Exemple de configuration d'Unity Connection version 10.5 SAML SSO

Contenu

Introduction

Ce document décrit comment configurer et vérifier l'authentification unique SAML (Security Assertion Markup Language) pour Cisco Unity Connection (UCXN).

Conditions préalables

Conditions requises

Configuration du protocole NTP (Network Time Protocol)

Pour que SAML SSO fonctionne, vous devez installer la configuration NTP correcte et vous assurer que la différence de temps entre le fournisseur d'identité (IdP) et les applications de communications unifiées ne dépasse pas trois secondes. Pour plus d'informations sur la synchronisation des horloges, reportez-vous à la section NTP Settings du Guide d'administration du système d'exploitation Cisco Unified Communications.

Configuration du serveur de noms de domaine (DNS)

Les applications de communications unifiées peuvent utiliser DNS afin de résoudre les noms de domaine complets (FQDN) en adresses IP. Les fournisseurs de services et l'IDP doivent pouvoir être résolus par le navigateur.

Le service de fédération Active Directory (AD FS) version 2.0 doit être installé et configuré pour gérer les requêtes SAML.

Components Used

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

- AD FS version 2.0 en tant qu'IDP
- UCXN en tant que fournisseur de services
- Microsoft Internet Explorer version 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

SAML est un format de données basé sur XML et ouvert pour l'échange de données. Il s'agit d'un protocole d'authentification utilisé par les fournisseurs de services pour authentifier un utilisateur. Les informations d'authentification de sécurité sont transmises entre un IDP et le fournisseur de services.

SAML est une norme ouverte qui permet aux clients de s'authentifier contre tout service de collaboration (ou de communication unifiée) compatible SAML, quelle que soit la plate-forme du client.

Toutes les interfaces Web Cisco Unified Communications, telles que Cisco Unified Communications Manager (CUCM) ou UCXN, utilisent le protocole SAML version 2.0 dans la fonctionnalité SSO SAML. Afin d'authentifier l'utilisateur LDAP (Lightweight Directory Access Protocol), UCXN délègue une demande d'authentification à l'IDP. Cette requête d'authentification générée par l'UCXN est une requête SAML. L'IDP authentifie et renvoie une assertion SAML. L'assertion SAML affiche Oui (authentifié) ou Non (échec de l'authentification).

SAML SSO permet à un utilisateur LDAP de se connecter aux applications clientes avec un nom d'utilisateur et un mot de passe qui s'authentifient sur l'IdP. Une fois que vous avez activé la fonctionnalité SAML SSO, une connexion utilisateur à l'une des applications Web prises en charge sur les produits Unified Communication permet également d'accéder à ces applications Web sur UCXN (à l'exception de CUCM et CUCM IM and Presence) :

Utilisateurs Unity Connection	Applications Web
Utilisateurs LDAP avec droits d'administrateur	• Administration UCXN • Facilité de maintenance de Cisco UCXN • Cisco Unified Servicability • Cisco Personal Communications Assistant • Boîte de réception Web • Mini boîte de réception Web (version bureau)
Utilisateurs LDAP sans droits d'administrateur	• Cisco Personal Communications Assistant • Boîte de réception Web • Mini boîte de réception Web (version bureau)

- Clients Cisco Jabber

Configuration

Diagramme du réseau

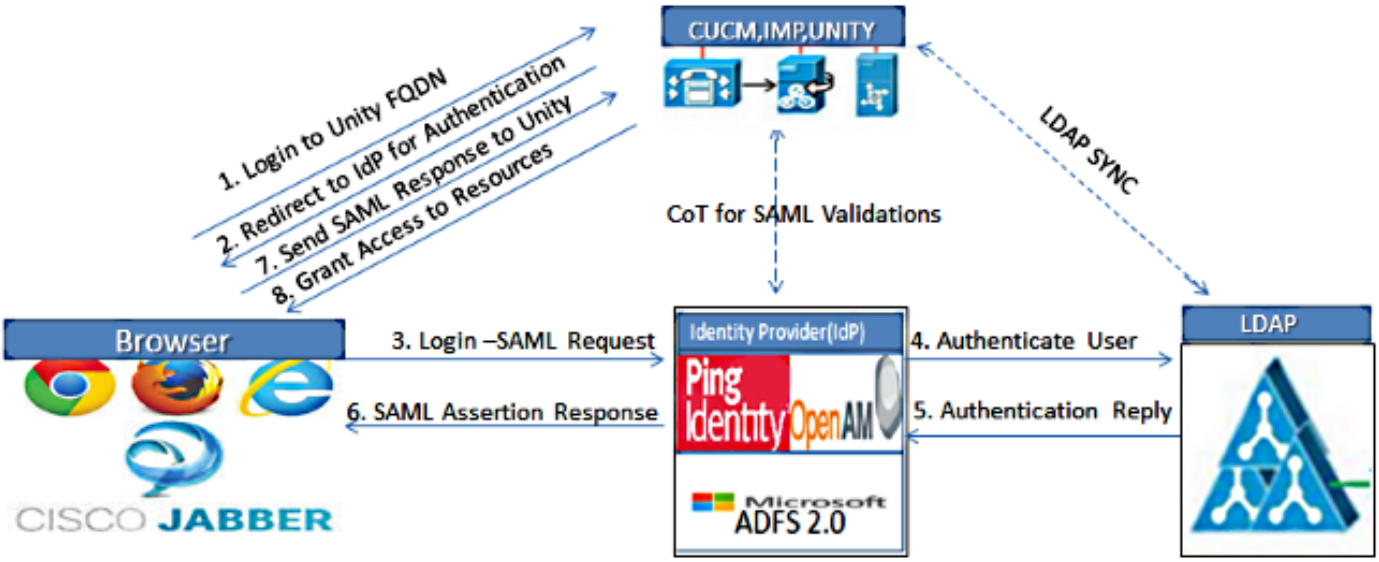
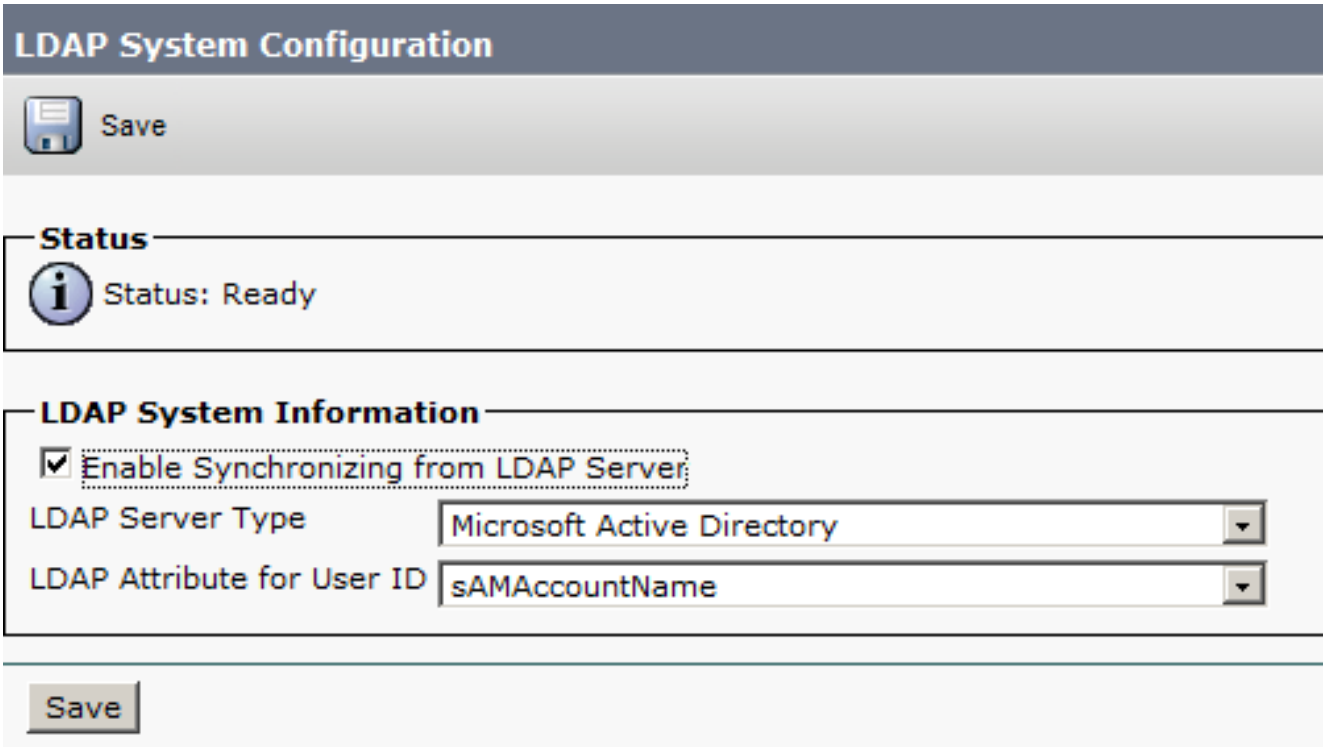


