SAML SSO の設定

SAML ベースの SSO の前提条件

SAML ベースの SSO 設定には、次のシステム設定が必要です。

- NTP の設定
- DNS の設定
- ディレクトリ セットアップ

NTP の設定

SAML SSO では、Network Time Protocol（NTP）によって、Unified Communications アプリケーションと IdP 間のクロック同期が可能になります。SAML は時間的な制約のあるプロトコルであり、IdP は SAML アサーションが有効であることを時間ベースで判断します。IdP と Unified Communications アプリケーションのクロックが同期していない場合、 アサーションは無効となり、SAML SSO 機能は停止します。IdPと Unified Communications アプリケーション間の最大許容時間差は 3 秒です。

（注） 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、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。

クロックを同期するための NTP サーバーの追加については、『*Cisco Unified Communications Manager* システム設定ガイド』の「デバイスプールのコア設定」の章を参照してください。

DNS の設定

Domain Name System（DNS）により、ホスト名とネットワーク サービスをネットワーク（複数可）内のIPアドレスにマッピングできるようになります。ネットワーク内に配置されたDNSサーバは、ネットワーク サービスをホスト名にマッピングし、次にホスト名を IP アドレスにマッピングするデータベースを備えています。ネットワーク上のデバイスは、DNSサーバに照会して、ネットワークにある他のデバイスの IP アドレスを受信できます。そのため、ネットワーク デバイス間の通信が容易になります。

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。たとえば、管理者がブラウザにサービスプロバイダーのホスト名（`http://www.cucm.com/ccmadmin`）を入力すると、ブラウザはホスト名を解決する必要があります。サービスプロバイダーが SAML SSOのためにブラウザを IdP（`http://www.idp.com/saml`）にリダイレクトする場合、ブラウザは IdP ホスト名も解決する必要があります。さらに、IdP がサービスプロバイダーの ACS URL にリダイレクトする場合、ブラウザはそれも解決する必要があります。

ディレクトリ セットアップ

ディレクトリ設定：さまざまなUnified Communications アプリケーション間での SAML SSO を有効にするために、LDAP ディレクトリの同期は事前に必要な必須の手順です。Unified Communications アプリケーションを LDAP ディレクトリと同期することにより、管理者は Unified Communications アプリケーションのデータ フィールドをディレクトリ属性にマッピングして、ユーザを容易にプロビジョニングできるようになります。

（注） SAML SSOを有効にするには、LDAP サーバーが IdP サーバーによって信頼され、Unified Communications アプリケーションによってサポートされている必要があります。

詳細については、以下にある『シスコ コラボレーション システム リファレンス ネットワーク設計（SRND）』の「ディレクトリ統合とアイデンティティ管理」の章を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

証明書の管理と検証

重要 シスコでは、SAML SSO 用にサーバー証明書を署名し、製品サポートが利用可能な場合はマルチサーバー証明書を使用することを強く推奨します。

（注）

- 共通名（CN）とサブジェクトの別名（SAN）は、IP アドレス、または要求されるアドレスの完全修飾ドメイン名（FQDN）への参照です。たとえば、https://www.cisco.com と入力すると、CN または SAN のヘッダーに 「www.cisco.com」 が含まれている必要があります。
- Unified Communications Manager がすでに混合/セキュアモードになっていて、証明書に変更が加えられている場合は、セキュア USB トークンを使用して CTL 証明書を更新する必要があります。そうしないと、 Cisco Jabber クライアントはテレフォニー機能を取得できません。CTL トークンの更新には、Unified Communications Manager の再起動が必要です。

SAML SSO では、SAML メッセージ交換に参加する各エンティティ（ユーザーの Web ブラウザを含む）は、必要なエンティティへのシームレスでセキュアな HTTPS 接続を確立する必要があります。シスコでは、SAML SSO 展開に参加する各 UC 製品で、信頼できる認証局によって発行された署名付き証明書を設定することを強く推奨します。

Unified Communications アプリケーションは、証明書の検証を使用してサーバーとのセキュアな接続を確立します。証明書は、データの信頼/認証と暗号化を構築するためにエンドポイント間で使用されます。これにより、エンドポイントが目的のデバイスと通信し、2 つのエンドポイント間でデータを暗号化するオプションがあることが確認されます。

