Authentification unique Unified MeetingPlace 7.0 avec WebEx Type II

Contenu

Introduction

Ce document décrit l'ouverture de session simple de Cisco Unified MeetingPlace 7.0 (SSO) pour l'usage avec le type II. de Cisco WebEx.

Caractéristiques

- Le serveur d'applications de Cisco Unified MeetingPlace pont le répertoire d'entreprise et le Centre de réunions Cisco WebEx de Cisco.
- Élimine la nécessité de gérer des comptes utilisateurs distincts d'Unified MeetingPlace et de WebEx (ajoute, des modifications, des mises hors fonction).
- Les utilisateurs finaux utilisent leurs user-id et mots de passe de Protocole LDAP (Lightweight Directory Access Protocol) et sont authentifiés sur des sites interface de établissement du programme pour de WebEx de productivité d'outils et de WebEx Web.

- Simplifie le déploiement des outils de productivité de WebEx.
- Crée des comptes d'hôte de WebEx créés dynamiquement quand les utilisateurs ouvrent une session.
- Prend en charge chacun des trois (3) types de contrat de WebEx : *hôte Désigné*, *ports simultanés*, et *par minute*.
- Pour le type II de WebEx programmant, l'Unified MeetingPlace utilise des *téléconférences non réservées* :Le numéro de profil est utilisé comme *ID de téléconférence non réservée* pour toutes les téléconférences.*L'hôte de la* téléconférence doit ouvrir une session utilisant leur *numéro de profil* et *mot de passe du profil d'*Unified MeetingPlace afin de commencer les téléconférences sonores.OUL'Unified MeetingPlace peut être configuré pour utiliser la caractéristique d'Automatique-*service* qui emploiera l'Identification de l'appelant pour se connecter des utilisateurs dans des téléconférences automatiquement. Tous les utilisateurs d'invité sont tenus dans une *salle attendante* jusqu'aux logins d'hôte ou (sur option) jusqu'à ce qu'un autre utilisateur système ouvre une session à cette téléconférence sonore.

Ouverture de session simple (SSO)

MeetingPlace SSO équilibre la facilité d'utilisation avec la Sécurité :

- Puisque l'Unified MeetingPlace réside complètement dans le réseau d'entreprise, l'Unified MeetingPlace SSO exige des hôtes de la téléconférence de se connecter au réseau d'entreprise avant qu'ils puissent ouvrir une session.
- L'Unified MeetingPlace SSO exige des hôtes de la téléconférence d'entrer leur user-id et mot de passe de Répertoire actif LDAP/Microsoft (AD) sur la procédure de connexion aux outils de page et de productivité de WebEx. Comme commodité, l'information de connexion est stockée pendant jusqu'à 90 minutes.
- Une fois qu'ils ouvrent une session, l'hôte de la téléconférence peut prévoir ou lancer des téléconférences.
- Se réunissant les invités ne doivent pas authentifier contre l'Unified MeetingPlace SSO pour joindre des téléconférences.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Unified MeetingPlace 7.0.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Architecture

