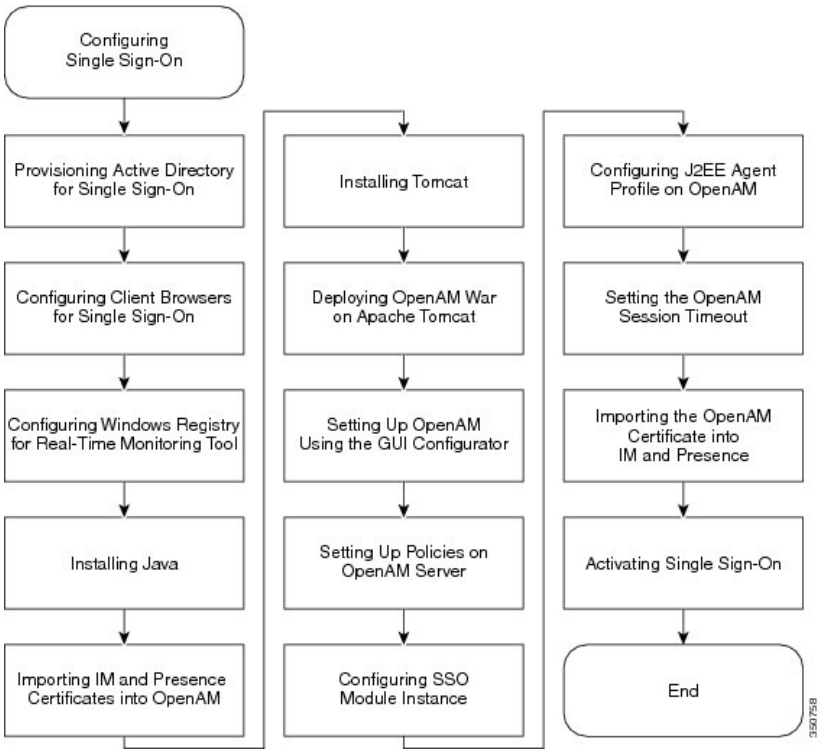
OpenAM シングル サインオン

シングル サインオン設定のタスクリスト

次の図は、正常にSSOを設定するために必要なタスクの手順について説明します。 この順序どおりに、このフローで説明している各タスクを実行することを推奨します。

図 *1*：シングル サインオン設定のタスク フロー



次の表は、シングル サインオンを設定するタスクを示します。

表 *1*：シングル サインオン設定のタスク リスト

項目	タスク
1	Active Directory（AD）サーバの シングル サインオンを使用する OpenAM サーバの新しいユーザ アカウントをプロビジョニングします。 （注） 先に進む前に、Windows Server 2008 のサポート ツールがインストールされていることを確認してください。
2	シングル サインオンのためにクライアント ブラウザを設定します。 サードパーティ製ソフトウェア、Web ブラウザのリストのシステム要件、およびサポート対象のバージョンの関連トピックを参照してください。

項目	タスク
3	Real-Time Monitoring Tool（RTMT）用の Microsoft Windows レジストリを設定します。
4	Java Runtime Environment（JRE）をインストールします。 （注） Java キー ストアと関連セキュリティ証明書は Apache Tomcat で動作する OpenAM サーバへのセキュア接続が必要になります。 Java をインストールする手順は、自己署名されたセキュリティ証明書を使用するか、または、証明局（CA）によって署名されたセキュリティ証明書を使用するかによって異なります。
5	OpenAM に IM and Presence サービス証明書をインポートします。 シングル サインオンを使用するための、各 IM and Presence サービス ノードに対してこの作業を実行します。
6	OpenAM Windows サーバで Apache Tomcat Web Container をインストールします。
7	Apache Tomcat で OpenAM War を展開します。
8	GUI Configurator を使用して OpenAM をセットアップします。 OpenAM サーバの FQDN を入力することで、Web ブラウザを使用する OpenAM web ベースの管理インターフェイスにアクセスします。
9	OpenAM サーバのポリシーの設定 この手順で定義されるポリシー規則に従う必要があります。 （注） Cisco Unified CM IM and Presenceの管理/ユーザ インターフェイスにアクセスするには、IM and Presence サービス ノードの FQDN を使用する必要があります。 ノードのホスト名を使用しないでください。
10	SSO モジュール インスタンスを設定します。 同じ Active Directory ドメインが展開全体で使用される場合、単一モジュール インスタンスを、SSO の複数の IM and Presence サービス ノードによって共有できます。
11	OpenAM の J2EE Agent プロファイルを設定します。 SSO を使用する各 IM and Presence サービス ノードの J2EE エージェント用の OpenAM サーバの関連 J2EE Agent プロファイルを設定する必要があります。
12	OpenAM セッション タイムアウトを IM and Presence サービス ノードのセッション タイムアウト パラメータ設定よりも大きい値に設定します。
13	SSO を使用して各 IM and Presence サービス ノード の tomcat-trust の信頼ストアに OpenAM 証明書をインポートします。

項目	タスク
14	シングル サイン オンのアクティブ化 **注意** SSO を有効にすると、サービスに影響を与えます。 メンテナンス時間枠の間に、SSO を有効にすることを強く推奨します。

シングル サインオンのセットアップ時に必要のない次の追加タスクを実行できます。

- シングル サイン オンの無効化
- Windows での OpenAM のアンインストール
- デバッグ レベルの設定
- シングル サインオンのトラブルシューティング

関連トピック

シングル サイン オンの無効化, （39 ページ）
Windows での OpenAM のアンインストール, （39 ページ）
デバッグ レベルの設定, （40 ページ）
シングル サインオンのトラブルシューティング

シングル サインオン設定の準備

シングルサインオンでのサードパーティ製ソフトウェアとシステムの要件

シングル サインオン（SSO）機能では、OpenAM と呼ばれる ForgeRock のサードパーティ製アプリケーションを使用します。 OpenAM アプリケーションのサポートは、ForgeRock のみから利用できます。 SSO 機能を OpenAM と連動できるようにするために、ソフトウェア要件と設定ガイドラインが提供されています。 Windows Server での OpenAM のインストールについても、説明されています。

ロードバランサの背後での OpenAM の展開や、OpenAM サーバ間でのセッション レプリケーションの使用などの、OpenAM の高度な設定は検証されていません。 これらの高度な機能の詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf を参照してください。

SSO 機能には、次のサードパーティ製アプリケーションが必要です。

- Microsoft Windows Server 2008 R2
- Microsoft Active Directory

- ForgeRock Open Access Manager（OpenAM）バージョン 9.0

（注） SSO 機能は、Active Directory と OpenAM を組み合わせて使用することにより、Web ベースのクライアント アプリケーションへの SSO アクセスを提供します。

これらのサードパーティ製品は、次の設定要件を満たす必要があります。

- Active Directory は、単に LDAP サーバとしてではなく、Windows ドメインベースのネットワーク設定で導入する必要があります。
- OpenAM サーバは、ネットワーク上のすべてのクライアント システムおよび Active Directory サーバからアクセスできる必要があります。
- Active Directory（ドメイン コントローラ）サーバ、Windows クライアント、IM and Presence Service、および OpenAM サーバは、同じドメイン内に存在する必要があります。
- DNS をドメイン内で有効にする必要があります。
- SSO に参加するすべてのエンティティのクロックを同期させる必要があります。

