Cisco Unified Communications アプリケーション SAML SSO 導入ガイド、リリース 11.0(1)

初版：2014 年 12 月 05 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

目的

『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』では、Security Assertion Markup Language のシングル サインオン（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。このソリューションにより、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。このマニュアルでは、SAML-based 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に加えて、ソリューションに対してユーザ認証を提供するサポートされた ID プロバイダ（IdP）について説明します。このマニュアルでは、特定のコラボレーション アプリケーションを設定するための、製品マニュアルへのリンクを示します。

対象読者

このマニュアルは、Cisco Unified Communications のさまざまなアプリケーションおよびサポートされる IdP 用の SAML-based SSO ソリューションの十分な知識があるシステム管理者を対象としています。このマニュアルでは、Network Time Protocol（NTP）および Domain Name System（DNS）のサーバ設定に関する知識も必要です。

構成

次の表に、このマニュアルの構成を示します。

章	説明
第 1 章	「SAML-based SSO ソリューション」 SAML-based SSO ソリューションがどのように動作するかの概要を説明し、SAML SSO機能の設定と操作に関する一般的なトピックやコンポーネントについて説明します。また、基本的な設定フローやシステム要件についても詳しく説明します。
第 2 章	「SAML-based SSO の設定」 SAML SSO のさまざまな機能、およびOpenAM SSO を SAML-based SSO ソリューションに再設定するプロセスについて説明します。

関連資料

SAML SSO ソリューションおよび設定の詳細については、以下のマニュアルを参照してください。

- 『*Cisco Unified Communications ManagerDocumentation Guide, Release 10.0(1)*』
- 『*Release Notes for Cisco Unified Communications Manager, Release 10.0(1)*』
- 『*Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*』
- 『*Cisco Prime Collaboration 10.0 Assurance Guide - Advanced*』
- 『*Cisco Unified Communications ManagerSystem Guide, Release 10.0(1)*』
- 『*Features and Services Guide for Cisco Unified Communications Manager, Release 10.0(1)*』
- 『*System Administration Guide for Cisco Unity Connection, Release 10.0(1)*』
- 『*Troubleshooting Guide for Cisco Unified Communications Manager, Release 10.0(1)*』
- 『*Cisco Unified Communications Operating System Administration Guide, Release 10.0(1)*』
- 『*Troubleshooting Guide for Cisco Unity Connection, Release 10.0(1)*』
- 『*Quick Start Guide for the Cisco Unity Connection SAML SSO, Release 10.0(1)*』

（注） 最新のマニュアルを入手するには、シスコ製品のマニュアルページにアクセスしてください。
https://www.cisco.com/cisco/web/support/index.html

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	ユーザが値を指定する引数は、イタリック体で示しています。
string	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。
スクリーン 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、スクリーン フォントで表示されます。
太字の screen フォント	ユーザが入力する必要がある情報は、太字のスクリーン フォントで表示されます。
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、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』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

『*What's New in Cisco Product Documentation*』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する必要があります。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

SAML-Based 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 と共に導入する場合、Cisco 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、ユーザを認証するために、サービス プロバイダ（Cisco Unified Communications Manager など）が使用する認証プロトコルです。SAML により、ID プロバイダ（IdP）とサービス プロバイダの間で、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 管理アクセスの許可は、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）に基づいています。

SAML SSO は、IdP とサービス プロバイダ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 プロバイダが認証に関わることはありません。SAML 2.0 では、サービス プロバイダではなく、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-Based SSO 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 を使用して、IdP とサービス プロバイダの間で信頼の輪を作成できます。サービス プロバイダは 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、ユーザの間で認証情報を保護します。SAML SSO では、外部ユーザに対して、IdP とサービス プロバイダの間で渡される認証メッセージを非表示に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

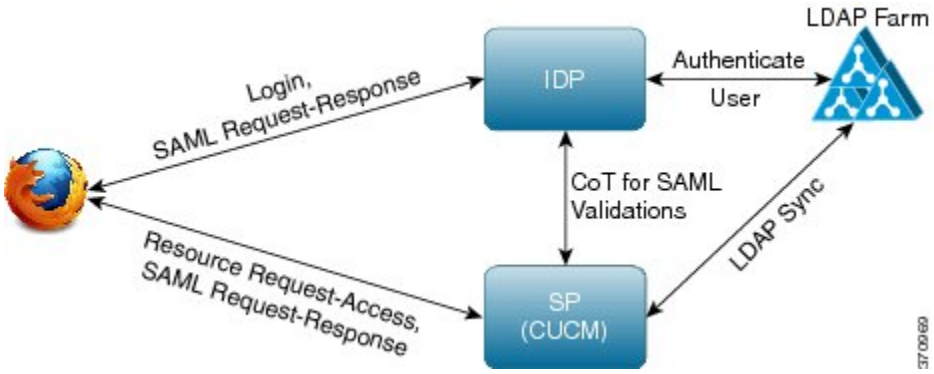
- クライアント（ユーザのクライアント）：これは、認証用にブラウザインスタンスを活用できる、ブラウザベースのクライアントまたはクライアントです。システム管理者のブラウザはその一例です。
- サービス プロバイダ：これは、クライアントがアクセスを試みるアプリケーションまたはサービスです。Cisco Unified Communications Manager はその一例です。

