

# Unity Connection バージョン 10.5 SAML SSO 設定例

TAC

Document ID: 118772

Updated: 2015 年 1 月 21 日

A.M.Mahesh Babu によって貢献される、Cisco TAC エンジニア。



[PDF のダウンロード](#)



[印刷](#)

[フィードバック](#)

## 関連製品

- [Cisco Unity Connection](#)
- [Cisco Unified Communications Manager \( CallManager \)](#)

## 目次

[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](#)

[Cisco サポート コミュニティ - 特集対話](#)

## 概要

この資料に Cisco Unity Connection ( UCXN ) のためのセキュリティ アサーション マークアップ 言語 ( SAML ) 単一 サインオン ( SSO ) を設定し確認する方法を記述されています。

# 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。クロックの同期化については、[Cisco Unified Communications オペレーティングシステム 管理 ガイド](#)の NTP 設定セクションを参照して下さい。

### 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。

アクティブ ディレクトリ連合サービス ( AD FS ) バージョン 2.0 はインストールされ、SAML 要求を処理するために設定する必要があります。

## 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くものです。

- IdP として AD FS バージョン 2.0
- サービスプロバイダーとして 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たものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 背景説明

SAML は XML ベース、データ交換のためのオープン スタンダード データ 形式です。ユーザを認証することをサービスプロバイダーによって使用される認証プロトコルです。セキュリティ 認証情報は IdP とサービスプロバイダーの間で渡されます。

SAML はクライアント プラットフォームに関係なくあらゆる SAML 有効にされた コラボレーション ( か統合された通信 ) サービスに対して認証することをクライアントが可能にするオープン スタンダードです。

すべての Cisco Unified コミュニケーション Webインターフェイス、Cisco Unified

Communications Manager ( CUCM ) または UCXN のような、SAML SSO 機能の使用 SAML バージョン 2.0 プロトコル。 Lightweight Directory Access Protocol ( LDAP ) ユーザを認証するために、UCXN は IdP に認証要求に委託します。 UCXN によって生成されるこの認証要求は SAML 要求です。 IdP は SAML アサーションを認証し、戻します。 SAML アサーションは ( 認証される ) またははい示しません ( 認証は失敗しました )。

SAML SSO は LDAP ユーザが IdP で認証するユーザ名 および パスワードのクライアントアプリケーションにログイン することを可能にします。 SAML SSO 機能を有効にした後、統合された通信 製品のサポートされた Webアプリケーションの何れかへのユーザ サインインはまた UCXN のこれらの Webアプリケーションへのアクセス権を得ます ( CUCM から離れておよび CUCM IM および存在 ):

Unity Connection ユーザ	Webアプリケーション
管理者権限の LDAP ユーザ	<ul style="list-style-type: none"><li>• UCXN 管理</li><li>• Cisco UCXN サービスビリティ</li><li>• Cisco Unified サービスビリティ</li><li>• アシスタント Cisco 個人的な通信</li><li>• Web インボックス</li><li>• 小型 Web インボックス ( デスクトップ版 )</li><li>• アシスタント Cisco 個人的な通信</li><li>• Web インボックス</li></ul>
管理者権限のない LDAP ユーザ	<ul style="list-style-type: none"><li>• 小型 Web インボックス ( デスクトップ版 )</li><li>• Cisco Jabber クライアント</li></ul>

## 設定

### ネットワーク図

### ディレクトリ セットアップ

1. ログインするは UCXN 管理 ページおよび選定された LDAP および LDAP セットアップをクリックします。
2. LDAPサーバから同期するイネーブルをチェックし、『SAVE』 をクリックして下さい。
3. LDAP をクリックして下さい。
4. LDAP ディレクトリ設定をクリックして下さい。
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  
ホスト名または IP アドレスおよびポート番号

- LDAP ディレクトリと通信するために Secure Socket Layer ( SSL ) を使用したいと思う場合**使用 SSL をチェック**して下さい。

**ヒント** : SSL 上の LDAP を設定する場合、CUCM に LDAP ディレクトリ 認証をアップロードして下さい。LDAP 同期の特定の LDAP 製品および一般の最良の方法のためのアカウント同期機構についての情報に関しては [Cisco Unified Communications Manager SRND](#) の LDAP ディレクトリ の 内容を参照して下さい。