サードパーティ製品の詳細については、各製品のマニュアルを参照してください。

次の表は、この章に示されている手順で使用され、テストされたソフトウェア アプリケーションとバージョンのリストです。 シスコのサポートを受けるには、シスコは設定時にこれらの推奨要件に従うことを推奨します。

表 *2*：ソフトウェア バージョン

コンポーネント	バージョン
Active Directory	Windows Server 2008 R2 Enterprise
エンド ユーザ クライアント用のデスクトップ オペレーティング システム	Windows 7 Professional（SP1）
OpenAM	OpenAM Release 10.0 http://forgerock.org/openam-archive.html 詳細については、次を参照してください。 https://wikis.forgerock.org/confluence/display/openam/OpenAM+Release+Documentation
OpenAM の基盤となるオペレーティング システム	Windows Server 2008 R2 Enterprise
OpenAM のロード先の Apache Tomcat	Tomcat 6.0.2.0、Tomcat 7.0.29 http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.29/bin

コンポーネント	バージョン
OpenAM の Java Development Kit（JDK）の基盤となるオペレーティング システム	JDK 7 アップデート
Web ブラウザ	Internet Explorer 8、9、および Mozilla Firefox 10、11

シングル サインオンの設定前の重要な情報

（注） Release 10.0(1) 以降、エージェントのフロー SSO は FIPS モードとの互換性がありません。

SSO の設定が可能な限り円滑に動作するよう、SSO を設定する前に次の情報を収集することを推奨します。

- OpenAM システムのインストール ベースのオペレーティング システム（Windows サーバなど）が動作していることを確認します。
- OpenAM が統合される Windows Active Directory（AD）サーバの完全修飾ドメイン名（FQDN）を書き留めます。
- OpenAM をインストールする Windows サーバの FQDN を書き留めます。
- IM and Presence Web アプリケーションのタイムアウトが、クラスタ内のすべての IM and Presence ノード間で一貫して設定されていることを確認し、そのタイムアウト値を書き留めます。 Cisco Unified CM IM and Presence の管理 CLI を使用して、show webapp session timeout コマンドを入力し、タイムアウト値を確認します。 詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*（Cisco Unified Communications ソリューション用コマンド ライン インターフェイス リファレンス ガイド）』を参照してください。
- 「sAMAccountName」をユーザ ID の LDAP 属性として使用して、Active Directory（AD）からユーザを同期するように Cisco Unified Communications Manager が設定されていることを確認します。 詳細については、『*Cisco Unified Communications Manager System Guide*（Cisco Unified Communications Manager システム ガイド）』の「DirSync サービス」の章を参照してください。

シングル サインオンの設定と管理のタスク

シングル サインオンの Active Directory のプロビジョニング

はじめる前に

Windows Server 2008 がインストールされたツールをサポートすることを確認します。 サポートツールは、Windows Server 2008 にデフォルトでインストールされています。

手順

ステップ 1 Active Directory（AD）サーバにログインします。

ステップ 2 [Start（開始）] メニューで、[Programs（プログラム）] > [Administration Tools（管理ツール）] を選択し、[Active Directory Users and Computers（アクティブ ディレクトリ ユーザとコンポーネント）] を選択します。

ステップ 3 [Users（ユーザ）] を右クリックし、[New（新規）] > [User（ユーザ）] を選択します。

ステップ 4 [User logon name（ユーザ ログイン名）] フィールドに、「OpenAM サーバのホスト名」を入力します。

（注） OpenAM サーバ のホスト名にドメイン名を含めることはできません。

ステップ 5 [Next（次へ）] をクリックします。

ステップ 6 パスワードを入力し、確認します。
このパスワードはステップ 10 で必要です。

ステップ 7 [User Must Change at Next login（ユーザは次のログイン時に変更する必要があります）] チェックボックスをオフにします。

ステップ 8 [Next（次へ）] をクリックします。

ステップ 9 新しいユーザ アカウントの作成を終了するには、[Finish（完了）] をクリックします。

ステップ 10 コマンド プロンプトから次のコマンドを使用して、AD サーバの keytab ファイルを作成します。

```
ktpass -princ HTTP/<hostname>.<domainname>@<DCDOMAIN> -pass <password> -mapuser <userName>
 -out <hostname>.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target <DCDOMAIN>
```

例：

```
ktpass -princ HTTP/server1.cisco.com@CISCO.COM -pass cisco!123 -mapuser server1 -out
server1.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target CISCO.COM
```

値は次のとおりです。

パラメータ	説明
hostname	OpenAM サーバのホスト名（FQDN ではなく）。 たとえば、server1
domainname	AD ドメイン名。 たとえば、cisco.com。

パラメータ	説明
DCDOMAIN	印刷字体の大文字で入力される AD ドメイン名。 この例では、CISCO.COM。
password	この前の手順で OpenAM サーバのユーザ アカウントを作成したときに指定したパスワード値。
userName	ステップ 4 で入力した AD アカウント名。 この値は OpenAM サーバのホスト名である必要があります。 この例では、server1。

（注） 後の手順で使用するため *-princ* 値を記録します。

ステップ 11 keytab ファイルが正常に作成されたら、OpenAM サーバの場所に keytab ファイルをコピーします。このパスは、後で OpenAM 設定で指定します。 ディレクトリを `C:\>` の下に作成して、上記のキータブ ファイルをコピーします。 たとえば、`C:/keytab/server1.HTTP.keytab`。

シングル サインオン用のクライアント ブラウザ設定

ブラウザベースのクライアント アプリケーションに SSO を使用する場合は、Web ブラウザを設定する必要があります。 ここでは、SSO を使用するようにクライアントブラウザを設定する方法について説明します。

シングル サインオン用の Internet Explorer の設定

SSO 機能は、Internet Explorer を実行している Windows クライアントをサポートします。 SSO を使用するために Internet Explorer を設定するには、次の手順を実行します。

ヒント サポートされる Web ブラウザの詳細については、サードパーティ製ソフトウェアとシングル サインオンのシステム要件に関連するトピックを参照してください。

手順

ステップ 1 [Tools（ツール）] > [Internet Options（インターネット オプション）] > [Advanced（詳細）] タブを選択します。

ステップ 2 [Enable Integrated Windows Authentication（統合 Windows 認証を有効にする）] をオンにします。

ステップ 3 [OK] をクリックして変更を保存します。

ステップ 4 Internet Explorer を再起動します。

ステップ 5 [Tools（ツール）] > [Internet Options（インターネット オプション）] > [Security（セキュリティ）] > [Local Intranet（ローカルイントラネット）] を選択し、[Custom Level（レベルのカスタマイズ）] をクリックします。

ステップ 6 [User Authentication（ユーザ認証）] で、[Automatic Logon Only in Intranet Zone（イントラネット ゾーンでのみ自動的にログオンする）] を選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Sites（サイト）] をクリックします。