- Le fournisseur de service téléphonique de WebEx (TSP) fournit à une connexion socket chiffrée persistante du TCP 443 des Certificats de Sécurité de Transport Layer Security (TLS) au site de WebEx de l'intérieur au Pare-feu extérieur pour la communication protégée par l'intermédiaire d'un jeu d'instructions XML API.L'intégration de LDAP de Cisco Unified Communications Manager (CUCM) avec l'authentification d'utilisateur est activée au système entreprise de LDAP, et tous les utilisateurs sont créés dans la base de données d'utilisateur CUCM.Puis, le service d'annuaire d'Unified MeetingPlace est activé synchroniser des utilisateurs CUCM à l'Unified MeetingPlace.SSO doit être activé sur le site de WebEx pendant le ravitaillement et ne peut pas être changé ensuite sans reconstruction du site.Tous les profils sur l'Unified MeetingPlace alors seront automatiquement propagés au WebEx, et SSO est fourni sur des sites.
- Aucun mot de passe de LDAP n'est envoyé ou est enregistré sur l'Unified MeetingPlace ou le WebEx ; toute l'authentification se produit sur des sites au LDAP.Si le service d'annuaire d'Unified MeetingPlace est activé avec CUCM 6.x ou plus tard, l'authentification est fournie par CUCM à l'authentification LDAP.Des mots de passe du profil d'Unified MeetingPlace sont créés dans le domaine *PIN* CUCM pendant la synchronisation de profil, et un PIN de par défaut est fourni à tous les utilisateurs. Des broches peuvent être changées seulement par les pages d'utilisateur CUCM par l'intermédiaire du GUI (<ccm *url>/ccmuser de* https://) ou par remise PIN d'administrateur système CUCM.L'authentification pourrait également être équipée d'user-id locaux d'Unified MeetingPlace et de mots de passe (aucune intégration de service de répertoire LDAP n'est activée sur CUCM ou Unified MeetingPlace).
- L'authentification d'utilisateur par Unified MeetingPlace traverse le Langage SAML (SAML) au WebEx comme un site *de confiance*.
- S'ils n'existent pas déjà, des profils sont créés sur le WebEx dans ces exemples :Quand un utilisateur prévoit une téléconférence de WebEx.Quand accès client leur compte de la page de planification.
- Le TSP de WebEx suppose que conflit de nom d'utilisateur ne se produira pas parce que le site de WebEx est dédié à ce client et exclusivement utilisé.
- Le WebEx exige de seules adresses électroniques pour tous les utilisateurs sur le site.
- Une fois intégrée avec le WebEx, la condition requise d'*ID de téléconférence non réservée de* nombre de profil utilisateur d'Unified MeetingPlace est 8 chiffres ou moins. Typiquement, le numéro de profil de *sans réservation* devrait être un numéro de téléphone de travail sans code de pays ou codes postaux.
- Des profils utilisateurs doivent être manuellement désactivés du centre de gestion de site de WebEx. Alternativement, vous pouvez activer le site de WebEx plaçant *pour désactiver automatiquement le compte après XX des jours de l'inactivité*. (Cette fonction n'est pas prise en charge automically par le TSP pour SSO ou systèmes de non-SSO.)

Synchronisation de profil de LDAP

AD 2000/3/7" de MS de	Profil utilisateur de	Services d'annuaire de MeetingPlace	Compte d'hôte de WebEx

LDAP de client «	gestionnaire UC		
givenName	Prénom	Prénom	Prénom
Sn	Nom de famille	Nom de famille	Nom de famille
sAMAccountName	User-id	User-id	User-id
Mot de passe	Mot de passe (du LDAP si l'authentification est activée)	Mot de passe (du mot de passe de LDAP ou de député britannique de gens du pays)	Le mot de passe local de mot de passe (non envoyé si le LDAP INTÉGRÉ est activé) dans le WebEx est utilisé si aucun LDAP INTÉGRÉ
telephoneNumber	Numéro de téléphone	Numéro de profil (modifiez 3 différentes méthodes pour ceci)	Numéro de profil (chiffres de limite 8)
S/O	Le PIN et confirment le PIN	Le mot de passe du profil et confirment	S/O
messagerie	ID de messagerie	Adresse e-mail	Adresse e-mail
telephoneNumber	Numéro de téléphone principal	Numéro de téléphone principal	Numéro du bureau
service	Service	Nom de groupe (le par défaut est le *système*)	
S/O	État de synchronisation de LDAP	État d'utilisateur : Active, désactivé, verrouillé	
S/O	S/O	Code de affichage (facultatif)	Code de affichage (facultatif)

Remarque: Si le LDAP de client est SunOne/iPlanet, les champs sont différents pour les noms de la base de données de LDAP, mais sont semblables à l'AD de Microsoft.