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Configuration du répertoire

1. Connectez-vous à la page Administration UCXN et sélectionnez **LDAP** et cliquez sur **Configuration LDAP**.

2. Cochez **Activer la synchronisation à partir du serveur LDAP** et cliquez sur **Enregistrer**.



3. Cliquez sur **LDAP**.

4. Cliquez sur **Configuration du répertoire LDAP**.

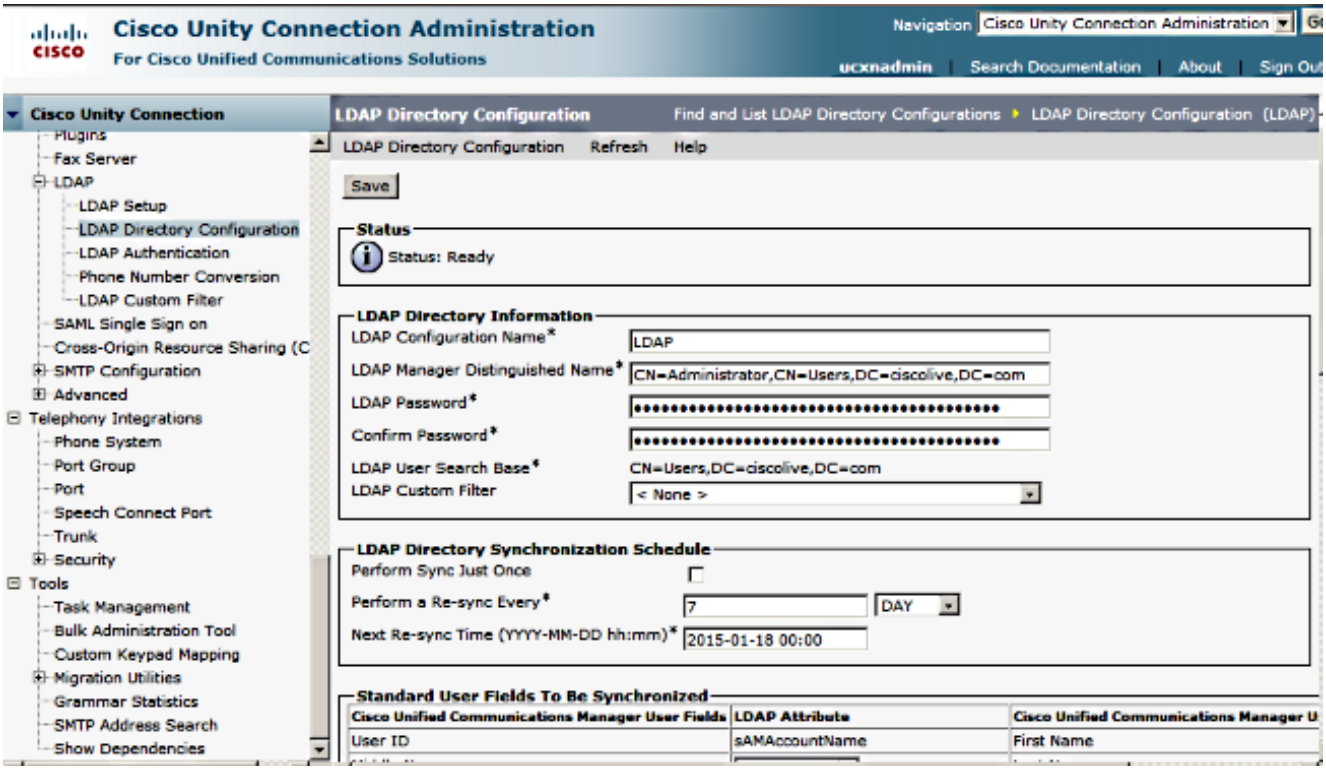
5. Cliquez sur **Ajouter nouveau**.

