SAMLシングルサインオン(SAML Single Sign-On)

この章では、Security Assertion Markup Language（SAML）シングルサインオン機能について説明します。この機能によって、管理者ユーザが一部の Cisco Unified Communications Manager および IM and Presence Service アプリケーションに再ログインなしでアクセスできるようになります。

SAML シングルサインオン（SSO）を有効にすると、ユーザは次の Web アプリケーションに再ログインなしでアクセスできるようになります。

- Cisco Unified Communications Manager の管理
- Cisco Unified Reporting
- Cisco Unified Serviceability
- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence サービスアビリティ
- Cisco Unified IM and Presence のレポート

（注） SAML SSO 対応の Web アプリケーションにアクセスできるのは、LDAP で同期されたユーザのみです。 ローカル エンド ユーザとアプリケーション ユーザはアクセスできません。

SAML SSO のシステム要件

SAML シングルサインオン機能を使用するには、次のソフトウェア コンポーネントが必要です。

- Cisco Unified Communications Manager リリース 10.0(1) 以降

（注） DNS が Cisco Unified Communications Manager クラスタ用に構成されていることを確認してください。

- IM and Presence サービス リリース 10.0 (1) 以降
- Identity Provider（IdP）サーバ
- IdP サーバに信頼され、Cisco Unified CM でサポートされている LDAP サーバ

SAML 2.0 を使用する次の IdP がサポートされています。

- Microsoft Active Directory フェデレーション サービス（ADFS）
- Oracle Identity Manager
- Ping Federate
- Open Access Manager（OpenAM）

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 “uid” が IdP に設定されていること。 この属性は、Cisco Unified Communications Manager の LDAP 同期済みユーザ ID に使用される属性にする必要があります。

（注） 必須属性マッピングの設定方法については、IdP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する必要があります。クロック同期の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の「NTP Settings（NTP 設定）」の項を参照してください。

SAML SSO のインストール

Cisco Unified Communications Manager 10.0(1) および IM and Presence Service 10.0(1) をインストール後、必要な設定タスクを行うと SAML シングル サインオン機能を使用することができます。 実行する必要がある設定作業については、SAML SSO の有効化, （7 ページ）を参照してください。

SAML SSO の設定

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)] メニュー パスを使用して、SAML SSO を設定します。 次のテーブルでは、[SAMLシングルサインオン(SAML Single Sign-On)] ウィンドウに表示される設定について説明しています。

（注） 管理者権限のないエンドユーザとして Cisco Unified CM の管理にログインし、[SAMLシングルサインオン(SAML Single Sign-On)] ウィンドウにアクセスしようとすると、403 エラーが表示されます。 その後、同じブラウザ ウィンドウで、管理者権限のないエンドユーザとしてログインしようとすると、403エラーが引き続き表示されます。 この場合は、ブラウザのキャッシュをクリアしてから再ログインする必要があります。

設定	説明
[サーバ名(Server Name)]	クラスタ内のすべてのサーバの名前を指定します。
[SSOステータス(SSO Status)]	次のステータスのいずれかが表示されます。 **[SAML]** サーバ上で SAML SSO が有効であることを示します。 **[無効(Disabled)]** サーバ上で SAML SSO が無効であることを示します。 **[OpenAM]** サーバ上で OpenAM SSO が有効であることを示します。 Cisco Unified CM：[Cisco Unified OSの管理(Cisco Unified OS Administration)] > [セキュリティ(Security)] > [シングルサインオン(Single Sign On)] IM and Presence サービス：[Cisco Unified IM and Presence OSの管理(Cisco Unified IM and Presence OS Administration)] > [セキュリティ(Security)] > [シングルサインオン(Single Sign On)]

設定	説明
[メタデータの再インポート(Re-import Metadata)]	[メタデータの再インポート(Re-import Metadata)] アイコンをクリックすると、パブリッシャからサブスクライバに IdP メタデータ ファイルがインポートされます。 （注） パブリッシャ ノードでは、このオプションは [該当なし(N/A)] として表示されます。
[前回のメタデータインポート(Last Metadata Import)]	IdP メタデータがサーバに最後にインポートされた日時を示します。 SAML SSO の設定を初めて行った場合、このフィールドには [なし(Never)] が表示されます。
[メタデータのエクスポート(Export Metadata)]	[メタデータのエクスポート(Export Metadata)] アイコンをクリックすると、サーバのメタデータ ファイルがダウンロードされます。 指定されたサーバの SAML メタデータ ファイルを生成し、ブラウザを使用してダウンロードする必要があります。 次に、このメタデータ ファイルを IdP サーバにインポートする必要があります。 **重要** ノードのホスト名とドメインを変更する場合、そのノードからメタデータ ファイルをダウンロードし、IdP サーバに再アップロードしてください。 詳細については、ドメインまたはホスト名変更後のサーバのメタデータの更新, （9 ページ）を参照してください。
[前回のメタデータエクスポート(Last Metadata Export)]	指定されたサーバの SAML メタデータ ファイルが最後にエクスポートされた日時を示します。 SAML SSO の設定を初めて行った場合、このフィールドには [なし(Never)] が表示されます。