- ID プロバイダ（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 ユーザは、Unified Communications サーバ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 要求：これは、Unified Communications アプリケーションにより生成される認証要求です。LDAP ユーザを認証するために、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、共通の 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（Cisco Unified Communications Manager、Cisco Unity Connection など）および IdP により生成される 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 プロバイダの間に信頼関係が確立されます。
- Assertion Consumer Service（ACS）URL：この URL は、アサーションを POST 形式で送信する場所を IdP に指示します。ACS URL は、最終的な SAML 応答を特定の URL に POST 形式で送信するように 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。

次の図を参照してください。

図 *1*：*SAML SSO* の基本要素



SAML SSO の Web ブラウザ

次のオペレーティング システム（OS）のブラウザは、SAML SSO ソリューションをサポートしています。

- Microsoft Windows 7（64 ビット）：
  - Microsoft Internet Explorer (IE) 10
- Microsoft Windows 8.1（64 ビット）：
  - Microsoft Internet Explorer 11
  - Mozilla Firefox、34.0.x
  - Google Chrome、39.0.x
- Apple OS X 以降：
  - Apple Safari（Mac OS 7.1）

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

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence サービス

（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 機能設定の補足情報については、『*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 の設定手順の詳細については、『*Cisco Prime Collaboration 10.0 Assurance Guide - Advanced*』ガイドにある、「Managing Users」の章の「Single Sign-On for Prime Collaboration」の項を参照してください。

（注） Cisco Unified Communications Manager 11.0(1) の SAML SSO 機能は、次のアプリケーションではサポートされていません。

- Cisco Unified Real-Time Monitoring Tool（RTMT）
- Cisco Unified Communications Operating System Administration：[Cisco Unified OS Administration] ウィンドウ
- ディザスタ リカバリ システム（DRS）：[ディザスタ リカバリ システム（Disaster Recovery System）] ウィンドウ

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。
- SAML 2.0 規格に準拠したサポート対象の IdP サーバ。

アイデンティティ プロバイダ（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からの UC サービス要求を認証するためのオプションです。現在は、Mobile & Remote Access（MRA）経由で外部から UC サービスを要求するクライアントにまで拡張されました。

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。シスコは 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 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

（注） 個々の IdP 設定に関する詳細については、IdP のマニュアルを参照してください。

シスコは、設定について次のサポート記事も提供しています。

- 『SAML SSO Configure Microsoft Active Directory Federation Services Identity Provider on Windows Platform』
- 『SAML SSO Configure PingFederate Identity Provider on Windows Platform』
- 『SAML SSO Configure Open Access Manager Identity Provider on Linux Platform』

SAML コンポーネント

SAML SSO ソリューションは、アサーション、プロトコル、バインディング、およびプロファイルの特定の組み合わせに基づいています。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アプリケーションおよびサイト間で交換され、これらのアサーションによってサイト間でユーザが認証されます。SAML のコンポーネントは次のとおりです。

- SAML アサーション：IdP からサービス プロバイダに転送される情報の構造と内容を定義します。これは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が、さまざまなレベルのアクセス制御を決定する際に使用するステートメントが含まれます。
  SAML SSO は、次の種類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、サービス プロバイダに対して、IdP とブラウザ間で特定の時点に行う認証の方法についてアサートします。

- 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、ユーザに関する特定の情報が含まれます。サービス プロバイダは、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た SAML 要求および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 クエリー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、標準メッセージング形式または SOAP 交換などの通信プロトコルで、SAMLアサーションやプロトコル メッセージ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

