les journaux pour le dépannage.

MEILLEURES PRATIQUES Les administrateurs doivent se familiariser avec la surveillance des postes de travail pour vérifier l'état et les versions de Smart Desktop dans votre organisation.

Mise à jour automatique

Webex WFO dispose d'une fonction de mise à jour automatique qui peut être activée ou désactivée à tout moment en accédant à **Gestion des** applications> **Administration** > **Paramètres globaux**. Dans la page Paramètres généraux, utilisez le bouton Activer la **mise à jour** automatique du client pour activer ou désactiver la fonction de mise à jour automatique.

Si cette option est activée, lorsqu'un utilisateur se connecte à un ordinateur exécutant Smart Desktop, l'ordinateur vérifie si une nouvelle mise à jour est disponible au téléchargement.

Mise à jour gérée par le client

Vous pouvez diffuser des mises à jour à l'aide d'une diffusion de logiciel géré (par exemple, GPO ou LANDesk).

MEILLEURES PRATIQUES La stratégie de votre organisation doit exiger que les agents déconnectent leur PC à la fin de leur quart de travail. Cette action peut être automatisée à l'aide des paramètres GPO.

Meilleures pratiques pour le téléchargement d'enregistrements sur Webex WFO

Obtenir des enregistrements audio et d'écran depuis le bureau d'un utilisateur dès que possible garantit que les enregistrements sont disponibles pour la lecture après l'enregistrement de l'appel. Il existe des options permettant de déplacer les enregistrements hors du bureau de l'utilisateur immédiatement ou à une heure donnée. La décision de télécharger les enregistrements est le fruit d'une collaboration entre l'entreprise et le personnel informatique en tenant compte des besoins en matière d'accessibilité audio et d'écran, de bande passante et de stockage. Cisco recommande les processus de téléchargement répertoriés ci-dessous.

- Téléchargement immédiat via des workflows QM : ce processus garantit que l'enregistrement est disponible pour la lecture après l'enregistrement de l'appel et que l'espace de stockage n'est pas trop sollicité sur le PC de l'agent. Cisco recommande de configurer les enregistrements de manière à ce

qu'ils soient immédiatement téléchargés à partir du PC de l'agent vers

Webex WFO si la bande passante WAN et LAN est suffisante. Utilisez la page d'administration **du** flux de travail de la **Gestion** des applications pour effectuer des téléchargements immédiats.

- Téléchargement différé à l'aide de workflows QM : vous pouvez configurer ce processus pour qu'il ait lieu après les heures de bureau. Les enregistrements audio et/ou d'écran sont téléchargés à une heure précise. Une fois vos enregistrements téléchargés, vous pouvez les télécharger à la demande. Utilisez la page d'administration du flux de travail de la **Gestion** des applications pour effectuer des téléchargements différés.
- Téléchargement immédiat à l'aide du Webex paramètres régionaux de téléchargement échelonné du serveur de données WFO : si la bande passante Internet est un problème, une approche de téléchargement échelonné peut atténuer le trafic WAN externe pendant les heures de bureau. Cette option nécessite de configurer les paramètres de téléchargement intermédiaire du serveur de données Cisco (voir Configurer le serveur de données et Configurer le téléchargement intermédiaire pour plus d'informations). Ce processus garantit que les appels sont déplacés d'un PC vers un stockage local pendant la journée. À une heure précise, après les heures de bureau, les enregistrements sont téléchargés. Une fois vos enregistrements téléchargés, vous pouvez les télécharger à la demande. Configurez "Regional Data Server Staged Upload Settings" sur la page Configuration du serveur de données de la Gestion des applications pour effectuer des téléchargements intermédiaires.

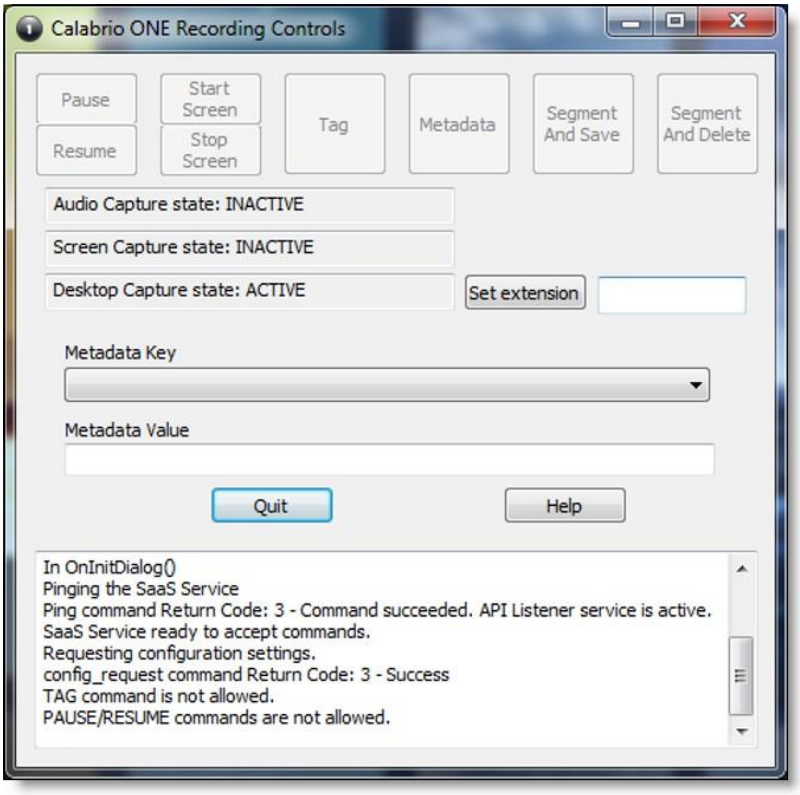
Application de commandes d'enregistrement

Webex Commandes d'enregistrement WFO est une application Web autonome qui vous permet de démarrer, mettre en pause, reprendre et arrêter l'enregistrement audio, d'écran et de frappe pour les appels actifs. Vous pouvez également marquer des appels et leur ajouter des métadonnées.

Pour lancer les commandes d'enregistrement, sélectionnez **Commandes** d'enregistrement Calabrio ONE dans le menu Démarrer. Pour fermer les commandes d'enregistrement, cliquez sur **Quitter**.

Les agents peuvent utiliser l'application de contrôle des enregistrements Smart Desktop, également connue sous le nom d'application DCC (Desktop Capture and Controller), pour contrôler les enregistrements et insérer des métadonnées à partir de leurs postes de travail. L'application de commandes d'enregistrement est installée avec Smart Desktop. Il apparaît dans la liste Programmes sous Cisco sur le bureau de l'agent après l'installation de Smart Desktop.

L'application de commandes d'enregistrement est illustrée ci-dessous :



Les rôles et autorisations corrects doivent être accordés aux agents par un administrateur du service partagé pour que ceux-ci puissent utiliser l'application Contrôles d'enregistrement.

L'application de commandes d'enregistrement permet aux utilisateurs d'effectuer les opérations suivantes :

- Marquer un appel actif ou l'enregistrement d'appel le plus récent
- Enregistrement des appels
- Mettre en pause et reprendre l'enregistrement audio
- Démarrer l'enregistrement d'un appel
- Supprimer l'écran et l'audio précédemment enregistrés lors d'un appel
- Supprimer l'enregistrement de l'appel actif : une fois l'appel terminé, vous ne pouvez pas supprimer l'enregistrement
- Connexion ou déconnexion pour l'enregistrement de réservation
- Ajouter des métadonnées à un appel actif ou à l'appel le plus récent
- Démarrer ou arrêter l'enregistrement audio et d'écran d'un appel actif
- Démarrer ou arrêter l'enregistrement de l'écran

L'application Commandes d'enregistrement prend en charge les types d'enregistrement suivants :

- Enregistrement de poste de travail
- Enregistrement réseau

Voir "Contrôles d'enregistrement API" dans le *API Guide* de référence pour plus d'informations sur les commandes DCC.

Webex serveur de données WFO

Le serveur de données WFO Webex est responsable des fonctions telles que la synchronisation des ACD et les téléchargements intermédiaires. Un administrateur de locataire peut installer le serveur de données pour un seul service partagé ou un administrateur système peut installer un serveur de données de base et le configurer en tant que serveur de données partagé pour plusieurs locataires.

Remarque : Si le serveur de données doit se connecter via un proxy Web, tous les services WFO qui s Webex'exécutent sur celui-ci doivent s'exécuter en tant que comptes de connexion Windows avec paramètres de proxy. Lors de la configuration du serveur de données avec Serveur proxy, le service de serveur de données doit être configuré pour s'exécuter en tant qu'administrateur local. Webex WFO ne prend pas en charge l'utilisation de scripts PAC pour se connecter à Internet.

Les services installés avec le logiciel Data Server sont les suivants.

- service de signalisation CTI
- Serveur de données
- Services Web du serveur de données
- Service d'enregistrement réseau
- SIPREC Service

Dans Webex WFO, voici les fonctions du serveur de données, leurs descriptions et le service sur lequel elles sont alignées.

- Paramètres de synchronisation ACD du serveur de données régional : permet de synchroniser les informations relatives aux utilisateurs et aux équipes à partir d'un ACD pris en charge (Webex le serveur de données WFO).
- Paramètres du serveur de capture d'enregistrement — Utilisé pour les environnements d'enregistrement audio de serveur Edge ou de passerelle (SBC). Le service de signalisation principal (CTI ou SIPREC) affecte les appels aux serveurs de capture dans un algorithme tourniquet (Webex service d'enregistrement réseau WFO).
- Emplacement du fichier SIG du serveur de données régional : permet d'importer des métadonnées de contact externe à partir d'un fichier de CSV dans Webex WFO (Webex serveur de données WFO).