Répertoire de client	Services d'annuaire CUCM

AD 2000 de Windows	Oui
AD 2003 de Windows	Oui
AD 2007 de Windows	Oui
AD 2008 de Windows	Oui
Netscape 4.x	Oui
iPlanet 4.x	Oui
Serveur de répertoire du Sun 5.1	Oui
Serveur de répertoire de Javas 5.2 de Sun	Oui
OpenLDAP	Oui
Services d'annuaire IBM Tivoli	Sur la feuille de route
Novell eDirectory	Oui
SunOne	Non
Répertoire de domino	Non

Recommandations PIN d'utilisateur d'Unified Communication Manager

- Placez une stratégie de créance par défaut pour tous les utilisateurs. Référez-vous au pour en savoir plus de créance de configuration par défaut de stratégie.
- N'UTILISEZ PAS UN PIN *FACILE DE* PAR DÉFAUT ; par exemple, « 123456" ne devrait pas être utilisé comme PIN de par défaut dû aux risques de sécurité.
- Àla page de créance de configuration par défaut de stratégie, cochez l'**utilisateur doit changer à la prochaine** case de **procédure de connexion**.
- Les utilisateurs finaux doivent accéder aux pages de *ccmuser d'*options utilisateur afin de changer leur PIN pour que le mot de passe du profil d'Unified MeetingPlace soit sécurisé : <UCManager *Hostname>/ccmuser de* https://
- Le PIN de courant est le par défaut, qui est placé à la page de créance de configuration par défaut de stratégie comme affiché ci-dessus.

MeetingPlace 7 filtres de service d'annuaire

Les filtres sont configurables pour créer des profils basés sur code de pays ou pour créer des fuseaux horaires basés sur des numéros de téléphone.

Filtres de service d'annuaire pour des fuseaux horaires

L'un de ces champs qui ne sont pas disponibles dans Cisco Unified Communications Manager (par l'intermédiaire du LDAP) sont blanc de gauche dans le profil utilisateur de Cisco Unified MeetingPlace :

- Prénom, nom de famille, ou user-id.
- Le numéro de profil, qui est un numéro unique a basé sur le numéro de téléphone principal.
- État d'utilisateur.
- Adresse électronique.

- Numéro de téléphone principal.

Filtres de service d'annuaire pour des groupes

- Filtré par le préfixe de numéro de téléphone (code postal, code de pays, etc.).
- Par défaut, l'heure locale du serveur d'applications est assignée des *filtres pour des groupes*.
- Le nom de groupe est filtré par le nombre de service.
- Par défaut, le groupe d'utilisateurs de *système* est assigné.

Numéros de profil

Procédure

1. Configurez les filtres pour des fuseaux horaires.
2. Configurez les filtres pour des groupes.
3. Configurez les filtres de numéro de profil.
4. Exécutez une synchronisation de répertoire avec CUCM.

Recommandations

- Utilisez un numéro de téléphone comme numéro de profil.**Remarques :**L'entrée de *champ Number de téléphone de* profil utilisateur CUCM est le numéro de profil.Si le numéro de téléphone pour un utilisateur est blanc ou est en conflit avec un numéro de profil existant dans l'Unified MeetingPlace, le système utilise un numéro de profil automatique-généré parchiffre.
- Utilisez les derniers chiffres « n » (nombre) d'un numéro de téléphone comme numéro de profil.**Remarque:** Si le numéro de téléphone pour un utilisateur est vide ou si l'application de cette méthode pour un utilisateur est en conflit avec un numéro de profil existant dans l'Unified MeetingPlace, alors le système utilise à la place un numéro de profil automatique-généré parchiffre.
- Utilisez les six (6) numéros de profil automatique-générés par chiffre.Le début automatique-généré de numéros de profil de 100001 et contiennent toujours six chiffres.Si l'entrée de champ Number de téléphone pour un utilisateur est plus courte que le nombre configuré de chiffres, le nombre sera utilisé comme est.
- Appliquez-vous la méthode de configuration de numéro de profil à ce qui suit :Nouveaux utilisateursChaque profil utilisateur qui obtient importéLes profils qui sont mis à jour pendant le profil utilisateur de service d'annuaire met à jourPleines synchronisations

Procédure d'authentification d'utilisateur final

L'authentification de l'utilisateur entière de WebEx est manipulée sur des sites par Unified MeetingPlace. Une fois que l'utilisateur est authentifié, un ID de session de WebEx est généré pour l'utilisateur, et la demande est réorientée au service de WebEx.

