Cisco Unified Communications アプリケーション SAML SSO 導入ガイド、リリース 15

初版：2023 年 12 月 18 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

目的

『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』 では、Security Assertion Markup Language Single Sign-On（SAML SSO）ソリューションを有効にする方法について説明します。アプリケーション。このドキュメントでは、SAML ベースの SSO ソリューションで使用できるさまざまなアプリケーションと、ソリューションのユーザー認証を提供するサポートされている ID プロバイダー（IdP）について説明します。このドキュメントには、特定のコラボレーションアプリケーションの設定に関する製品マニュアルへのリンクが記載されています。

対象読者

このドキュメントは、さまざまな Cisco Unified Communications アプリケーションとサポートされている IdP の SAML ベースの SSO ソリューションに精通しているシステム管理者を対象としています。このガイドでは、Network Time Protocol（NTP）およびドメインネームシステム（DNS）サーバーの設定に関する知識も必要です。

マニュアルの構成

次の表に、このマニュアルの構成を示します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザーが値を指定する引数は、イタリック体で示しています。
文字列	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`screen フォント`	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字のスクリーン フォントで示しています。
`イタリック体の screen フォント`	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。

（注）は、次のように表しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒントは、次のように表しています。

ヒント 役立つ「ヒント」の意味です。

その他の情報

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、毎月更新される『シスコ製品ドキュメントの最新情報』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

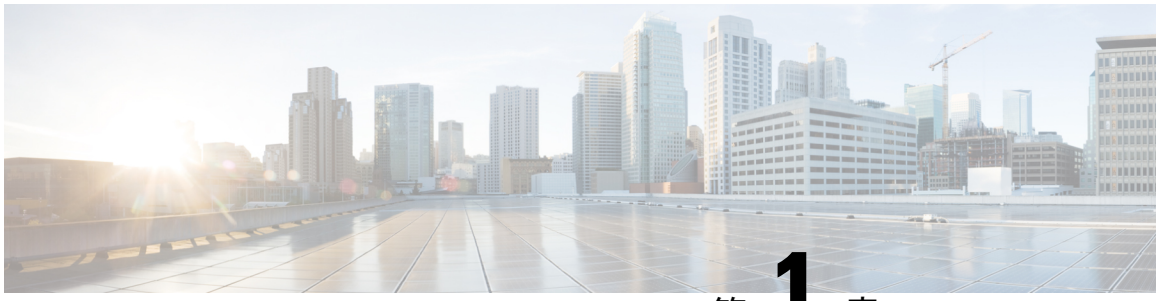
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『シスコ製品ドキュメントの最新情報』はRSSフィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意したものとみなされます。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、
http://www.access.gpo.gov/bis/ear/ear_data.html で参照できます。



第 1 章

新機能および変更された機能に関する情報

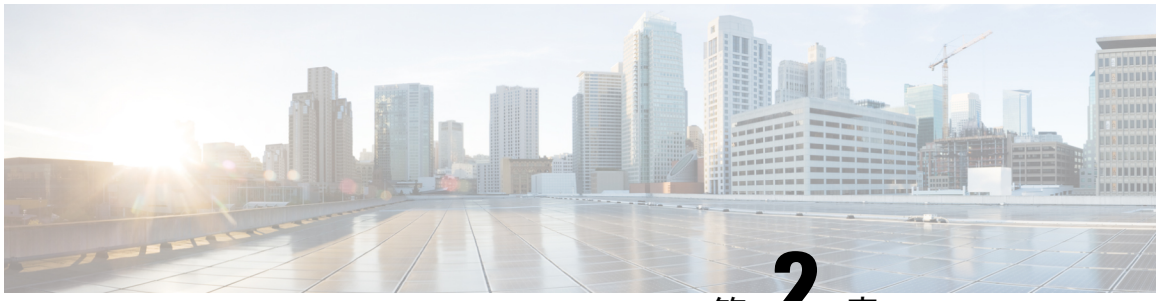
新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

***Table 1: Unified Communications Manager* と *IM and Presence* サービスの新機能と変更された動作**

日付	説明	参照先
2023 年 12 月 18 日	ネットワーク移行後の再プロビジョニングのサポートが追加されました。	ネットワーク移行後のクラスタの再プロビジョニング, on page 38

新機能および変更された機能に関する情報



第 2 章

SAML ベースの SSO ソリューション

SAML SSO ソリューションについて

重要 Cisco Jabber を Cisco Webex Meeting Server と共に展開する場合、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（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認証と承認データを交換できます。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通の資格情報や関連情報を使用します。

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。

シングル サインオン単一サービス プロバイダー合意

シングル サインオンを使用すると、いずれか 1 つのシスコ コラボレーション アプリケーションにログオンした後、複数のコラボレーション アプリケーションにアクセスできます。Unified Communications Manager リリース 11.5 より前のリリースでは、管理者が SSO を有効にすると、各クラスタ ノードが URL と証明書を使って独自のサービス プロバイダ メタデータ（SP メタデータ）ファイルを作成しました。作成された各ファイルを ID プロバイダ（IDP）サーバに個別にアップロードする必要がありました。IDP サーバがそれぞれの IDP/SAML 交換を個別の合意と見なしたので、クラスタ内のノード数と等しい数の合意が作成されました。

ユーザ エクスペリエンスを改善し、大規模な導入でのソリューション全体のコストを削減するために、このリリースでは機能強化されました。現在では、Unified Communications Manager クラスタ（Unified Communications Manager とインスタント メッセージングおよびプレゼンス（IM and Presence））で単一の SAML 合意がサポートされます。

SAML-Based SSO の機能

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザー名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。SAML SSO を使用することで、IdP とサービスプロバイダーの間で信頼の輪を作成できます。サービス プロバイダーは IdP 信頼して、ユーザを認証します。

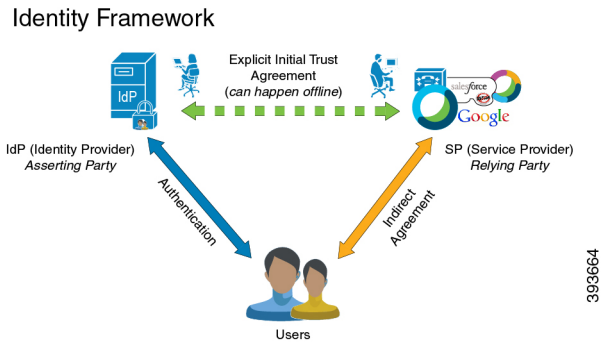
- 認証情報を保護し、安全に保ちます。暗号化機能により、IdP、サービス プロバイダー、ユーザの間で認証情報を保護します。SAML SSO では、IdP とサービスプロバイダー間で転送される認証メッセージを外部ユーザーから保護することもできます。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

