

Unity Connection バージョン 10.5 SAML SSO 設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[Network Time Protocol \(NTP \) の設定](#)

[ドメイン ネーム サーバ \(DNS \) の設定](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ディレクトリ セットアップ](#)

[SAML SSO の有効化](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Unity Connection (UCXN) 用の Security Assertion Markup Language (SAML) シングル サインオン (SSO) の設定と検証の方法について説明します。

前提条件

要件

Network Time Protocol (NTP) の設定

SAML SSO を動作させるには、正しい NTP 設定をインストールする必要があり、ID プロバイダー (IdP) と Unified Communications アプリケーションの間の時間差が 3 秒を超えていないことを確認する必要があります。クロックの同期については、[Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド \[英語\]](#) で、NTP の設定についての項を参照してください。

ドメイン ネーム サーバ (DNS) の設定

Unified Communications アプリケーションは、完全修飾ドメイン名を IP アドレスに解決するために DNS を使用することができます。サービス プロバイダーと IdP は、ブラウザにより確定できる必要があります。

SAML 要求を処理するには、Active Directory フェデレーション サービス (AD FS) バージョン 2.0 をインストールおよび設定しておく必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IdP としての AD FS バージョン 2.0
- サービスプロバイダーとしての UCXN
- Microsoft Internet Explorer バージョン 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

SAML は、XML をベースとしたオープン スタンダードのデータ交換形式です。サービスプロバイダーによってユーザの認証に使用される認証プロトコルです。IdP とサービスプロバイダーとの間で、セキュリティ認証情報がやり取りされます。

オープン スタンダードである SAML を使用すると、クライアントはそのプラットフォームの種類に関係なく、SAML 対応のどのようなコラボレーション（またはユニファイド コミュニケーション）サービスに対しても認証を実行できます。

Cisco Unified Communications Manager (CUCM)、UCXN など、あらゆる Cisco Unified Communications Web インターフェイスでは、SAML SSO 機能の SAML バージョン 2.0 プロトコルを使用します。Lightweight Directory Access Protocol (LDAP) ユーザを認証する場合、UCXN は認証要求を IdP に委任します。UCXN が生成するこのような認証要求を、SAML 要求と呼びます。IdP は認証を実行し、SAML アサーションを返します。SAML アサーションは、Yes (認証成功) または No (認証失敗) のいずれかを示します。

SAML SSO を有効化すると、LDAP ユーザは IdP での認証に使用したユーザ名とパスワードで、クライアント アプリケーションにログインできます。ユニファイド コミュニケーション製品でサポートされるいずれかの Web アプリケーションにサインインしたユーザは、SAML SSO 機能が有効化されると、UCXN 上のこれらの Web アプリケーションにもアクセスできるようになります (ただし CUCM、CUCM IM とプレゼンスを除く)。

Unity Connection ユーザ	Web アプリケーション
	<ul style="list-style-type: none">• UCXN Administration• Cisco UCXN Serviceability• Cisco Unified サービスアビリティ
管理者権限を持つ LDAP ユーザ	<ul style="list-style-type: none">• Cisco Personal Communications Assistant• Web Inbox• Mini Web Inbox (デスクトップ バージョン)• Cisco Personal Communications Assistant• Web Inbox
管理者権限のない LDAP ユーザ	<ul style="list-style-type: none">• Mini Web Inbox (デスクトップ バージョン)• Cisco Jabber クライアント

設定

ネットワーク図

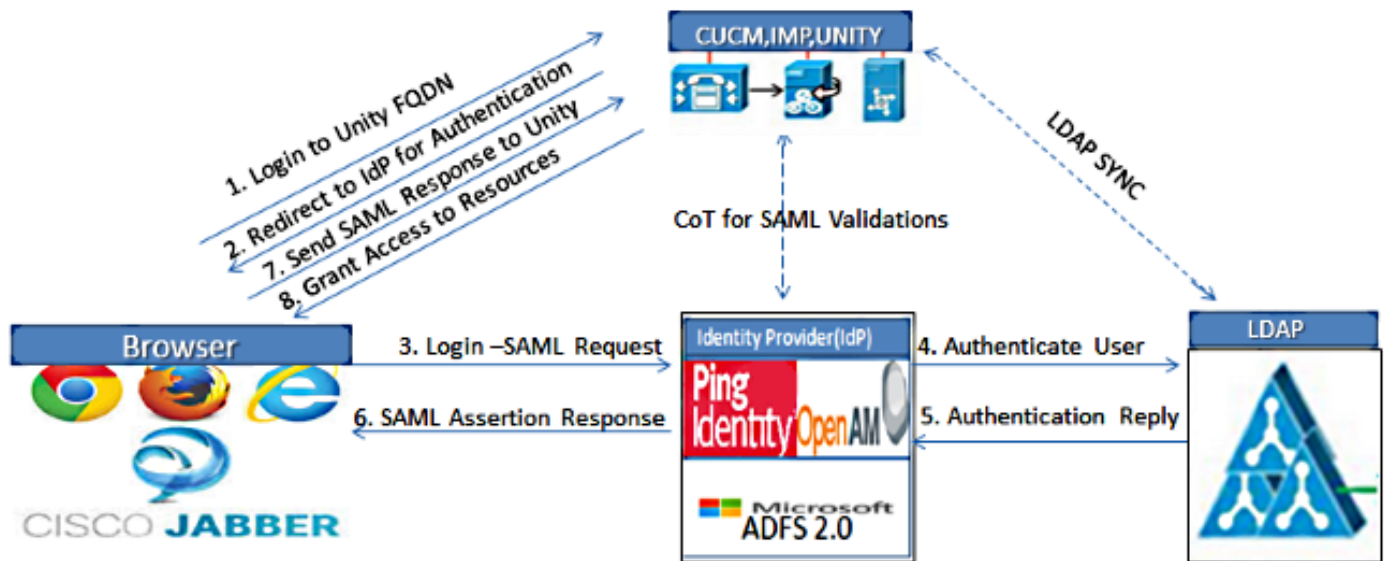



Figure :SAML Single sign SSO Call Flow for Collaboration Servers


ディレクトリ セットアップ

1. [UCXN Administration] ページにサインインし、[LDAP] を選択して、[LDAP Setup] をクリックします。
2. [Enable Synchronizing from LDAP Server] チェックボックスをオンにし、[Save] をクリックします。