- Enregistrement Paramètres du serveur de signalisation SIPREC : utilisé pour suivre les événements de début et d'arrêt et capturer les métadonnées pour les enregistrements d'appels. Un service de signalisation SIPREC est utilisé pour les environnements d'enregistrement de passerelle périphérique (contrôleur de limites de session) (Webex le service WFO SIPREC).
- Paramètres du serveur d'enregistrement CTI de signalisation — Utilisé pour suivre les événements de début et d'arrêt et capturer les métadonnées pour les enregistrements d'appels. Un service de signalisation CTI est utilisé pour les environnements d'enregistrement de serveurs périphériques (Webex WFO CTI Signaling Service).
- Paramètres de téléchargement intermédiaire du serveur de données régional — Utilisé pour collecter localement les données de contact des utilisateurs de Smart Desktop et télécharger périodiquement les fichiers vers les composants WFO Webex dans le cloud (Webex le serveur de données WFO).
- Regional Data Server ACD Capture Settings — Utilisé pour capturer des métadonnées personnalisées et rapprocher les appels reçus via une passerelle (Webex le serveur de données WFO).
- Regional Data Server Real-Time Event Settings (Paramètres d'événement en temps réel du serveur de données régionales) : utilisé pour capturer des données d'ACD historiques et en temps réel pour WFM et ACD métadonnées à joindre aux contacts d'appel sous forme de métadonnées personnalisées (Webex serveur de données WFO).
- Paramètres de rapprochement du serveur de données régional — Le rapprochement est un processus qui connecte des enregistrements racine de passerelle, qui comportent des données d'appel limitées, avec des données d'appel supplémentaires incluant l'association avec l'agent approprié (Webex serveur de données WFO).
- Synchronisation Active Directory — Permet à Webex WFO de faire correspondre et de synchroniser Webex utilisateurs WFO avec des utilisateurs Active Directory (Webex serveur de données WFO).
- Paramètres de synchronisation des périphériques du serveur de données — Vous permet de synchroniser des appareils via le serveur de données. Ces périphériques peuvent ensuite être associés à des utilisateurs, des groupes d'enregistrement et des types d'enregistrement à l'aide de la page Associations de périphériques de la Gestion des applications (Webex serveur de données WFO).
- Paramètres du service Web local — Permet API’intégration sur ce serveur de données. Si cette option est activée, vous avez la possibilité d'activer ce qui suit :
    - Contrôles des services Cisco IP Phone : autorise les contrôles d'enregistrement Cisco à partir des périphériques Cisco pris en charge.
    - Commandes d'enregistrement simplifiées API : vous permet d'utiliser l'authentification native du serveur de données pour les contrôles d'enregistrement Cisco.
- Configuration HRMS — Permet au serveur de données d'exporter des données vers un système de gestion des ressources humaines (HRMS) (Webex serveur de données WFO).

- SFTP Configuration : vous permet de configurer votre serveur de SFTP (Webex le serveur de données WFO).

- Paramètres du serveur d'importation de médias — Permet l'importation de fichiers d'enregistrement à partir d'un emplacement externe (Webex serveur de données WFO).

Configuration système requise

Les sections suivantes énumèrent la configuration minimale requise pour Webex

WFO. Pour obtenir les dernières informations de compatibilité prises en charge,

reportez-vous à # www.cisco.com.

Matériel de bureau

La configuration matérielle requise pour Webex postes de travail WFO est la suivante :

Matériel de bureau	
Carte réseau	Carte réseau 100 Mbit Les cartes réseau doivent prendre en charge le mode Promiscuous. Configurez les paramètres d'alimentation de Windows pour désactiver "Autoriser l'ordinateur à éteindre ce périphérique pour économiser de l'énergie" sur les cartes d'interface réseau.
Espace disque	20 Go Stockage des enregistrements vocaux (MB) = nombre d'enregistrements × durée moyenne d'appel × 0,5 MB par minute **NOTE** Cette formule est basée sur un débit audio de 64 kbps (kilobits par seconde). [(64 kbps × 60 sec) ÷ 8 bits] ÷ 1024 Ko = 0.46875 MB par minute Stockage des enregistrements d'écran (MB) = nombre d'enregistrements × durée moyenne d'appel × 1,5 MB par minute **Remarque** : Les exigences de stockage pour les enregistrements d'écran dépendent de trois facteurs : la longueur d'enregistrement, la résolution du moniteur et le nombre des moniteurs en cours d'enregistrement. La valeur affichée ici est basée sur un seul moniteur. Chaque moniteur supplémentaire est

enregistré séparément, donc

Matériel de bureau	
	vous devez appliquer cette formule pour chaque moniteur.
CPU	Intel Core 2 Duo 2,0 GHz, Core i3, AMD Athlon 64 X2 ou supérieur
Mémoire	2 Go

Logiciel de bureau

.NET Framework

Webex WFO Smart Desktop nécessite .NET Framework 4.5 pour les fonctionnalités Webex WFO Analytics. Si .NET Framework n'est pas installé, Webex WFO ne peut pas capturer les événements du navigateur dans le cadre des données Desktop Analytics. Vous pouvez télécharger le .NET Framework depuis http://www.microsoft.com/en- us/download/details.aspx?id=30653.

Navigateurs

Tout navigateur que vous utilisez doit autoriser les téléchargements de fichiers. Les bloqueurs de popups doivent être désactivés.

Plug-in/extension Desktop Analytics

Les utilisateurs qui administrent les champs pour Desktop Analytics via la page Gestionnaire de champs dans Webex WFO et les bureaux d'agent sur lesquels Smart Desktop est installé doivent avoir l'extension/le plug-in de navigateur Calabrio Analytics activé. Le plug-in est nécessaire non seulement pour marquer les champs dans le navigateur, mais également pour surveiller l'activité Web de l'agent dans le navigateur.

Activer l'extension Desktop Analytics dans Firefox

La première fois que vous vous connectez à Webex WFO en utilisant Firefox, vous voyez une boîte de dialogue vous demandant d'installer l'extension de navigateur Calabrio. Sélectionnez **Autoriser cette installation** et cliquez sur **Continuer**. Aucune autre action n'est requise.

Activer le plug-in Desktop Analytics dans Microsoft Edge Chromium

Dans Edge Chromium, accédez à https://chrome.google.com/webstore/detail/calabrio-analytics-plugin/hecgknieibccghjmmhhckdfeobjoffdf et cliquez sur **Ajouter à Chrome**.

Activer le plug-in Desktop Analytics dans Chrome

L'extension Chrome peut être téléchargée ou installée via les paramètres GPO. Téléchargez et installez le plug-in Calabrio Analytics, version 0.2.0.4. Le plug-in se trouve à :

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

REMARQUE Si cliquer sur le lien ne fonctionne pas, copiez l'URL et collez-la dans votre navigateur.

Adobe Acrobat Reader

Adobe Reader est requis pour ouvrir les fichiers PDF exportés et la documentation utilisateur. Un téléchargement gratuit d'Acrobat Reader est disponible sur www.adobe.com.

IMPORTANT Il existe des problèmes connus avec les versions d'Adobe Reader qui utilisent la fonctionnalité Sécurité (renforcée). Si vous prévoyez d'utiliser la fonctionnalité Desktop Analytics, vous devez accéder à **Sécurité (renforcée)** sous **Préférences** dans Adobe Reader, décocher la case **Activer le mode protégé au démarrage**
et **Sécurité renforcée** cochez les cases, cliquez sur **Oui** pour tous les messages d'avertissement, puis cliquez sur **OK** pour enregistrer vos modifications. Une fois terminé, redémarrez Adobe Reader pour que les modifications prennent effet. Si Adobe Reader n'est pas configuré correctement, Desktop Analytics ne pourra pas capturer les événements liés à Adobe Reader.

Logiciel de bureau et capture audio

Pour que Smart Desktop puisse effectuer une détection de téléphone et une capture audio appropriées, la capacité de détecter et de capturer certains protocoles réseau (tels que SIP, SCCP et RTP) est requise. Tout logiciel exécuté sur le PC qui interfère avec, redirige ou masque le trafic réseau empêchera Smart Desktop de fonctionner correctement.

EXEMPLE Le client SonicWall VPN avec le filtre léger Deterministic Network Enhancer (DNE) activé provoque la redirection du trafic réseau sortant depuis la carte réseau
Que Smart Desktop utilise. Dans ce cas, le filtre léger DNE doit être désactivé pour permettre à Smart Desktop de fonctionner correctement.

Activez l'extension Desktop Analytics dans votre navigateur

Smart Desktop doit être installé sur votre ordinateur et activé avant de pouvoir marquer des champs. Les utilisateurs autorisés à administrer les champs de Desktop Analytics à l'aide de la page Gestionnaire de champs et sur les bureaux des agents sur lesquels Smart Desktop est installé doivent avoir le plug-in de navigateur Desktop Analytics approprié configuré pour le navigateur qu'ils utilisent.

Prérequis

- Votre organisation possède l'une des licences suivantes :
  - Notions essentielles sur l'analyse
  - Analytics Enterprise

- Analyse de bureau

- Smart Desktop est installé et activé sur votre ordinateur.

Procédures

Activer l'extension Desktop Analytics dans Firefox

La première fois que vous vous connectez à Webex WFO en utilisant Firefox, vous voyez une boîte de dialogue vous demandant d'installer l'extension de navigateur Calabrio. Sélectionnez **Autoriser cette installation** et cliquez sur **Continuer**. Aucune autre action n'est requise.

Activer le plug-in Desktop Analytics dans Microsoft Edge Chromium

Dans Edge Chromium, accédez à https://chrome.google.com/webstore/detail/calabrio-analytics-plugin/hecgknieibccghjmmhhckdfeobjoffdf et cliquez sur **Ajouter à Chrome**.

Activer le plug-in Desktop Analytics dans Chrome

L'extension Chrome peut être téléchargée ou installée via les paramètres GPO. Téléchargez et installez le plug-in Calabrio Analytics, version 0.2.0.4. Le plug-in se trouve à l'adresse suivante :

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

REMARQUE Si cliquer sur le lien ne fonctionne pas, copiez l'URL et collez-la dans votre navigateur.

Rubriques connexes

"Installation Webex WFO Smart Desktop" dans le *Webex Guide d'installation de WFO*

Serveurs clients légers

NOTE prend en charge Citrix XenApp installé uniquement sur un serveur Windows pris en charge.

Lorsque vous utilisez un serveur client léger, notez :

- Les clients légers qui utilisent le Smart Desktop nécessitent une session de bureau à distance pour capturer toutes les données de l'utilisateur (audio, écran et enregistrement de bureau). Si aucune session de bureau à distance n'est présente, installez Smart Desktop sur les bureaux d'agent pour capturer toutes les données utilisateur sur le bureau pendant que l'utilisateur est connecté.
- Configurez les flux de travail de manière à utiliser le téléchargement immédiat pour l'écran et la voix afin de garantir l'accessibilité de tous les enregistrements.

- Si vous utilisez Smart Desktop à des fins d'enregistrement, le serveur client léger nécessite des ressources serveur supplémentaires pour les enregistrements d'écran. Les besoins en ressources varieront selon la conception réelle et peuvent nécessiter des conceptions matérielles détaillées qui devraient être examinées par Cisco avant le déploiement.
- Si vous utilisez une image virtuelle et qu'elle a accès à votre carte d'interface réseau locale, vous pouvez utiliser Smart Desktop pour l'enregistrement côté agent.

Installation du serveur client léger

Installez Citrix XenApp ou Windows Terminal Services conformément à la documentation du produit.

Utilisez les paramètres suivants requis pour prendre en charge les fonctions d'enregistrement et de lecture audio et d'écran dans Webex WFO :

Aire	Considération
Navigateur	▪ Inclure un navigateur pris en charge dans les déploiements de clients légers-serveurs. Les serveurs de clients légers doivent inclure un navigateur pris en charge pour accéder Webex WFO. ▪ Publiez le navigateur localement sur chaque serveur. ▪ Vérifiez que les paramètres de sécurité du navigateur permettent aux utilisateurs finals de lire des enregistrements via le client léger.
Sessions	Limitez le nombre de sessions simultanées par utilisateur à une seule session.
Client bureau intelligent Desktop	▪ Pour les services clients Citrix, vous devez également installer Smart Client sur le serveur client léger, afin d'enregistrer l'activité du bureau de l'utilisateur (Desktop Analytics) et les appels téléphoniques, à l'aide d'un softphone pris en charge. ▪ Le client Smart Desktop se connecte à la plate-forme WFO Webex à l'aide de la connexion unique Domain\Windows de l'utilisateur.