SAML SSO ソリューションの基本要素

- クライアント（ユーザのクライアント）：これは、認証用にブラウザインスタンスを活用できる、ブラウザベースのクライアントまたはクライアントです。システム管理者のブラウザはその一例です。
- サービスプロバイダー：これは、クライアントがアクセスを試みるアプリケーションまたはサービスです。たとえば、Cisco Unified Communications Manager です。
- ID プロバイダー（IdP）サーバ：これは、ユーザ資格情報を認証し、SAML アサーションを発行するエンティティです。
- Lightweight Directory Access Protocol（LDAP）ユーザ：これらのユーザは、Microsoft Active DirectoryやOpenLDAPなどのLDAPディレクトリと統合されます。非LDAPユーザーは、Unified Communications サーバー上にローカルに存在します。
- SAML アサーション：これは、ユーザ認証のために、IdP からサービス プロバイダーに転送されるセキュリティ情報で構成されます。アサーションは、ユーザ名や権限などのサブジェクトに関する信頼されたステートメントを含む、XML ドキュメントです。通常では、信頼性を確保するために、SAML アサーションはデジタル署名されます。
- SAML リクエスト：これは、Unified Communications アプリケーションにより生成される認証リクエストです。LDAP ユーザーを認証するために、Unified Communications アプリケーションは認証要求を IdP に委任します。
- 信頼の輪（CoT）：これは、共同で 1 つの IdP に対して共有と認証を行うさまざまなサービス プロバイダーで構成されます。
- メタデータ：これは、SSO 対応の Unified Communications アプリケーション（Unified Communications Manager、Cisco Unity Connection など）や IdP によって生成される XML ファイルです。SAML メタデータの交換により、IdP とサービス プロバイダーの間に信頼関係が確立します。
- Assertion Consumer Service（ACS）URL：この URL は、アサーションをポストする場所を IdP に指示します。ACS URL は、最終的な SAML 応答を特定の URL にポストすることを IdP に指示します。

（注） 認証が必要なすべてのインスコープ サービスでは、SSO のメカニズムとして SAML 2.0 を使用します。

SAML SSO ソリューションの ID フレームワークについては、次の図を参照してください。



SAML SSO をサポートする Cisco Unified Communications アプリケーション

- Unified Communications Manager
- Unified Communications Manager IM and Presence Service

（注） SAML SSO の設定の詳細については、『*Features and Services Guide for Cisco Unified Communications Manager, Release 10.0(1)*』の「SAML Single Sign-On」の章を参照してください。

- Cisco Unity Connection

（注） Cisco Unity Connection サーバでの SAML SSO 機能の設定の詳細については、『*System Administration Guide for Cisco Unity Connection Release 10.x*』の「Managing SAML SSO in Cisco Unity Connection」の章を参照してください。

- Cisco Prime Collaboration

（注） Cisco Prime Collaboration サーバでの SAML SSO 設定手順の詳細については、『 *Cisco Prime Collaboration 10.0 Assurance* ガイド - アドバンスド』ガイドの「Managing Users」の章にある「Single Sign-On for Prime Collaboration」の項を参照してください。

- Cisco Unified Real-Time Monitoring Tool（RTMT）

（注） RTMT の SAML SSO を有効にする方法の詳細については、『 *System Configuration Guide for Cisco Unified Communications Manager*』の「Configure Initial System and Enterprise Parameters」の章にある「Configure SSO for RTMT」の手順を参照してください。

- Cisco Expressway

（注） Cisco Expressway の SAML SSO 設定情報を取得するには、『 *Cisco Expressway* 管理者ガイド』 を参照してください。

Cisco Unified Communications Manager Web インターフェイスの SAML SSO サポート

このリリースでは、Cisco Unified OS Administration およびディザスタリカバリシステムが Security Assertion Markup Language（SAML）SSO でサポートされるアプリケーションになりました。SAML SSO が有効になっている場合、ID プロバイダ（IdP）でシングル サインインした後、RTMT アプリケーションや、サポートされる他のアプリケーション（Ciscoユニファイドコミュニケーション マネージャ など）を起動できます。これらのアプリケーションに個別にサインインする必要はなくなりました。

Cisco Unified OS Administration およびディザスタリカバリシステムで SAML SSO をサポートするために、レベル 4 の管理者は Active Directory にレベル 0 とレベル 1 の管理者を作成します。レベル 4 の管理者は、クラスタのすべてのノードにプラットフォーム管理者を追加します。この追加により、プラットフォーム管理者は Active Directory とプラットフォーム データベースの間で同期されます。プラットフォームデータベースでユーザーを設定する際、管理者はユーザーの **uid** 値を設定する必要があります。Cisco Unified OS Administration およびディザスタリカバリシステムアプリケーションは、**uid** 値を使用してユーザを承認します。IdP サーバーは、Active Directory サーバーに対してクレデンシャルを認証し、SAML 応答を送信します。認証後、Unified Communications Manager は **uid** 値を使用してプラットフォーム データベースからユーザを承認します。**uid** 値の詳細については、「プラットフォームユーザーの一意の識別値の設定 （8 ページ） 」の手順を参照してください。

既存のリリースでSAML SSOが有効になっていて、以前のリリースから新しいリリースにアップグレードする場合、SAML SSO サポートは新しいリリースの Unified OS Administration および Disaster Recovery System アプリケーションで使用できます。Unified Communications Manager Web アプリケーションの SAML SSO を有効にすると、これらのアプリケーションの SAML SSO サポートも有効になります。新しいリリースで SAML SSO サポートを有効にするには、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』の「SAML SSO Enablement」トピックを参照してください。

（注） Unified Communications Manager 管理者に対して SAML SSO サポートが有効になっている場合、クラスタ全体に適用できます。ただし、Cisco Unified OS Administration および Disaster Recovery System アプリケーションの場合、各プラットフォーム管理者はノードに固有であり、これらのユーザの詳細はクラスタ全体に複製されません。したがって、各プラットフォームユーザは、クラスタの各サブスクライバ ノードに作成されます。

プラットフォームユーザーの一意の識別値の設定

一意の識別（UID）値は、プラットフォーム ユーザがプラットフォーム ページで SSO ログインを実行することを許可するために使用されます。レベル4の管理者は、次のいずれかの方法でプラットフォーム管理者用にこの値を設定できます。