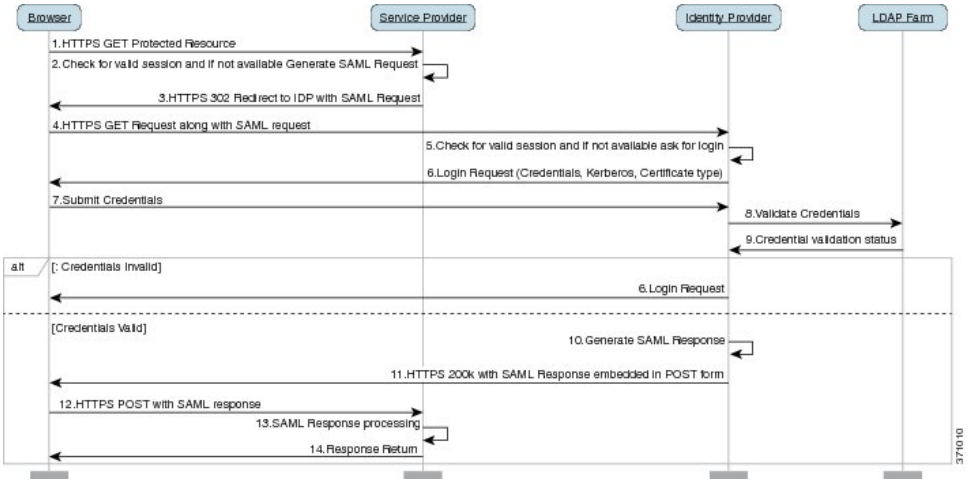
- SAML プロファイル：SAML プロファイルでは、明確に定義された使用例をサポートするために、SAML アサーション、プロトコル、およびバインディングの組み合わせについて詳細に説明しています。Unified Communications 10.0 は、SAML 2.0 の Web ブラウザ SSO プロファイルをサポートしています。

SAML SSO コール フロー

この項では、SAML SSO 機能が、Unified Communications アプリケーションに対してシングル サインオンをどのように有効にするかについて説明します。この項では、IdP とサービス プロバイダの関係も説明し、シングル サインオンを有効にするために、さまざまな設定が重要であることを示します。

次の図は、SAML SSO のコール フローです。

図 *2*：*SAML SSO* コール フロー



1	ブラウザ ベースのクライアントは、サービス プロバイダ上の保護されたリソースにアクセスしようとします。 （注）　ブラウザには、サービス プロバイダとの既存セッションはありません。
2	ブラウザから要求を受信すると、サービス プロバイダは SAML 認証要求を生成します。 （注）　SAML 要求には、どのサービス プロバイダが要求を生成したかを示す情報が含まれています。これにより、IdP は、どのサービス プロバイダが要求を開始したかを後で知ることができます。 IdP は、SAML 認証を正常に完了させるために、Assertion Consumer Service（ACS）URL を保持する必要があります。ACS URL は、最終的な SAML 応答を特定の URL に POST 形式で送信するように IdP に指示します。 （注）　リダイレクトまたは POST バインディングのいずれかを経由して、認証要求を IdP に送信でき、アサーションをサービス プロバイダに送信できます。たとえば、Cisco Unified Communications Manager は、いずれかの方向の POST バインディングをサポートしています。
3	サービス プロバイダは、要求をブラウザにリダイレクトします。 （注）　IdP の URL は、SAML メタデータ交換の一部として、サービス プロバイダで事前設定されます。
4	ブラウザはリダイレクトに従い、IdP に HTTPS GET 要求を発行します。SAML 要求は、GET 要求でのクエリ パラメータとして維持されます。
5	IdP は、ブラウザとのセッションが有効であることを確認します。

6	ブラウザとの既存セッションがない場合、IdPはブラウザへのログイン要求を生成します。また、IdP によって設定および適用され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、お客様のセキュリティ要件と認証要件によって決定されます。これは、ユーザ名とパスワード、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	ユーザは、必要な資格情報をログイン フォームに入力し、IdP に POST 形式で戻します。 （注） ロギング対象となる認証チャレンジは、ブラウザと IdP の間です。サービス プロバイダは、ユーザ認証に関わりません。
8	IdP は、LDAP サーバに資格情報を送信します。
9	LDAP サーバは、資格情報のディレクトリを確認し、IdP に検証ステータスを返信します。
10	IdP は、資格情報を検証し、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 よりデジタル署名され、ユーザはサービス プロバイダが保護するリソースにアクセスできるようになります。IdP は、そのクッキーもここに設定します。
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、非表示フォームの POST 指示に従い、サービス プロバイダの ACS URL に POST 形式でアサーションを送信します。
13	サービス プロバイダは、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。
18	サービス プロバイダは、保護されたリソースへのアクセス権を許可し、ブラウザに 200 OK で返答することで、リソースの内容を提供します。 （注） サービス プロバイダは、そのクッキーをここに設定します。ブラウザがその他のリソースの要求を続けて行う場合、ブラウザはサービスプロバイダのクッキーを要求に加えます。サービス プロバイダは、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 ブラウザにリソースの内容が戻されます。

第 2 章

SAML-Based SSO の設定

前提条件

NTP の設定

SAML SSO では、Network Time Protocol（NTP）が Unified Communications アプリケーションと IdP 間のクロック同期を有効にします。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は、アサーションが無効になり、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。

クロックの同期については、『*Cisco Unified Communications Operating System Administration Guide*』の「NTP Settings」の項を参照してください。

