Unity Connection バージョン 10.5 SAML SSO 設定例

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

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の情報に関しては、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

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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 イネーブルになっ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インターフェイスは、Cisco Unified

Communications Manager（CUCM）または UCXN のような SAML SSO 機能で、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（失敗される認証）。

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	• UCXN 管理 • Cisco UCXN サービサビリティ • Cisco Unified サービサビリティ • アシスタント Cisco 個人的な通信 • Web インボックス • 小型 Web インボックス（デスクトップ版）
管理者権限のない LDAP ユーザ	• アシスタント Cisco 個人的な通信 • Web インボックス • 小型 Web インボックス（デスクトップ版） • Cisco Jabber クライアント

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 設定を**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

7. 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 ディレクトリ証明書をアップロードして下さい。 特定の LDAP 製品のためのアカウント同期機構および LDAP 同期のための一般の最良の方法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。

8. **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。

9. **ユーザを**拡張し、**ユーザを**『Import』 を選択 して下さい。

10. **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。

11. 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。

12. 『Find』 を選択 して下さい。

13. 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。

14. **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

1. UCXN 管理 ユーザインターフェイスにログイン して下さい。

2. **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、DownloadIdp **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。 信任状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）証明書を使用すれば、適切な証明書は 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。

必須メモ: 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イネーブルになっています。

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 によって信任状のためにプロンプト表示されます。 ユーザ SSO 信任状を入力した後、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 SAML SSO のトラブルシューティングを](#)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）。](#)

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