ステップ 9 [Automatically detect intranet network（イントラネットのネットワークを自動的に検出する）] をオンにします。

ステップ 10 [Advanced（詳細）] をクリックします。

ステップ 11 [Add this web site to the zone（この Web サイトをゾーンに追加する）] フィールドに、OpenAM サーバの FQDN を https://OpenAM_FQDN の形式で入力します。

ステップ 12 [Add（追加）] をクリックします。

ステップ 13 [Close（閉じる）] をクリックします。

ステップ 14 [OK] をクリックします。

ステップ 15 [Enable Protected Mode（保護モードを有効にする）] をオフにします。

ステップ 16 [Apply（適用）] をクリックします。

ステップ 17 [OK] をクリックします。

ステップ 18 Internet Explorer を再起動します。

ステップ 19 Windows レジストリ エディタを開きます。 次のいずれかの操作を実行します。

- Windows XP または Windows 2008 では、[Start（開始）] > [Run（実行）] を選択し、「*regedit*」と入力します。
- Windows Vista および Windows 7.0 では、[Start（開始）] をクリックし、「*regedit*」と入力します。 Windows Vista では、[Continue（継続）] をクリックする必要があります。

ステップ 20 登録キー [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\] の下の [New（新規）] > [NewDWORD（32-bit）value（DWORD（32 ビット）値）] を右クリックして、選択し、*SuppressExtendedProtection* に名前を変更します。
管理者のみ DWORD を設定できます。

ステップ 21 次の値を設定します。

- [Base（表記）] : [hexadecimal（16 進）]

- [Value data（値のデータ）]：002

新しく作成された DWORD は、LSA ディレクトリ リストに次のように表示されます。

- Name: SuppressExtendedProtection
- Type: REG_DWORD
- Value: 0x00000002 (2)

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （4 ページ）

シングル サインオン用の Firefox の設定

SSO 機能は、Firefox を実行する Windows クライアントをサポートしています。

ヒント サポートされている Web ブラウザの一覧については、「サードパーティ製ソフトウェアとシングル サインオンのシステム要件」に関するトピックを参照してください。

手順

ステップ 1 Firefox を開き、次の URL を入力します。**about:config**

ステップ 2 [network.negotiate-auth.trusted-uris] へスクロール ダウンし、[Preference Name（プリファレンス名）] を右クリックし、[Modify（変更）] を選択します。

ステップ 3 ドメイン（たとえば、cisco.com）に文字列値を設定します。

ステップ 4 [OK] をクリックします。

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （4 ページ）

Real-Time Monitoring Tool（RTMT）用の Windows レジストリ設定

Real-Time Monitoring Tool（RTMT）用の SSO 設定は任意です。 この設定を実現するには、デスクトップ クライアントの新しいレジストリ キーを作成する必要があります（Windows XP または Windows 7）。

（注） 管理者は、デスクトップ クライアント用の「allowtgtsessionkey」レジストリ キー エントリを設定する必要があります。

この新しいレジストリ キーは、オペレーティング システムに応じて、次の場所のいずれかに保存します。

手順

ステップ 1 使用するオペレーティング システムに応じて、次の場所のいずれかに移動します。

- Windows XP：`HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Control \ Lsa \ Kerberos`
- Windows Vista/Windows 7：`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters`

ステップ 2 フォルダを右クリックし、[New（新規）]>[DWORD（32-bit）Value（DWORD（32-ビット）値）] を選択し、「*allowtgtsessionkey*」に名前を変更します。

ステップ 3 新しく作成されたレジストリ キーを右クリックし、[Modify（変更）] を選択します。

ステップ 4 [Value data（値のデータ）] フィールドに、「I」と入力します。

Java のインストール

OpenAM は Java Runtime Environment（JRE）が動作している必要があります。 次の手順は、OpenAM ベースのシステムを形成する Windows サーバに JRE をインストールするための詳細を提供します。

手順

ステップ 1 http://www.oracle.com/technetwork/java/archive-139210.html に進みます。

ステップ 2 サーバ アーキテクチャ（Windows x86 または Windows x64）に対応する実行ファイル選択して、JDK のインストール ファイルの推奨バージョンをダウンロードします。

（注） 推奨されるソフトウェアのバージョンの一覧については、シングル サインオンのサードパーティ製ソフトウェアのシステム要件に関連したトピックを参照してください。

ステップ 3 ダウンロードしたファイルをダブルクリックして、JDK のインストールを開始し、インストール ウィザードで提供されるデフォルト値を受け入れます。

（注） インストールディレクトリを書き留めてください。 この値は、Java JRE の位置を示し、JDK のディレクトリ パスを判断するために使用できます。 使用される JDK 値に応じて、サンプルの値は次のようになります。

- `jre-path=C:\Program Files\Java\jre7`
- `jdk-path=C:\Program Files\Java\jdk1.7.0_03`

ステップ 4 Java キー ストアと関連付けられたセキュリティ証明書は、Apache Tomcat で動作する OpenAM サーバへのセキュア接続を容易にするために必要とされます。 次のいずれかの操作を実行します。

- OpenAM/Tomcat の自己署名セキュリティ証明書を使用する場合は、ステップ 5 に進みます。
- OpenAM/Tomcat の認証局（CA）署名付きセキュリティ証明書を使用する場合は、ステップ 11 に進みます。

ステップ 5 Windows サーバ の Windows コマンド プロンプトを開くことによって、また、コマンドを実行することによってJavaキーストアを作成します。実行するコマンドは次のとおりです。`C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore C:\keystore`
このコマンドは、`C:\keystore` に Java キーストア ファイルを作成します。 keytool コマンドは、<jdk-path>/bin ディレクトリにあり、上記のコマンドの keytool コマンドへの正確なパスは使用される JDK のバージョンによって異なる場合があります。 keytool コマンドの詳細については、http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html を参照してください。

ステップ 6 キーストア パスワードを入力するよう求められたら、有効なキーストア パスワードを入力します。 たとえば、「cisco!123」などです。 キーストアにアクセスする必要があるので、キーストア パスワードを書き留めておいてください。

（注） 実稼働サーバで値の例を使用せず、キーストアの固有のパスワード値を使用してください。 このパスワードは、Apache Tomcat コンフィギュレーション ファイルおよびユーティリティのプレーン テキストで表示されます。

ステップ 7 名および姓を入力するよう求められたら、OpenAM サーバの FQDN （hostname.domainname）を入力します。
また、組織ユニット名、組織名、市または地域、都道府県、および 2 文字の国番号を入力するよう求められます。

ステップ 8 Tomcat パスワードを入力するよう求められたら、Tomcat プライベート キーに同じキー ストアのパスワードを使用するには、[Return] キーを押します。 Java キーストアは keytool コマンドで指定された場所に作成されます。 たとえば、`C:\keystore` です。

ステップ 9 次のコマンドを使用して、キーストアの Tomcat 証明書を表示できます。

例：
```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore C:\keystore
```

ステップ 10 *Tomcat* の自己署名セキュリティ証明書を選択する場合は、この手順の最後に進み、このタスクを実行を検討してください。

ステップ 11 OpenAM/Tomcat の認証局（CA）署名のセキュリティ証明書を保存するために Java キーストアを作成します。 Windows サーバでコマンド プロンプトを開き、次のコマンドを実行します。