- CLI で **set account name** コマンドを使用します。
- 既存の **uid** 値を更新します。

（注） 詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「**set account name**」コマンドと「**set account ssouidvalue**」を参照してください。

Cisco Unified OS Administration のリカバリ URL サインインオプション

このリリースでは、プラットフォーム管理者は、SAML SSO 対応アプリケーションのいずれかにサインインするか、リカバリ URL オプションを使用して、Cisco Unified OS Administration にアクセスできます。このオプションは、SSO 対応ノードのメインページで [シングルサインオン（**Single Sign On**）] リンクをバイパスするための**リカバリ URL** として使用できます。プラットフォームユーザは、リカバリ URL アクセス権を持っている場合、Cisco Unified OS Administration にサインインできます。

（注） SSO のみを有効にし、リカバリ URL を有効にせず、認証ユーザーに十分なアクセス権限がない場合、403 エラー（アクセス拒否応答）のみが表示されます。ただし、[リカバリ URL（Recovery URL）] を有効にすると、エラーが発生すると、認証ユーザは [リカバリ URL（Recovery URL）] ページにリダイレクトされます。

レベル 4 の管理者は、プラットフォームユーザーのリカバリ URL サインインオプションを設定します。管理者は、CLI を使用してプラットフォーム管理者を作成している間、または CLI コマンドを使用して詳細を更新しているときに、このオプションを有効にできます。新規および既存のプラットフォーム管理者用のリカバリ URL ログイン用の CLI コマンドの詳細については、『 *Cisco Unified Communications* ソリューション コマンド ライン インターフェイス リファレンス ガイド』 の **set account ssorecoveryurlaccess**コマンドを参照してください。

（注） デフォルトでは、レベル 4 の管理者に対して [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** ）] リンクが有効になっています。このリンクは、以前のリリースから新しいリリースにアップグレードする場合、プラットフォーム管理者レベル 0 およびレベル 1 に対して有効になります。

ソフトウェア要件

SAML SSO 機能には、次のソフトウェア コンポーネントが必要です。

- Cisco Unified Communications アプリケーション、リリース 10.0(1) 以降。
- IdP サーバーによって信頼され、Cisco Unified Communications アプリケーションによってサポートされる LDAP サーバー。
- SAML 2.0 標準に準拠する IdP サーバー。
- Unified Communications Manager でサポートされるログインフローは SP によって開始されます。

ID プロバイダー（IdP）の選択

シスコ コラボレーション ソリューションは、SAML 2.0（セキュリティ アサーション マークアップ言語）を使用して、ユニファイド コミュニケーション サービスを利用するクライアント用の SSO（シングル サインオン）を有効にします。

SAML ベースの SSO は、企業ネットワーク内部から発信された UC サービス要求を認証するためのオプションであり、モバイルおよびリモートアクセス（MRA）を介して外部から UC サービスを要求するクライアントに拡張されました。

使用する環境に SAML ベース SSO を選択した場合は、次の点に注意してください。

- SAML 2.0 は、SAML 1.1 との互換性がないため、SAML 2.0 標準を使用する IdP を選択する必要があります。
- SAML ベースのアイデンティティ管理は、コンピューティングとネットワーキング業界のベンダーによって異なる方法で実装されています。したがって、SAML 標準に準拠するための幅広く受け入れられている規制はありません。
- 選択した IdP の設定や管理ポリシーは、Cisco TAC（テクニカル アシスタンス センター）のサポート対象外です。IdP ベンダーとの関係とサポート契約を利用して、IdP を正しく設定する上での支援を得られるようにしてください。Cisco は IdP に関するエラー、制限、または特定の設定に関する責任を負いません。

シスコ コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、シスコ コラボレーション ソリューションでテストされているのは次の IdP だけです。

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0、3.0、4.0、5.0
- Microsoft Azure
- PingFederate® 6.10.0.4
- F5 BIG-IP 11.6.0
- Okta 2017.38

SAML のコンポーネント

SAML SSO ソリューションは、特定のアサーション、プロトコル、バインディング、プロファイルの組み合わせに基づきます。さまざまなアサーションは、プロトコルやバインディングを使用しているアプリケーション間やサイト間で交換され、これらのアサーションによりサイト間でユーザを認証します。SAML のコンポーネントは次のとおりです。

- SAML アサーション：これは、IdP からサービス プロバイダーに転送される情報の構造と内容を定義します。セキュリティ情報のパケットで構成され、サービスプロバイダーがさまざまなレベルのアクセスコントロールの決定に使用するステートメントが含まれています。

  SAML SSO は、次のタイプのステートメントを提供します。

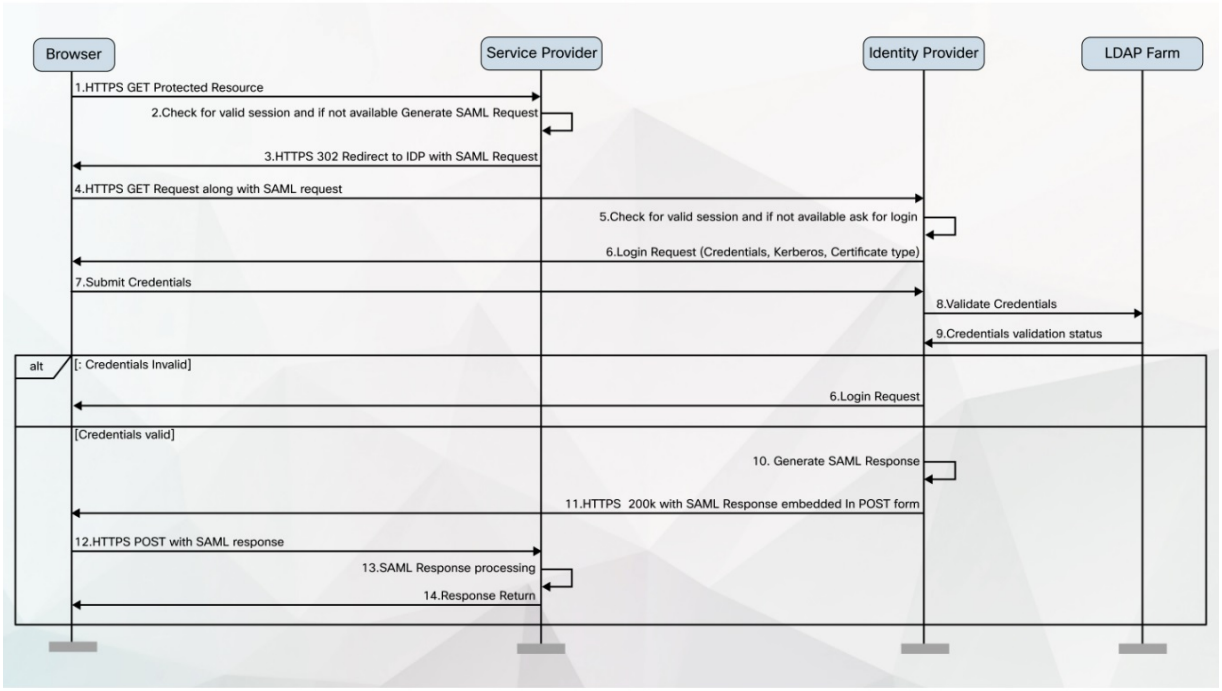
  - 認証ステートメント：これらのステートメントは、IdP とブラウザの間で特定の時間に行う認証の方法について、サービス プロバイダーにアサートします。
  - 属性ステートメント：これらのステートメントは、ユーザに関連付ける特定の属性（名前と値のペア）についてアサートします。属性アサーションには、ユーザに関する具体的な情報が含まれます。サービスプロバイダーは、属性を使用してアクセス制御の決定を行います。