DNS の設定

Domain Name System（DNS）を使用すると、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 アプリケーションでは、DNS を使用して、完全修飾ドメイン名を IP アドレスに解決できます。サービス プロバイダと IdP は、ブラウザで解決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 プロバイダのホスト名（`http://www.cucm.com/ccmadmin`）を入力する場合、ブラウザはホスト名を解決する必要があります。また、サービス プロバイダが SAML SSO の IdP（`http://www.idp.com/saml`）にブラウザをリダイレクトする場合、ブラウザは IdP のホスト名を解決する要があります。さらに、IdP がサービス プロバイダの ACS URL にリダイレクトし直す場合、ブラウザは同様に解決する必要があります。

ディレクトリの設定

LDAP ディレクトリの同期化は、さまざまな Unified Communications アプリケーションにわたって SAML SSO を有効にする場合の前提条件であり、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化すると、Unified Communications アプリケーションのデータ フィールドのディレクトリ属性へのマッピングによって、管理者はユーザを簡単にプロビジョニングできます。

（注） SAML SSO を有効にするには、LDAP サーバが IdP サーバによって信頼されていて、Unified Communications アプリケーションでサポートされる必要があります。

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab10/directry.html

証明書の管理と検証

重要 シスコは、SAML SSO 用にサーバ証明書に署名すること、および製品サポートが利用可能な場合はマルチサーバ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 と入力する場合、CN または SAN では “www.cisco.com” がヘッダーに存在する必要があります。
- Cisco Unified Communications Manager がすでに混合またはセキュア モードであり、証明書に変更が行われている場合は、安全な 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なくなります。CTL トークンを更新するには、Cisco Unified Communications Manager の再起動が必要です。

SAML SSO では、ユーザの Web ブラウザなどの、SAML メッセージ交換に関与している各エンティティは、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。シスコは、SAML SSO の導入環境に参加する各 UC 製品で、信頼できる認証局が発行し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、サーバとのセキュアな接続を確立します。エンドポイント間での信頼性の確保、認証、およびデータの暗号化には、証明書を使用します。これにより、エンドポイントが確実に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有効になります。

セキュアな接続を確立する場合、サーバは 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、ユーザに証明書を受け入れるかどうか確認するよう指示されます。

認証局により署名された証明書

シスコは、次の認証局（CA）のいずれかにより署名された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、サーバの識別情報を検証し、信頼できる証明書を発行します。
- **プライベート CA**：自分でローカルの 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、手順の概要を次に示します。

手順

ステップ 1 クライアントに証明書を提示できる製品ごとに、証明書署名要求（CSR）を作成します。
ステップ 2 CA に各 CSR を送信します。
ステップ 3 CA が各サーバに発行する証明書をアップロードします。

サーバ証明書はクライアント コンピュータの信頼ストアに存在する関連のルート証明書が必要です。Cisco UC アプリケーションは、信頼ストアでサーバが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 によって署名されたサーバ証明書を取得する場合、パブリック CA はすでにクライアント コンピュータの信頼ストアで提示されるルート証明書を持っている必要があります。この場合、クライアント コンピュータの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 アップ警告を表示します。

たとえば、管理者がブラウザで `https://www.cucm.com/ccmadmin` を指定する場合、CUCM ポータルがブラウザに CA 証明書を提示します。ブラウザが `https://www.idp.com/saml` にリダイレクトされる場合は、IdP が CA 証明書を提示します。ブラウザは、サーバが提示する証明書にそのドメイン用の CN または SAN フィールドがあること、そして証明書が信頼できる CA により署名されていることを確認します。

また、お客様に固有のプライベート CA がある場合は、管理者がブラウザを起動しているコンピュータで、ルート トラスト アンカーとして、その CA をインストールする必要があります。

マルチサーバ SAN 証明書の設定

それぞれのシスコ製品には、マルチサーバ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SAN証明書をサポートしているシスコ製品については、関連の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, Release 10.5(1)』
Cisco Unified Communications Operating System アドミニストレーション ガイド for Cisco Unity Connection リリース 10.x
Cisco Prime Collaboration

ハイレベルな信頼の輪の設定

Unified Communications アプリケーション全体で SAML SSO を有効にするには、管理者がサービス プロバイダと IdP 間で信頼の輪（CoT）を確立する必要があります。手順の概要を次に示します。

手順

ステップ 1 IdP とサービス プロバイダの間での証明書の交換：

a) サービス プロバイダから CA 証明書をエクスポートします。

b) IdP サーバに移動し、サービス プロバイダから CA 証明書をインポートします。

c) IdP サーバから CA 証明書をエクスポートします。

d) サービス プロバイダに移動し、IdP サーバから CA 証明書をインポートします。

（注） 管理者は、IdP がサービス プロバイダのメタデータに含まれる証明書を信頼していることを確認する必要があります。メタデータを IdP にインポートするだけで十分な場合を除いて、サービスプロバイダの署名証明書を IdP の証明書信頼ストアに手動でインポートする必要があります。