Voici un aperçu de l'écoulement pour le SAMLv2 SSO :

1. L'utilisateur clique sur une ressource protégée sur le site de WebEx.
2. Le WebEx se rend compte que l'utilisateur n'a pas ouvert une session basé sur les informations de session.
3. Le WebEx réoriente l'utilisateur au fournisseur d'identité (Unified MeetingPlace).

4. L'Unified MeetingPlace note également que l'utilisateur n'est pas ouvert une session basé sur ses propres informations de session.
5. L'Unified MeetingPlace affiche à l'utilisateur sa propre page de connexion et les authentifie.
6. L'Unified MeetingPlace génère l'assertion SAML et réoriente l'utilisateur pour envoyer cette assertion au WebEx.
7. Le WebEx valide l'assertion, et l'utilisateur est authentifié.
8. L'utilisateur peut maintenant accéder à la ressource protégée sur le WebEx.

Voici l'écoulement pas à pas pour le SAMLv2 SSO :

1. Le site de WebEx réoriente automatiquement l'utilisateur au serveur d'applications interne d'Unified MeetingPlace pour sur l'authentification de sites.
2. Accès client la page d'authentification d'Unified MeetingPlace sur des sites derrière le Pare-feu entreprise.
3. Basé sur les identifiants utilisateurs, le serveur d'Unified MeetingPlace authentifie l'utilisateur contre sa propre base de données locale d'Unified MeetingPlace ou le répertoire LDAP entreprise (si activé par l'intermédiaire du service d'annuaire).
4. Le serveur d'Unified MeetingPlace envoie une demande de *sessionGenerate de l'*utilisateur au WebEx.
5. Le WebEx suppose que l'utilisateur est déjà authentifié et envoie un seul ID de session pour l'utilisateur à MeetingPlace.
6. MeetingPlace réoriente les utilisateurs au WebEx (avec l'ID de session dans la chaîne de requête de l'URL).
7. L'Unified MeetingPlace authentifie l'utilisateur et affirme qu'ils sont qui ils sont.
8. Le WebEx valide l'assertion en vérifiant la signature avec le certificat d'Unified MeetingPlace qui provisioned et puis fait confiance à la demande qui Unified MeetingPlace fait si la validation réussissait.
9. L'utilisateur peut maintenant prévoir ou assister à des téléconférences de l'interface web de WebEx.

User-id et configurations enregistrées par mot de passe

La configuration de site de WebEx a une option de contrôler la durée du service d'authentification sous l'Add/Edit.

Les utilisateurs ouvrent une session, et les paramètres de site de WebEx spécifient combien de temps cette procédure de connexion est permise dans le système avant que l'utilisateur soit incité de nouveau pour leurs qualifications de procédure de connexion.

Configurations facultatives de sécurité du mot de passe de navigateur Web

Si le paramètre de sécurité de navigateur est activé l'utiliser *souvenez-vous moi les* configurations enregistrées par mot de passe, les utilisateurs n'est pas incité de nouveau à ouvrir une session au système d'Unified MeetingPlace. Par conception, l'Unified MeetingPlace incite pour des qualifications de procédure de connexion afin de préserver l'intégrité de Sécurité des utilisateurs se connectant dans le système. (L'Unified MeetingPlace ne sauvegarde pas des mots de passe.) Ceci est contrôlé entièrement par les autorisations utilisateur d'entreprise permises ou non permises par des contrôles de service TI.

Pour Firefox, ce paramètre de sécurité se trouve dans la boîte de dialogue d'options de Sécurité.