- 今行います完全な同期化をクリック**して下さい。

**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。

- ユーザを拡張し、ユーザを『Import』** を選択 して下さい。
- エンドユーザがリストしたり検索 Unified Communications Manager** で、LDAP ディレクトリを選択して下さい。
- UCXN を統合 LDAP ディレクトリのユーザのサブセットだけインポートしたいと思ったら、検索フィールドで適当な仕様を入力して下さい。
- 『Find』 を選択 して下さい。
- テンプレート リストに基づいてでは選択したユーザを作成するとき UCXN に使用してほしいこと**管理者 テンプレート**を選択して下さい。  
  
**注意** : 管理者 テンプレートを規定 する場合、ユーザはメールボックスを持っていません。
- Select UCXN ユーザ**を作成し、『Import』 をクリック したいと思う LDAP ユーザがあるように**チェックボックス**を確認して下さい。

## SAML SSO の有効化

- UCXN 管理 ユーザインターフェイスにログイン して下さい。
- システム > SAML 単一 サインオン**を選択すれば SAML SSO コンフィギュレーションウィンドウは開きます。

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、Downloadldp **メタデータ ステップ**の FederationMetadata.xml **メタデータ XML** ファイルをインポートするために『Browse』 をクリックして下さい。
  6. メタデータ ファイルがアップロードされたら、UCXN に IdP 情報をインポートするために **IdP メタデータ**を『Import』 をクリックして下さい。インポートが正常だった確認し、**の隣で続きます**ことをクリックして下さい。
  7. [パーティ信頼を中継で送ると同時に](#) UCXN メタデータで ADFS を既に設定しなかったときだけ UCXN メタデータをローカル フォルダーに保存し、[UCXN を追加すること](#)を行くために **信頼メタデータ ファイルセット**を (これをして下さい) 『Download』 をクリックして下さい。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。資格情報のためにプロンプト表示されるとき、ユーザ SSO ユーザ名 および パスワードを入力し、『OK』 をクリックして下さい。
- 注: この設定例は UCXN および AD FS 自己署名証明書に基づいています。認証局 (CA) 認証を使用すれば、適切な認証は AD FS および UCXN 両方でインストールする必要があります。詳細については[証明書管理および検証](#)を参照して下さい。
10. 結局ステップは完了しました、受け取ります「成功する SSO テストを!」メッセージに応答します。『Close』 をクリックし、続くために **終えて**下さい。

今正常に AD FS の UCXN の SSO を有効にする コンフィギュレーション タスクを完了しました。

**必須注:** それがクラスタ SAML SSO を有効にするためにである場合 UCXN サブスクライバのための SSO テストを実行して下さい。AD FS はクラスタの UCXN のノードすべてのために設定する必要があります。

**ヒント:** IdP のすべてのノードのメタデータ XML ファイルを設定し、1 つのノードの SSO オペレーションを有効にし始めれば SAML SSO はクラスタのノードすべてで自動的に有効になります。

SAML SSO を Cisco Jabber クライアントのために使用し、エンドユーザに本当 SSO エクスペリエンスを与えたいと思う場合また CUCM および CUCM IM および SAML SSO のための存在設定できます。

## 確認

Webブラウザを開き、UCXN の FQDN を入力すれば **Recovery URL** と呼ばれるインストールアプリケーションの下で**単一サインオン (SSO) をバイパスするために新しいオプション**を見ます。**Cisco Unity Connection** リンクをクリックすれば、AD FS によって資格情報のためにプロンプト表示されます。ユーザ SSO 資格情報を入力した後、正常に Unity ログインされた管理ページ、統一されたサービサビリティ ページです。

**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

現在のところ、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[コラボレーション製品 10.x のためのトラブルシューティング SAML SSO](#)を参照して下さい。

このドキュメントは有用でしたか。 [はいいいえ](#)

フィードバックいただき、ありがとうございました。

[サポート ケースのオープン](#) ( [シスコ サービス契約< ts generic='1' nval='P%1,2%%'が必要ですか](#) )。

## Cisco サポート コミュニティ - 特集対話

[Cisco サポート コミュニティ](#)では、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『[シスコ テクニカル ティップスの表記法](#)』

を参照してください。

Updated: 2015 年 1 月 21 日

Document ID: 118772