6. Configurez ces éléments :

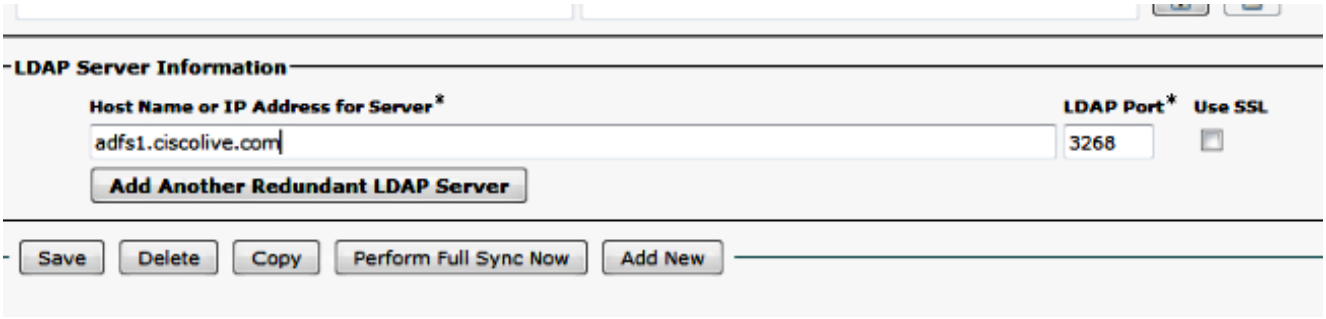
   Paramètres du compte d'annuaire LDAPAttributs utilisateur à synchroniserCalendrier de synchronisationNom d'hôte ou adresse IP du serveur LDAP et numéro de port

7. Cochez **Use SSL** si vous voulez utiliser SSL (Secure Socket Layer) afin de communiquer avec l'annuaire LDAP.

   Astuce : Si vous configurez LDAP sur SSL, téléchargez le certificat d'annuaire LDAP sur CUCM. Reportez-vous au contenu de l'annuaire LDAP dans Cisco Unified Communications Manager SRND pour plus d'informations sur le mécanisme de synchronisation des comptes pour des produits LDAP spécifiques et les meilleures pratiques générales pour la synchronisation LDAP.



8. Cliquez sur **Exécuter la synchronisation complète maintenant**.



Note: Assurez-vous que **Cisco DirSync** est activé dans la page Web de maintenance avant de cliquer sur Enregistrer.

9. Développez **Utilisateurs** et sélectionnez **Importer des utilisateurs**.

10. Dans la liste **Rechercher les utilisateurs finaux de Unified Communications Manager**, sélectionnez **Répertoire LDAP**.

11. Si vous souhaitez importer uniquement un sous-ensemble des utilisateurs dans l'annuaire LDAP avec lequel vous avez intégré UCXN, saisissez les spécifications applicables dans les champs de recherche.

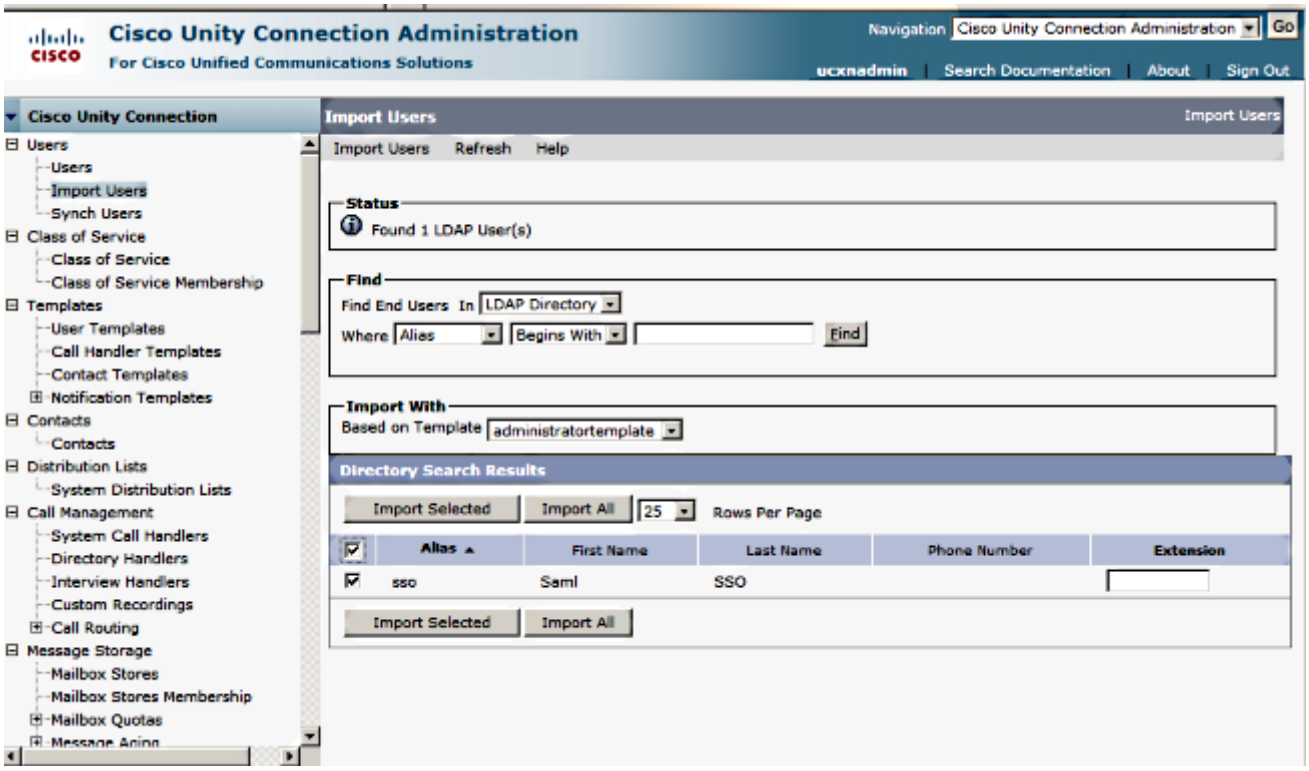
12. Sélectionnez **Rechercher**.

13. Dans la liste Basé sur le modèle, sélectionnez le **modèle Administrateur** que UCXN doit utiliser lorsqu'il crée les utilisateurs sélectionnés.

    Attention : Si vous spécifiez un modèle administrateur, les utilisateurs ne disposeront pas

de boîtes aux lettres.

