SAML シングル サインオンの管理

SAML シングル サインオンの概要

定義された一連の Cisco アプリケーションのうちの 1 つにサインインした後は、SAML シングル サインオン（SSO）を使用して、それらすべてのアプリケーション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、ユーザを認証するために、サービス プロバイダー（Cisco Unified Communications Manager など）が使用する認証プロトコルです。SAML では、ID プロバイダー（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交換されます。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 は、IdP とサービス プロバイダーの間で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、さまざまなサービスやアプリケーションへのアクセスを許可します。

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提示します。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。

iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプトイン制御

このリリースの Cisco Unified Communications Manager には、iOS での Cisco Jabber の SSO ログイン動作を ID プロバイダー（IdP）によって制御するためのオプトイン設定オプションが導入

されています。このオプションを使用すると、制御されたモバイル デバイス管理（MDM）環境内で、Cisco Jabber が IdP による証明書ベースの認証を実行できるようになります。

オプトイン制御を設定するには、Cisco Unified Communications Manager で [iOS の SSO ログイン動作（SSO Login Behavior for iOS）] エンタープライズ パラメータを使用します。

（注） このパラメータのデフォルト値を変更する前に、http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html で Cisco Jabber 機能のサポートおよびドキュメントを参照して、SSO ログイン動作と証明書ベースの認証に対する iOS 上での Cisco Jabber のサポートを確認してください。

この機能を有効にするには、iOS Cisco Jabber の SSO ログインの動作設定 （4 ページ）の手順を参照してください。

SAML シングル サインオンの前提条件

- Cisco Unified Communications Manager クラスタに DNS が設定されていること
- ID プロバイダー（IdP）サーバ
- IdP サーバによって信頼され、システムでサポートされる LDAP サーバ

SAML SSO 機能のテストは、SAML 2.0 を使用した以下の IdP で行われています。

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

サードパーティ アプリケーションは、次の設定要件を満たす必要があります。

- 必須属性の 「uid」 が IdP で設定されていること。この属性は、Cisco Unified Communications Manager の LDAP と同期されたユーザ ID に使用されている属性と一致している必要があります。

（注） Cisco Unified Communications Manager では現在のところ、ユーザ ID 設定の LDAP 属性として sAMAccountName オプションのみをサポートしています。

必須属性マッピングの設定の詳細については、IdP の製品マニュアルを参照してください。

- SAML SSO に参加するすべてのエンティティのクロックを同期させる必要があります。クロックの同期の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）の「「NTP Settings」」を参照してください。

SAML シングル サインオンの管理

SAML シングル サインオンの有効化

（注） 同期エージェントの確認テストに合格するまで、SAML SSO を有効にすることができません。

始める前に

- 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。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- Cisco Unified CM IM and Presence サービスと Cisco Sync Agent サービスのデータ同期が完了していることを確認します。このテストのステータスをチェックするには、**[Cisco Unified CM IM and Presence Administration]** > **[診断（Diagnostics）]** > **[システム トラブルシューター（System Troubleshooter）]** を選択します。[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）]「」 テストは、データ同期が正常に完了した場合にテスト合格の結果が示されています。
- Cisco Unified CM の管理へのアクセスを有効にするには、少なくとも 1 人の LDAP 同期ユーザが Standard CCM Super Users グループに追加されていることを確認します。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- 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。

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 の有功化（Enable SAML SSO）] をクリックします。

ステップ 3 すべてのサーバ接続が再起動されることを通知する警告メッセージが表示されたら、[続行（Continue）] をクリックします。

ステップ 4 [参照（Browse）] をクリックし、IdP メタデータ ファイルを探してアップロードします。

ステップ 5 [IdP メタデータのインポート（Import IdP Metadata）] をクリックします。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [信頼メタデータ ファイルセットのダウンロード（Download Trust Metadata Fileset）] をクリックして、サーバ メタデータをシステムにダウンロードします。

ステップ 8 IdP サーバ上にサーバ メタデータをアップロードします。

ステップ 9 [次へ（Next）] をクリックして続行します。

ステップ 10 有効な管理者 ID のリストから、管理者権限を持つ LDAP 同期ユーザを選択します。

ステップ 11 [テストを実行（Run Test）] をクリックします。

ステップ 12 有効なユーザ名およびパスワードを入力します。

ステップ 13 成功メッセージが表示されたら、ブラウザ ウィンドウを閉じます。

ステップ 14 [完了（Finish）] をクリックし、Web アプリケーションが再起動するまで 1～2 分待ちます。

iOS Cisco Jabber の SSO ログインの動作設定

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 オプトイン制御を設定するには、[SSO の設定（SSO Configuration）] セクションで、[iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータで、[ネイティブ ブラウザの使用（Use Native Browser）] オプションを選択します。

（注） [iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータには次のオプションが含まれます。

- [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。このオプションは、デフォルトで有効です。
- [ネイティブ ブラウザの使用（Use Native Browser）]：このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー（IdP）を利用する証明書ベースの認証を実行します。