LDAP System Configuration

 Save

Status


 Status: Ready

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

LDAP Attribute for User ID

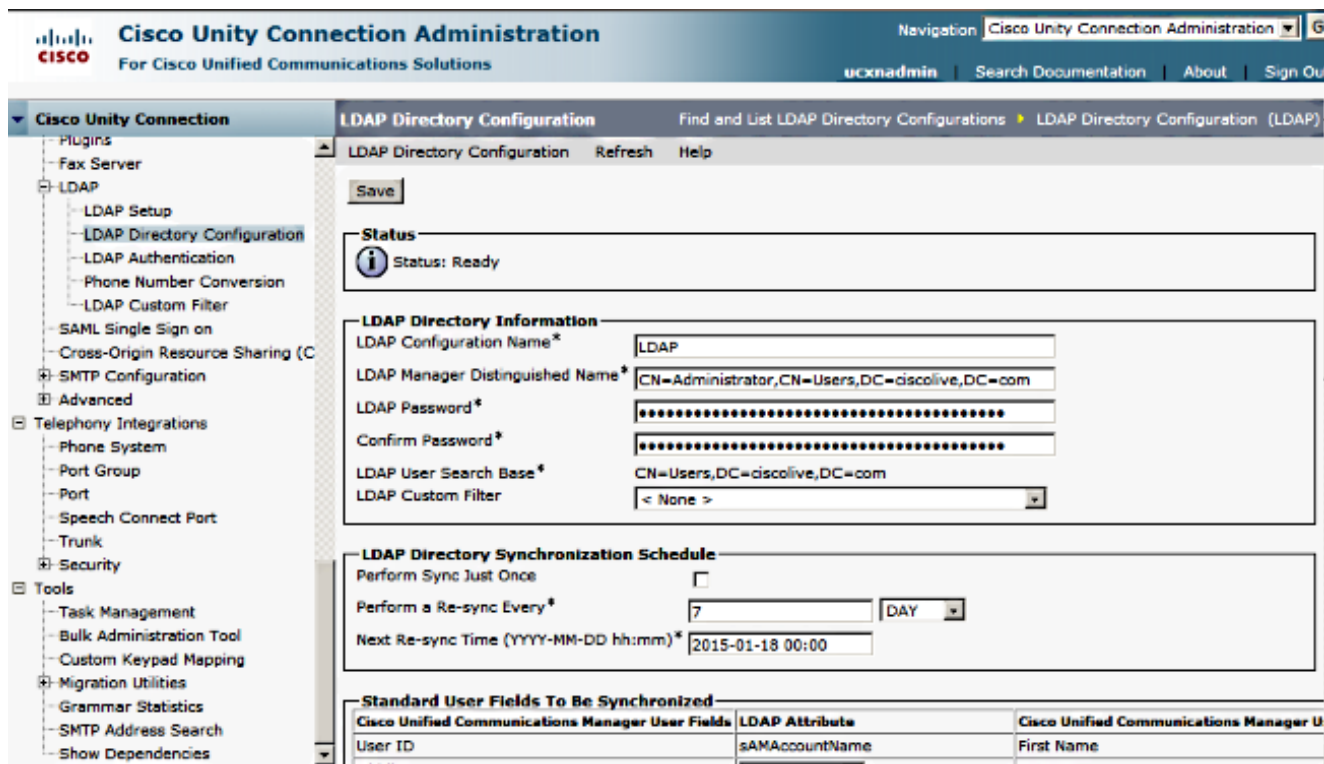
 Save

3. [LDAP] をクリックします。
4. [LDAP Directory Configuration] をクリックします。
5. [Add New] をクリックします。
6. 次の項目を設定します。

LDAP ディレクトリ アカウント設定同期対象のユーザ属性同期スケジュールLDAP サーバの
 ホスト名、または IP アドレスおよびポート番号

7. Secure Socket Layer (SSL) を使用して LDAP ディレクトリと通信するには、[Use SSL] を
 オンにします。

ヒント : LDAP over SSL を設定するには、LDAP ディレクトリ証明書を CUCM にアップロ
 ードします。特定の LDAP 製品のアカウント同期メカニズム、および LDAP 同期の一般的
 なベスト プラクティスの詳細については、[Cisco Unified Communications Manager SRND
 の LDAP ディレクトリの情報を参照してください。](#)



