シングル サインオンの設定

SAML SSO ソリューションについて

重要 Cisco Jabber を Cisco Webex Meeting Server と共に導入する場合、Unified Communications Manager と Webex Meeting Server は同じドメインに存在している必要があります。

SAML は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のシスコのコラボレーション アプリケーションにシームレスにアクセスできます。 SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。 これは、サービス プロバイダー（例：Unified Communications Manager）がユーザの認証に使用する認証プロトコルです。 SAML により、ID プロバイダー（IdP）とサービス プロバイダーの間で、セキュリティ認証情報を交換できます。

SAML SSO は SAML 2.0 プロトコルを使用して、シスコのコラボレーション ソリューションのドメイン間と製品間で、シングル サインオンを実現しています。 SAML 2.0 は、Cisco アプリケーション全体で SSO を有効にし、Cisco アプリケーションと IdP 間でフェデレーションを有効にします。 SAML 2.0 では、高度なセキュリティ レベルを維持しながら、シスコの管理ユーザが安全なウェブ ドメインにアクセスして、IdP とサービス プロバイダーの間でユーザー認証と承認データを交換できます。 この機能は、さまざまなアプリケーションにわたり、共通の資格情報と関連情報を使用するための安全な機構を提供します。

SAML SSO の管理者権限は、シスコのコラボレーション アプリケーションでローカルに設定されたロールベース アクセス コントロール（RBAC）に基づき認証されます。

SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。 サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

重要　サービス プロバイダーが認証にかかわることはありません。 SAML 2.0 では、サービス プロバイダーではなく、IdP に認証を委任します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。 クライアントはサービス プロバイダーにアサーションを示します。 CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

SAML SSO 設定タスクフロー

SAML SSO 用にユニファイドコミュニケーションマネージャを設定するには、次のタスクを実行します。

始める前に

SAML SSO の設定では、ユニファイドコミュニケーションマネージャを設定するのと同時にアイデンティティプロバイダー (IdP) を設定する必要があります。IdP 固有の構成例については、以下を参照してください。

- Active Directory フェデレーション サービス
- Okta
- Open Access Manager
- PingFederate

（注）　上記のリンクは単なる例です。公式なマニュアルについては、IdP のマニュアルを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Communications Manager からの UC メタデータのエクスポート （3 ページ）	信頼関係を作成するには、ユニファイドコミュニケーションマネージャと IdP の間でメタデータファイルを交換する必要があります。
ステップ 2	ID プロバイダ（IdP）での SAML SSO の設定	以下のタスクを実行します。 • 信頼関係の輪を完了するために、ユニファイドコミュニケーションマネージャからエクスポートされた

	コマンドまたはアクション	目的
		UC メタデータファイルをアップロードします。 • IdP での SAML SSO の設定 • IdP メタデータファイルをエクスポートします。このファイルは、ユニファイドコミュニケーションマネージャにインポートされます。
ステップ 3	Cisco Unified Communications Manager での SAML SSO の有効化	IdP メタデータをインポートし、ユニファイドコミュニケーションマネージャで SAML SSO を有効にします。
ステップ 4	Cisco Tomcat サービスの再起動 （6 ページ）	SSO の有効化の前後には、SSO が有効になっているすべてのクラスタノードで Cisco tomcat サービスを再起動する必要があります。
ステップ 5	SAML SSO 設定の検証 （7 ページ）	SAML SSO が正常に設定されていることを確認します。

Cisco Unified Communications Manager からの UC メタデータのエクスポート

サービスプロバイダー (ユニファイドコミュニケーションマネージャ) から UC メタデータファイルをエクスポートするには、次の手順を使用します。「信頼の輪」関係を構築する目的で、メタデータ ファイルが ID プロバイダー（IdP）にインポートされます。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[SAML シングル サインオン（SAML Single Sign-On）]** を選択します

ステップ 2 [SAML シングル サインオン（SAML Single Sign-On）]ウィンドウの [SSO モード（SSO Mode）] フィールドで、以下のいずれかのオプションを選択します。