例：

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA
-validity 1825 -keystore C:\keystore
```

このコマンドは、C:\keystore に Java キーストア ファイルを作成します。 keytool コマンドは、<jdk-path>/bin ディレクトリにあり、上記の例の keytool コマンドへの正確なパスは使用される JDK のバージョンによって異なる場合があります。 keytool コマンドの詳細については、http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html を参照してください。

ステップ 12 キーストア パスワードを入力するよう求められたら、有効なキーストア パスワードを入力します。 たとえば、「cisco!123」などです。 キーストアにアクセスする必要があるので、キーストア パスワードを書き留めておいてください。
実稼働サーバで値の例を使用せず、キーストアの固有のパスワード値を使用してください。 このパスワードは、Apache Tomcat コンフィギュレーション ファイルおよびユーティリティのプレーン テキストで表示されます。

ステップ 13 名および姓を入力するよう求められたら、OpenAM サーバの FQDN （hostname.domainname）を入力します。
また、組織ユニット名、組織名、市または地域、都道府県、および 2 文字の国番号を入力するよう求められます。

ステップ 14 Tomcat パスワードを入力するよう求められたら、Tomcat プライベート キーに同じキー ストアのパスワードを使用するには、[Return] キーを押します。 Java キーストアは keytool コマンドで指定された場所に作成されます。 たとえば、`C:\keystore` です。

ステップ 15 次のコマンドを使用して、キーストアの Tomcat 証明書を表示できます。

例：

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore
C:\keystore
```

ステップ 16 OpenAM/Tomcat インスタンスの証明書署名要求（CSR）を生成します。 Windows サーバでコマンド プロンプトを開き、次のコマンドを実行します。

例：

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -certreq -keyalg RSA -alias tomcat
-file certreq.csr -keystore C:\keystore
```

ステップ 17 CSR を CA に送信し、CSR に署名し、証明書を作成することを CA に要求します。 OpenAM サーバとなる Windows サーバに次の証明書を取得し、コピーします。

- CA の署名またはルート証明書
- 中間署名証明書（該当する場合）
- 最新の署名付き OpenAM/Tomcat 証明書

（注） これらのタスクを完了する手順については、CA のマニュアルを参照してください。

ステップ 18 ステップ 11 で作成された Java キーストアに CA の署名またはルート証明書をインポートします。 Windows サーバでコマンド プロンプトを開き、「この証明書を実行しますか」というプロンプトに「はい（yes）」と応答する次のコマンドを実行します。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
root -trustcacerts -file <filename_of_the_CA_root_certificate> -keystore
C:\keystore
```

ステップ 19 次のコマンドを使用して、キーストアの CA 署名の証明書を検索できます。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
root -keystore C:\keystore
```

ステップ 20 ステップ 11 で作成された Java キーストアに他の中間署名証明書（該当する場合）をインポートします。 Windows サーバでコマンドプロンプトを開き、「この証明書を実行しますか」というプロンプトに「はい（yes）」と応答する次のコマンドを実行します。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
inter01 -trustcacerts -file
<filepath_of_the_intermediate_signing_certificate> -keystore C:\keystore
```
- alias オプションを Java キーストアに固定の値で更新する必要があります。そうしない場合、インポート操作は「インポートされていない証明書は、alias<inter01> はすでに存在します」のようなエラーになります。

ステップ 21 次のコマンドを使用してキーストアの中間署名証明書を表示できます。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
inter01 C:\keystore
```
- alias オプションを表示する中間証明書の対応するエイリアス値で更新する必要があります。 上記の例は、「inter01」のサンプル エイリアス値を使用します。

ステップ 22 ステップ 11 で作成された Java キーストアに最新の署名付き証明書の OpenAM/tomcat 証明書をインポートします。 Windows サーバでコマンド プロンプトを開き、次のコマンドを実行します。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
tomcat -file <new_certificate_filepath> -keystore C:\keystore
```

ステップ 23 次のコマンドを使用して、キーストアの新しい OpenAM/Tomcat 証明書を表示できます。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
tomcat -keystore C:\keystore
```
この新しい tomcat 証明書の発行者は CA または中間 CA の 1 つです（該当する場合）。

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件，（4 ページ）
IM and Presence サービスへの OpenAM 証明書のインポート，（30 ページ）

OpenAM への IM and Presence 証明書のインポート

OpenAM は SSO が有効に設定された各 IM and Presence サービス ノードに存在する J2EE エージェント コンポーネントと通信する必要があります。 この通信は暗号化されたチャネル経由であるため、必要なセキュリティ証明書を OpenAM にインポートする必要があります。

OpenAM サーバは確立される暗号化された通信チャネルの各 IM and Presence サービス ノードが提示するセキュリティ証明書を信頼する必要があります。 OpenAM は OpenAM キーストアへ必要なセキュリティ証明書をインポートすることでセキュリティ証明書を信頼します。 特定の IM and Presence サービス ノードは、セキュリティ証明書の 2 種類うち 1 つを提示できます。

- 自己署名証明書
- CA-signed 証明書

（注） IM and Presence サービスの Tomcat 証明書と tomcat-trust の信頼ストアは OpenAM のセキュア通信のためのセキュリティ証明書が含まれます。 他の IM and Presence サービスの証明書と関連する信頼ストアは SSO には関連しません（たとえば、cup、cup-xmpp、cup-xmpp-s2s または ipsec）。

自己署名証明書を使用するように SSO 対応の IM and Presence サービス展開を設定する場合は、自己署名証明書をそれぞれ、OpenAM にインポートする必要があります。

CA 署名付き証明書を使用するように SSO 対応の IM and Presence サービス展開が設定される場合は、CA ルート証明書および関連する中間証明書を OpenAM にインポートする必要があります。 また OpenAM/Tomcat インスタンスに CA 署名付き証明書を使用する場合も、要求される CA ルート証明書および中間証明書は OpenAM キーストアにすでにインポートされている可能性があります。

この手順は、Java をインストールした時に、IM and Presence サービス ノードによって使用されるセキュリティ証明書のタイプを識別する方法と、作成された OpenAM キーストアに証明書をインポートする方法の詳細を提供します。

手順

ステップ 1 SSO 対応の IM and Presence サービス ノードの Cisco Unified IM and Presence オペレーティング システムの管理にサインインします。

ステップ 2 [Security（セキュリティ）] > [Certificate Management（証明書の管理）] を選択します。

ステップ 3 [Find（検索）] をクリックします。

ステップ 4 Tomcat の証明書の名前のエントリを見つけます。

ステップ 5 Tomcat 証明書の[Description（説明）] 列を確認します。

ステップ 6 説明が、Tomcat 証明書はシステムによって生成された自己署名証明書であることを示す場合は、IM and Presence サービス ノードが自己署名証明書を使用していることを示します。 この説明がない場合、CA 署名付き証明書が使用できます。

- 自己署名証明書の場合は、ステップ 7 に進みます。
- CA 署名付き証明書の場合は、ステップ 13 に進みます。

ステップ 7 [tomcat.pem（tomcat.pem）] リンクをクリックします。

ステップ 8 tomcat.pem ファイルをダウンロードするには、[Download（ダウンロード）] をクリックします。

ステップ 9 OpenAM サーバに tomcat.pem ファイルをコピーします。

ステップ 10 Java をインストールした時に、OpenAM サーバで作成されるキーストアに信頼できる証明書として tomcat.pem ファイルをインポートします。 Windows サーバ（OpenAM）でコマンドプロンプトを開き、次のコマンドを実行します。環境に合わせて keytool コマンドのパスとキーストアの場所の値のコマンドを更新するには、「この証明書を信頼しますか」というプロンプトに「はい（yes）」と応答します。 `C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keystool.exe" -import -alias cup01 -trustcacerts -file <full_filepath_of_the_tomcat.pem> -keystore C:\keystore`

（注） -alias オプションは Java キーストアに固有の値で更新する必要があります。そうでない場合は、インポート操作が次のようなエラーになる可能性があります。「インポートされていない証明書、alias <cup01> はすでに存在します」

ステップ 11 環境に合わせて keytool コマンドのパスとキーストアの場所の値を更新することで、次のコマンドを使用してキーストアの tomcat.pem を表示できます。

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v -alias cup01 -keystore C:\keystore
```