8. [Perform Full Sync Now] をクリックします。

LDAP Server Information

Host Name or IP Address for Server*
adfs1.ciscolive.com

LDAP Port*
3268

Use SSL

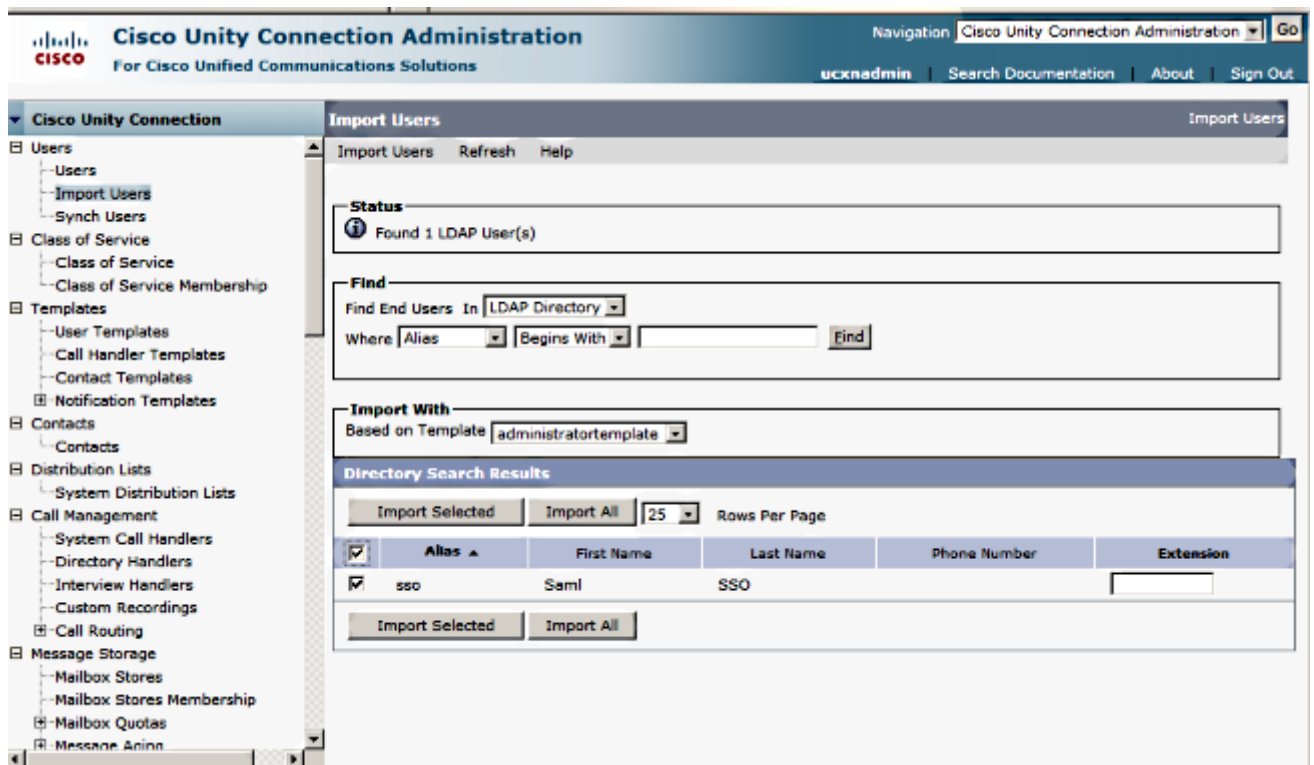
Add Another Redundant LDAP Server

Save Delete Copy Perform Full Sync Now Add New

注：[Save] をクリックする前に、Cisco DirSync サービスが Serviceability Web ページで有効になっていることを確認します。

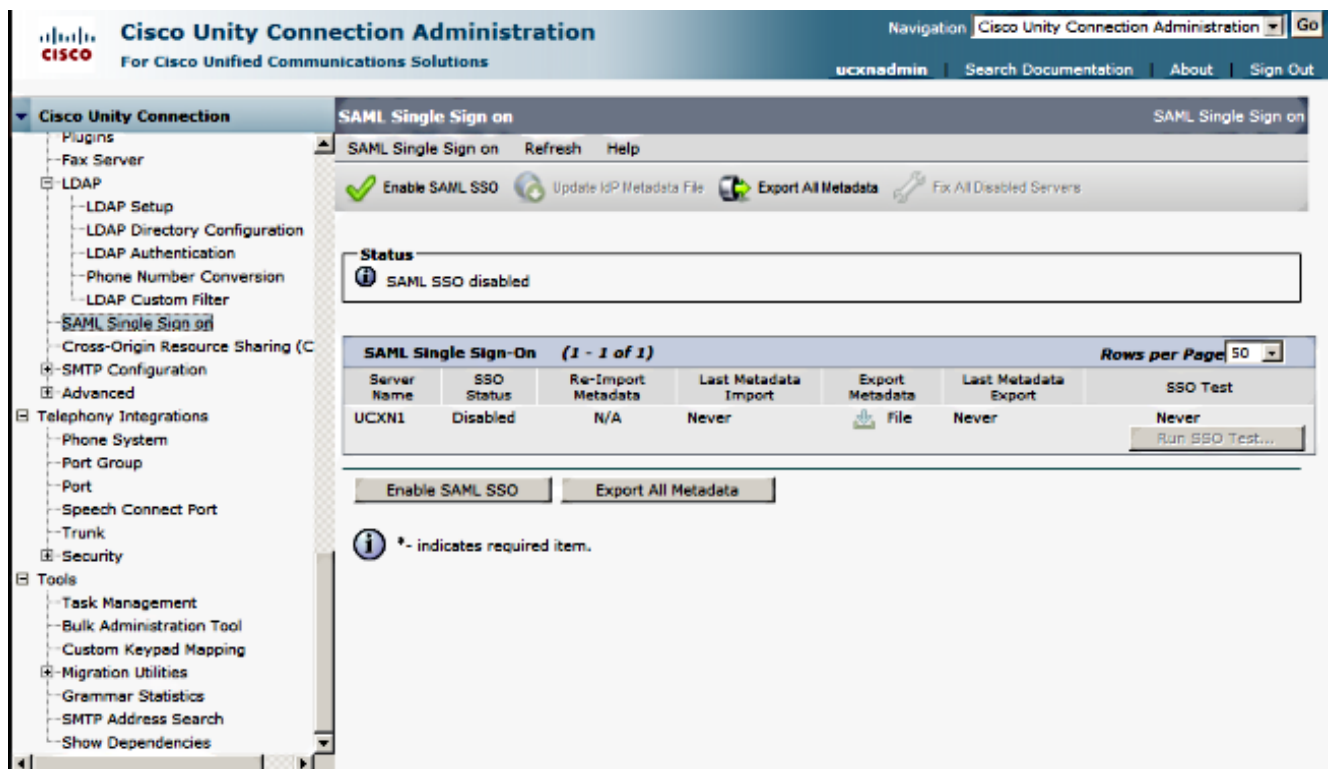
9. [Users] を展開して、[Import Users] を選択します。
10. [Find Unified Communications Manager End Users] リストから、[LDAP Directory] を選択します。
11. UCXN を統合した LDAP ディレクトリからユーザのサブセットのみをインポートする場合は、検索フィールドに該当する条件を入力します。
12. [Find] を選択します。
13. [Based on Template] リストから、選択したユーザの作成時に UCXN で使用するための管理者テンプレートを選択します。

注意：管理者テンプレートを指定した場合、ユーザはメールボックスを持たなくなります。
14. UCXN ユーザを作成する LDAP ユーザのチェックボックスをオンにし、[Import Selected] をクリックします。