セキュアな接続を確立しようとする場合、サーバーは Unified Communications クライアントに証明書を提示します。クライアントが証明書を検証できない場合、証明書を受け入れるかどうかを確認するプロンプトが表示されます。

認証局によって署名された証明書

シスコは、次のいずれかの種類の認証局（CA）により署名されるサーバ証明書を使用することを推奨します。

- **パブリック CA**：サードパーティ企業が、サーバーの識別情報を確認し、信頼できる証明書を発行します。
- **プライベート CA**：自身でローカルの CA を作成および管理し、信頼できる証明書を発行します。

署名プロセスは製品ごとに異なり、サーバのバージョン間でも異なる場合があります。各サーバのすべてのバージョンに関する詳細な手順については、このマニュアルの範囲外になります。CA により署名された証明書を取得する方法の詳細な手順については、該当するサーバのマニュアルを参照してください。

ただし、次の手順では、手順の概要を説明します。

ステップ 1 クライアントに証明書を提示できる各製品で証明書署名要求（CSR）を生成します。

ステップ 2 各 CSR を CA に送信します。

ステップ 3 CA が各サーバーに発行する証明書をアップロードします。

どのサーバー証明書でも、クライアントのコンピューターの信頼ストアで、関連するルート証明書を提示しておくようにします。Cisco UC アプリケーションは、サーバーが信頼ストアのルート証明書に対して提示する証明書を検証します。

パブリック CA により署名されたサーバ証明書を取得する場合、パブリック CA は、クライアントコンピュータの信頼ストアで、ルート証明書をあらかじめ提示しておくようにします。この場合、クライアント コンピュータでルート証明書をインポートする必要はありません。

プライベート CA など、CA により署名される証明書が信頼ストアにまだ存在しない場合は、ルート証明書をインポートしてください。

SAML SSO では、CN または SAN での正しいドメインが記載された CA 署名付き証明書が、IdP およびサービスプロバイダーに必要になります。正しい CA 証明書が検証されない場合、ブラウザはポップ アップ警告を出します。

たとえば、管理者がブラウザを `https://www.cucm.com/ccmadmin` に向けると、Unified Communications Manager ポータルは CA 証明書をブラウザに提示します。ブラウザが `https://www.idp.com/saml` にリダイレクトされると、IdP は CA 証明書を提示します。ブラウザは、サーバーによって提示された証明書にそのドメインの CN または SAN フィールドが含まれていること、および証明書が信頼できる CA によって署名されていることを確認します。

または、顧客が独自のプライベート CA を持っている場合は、その CA を、管理者がブラウザを起動しているコンピュータにルート トラスト アンカーとしてインストールする必要があります。

マルチサーバー SAN 証明書の設定

各シスコ製品には、マルチサーバー SAN 証明書を生成するための独自のプロセスがあります。マルチサーバー SAN 証明書をサポートするシスコ製品については、関連するガイドを参照してください。

関連トピック

『Release Notes for Cisco Unified Communications Manager、リリース 10.5(1)』
Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド、リリース 10.x
Cisco Prime Collaboration

Microsoft Edge 相互運用性のための証明書発行者の展開

Microsoft Edge ブラウザが展開されている SAML SSO 展開内には、相互運用性の問題が存在します。Edge ブラウザが SSO 対応マシンに展開されている場合、Edge ブラウザは Unified Communications Manager 証明書の証明書発行者を認識せず、アクセスを提供しません。

この手順を使用して、グループポリシーオブジェクト（GPO）と Active Directory を介してこの問題を修正します。これにより、Unified Communications Manager 証明書の証明書発行者を、Edge ブラウザを使用するローカルマシンの信頼されたルート証明書にプッシュできます。

（注） 「証明書発行者」は、証明書の設定方法によって異なります。たとえば、サードパーティ CA 証明書の場合、CA 自体が Unified Communications Manager 証明書に署名する場合にのみ、CA 証明書をプッシュする必要があります。ただし、中間 CA が Unified Communications Manager 証明書に署名する場合は、ルート証明書、中間証明書、およびリーフ証明書を含む完全な証明書チェーンをプッシュする必要があります。