Utilisation des ports

Les exigences de port pour les composants WFO Webex sont répertoriées ci-dessous.

En règle générale, les ports 80 et 443 vers un serveur Web doivent être ouverts pour se connecter à Webex WFO pour toutes les intégrations cloud avec Webex WFO. Les exigences exactes en matière de port varient en fonction de votre modèle de déploiement cloud.

Composants de périphérie :

- Bureau intelligent

Composants du serveur de données :

- Serveur de données : synchronisation ACD : Avaya CM avec Contact Center Elite
- Serveur de données : synchronisation ACD : intégrations CCaaS
- Serveur de données : synchronisation ACD : enregistrement réseau CUCM
- Serveur de données : synchronisation ACD : Cisco Unified Contact Center Enterprise (Unified CCE)
- Serveur de données : ACD Synchronisation : Cisco Unified Contact Center Express (Unified CCX)
- Serveur de données : SIG
- Serveur de données : Enregistrement/Capture
- Serveur de données : Signalisation : CTI
- Serveur de données : signalisation : enregistrement CTI, Avaya Aura Communication Manager
- Serveur de données : signalisation : CTI, Cisco Unified Communications Manager enregistrement réseau
- Serveur de données - Signalisation : SIPREC

Composants Edge

Port	Utiliser	Source	Destination	Remarques
Bureau intelligent				
UDP 49152–65535	Surveillance dynamique audio : RTP Surveillance dynamique de l'écran : flux RDP	PC de l'agent	Navigateur du superviseur	—
TCP 52102	Communication entre les serveurs de données Cisco CTI et la SDC	Bureau intelligent	Serveur de données	

Composants du serveur de données

Port	Util	Source	Destination	Rem
Serveur de données : synchronisation ACD : intégrations CCaaS				
TCP 443	Communication entre les intégrations CCaaS et les paramètres suivants sur le serveur de données : paramètres régionaux de saisie ACD du serveur de données, paramètres du serveur d'enregistrement CTI de signalisation et paramètres régionaux de saisie ACD du serveur de données	—	—	—
Serveur de données : synchronisation ACD : enregistrement réseau CUCM				
TCP 22	Communication entre les paramètres de configuration de l’SFTP et du serveur de données régional sur le serveur de données et le service de facturation CUCM	SFTP, Serveur de données	CUCM Facturation Signification	—

Port	Utiliser	Source	Destination	Remarques
TCP 8443	Communication entre le CUCM AXL et le serveur de données régional Paramètres de synchronisation ACD sur le serveur de données	Serveur de données	CUCM AXL	—
Serveur de données : synchronisation ACD : Cisco Unified CCE				
TCP 1433	Communication entre le serveur Cisco Unified CCE AW SQL	Serveur de données	Cisco Unified	—
TCP 1434	La base de données et le serveur de données régional ACD les paramètres de synchronisation dans le Serveur de données		CCE SQL AWDB Base de données du serveur	
TCP 1433	Communication entre le serveur Cisco Unified CCE HDS SQL	Serveur de données	Cisco Unified	—
TCP 1434	Paramètres de rapprochement de la base de données et du serveur de données régional et le serveur régional de données ACD paramètres de capture des données Serveur		CCE HDS SQL Base de données du serveur	
TCP 42027	Communication entre le service Cisco Unified CCE CTI (côté a) et les paramètres du serveur d'enregistrement CTI de signalisation sur les données Serveur	Serveur de données	Cisco Unified Service CCE CTI (Côté A)	Côté A par défaut si vous utilisez PG1. Les ports varient en fonction du PG que vous utilisez. Le port du serveur d’CTI configuré dans l' Unified CCE ACD configuration.
TCP 43027	Communication entre le service Cisco Unified CCE CTI (côté b) et les paramètres du serveur d'enregistrement CTI de signalisation sur les données Serveur	Serveur de données	Cisco Unified Service CCE CTI (Côté B)	Côté B par défaut si vous utilisez PG1. Les ports varient en fonction du PG que vous utilisez. Le port du serveur d’CTI configuré dans l' Unified CCE ACD configuration.

Serveur de données : synchronisation ACD : Cisco Unified CCX				
TCP 1504	Communication entre la base de données Informix Unified CCX et	Serveur de données	Unified CCX	—

Port	Utiliser	Source	Destination	Remarques
	les paramètres régionaux de synchronisation du serveur de données ACD et les paramètres régionaux Paramètres de capture ACD du serveur de données		Base de données Informix	
TCP 12028	Communication entre le service Cisco Unified CCX CTI (Côté a) et les paramètres du serveur d'enregistrement CTI de signalisation sur les données Serveur	Serveur de données	Cisco Unified Service de CTI CCX (Côté A)	Côté A Par défaut. C'est le CMMR TCP port configuré dans Unified CCX Paramètres système. Serveur CTI Port configuré dans le Unified CCX ACD configuration.
TCP 12028	Communication entre le service Cisco Unified CCX CTI (Côté b) et les paramètres du serveur d'enregistrement CTI de signalisation sur les données Serveur	Serveur de données	Cisco Unified Service de CTI CCX (Côté B)	Côté B Par défaut. C'est le CMMR TCP port configuré dans Unified CCX Paramètres système. Serveur CTI Port configuré dans le Unified CCX ACD configuration.
Serveur de données : SIG				
—	—	—	—	Bien que le SIG n'écoute pas directement sur un port, les fichiers doivent être copiés sur le serveur de données. Si la copie est effectuée Via FTP, les ports 20 et 21 sont utilisés.
Serveur de données : Enregistrement/Capture				
UDP 39500–43500	RTP d'enregistrement	Téléphone ou vocal	Audio Capture	—

		passerelle	(Serveur d'enregistrement)

Port	Utiliser	Source	Destination	Remarques
UPD 49152–65535	Surveillance dynamique audio : RTP	Capture audio (serveur d'enregistrement)	Navigateur du superviseur	—
Serveur de données : Signalisation : CTI				
TCP 443	Serveur de signalisation	Serveur de signalisation	Cisco API	—
TCP 52102	Signalisation d'enregistrement	Clients de capture audio (serveurs d'enregistrement) ou de bureau intelligent	Serveur de signalisation	—
TCP 52103	Noisetier	Partenaire Serveur de signalisation	Serveur de signalisation	—
Serveur de données : signalisation : CTI, Cisco Unified Communications Manager enregistrement réseau				
TCP 2748	JTAPI de signalisation	Serveur de signalisation	Unifié CM éditeurs et abonnés	—
TCP 5060 UDP 5060	Signalisation SIP depuis Unified CM	Tout éditeur ou abonné Unified CM	Serveur de signalisation	Non sécurisé
TCP 5060	Serveur de signalisation	serveur de signalisation principal	serveur de signalisation secondaire	Bidirectionnel

Port	Utiliser	Source	Destination	Remarques
TCP 5061	Signalisation SIP sécurisée provenant de Unified CM	Tout éditeur ou abonné Unified CM	Serveur de signalisation	Sûr. Utilisé uniquement lorsque le système est configuré pour SRTP.
Serveur de données - Signalisation : SIPREC				
TCP 443	requêtes Cisco API	Serveur de signalisation	Cisco API	—
TCP 5060 UDP 5060	Signalisation SIP à partir de la passerelle	Passerelle	Serveur de signalisation	—
TCP 59106	Signalisation d'enregistrement	Capture audio (serveurs d'enregistrement)	Serveur de signalisation	—
TCP 59107	Noisetier	Partenaire Serveur de signalisation	Serveur de signalisation	—

Chiffrement des fichiers

Les médias et les données sont cryptés pour des raisons de sécurité. Webex WFO utilise une clé pour déchiffrer les conversations client enregistrées. La clé de chiffrement se trouve dans la base de données. Chaque locataire possède sa propre clé de chiffrement. Les clés de chiffrement peuvent être mises à jour.

Politique de mot de passe

Exigences relatives à la complexité des mots de passe

Les exigences de complexité des mots de passe sont basées sur la politique de mot de passe de Microsoft : https://technet.microsoft.com/en-us/library/hh994562.aspx.

Les règles suivantes s'appliquent lorsque vous créez ou modifiez un utilisateur, ou lorsque vous modifiez ou réinitialisez un mot de passe.

- Les mots de passe ne doivent pas contenir d'espaces blancs (blancs).
- Les mots de passe doivent comporter au moins huit caractères. La longueur minimale peut être configurée par un administrateur.
- Les mots de passe doivent contenir des caractères de trois des quatre catégories suivantes :

Catégorie	Description
Lettres majuscules	A à Z Caractères unicode majuscules : http://www.fileformat.info/info/unicode/category/Lu/list.htm
Lettres minuscules	A à Z Caractères unicode en minuscules : http://www.fileformat.info/info/unicode/category/Lu/list.htm
Chiffres	0–9
Caractères spéciaux	Les caractères suivants sont autorisés pour un mot de passe de base de données cliente : ! # $ % et ( ), . / : ; = ? @ ^ ` | Les caractères suivants sont autorisés pour tous les autres mots de passe : ! " # $ % et ' ( ) * +, - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

Ces règles s'appliquent uniquement lorsque vous configurez un mot de passe contrôlé par Webex WFO. Si un utilisateur saisit un mot de passe pour un système externe qui n'est pas contrôlé par Webex WFO, Webex WFO ne validera pas le mot de passe (par exemple, ACD configuration).

REMARQUE Un utilisateur peut être créé sans mot de passe (manuellement ou automatiquement via ACD synchronisation). Un utilisateur sans mot de passe ne peut pas se connecter. Cet utilisateur doit utiliser le lien "Mot de passe oublié" et configurer
Mot de passe.

Authentification

Par défaut, l'authentification des utilisateurs et les mots de passe sont gérés à l'aide de Webex WFO. Dans les systèmes qui se synchronisent avec un ACD, les utilisateurs sont créés et gérés dans le ACD, mais vous pouvez toujours créer des utilisateurs dans Webex WFO.

Vous pouvez choisir d'utiliser l'authentification SAML (Security Assertion Markup Language). SAML permet d'utiliser un fournisseur d'identité externe (IdP) pour authentifier les noms d'utilisateur et les mots de passe. Cette méthode d'authentification des utilisateurs et de gestion des mots de passe est communément appelée "authentification unique".

Méthodes de capture de plate-forme

Cette rubrique explique comment configurer Webex WFO avec différentes plates-formes de centre de contact.