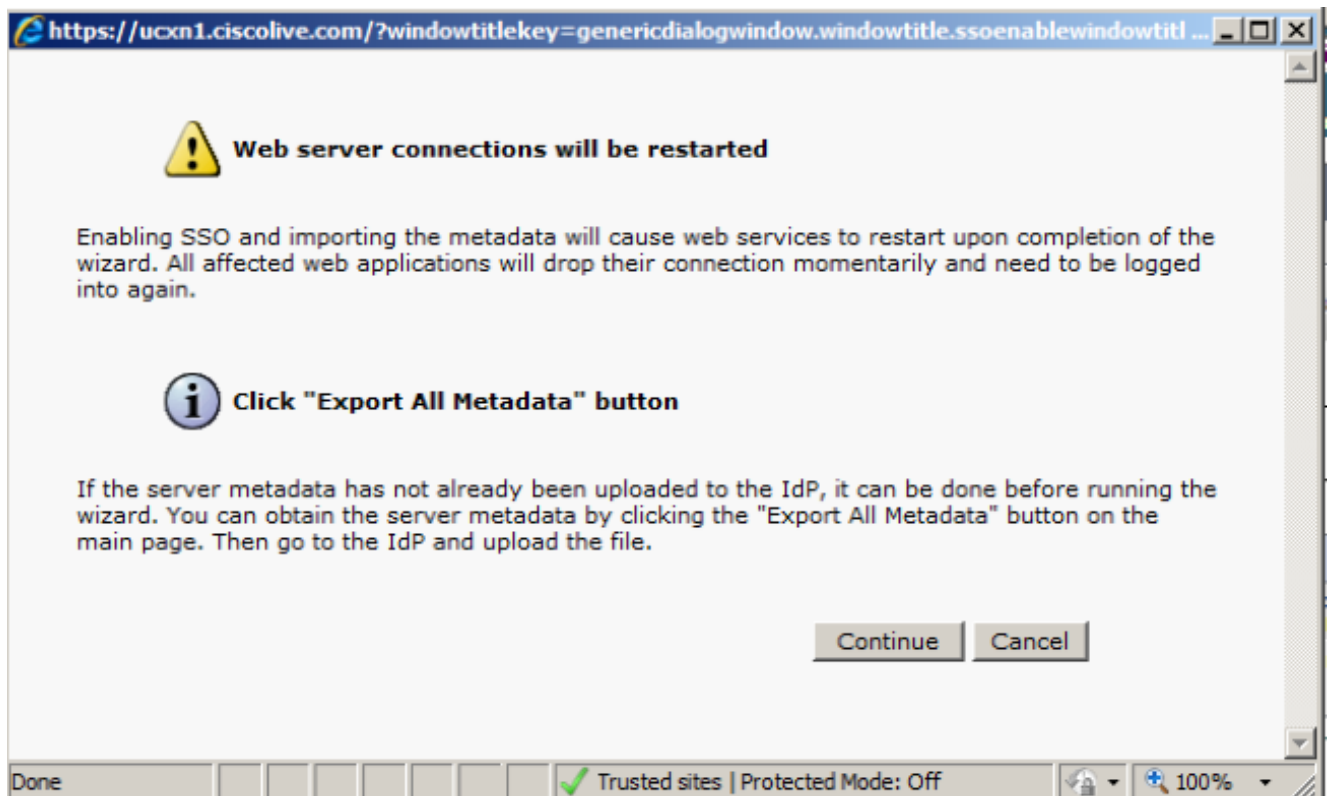


SAML SSO の有効化

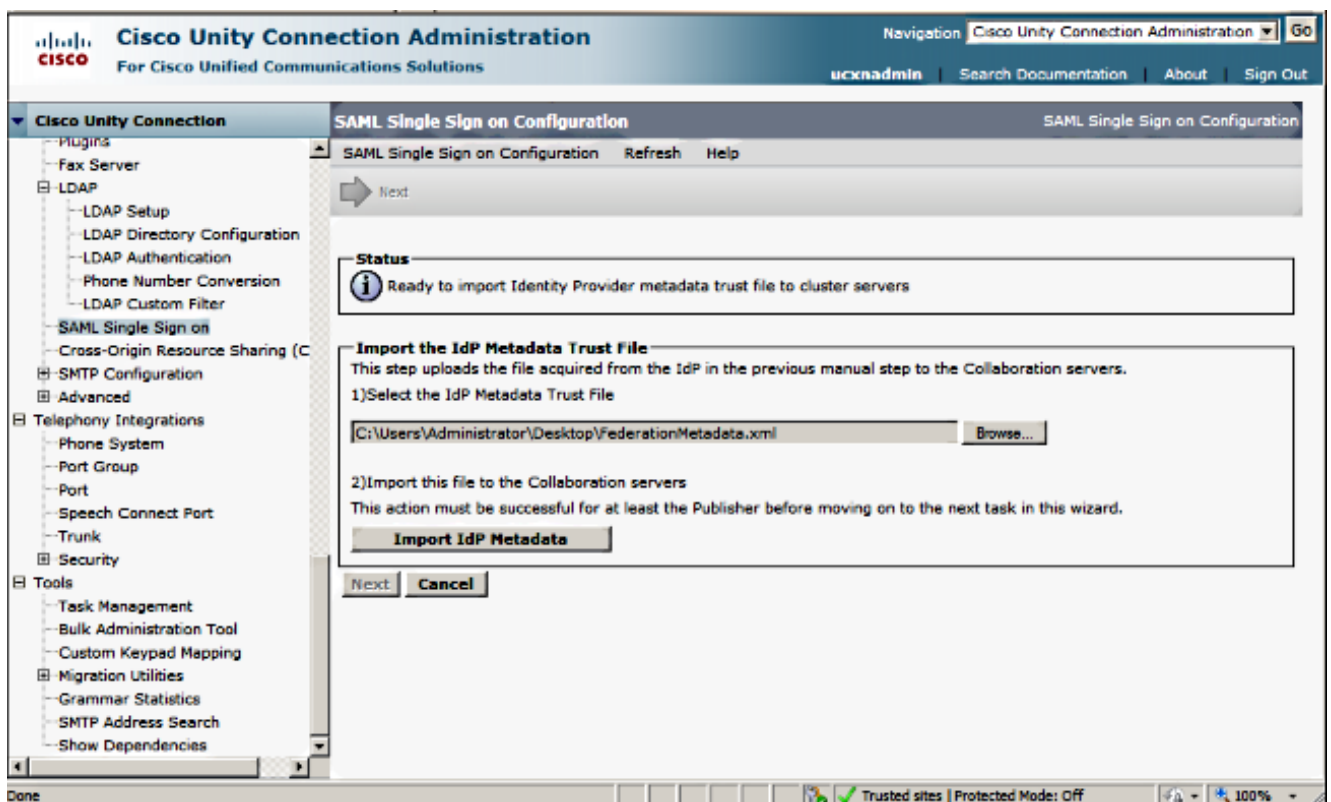
1. UCXN 管理ユーザ インターフェイスにログインします。
2. [System] > [SAML Single Sign-on] の順にクリックすると、[SAML SSO Configuration] ウィンドウが開きます。