始める前に

この手順を完了するには、少なくともローカルコンピュータに対する管理者のメンバーシップ、またはこれと同等の権限が必要です。

ステップ 1 Active Directoryで、グループポリシー管理コンソールを開きます。

ステップ 2 既存の GPO を検索するか、証明書設定を含める新しい GPO を作成します。GPO は、ポリシーの影響を受けるユーザーのドメイン、サイト、または組織単位に関連付ける必要があります。

ステップ 3 GPO を右クリックし、[編集（**Edit**）] を選択します。
グループ ポリシー管理エディタ が開き、ポリシー オブジェクトの現在の内容が表示されます。

ステップ 4 ナビゲーション ウィンドウで、**[コンピュータの構成 >] [Windows の設定] [> セキュリティの設定] [> 公開キーのポリシー] > [信頼された発行元]**を開きます。

ステップ 5 [**アクション**（Action）] メニューをクリックし、[インポート（**Import**）] をクリックします。

ステップ 6 証明書の **インポートウィザードの指示に従って、証明書** を検索してインポートします。

ステップ 7 証明書が自己署名されており、**信頼されたルート証明機関** の証明書ストアにある証明書を追跡できない場合は、そのストアに証明書をコピーする必要もあります。ナビゲーション ウィンドウで、[信頼されたルート証明機関（**Trusted Root Certification Authorities**）] をクリックし、手順 5 と 6 を繰り返して、そのストアに証明書のコピーをインストールします。

（注） Active Directory での信頼されたルート証明書の管理の詳細については、「https://technet.microsoft.com/en-us/library/cc754841(v=ws.11).aspx」を参照してください。

SAML SSO 設定タスクフロー

シスコ コラボレーション環境で SAML SSO を設定するには、次のタスクを実行します。このプロセスには、次のアプリケーションの手順が含まれます。

- Cisco Unified Communications Manager
- IM and Presence Service
- Cisco Unity Connection

• Cisco Expressway（MRA 展開あり）

手順

	コマンドまたはアクション	目的
ステップ 1	コラボレーション アプリケーションでの SSO 設定の開始 （6 ページ）	Cisco Collaboration 環境で、SSO 設定を開始し、UC メタデータをエクスポートします。
ステップ 2	ID プロバイダでの SAML SSO の設定 （9 ページ）	アイデンティティ プロバイダー： • メタデータのアップロード • SAML SSO 契約の設定 • IdP メタデータファイルをエクスポートします。
ステップ 3	シスコ コラボレーション アプリケーションの SAML SSO の有効化 （9 ページ）	IdP メタデータをシスコ コラボレーション環境にインポートし、設定を完了します。

コラボレーション アプリケーションでの SSO 設定の開始

シスコ コラボレーション環境で、SAML SSO 設定を開始し、UC メタデータをエクスポートして ID プロバイダーにアップロードします。SAML SSO を設定するアプリケーションと選択したオプションによっては、複数のダウンロード ファイルが存在する場合があります。

始める前に

証明書のタイプとともに、必要な SAML SSO 契約のタイプ（クラスタ全体またはノードごと）を事前に計画してください。

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

a) 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。
b) [SSO モード（**SSO Mode**）] オプション（[クラスタ全体（**Cluster Wide**）] または [ノードごと（**Per Node**）]）を選択します。
c) [証明書（**Certificate**）] オプション（**システムで生成された自己署名証明書** または **Cisco Tomcat** 証明書）を選択します。
d) [メタデータのエクスポート（Export Metadata）] をクリックして、メタデータ ファイルを保存します。クラスタ全体の契約では、単一のメタデータファイルを受け取ります。ノードごとの契約では、zip ファイルのダウンロードには、クラスタノードごとに個別の XML ファイルが含まれています。IM and Presence Service が標準展開に展開されている場合、

ステップ 2 IM and Presence サービス：IM and Presence サービスの集中型展開がある場合は、IM and Presence 中央クラスタの一部であるスタンドアロン Unified CM パブリッシャ ノードでステップ 1 を繰り返します。