- [クラスタ全体（Cluster wide）]：クラスタで 1 つの SAML 合意。

  （注） このオプションを選択する場合は、クラスタ内のすべてのノードの Tomcat サーバの証明書が同じ（マルチ サーバ SAN 証明書）であることを確認してください。

- [ノードごと（Per Node）]：それぞれのノードに個別の SAML 合意があります。

ステップ 3 [SAML シングル サインオン（SAML Single Sign-On）]ウィンドウの [証明書（Certificate）] フィールドで、以下のいずれかのオプションを選択します。

- **システムで生成された自己署名証明書の使用（Use system generated self-signed certificate）**
- **Tomcat 証明書の使用（Use Tomcat certificate）**

ステップ 4 [すべてのメタデータのエクスポート（Export All Metadata）]をクリックして、メタデータ ファイルをエクスポートします。

（注） ステップ 3 で [クラスタ全体（Cluster wide）]オプションを選択すると、クラスタ用の単一のメタデータ XML ファイルがダウンロード対象として表示されます。 一方、[ノードごと（Per Node）]オプションを選択すると、クラスタのノードごとに単一のメタデータ XML ファイルがダウンロード対象として表示されます。

次のタスク

IdP で次の作業を完了します。

- Unified Communications Manager からエクスポートされた UC メタデータ ファイルをアップロードします。
- IdP で SAML SSO を設定します。
- IdP メタデータ ファイルをエクスポートします。 「信頼の輪」関係を完成させるために、このファイルが Unified Communications Manager にインポートされます。

Cisco Unified Communications Manager での SAML SSO の有効化

サービス プロバイダー（Unified Communications Manager）で SAML SSO を有効化するには、この手順を使用します。 このプロセスには、Unified Communications Manager サーバに IdP メタデータをインポートする操作が含まれます。

重要 シスコでは、SAML SSO を有効化または無効化にした後は、Cisco Tomcat サービスを再起動することを推奨しています。

（注） SAML SSO を有効化または無効化した後は、Cisco CallManager Admin、Unified CM IM and Presence Administration、Cisco CallManager Serviceability、および Unified IM and Presence Serviceability サービスが再起動されます。

始める前に

この手順を完了する前に、次の点を確認してください。

- IdP からのエクスポート済みメタデータ ファイルが必要です。
- エンド ユーザ データが Unified Communications Manager データベースに同期されていることを確認します。
- Unified Communications Manager IM and Presence Cisco Sync Agent サービスが、正常にデータの同期を完了していることを確認します。 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] でこの検査のステータスを確認するには、**[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）]** を選択します。データ同期が正常に完了した場合は[Sync Agent が関連データ（デバイス、ユーザ、ライセンス情報など）を使用して同期したことを確認する（Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)）] に [テスト合格（Test Passed）] という結果が表示されます
- Cisco Unified Administration へのアクセスを可能にするために、Standard CCM Super Users グループに少なくとも 1 人の LDAP 同期済みユーザが追加されている。 エンド ユーザ データの同期と LDAP 同期済みユーザのグループへの追加の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「システムの設定」および「エンド ユーザの設定」のセクションを参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

ステップ 2 [SAML SSO の有効化（Enable SAML SSO）]をクリックして、[続行（Continue）]をクリックします。

すべてのサーバ接続が再起動されることを伝える警告メッセージが示されます。

ステップ 3 [クラスタ全体（Cluster wide）]SSO モードが設定済みの場合、[マルチサーバ tomcat 証明書のテスト（Test for Multi-server tomcat certificate）]ボタンをクリックします。 それ以外の場合は、このステップを省略できます。

ステップ 4 [次へ（Next）]をクリックします。

ダイアログボックスが開き、ここで IdP メタデータをインポートできます。 IdP とサーバ間の信頼関係を設定するには、IdP から信頼メタデータ ファイルを取得し、それをすべてのサーバにインポートする必要があります。