Pour l'Internet Explorer, ce paramètre de sécurité se trouve dans la boîte de dialogue Settings d'AutoComplete.

Outlook et Lotus Notes SSO

Des téléconférences de WebEx/Unified MeetingPlace peuvent être prévues par des outils de productivité de WebEx avec des clients de Microsoft Outlook ou de Lotus Notes. L'utilisateur doit être configuré et authentifié dans le système de LDAP de client avant qu'ils puissent prévoir une téléconférence par l'intermédiaire du module d'extension. Il y a deux modèles pour l'authentification de l'utilisateur : un avec le service d'annuaire et l'autre sans le service d'annuaire.

Procédure

Terminez-vous ces étapes afin de prévoir une téléconférence dans Microsoft Outlook :

1. Calendrier d'Access Microsoft Outlook.
2. **Planification de téléconférence de** clic.
3. Cliquez sur Add la **téléconférence de WebEx**.La boîte de dialogue d'outils de productivité de WebEx apparaît.
4. Entrez votre nom d'utilisateur et mot de passe, et cliquez sur la **procédure de connexion.**La téléconférence de WebEx est prévue. Les utilisateurs peuvent annuler la téléconférence de WebEx ou changer des configurations par le module d'extension de Microsoft Outlook.

API et module d'extension

Pour l'authentification par SSO, l'Unified MeetingPlace fournit un API, qui permet au module d'extension de WebEx pour l'identifier s'il y a d'intégration SSO avec l'Unified MeetingPlace. L'API permet également à l'utilisateur pour se terminer l'authentification. Dans le cas où il n'y a aucun service d'annuaire, le module d'extension de client de WebEx obtient l'authentification du WebEx directement.

Si l'Unified MeetingPlace est déployé avec SSO, le module d'extension doit envoyer le message d'authentification à l'Unified MeetingPlace. S'il n'y a aucun SSO, le message d'authentification va au WebEx.

Le module d'extension de WebEx exige de ces informations afin d'envoyer le message d'authentification à l'URL correct de service d'authentification :

- URL de service d'authentification d'Unified MeetingPlace : <meetingplace-app-serveur >/public/login/applogin de https://
- URL de service de WebEx
- Si l'Unified MeetingPlace a le service d'annuaire configuré

Le module d'extension de WebEx pourrait ou ne pourrait pas être préconfiguré avec ces informations tout en installant sur l'ordinateur de client. Si toutes les informations sont préconfigurées, le module d'extension peut être utilisé pour authentifier des utilisateurs en envoyant des messages d'authentification à l'Unified MeetingPlace/au WebEx basés sur la configuration.

Si le module d'extension n'est pas préconfiguré avec les informations, l'embrochable doit envoyer un message une fois à l'Unified MeetingPlace pour obtenir les informations de configuration.

L'utilisateur doit manuellement taper l'URL de service d'authentification d'Unified MeetingPlace et soumettre le message. (C'est une étape manuelle une fois pour l'utilisateur.)

Dans la réponse, MeetingPlace renvoie ces informations :

- Si l'Unified MeetingPlace a le service d'annuaire configuré
- URL de service de WebEx

Une fois que le module d'extension reçoit ces informations, il peut être utilisé pour l'authentification de l'utilisateur. L'utilisateur est incité à entrer leur nom d'utilisateur et mot de passe.

S'il y a un service d'annuaire, il enverra un message à l'Unified MeetingPlace API une fois que les données sont soumises. L'Unified MeetingPlace authentifie l'utilisateur basé sur leur user-id et mot de passe et communique avec le WebEx API pour générer une clé de session. S'il est réussi, la clé de session est retournée par une réponse XML. Si l'exécution échoue, le message XML contiendra un message d'erreur et un code d'erreur.

Installation d'outil de productivité de WebEx

Après que vous installiez la productivité de WebEx usine pour la première fois, les outils de productivité de Web que la page de connexion paraît. Par conception, les champs de nom d'utilisateur et de mot de passe sont désactivés puisque l'Unified MeetingPlace fournit l'authentification.