（注） -alias オプションは、ステップ 10 で使用する値に一致する必要があります。そうでない場合は、キーストア エントリが見つからない場合があります。

ステップ 12 ステップ 16 に進みます。

ステップ 13 IM and Presence サービス のTomcat 証明書の署名に使用された CA ルート証明書と中間証明書を識別します。 CA から OpenAM サーバに必要な証明書（CA ルート証明書および中間証明書）をダウンロードします。

ステップ 14 信頼される証明書として OpenAM サーバのキーストアにこれらの証明書をインポートします。 Windows サーバ（OpenAM）でコマンドプロンプトを開き、環境に合わせて keytool コマンドのパスとキーストアの場所の値のコマンドを更新することで、ダウンロードした証明書それぞれに次

のコマンドを実行し、「この証明書を信頼しますか」というプロンプトに「はい（Yes）」と答えます。

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias
root_ca -trustcacerts -file <full_filepath_of_the_certificate> -keystore
C:\keystore
```

（注） -alias オプションは Java キー ストアに固定な値で更新する必要があります。そうでない場合は、インポート操作が次のようなエラーになる可能性があります。「インポートされていない証明書、エイリアス <root_ca> はすでに存在します」

ステップ 15 環境に合わせて keytool コマンドのパスとキーストアの場所の値を更新することで、次のコマンドを使用してキーストアの証明書を表示できます。

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v -alias
root_ca -keystore C:\keystore
```

（注） -alias オプションは、ステップ 14 で使用する値に一致する必要があります。そうでない場合は、キーストア エントリが見つからない場合があります。

ステップ 16 SSO が有効に設定されている IM and Presence ノードそれぞれで、この手順を繰り返します。

（注） IM and Presence サービス ノードで使用される CA 署名付き証明書では、同じ CA 証明書と中間証明書をOpenAM キーストアに複数回インポートする必要はありません。 IM and Presence サービス ノードが同じ CA 証明書および中間証明書によって署名されたことを検出する場合、OpenAM キーストアにそれらの証明書をインポートする必要はありません。

Tomcat のインストール

OpenAM では Apache Tomcat Web コンテナを OpenAM サーバ の Windows サーバ ベース のシステムにインストールする必要があります。 この手順では、OpenAM Windows ベースのシステムでの Apache Tomcat のインストールの手順の詳細を説明します。 この手順で参照される変数の説明については、次の表を参照してください。

表 *3*：変数の説明

変数	説明
<certstore-path>	Java アプリケーションと Apache Tomcat で使用される Java キーストアへのファイル パス。 信頼できるサーバの公開証明書はこのキーストアに保存されます。 Java キー ストアのファイル パスを設定するために次の手順のステップ 5 または 11 を参照してください。

変数	説明
<certstore-password>	<certstore-path> にある Java キーストアへのアクセスに使用するパスワード。 Java キーストア パスワードに使用する値を設定するには、次の手順のステップ 6 または 12 を参照してください。

手順

ステップ 1 OpenAM ベース システムを構成する Windows サーバに Apache Tomcat の推奨バージョンをダウンロードします。推奨されるソフトウェアとバージョンの一覧については、シングルサインオンのサードパーティ製ソフトウェアとシステム要件に関するトピックを参照してください。

（注） 32bit/64bit Windows サービス インストーラの実行可能ファイルをダウンロードします。

ステップ 2 Apache Tomcat のインストールを開始するには、ダウンロードしたファイルをダブルクリックします。

ステップ 3 Apache Tomcat セットアップ ウィザードで [Next（次へ）] をクリックします。

ステップ 4 [License Agreement（ライセンス契約書）] ダイアログボックスで、[I agree（同意する）] をクリックします。

ステップ 5 [Choose Components（コンポーネントを選択）] ダイアログボックスで、インストールのタイプとして、[Minimum（最少）] をクリックして [Next（次へ）] を選択します。

ステップ 6 [Configuration（設定）] ダイアログボックスで、デフォルト設定に同意し、[Next（次へ）] をクリックします。

ステップ 7 [Java Virtual Machine（Java 仮想マシーン）] ダイアログボックスで、インストールされている JRE のパスが jre-path の値に設定されていることを確認します。

（注） Java の推奨バージョンを使用する場合、パスはデフォルトで表示されます。 Java の推奨バージョンを使用しない場合は、入力したパスが Java のインストール時に使用されたパスに一致することを確認します。

ステップ 8 [Next（次へ）] をクリックします。

ステップ 9 [Choose Install Location（インストール先の選択）] ダイアログボックスで、デフォルト設定を受け入れて、[Install（インストール）] をクリックします。 後で必要になるので、Tomcat のインストール先を書き留めてください。

（注） インストール先は、この後の手順で「tomcat-dir」と呼ばれます。

ステップ 10 [Finish（終了）] をクリックします。

ステップ 11 自動的に起動するように Apache Tomcat を設定します。

a) [Start（開始）] > [All Programs（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Configure Tomcat（Tomcat の設定）] を選択します。

b) [General（全般）] タブで、[Startup type（起動タイプ）] を [Automatic（自動）] に設定します。

c) [Apply（適用）] をクリックします。
d) [OK] をクリックします。

ステップ 12 Apache Tomcat ランタイム パラメータを設定します。

a) [Start（開始）] > [All Programs（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Configure Tomcat（Tomcat の設定）] を選択します。
b) [Java] タブから、次の [Java options（Java オプション）] を追加します。

```
-Djavax.net.ssl.trustStore=<certstore-path>
-Djavax.net.ssl.trustStorePassword=<certstore-password>
-XX:MaxPermSize=256m
```

ヒント 変数の説明については、この手順の初めのパラメータ テーブルを参照してください。

例：

```
-Djavax.net.ssl.trustStore=C:\keystore
-Djavax.net.ssl.trustStorePassword=cisco!123
-XX:MaxPermSize=256m
```

c) [Initial memory pool（最初のメモリ プール）] を 512 に設定します。
d) [Maximum memory pool（最大のメモリ プール）] を1024 に設定します。
e) [Apply（適用）] をクリックします。
f) [OK] をクリックします。