Méthodes de capture prises en charge par plate-forme

Le tableau suivant décrit la manière dont les plates-formes de centres d'appels prennent en charge la capture d'enregistrements.

NOTE

Webex WFO prend uniquement en charge les SRTP avec les méthodes de capture suivantes :

- Paquet ACME
- Cisco Unified CM

Plate-forme	Méthode de capture	Signalisation	Description de la signalisation
Cisco	Enregistrement réseau de pont intégré	JTAPI	S'enregistre auprès du gestionnaire d'appels pour les événements JTAPI
Cisco	Enregistrement de poste de travail	JTAPI	S'enregistre auprès du gestionnaire d'appels pour les événements JTAPI
Cisco	Passerelle (Cisco Unified Border Element—CUBE)	SIPREC	Registres auprès de CUBE pour la signalisation SIPREC
Cisco	Client bureau intelligent	IP Communicator (SIP/SCCP)	SCCP messages sur le bureau

Plate-forme	Méthode de capture	Signalisation	Description de la signalisation
Cisco	Client bureau intelligent	Jabber (SIP/SCCP)	Renifle les messages SIP/SCCP du bureau
Cisco	Client bureau intelligent	Téléphone dur Cisco IP (SIP/SCCP)	Renifle les messages SIP/SCCP du bureau
Cisco Webex Contact Center (CCFC)	Importation automatisée	Analyseur CWCC API	Interrogez l'analyseur CWCC pour le traitement CDR et post-appel post-appel
ACME	Passerelle (paquets ACME)	SIPREC	Registres avec ACME pour la signalisation SIPREC
SONUS	Passerelle (SONUS)	SIPREC	Enregistrements auprès de SONUS pour la signalisation SIPREC

Méthodes Cisco de capture vocale

Le tableau suivant fournit des informations sur l'intégration des types de capture et de signalisation pris en charge et testés par Cisco :

Méthode de capture	Signalisation	Description	Support Ruisseau	Bureau intelligent Capture d'écran	Audio en direct Surveiller
Réseau Enregistrement—Pont intégré (BISB)	JTAPI	S'inscrit auprès de CUCM/JTAPI Épreuves	BISS—Médias Diffusé depuis Téléphone	Oui (Smart Client du bureau Nécessite CTI Connexion)	Oui (Smart Bureau Client) via WebRTC
Bureau intelligent Client – IP Communicateur	SIP/SCCP	Contrôler le protocole SIP/SCCP messages désactivés Téléphone de bureau/Softphone (Téléphone logiciel)	Flux multimédia Capturé directement sur bureau	Oui (Smart Client de bureau)	Oui (Smart Bureau Client) via WebRTC
Bureau intelligent Client – Jabber	SIP/SCCP	Surveillance SIP/SCCP Messages désactivés Bureau	Flux multimédia Capturé directement sur	Oui (Smart Client de bureau)	Oui (Smart Bureau Client) via

Méthode de capture	Signalisation	Description	Support Ruisseau	Bureau intelligent Capture d'écran	Audio en direct Surveiller
			bureau		WebRTC
Bureau intelligent Client – Cisco IP Téléphone (Daisy Enchaîné)	SIP/SCCP	Surveillance SIP/SCCP Messages désactivés Bureau	Flux multimédia Capturé directement sur bureau	Oui (Smart Client de bureau)	Oui (Smart Bureau Client) via WebRTC
Passerelle (CUBE)	SIPREC	S'inscrit auprès de CUBE pour SIPREC Signalisation	SIPREC – Forking de médias de Cisco CUBE	Oui (Smart Client de bureau)	Non
Bulk Contact Importation	Basé sur l'API	S'inscrit auprès de CUBE pour SIPREC Signalisation	Automatisé importation Clair . WAV et associé contact fichiers de métadonnées en gros	S.O. – Fichiers Chiffré et Importé	Non

Intégrations Five9 Voice Capture héritées

Le tableau suivant fournit des informations sur l'intégration des types de capture et de signalisation pris en charge et testés par Five9. Il fait spécifiquement référence à l'ancienne intégration Five9, et non à Five9 ARU ou Five9 VCC avec VoiceStream.

Capture Type	Signalisation	Description	Flux multimédia	Écran de bureau actif Capturer	Audio en direct Surveiller

| **Méthodes de capture de**

Client bureau intelligent	Kafka CTI	Webex plate-forme WFO s'inscrit auprès de Five9 Kafka Events API	Flux multimédia capturé directement sur	Oui (client Bureau intelligent)	Oui (client Smart Desktop) via WebRTC

Capture Type	Signalisation	Description	Flux multimédia	Écran de bureau actif Capturer	Audio en direct Surveiller
			bureau – Publier appel CDR et Réconciliation traitement caviardage et Insère des événements basé sur Kafka événements d'appel		
Bureau intelligent Client	Five9 Agent Bureau Plus (ADP) - Kafka CTI	Contrôler le protocole SIP/SCCP messages désactivés Téléphone de bureau/Softphone (Téléphone logiciel)	Flux multimédia Capturé directement sur bureau – Publier appel CDR et Réconciliation traitement caviardage et Insère des événements basé sur Kafka événements d'appel	Oui (Smart Bureau Client)	Oui (Smart Bureau Client) via WebRTC
Bureau intelligent Client	Five9 Agent Bureau Toolkit (ADT) - Kafka CTI	Surveillance SIP/SCCP Messages désactivés Bureau	Flux multimédia Capturé directement sur bureau – Publier appel CDR et Réconciliation traitement caviardage et Insère des événements basé sur Kafka	Oui (Smart Bureau Client)	Oui (Smart Bureau Client) via WebRTC

événements
d'appel

Capture Type	Signalisation	Description	Flux multimédia	Écran de bureau actif Capturer	Audio en direct Surveiller
Bureau intelligent Client	Cinq9 Java Agent Bureau-Kafka CTI	Surveillance SIP/SCCP Messages désactivés Bureau	Flux multimédia Capturé directement sur bureau – Publier appel CDR et Réconciliation traitement caviardage et Insère des événements basé sur Kafka événements d'appel	Oui (Smart Bureau Client)	Oui (Smart Bureau Client) via WebRTC
Bureau intelligent Client	Cinq9 VCC Importation	Five9/Webex WFO Intégration du cloud à Importer Five9 VCC enregistrements audio dans Webex Cloud WFO	S.O. – Importation Seulement	Oui (Smart Bureau Client)	Non

Enregistrement Sonus Gateway

Cisco prend en charge la résilience pour l'enregistrement de passerelle Sonus.

Vous devez ajouter des règles Sonus SIP Message Manipulation (SMM) aux en-têtes SIP et SIPREC INVITE dans Cisco-Guid pour Sonus SBC pour utiliser QM. Cela QM permet de rapprocher les appels avec les enregistrements CDR de Cisco Unified CM. Les règles feront ce qui suit :

- Pour les appels entrants dans le SBC sans en-tête "Cisco-Guid", le SMM crée un Guid Cisco en utilisant les 4 tuples hexadécimaux de l'ID d'appel sortant. Chaque tuple sera converti en un nombre décimal rembourré à 10 chiffres à 0 qui sera séparé par des tirets du Cisco-Guid.
- Pour les appels qui contiennent déjà un en-tête Cisco-Guid, celui-ci reste tel quel.

> **REMARQUE :** Le Cisco_Guid ne sera PAS remplacé par un nouveau guide Cisco créé par un ID d'appel.

- L'invite SIPREC vers l'enregistreur contient un en-tête Cisco-Guid correspondant au Cisco Guid ci-dessus.

Les règles doivent être associées au tronc enregistré et au tronc Unified CM utilisé par votre Unified CM. Vous n'avez besoin de créer ces règles qu'une seule fois. Si vous créez des zones et des faisceaux, vous pouvez les réutiliser.

Pour configurer les contrôleurs Sonus Session Border Controllers pour une utilisation avec QM :

1. À partir de l'interface de ligne de commande (CLI) de Sonus, créez et activez les règles SMM
    a. Créez et activez les règles SMM entrantes Unified CM. Voir Exemple de règles SMM entrantes pour Unified CM pour plus d'informations.
    b. Ajoutez les Unified CM règles SMM sortantes. Voir Exemple de règles SMM sortantes pour Unified CM pour plus d'informations.
    c. Ajoutez les règles SMM sortantes de l'enregistreur. Voir Exemple de règles SMM sortantes pour l'enregistreur pour plus d'informations .
2. Utilisez la Sonus CLI pour activer SIPREC pour le port SIp Sig dans la zone qui contient votre Unified CM principale.
3. Utilisez Sonus CLI ou Navigator pour créer un groupe de faisceaux SIP pour le serveur Sonus SIPREC de QM. Attribuez le préfixe de IP d'entrée à l'adresse IP de l'ordinateur QM qui exécute le service SIPREC Sonus de surveillance.
4. Utilisez la CLI/Navigation Sonus pour affecter des règles SMM à vos agrégations comme suit :
    a. Affectez UCM_INBOUND profil d'entrée de l'adaptateur SMM à la manipulation des messages de signalisation de votre ligne principale Unified CM.
    b. Affectez UCM_OUTBOUND SMM au profil de sortie de l'adaptateur de manipulation des messages de signalisation de votre ligne principale Unified CM.
    c. Attribuez RECORDER_OUTBOUND SMM au profil de sortie de l'adaptateur Signaling Message Manipulation pour la ligne principale Sonus SIPREC de QM.
5. Utilisez le Sonus PSX pour créer un groupe de IP homologues de signalisation pour le serveur Sonus SIPREC du QM. Attribuez le préfixe de IP d'entrée à l'adresse IP de l'ordinateur QM qui exécute le service SIPREC Sonus de surveillance.
6. Utilisez le Sonus PSX pour créer un groupe de faisceaux pour le serveur Sonus SIPREC du QM. Utilisez exactement le même nom que celui que vous avez utilisé à l'étape 3.

7. Utilisez Sonus PSX pour créer un profil d'enregistreur pour votre serveur SIPREC QM Sonus. Attribuez l'adresse IP4 à la machine QM qui exécute le "Monitoring and Recording Sonus SIPREC Service", définissez le numéro de port sur 5060.
8. Utilisez Sonus PSX pour créer des critères d'enregistrement d'appels.