  （注） ネイティブ ブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 **[保存（Save）]** をクリックします。

アップグレード後の WebDialer 上での SAML シングル サインオンの有効化

次のタスクに従って、アップグレード後に Cisco WebDialer 上で SAML シングル サインオンを再度アクティブ化します。SAML シングル サインオンを有効化する前に Cisco WebDialer をアクティブ化すると、デフォルトで、Cisco WebDialer 上で SAML シングル サインオンが有効になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco WebDialer サービスの非アクティブ化 （6 ページ）	Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。
ステップ 2	SAML シングル サインオンの無効化 （6 ページ）	SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。
ステップ 3	Cisco WebDialer サービスのアクティブ化 （6 ページ）	
ステップ 4	SAML シングル サインオンの有効化 （3 ページ）	

Cisco WebDialer サービスの非アクティブ化

Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Servers）] ドロップダウン リストから、リストされている Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [CTI サービス（CTI Services）] で、[Cisco WebDialer Web サービス（Cisco WebDialer Web Service）] チェック ボックスをオフにします。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

SAML シングル サインオンの無効化 （6 ページ）

SAML シングル サインオンの無効化

SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。

始める前に

Cisco WebDialer サービスの非アクティブ化 （6 ページ）

手順

CLI から、**utils sso disable** コマンドを実行します。

次のタスク

Cisco WebDialer サービスのアクティブ化 （6 ページ）

Cisco WebDialer サービスのアクティブ化

始める前に

SAML シングル サインオンの無効化 （6 ページ）

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Servers）] ドロップダウン リストから、リストされている Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [CTI サービス（CTI Services）] から、[Cisco WebDialer Web サービス（Cisco WebDialer Web Service）] チェック ボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 Cisco Unified Serviceability から、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択して、CTI Manager サービスがアクティブでスタート モードになっていることを確認します。

WebDialer を正しく機能させるには、CTI Manager サービスをアクティブにして、スタート モードにする必要があります。

次のタスク

SAML シングル サインオンの有効化 （3 ページ）

リカバリ URL へのアクセス

トラブルシューティングのために、SAML シングル サインオンをバイパスして、Cisco Unified Communications Manager Administration インターフェイスと Cisco Unified CM IM and Presence サービス インターフェイスにログインする場合に、リカバリ URL を使用します。たとえば、サーバのドメインまたはホスト名を変更する前に、リカバリ URL を有効にします。リカバリ URL にログインすると、サーバ メタデータの更新が容易になります。

始める前に

- 管理権限を持っているアプリケーション ユーザのみがリカバリ URL にアクセスできます。
- SAML SSO が有効になっている場合は、リカバリ URL がデフォルトで有効になります。CLI からリカバリ URL を有効/無効にすることができます。リカバリ URL を有効または無効にする CLI コマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

手順

ブラウザで、「`https://hostname:8443/ssosp/local/login`」と入力します。

ドメインまたはホスト名変更後のサーバ メタデータの更新

ドメインまたはホスト名の変更後は、この手順を実行するまで、SAML シングル サインオンが機能しません。

（注） この手順を実行しても [SAML シングル サインオン（SAML Single Sign-On）] ウィンドウ にログインできない場合は、ブラウザのキャッシュをクリアしてもう一度ログインしてみてください。

始める前に

リカバリ URL が無効になっている場合、シングル サインオン リンクをバイパスするようには表示されません。リカバリ URL を有効にするには、CLI にログインして次のコマンドを実行します：**utils sso recovery-url enable**。

手順

ステップ 1 Web ブラウザのアドレス バーに次の URL を入力します。

```
https://<Unified CM-server-name>
```

`<Unified CM-server-name>` はホスト名またはサーバの IP アドレスです。

ステップ 2 [シングル サインオンをバイパスするリカバリURL（Recovery URL to bypass Single Sign-On (SSO)）] をクリックします。

ステップ 3 管理者ロールを持つアプリケーション ユーザのクレデンシャルを入力し、[ログイン（Login）] をクリックします。

ステップ 4 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 5 [メタデータのエクスポート（Export Metadata）] をクリックしてサーバ メタデータをダウンロードします。

ステップ 6 サーバ メタデータ ファイルを IdP にアップロードします。

ステップ 7 [テストを実行（Run Test）] をクリックします。

ステップ 8 有効なユーザ ID とパスワードを入力します。

ステップ 9 成功のメッセージが表示されたら、ブラウザウィンドウを閉じます。

サーバ メタデータの手動プロビジョニング

ID プロバイダーで複数の UC アプリケーション用の単一接続をプロビジョニングするには、ID プロバイダーとサービス プロバイダー間の信頼の輪を設定しながら、サーバ メタデータを手

動でプロビジョニングする必要があります。信頼の輪の設定方法については、IdP 製品のマニュアルを参照してください。

一般的な URL 構文は次のとおりです。

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

手順

サーバ メタデータを手動でプロビジョニングするには、Assertion Customer Service（ACS）URL を使用します。

例：

サンプル ACS URL：

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```