（注） IM and Presence Service Standard 展開では、前の手順で Unified Communications Manager からダウンロードしたメタデータ ファイルに IM and Presence Service クラスタのメタデータが含まれているため、このタスクをスキップできます。

ステップ 3 Cisco Unity Connection で、メタデータ ファイルをエクスポートします。

a) Cisco Unity Connection Administration で、[システム設定（System Settings）][SAMLシングルサインオン（**System Settings** > **SAML Single Sign On** ）]に移動します。

b) [SSO モード（**SSO Mode** ）] オプション（[クラスタ全体（**Cluster Wide** ）] または [ノードごと（**Per node**）]）を選択します。

c) [メタデータのエクスポート（Export Metadata）] をクリックします。

ステップ 4 Cisco Expressway-C で、メタデータ ファイルをエクスポートします。

a) Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（onfiguration）]** の順に選択します。

b) [MRAアクセス制御（**MRA Access Control** ）] セクションで、[認証パス（ **Authentication path**）] に次のいずれかのオプションを選択します。

- **SAML SSO 認証**
- **SAML SSO および UCM/LDAP**—両方のメソッドを許可します。

c) [SAML メタデータ（**SAML Metadata** ）] オプションを選択します（[クラスタ（Cluster）] または [ピア（Peer）]）。

- **クラスタ**：クラスタ用の単一のメタデータファイル
- [ピア（**Peer**）]：ノードごとに個別のメタデータ ファイル。

d) **[SAMLデータをエクスポート（Export SAML data）]** をクリックします。

- クラスタ契約の場合は、[証明書の生成（**Generate Certificate** ）] をクリックし、[証明書のダウンロード（**Download** the certificate）] をクリックします。
- ピア契約の場合は、[すべてダウンロード（**Download All**）] を選択します。

e) 安全な場所にファイルを保存します。

この手順が完了すると、コラボレーション アプリケーションごとにメタデータ ファイルが作成されます。メタデータファイルの数は、設定と展開タイプによって異なります。

メタデータのダウンロードの例

Cisco Collaboration 展開で予想されるファイルのダウンロード数の例については、次を参照してください。次のアプリケーションの SSO を設定するとします。

- Cisco Unified Communications Manager Cluster の 5 つのノード
- IM and Presence Service クラスタの 3 つのノード

- Cisco Unity Connection クラスタの 2 つのノード
- Expressway-C クラスタの 3 つのノードと Expressway-E クラスタ（MRA 展開）の 3 つのノード

次の表に、クラスタ全体の契約を使用しているかどうか、および IM and Presence Service が標準展開と集中型展開のどちらにあるかによって予想される合計ダウンロードファイルの内訳を示します。

表 *1:* 予想されるメタデータのダウンロード

契約タイプ	**IM and Presence** が標準展開の場合にダウンロードされるファイルの総数	**IM and Presence** が集中型展開の場合にダウンロードされるファイルの総数*
[クラスタ全体（Cluster wide）]	次のクラスタを表す 3 つのメタデータ XML ファイル： • Cisco Unified Communications Manager および IM and Presence Service クラスタ • Unity Connection クラスタ • Expressway-C クラスタ	次のクラスタを表す 4 つのメタデータ XML ファイル： • Unified Communications Manager クラスタ • IM and Presence Service クラスタ • Unity Connection クラスタ • Expressway-C クラスタ
[ノードごと（Per node）]	13 個のメタデータ XML ファイルを含む 3 つの zip ファイル： • Unified CM および IM and Presence ノード用の 8 つの XML ファイルを含む 1 つの zip ファイル • Unity Connection ノード用の 2 つの XML ファイルを含む 1 つの zip ファイル • Expressway-C ノード用の 3 つの XML ファイルを含む 1 つの zip ファイル	14 個のメタデータ XML ファイルを含む 4 つの zip ファイル： • Unified CM ノード用の 5 つの XML ファイルを含む 1 つの zip ファイル • IM and Presence ノード用の 3 つの XML ファイルと、IM and Presence 中央クラスタにあるスタンドアロン Unified CM パブリッシャノード用の追加の XML ファイルを含む 1 つの zip ファイル • Unity Connection ノード用の 2 つの XML ファイルを含む 1 つの zip ファイル • Expressway-C ノード用の 3 つの XML ファイルを含む 1 つの zip ファイル