Exemple de règles SSM entrantes pour Unified CM

configurer

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 1 applyMatchHeader all

définir des profils signalant sipAdaptorProfile UCM_INBOUND message de type critère 1 de règle 1

set profiles signaling sipAdaptorProfile UCM_INBOUND règle 1 critère 1 message messageTypes all

définir des profils signalant sipAdaptorProfile UCM_INBOUND l'en-tête de type du critère 2 de la règle 1

définir des profils signalant sipAdaptorProfile UCM_INBOUND Règle 1 critère 2 nom d'en-tête Cisco-Guid

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 1 critère 2 condition d'en-tête existent

définir des profils signalant sipAdaptorProfile UCM_INBOUND en-tête de type d'action 1 de règle 1

définir des profils signalant sipAdaptorProfile UCM_INBOUND Règle 1 Action 1 magasin d'opérations

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 1 action 1 headerInfo, champValeur

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 1 action 1 à partir de l'en-tête Type

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 1 action 1 de la valeur Cisco-Guid

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 1 action 1 à la variable de type

définir les profils signalant sipAdaptorProfile UCM_INBOUND règle 1 action 1 sur variableValue var1

définir des profils signalant sipAdaptorProfile UCM_INBOUND règle 2 applyMatchHeader one

définir des profils signalant sipAdaptorProfile UCM_INBOUND type de critère 1 de règle 2

message

set profiles signaling sipAdaptorProfile message UCM_INBOUND règle 2 critère 1
messageTypes request

set profiles signaling sipAdaptorProfile message UCM_INBOUND règle 2 critère 1
methodTypes invite

définir des profils signalant que la condition de UCM_INBOUND règle 2 critère 1
message sipAdaptorProfile existe

définir des profils signalant l'en-tête sipAdaptorProfile UCM_INBOUND règle 2 critère 2 type

définir des profils signalant le nom de l'en-tête
sipAdaptorProfile From UCM_INBOUND règle 2 critère 2

définir des profils signalant que la condition d'en-tête
sipAdaptorProfile existe UCM_INBOUND règle 2 critère 2

set profiles signalisation de la variable
sipAdaptorProfile UCM_INBOUND règle 2 critère 3 type

définir des profils signalant que la condition de
variable sipAdaptorProfile existe UCM_INBOUND règle 2 critère 3

set profiles signalisation sipAdaptorProfile variable
variableID var1 UCM_INBOUND règle 2 critère 3

définir des profils, sipAdaptorProfile UCM_INBOUND règle 2 action 1 type
paramètre de signalisation

Définition des profils sipAdaptorProfile UCM_INBOUND règle 2 action 1
Opération de signalisation

Ajouter sipAdaptorProfile UCM_INBOUND règle 2 action 1

définir des profils
signalisation, paramType sipAdaptorProfile UCM_INBOUND règle 2 action 1 De
générique

définition des profils sipAdaptorProfile UCM_INBOUND règle 2 action 1 De
variable de type de
signalisation sipAdaptorProfile UCM_INBOUND règle 2 action 1 pour taper

définir des profils variable
de signalisationValeur var1 sipAdaptorProfile UCM_INBOUND règle 2 action 1 à la valeur

définir des profils,
paramètre de signalisation

Définir des profils signalant
Cisco-GUID

commettre

set profiles signaling sipAdaptorProfile UCM_INBOUND state enabled commit

Exemple de règles SMM sortantes pour Unified CM

configurer

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND message de type critère 1 de règle 1

définir des profils signalement sipAdaptorProfile UCM_OUTBOUND Règle 1 critère 1 message messageTypes request

définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 1 critère 1 méthode de messageTypes invite

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND l'en-tête de type du critère 2 de la règle 1

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND Règle 1 critère 2 Nom d'en-tête Cisco-GUID

définir des profils signalisation, sipAdaptorProfile UCM_OUTBOUND Règle 1 : condition d'en-tête 2 absente

définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 1 action 1 variable de type

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND Règle 1 Action 1 Magasin d'opérations

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 1 action 1 à partir de la valeur de type

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 1 action 1 de la valeur cisco-guid

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 1 action 1 à la variable de type

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 1 action 1 à variableValue var1

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND message de type critère 1 de règle 2

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 critère 1 message messageTypes demande

définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 critère 1 méthode de messageTypes invitent

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND Règle 2 Variable de type critère 2

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 critère 2 condition variable existent

définir des profils signalant sipAdaptorProfile UCM_OUTBOUND critère 2 de la règle 2

variable variableID var1
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND l'en-tête de type du critère 3 de la règle 2
définir des profils signalisation, sipAdaptorProfile UCM_OUTBOUND Règle 2 Critère 3 Nom de l'en-tête ID_appel
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND la condition d'en-tête du critère 3 de la règle 2 existe
set profiles signaling sipAdaptorProfile UCM_OUTBOUND Rule 2 action 1 type header
définir des profils signalisation, magasin d'opérations sipAdaptorProfile UCM_OUTBOUND règle 2 action 1
définir des profils signalement sipAdaptorProfile UCM_OUTBOUND règle 2 action 1 headerInfo, champValeur
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 1 à partir de l'en-tête Type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 1 de la valeur id_appel
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 1 à la variable de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 1 à variableValue var2
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 2 variable de type
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 2 opération regdel
définir les profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 2 à la variable de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 2 à variableValue var2
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 2 regexp string @.*
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 2 regexp matchInstance un
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 3 variable de type
Définir des profils signalant sipAdaptorProfile UCM_OUTBOUND Règle 2 Action 3 Magasin d'opérations
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 3 à partir de

type, variable
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 3 from variableValue var2
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 3 à la variable de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 3 à variableValue var3
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND la variable de type d'action 4 de règle 2
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 4 opération regdel
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 4 à type variable
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 4 à variableValue var2
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 4 regexp string _.*
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 4 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 5 variable de type
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 5 opération regdel
définir les profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 5 à la variable de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 5 à variableValue var3
définir les profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 5 regexp chaîne .*_
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 5 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 variable de type
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 opération regappend
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 à partir de la valeur de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 à partir de

valeur 000000000
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 à la variable de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 à variableValue var2
définir les profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 regexp string ^
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 6 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 type variable
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 opération regappend
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 à partir de la valeur de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 from value 000000000
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 à la variable de type
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 à variableValue var3
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 regexp string ^
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 7 regexp matchInstance one
définir des profils signalant sipAdaptorProfile UCM_OUTBOUND Règle 2 action 8 variable de type
définir des profils signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 8 opération regpredel
définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 8 pour taper la variable
définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 8 sur variableValue var2
définir les profils de signalisation sipAdaptorProfile règle UCM_OUTBOUND 2 action 8 chaîne d'expression régulière $
définir les profils de signalisation sipAdaptorProfile règle UCM_OUTBOUND 2 action 8 regexp matchInstance one
définir les profils de signalisation sipAdaptorProfile UCM_OUTBOUND règle 2 action 9 type

variable
définir les profils de signalisation sipAdaptorProfile règle UCM_OUTBOUND 2 action 9
opération regpredel
définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 9 pour taper la variable
définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 9 sur variableValue var3
définir les profils de signalisation sipAdaptorProfile règle UCM_OUTBOUND 2 action 9 chaîne d'expression régulière $
définir les profils de signalisation sipAdaptorProfile règle UCM_OUTBOUND 2 action 9 regexp matchInstance one
définir des profils de signalisation variables profil d'adaptateur sip UCM_OUTBOUND règle 2 action 10 type
définir les profils opération de signalisation append profil d'adaptateur sip UCM_OUTBOUND règle 2 action 10
définir le type de signalisation des profils profil d'adaptateur sip UCM_OUTBOUND règle 2 action 10 depuis
valeur profil d'adaptateur sip UCM_OUTBOUND règle 2 action 10 depuis
définir des profils de valeur de signalisation - profil d'adaptateur sip UCM_OUTBOUND règle 2 action 10 à
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 10 à
définir les profils de signalisation variableValue profil d'adaptateur sip UCM_OUTBOUND règle 2 action 11 type
var2
définir des profils de signalisation variables profil d'adaptateur sip UCM_OUTBOUND règle 2 action 11
définir les profils opération de signalisation append profil d'adaptateur sip UCM_OUTBOUND règle 2 action 11 depuis
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 11 depuis
définir les profils de signalisation variableValue profil d'adaptateur sip UCM_OUTBOUND règle 2 action 11 à
var3 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 11 à
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 12 type
définir les profils de signalisation variableValue profil d'adaptateur sip UCM_OUTBOUND règle 2 action 12
var2
définir des profils de

définir des profils de signalisation

magasin d'exploitation
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 12 depuis
définir les profils de signalisation variableValue var2 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 12 depuis
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 12 à
définir les profils de signalisation variableValue var3 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 12 à
définir des profils de signalisation variables profil d'adaptateur sip UCM_OUTBOUND règle 2 action 13 type
définir les profils opération de signalisation append profil d'adaptateur sip UCM_OUTBOUND règle 2 action 13
définir le type de signalisation des profils valeur profil d'adaptateur sip UCM_OUTBOUND règle 2 action 13 depuis
définir des profils de valeur de signalisation - profil d'adaptateur sip UCM_OUTBOUND règle 2 action 13 depuis
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 13 à
définir les profils de signalisation variableValue var2 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 13 à
définir des profils de signalisation variables profil d'adaptateur sip UCM_OUTBOUND règle 2 action 14 type
définir les profils opération de signalisation append profil d'adaptateur sip UCM_OUTBOUND règle 2 action 14
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 14 depuis
définir les profils de signalisation variableValue var3 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 14 depuis
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 14 à
définir les profils de signalisation variableValue var2 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 14 à
définir l'en-tête de profil d'adaptateur sip UCM_OUTBOUND règle 2 action 15 type
définir des profils de type de signalisation variable profil d'adaptateur sip UCM_OUTBOUND règle 2 action 15
définir les profils de signalisation variableValue var2 profil d'adaptateur sip UCM_OUTBOUND règle 2 action 15

signalisation des profils

définir des profils opération

de signalisation ajouter

définir des profils de signalisation

headerPosition dernier

définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 15 à partir d'une variable de type

définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 15 à partir de la variableValue var2

définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 15 pour taper l'en-tête

définir les profils signalant la règle sipAdaptorProfile UCM_OUTBOUND 2 action 15 valoriser Cisco-Guid

commettre

définir les profils de signalisation sipAdaptorProfile UCM_OUTBOUND état activé commit