ステップ 5 IdP からエクスポートしたメタデータ ファイルをインポートします。

a) [参照（Browse）]を使用し、エクスポート済みの IdP メタデータ ファイルを見つけて選択します。
b) [IdP メタデータのインポート(Import IdP Metadata)]をクリックします。
c) [次へ（Next）]をクリックします。
d) [サーバ メタデータをダウンロードして IdP にインストールする（Download Server Metadata and Install on IdP）]画面で、[次へ（Next）]をクリックします。

（注） **[次へ(Next)]** ボタンは、クラスタ内の 1 つ以上のノードに IdP メタデータ ファイルが正しくインポートされた場合のみ有効になります。

ステップ 6 次のように接続をテストして、設定を完了します。

a) **[エンドユーザの設定（End User Configuration）]** ウィンドウで、LDAP 同期される、**[権限情報（Permissions Information）]** リストボックスの「[標準 CCM スーパーユーザ（Standard CCM Super User）]」 権限を持つユーザを選択します。

b) [テスト実行(Run Test)]をクリックします。

IdP ログイン ウィンドウが表示されます。

（注） テストが正常に完了するまでは、SAML SSO を有効化できません。

c) 有効なユーザ名およびパスワードを入力します。

認証に成功すると、次のメッセージが表示されます。

「SSO のテストに成功しました（SSO Test Succeeded）」

このメッセージが表示されたら、ブラウザのウィンドウを閉じます。

認証に失敗するか、認証に 60 秒以上かかる場合は、[ログインに失敗しました（Login Failed）] というメッセージが IdP ログイン ウィンドウに表示されます。「」 [SAMLシングルサインオン(SAML Single Sign-On)] ウィンドウに、次のメッセージが表示されます。

「SSO メタデータのテストがタイムアウトになりました（SSO Metadata Test Timed Out）」

IdP へのログインを再試行するには、別のユーザを選択して再びテストを実行します。

d) [完了(Finish)]をクリックして、SAML SSO のセットアップを完了します。

SAML SSO が有効になり、SAML SSO に参加しているすべての Web アプリケーションが再起動されます。 Web アプリケーションの再起動には 1 ～ 2 分かかります。

Cisco Tomcat サービスの再起動

SAML シングルサインオンを有効化または無効化した前後は、シングルサインオンが実行されているすべての Unified CM クラスタノードと IM and Presence Service クラスタノードで、Cisco Tomcat サービスを再起動します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 `utils service restart Cisco Tomcat` CLI コマンドを実行します。

ステップ 3 シングル サインオンが有効化されているすべてのクラスタ ノードで、この手順を繰り返します。

SAML SSO 設定の検証

サービス プロバイダー（Unified Communications Manager）と IdP の両方で SAML SSO を設定した後、Unified Communications Manager でこの手順に従って、設定が機能することを確認します。

始める前に

次を確認します。

- Unified CM Administration の [SAMLシングルサインオンの設定（SAML Single Sign-On Configuration）]ウィンドウに、**IdP メタデータ信頼**ファイルが正常にインポートされたことが表示されます。
- サービス プロバイダー メタデータ ファイルが IdP にインストールされます。

手順

ステップ 1 Cisco Unified CM Administration のユーザ インターフェイスで、**[システム（System）] > [SAML シングルサインオン（SAML Single Sign-On）]** を選択して [SAMLシングルサインオンの設定（SAML Single Sign-On Configuration）]ウィンドウを開き、[次へ（Next）]をクリックします。

ステップ 2 [有効な管理者のユーザ名（Valid Administrator Usernames）]領域から管理ユーザを選択し、[SSO テストの実行…（Run SSO Test…）]ボタンをクリックします。

（注） テスト用のユーザには管理者権限が必要であり、IdP サーバではユーザとして追加されています。 [Valid Administrator Usernames（有効な管理者のユーザ名）] 領域には、テストの実行を指示できるユーザのリストが表示されます。

テストが成功した場合は、SAML SSO が正常に設定されています。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。