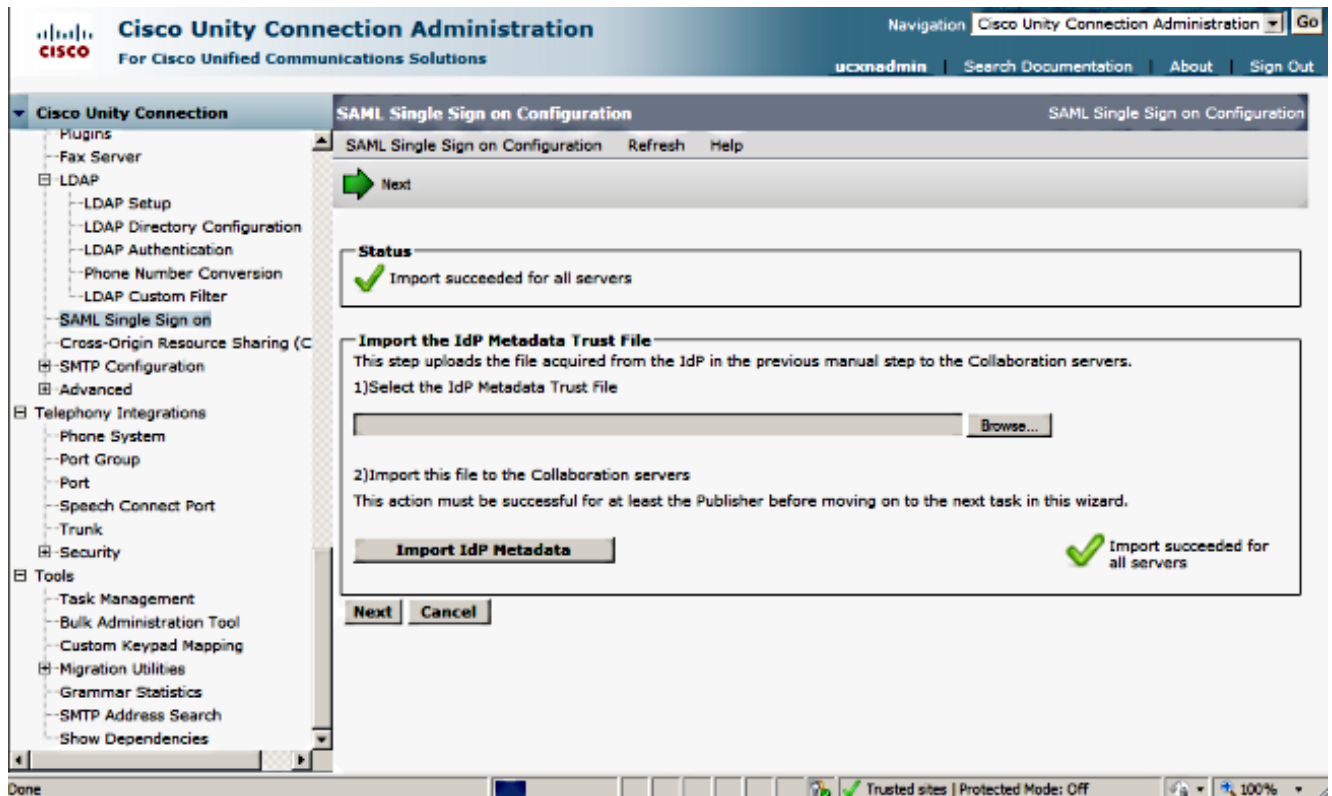
3. クラスタで SAML SSO を有効にするには、[Enable SAML SSO] をクリックします。
4. [Reset Warning] ウィンドウで [Continue] をクリックします。