Exemple de règles SMM sortantes pour l'enregistreur

configurer

ensemble profils de signalisation sipAdaptorProfile ENREGISTREUR_SORTANT règle 1 applyMatchHeader tous

ensemble profils signalant sipAdaptorProfile taper ENREGISTREUR_SORTANT règle 1 critère 1 message

ensemble profils signalisation sipAdaptorProfile ENREGISTREUR_SORTANT règle 1 critère 1 message messageTypes tous

ensemble profils signalant sipAdaptorProfile taper ENREGISTREUR_SORTANT règle 1 critère 2 Corps du message

ensemble profils signalant sipAdaptorProfile ENREGISTREUR_SORTANT règle 1 critère 2 messageBody condition regex-match

ensemble profils signalisation sipAdaptorProfile ENREGISTREUR_SORTANT règle 1 critère 2 messageBody regexp chaîne cisco-guid=.*

ensemble profils signalisation sipAdaptorProfile ENREGISTREUR_SORTANT règle 1 critère 2 messageBody regexp numMatch match

ensemble profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 1 taper Corps du message

ensemble profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 1 opération regstore

ensemble profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 1 de taper Corps du message

ensemble profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 1

de messageBodyValue tout
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 1 action 1 sur la variable de type
définir les profils signalant la règle 1 de l'action 1 de sipAdaptorProfile RECORDER_OUTBOUND sur variableValue var1
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 1 chaîne d'expression régulière "cisco-guid=.*?(?=;tag)"
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 1 regexp matchInstance dernière
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 2 type variable
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 2 opération regdel
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 2 de type variable
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 2 à partir de variableValue var1
définir les profils signalant la règle 1 action 2 de sipAdaptorProfile RECORDER_OUTBOUND sur une variable de type
définir les profils signalant la règle 1 action 2 de sipAdaptorProfile RECORDER_OUTBOUND sur variableValue var1
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 2 regexp chaîne cisco-guid=
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 4 type en-tête
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 4 opération ajouter
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 4 headerPosition dernier
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 4 de type variable
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 1 action 4 à partir de variableValue var1
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 1 action 4 sur le type d'en-tête
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 1 action 4 sur la valeur Cisco-Guid
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 2 critère 1

type message

définir profils signalisation sipAdaptorProfile ENREGISTREUR_SORTANT règle 2 critère 1 message messageTypes demande

définir profils signalisation sipAdaptorProfile ENREGISTREUR_SORTANT règle 2 critère 1 message methodTypes invite

définir profils de signalisation sipAdaptorProfile type ENREGISTREUR_SORTANT règle 2 critère 2 en-tête

définir profils signalisation sipAdaptorProfile nom ENREGISTREUR_SORTANT règle 2 critère 2 d'en-tête cisco-guid

set profiles signalant l'absence de condition d'en-tête ENREGISTREUR_S règle 2 critère 2 sipAdaptorProfile

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 2 action 1 type variable

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 2 action 1 opération stocker

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 2 action 1 de type valeur

définir les profils de signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 2 action 1 à partir de la valeur cisco-guid

définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 2 action 1 sur la variable de type

définir les profils signalant la règle 2 de l'action 1 de sipAdaptorProfile RECORDER_OUTBOUND sur variableValue var1

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 applyMatchHeader tous

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 critère 1 type message

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 critère 1 message messageTypes tous

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 critère 2 type messageBody

définir des profils de signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 critère 2 messageBody condition regex-match

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 critère 2 messageBody regexp chaîne cisco-guid=.*

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 critère 2 messageBody regexp numMatch correspondance

définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 action 1

type variable
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 action 1 opération stocker
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 3 action 1 de type valeur
définir profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 3 action 1 à partir de la valeur cisco-guid
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 3 action 1 sur la variable de type
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 3 action 1 sur variableValue var10
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 critère 1 type variable
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 critère 1 variable condition absente
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 critère 1 variable variableID var10
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 1 type messageBody
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 1 opération regstore
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 1 de type messageBody
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 1 de messageBodyValue tout
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 4 action 1 sur la variable de type
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 4 action 1 sur variableValue var2
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 1 expression régulière chaîne <callid>.*</callid>
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 1 regexp matchInstance un
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 2 type variable
définir profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 2 opération regdel
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 4 action 2 sur

type variable
définir les profils signalant la règle sipAdaptorProfile RECORDER_OUTBOUND 4 action 2 sur variableValue var2
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND Rule 4 action 2 regexp string <callid>
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 2 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 3 variable de type
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 3 opération regdel
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 3 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 3 à variableValue var2
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 3 regexp string @.*
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 3 regexp matchInstance un
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 4 variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND Règle 4 Action 4 Magasin d'opérations
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 4 à partir de la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 4 de variableValue var2
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 4 à type variable
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 4 à variableValue var3
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 5 de règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 5 opération regdel
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 5 à type variable
définissez les profils signalant sipAdaptorProfile RECORDER_OUTBOUND l'action 5 de la règle 4 sur

variableValue var2
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 5 regexp string _.*
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 5 regexp matchInstance one
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 6 de la règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 6 opération regdel
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 6 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 6 à variableValue var3
définir les profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 6 regexp chaîne .*_
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 6 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 7 de règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 opération regappend
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 à partir de la valeur de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 à partir de la valeur 000000000
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 à variableValue var2
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 regexp string ^
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 7 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8 variable de type
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8 opération regappend
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8

à partir de la valeur de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8 à partir de la valeur 000000000
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND la règle 4 action 8 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8 à variableValue var3
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8 regexp string ^
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 8 regexp matchInstance one
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 9 de règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 9 opération regpredel
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 9 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 9 à variableValue var2
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 9 chaîne regexp .....$
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 9 regexp matchInstance un
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 10 variable de type
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 10 opération regpredel
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 10 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 10 à variableValue var3
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 10 regexp chaîne .....$
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 10 regexp matchInstance un
définir des profils signalement sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 11 de la règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 11

Opération Ajouter
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 11 à partir de la valeur de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 11 à partir de la valeur -
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 11 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 11 à variableValue var2
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 12 de la règle 4
définir des profils signalement sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 12 opération ajouter
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 12 à partir de la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 12 from variableValue var3
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND la règle 4 action 12 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 12 à variableValue var2
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 13 variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND Règle 4 Action 13 Magasin d'opérations
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 13 à partir de la variable de type
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 13 from variableValue var2
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 13 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 13 à variableValue var3
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND Règle 4 action 14 variable de type
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 14 opération ajouter
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 14

à partir de la valeur de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 14 à partir de la valeur -
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 14 à la variable de type
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 14 à variableValue var2
définir des profils signalement sipAdaptorProfile RECORDER_OUTBOUND la variable de type d'action 15 de la règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 15 opération ajouter
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 15 à partir de la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 15 from variableValue var3
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 15 à la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 15 à variableValue var2
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND l'en-tête du type d'action 16 de règle 4
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 16 opération ajouter
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 16 en-têtePosition en dernier
définir des profils signalisation sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 16 à partir de la variable de type
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 16 from variableValue var2
définir les profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 16 pour taper l'en-tête
définir des profils signalant sipAdaptorProfile RECORDER_OUTBOUND règle 4 action 16 à la valeur Cisco-Guid
commettre
set profiles signaling sipAdaptorProfile RECORDER_OUTBOUND state enabled commit

Installation

Cette section décrit comment installer les différents composants de Webex WFO.

Installation du serveur de données

Un administrateur de locataire peut installer le serveur de données pour un locataire unique, ou un administrateur système peut installer un serveur de données de base et le configurer en tant que serveur de données partagées pour plusieurs locataires. Après avoir installé le serveur de données WFO Webex, vous pouvez le configurer davantage sur la page Configuration du serveur de données dans Gestion des applications > configuration du système > global > configuration du serveur de données.

> **MEILLEURES PRATIQUES** Les utilisateurs disposant d'appareils de périphérie doivent établir un calendrier régulier pour le téléchargement et la mise à niveau de leurs serveurs de données WFO Webex vers Webex la dernière version du logiciel WFO. En règle générale, chaque Cloud
> Comprend une nouvelle version du logiciel Webex WFO Data Server que les utilisateurs peuvent télécharger à partir de leur locataire.

Si votre organisation dispose de l'une des intégrations suivantes, consultez le guide d'intégration de cette ACD pour connaître d'autres configurations de serveur de données spécifiques au ACD.

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

Conditions préalablement requises

Si un serveur de données doit se connecter via un proxy Web, chaque service de serveur de données doit être configuré pour utiliser un compte de service. Cela affecte les services Windows suivants :

- Webex service de signalisation CTI WFO
- Webex serveur de données WFO
- Webex service d'enregistrement réseau WFO
- Webex Service WFO SIPREC
- Webex des services Web du serveur de

données WFO Pour connaître les conditions

d'utilisation des ports, reportez-vous à :

Utilisation des ports.

Installer le serveur de données pour un service partagé unique

Un administrateur de service partagé peut installer le serveur de données pour un seul service partagé.

Installer le serveur de données pour un service partagé unique

1. À partir du serveur sur lequel vous souhaitez installer le serveur de données, ouvrez un navigateur et connectez-vous à Webex WFO à l'aide des informations d'identification de l'administrateur du locataire.
2. Dans la **page Téléchargements** (Gestion des applications > administration > téléchargements), cliquez sur le lien approprié pour télécharger le programme d'installation du serveur de données.
3. Suivez les invites.

Tester le serveur de données

1. Connectez-vous à Webex WFO en tant qu'administrateur de locataire.
2. Sur la page Surveillance **de l'agent** (Gestion des applications > surveillance > surveillance de l'agent), sélectionnez le serveur de données dans la section Journaux du serveur de données, puis cliquez sur **Récupérer les journaux**. Si la demande de journal réussit, le serveur de données est connecté.

   Remarque : Cette opération peut prendre quelques minutes.

Installer le serveur de données pour plusieurs services partagés

Un administrateur système peut configurer un serveur de données pour qu'il soit partagé par plusieurs locataires. Chaque fois qu'un serveur de données partagées est mis à jour (par exemple, lorsqu'un nouveau service partagé y est ajouté), vous devez mettre à jour sa configuration. Cela se fait par le fichier Data Server Updater qui est généré lorsque vous enregistrez vos modifications et choisissez de télécharger la configuration.

Pour configurer un serveur de données pour plusieurs locataires, un administrateur système doit installer un serveur de données de base, puis configurer le serveur de données de base en tant que serveur de données partagées. Les administrateurs système peuvent télécharger un serveur de données de base sur la page Gestion des applications > téléchargements ou Gestion des applications > serveur de données partagées.

Installer le serveur de données de base

La première chose à faire est de télécharger et d'installer le serveur de données de base. Ce serveur de données de base devient un serveur de données partagées lorsqu'il est configuré. Vous pouvez installer plusieurs serveurs de données de base.

1. Dans la section Serveur **de** données de base de téléchargement, cliquez sur **Serveur** de données Calabrio ONE. Le fichier CalabrioONEDataServerSetup.exe est téléchargé sur votre ordinateur.
2. Double-cliquez sur le fichier exécutable pour démarrer l'Assistant Installation du serveur de données.
3. Suivez les instructions de l'assistant pour terminer l'installation.

Configurer le serveur de données de base

Ensuite, configurez le serveur de données de base pour qu'il devienne un serveur de données partagées.

1. Sélectionnez **Ajouter une nouvelle configuration au serveur** de données.

   > **REMARQUE** Pour modifier une configuration existante, sélectionnez **Modifier une configuration** de serveur de données existante et sélectionnez le serveur de données que vous souhaitez modifier.

2. Remplissez les champs comme défini dans le tableau suivant.

Champ	Description
Nom du serveur	Saisissez un nom pour le serveur de données.
Serveur Calabrio ONE	Saisissez l'adresse IP ou le nom d'hôte du serveur Webex WFO qui Héberge le service Data Server.
Port	Entrez le numéro de port du serveur qui héberge le service Data Server. Le port par défaut est le port 443.
Disponible	Liste des services partagés disponibles.
Assigné	Liste des services partagés affectés à ce service de serveur de données.