ステップ 13 テキスト エディタを使用して、`<tomcat-dir>\conf` フォルダの下にある server.xml ファイルを開きます。 <tomcat-dir> の値を設定するには、ステップ 9 を参照してください。

例：
値の例は「`C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf`」です。

ステップ 14 8080 コネクタ ポートをコメントにします。 次のようにコードを入力します。

例：

```
<!-- <Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" /> -->
```

ステップ 15 8443 コネクタ ポートをアンコメントにします。 8443 コネクタの最後の <!- - code at the beginning and - -> を削除します。 コネクタの設定に、さらに 3 つの属性を追加する必要があります。

- keystoreFile（Java をインストールしたときに作成されたキーストア ファイルの場所。 この例では、`C:\keystore` に作成されました）
- keystorePass
- keystoreType

次のようにコードを入力します。

例：

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<certstore-path>"
keystorePass="<certstore-password>"
keystoreType"JKS"/>
```

ヒント 変数の説明については、この手順の初めのパラメータ テーブルを参照してください。

ステップ 16 server.xml ファイルを保存します。

ステップ 17 Tomcat サービスを開始します。

a) [Start（開始）] > [All Programs（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Configure Tomcat（Tomcat の設定）]

b) [General（全般）] タブで [Start（開始）] をクリックします。 Tomcat サービスがすでに実行されていた場合は、[Stop（停止）] をクリックし、次に [Start（開始）] をクリックします。

ステップ 18 設定をテストするには、Tomcat インスタンスを Windows サーバの Web ブラウザを開始し、`https://localhost:8443/tomcat.gif` にアクセスしてください。 Web ブラウザが Tomcat インスタンスによって表示されるセキュリティ証明書を信頼しないので、Webブラウザで非セキュアな接続に関する警告ダイアログが表示される場合があります。 証明書を確認するか、ローカル証明書ストアに証明書を追加することで、ブラウザが証明書を信頼するか、使用可能なブラウザ コントロールを使用してWeb アプリケーション（より低いセキュア オプション）の手順を実行できます。 設定が正しい場合、Tomcat ロゴは Web ブラウザ ウィンドウに表示されます。

ステップ 19 Apache Tomcat への着信接続を許可するために Windows ファイアウォールを設定します。

a) [Start（開始）] > [Administrative Tools（管理ツール）] > [Windows Firewall and Advanced Security（Windows ファイアウォールおよびアドバンスド セキュリティ）] を選択します。

b) [Windows Firewall and Advanced Security（Windows ファイアウォールおよびアドバンスド セキュリティ）] > [Inbound Rules（インバウンド ルール）] を選択します。

c) [Inbound Rules（インバウンド ルール）] を右クリックします。

d) [New Rule（新しいルール）] をクリックします。

e) [What type of rule would you like to create（どのタイプのルールを作成しますか）] オプションのリストで [Port（ポート）] を選択します。

f) [Next（次へ）] をクリックします。

g) [Does this rule apply to TCP or UDP?（このルールをTCPまたはUDPに適用しますか）] オプションのリストで [TCP（TCP）] を選択します。

h) [Does this rule apply to all local ports or specific local ports?（このルールをすべてのローカル ポートまたは特定のローカル ポートに適用しますか）] オプションのリストで [Specific local ports（特定のローカルポート）] を選択します。

i) 「8443」を入力し、[Next（次へ）] をクリックします。

j) [What action should be taken when a connection matches the specified conditions?（接続が指定条件に一致する場合、どの操作をしますか）] オプションのリストで [Allow the connection（接続に適用する）] を選択します。

k) [Next（次へ）] をクリックします。

l) [When does the rule apply?（いつルールを適用しますか）] オプションのリストで [Domain（ドメイン）] だけを選択します。
m) [Next（次へ）] をクリックします。
n) 選択する名前と説明を入力し、[Finish（終了）] をクリックします。

ステップ 20 設定をテストするには、ネットワークの別のホストにログインして、Tomcat インスタンスを含む Windows サーバの Web ブラウザを開始し、`https://<openam-fqdn>:8443/tomcat.gif` の Tomcat インスタンスを含む Windows サーバの完全修飾ドメイン名である `<openam-fqdn>` を参照します。 Web ブラウザが Tomcat インスタンスによって表示されるセキュリティ証明書を信頼しないので、Web ブラウザで非セキュアな接続に関する警告ダイアログが表示される場合があります。 証明書を確認するか、ローカル証明書ストアに証明書を追加することで、ブラウザが証明書を信頼するか、使用可能なブラウザ コントロールを使用してWeb アプリケーション（より低いセキュア オプション）の手順を実行できます。 設定が正しい場合、Tomcat ロゴは Web ブラウザ ウィンドウにロードされ表示されます。

Apache Tomcat での OpenAM War の展開

手順

ステップ 1 ForgeRock の Web サイトから推奨される OpenAM リリースをダウンロードします。
ヒント 詳細については、シングル サインオンにおけるサードパーティ製ソフトウェアとシステム要件に関するトピックを参照してください。

ステップ 2 .zip ファイルを取得し、.zip ファイルに含まれる opensso.war ファイルを検索します。

ステップ 3 OpenAM サーバとなる Windows サーバに WAR ファイルをコピーします。 この Windows サーバは、以前に設定された Tomcat サービスを実行する必要があります。

ステップ 4 Apache Tomcat サービスが実行中の場合は、Apache Tomcat サービスを停止します
a) [Start（開始）] > [All Programs（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Configure Tomcat（Tomcat の設定）] を選択します。
b) [General（全般）] タブで、[Stop（停止）] をクリックします。

ステップ 5 WAR ファイルを次の場所にコピーすることによって Tomcat インスタンスを含むWindows サーバの WAR ファイルを展開します。`<tomcat-dir>\webapps`

例：
`C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps`
（注） *<tomcat-dir>* 変数の説明については、Tomcat のインストールに関するトピックを参照してください。

ステップ 6 Apache Tomcat サービスを開始します。
a) [Start（開始）] > [All Programs（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Configure Tomcat Tomcat7（Tomcat Tomcat7の設定）] を選択します。

b) [General（全般）] タブで [Start（開始）] をクリックします。

（注） WAR ファイルは、数分以内に完全に展開されます。 webapps フォルダに、WAR ファイルと同じ名前ではなく拡張子（.war）が削除された名前で新しいフォルダが作成されます。

ステップ 7 Web ブラウザを起動するか、または `https://<openam-fqdn>:8443/<war-file-name>` を入力して設定を確認します。そこでの *<openam-fqdn>* は、OpenAM/Tomcat インスタンスを含む Windows サーバの FQDN であり、*<war-file-name>* は拡張子（.war）が削除された OpenAM WAR ファイルの名前です。 設定が正しい場合は、OpenAM 管理インターフェイスで Web ブラウザ ウィンドウがロードされます。