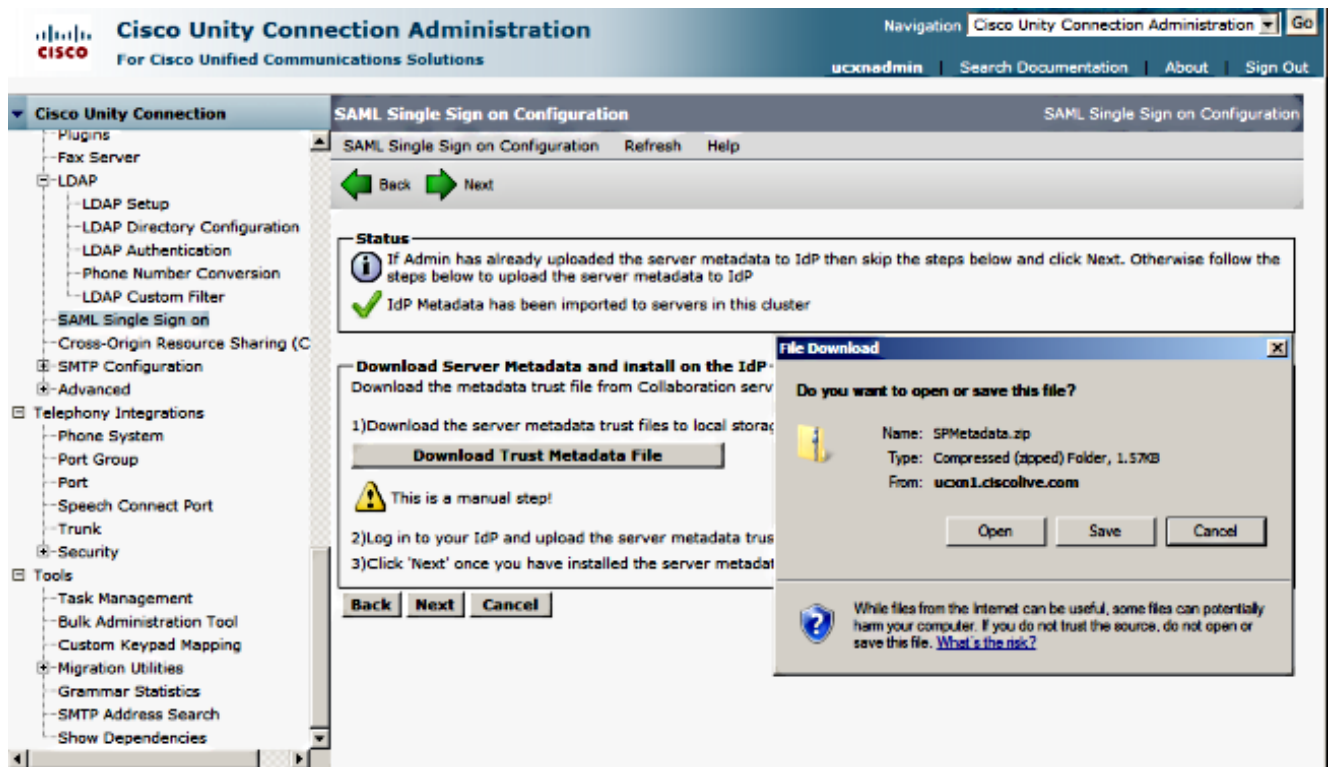
5. SSO画面で[Browse]をクリックし、FederationMetadata.xmlメタデータXMLファイルを[Download Idp Metadata]ステップを使用してインポートします。



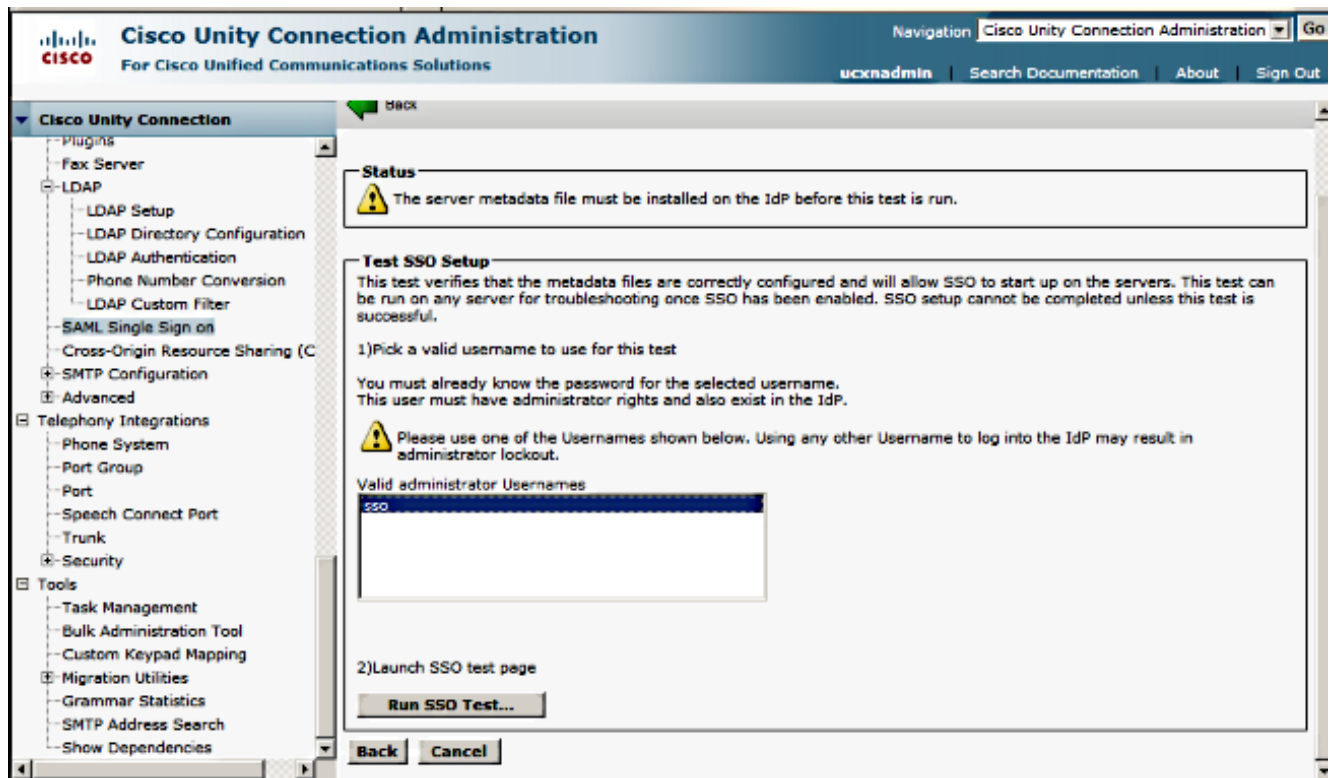
6. メタデータファイルがアップロードされたら、[Import IdP Metadata] をクリックして IdP 情報を UCXN にインポートします。インポートが成功したことを確認し、[Next] をクリックして続行します。