（注） 標準展開では、Cisco Unified Communications Manager と IM and Presence Service が同じクラスタにあります。IM and Presence Service のメタデータは、Cisco Unified Communications Manager からのメタデータのダウンロードに含まれています。

集中型展開では、IM and Presence Service は Cisco Unified Communications Manager のテレフォニークラスターとは別のクラスターにあり、IM and Presence Service のメタデータは、IM and Presence 中央クラスター内にあるスタンドアロンの非テレフォニー Unified CM パブリッシャノードを使用して個別にエクスポートする必要があります。

ID プロバイダでの SAML SSO の設定

アイデンティティ プロバイダー上

- シスコ コラボレーション環境からダウンロードした UC メタデータ ファイルをインポートします。
- Cisco Collaboration アプリケーションに対する SAML SSO 契約の設定
- 後でシスコ コラボレーション アプリケーションにインポートするアイデンティティ プロバイダー メタデータ ファイルをエクスポートします。

シスコでは、次の Idp 固有の設定例をガイドとして提供しています。

- Microsoft Active Directory Federation Services 2.0
- Microsoft Active Directory Federation Services 3.0
- Microsoft Active Directory Federation Services 4.0
- Microsoft Azure
- Okta
- Open AM
- 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。

シスコ コラボレーション アプリケーションの SAML SSO の有効化

始める前に

ID プロバイダーのメタデータをシスコ コラボレーション アプリケーションにインポートし、SAML SSO 設定を完了します。

重要 これは、リリース 14SU2 以降に適用されます。

（注） ドメインを設定する際は、SAML SSOの有効化後に表示される接続の失敗とメタデータの不一致の警告メッセージを回避するために、「CUCM サーバー定義を IP アドレスまたはホスト名から FQDN 形式に変更する」の「設定」セクションを参照することをお勧めします。これは、BCFIPS 機能中に導入されました。

ステップ 1 Cisco Unified Communications Manager の SSO 設定はこれで完了です。

a) SAML SSO を有効にする前に、Cisco Tomcat サーバーを再起動します。
b) 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。
c) [SAML SSO の有効化（Enable SAML SSO）] をクリックします。
d) **[続行（Continue）]** を選択して、プロンプトに従います。
e) クラスタ全体の契約のみ。[マルチサーバ Tomcat 証明書のテスト（Test for Multi-Server Tomcat Certificate）] をクリックします。
f) [次へ（Next）] をクリックします。
g) **[参照 (Browse)]** をクリックして、エクスポートした IdP メタデータファイルを見つけて選択します。ファイルを開いたら、[IdP メタデータのインポート（**Import IdP Metadata**）] をクリックします。
h) [次へ] をクリックします。
i) 標準 CCM スーパーユーザー権限を持ち、[SSO テストの実行（**Run SSO test**）] を持つ LDAP 同期対象ユーザーを選択します。
j) ユーザの証明書によるサインイン
k) [完了（Finish）] をクリックして、SAML SSO の設定を完了します。
l) Cisco Tomcat サービスを再起動します。
m) ノード単位の契約のみ。すべての Unified Communications Manager クラスタ ノードでこの手順を繰り返します。

（注） Unified Communications Manager で FIPS または ESM が有効になっている場合は、SSO 署名アルゴリズムを sha256 に設定する必要があります。

Cisco Unified CM のすべてのノードの管理 CLI でこのコマンドを実行します。

```
utils sso set 署名アルゴリズム sha256
```

ステップ 2 IM and Presence サービス：IM and Presence サービスの集中型展開がある場合は、IM and Presence 中央クラスタの一部であるスタンドアロン Unified CM パブリッシャ ノードで前の手順を繰り返します。