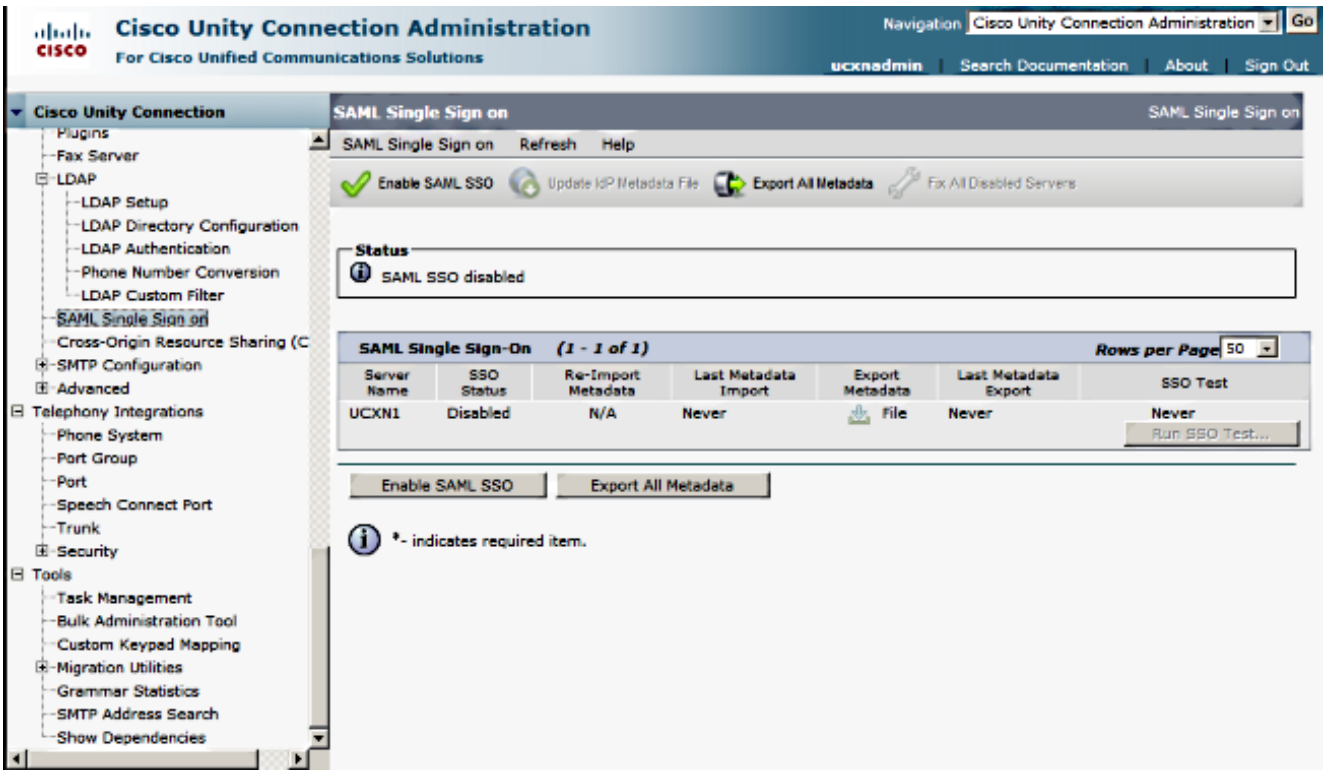
14. Cochez les cases correspondant aux utilisateurs LDAP pour lesquels vous souhaitez créer des utilisateurs UCXN et cliquez sur **Importer la sélection**.



Activer SAML SSO

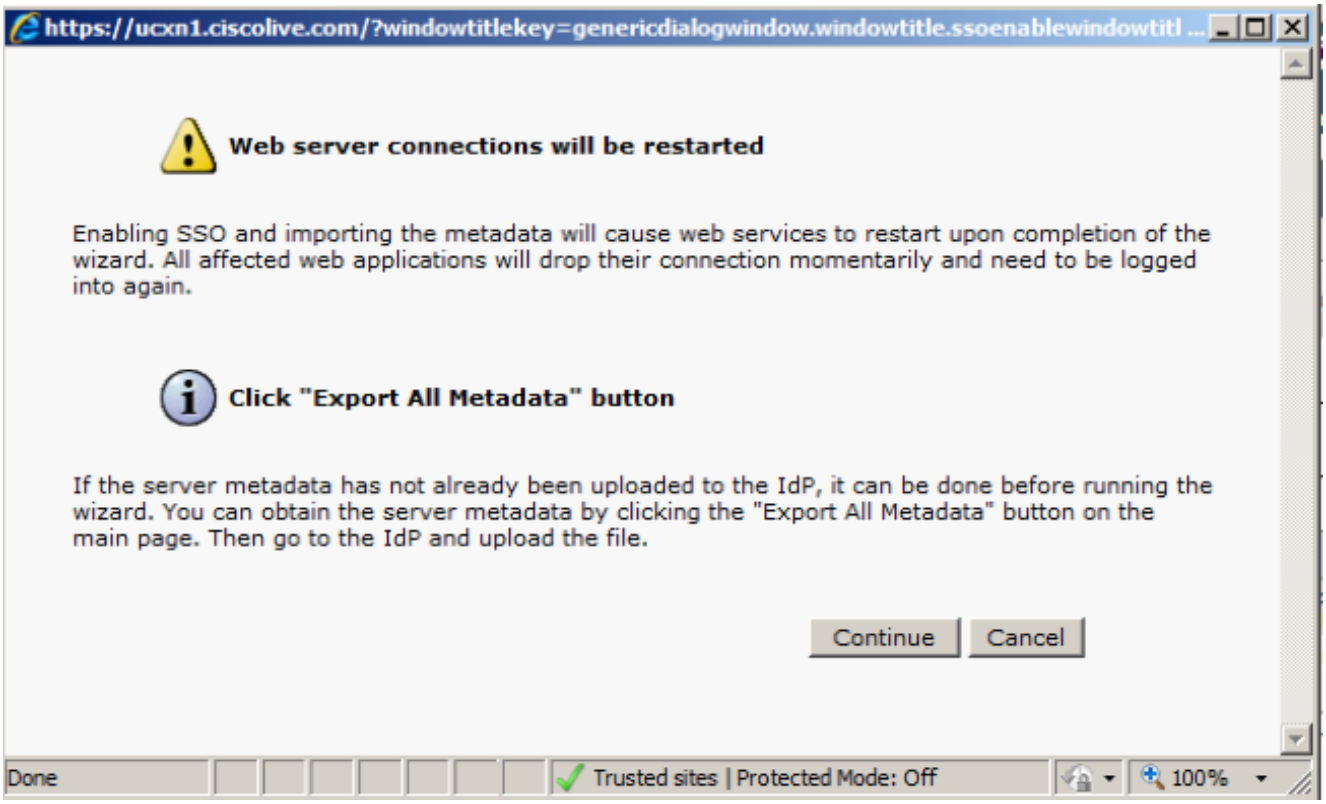
1. Connectez-vous à l'interface utilisateur UCXN Administration.