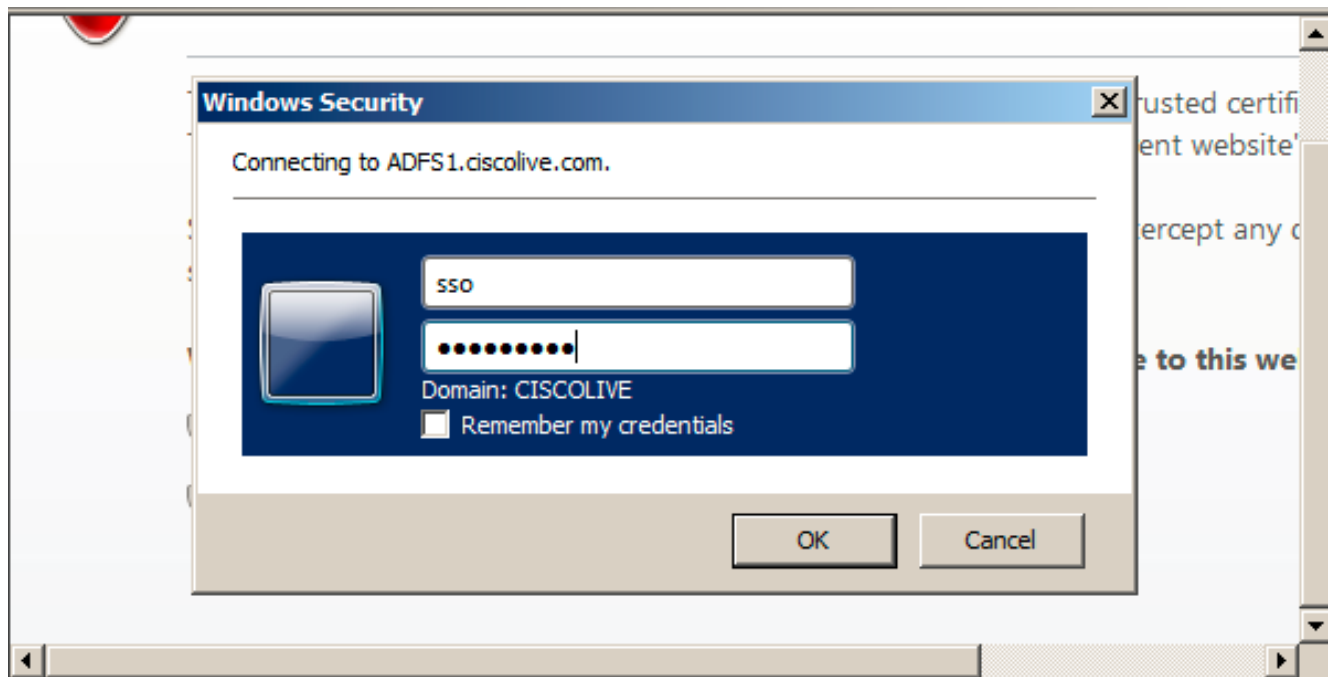
7. [Download Trust Metadata Fileset] をクリックして (UCXN メタデータによる ADFS の設定がまだ済んでない場合のみ)、UCXN メタデータをローカルフォルダに保存し、[Add UCXN as Relaying Party Trust](#) に移動します。AD FS 設定が完了したら、手順 8 に進みます。



8. 管理ユーザとして SSO を選択し、Run SSO Test をクリックします。

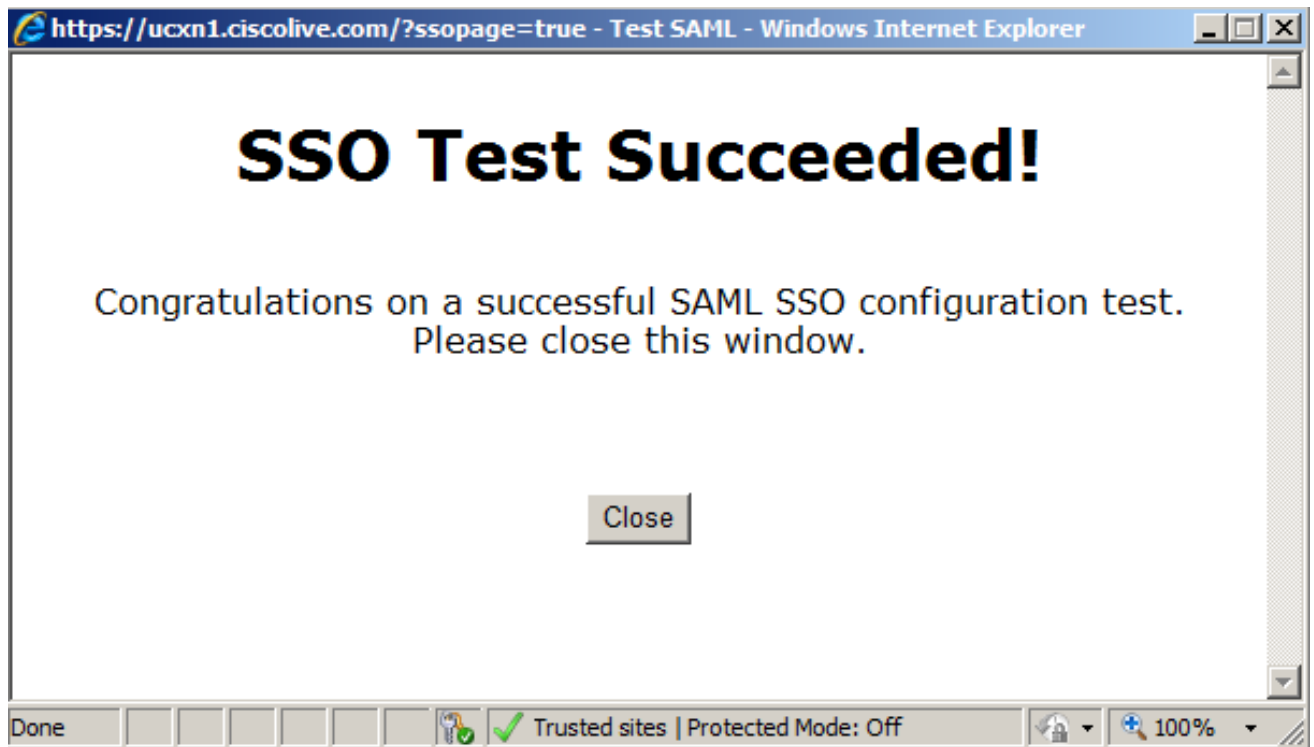


9. 証明書に関する警告は無視し、次に進みます。クレデンシャルの入力を促されたら、ユーザ SSO のユーザ名およびパスワードを入力し、[OK] をクリックします。