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （4 ページ）

GUI Configurator を使用した OpenAM のセットアップ

次の手順では、OpenAM の設定方法を指定します。 既存の OpenAM サーバがある場合、または OpenAM について確実に理解している場合は、サーバを別に設定できます。

OpenAM サーバおよび J2EE Policy エージェントには、インストールを実行するマシンのホスト名の FQDN が必要です。 インストール、設定、使用の問題が発生しないように、「localhost」のようなホスト名または「192.168.1.2」のような数字の IP アドレスの使用を避けることを強く推奨します。

OpenAM は Web ブラウザを使用してアクセスする必要がある、Mozilla Firefox などの Web ベースの管理インターフェイス を提供します。 OpenAM に初めてアクセスする場合は、`https://server1.cisco.com:8443/opensso` などの URL で、OpenAM サーバの FQDN を使用する必要があります。このサンプルの URL 値では、OpenAM WAR ファイルが `opensso` として導入されることが想定されます。

OpenAM 設定およびロギング情報は OpenAM/Tomcat インスタンスを実行するユーザのホーム ディレクトリにある 2 つのディレクトリに通常保存されています。たとえば、

- `C:\opensso`（この場合、フォルダ名は OpenAM WAR ファイルのために展開される URI に一致します。 たとえば、opensso）
- `C:\.openssocfg`

設定中に問題が発生した場合、コンフィギュレータはエラー メッセージを表示します。 可能な場合は、エラーを修正して、設定をやり直します。 次のログ ファイル ディレクトリは役立つ情報を提供する場合があります。

- Tomcat Web コンテナのログ： `tomcat-dir\logs`
- OpenAM のインストール ログ：`C:\opensso`（フォルダ名は OpenAM WAR ファイルのために展開される URI に一致します。 たとえば、opensso）

デフォルトでは、OpenAM は Windows プラットフォームの `C:\opensso` の下に展開されます。

手順

ステップ 1 Web ブラウザを開き、次の URL を使用して OpenAM サーバに移動します。`https://<fqdn of openam server>:8443/<WAR filename>`。

例：
`https://server1.cisco.com:8443/opensso`

（注） OpenAM に初めてアクセスするときは、OpenAM の初期設定を行うために Configurator に転送されます。 OpenAM に初めてアクセスするときは、[Configuration Options（設定オプション）] ウィンドウが表示されます。

ステップ 2 [Create Default Configuration（デフォルト設定の作成）] を選択します。

（注） エラーが発生した場合は、ローカル マシンでステップ 1 と 2 を繰り返してください。

ステップ 3 [OpenSSO Configurator（OpenSSO コンフィギュレータ）] ウィンドウで、OpenAM 管理者（amAdmin）とデフォルト ポリシー エージェントのユーザ（UrlAccessAgent）のパスワードを指定し、確認します。 デフォルト ポリシー エージェント ユーザは、この設定例では後で使用しません。amAdmin は、設定を変更するために OpenAM にログインするたびに使用します。

（注） amAdmin は OpenAM 管理者のみに適用される推奨値です。

ステップ 4 [Create Configuration（構成の作成）] をクリックします。
設定が完了すると通知されます。

ステップ 5 [Proceed to Login（ログインへ進む）] を選択します。

ステップ 6 amAdmin 用に、前に設定したユーザ名とパスワードを使用して展開した OpenAM Web アプリケーションにログインします。

ステップ 7 [Access Control（アクセス コントロール）] タブで、[/（Top Level Realm）（/（最上位領域））] をクリックします。

ステップ 8 [Authentication（認証）] タブで、[Core（コア）] をクリックします。

ステップ 9 [All Core Settings（すべてのコアの設定）] クリックします。

ステップ 10 [User Profile（ユーザ プロファイル）] を [Ignored（無視）] に設定します。

ステップ 11 プロファイルを更新するには、[Save（保存）] をクリックします。

ステップ 12 OpenAM GUI からログアウトします。

OpenAM サーバでのポリシーの設定

次の表で詳しく説明するポリシー ルールを使用して OpenAM サーバ ポリシーをセットアップします。

表 *4* : ポリシー ルール

サービス タイプ	名前	リソース名	アクション
URL のポリシー エージェント（リソース名を含む）	<hostname>-01	`https://<IMP FQDN>/*`	Enable GET, Value = Allow Enable POST , Value = Allow
	<hostname>-02	`https://<IMP FQDN>/*?*`	
	<hostname>-03	`https://<IMP FQDN>/*?*?*`	
	<hostname>-04	`https://<IMP FQDN>:8443/*`	
	<hostname>-05	`https://<IMP FQDN>:8443/*?*`	
	<hostname>-06	`https://<IMP FQDN>:8443/*?*?*`	

この手順で定義されているとおりにポリシー ルールを適用すると、IM and Presence の管理/ユーザ インターフェースは次の URL 形式を使用して Web ブラウザでのみアクセスが可能になります。

- `https://<IMP FQDN>`：たとえば、`https://IMP-Node-01.cisco.com`
- `https://<IMP FQDN>:8443`：たとえば、`https://IMP-Node-01.cisco.com:8443/`

`https://<IMP HOSTNAME>`（たとえば、`https://IMP-Node-01/`）などのホスト名だけを指定する URL を使用して Cisco Unified CM IM and Presence の管理/ユーザ インターフェイスにアクセスすることはできません。

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [Access Control（アクセス コントロール）] タブで、[/（Top Level Realm）（/（トップ レベルのレルム））] を選択します。

ステップ 3 [Policies（ポリシー）] タブで、[New Policy（新規ポリシー）] をクリックします。

ステップ 4 [Name（名前）] フィールドに、ポリシー名（IMPPolicy など）を入力し、[OK（OK）] をクリックします。
IMPPolicy はあくまでも推奨値です。 有効な名前の値を使用できます。 この後の設定では、この値は必要ありません。

ステップ 5 編集のために、新しいポリシー [IMPPolicy（IMPPolicy）] を選択します。

ステップ 6 [Rules（ルール）] をクリックします。

ステップ 7 次の順序でルールを追加します。

a) [Rules（ルール）] セクションで、[New（新規）] をクリックします。

b) [URL Policy Agent（with resource name）（URL のポリシー エージェント（リソース名を含む））] として [Service Type（サービス タイプ）] を選択します。
c) [Next（次へ）] をクリックします。
d) [Name（名前）] フィールドでは、上記のポリシー ルール テーブルの推奨されたルールの名前を入力し、<hostname> を IM and Presence ノードの実際のホスト名で置き換えます。
e) 提供される [ResourceName（リソース名）] フィールドで IM and Presence ノードの実際の完全修飾ドメイン名と <IMP FQDN> に代わり、このルールに対応するリソース名を入力します。
f) Allow 値で Get アクションを確認します。
g) Allow 値で POST アクションを確認します。
h) ルールの更新を完了するには、[Finish（終了）] をクリックします。
i) ポリシー アップデートを保存するには、[Save（保存）] をクリックします。
j) 上記テーブルのルールごとにこの手順全体を繰り返し、[Finish（終了）] をクリックします。

SSO の有効な各 IM and Presence サービス ノードに、この 6 つのルールのセットを追加する必要があります。