ステップ 3 Cisco Unity Connection で、SAML SSO 設定を完了します。

a) SAML SSO を有効にする前に、Cisco Tomcat サーバーを再起動します。

b) Cisco Unity Connection Administration で、[システム設定（System Settings）][SAMLシングルサインオン（ **System Settings** > **SAML Single Sign On** ）]に移動します。
c) **[SAML シングル サインオンの有効化（Enable SAML Single Sign On）]** をクリックします。
d) **[続行（Continue）]** を選択して、プロンプトに従います。
e) IdP メタデータ ファイルを Cisco Unity Connection にインポートします。
f) SSO 接続をテストします。
g) Cisco Tomcat サービスを再起動します。
h) ノード単位の契約のみ。クラスタごとに、この手順を繰り返します。

ステップ 4 Expressway-C プライマリ ピアで、SAML SSO 設定を完了します。

a) **[構成（Configuration）]** > **[ユニファイド コミュニケーション（Unified Communications）]** > **[アイデンティティ プロバイダー（IdP）（Identity providers (IdP)）]** に移動します。
b) **[SAMLから新しいIdPをインポート（Import new IdP from SAML）]** をクリックします。
c) **[SAMLファイルをインポート（Import SAML file）]** コントロールを使用して、IdP から SMAL メタデータファイルを検索します。
d) **[ダイジェスト（Digest）]** を必要な SHA ハッシュアルゴリズムに設定します。
e) [アップロード（Upload）] をクリックします。

（注） メタデータをインポートした後は、**[（Configuration）]** > **[Unified Communications]** > **[アイデンティティプロバイダ（IdP）（Identity providers (IdP)）]** の順に選択し、IdP 行を検索し、アクション列で **[ダイジェストの構成（Configure Digest）]** をクリックすると署名アルゴリズムを変更できます。

f) IdP が ID プロバイダーのリストに表示されていることを確認します。
g) IdP の行で **[ドメインの関連付け（Associate domains）]** をクリックします。
h) このアイデンティティ プロバイダーに割り当てるドメインをオンにします。
i) [保存（Save）] をクリックします。

（注） SAML SSO 用に Active Directory フェデレーション サービス（ADFS）を使用して Cisco Expressway を展開する場合は、「ADFS の追加の Expressway 設定 （12 ページ）」で追加の Expressway 設定を参照してください。

SAML SSO の追加タスク

次の追加タスクを実行して、要件に従って SAML SSO セットアップを有効にすることができます。

Cisco Tomcat サービスの再起動

SAML シングルサインオンの有効化または無効化の前後には、シングルサインオンが実行されているすべての Cisco 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。

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。

ADFS の追加の Expressway 設定

Active Directory フェデレーション サービスを使用して Expressway の SAML SSO を展開する場合は、次の追加の Expressway 設定を実行します。

ステップ 1 信頼当事者証明が ADFS で作成されたら、Windows PowerShell® で、各 Expressway-E <Name> に対して次のコマンドを実行します。

`Set-ADFSRelyingPartyTrust -TargetName "<EntityName>" -SAMLResponseSignature MessageAndAssertion`。`<EntityName>` は、ADFS で設定されている Expressway-E の 信頼当事者証明の名前に置き換えてください。

ステップ 2 ADFS で、各信頼当事者証明にクレームルールを追加します。

a) **[クレームルールの編集（Edit Claims Rule）]** ダイアログを開き、AD 属性にクレームとして送信される新規クレームルールを作成します。

b) 内部システムに対して OAuth ユーザーを識別するもの（通常は電子メールまたは SAMAccountName）に一致する AD 属性を選択します。

c) [進行中のクレームタイプ（Outgoing Claim Type）] として **uid** を入力します。

iOS Cisco Jabber の SSO ログインの動作設定

ステップ 1 Cisco Unified CM Administration 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。

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。

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**。

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 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 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。

IdP メタデータの更新

クラスタ内のすべてのサーバーで IdP メタデータ信頼ファイルを更新するには、次の手順を使用します。

Before you begin

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`。

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 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 5 [IdP メタデータファイルの更新（**Update IdP Metadata File**）] をクリックして、IdP メタデータ信頼ファイルをインポートします。