設定	説明
SSOテスト(SSO Test)	IdP での SAML 設定のテスト結果が表示されます。 テストでは、指定されたサーバが IdP を信頼していること、および IdP が指定されたサーバを信頼していることが確認されます。 サーバと IdP 間の信頼関係は、SAML メタデータ ファイルのエクスポートとインポートが正常に実行されたかどうかによって異なります。 次のいずれかの値が表示されます。 **[なし(Never)]** このサーバではテストが実行されていないことを示します。 **[合格(Passed)]** このサーバでテストが正常に実行されていること、およびサーバと IdP が互いに信頼していることを示します。 **[失敗(Failed)]** 指定されたサーバでテストが試行された一方で、サーバが IdP を信頼していないか、IdP がサーバを信頼していないか、ネットワークまたは IdP で発生した別の問題が原因でテストに合格しなかったことが示されます。

設定	説明
[テストの実行(Run Test)]	[テストの実行(Run Test)] をクリックすると、SSO テストが実行されます。 このテストは、SAML SSO を有効化する前に実行する必要があります。このテストが正常に実行されるまで、SAML SSO の設定を完了することはできません。 このテストを実行するには、少なくとも 1 人の LDAP同期済みユーザに管理者権限が必要です。 また、そのユーザ ID のパスワードも必要です。 （注） IdP メタデータ ファイルがサーバにインポートされるまで、このテストを実行することはできません。サーバのメタデータ ファイルは IdP サーバにインポートされます。 （注） OpenAM を IdP として使用している場合は、このテストを実行する前に IdP からログアウトする必要があります。
[SAML SSOの有効化(Enable SAML SSO)]	[SAML SSOの有効化(Enable SAML SSO)] をクリックすると、SAML SSO の設定が開始されます。
[IdPメタデータファイルの更新(Update IdP Metadata File)]	[IdPメタデータファイルの更新(Update IdP Metadata File)] をクリックすると、クラスタのすべてのサーバ上で IdP メタデータが更新されます。
[すべてのメタデータのエクスポート(Export All Metadata)]	[すべてのメタデータのエクスポート(Export All Metadata)] をクリックすると、各サーバから SAML メタデータ ファイルがエクスポートされます。 これらのファイルは圧縮ファイル（.zip）に変換されるため、簡単にダウンロードすることができます。 ファイルを抽出し、各ファイルを IdP にインポートする必要があります。
[すべての無効なサーバの修正(Fix All Disabled Servers)]	[すべての無効なサーバの修正(Fix All Disabled Servers)] をクリックすると、各サーバ上で無効化されている SAML SSO が有効になります。
[IdP信頼メタデータファイルを表示(View IdP Trust Metadata File)]	[IdP信頼メタデータファイルを表示(View IdP Trust Metadata File)] をクリックすると、IdP メタデータ ファイルのコピーがダウンロードされます。

SAML SSO の有効化

（注） Cisco CallManager Admin、Cisco Unified CM IM and Presenceの管理、Cisco CallManager Serviceability および Cisco Unified IM and Presence Serviceability サービスは、SAML SSO を有効または無効にすると再起動されます。

SAML SSO を有効にするには、次の手順を実行します。

はじめる前に

次の条件を満たしていることを確認してから手順に進んでください。

- エンド ユーザのデータは、Cisco Unified Communications Manager データベースに同期されます。
- Cisco Unified CM 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 Administration] > [診断(Diagnostics)] > [システム トラブルシューター(System Troubleshooter)] を選択して、このテストの状態を確認します。 「Verify Sync Agent は関連データ（デバイス、ユーザ、ライセンス情報など）と同期しています（Verify Sync Agent has sync'ed over relevant data“ ”(e.g. devices, users, licensing information)）」というテスト結果は、データの同期が正常に完了した場合の「テストに合格しました（Test Passed）」という結果を示します。
- LDAP で同期されたユーザを 1 人以上 Standard CCM Super Users グループに追加して、Cisco Unified Administration へのアクセスを有効にします。

（注） エンド ユーザの同期と LDAP で同期された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「システムのセットアップ」および「エンド ユーザのセットアップ」セクションを参照してください。

- OpenAM SSO（[Cisco Unified OSの管理(Cisco Unified OS Administration)] > [セキュリティ(Security)] > [シングル サインオン(Single Sign On)] または [Cisco Unified IM and Presence OSの管理(Cisco Unified IM and Presence OS Administration)] > [セキュリティ(Security)] > [シングル サインオン(Single Sign On)]）は、すべてのノードで無効になっています。 OpenAM SSO の詳細については、シングル サインオン および『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[システム(System)] > [SAML シングル サインオン(SAML Single Sign-On)] をクリックします。

ステップ 2 [SAML SSO の有効化(Enable SAML SSO)] をクリックします。
すべてのサーバ接続が再実行されることを示す警告メッセージが表示されます。