2. Choisissez **System > SAML Single Sign-on** et la fenêtre SAML SSO Configuration s'ouvre.

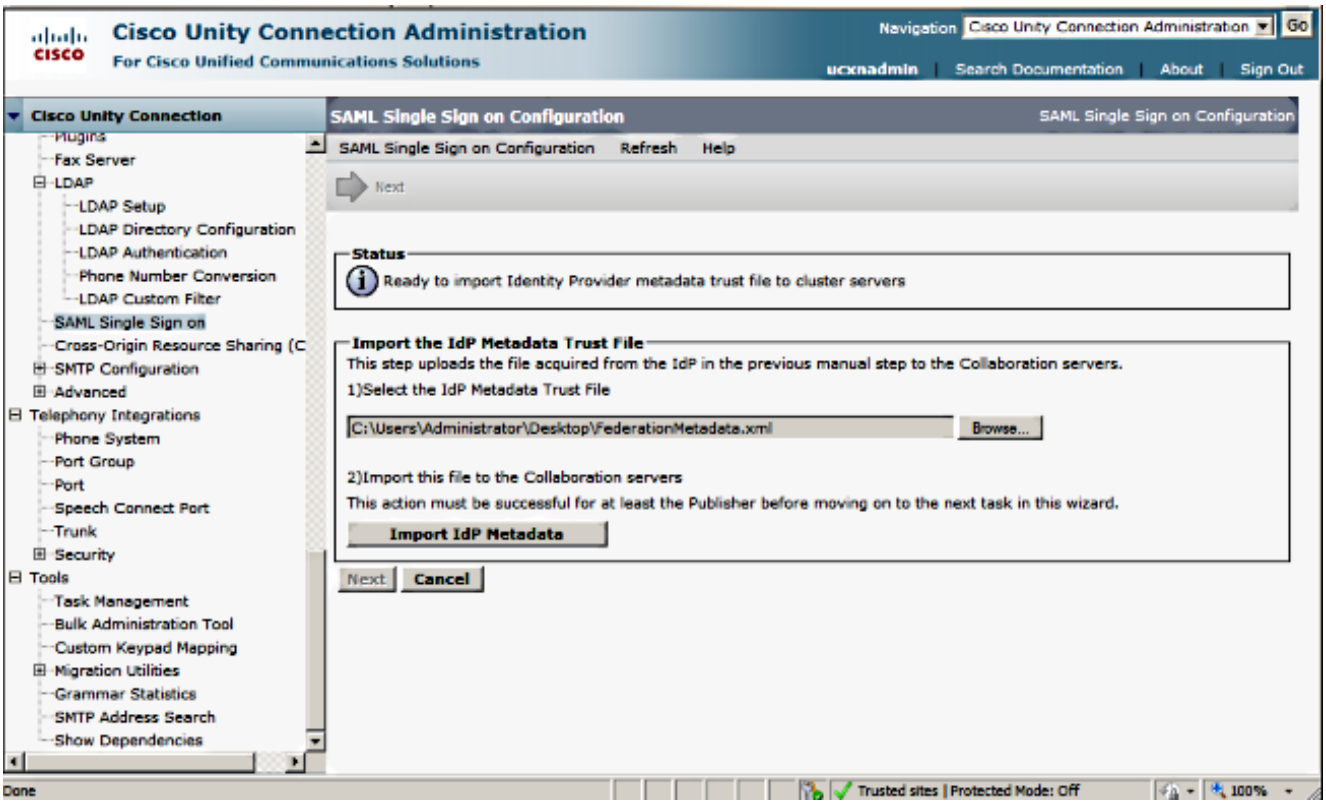


3. Afin d'activer SAML SSO sur le cluster, cliquez sur **Enable SAML SSO**.

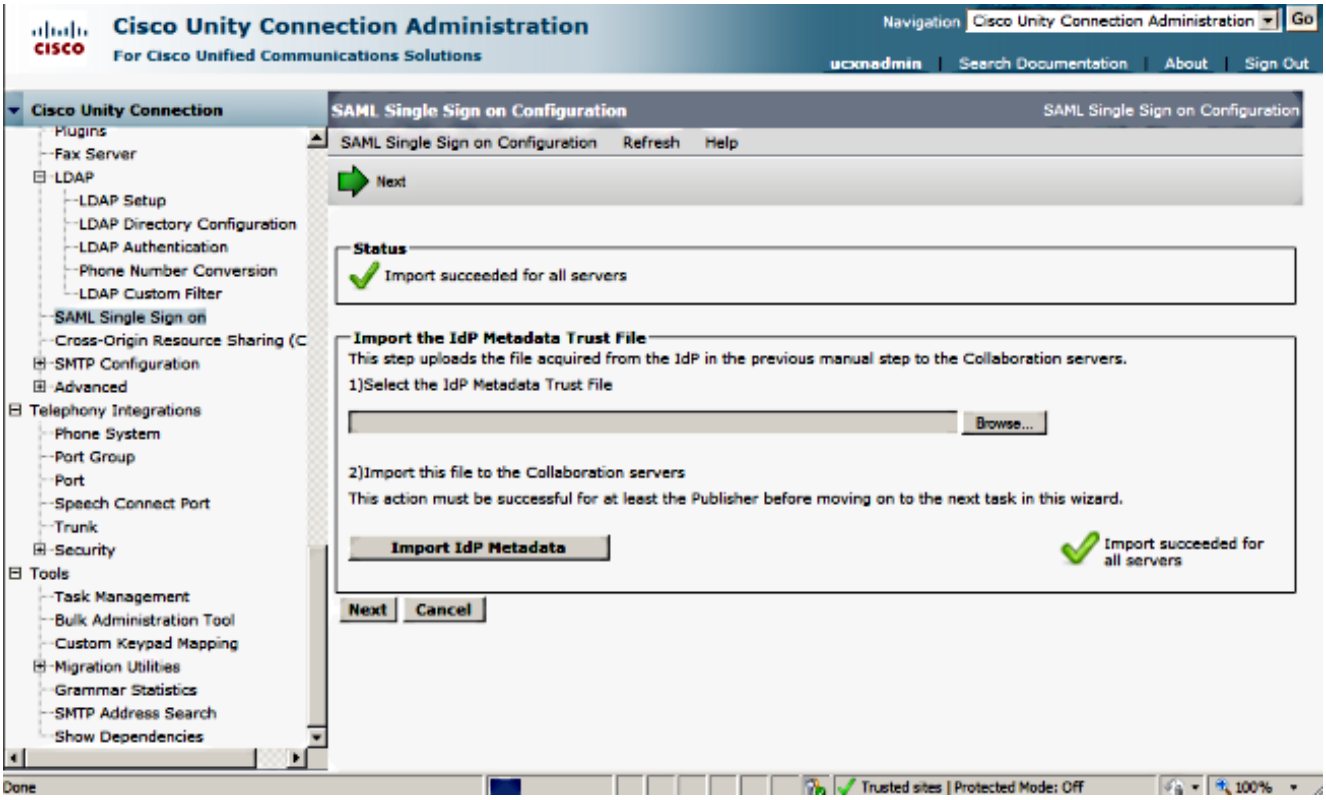
4. Dans la fenêtre Avertissement de réinitialisation, cliquez sur **Continuer.**