Afin d'ouvrir une session, écrivez le nom de domaine (par exemple, *t27lmp.webex.com*) dans le champ URL de site, et cliquez sur la **procédure de connexion**.

Remarque: La durée qui passe avant que l'utilisateur soit incité de nouveau pour des qualifications de procédure de connexion est placée par le paramètre de service d'authentification de site de WebEx. Le délai par défaut est de 90 minutes.

Alternativement, vous pouvez ouvrir une session par la boîte de dialogue de seul clic de Cisco WebEx. Cliquez sur le lien de **configurations de WebEx d'éditer**.

L'onglet de compte s'ouvre, et les champs de nom d'utilisateur et de mot de passe sont désactivés. Écrivez le nom de domaine (par exemple, *t27lmp.webex.com*), et cliquez sur Apply.

La page de connexion d'outils de productivité de WebEx paraît, et le nom d'utilisateur et le mot de passe sont enregistrés localement par l'intermédiaire du client de seul clic. Des utilisateurs ne sont pas incités à se connecter dans le système de nouveau.

Enregistrements

- Les utilisateurs finaux doivent toujours commencer des enregistrements de l'interface de WebEx Meeting Center.
- Si vous commencez un enregistrement à partir du relais multifréquence de double tonalité de l'interface utilisateur de Voix d'Unified MeetingPlace (VUI) (DTMF), il enregistre seulement sonore et n'est pas accessible pour la lecture comme enregistrement réservé à l'audio.
- Si vous commencez l'enregistrement à partir des Conférences Web de WebEx, elles enregistrent l'audio et le Web.
- Quand un enregistrement de téléconférence est commencé de l'interface de Conférences

Web de WebEx, le service Fondé(e) sur le réseau de l'enregistrement (NBR) suit un ordre d'en sortie utilisant un nombre sonore édité d'accès distant d'Unified MeetingPlace.
- Le serveur sonore identifie l'ordre spécial, sait que l'utilisateur est un serveur d'enregistrement de WebEx, et admet que lien de Voix à connecter.
- Le WebEx peut créer l'audio et les enregistrements Web synchronisés, qui sont enregistrés dans le service du WebEx NBR. Vous pouvez placer des paramètres de mémoire dans le service NBR.
- Les utilisateurs doivent ouvrir une session à leur propre portail de WebEx pour accéder à des enregistrements.
- *L'option de téléconférence record* est placée de rectifier pour toutes les téléconférences de WebEx, et la demande générique, des « parties de cette téléconférence peut être enregistrée, » est lue pour tous les utilisateurs. (Cette valeur par défaut peut être désactivée si désirée.)
- des téléconférences réservées à l'audio qui doivent être enregistrées peuvent être prévues avec le WebEx et être enregistrées par le WebEx.

Utilisateurs réservés à l'audio sur les sites Désignés de WebEx de Meeting Center d'hôte avec le Scheduling du type II

L'administrateur système de client doit manuellement exécuter ces étapes pendant que des utilisateurs sont créés sur le système.

1. L'administrateur du site crée un compte d'hôte avec de pleins privilèges de WebEx (avec la session suivante tape : PRO et AUO*).**Remarque:** Ce compte d'hôte compte temporairement vers le quota Désigné d'hôte acheté par le client.
2. L'administrateur du site désactive le PRO type de session pour ce nouveau compte d'hôte, partant seulement d'AUO activé.
3. L'administrateur du site exporte les autorisations à un fichier CSV d'Exceler, le lot met à jour les autorisations, et puis importe les autorisations.**Remarque:** Ceci décrémente le compte Désigné d'hôte de sorte qu'on permette à un un nombre illimité de comptes d'hôte d'*audio seulement* pour programmer par l'intermédiaire des outils de productivité de WebEx.

Informations connexes

- Produits et services de Cisco Unified MeetingPlace 7.0
- Support et documentation techniques - Cisco Systems