- SAMLプロトコル：SAMLプロトコルは、SAMLがアサーションをどのように要求し、取得するかを定義します。このプロトコルは、特定の SAML エレメントまたはアサーションで構成されている、SAML 要求と応答エレメントに対応します。SAML 2.0 には次のプロトコルがあります。
  - アサーション クエリと要求のプロトコル
  - 認証要求のプロトコル
- SAML バインディング：SAML バインディングは、SOAP 交換のような、標準メッセージング形式または通信プロトコルとのSAMLアサーションまたはプロトコルメッセージ（またはその両方）の交換のマッピングを指定します。Unified Communications 10.0 は次の SAML 2.0 バインディングをサポートしています。
  - HTTP Redirect（GET）バインディング
  - HTTP POST バインディング
- SAMLプロファイル：SAMLプロファイルでは、明確に定義された使用事例をサポートするために、SAMLアサーション、プロトコル、およびバインディングの組み合わせについて詳細に説明しています。Unified Communications 10.0 は、SAML 2.0 Web ブラウザ SSO プロファイルをサポートしています。

SAML SSO コールフロー

このセクションでは、 SAML SSO 機能を使用して Unified Communications アプリケーションのシングルサインオンを有効にする方法について説明します。このセクションでは、IdP とサービスプロバイダーの関係についても説明し、シングルサインオンを有効にするためのさまざまな構成設定の重要性を特定するのに役立ちます。

図 *1 : IdP* からのクレデンシャル要求の *SAML SSO* コール フロー



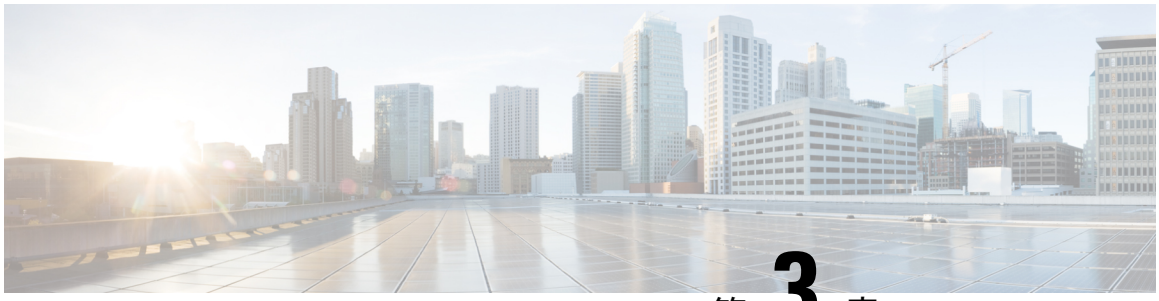
1	ブラウザベースのクライアントが、サービスプロバイダーの保護されたリソースにアクセスしようとします。 （注）　ブラウザにサービスプロバイダーとの既存のセッションがありません。

2	ブラウザから要求を受信すると、サービスプロバイダーは SAML 認証要求を生成します。 （注） SAML 要求には、要求を生成したサービス プロバイダーを示す情報が含まれます。後で、これにより、IdP は要求を開始した特定のサービスプロバイダーを知ることができます。 SAML 認証を正常に完了するには、IdP にアサーション コンシューマ サービス（ACS）URL が必要です。ACS URL は、最終的な SAML 応答を特定の URL にポストすることを IdP に指示します。 （注） Unified Communications Manager および VOS 製品は、SAML 2.0 標準に準拠したアサーション コンシューマ サービス インデックス URL を使用します。 （注） 認証要求は IdP に送信でき、アサーションはリダイレクトまたは POST バインディングを介してサービス プロバイダーに送信できます。たとえば、Unified Communications Manager は、いずれの方向でも POST バインディングをサポートします。
3	サービス プロバイダーは、ブラウザに要求をリダイレクトします。 （注） IdP URL は、SAML メタデータ交換の一部としてサービスプロバイダーで事前設定されています。
4	ブラウザはリダイレクトに従い、HTTPS GET 要求を IdP に発行します。SAML 要求は、GET 要求のクエリパラメータとして維持されます。
5	IdP は、ブラウザとの有効なセッションをチェックします。
6	ブラウザ内に既存の Cookie がない場合、IdP はブラウザへのログイン要求を生成し、IdP によって設定および適用されている認証メカニズムを使用してブラウザを認証します。 （注） 認証メカニズムは、顧客のセキュリティおよび認証要件によって決定されます。これは、ユーザー名とパスワード、Kerberos、PKI などを使用したフォームベースの認証である可能性があります。この例では、フォームベースの認証を想定しています。
7	ユーザーはログインフォームに必要なログイン情報を入力し、IdP にポストバックします。 （注） ロギングの認証チャレンジは、ブラウザと IdP の間で行われます。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。
8	IdP は LDAP サーバーにクレデンシャルを送信します。
9	LDAP サーバーは、クレデンシャルのディレクトリをチェックし、検証ステータスを IdP に返します。