ステップ 2 IdP とサービス プロバイダの間でのメタデータの交換：

a) IdP からメタデータをエクスポートします。

b) サービス プロバイダにメタデータをインポートします。

c) サービス プロバイダからメタデータをエクスポートします。

d) IdP サーバに移動し、サービスプロバイダからメタデータをインポートして、サービスプロバイダをプロビジョニングします。

ステップ 3 IdP で必須属性の UID を設定します。この属性は、Unified Communications アプリケーションで使用される、LDAP が同期したユーザ ID 属性と一致している必要があります。

（注） ユーザ ID は、IdP が特定のサービス プロバイダに設定する必須属性です。サービス プロバイダは、この属性から認証済みユーザの ID を識別します。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。

（注） SAML SSO を正しく動作させるには、サービスプロバイダと IdP が同じ CoT に存在している必要があります。

信頼の輪の作成

Cisco Unified Communications Manager を追加する既存の CoT が存在しない場合、SAML SSO がアクティブになる前に CoT を作成する必要があります。

次の例では、OpenAM を使用して CoT を作成しています。

手順

ステップ 1 OpenAM サーバのユーザ インターフェイスにログインします。

ステップ 2 [フェデレーション（Federation）] タブを選択し、[信頼の輪（Circle of Trust）] 領域で [新規（New）] ボタンをクリックします。

a) IdP の CoT に固有の名前を付けて、信頼の輪を作成します。SAML SSO を動作させるには、サービス プロバイダ（この場合は Cisco Unified Communications Manager）と IdP は同じ CoT に存在している必要があります。

（注） これ以降の手順で、サービス プロバイダと IdP を同じ CoT に存在するように割り当てます。

ステップ 3 サーバで SAMLv2 ID プロバイダを作成します。

a) [共通タスク（Common Tasks）] タブを選択し、[ホスト型 ID プロバイダの作成（Create Hosted Identity Provider）] ボタンをクリックしてホスト型 IdP を作成します。

b) [既存の信頼の輪（Existing Circle of Trust）] ドロップダウン リストで、ステップ 2 で作成した CoT を選択します。

c) [属性マッピング（Attributes mapping）] 領域で、[アサーションでの名前（Name in Assertion）] と [ローカル属性（Local Attribute）] の両方の値を設定して UID にします。

d) [設定（Configure）] をクリックします。

e) [フェデレーション（Federation）] タブを選択し、作成したホスト型エンティティ プロバイダをクリックします。

f) [アサーション コンテンツ（Assertion Content）] のセクションを参照し、[証明書エイリアス（Certificate Aliases）] 領域で [署名（Signing）] フィールド値として「test」と入力します。

（注） これは、SAML アサーションをエイリアスで署名する場合に必要です。

SAML SSO の設定ワークフロー

SAML SSO

使用する IdP にかかわらず、SAML SSO を有効にための次の 3 つの必須タスクと 1 つのオプション タスクがあります。

- 信頼の輪の作成
- SAML SSO をアクティブにするための Cisco Unified Communications Manager の設定
- IdP の設定（次の例では、OpenAM を設定します）
- （任意）SAML SSO 設定の検証

ヒント　SAML SSO を動作させるには、Cisco Unified Communications Manager と IdP（この場合は OpenAM）のクロックを同期させる必要があります。

シスコは、サポートされている各 IDPS の設定について、次の記事も提供しています。

- 『SAML SSO Configure Microsoft Active Directory Federation Services Identity Provider on Windows Platform』
- 『SAML SSO Configure PingFederate Identity Provider on Windows Platform』
- 『SAML SSO Configure Open Access Manager Identity Provider on Linux Platform』

SAML SSO をアクティブにするための Cisco Unified Communications Manager の設定

手順

ステップ 1　**Cisco Unified CM Administration** のユーザ インターフェイスにログインします。

ステップ 2　[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。[SAML シングル サインオンの設定（SAML Single Sign-On Configuration）] ウィンドウが開きます。

ステップ 3　クラスタで SAML SSO を有効にするには、[SAML SSO の有効化（Enable SAML SSO）] リンクをクリックします。

ステップ 4　[警告のリセット（Reset Warning）] ウィンドウで [続ける（Continue）] をクリックします。

（注）　SAML SSO の場合、シスコは次の 4 つの IdP をサポートしています。

- Microsoft Active Directory Federation Services（ADFS）
- Ping Federate

IdP メタデータ信頼ファイルを保存する場合や、正常な設定を検証する場合に戻れるように、[SAML シングル サインオンの設定（SAML Single Sign-On Configuration）] ウィンドウは開いたままにしておきます。

