# Exemple de configuration de la version 10.5 SAML SSO d'Unity Connection

**ID de document** : 118772

**Mis à jour** : Janv. 21, 2015

Contribué par A.M.Mahesh Babu, ingénieur TAC Cisco.

PDF de téléchargement
Copie
Commentaires

## Produits connexes

- Cisco Unity Connection
- Cisco Unified Communications Manager (CallManager)

## Contenu



## Introduction

Ce document décrit comment configurer et vérifier l'ouverture de session simple du Langage SAML (SAML) (SSO) pour le Cisco Unity Connection (UCXN).

# Conditions préalables

## Conditions requises

### Installation de Protocole NTP (Network Time Protocol)

Pour SAML SSO à fonctionner, vous devez installer le NTP correct installé et s'assurer que la différence de temps entre le fournisseur d'identité (IDP) et les Applications de communications unifiées ne dépassent pas trois secondes. Pour des informations sur synchroniser des horloges, voyez la section de configurations de NTP dans le guide d'administration de système d'exploitation de Cisco Unified Communications.

### Domain Name Server (DN) installé

Les Applications de communications unifiées peuvent utiliser des DN afin de résoudre les noms de domaine complet (FQDN) aux adresses IP. Les fournisseurs de services et l'IDP doivent être résolubles par le navigateur.

La version 2.0 active de service de fédération de répertoire (AD FS) doit être installée et configurée afin de traiter des demandes SAML.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.0 FS d'AD comme IDP
- UCXN comme fournisseur de services
- Version 10 de Microsoft Internet Explorer

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.

# Informations générales

Le SAML est un XML, format des données de standard ouvert pour d'échange de données. C'est un protocole d'authentification utilisé par des fournisseurs de services afin d'authentifier un utilisateur. Les informations d'authentification de Sécurité sont passées entre un IDP et le fournisseur de services.

Le SAML est un standard ouvert qui permet à des clients d'authentifier contre n'importe quel service SAML-activé de Collaboration (ou a unifié la transmission) indépendamment de la plateforme cliente.

Toutes les interfaces de Web de Cisco Unified Communications, telles que Cisco Unified Communications Manager (CUCM) ou UCXN, utilisent le protocole de version 2.0 SAML dans la caractéristique SAML SSO. Afin d'authentifier l'utilisateur de Protocole LDAP (Lightweight Directory Access Protocol), UCXN délègue une demande d'authentification à l'IDP. Cette demande d'authentification générée par l'UCXN est une demande SAML. L'IDP authentifie et renvoie une assertion SAML. L'assertion SAML affiche ou oui (authentifié) ou no (échec de l'authentification).

SAML SSO permet à un utilisateur de LDAP pour se connecter dans des applications cliente avec un nom d'utilisateur et mot de passe qui authentifie sur l'IDP. Une connexion d'utilisateur aux applications Web prises en charge l'unes des sur les Produits unifiés de transmission, après que vous activiez la caractéristique SAML SSO, accède également à ces applications Web sur UCXN (indépendamment de CUCM et CUCM IM et présence) :

| Utilisateurs d'Unity Connection | Applications Web |
|---|---|
| Utilisateurs de LDAP avec des droits d'administrateur | • Gestion UCXN<br>• Utilité de Cisco UCXN<br>• Utilité de Cisco Unified<br>• Cisco Personal Communications Assistant<br>• Boîte de réception de Web<br>• Mini boîte de réception de Web (version de desktop) |
| Utilisateurs de LDAP sans droits d'administrateur | • Cisco Personal Communications Assistant<br>• Boîte de réception de Web<br>• Mini boîte de réception de Web (version de desktop)<br>• Clients de Cisco Jabber |

# Configurez

## Diagramme du réseau

### Installation de répertoire

1. Signez dans la page de gestion UCXN et le **LDAP** choisi et cliquez sur l'**installation de LDAP**.
2. Vérifiez l'**enable synchronisant du serveur LDAP** et cliquez sur la **sauvegarde**.
3. **LDAP de** clic.
4. **Configuration de répertoire LDAP de** clic.
5. Cliquez sur Add **nouveau**.

6. Configurez ces éléments :

   Paramètres des comptes de répertoire LDAPAttributs d'utilisateur à synchroniserProgramme de synchronisationAdresse Internet de serveur LDAP ou adresse IP et numéro de port

7. Vérifiez le **SSL d'utilisation** si vous voulez employer le Protocole SSL (Secure Socket Layer) afin de communiquer avec le répertoire LDAP.

   **Conseil** : Si vous configurez le LDAP au-dessus du SSL, téléchargez le certificat de répertoire LDAP sur CUCM. Référez-vous au contenu de répertoire LDAP dans Cisco Unified Communications Manager SRND pour des informations sur le mécanisme de synchronisation de compte pour les Produits spécifiques de LDAP et les pratiques recommandées générales pour la synchronisation de LDAP.