ステップ 3 [続行(Continue)] をクリックします。
IdP メタデータをインポートできるダイアログ ボックスが表示されます。 IdP と自分のサーバの間に信頼関係を設定するには、IdP から信頼メタデータ ファイルを取得して、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 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。

（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 7 [信頼メタデータ ファイルセットをダウンロード(Download Trust Metadata Fileset)] をクリックして、サーバの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 サーバのメタデータを IdP サーバにアップロードします。
サーバのメタデータを IdP サーバにインストールしたら、SSO テストを実行して、そのメタデータ ファイルが正しく設定されていることを確認する必要があります。

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 で同期されたユーザを選択します。

ステップ 11 [テスト実行(Run Test)] をクリックします。
IdP のログイン ウィンドウが表示されます。

（注） テスト実行が成功するまで、SAML SSO を有効化することはできません。

ステップ 12 正しいユーザ名と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。

認証に失敗した場合、または認証に 60 秒以上かかった場合、IdP のログイン画面に「ログインに失敗しました(Login Failed)」というメッセージが表示されます。 [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 に再度ログインを試すには、手順 11 と 12 を繰り返します。

ステップ 13 [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。

リカバリ URL

リカバリ URL を使用すると、トラブルシューティング時に、SAML シングル サインオンをバイパスし、Cisco Unified CM の管理、および Cisco Unified CM IM and Presence インターフェイスにログインすることができます。 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 にログインすることで、サーバ メタデータを簡単に更新することができます。 リカバリ URL は https://hostname:8443/ssosp/local/login です。

（注） また、リカバリ URL には、Cisco Unified Communications Manager のホーム ページおよび IM and Presence サービス ノードからアクセスすることができます。これは、サーバのホスト名または IP アドレスを Web ブラウザに入力したときに表示される Web ページです。

（注） リカバリ URL にアクセスできるのは、管理者権限を持つアプリケーション ユーザのみです。

SAML SSO が有効である場合、リカバリ URL はデフォルトで有効になります。 リカバリ URL は CLI から有効化および無効化することができます。 CLI のコマンドを使用してリカバリ URL を有効化および無効化する方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)*』を参照してください。

ドメインまたはホスト名変更後のサーバのメタデータの更新

サーバのドメインまたはホスト名を変更した後にサーバのメタデータを更新するには、次の手順を実行します。

注意 サーバのドメインまたはホスト名を変更した後、この手順を実行しないと SAML SSO が動作しません。

（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、もう一度ログインしてみてください。

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>` はサーバの名前または IP アドレスです。

ステップ 2 表示されたメイン ウィンドウから、[シングルサインオン（SSO）をバイパスするためのリカバリ URL(Recovery URL to bypass Single Sign-On (SSO))] を選択します。
[Ciscoシングルサインオンリカバリ管理(Cisco Single Sign-On Recovery Administration)] ウィンドウが表示されます。

（注） リカバリ URL が無効になっていると、[シングル サインオン（SSO）をバイパスするためのリカバリ URL(Recovery URL to bypass Single Sign-On (SSO))] のリンクが表示されません。 リカバリ URL を有効にするには、CLI にログインし、コマンド **utils sso recovery-url enable** を実行します。

ステップ 3 管理者権限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て、[ログイン(Login)] をクリックします。
[Cisco Unified CMの管理(Cisco Unified CM Administration)] ウィンドウが表示されます。

ステップ 4 Cisco Unified CMの管理から、[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、サーバのメタデータをダウンロードします。

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

ステップ 7 [テスト実行(Run Test)] をクリックします。
IdP のログイン ウィンドウが表示されます。

（注） テスト実行が成功するまで、SAML SSO を有効化することはできません。

ステップ 8 有効なユーザ ID と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。

認証に失敗した場合、または認証に 60 秒以上かかった場合、IdP のログイン画面に「ログインに失敗しました(Login Failed)」というメッセージが表示されます。 [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 に再度ログインを試すには、手順 7 と 8 を繰り返します。

サーバのメタデータの手動プロビジョニング

複数の UC アプリケーションに対し、Identity Provider で 1 つの接続をプロビジョニングする場合は、Identity Provider とサービス プロバイダーの間で信頼の輪（Circle of Trust）を構成しつつ、サーバの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（Circle of Trust）の構成の詳細については、IdP 製品の資料を参照してください。

サーバのメタデータを手動でプロビジョニングするには、アサーション カスタマー サービス（ACS）の URL を使用する必要があります。

ACS の URL の例

```
<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"/>
```

一般的な URL の構文

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

SAML SSO の CLI コマンド

この項では SAML シングル サインオン用の CLI コマンドを一覧で示します。

- utils sso enable
- utils sso disable
- utils sso status
- utils sso recovery-url enable
- utils sso recovery-url disable
- show samltrace level
- show samltrace level

CLI コマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions Release 10.0(1)*』を参照してください。