10	IdP はクレデンシャルを検証し、SAML アサーションを含む SAML 応答を生成します。 （注） アサーションは IdP によってデジタル署名され、ユーザーはサービス プロバイダーで保護されたリソースへのアクセスが許可されます。IdP もここでクッキーを設定します。
11	IdP は SAML 応答をブラウザにリダイレクトします。
12	ブラウザは非表示形式の POST 命令に従い、サービス プロバイダーの ACS URL にアサーションをポストします。
13	サービスプロバイダーは、アサーションを抽出し、デジタル署名を検証します。 （注） サービスプロバイダーは、このデジタル署名を使用して、IdP との信頼の輪を確立します。
14	サービス プロバイダーは、保護されたリソースへのアクセスを許可し、ブラウザに 200 OK と応答してリソース コンテンツを提供します。 （注） サービス プロバイダーは、リソース認証を担当します。たとえば、ユーザが IdP によって正常に認証されても、Cisco Unified Communications Manager で設定されている管理者ロールの権限を持っていない限り、Cisco Unified CM Administration インターフェイスにログインできない場合があります。 （注） サービスプロバイダーは、ここでクッキーを設定します。追加のリソースに対するブラウザによる後続の要求がある場合、ブラウザは要求にサービスプロバイダーのクッキーを含めます。サービスプロバイダーは、ブラウザとのセッションがすでに存在するかどうかを確認します。セッションが存在する場合、Web ブラウザはリソースの内容を返します。

Okta 経由の RTMT への SAML SSO ログインの Java 要件

Okta が id プロバイダーとして設定されている SAML SSO があり、SSO を使用して Cisco ユニファイド リアルタイム モニタリング ツールにログインする場合は、最小 Java バージョン8.221 を実行している必要があります。この要件は Ciscoユニファイド コミュニケーション マネージャ および IM and Presence Service の 12.5(x) リリースに適用されます。



第 3 章

ID プロバイダーの SAML SSO の要件

ID プロバイダーの要件

このセクションでは、シスコ コラボレーション アプリケーションに SAML SSO サービスを導入するためにアイデンティティ プロバイダーが満たす必要がある要件の概要を示します。

ID プロバイダーは、次のガイドラインに従う必要があります。

- サポートは SAML 2.0 のみです。
- サービスプロバイダーが開始した SSO のみをサポートします。
- NameID Format 属性を *urn:oasis:names:tc:SAML:2.0:nameid-format:transient* に設定します。
- LDAP 属性にマッピングされた値（SAMAccountName など）に *uid* 属性名を含めるように、IdP で要求を設定します。
- Cisco Unified Communications Manager は、認証要求で ACS URL インデックスを使用します。IdP は、サービスプロバイダーのメタデータで ACS URL へのインデックスを作成できる必要があります。これは SAML 標準に準拠しています。
- SAML アサーションの署名と暗号化の部分で複数の証明書を使用することはサポートされていません。 CSCvq78479を参照してください。

SAML SSO を設定する場合は、Cisco Collaboration Deployment に以下を展開してください。

- Network Time Protocol：Cisco Collaboration Deployment と ID プロバイダーの時刻が同期されるように、NTP を環境に展開します。IdP とシスコ コラボレーション展開の時間差が 3 秒を超えないようにしてください。

- DNS：シスコ コラボレーション アプリケーションと ID プロバイダーは、互いのアドレスを解決できる必要があります。
- [LDAP]：Cisco Collaboration 展開で LDAP ディレクトリ同期を設定する必要があります。ただし、LDAP 認証を無効にすることを推奨します。
- 証明書：シスコ コラボレーション展開と ID プロバイダーの間でメタデータ ファイルを交換する必要があります。メタデータには、コラボレーション展開と ID プロバイダー間の信頼関係を作成するために必要な証明書が含まれています。Tomcat 証明書またはシステム生成の自己署名証明書を使用して、信頼を確立できます。

SAML 契約タイプ

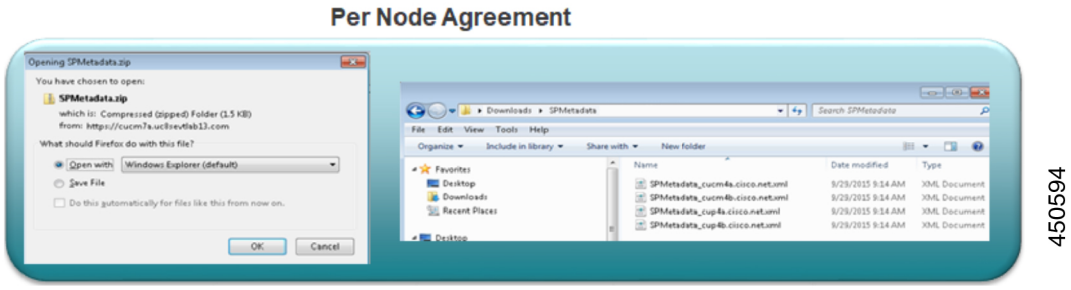
Cisco Unified Communications Manager は、次の 2 種類の SAML メタデータ契約をサポートしています。

- クラスタ全体：この展開では、クラスタ全体をカバーする単一のメタデータ契約を設定する必要があります。
- [ノードごと（Per Node）]：この展開では、クラスタノードごとに個別の契約を使用して、複数のメタデータ契約を設定する必要があります。各クラスタノードには、ID プロバイダーとの個別のメタデータ交換があります。

図 *2 : Cisco Unified Communications Manger* の *2* 種類の *SAML* メタデータ契約

次の図は、ノードごとの契約を使用して Cisco Unified Communications Manager で生成されたメタデータ zip ファイルの内容を示しています。この例では、IM and Presence Service は標準展開（非集中型）を使用して展開されるため、zip ファイルには、Unified Communications Manager および IM and Presence Service クラスタノードごとに個別のメタデータ xml ファイルが含まれています。

図 *3 : Cisco Unified Communications Manger* からダウンロードした *UC* メタデータファイル

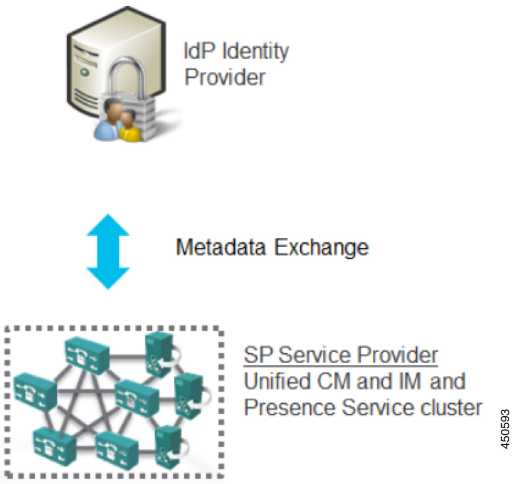


（注） IM and Presence Service の集中配置を使用している場合、IM and Presence 配置はテレフォニークラスタとは別のクラスタにあります。クラスタ全体の契約では、テレフォニークラスタと IM and Presence クラスタのメタデータを個別に生成する必要があります。