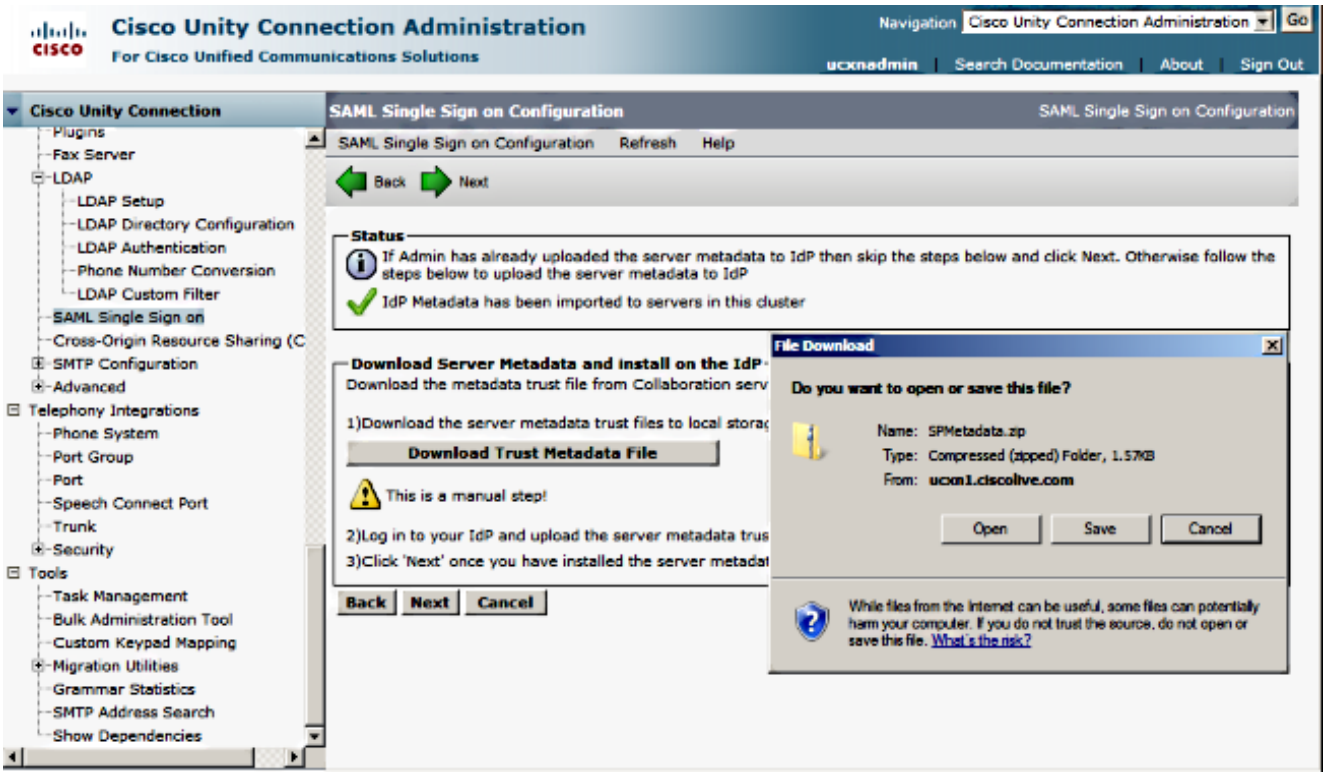
5. Dans l'écran SSO, cliquez sur **Parcourir** afin d'importer le fichier XML de métadonnées **FederationMetadata.xml** à l'aide de l'étape **Télécharger les métadonnées Idp**.



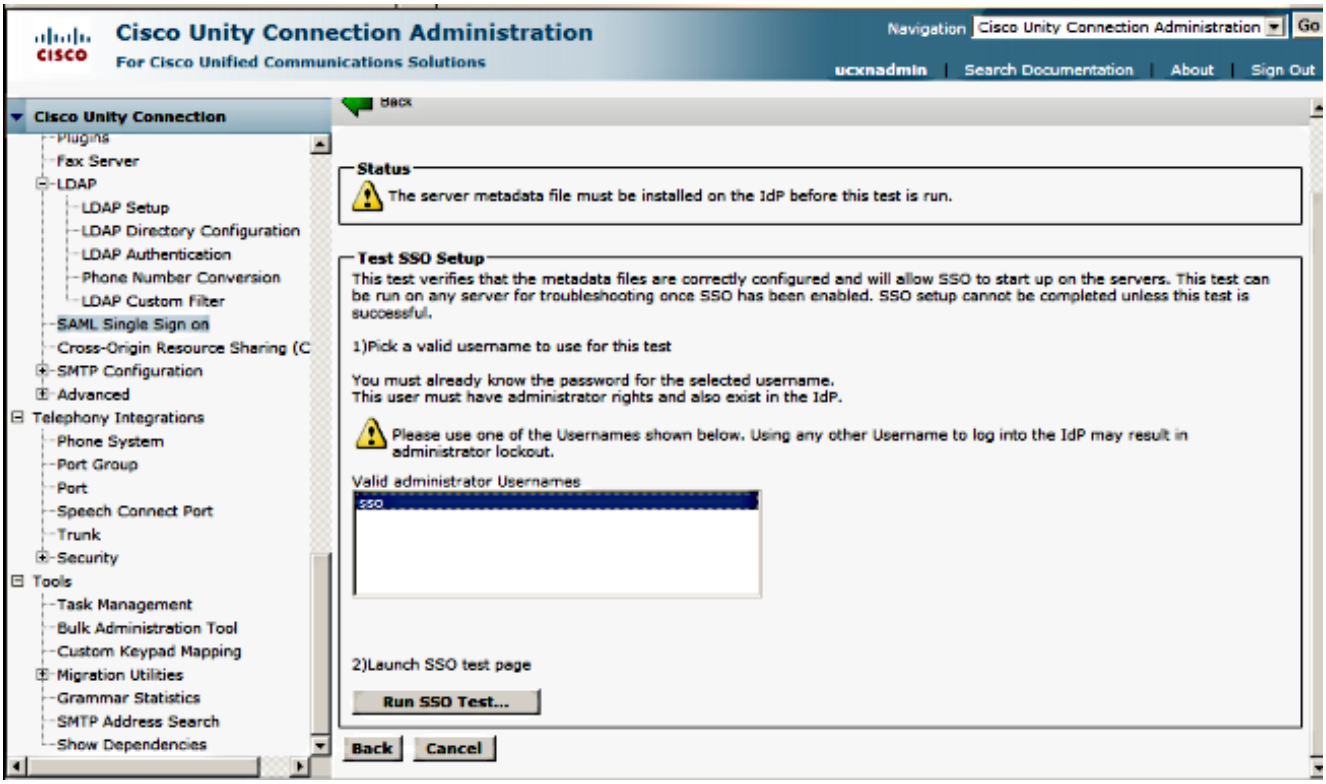
6. Une fois le fichier de métadonnées téléchargé, cliquez sur **Import IdP Metadata** afin d'importer les informations IdP dans UCXN. Vérifiez que l'importation a réussi et cliquez sur **Suivant** pour continuer.