次の例では、Open AM を使用しています。

次の作業

信頼の輪をまだ作成していない場合は、この時点で作成するか、または IdP 設定時にタスクをシフトできます。SAML SSO に対して IdP を設定する前に、信頼の輪を作成することを推奨します。

SAML SSO のための IdP（OpenAM）と Cisco Unified Communications Manager の設定

この例では、OpenAM IdP を使用します。このタスクには、OpenAM IdP サーバと Cisco Unified Communication Manager ノードの間の切り替え操作があります。

はじめる前に

信頼の輪（CoT）の作成

SAML SSO のための Cisco Unified Communications Manager の設定

手順

ステップ 1 **OpenAM IdP** サーバにログインし、メタデータ信頼ファイルをダウンロードします。

a) OpenAM IdP サーバ用の **IdP メタデータ信頼**ファイルをダウンロードするには、ブラウザに次のいずれかの URL を入力します。ここで、*server.example.com* は OpenAM サーバの FQDN、8443 はデフォルトのポート番号です。

- OpenAM サーバで 1 つの領域が定義されている場合：

  https://*server.example.com*:8443/openam/saml2/jsp/exportmetadata.jsp.

- OpenAM サーバで複数の領域が定義されている場合：

  https://*server.example.com*:8443/openam/saml2/jsp/exportmetadata.jsp?entityid=

  https://*server.example.com*:8443/openam&realm=realm-name

  （注） 上記 2 行の組み合わせは、複数領域の完全な URL になっています。

ステップ 2 **Cisco Unified CM Administration** のユーザ インターフェイスにアクセスし、次のタスクを実行します。

a) **IdP メタデータ信頼**ファイルを保存し、Cisco Unified Communications Manager ノードにインポートします。インポートが成功すると、[SAML シングル サインオンの設定（SAML Single Sign-On Configuration）] ウィンドウが開きます。

1. [IdP メタデータ信頼ファイルのインポート（Import the IdP Metadata Trust File）] 領域で、[参照（Browse）] をクリックして IdP メタデータ信頼ファイルの場所に移動します。
2. [IdP メタデータのインポート（Import IdP Metadata）] ボタンをクリックします。
   （注） インポートが成功すると、インポートが全ノードで成功したことを示すチェックマークが表示されます。
3. [次へ（Next）] をクリックします。

b) クラスタ内の Cisco Unified Communications Manager ノード用に、**サーバ メタデータ**をローカル ファイル システム内の適切な場所にダウンロードします。

1. [信頼メタデータ ファイルのダウンロード（Download Trust Metadata File）] リンクをクリックして、[開いている SP メタデータ（Opening SPMetadata）] ダイアログ ボックスを開きます。
2. 圧縮ファイルをローカルに保存します。
3. メタデータ ファイル フォルダを解凍します。フォルダを解凍すると、クラスタ内のノードごとに 1 つのメタデータ ファイルが存在します。

ステップ 3 OpenAM サーバのユーザ インターフェイスにアクセスし、クラスタ内の各ノードにメタデータ ファイルをアップロードします。

（注） Cisco Unified Communications Manager に追加する CoT が存在しない場合、次のステップに進む前に CoT を作成する必要があります。**信頼の輪の作成**タスクを参照してください。

ステップ 4 CoT が作成されたら、Cisco Unified Communications Manager ノードをエンティティ プロバイダとして追加する必要があります。手順は次のとおりです。

a) OpenAM サーバのユーザ インターフェイスで [フェデレーション（Federation）] タブを選択し、[エンティティ プロバイダ（Entity Providers）] セクションで [エンティティのインポート（Import Entity）] ボタンをクリックして Cisco Unified Communications Manager メタデータ ファイル（*server*.xml）をインポートします。ここで、*server* は Cisco Unified Communications Manager ノードの名前です。

b) [保存（Save）] をクリックします。

c) ステップ 3a でインポートしたエンティティをクリックし、アサーション処理セクションに移動し、ディレクトリと OpenAM の設定に従って UID のマッピング属性を追加します。

（注） UID は、所定のサービス プロバイダ用に IdP で設定する必要がある必須属性です。これは、サービス プロバイダが認証済みユーザを識別する方法です。UID 属性を追加する際に、ディレクトリまたはユーザ ストアの設定に従い、それを正しい属性にマップする必要があります。

d) SAML SSO を有効にする必要のある、クラスタ内のその他のノードに対して、ステップ 3a～3c を繰り返します。

e) [フェデレーション（Federation）] タブを選択し、追加した [信頼の輪（Circle of Trust）] をクリックします。

f) [エンティティ プロバイダ（Entity Providers）] セクションで、IdP（OpenAm サーバ）と Cisco Unified Communications Manager のエンティティを、[使用可能（Available）] から [選択済み（Selected）] セクションに移動します。