メタデータ交換

SAML SSO を設定するプロセスの一環として、UC 展開と ID プロバイダーの間でメタデータファイルを交換する必要があります。

図 *4 : SAML* メタデータ交換



次に、サービス プロバイダー（Cisco Unified Communications Manager）から生成された UC メタデータ ファイルの例を示します。

Cisco Unified Communications ManagerからのIdPメタデータファイルのエクスポート

```
<?xml version="1.0" encoding="UTF-8"?>
<!--With Single Cluster agreement the entityID is always the publisher FQDN-->
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="cucm0a.identitylab20.ciscolabs.com" entity ID="cucm0a.identitylab20.ciscolabs.com">
    <!--We don't require AuthN or signed Assertions but comply to what the IdP requests-->

     <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
       <md:KeyDescriptor use="signing">
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:X509Data>
       <ds:X509Certificate>MIIDzzCCA........</ds:X509Certificate>
     </ds:X509Data>
   </ds:KeyInfo>
  </md:KeyDescriptor>
   <!--Certificate for Signing and/or Encryption-->
  <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIIDzzCCA........</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
   <!--We only support name-id format transient-->
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>

         <!--ACS URL for the Client to POST the answer from the IdP, two per node in
the cluster-->
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

Location="https://cucm0a.identitylab20.ciscolabs.com:8443/ssosp/saml/SSO/alias/cucm0a.identitylab20.ciscolabs.com"
 index="0"/>
              <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://cucm0a.identitylab20.ciscolabs.com:8443/ssosp/saml/SSO/alias/cucm0a.identitylab20.ciscolabs.com"
 index="1"/>
     </md:SPSSODescriptor>
</md:EntityDescriptor>
```

次に、IDプロバイダー（Active Directoryフェデレーション サービス）から生成されたメタデータ ファイルの例を示します。

IDプロバイダーからのメタデータファイル（Active Directoryフェデレーションサービス）

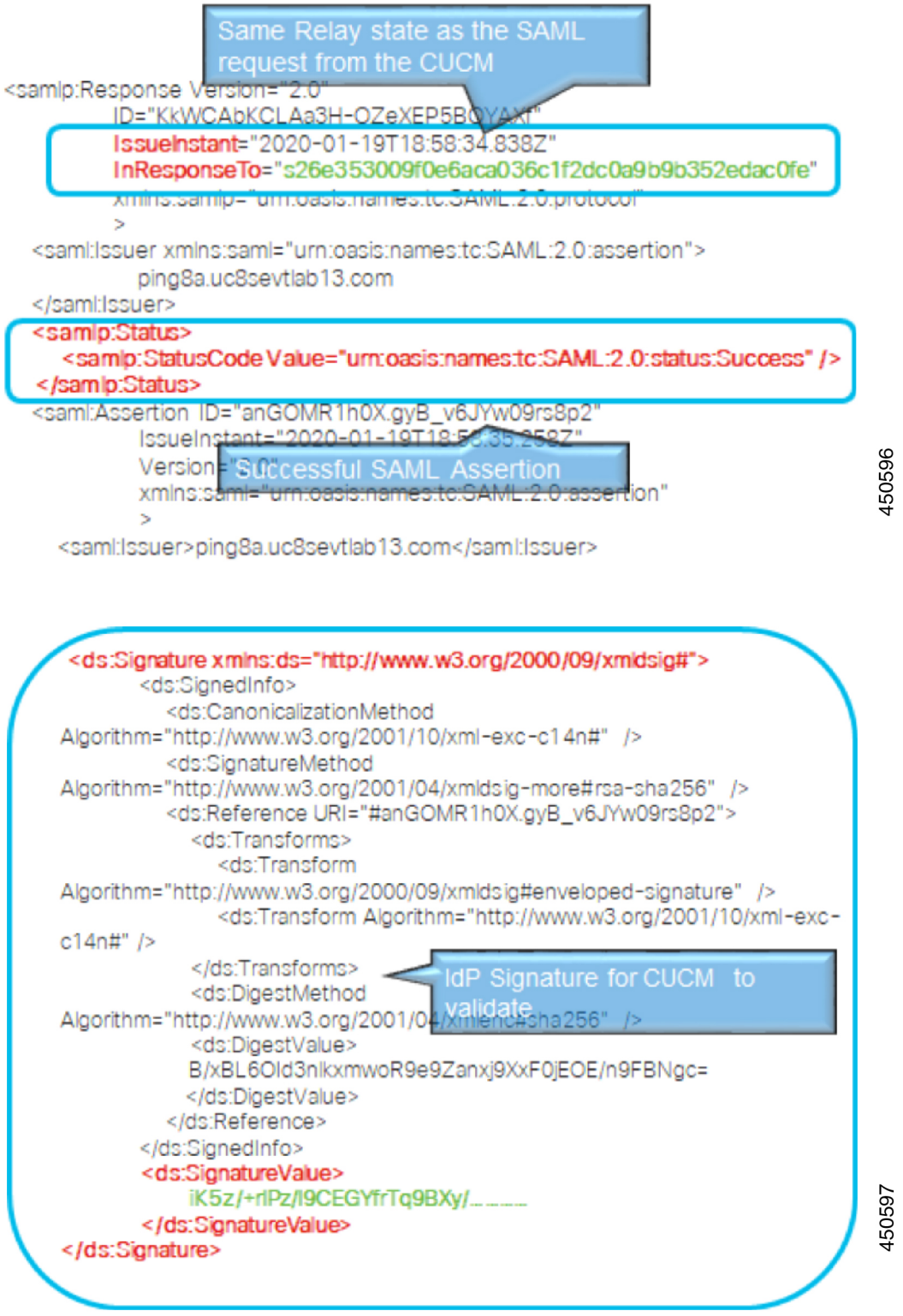
```
<?xml version="1.0"?
<!--entityID=IdP Entity ID-->
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_b12fe1b5-6866-40cc-94be-9d9d8cb71916"
   entityID="http://WIN-2019SSO.cisco-dod.com/adfs/services/trust">
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

    <ds:Reference URI="#_b12fe1b5-6866-40cc-94be-9d9d8cb71916">
                  <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
      <!--Sign the metadata provided to the SP for extra security-->
```

```
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>VAcIv2uw6zG8YVVWP0IDYMZ/e7CN9o4oR8XBGiysujY=</ds:DigestValue>
    </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue>44RAgZ17YfwLdcRodZPcZ5PH05sLVbkDx4uAYq+EC4K+ZhiTs8aUZQ/.........
   </ds:SignatureValue>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <X509Data>
   <IDPSSODescriptor
protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
http://schemas.xmlsoap.org/ws/2005/02/trust
http://docs.oasis-open.org/wsfed/federation/200706"
ServiceDisplayName="administrator.cisco-dod.com">
 <KeyDescriptor use="encryption">
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <X509Data>
  <X509Certificate>MIIGHzCCBQegAwIBAgITHAAADUerWbVHyqoM.........
  </X509Certificate>
     </X509Data>
   </KeyInfo>
 </KeyDescriptor>
 <KeyDescriptor use="signing">
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <X509Data>
         <!--Cert for signing and/or encrypting the SAML Assertion-->
  <X509Certificate>MIIC7jCCAdagAwIBAgIQJH7di/.........</ds:X509Certificate>
    </KeyInfo>
 </KeyDescriptor>
   <!--Single Sign On Service details for HTTP-Redirect and HTTP-POST-->
   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/"/
   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/"/>
   <!--NameID format offer for this agreement-->
   <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
   <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="0" isDefault="true"/>
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
 Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="1"/>
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="2"/>
   </IDPSSODescriptor>
</EntityDescriptor>
```