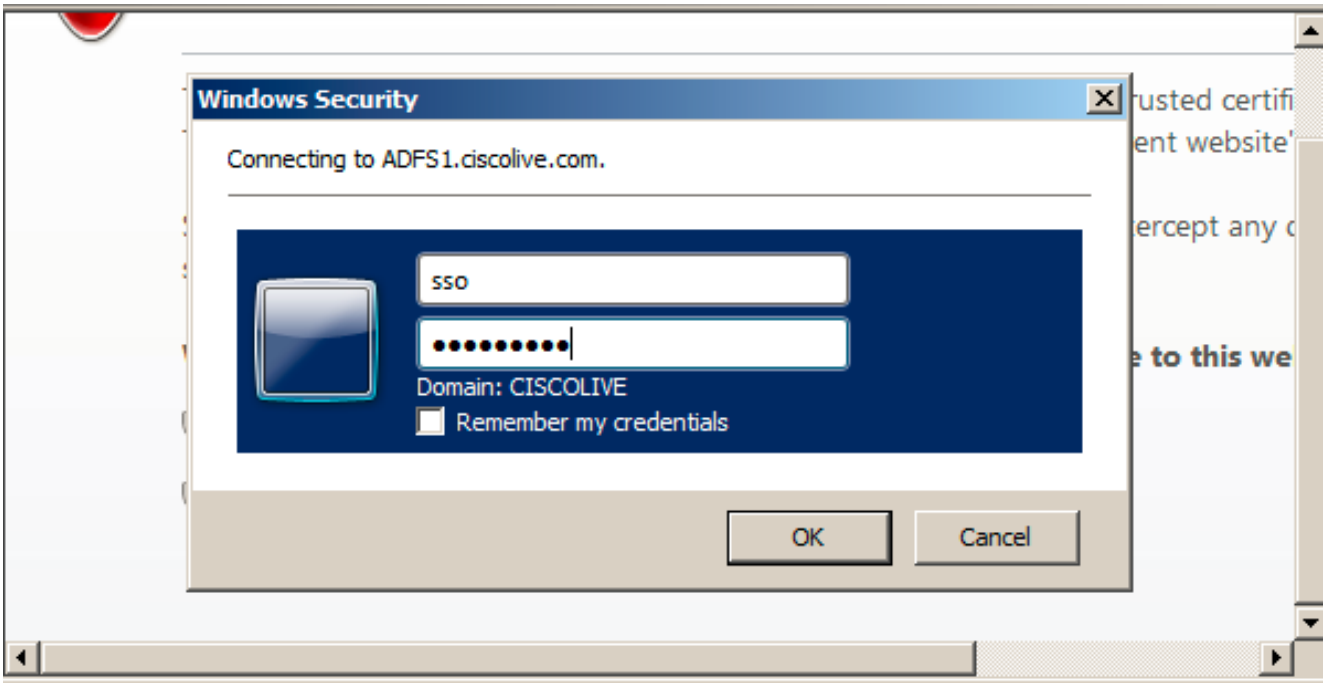
7. Cliquez sur **Download Trust Metadata Fileset** (effectuez cette opération uniquement si vous n'avez pas configuré ADFS déjà avec des métadonnées UCXN) afin d'enregistrer les métadonnées UCXN dans un dossier local et accédez à [Ajouter UCXN comme approbation de partie relais](). Une fois la configuration AD FS terminée, passez à l'étape 8.



8. Sélectionnez **SSO** comme utilisateur administratif et cliquez sur **Exécuter le test SSO**.

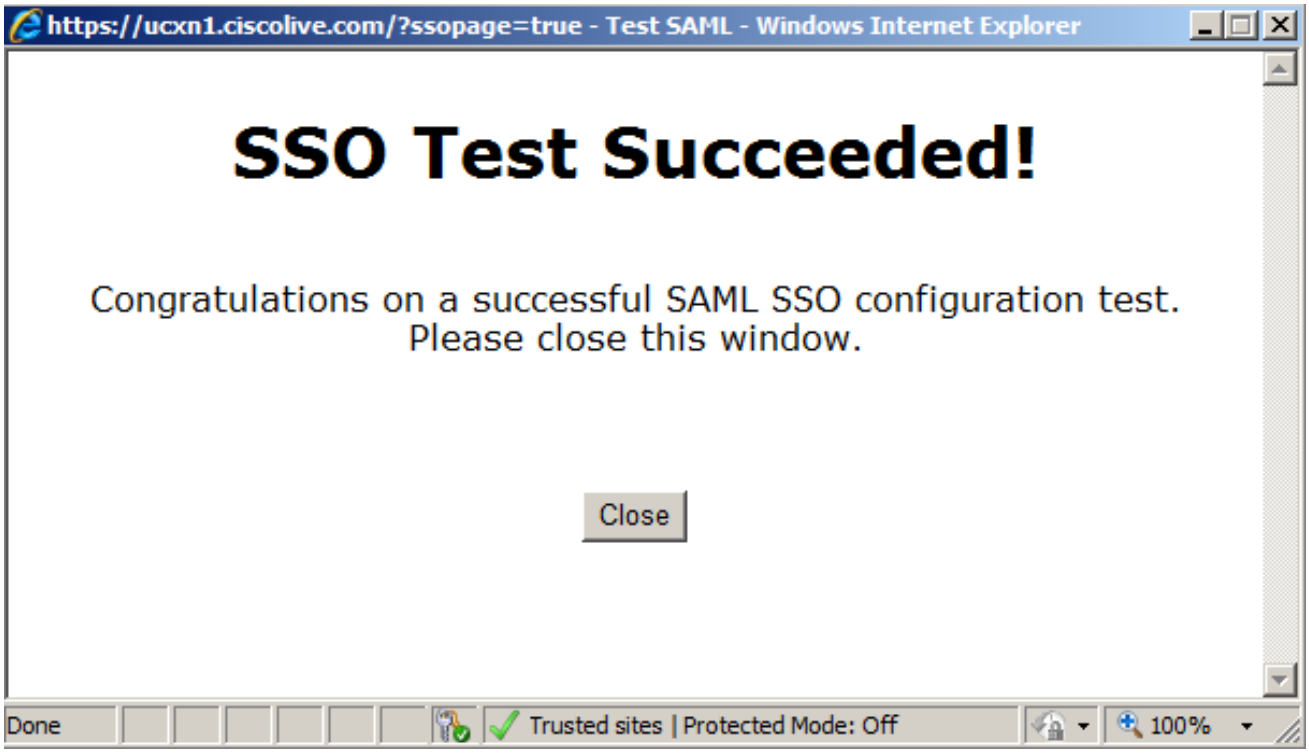


9. Ignorez les avertissements de certificat et poursuivez. Lorsque vous êtes invité à saisir des informations d'identification, saisissez le nom d'utilisateur et le mot de passe de l'utilisateur SSO, puis cliquez sur **OK**.