ステップ 6 [参照（**Browse**）] をクリックして IdP メタデータ信頼ファイルを選択し、[IdP メタデータのインポート（**Import IdP Metadata**）] をクリックしてファイルをコラボレーション サーバーにインポートします。

ステップ 7 [次へ] をクリックします。

ステップ 8 標準 CCM スーパーユーザー権限を持つ LDAP 同期を選択して、メタデータファイルが適切に設定されているかどうかを確認し、[SSO テストを実行（**Run SSO Test**）] をクリックします。

ステップ 9 有効なユーザーの認証情報を使ってサインインします。

ステップ 10 [完了（**Finish**）] をクリックして、クラスタ内のすべてのサーバーで SAML SSO セットアップを有効にします。

Note アプリケーションの更新のために短い遅延が発生します。SSO モードが「クラスタ全体」の場合、「Cisco Tomcat」、「Cisco SSOSP Tomcat」、および「Cisco UDS Tomcat」 サービスはクラスタ内のすべてのノードで再起動します。それ以外の場合は、IDP メタデータが更新された特定のノードでサービスが再起動します。

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>
```

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"/>
```

アップグレード後の OpenAM SSO から SAML SSO への再設定

リリース 11.0(1) の時点で、Unified Communications Manager は OpenAM SSO ソリューションを提供しなくなりました。Open AM SSO ソリューションが設定された以前のリリースからアップグレードした場合は、サポートされている IdP のいずれかを使用して SAML SSO ソリューションを使用するようにシステムを再設定する必要があります。このガイドに記載されている設定を使用して、SAML SSO を使用するようにシステムを再設定します。

（注） OpenAM SSO ソリューションと、アイデンティティプロバイダーに OpenAM を使用する SAML SSO ソリューションは異なるソリューションであるため、混同しないでください。SAML SSO を使用するようにシステムを再設定する場合は、このドキュメントに記載されている任意の IdP を使用できます。

ネットワーク移行後のクラスタの再プロビジョニング

SSO ログインを適切に機能させるには、ネットワーク移行後にクラスタを再プロビジョニングしてください。

（注） この手順は、SSO が有効になっているネットワーク移行クラスタにのみ適用されます。この手順は、単純な移行には適用されません。

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。

ステップ 1 Web ブラウザのアドレスバーに https://<*Unified CM-server-name*> の URL を入力します。ここで、<*Unified CM-server-name*> はサーバーのホスト名または 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 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 5 [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、アイデンティティ プロバイダーにアップロードするサーバー メタデータをダウンロードします。

ステップ 6 [IdP メタデータファイルの更新（**Update IdP Metadata File**）] をクリックして、IdP メタデータ信頼ファイルをインポートします。

ステップ 7 [参照（**Browse**）] をクリックして IdP メタデータ信頼ファイルを選択し、[IdP メタデータのインポート（**Import IdP Metadata**）] をクリックしてファイルをコラボレーション サーバーにインポートします。[次へ] をクリックします。

ステップ 8 標準 CCM スーパー ユーザー権限を持つ LDAP 同期を選択して、メタデータ ファイルが適切に設定されているかどうかを確認し、[テストの実行（**Run Test**）] をクリックします。

ステップ 9 [完了（**Finish**）] をクリックして、クラスタ内のすべてのサーバーで SAML SSO セットアップを有効にします。

アプリケーションの更新のために短い遅延が発生します。SSO モードが「クラスタ全体」の場合、「Cisco SSOSP Tomcat」、および「Cisco UDS Tomcat」サービスはクラスタ内のすべてのノードで再起動します。

SAML SSO 導入の相互作用および制限事項

特長	機能の相互作用
tomcat 証明書の再生成	Tomcat 証明書を再生成する場合は、サービスプロバイダーで新しいメタデータファイルを生成し、そのメタデータファイルを IdP にアップロードします。
メタデータの再生成	次のいずれかを実行すると、メタデータ ファイルが再生成されます。 • 自己署名証明書を Tomcat 証明書に、またはその逆に変更します。 • ITL リカバリ証明書への Tomcat 証明書の再生成。 Cisco Unified Communications Manager は、再生成されたメタデータ ファイルをダウンロードし、IdP にアップロードします。

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。