8. Le clic **exécutent le plein sync maintenant**.

   **Note**: Assurez-vous que service de **Cisco DirSync** est activé dans la page Web d'utilité avant que vous cliquiez sur la sauvegarde.

9. Développez les **utilisateurs** et sélectionnez les **utilisateurs d'importation**.

10. Dans l'**Unified Communications Manager de découverte les utilisateurs finaux** les répertorient, **répertoire LDAP** choisi.

11. Si vous voulez importer seulement un sous-ensemble des utilisateurs dans le répertoire LDAP avec lequel vous avez intégré UCXN, écrivez les caractéristiques applicables dans les champs Rechercher.

12. Sélectionnez la **découverte**.

13. Dans basé sur la liste de modèle, sélectionnez le **modèle d'administrateur** que vous voulez qu'UCXN l'utilise quand il crée les utilisateurs sélectionnés.

    **Attention** : Si vous spécifiez un modèle d'administrateur, les utilisateurs n'auront pas des boîtes aux lettres.

14. Vérifiez les cases pour les utilisateurs de LDAP pour qui vous voulez créer les utilisateurs UCXN et l'**importation de** clic **sélectionnés**.

## Enable SAML SSO

1. Connectez-vous dans l'interface utilisateur de gestion UCXN.

2. Choisissez le **système** > l'**ouverture de session simple SAML** et la fenêtre de configuration SAML SSO s'ouvre.

3. Afin d'activer SAML SSO sur la batterie, **enable SAML SSO de** clic.

4. Dans la fenêtre d'avertissement de remise, le clic **continuent.**

5. Sur l'écran SSO, le clic **parcourent** afin d'importer le fichier XML de **métadonnées FederationMetadata.xml** avec l'**étape de métadonnées de** DownloadIdp.

6. Une fois que le fichier de métadonnées est téléchargé, cliquez sur les **métadonnées d'IDP d'importation** afin d'importer les informations d'IDP à UCXN. Confirmez que l'importation était réussie et le clic **à côté de** continuent.

7. Cliquez sur Download l'**ensemble de fichiers de métadonnées de confiance** (faites ceci seulement si vous n'avez pas configuré ADFS déjà avec des métadonnées UCXN) afin de sauvegarder les métadonnées UCXN à un répertoire local et aller ajouter UCXN pendant que transmettant par relais la confiance d'interlocuteur. Une fois que la configuration FS d'AD est terminée, passez à l'étape 8.

8. **SSO** choisis en tant qu'utilisateur administratif et cliquent sur Run le **test SSO**.

9. Ignorez les avertissements de certificat et poursuivez plus loin. Quand vous êtes incité pour des qualifications, écrivez le nom d'utilisateur et mot de passe de l'utilisateur SSO et cliquez sur OK.

   **Note**: Cet exemple de configuration est basé sur les Certificats auto-signés par FS UCXN et d'AD. Au cas où vous utiliseriez des Certificats d'Autorité de certification (CA), des Certificats appropriés doivent être installés sur l'AD FS et l'UCXN. Référez-vous au pour en savoir plus de Gestion et de validation de certificat.

10. Après tout les étapes sont complètes, vous reçoivent le « test SSO réussi ! » message. **Fin** et **finition de** clic afin de continuer.

Vous vous êtes maintenant avec succès terminé les tâches de configuration d'activer SSO sur UCXN avec l'AD FS.

**Note obligatoire** : Exécutez le test SSO pour l'abonné UCXN si c'est une batterie afin d'activer SAML SSO. L'AD FS doit être configuré pour tous les Noeuds d'UCXN dans une batterie.

**Conseil** : Si vous configurez les fichiers XML des métadonnées de tous les Noeuds sur l'IDP et vous commencez à activer l'exécution SSO sur un noeud, alors SAML SSO sera activé sur tous les Noeuds dans la batterie automatiquement.

Vous pouvez également configurer CUCM et CUCM IM et présence pour SAML SSO si vous voulez utiliser SAML SSO pour des clients de Cisco Jabber et donner une véritable expérience SSO aux utilisateurs finaux.

# Vérifiez

Ouvrez un navigateur Web et écrivez le FQDN d'UCXN et vous voyez une nouvelle option sous des applications installées appelées **Recovery URL pour sauter l'ouverture de session simple (SSO)**. Une fois que vous cliquez sur le lien de **Cisco Unity Connection**, vous êtes incité pour des qualifications par l'AD FS. Après que vous entriez dans des qualifications de l'utilisateur SSO, vous serez avec succès connecté dans la page de gestion d'Unity, page unifiée d'utilité.

**Note**: SAML SSO n'active pas l'accès à ces pages :
- Gestionnaire de autorisation principal
- Gestion de SYSTÈME D'EXPLOITATION
- Système de Reprise sur sinistre

# Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Référez-vous dépannage derrière SAML SSO pour le pour en savoir plus des Produits 10.x de Collaboration.

# Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Janv. 21, 2015
ID de document : 118772