これは、IdP サーバと Cisco Unified Communications Manager ノードを同じ CoT に割り当てます。

ステップ 5 OpenAM サーバで、資格情報が管理者レベルのユーザと一致するユーザを追加する必要もあります。そのユーザは、Cisco Unified Communications Manager で SSO を有効にするために使用されていました。

a) [アクセス制御（Access Control）] > [トップ レベル領域（Top Level Realm）][サブジェクト（Subject）] を選択し、管理者レベルのユーザを追加します。

OpenAM サーバと Cisco Unified Communications Manager ノードを設定したら、**Cisco Unified CM Administration** のユーザ インターフェイスで SAML SSO が正常に有効になったことを検証できます。

次の作業

SAML SSO 設定の検証, （20 ページ）

関連トピック

SAML SSO をアクティブにするための Cisco Unified Communications Manager の設定, （17 ページ）
信頼の輪の作成, （15 ページ）

SAML SSO 設定の検証

はじめる前に

- IdP に必要なサーバ メタデータ ファイルをインストールしました。
- **Cisco Unified CM Administration** のユーザ インターフェイスで、[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**ファイルを正常にインポートしたことが表示されています。

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。[有効な管理者のユーザ名（Valid Administrator Usernames）] 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 は正常に設定されていることになります。

アップグレード後の SAML SSO への OpenAM SSO の再設定

Cisco Unified Communications Manager 11.0(1) は、SAML シングルサインオン（SSO）のみを提供します。

（注） シスコのコラボレーション アプリケーションは、Cisco Unified Communications Manager 8.6 ～ 10.5 で独自の OpenAM SSO ソリューションをサポートします。エージェント フローを使用して導入された OpenAM SSO は、そのソリューションを現在使用しているパートナーに役立つよう、リリース 10.5(1) でも使用できます。OpenAM IdP と Cisco Unified Communications Manager を再設定した後は、SAML SSO 用の既存の OpenAM 展開を再利用できます。

（注） リリース 10.0(1) 以降では、エージェント フロー SSO は FIPS モードと互換性がありません。

OpenAM SSO を SAML SSO に再設定するには、管理者は新しいフェデレーション サービスとサービス アカウントを作成する必要があります。SAML SSO を正しく動作させるには、サービスプロバイダと IdP は同じ信頼の輪（CoT）に存在している必要があります。管理者は、サービスプロバイダと IdP の間で信頼関係を設定する必要があります。次の手順を実行して Cisco Unified Communications Manager の OpenAM SSO を SAML SSO に設定します。

この場合、OpenAM を IdP として引き続き使用します。ただし、OpenAM を SAML に再設定する必要があります。

はじめる前に

SAML SSO を動作させるには、Cisco Unified Communications Manager と OpenAM のクロックを相互に同期させる必要があります。

手順

ステップ 1 これらのサーバで SAML SSO を有効にします。
（注） SAML SSO を有効にする方法については、各 Cisco Unified Communications のマニュアルを参照してください。

ステップ 2 OpenAM サーバのユーザ インターフェイスにログインします。

ステップ 3 [フェデレーション（Federation）] タブを選択し、[信頼の輪（Circle of Trust）] で [新規（New）] をクリックします。

ステップ 4 IdP の信頼の輪に固有の名前を入力して CoT を作成します。

ステップ 5 ホスト型 IdP を作成するには、[共通タスク（Common Tasks）] タブを選択し、[ホスト型 ID プロバイダの作成（Create hosted Identity Provider）] をクリックします。

ステップ 6 その他のパラメータにはデフォルト値を使用し、[保存（Save）] をクリックします。
（注） 作成した信頼の輪は、[信頼の輪（Circle of Trust）] セクションで確認できます。

ステップ 7 [Entity Providers（エンティティ プロバイダ）] セクションで [Federation（フェデレーション）] タブを選択し、作成した [ホスト型 ID プロバイダ（Hosted Identity Provider）] をクリックします。

ステップ 8 [証明書エイリアス（Certificate Aliases）] セクションで [アサーション コンテンツ（Assertion Content）] タブを選択し、[署名（Signing）] フィールドで SAML アサーション署名のエイリアスとして <test> と入力します。

ステップ 9 [フェデレーション（Federation）] タブを選択し、[エンティティ プロバイダ（Entity Providers）] セクションで [エンティティのインポート（Import Entity）] をクリックします。

ステップ 10 Cisco Unified Communications Manager のメタデータ ファイル（sp.xml）をアップロードし、[保存（Save）] をクリックします。