SAML アサーション

次に、ID プロバイダーから Cisco Unified Communications Manager に送信される SAML アサーションの例を示します。

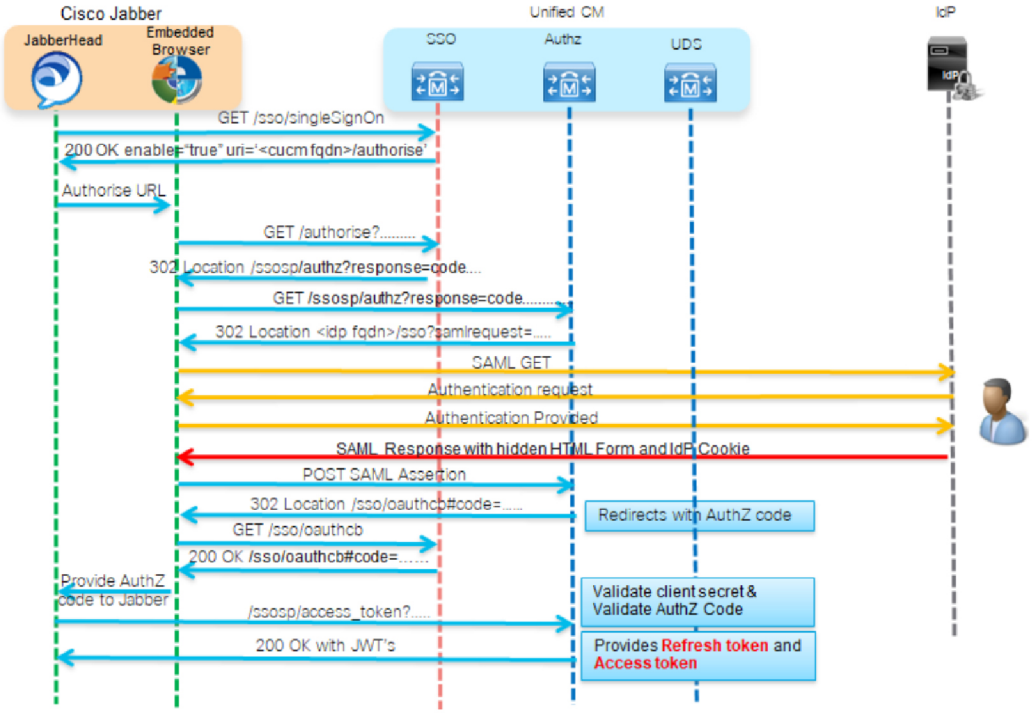
図 *5 : SAML* アサーションの例

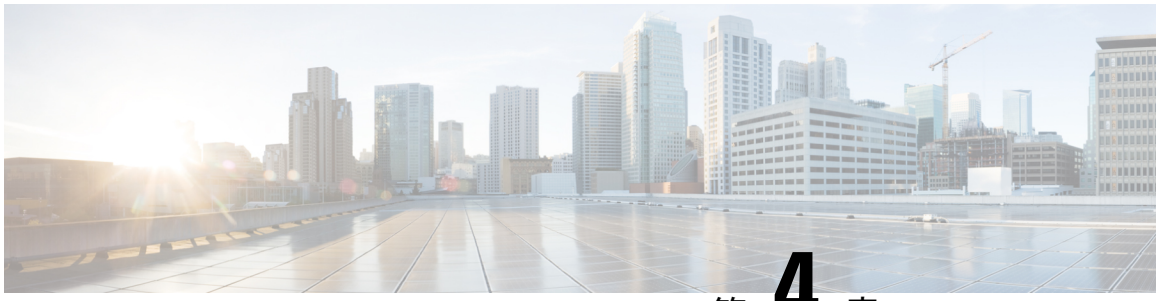


SAML OAuth 認証フロー

次に、ID プロバイダーを使用した OAuth 認証要求の認証フローの例を示します。

図 *6 : SAML OAuth* 認証フロー





第 4 章

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 （28 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 （31 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 （31 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 *2:* 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 （34 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。

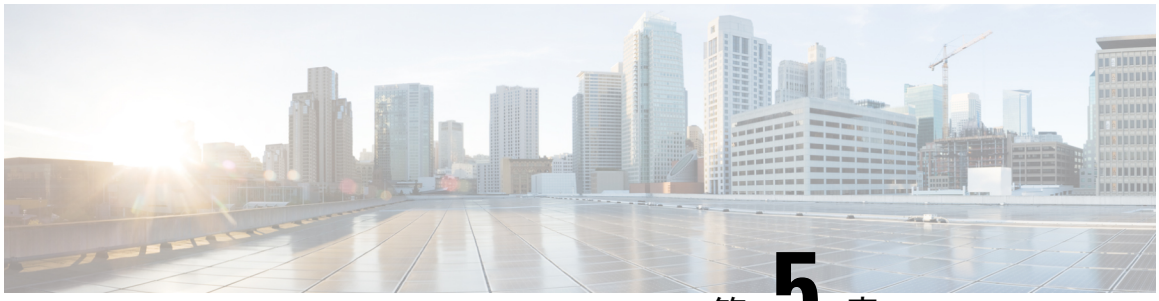
ステップ 8 標準 CCM スーパー ユーザー権限を持つ LDAP 同期を選択して、メタデータ ファイルが適切に設定されているかどうかを確認し、[テストの実行（**Run Test**）] をクリックします。