Note: Cet exemple de configuration est basé sur des certificats autosignés UCXN et AD FS. Si vous utilisez des certificats d'autorité de certification, les certificats appropriés doivent être installés sur AD FS et UCXN. Référez-vous à Gestion et validation des certificats pour plus d'informations.

10. Une fois toutes les étapes terminées, vous recevez le « Test SSO réussi ! » message. Cliquez sur **Fermer** et **Terminer** pour continuer.



Vous avez maintenant terminé les tâches de configuration pour activer SSO sur UCXN avec AD FS.

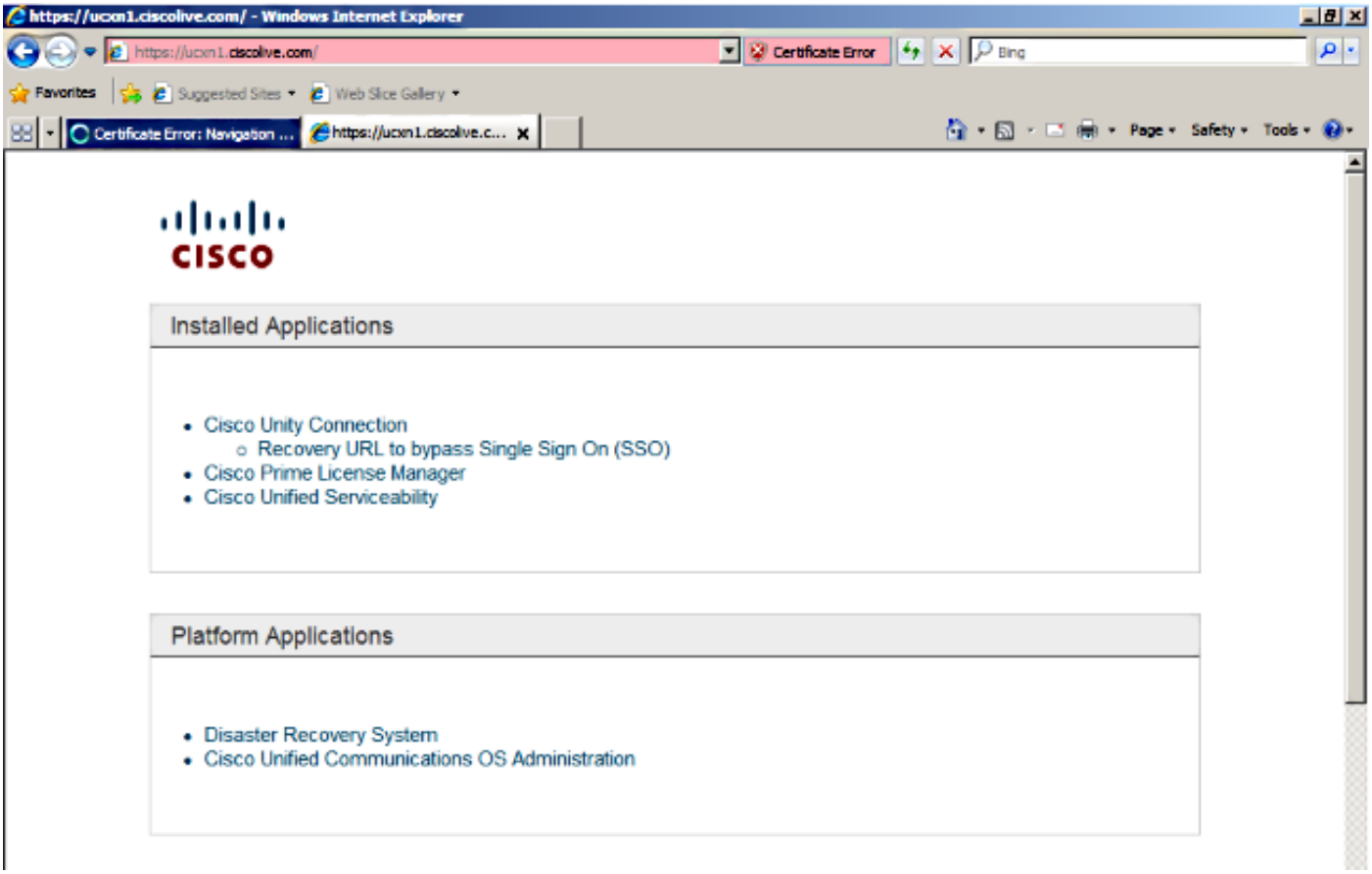
Note obligatoire : Exécutez le test SSO pour UCXN Subscriber s'il s'agit d'un cluster afin d'activer SAML SSO. AD FS doit être configuré pour tous les noeuds d'UCXN dans un cluster.

Astuce : Si vous configurez les fichiers XML de métadonnées de tous les noeuds sur IdP et que vous commencez à activer l'opération SSO sur un noeud, SAML SSO sera activé automatiquement sur tous les noeuds du cluster.

Vous pouvez également configurer CUCM et CUCM IM and Presence pour SAML SSO si vous voulez utiliser SAML SSO pour les clients Cisco Jabber et offrir une véritable expérience SSO aux utilisateurs finaux.

Vérification

Ouvrez un navigateur Web et saisissez le nom de domaine complet d'UCXN. Une nouvelle option apparaît sous Applications installées, appelée **URL de récupération, pour contourner l'authentification unique (SSO)**. Une fois que vous avez cliqué sur le lien **Cisco Unity Connection**, les services AD FS vous demandent des informations d'identification. Une fois que vous avez entré les informations d'identification de l'utilisateur SSO, vous serez connecté correctement à la page Unity Administration, page Unified Serviceability.



Note: SAML SSO n'active pas l'accès à ces pages :
- Gestionnaire de licences Prime
- Administration du système d'exploitation
- Système de reprise après sinistre

Dépannage

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

Référez-vous à Dépannage SAML SSO pour les produits de collaboration 10.x pour plus d'informations.