注：この設定例は、UCXN と AD FS 自己署名証明書に基づいています。認証局 (CA) の証明書を使用する場合、適切な証明書を AD FS と UCXN の両方にインストールする必要があります。詳細については、「[証明書の管理と検証](#)」を参照してください。

10. すべての手順が完了すると、「SSO Test Succeeded!」メッセージに応答します。[Close]、[Finish] の順にクリックして続行します。



以上で、AD FS を使用して UCXN で SSO を有効にするための設定作業が完了しました。

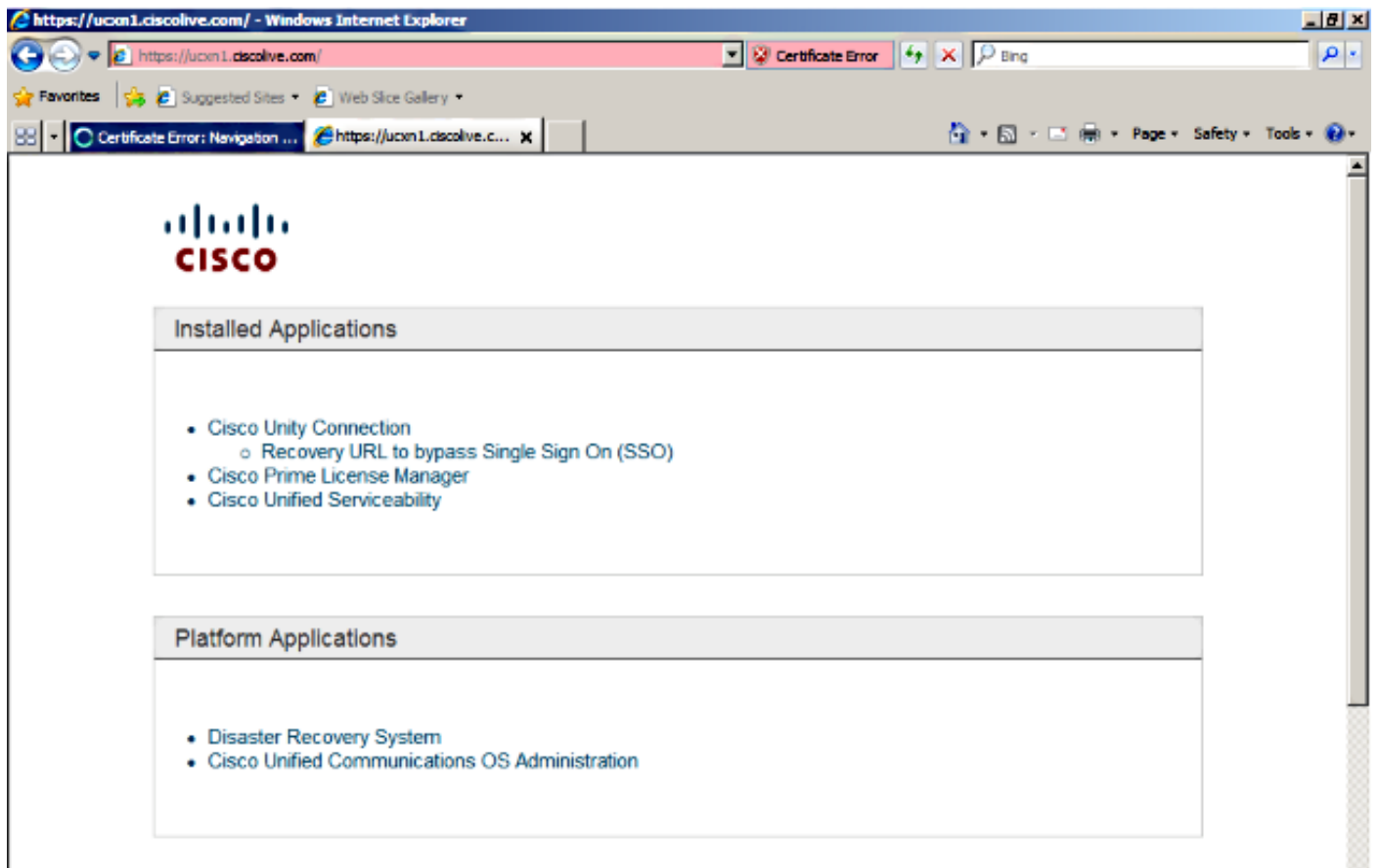
重要な注意事項 : SAML SSO を有効化するには、クラスタの場合は、UCXN サブスクライバに対して SSO テストを実行します。クラスタ内のすべての UCXN ノードに対し、AD FS を設定する必要があります。

ヒント : IdP ですべてのノードのメタデータ XML ファイルを設定し、1つのノードで SSO の動作を有効にすると、SAML SSO はクラスタのすべてのノードで自動的に有効になります。

また、SAML SSO に CUCM、CUCM IM とプレゼンスを設定することで、Cisco Jabber Clients に対して SAML SSO を使用し、エンドユーザに本来の SSO 体験を提供できます。

確認

Web ブラウザを開き、UCXN の FQDN を入力すると、[Installed Applications] の下位に、新たに [Recovery URL to bypass Single Sign-on (SSO)] というオプションが表示されます。[Cisco Unity Connection] リンクをクリックすると、AD FS によってクレデンシャルの入力が促されます。ユーザの SSO 用のクレデンシャルを入力すると、[Unity Administration] ページおよび [Unified Serviceability] ページにログインできます。



注：SAML SSO では次のページにアクセスはできません。

- Prime Licensing Manager
- OS Administration
- Disaster Recovery system

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

詳細については、[Collaboration 製品 10.x における SAML SSO のトラブルシューティング \[英語\]](#)を参照してください。