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。



第 5 章

エンドユーザーSAML SSO

エンドユーザー SAML SSO の設定

エンドユーザーまたはフェデレーテッド SSO は、製品が顧客のコンプライアンス要件を満たし、総所有コストを削減し、エンドユーザーエクスペリエンスを向上させるための標準です。コラボレーション製品でのこのサポートの基盤は、10.0 および 10.5 リリースで導入されました。これにより、管理者は、2014 年後半にリリース 10.5 でユーザのサポートを展開する Cisco Unity Connection や Cisco Jabberなどのエンド ユーザ クライアントに備えてインフラストラクチャを設定できます。

管理者がユーザに対してこの機能を有効にすると、シスコ コラボレーション アプリケーションのユーザは、企業のユーザ名とパスワードを使用して、サポートされているアプリケーションにログインできます。シスコのアプリケーションにブラウザ経由でアクセスする場合、ユーザは同じ企業ユーザ名とパスワードを使用してログインできます。ユーザが同じブラウザで別の企業アプリケーションにすでにログインしている場合は、をクリックして、ユーザー名とパスワードを入力します。これらの機能はすべて、お客様のネットワーク内で使用することも、VPN 経由でアクセスすることもできます。

サポートされている製品は次のとおりです。

製品	リリースからのエンドユーザー SAML SSO のサポート	詳細情報
Cisco Unified Communications Manager	10.5	ここをクリックしてください。
IM and Presence Service	10.5	ここをクリックしてください。
Cisco Unity Connection	10.5	ここをクリックしてください。
Webex Meeting Center	Cloud	ここをクリックしてください。

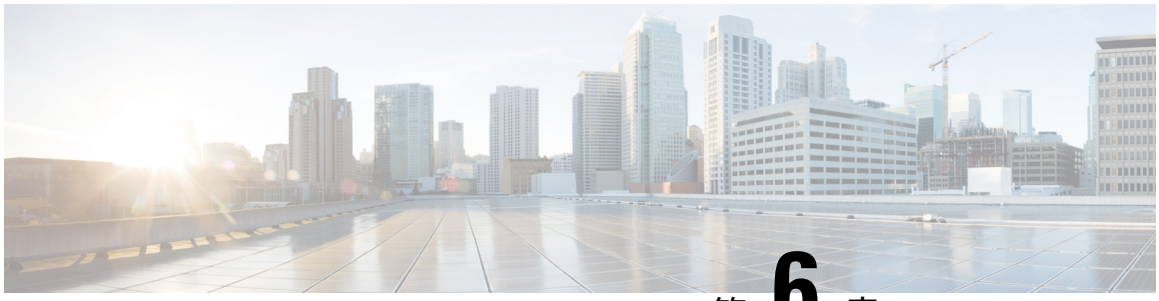
製品	リリースからのエンドユーザー SAML SSO のサポート	詳細情報
Webex Connect と Messenger	Cloud	ここをクリックしてください。
Cisco Webex Meetings Server	1.5 および 2.0	ここをクリックしてください。

サポートされているエンド ユーザー クライアントは次のとおりです。

製品	リリース	詳細情報
Webex iOS	提供中のリリース バージョンの種類	ここをクリックしてください。
WebEx Android	提供中のリリース バージョンの種類	ここをクリックしてください。
Webex Connect	提供中のリリース バージョンの種類	ここをクリックしてください。
Webex Messenger	提供中のリリース バージョンの種類	ここをクリックしてください。
Jabber for Windows	10.5	2014 年後半に提供開始
Jabber IOS	10.5	2014 年後半に提供開始
Android 向けの Jabber	10.5	2014 年後半に提供開始
Jabber for Mac	10.5	2014 年後半に提供開始

（注）

- Cisco Jabber を Cisco Webex Meeting Server と共に展開する場合、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。
- Mac で Cisco Jabber が SSO を使用して実行されている場合、Jabber サービスに対して承認されると、Jabber は自動的に cookie を設定できません。Mac の動作では、デフォルトでは、ユーザが移動するサイトの Cookie のみが許可されます。Jabber は、認証を確認する必要があるたびに、IdP に移動する必要があります。
- SAML アサーションには、Webex の電子メールアドレスを含める必要があります。 SAML スキーマは、それをカバーするように調整する必要があります。
- OAuth タイマーの期限切れを正しくトリガーするには、Unified Communications Manager での OAuthTokenExpiry の値が、Tomcat での WebsessionApp expiry の値よりも大きいことを確認します。



第 6 章

SAML ベースの SLO

SAML ベースのシングルログアウト（SLO）のサポート

Unified CM は、SAML ベースのシングルログアウト（SLO）をサポートしています。SLO を使用すると、シングルサインオン（SSO）を使用してサインインしたブラウザのすべてのセッションから同時にログアウトすることができます。

IdP メタデータを変更し、ルートアクセスを使用してサーバー上の idp.xml を置き換える場合は、Cisco Tomcat および Cisco SSOSP Tomcat サービスを再起動する必要があります。SSO の有効化中に SLO を設定する場合は、サービスを再起動する必要はありません。また、IdP メタデータを変更し、[SAML SSO] ページの [IdP メタデータの更新（Update IdP metadata）] オプションを使用して、サーバーの idp.xml を置き換えることもできます。

SLO は、実行中のすべてのセッションを同時に終了しません。たとえば、2 つの異なるブラウザで 4 つのセッションが実行されている場合、ログアウトを開始したブラウザに関連付けられているセッションは閉じられます。他のブラウザに関連付けられているセッションは開いたままです。

次の IdP（ID プロバイダー）がシングルログアウトをサポートしています。

- OpenAM 10.0.1
- F5 BIG-IP 11.6.0
- Okta 2017.38
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0) Microsoft Active Directory フェデレーション サービス idPs 2.0 を使用してログアウトするには、idp.xml ファイルでログアウト URL を設定します。

（注） PingFederate 6.10.0.4 IdP はシングルログアウトをサポートしていません。

SLO での IdP の設定例の詳細については、「コンフィギュレーションの例およびテクニカルノート」を参照してください。

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。