3. Cliquez sur **Enregistrer/Télécharger la configuration** pour enregistrer la configuration et télécharger l'utilitaire de configuration (CalabrioONEDataServerUpdaterSetup.exe) sur votre ordinateur.

   > **REMARQUE** Vous pouvez également cliquer sur **Enregistrer** pour enregistrer la configuration sans télécharger l'utilitaire de configuration. Vous pouvez choisir de le faire si vous n'avez pas fini de configurer le serveur de données mais souhaitez enregistrer la configuration incomplète.

4. Double-cliquez sur l'exécutable de l'utilitaire de configuration pour lancer l'Assistant Installation du programme de mise à jour du serveur de données.
5. Suivez les instructions de l'Assistant pour terminer la configuration du serveur de données partagées.

Utilisateurs de Cisco Unified Communications Manager

Si vous utilisez Cisco Unified Call Manager (UCM) pour collecter des CDR via SFTP, vous devrez peut-être définir la propriété système Service serveur de données pour réconcilier les algorithmes d'échange de clés (kex) entre Webex WFO et les versions prises en charge de Cisco UCM.

Ces algorithmes kex ne nécessitent pas de configuration supplémentaire :

- ecdh-sha2-nistp521
- ecdh-sha2-nistp384
- diffie-hellman-group-exchange-sha256

Ces algorithmes nécessitent une configuration

supplémentaire :

- diffie-hellman-groupe14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha1

Définissez la propriété système Service de serveur de données pour spécifier les algorithmes kex autorisés

1. Sur le serveur CDR SFTP, naviguez jusqu'à
   C:\Program Files\Common Files\Calabrio ONE\Data Serveur\config
2. Ouvrez le fichier dataGatheringService.properties.
3. Recherchez la ligne commençant par **service4j.jvmOptions** et ajoutez le texte suivant à la fin de la ligne : **| -Dsftp.KexAlgorithms=diffie-hellman-group1-sha1,diffie-hellman-group14- sha1,diffie-hellman-group-exchange-sha1**
4. Enregistrez le fichier et redémarrez Webex service de serveur de données WFO.

Remarque Si vous effectuez une mise à niveau vers une version plus récente de Cisco UCM qui ne prend en charge aucun de ces algorithmes kex, vous devez reconfigurer cette propriété système pour spécifier les nouveaux algorithmes pris en charge.

Installation de Smart Desktop

Webex WFO Smart Desktop peut être installé sur l'ordinateur d'un agent de l'une des trois manières suivantes :

- manuellement sur l'ordinateur de chaque agent
- Utilisation de scripts d'objet de stratégie de groupe (GPO)
- Utilisation des paramètres des commandes silencieuses

Remarque : Si vous souhaitez que Smart Desktop capture Desktop Analytics, le rôle d'agent doit disposer de l'autorisation "Capture Desktop Analytics" activée avant d'installer Smart Desktop. Si l'autorisation est

Non activés, les plug-ins de capture ne sont pas installés sur le bureau client.

Considérations supplémentaires

- Vous avez besoin d'un plug-in/extension Desktop Analytics si vous souhaitez utiliser la fonctionnalité Desktop Analytics ou suspendre et reprendre.
- Les extensions de navigateur pour Chrome et Edge doivent être déployées via GPO ou tout autre processus utilisé par le service informatique local. Les extensions de navigateur sont nécessaires pour l'analyse, la pause et la reprise.
- Cisco fournit le fichier exe de base. Il est de la responsabilité du client de convertir le fichier en MSI.
- Si vous effectuez l'installation via SCCM ou Microsoft Endpoint Configuration Manager, vous, le client, êtes responsable de la création du package pour le déploiement.
- Cisco offre la possibilité de mettre à jour le logiciel automatiquement. Si votre équipe d'empaquetage gère des versions de bureau ou Microsoft Endpoint Configuration Manager et qu'ils interfèrent avec les mises à jour automatiques, Cisco peut désactiver la fonctionnalité de mise à jour automatique et votre équipe peut télécharger une nouvelle version du logiciel tous les trois à six mois et la déployer via une diffusion de package.
- Votre équipe peut modifier les requêtes dans le logiciel Microsoft pour ne pas gérer les numéros de version ou les identificateurs uniques si le groupe souhaite gérer les mises à jour automatiques.

  REMARQUE : Les mises à jour automatiques doivent être désactivées si votre organisation utilise des serveurs Citrix ou Terminal Server. Il est impossible de séparer les différents environnements.

- Si vous effectuez une mise à niveau de Webex WFO version 11.5 sur site vers Webex WFO Cloud, vous avez besoin de trois machines de test. Une machine est destinée à une installation manuelle. La deuxième machine est destinée à une installation automatique sur une machine propre. La troisième machine est destinée à la version 11.5 existante de Webex WFO pour tester le package de désinstallation créé par votre équipe informatique et le package d'installation pour Webex WFO Cloud. Fournissez à l'ingénieur d'implémentation une liste de tous les paquets installés sur la machine, y compris les extensions de navigateur. Travaillez avec votre équipe informatique pour supprimer tous les Webex logiciels WFO version 11.5 de WFO avant d'installer Webex WFO Cloud.
    - Si votre organisation change de fournisseur d'une autre solution de gestion de l'engagement de la main-d'œuvre (WEM) (telle que Verint ou Nice) à Webex WFO, travaillez avec votre équipe informatique pour désinstaller le logiciel d'origine sur une troisième machine de test et déployer le package automatisé créé par votre équipe.
- Si vous mettez à niveau une version de 11.5 sur site vers une version plus récente de 11.5, vous devez télécharger à nouveau une nouvelle version de Smart Desktop et la redéployer.

Installation manuelle

Utilisez cette procédure pour installer Smart Desktop manuellement sur l'ordinateur d'un agent ou sur un serveur client léger. Assurez-vous que tous les navigateurs sont fermés avant de procéder à l'installation et utilisez le Gestionnaire des tâches. Assurez-vous que vos navigateurs ne fonctionnent pas en arrière-plan.

Installez Smart Desktop manuellement

1. Depuis l'ordinateur de l'agent ou du serveur client léger, connectez-vous à Webex WFO avec les informations d'identification de l'administrateur.
2. Sur la page Téléchargements (Gestion des applications > administration > globale > téléchargements), cliquez sur le lien du programme d'installation de **Calabrio ONE Smart Desktop** . Webex WFO fournit un fichier .exe pour une installation manuelle.
3. Acceptez le contrat de licence utilisateur final (CLUF) lorsque vous y êtes invité.
4. Exécutez le programme d'installation et suivez les invites de l'assistant d'installation.
5. Cochez la **case Activer** si vous y êtes invité et cliquez sur **Terminer**.
6. Après avoir exécuté le programme d'installation du Bureau intelligent, redémarrez votre système.
7. Exécutez l'outil de vérification client. Voir Outil de vérification client pour plus d'informations.
8. Testez Smart Desktop. Voir Test Smart Desktop pour plus d'informations.

Installation à l'aide d'un objet de stratégie de groupe

Un objet de stratégie de groupe (GPO) est un ensemble de paramètres qui définissent à quoi ressemblera un système et comment il se comportera pour un groupe défini d'utilisateurs. Microsoft fournit un composant logiciel enfichable qui vous permet d'utiliser la stratégie de groupe Microsoft Management Console pour définir diverses options, y compris des options de scripts. Reportez-vous aux codes de retour d'installation de diffusion si nécessaire après avoir poussé le client.

Déployer Smart Desktop à l'aide d'un objet de stratégie de groupe

1. Connectez-vous à Webex WFO avec les informations d'identification de l'administrateur.
2. Sur la page Téléchargements (Gestion des applications > administration > globale > téléchargements), cliquez sur le lien du programme d'installation de **Calabrio ONE Smart Desktop** . Webex WFO fournit un fichier .exe pour une installation manuelle.
3. Acceptez le contrat de licence utilisateur final (CLUF) lorsque vous y êtes invité.
4. Copiez **CalabrioONEDesktopSetup_<TenantName>.exe** à partir de votre dossier Téléchargements et collez-le dans l'emplacement de partage du serveur.

5. Créez un script de traitement par lots pour exécuter le programme d'installation qui contient le script suivant :

   <nom d'hôte ou adresse IP de l'emplacement de partage du serveur>\CalabrioONEDesktopSetup_
   <NomLocataire>.exe /LOG /VERYSILENT /ACTIVATE /NORESTART/NONPCAP

6. Démarrez l'éditeur de gestion des stratégies de groupe et accédez à Stratégies de configuration > ordinateur > paramètres > scripts Windows (démarrage/arrêt) et ajoutez le script de traitement par lots.

Installer Smart Desktop en utilisant les paramètres de commande silencieuse

Les paramètres silencieux permettent d'installer Webex WFO à l'aide de votre interface de ligne de commande. Voir "Configurer les paramètres de ligne de commande" dans https://jrsoftware.org/ishelp/index.php?topic=setupcmdline pour les options. Les commandes couramment utilisées sont les suivantes.

- /RAPPORT
- /VERYSILENT
- /ACTIVER
- /NORESTART
- /NONPCAP

Réplication d'une installation à l'aide de l'imagerie de bureau

Après avoir installé le service Smart Desktop Record sur un PC à l'aide de l'une des méthodes d'installation précédentes (voir Installation manuelle ou Installation à l'aide d'objets de stratégie de groupe), vous pouvez répliquer cette installation sur plusieurs PC en créant une image système générique pouvant être utilisée sur plusieurs conceptions matérielles. Lorsque Smart Desktop est installé sur un PC pour l'imagerie, certaines informations doivent être supprimées qui permettront à l'image de s'exécuter sur différents PC sans causer de problèmes.

Méthode recommandée : Le crochet de préparation du système de Cisco

Pour supprimer les informations spécifiques à un PC d'une installation Windows et les "généraliser" afin qu'elles puissent être installées sur différents PC, nous vous recommandons vivement d'utiliser le crochet de préparation du système (sysprep) de Cisco. Sysprep est l'outil de préparation du système de Microsoft utilisé pour préparer une image système en vue de son déploiement sur plusieurs PC.
Sysprep prépare une installation Windows (client Windows et serveur Windows) pour l'imagerie, ce qui vous permet de capturer une installation personnalisée. Le hook sysprep est installé avec Smart Desktop et s'enregistre automatiquement auprès du système. Lorsque vous exécutez sysprep, il appelle automatiquement tous les hooks enregistrés auprès du système.

Méthode secondaire : configurer l'image manuellement

Si vous ne pouvez pas utiliser sysprep, vous devez effectuer manuellement les étapes suivantes pour toute image sur laquelle le service Smart Desktop Record Service est installé avant de déployer cette image sur des PC supplémentaires.

IMPORTANT Si vous choisissez d'effectuer ces étapes, consultez ce document fréquemment pour vous tenir au courant des modifications apportées à ces étapes.