（注） メタデータが署名されている場合、メタデータ ファイルのアップロードは失敗します。このような場合は、Cisco Unified Communications Manager の tomcat 証明書を openAMKeystore に追加します。次の手順を実行します。

1. tomcat 証明書（tomcat.pem）を **Cisco Unified Communications Manager OS Administration** ページからダウンロードし、その証明書を OpenAM サーバ内のいずれかの場所にアップロードします。例：`/temp/tomcat.pem`
2. OpenAM で次のコマンドを実行します。
   keytool -import -v -alias*aliasname***-keystore /root/openam/openam/keystore.jks -trustcacerts -file***location_of_cucm_tomcat_cert*
3. パスワードを <changeit> として入力します。
4. 証明書を信頼するかどうかを尋ねるダイアログ ボックスが表示されたら、[はい（Yes）] をクリックします。
   次のメッセージが表示されます。

   ```
   Certificate was added to keystore
   [Storing /root/openam/openam/keystore.jks]
   ```

5. OpenAM で tomcat を再起動し、sp.xml メタデータ ファイルのアップロードを再試行します。
6. エンティティ プロバイダのアップロード時に [ファイル（File）] を選択します。

（注） Cisco Unified Communications Manager では、[ファイル（File）] オプションのみからのメタデータ ファイルのアップロードをサポートしています。

ステップ 11 ステップ 9 でインポートしたエンティティを選択します。

ステップ 12 [アサーション処理（Assertion Processing）] タブを選択し、ディレクトリと OpenAM の設定に従い、UID のマッピング属性を追加します。

（注） UID 属性を追加する際に、ディレクトリまたはユーザ ストアの設定に従い、それを正しい属性にマップします。たとえば、uid=sAMAccountName、uid=mail、または uid=uid を入力できます。

ステップ 13 [フェデレーション（Federation）] タブを選択し、[信頼の輪（Circle of Trust）] をクリックします。

ステップ 14 IdP と Cisco Unified Communications Manager を同じ CoT に存在するように割り当てるには、[エンティティ プロバイダ（Entity Providers）] 領域で、IdP（OpenAM サーバ）と Cisco Unified Communications Manager のエンティティを、[使用可能（Available）] セクションから [選択済み（Selected）] セクションに移動します。

OpenAM サーバは IdP として設定されます。

第 3 章

エンドユーザ SAML SSO

エンドユーザ SAML SSO の設定

エンドユーザまたはフェデレーション済みSSOは標準機能です。これにより製品は、お客様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、エンドユーザの経験を向上させることができます。コラボレーション製品におけるこのサポート基盤は、リリース10.0および10.5で導入されました。これにより管理者は、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することができます。Cisco Jabberのサポートは、2014年後半からリリース10.5のユーザに本格的に提供される予定です。

管理者がユーザ向けにこの機能を有効にした場合、シスコのコラボレーションアプリケーションのユーザは、サポートされているアプリケーションでは企業のユーザ名とパスワードでログインできるようになります。シスコのアプリケーションにブラウザでアクセスするユーザは、企業のユーザ名とパスワードを使ってログインできます。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ユーザは、ユーザ名とパスワードを指定せずに、アプリケーションにアクセスできます。これらのすべての機能は、お客様のネットワーク内で使用するか、またはVPN経由でアクセスすることができます。

サポートされる製品：

製品	エンドユーザ SAML SSO のサポートが有効なリリース	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 サービス	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

製品	エンド ユーザ SAML SSO のサポートが有効なリリース	詳細情報
WebEx Meeting Center	クラウド	ここをクリックしてください
WebEx Connect and Messenger	クラウド	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

サポートされるエンド ユーザ クライアント：

製品	リリース	詳細情報
WebEx IOS	すべてのリリースで利用可能	ここをクリックしてください
WebEx Android	すべてのリリースで利用可能	ここをクリックしてください
WebEx Connect	すべてのリリースで利用可能	ここをクリックしてください
WebEx Messenger	すべてのリリースで利用可能	ここをクリックしてください
Jabber for Windows	10.5	2014 年後半に利用可能
Jabber IOS	10.5	2014 年後半に利用可能
Jabber for Android	10.5	2014 年後半に利用可能
Jabber for Mac	10.5	2014 年後半に利用可能

（注）

- Cisco Jabber を Cisco WebEx Meeting Server と共に導入する場合、Cisco 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 を SSO とともに実行している場合、Jabber サービス向けに承認されると、Jabber はクッキーを自動的に設定できません。Mac のデフォルトの動作では、ユーザが移動するサイト以外のクッキーは許可されません。Jabber で認証の確認が必要になるたびに、IdP に移動する必要があります。
- SAML アサーションには、WebEx のメール アドレスを含める必要があります。そのために、SAML スキーマを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。

索 引