1. Arrêtez le service d'enregistrement de bureau intelligent.
2. Ouvrez le dossier "log" où le service Smart Desktop Record Service est installé (par défaut, il s'agit de C :\Program Files (x86)\Calabrio ONE\Desktop\Active\log) et supprimez tous les fichiers qui ne contiennent pas le mot "postinstall".
3. Supprimez tous les sous-dossiers (y compris leur contenu) du dossier "log".
4. Ouvrez "C :\Program Files (x86)\Common Files\Calabrio ONE\Desktop\config" et supprimez tous les fichiers sauf "Install.ini" et "sysproperties.cfg".
5. Supprimez tous les sous-dossiers (y compris leur contenu) du dossier "config".
6. Ouvrez "C :\Program Files (x86)\Common Files\Calabrio ONE\Desktop\recordings" et supprimez tous les fichiers et sous-dossiers (y compris leur contenu). Le dossier "enregistrements" doit être vide.
7. Ouvrez "C :\Program Files (x86)\Common Files\Calabrio ONE\Desktop\chunks" et supprimez tous les fichiers et sous-dossiers (y compris leur contenu). Le dossier "chunks" doit être vide.

   Remarque : Le dossier "chunks" peut ne pas exister. Si le dossier "chunks" n'existe pas, vous pouvez ignorer cette étape.

Envoyer les codes de retour de l'installation

Lorsque vous utilisez une méthode d'installation par diffusion (telle que GPO), vous recevez des codes de retour indiquant la réussite ou l'échec de l'installation. Les éventuels codes de retour sont décrits ci-dessous.

Code de retour	Description
0	Installation réussie
1	Échec de l'installation

En outre, les événements seront écrits dans le journal des événements Windows. Les détails de l'événement indiqueront une description de ce qui s'est passé. Trois ID d'événement différents seront écrits. L'événement lui-même contiendra plus de détails, mais en général, les ID indiquent ce qui suit :

ID d'événement	Description
8080	Installation réussie

ID d'événement	Description
8081	Échec de l'installation
8084	Message d'information

Les détails d'une installation réussie ou échouée seront écrits à la fois dans le journal des événements Windows et dans les journaux contenus dans le dossier wrapper sous le dossier d'installation de Smart Desktop Client.

Outil de vérification des clients

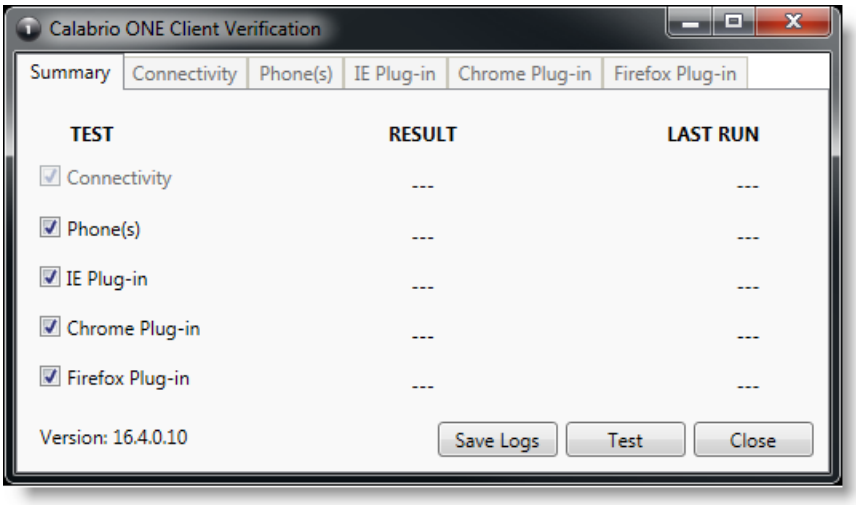
L'outil de vérification client teste le PC client pour s'assurer que la connectivité avec les serveurs et le téléphone est adaptée à l'exécution de Smart Desktop. Il est installé lorsque Smart Desktop est installé. L'outil exécute divers tests et rapporte les résultats sous forme de réussite ou d'échec.

Exécuter l'outil de vérification client

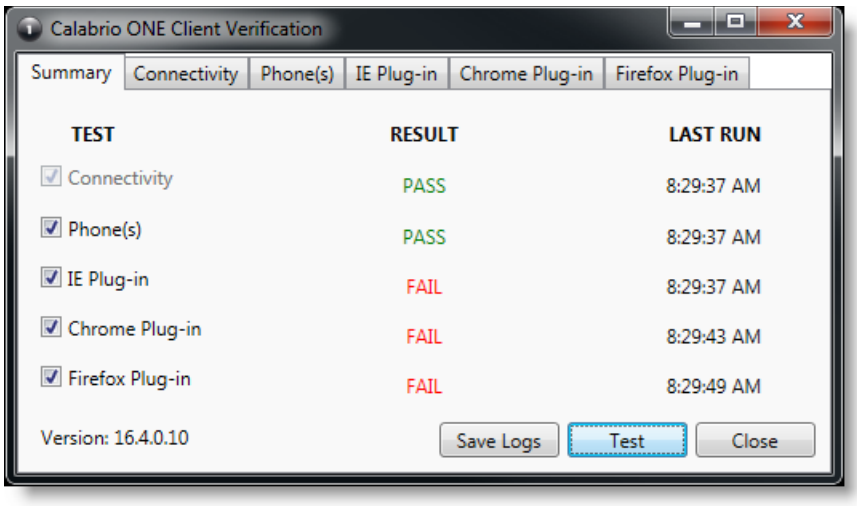
1. Après avoir installé Smart Desktop, accédez au dossier suivant sur le PC client :

   C :\Fichiers programmes (x86)\Calabrio ONE\Bureau\Actif\bin\

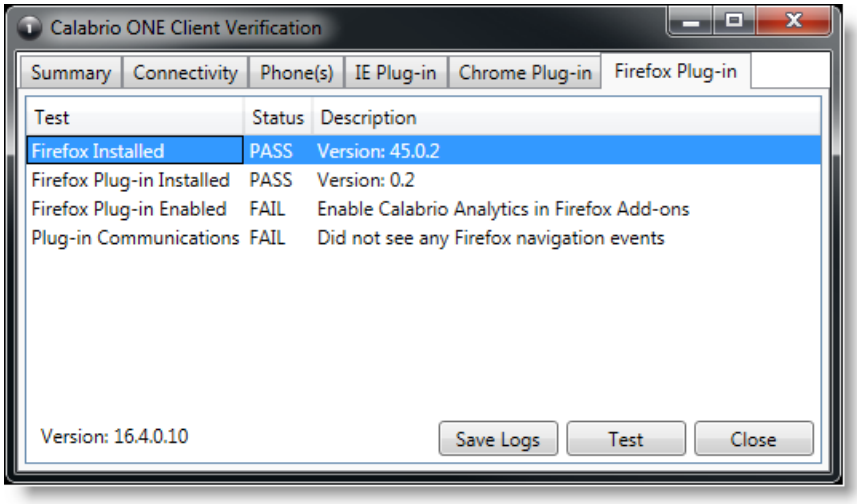
2. Double-cliquez sur **ClientDiag.exe**. L'outil de vérification du client démarre.



3. Par défaut, tous les tests sont sélectionnés. Cliquez sur **Tester**.
4. L'outil rapporte les résultats du test comme une réussite ou un échec.



5. Il y a un onglet pour chaque test où les détails du test sont affichés. Si le test échoue, les détails sur l'onglet fourniront des indications sur ce qui ne va pas.



6. Si nécessaire, vous pouvez cliquer sur **Enregistrer les** journaux pour compresser les journaux pour Post-installation et Smart Desktop afin de vous aider à identifier les problèmes. Les journaux sont automatiquement compressés dans un fichier nommé Clientlogs.zip.

Commandes d'enregistrement

L'application autonome Commandes d'enregistrement est automatiquement installée avec Smart Desktop. Les contrôles d'enregistrement permettent à un agent de démarrer, de mettre en pause, de reprendre et d'arrêter l'enregistrement audio, d'écran et de frappe pour les appels actifs, ainsi que d'étiqueter les appels et d'y ajouter des métadonnées.

L'utilisation de commandes d'enregistrement est facultative.

REMARQUE : L'application Contrôles d'enregistrement n'est pas prise en charge avec certains déploiements de fournisseurs CCaaS.

L'exécutable Contrôles d'enregistrement est installé ici :

C :\Fichiers programmes (x86)\Calabrio ONE\Bureau\Actif\bin\DCC.exe

Dans le menu Démarrer, l'application est nommée Webex WFORecording Controls et se trouve par défaut sous Webex WFO.

Enlèvement

Les rubriques suivantes décrivent comment désinstaller Webex composants WFO.

Désinstallation Webex WFO Smart Desktop

REMARQUE : Vous devez vous connecter en tant qu'administrateur pour désinstaller Smart Desktop.

1. Sur le bureau ou le serveur client léger sur lequel Smart Desktop est installé, ouvrez le Panneau de configuration Windows.
2. Démarrez l'utilitaire Ajout/Suppression de programmes.
3. Dans la liste, sélectionnez l'application que vous souhaitez supprimer et cliquez sur **Désinstaller**.

   Si vous avez l'intention de réinstaller Smart Desktop après avoir complètement supprimé une ancienne version (nouvelle installation), vérifiez que les structures de dossiers de stockage des enregistrements sont supprimées avant d'installer la nouvelle version.

4. Redémarrez le bureau ou le serveur client léger.

Désinstallation à l'aide de l'objet de stratégie de groupe

Un objet de stratégie de groupe (GPO) est un ensemble de paramètres qui définissent à quoi ressemblera un système et comment il se comportera pour un groupe défini d'utilisateurs. Microsoft fournit un composant logiciel enfichable qui vous permet d'utiliser la stratégie de groupe Microsoft Management Console pour définir diverses options, y compris des options de scripts.

1. Créez un script de traitement par lots pour exécuter le programme d'installation qui contient le script suivant :

   ```
   <C :\Fichiers programmes (x86)\Calabrio ONE\Bureau\Wrapper\unins000.exe /LOG
       /VERYSILENT /NORESTART>
   ```

2. Démarrez l'éditeur de gestion des stratégies de groupe et accédez à Stratégies de configuration > ordinateur > paramètres > scripts Windows (démarrage/arrêt) et ajoutez le script de traitement par lots.

IMPORTANT Cela forcera tous les navigateurs ouverts à se fermer. Si les navigateurs sont rouverts avant la fin de la désinstallation, il se peut que la désinstallation échoue et qu'elle doive être redémarrée.

Désinstaller Smart Desktop à l'aide des paramètres de commande silencieuse

Les paramètres silencieux vous permettent de désinstaller Webex WFO à l'aide de votre interface de ligne de commande. Voir "Uninstaller Command Line Parameters" dans https://jrsoftware.org/ishelp/index.php?topic=setupcmdline pour les options.