ステップ 8 ポリシーに 1 つのサブジェクトを追加する必要があります。 次のようにサブジェクトを追加します。

a) [Subject（サブジェクト）] セクションで、[New（新規）] をクリックします。
b) [Subject（サブジェクト）] タイプとして[Authenticated Users（認証ユーザ）] を選択します。
c) [Next（次へ）] をクリックします。
d) [Name（名前）] 値として「IMPSubject」を入力します。
IMPSubject はあくまでも推奨値です。 任意の有効な値を使用できます。 この後の設定で、この値は必要ありません。
e) サブジェクトの更新を完了するには、[Finish（終了）] をクリックします。
f) ポリシー アップデートを保存するには、[Save（保存）] をクリックします。

複数の IM and Presence サービス ノードがシングル サインオンで有効な場合は、1 つのサブジェクトだけがこのポリシーで必要です。

ステップ 9 ポリシーに 1 つの条件を追加する必要があります。 次のように条件を追加します。

a) [Conditions（条件）] セクションで、[New（新規）] をクリックします。
b) 条件タイプとして [Active Session Time（アクティブ セッション タイム）] を選択します。
c) [Next（次へ）] をクリックします。
d) [Name（名前）] 値として「IMPTimeOutCondition」を入力します。
IMPTimeOutConditionはあくまでも推奨値です。 有効な名前の値を使用できます。 この後の設定で、この値が必要です。
e) [Maximum Session Time（minutes）（最大セッション時間（分））] として「120」を入力します。
f) [Terminate Session（セッションの終了）] フィールドが [No（いいえ）] に設定されていることを確認します。
g) サブジェクトの更新を完了するには、[Finish（終了）] をクリックします。
h) ポリシー アップデートを保存するには、[Save（保存）] をクリックします。

複数の IM and Presence サービス ノードが SSO で有効な場合は、1 つの条件だけがこのポリシーで必要であることに注意してください。

SSO モジュール インスタンスの設定

この単一のモジュール インスタンスは、同じ Active Directory ドメインが展開全体で使用されている限り、SSO が設定されている複数の IM and Presence サービス ノードを共有することができます。 複数の Active Directory ドメインを含む導入シナリオでは、このマニュアルでは説明しません。

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [Access Control（アクセス コントロール）] タブから、[Top Level Realm（トップ レベルのレルム）] をクリックします。

ステップ 3 [Authentication（認証）] タブで、[Module Instances（モジュール インスタンス）] をクリックします。

ステップ 4 [Module Instances（モジュール インスタンス）] ウィンドウで、[New（新規）] をクリックします。

ステップ 5 新しいログイン モジュール インスタンス名（IMPKRBなど）を入力して、[Type（タイプ）] リストから [Windows Desktop SSO（Windows デスクトップ SSO）] を選択します。

ステップ 6 [OK] をクリックします。
このモジュール インスタンス名は、後で IM and Presence ノードで SSO を有効にするときに使用されます。

ステップ 7 [Save（保存）] をクリックします。

ステップ 8 [Module Instances（モジュール インスタンス）] ウィンドウで、新しいログイン モジュールの名前（たとえば、IMPKRB）を選択し、次の情報を入力します。

パラメータ	説明
サービス プリンシパル（Service Principal）	この値はシングル サインオンの Active Directory をプロビジョニングするときに指定された値とまったく同じである必要があります。たとえば、- princ 値です。 たとえば、（openAM のサーバ名とドメインを使用して）`HTTP/server1.cisco.com@CISCO.COM`。
キータブ ファイル名	この値はシングル サインオンの Active Directory をプロビジョニングしたときに作成されたキータブ ファイルの場所である必要があります。 たとえば、（Windows プラットフォームで）`C:\keytab\server1.HTTP .keytab` です。

パラメータ	説明
Kerberos レルム	OpenAM サーバのドメイン。 たとえば、CISCO.COM。
Kerberos のサーバ名（Active Directory）	AD サーバの FQDN を提供します。 AD サーバは通常、Kerberos ドメイン コントローラです。 フェールオーバーの目的で複数の Kerberos ドメイン コントローラが存在する場合は、区切り文字としてコロン（:）を使用してすべての Kerberos ドメイン コントローラを設定できます。 たとえば、ad.cisco.com です。
Authentication Level	たとえば、22 です。

ステップ 9 [Save（保存）] をクリックします。
モジュール インスタンスが IMPKRB という名前で作成されます。

ステップ 10 SSO モジュールが有効な Windows ユーザとしてWindows デスクトップ セッションにログインすることで正常に機能することを確認します（AD に存在する有効なエンド ユーザでログインし、管理者アカウントは使用しないでください）。 次の URL にアクセスしてください。

（注） ブラウザに SSO が設定されている必要があります。

`https://<openam-FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>`

それぞれの説明は次のとおりです。

パラメータ	説明
<openam-FQDN>	OpenAM サーバの FQDN。
<war-file-name>	導入される OpenAM War ファイルの名前。たとえば、opensso。
<SSO_Module>	WindowsDesktopSSO モジュールの名前。

画面がログインに成功したことを通知します。

OpenAM サーバでの J2EE エージェント プロファイルの設定

J2EE エージェントは、SSO が有効な各 IM and Presence Service ノードでインスタンス化される内部コンポーネントです。 J2EE エージェントごとに、OpenAM サーバで関連する J2EE エージェント プロファイルを設定する必要があります。 したがって、J2EE エージェント プロファイルは SSO が有効なすべての IM and Presence Service ノードで必要です。 複数のノードを SSO 用に設定する場合は、J2EE エージェント プロファイルを追加の各ノードに作成する必要があります。

次の表に、IM and Presence Service ノードに必要な J2EE プロファイル エージェントのパラメータを一覧表示します。

表 *5* : ***J2EE*** プロファイルのエージェント セットアップ パラメータの説明

パラメータ	説明
Name（名前）	J2EE Policy Agent の名前。 たとえば、<*hostname-j2ee-agent*>。この場合、*hostname* は IM and Presence Service ノードのホスト名（たとえば、impNode01 j2ee agent）です。
Password（パスワード）	J2EE Policy Agent のパスワード。 （注） パスワードは IM and Presence Service で SSO を有効にするときに使用されます。
Configuration（設定）	J2EE Policy Agent 設定が保存されている場所を制御します。 [Centralized（一元化）] を選択します。
Server URL（サーバ URL）	OpenAM サーバの完全な URL。 たとえば、`https://<OpenAM FQDN>:8443/opensso`。この場合、`opensso` は .war 拡張子が削除された OpenAM War ファイルの名前です。
Agent URL（エージェント URL）	OpenAM が通知をパブリッシュする J2EE Policy Agent の URL。 たとえば、`https://<IMP FQDN>:8443/agentapp` （注） 値「`agentapp`」は上記のサンプル URL の重要項目です。`agentapp` 値を使用する場合、「ポリシー エージェントが展開される場所に関連するパスを入力してください」というプロンプトが表示されたときに「`agentapp`」と入力します。

次の表に、IM and Presence Service の各 Web GUI アプリケーションのログイン フォームの URI を一覧表示します。

表 *6* : ***IM and Presence Service*** の ***Web GUI*** アプリケーションの ログイン フォームの ***URI***

アプリケーション	サンプル値
Cisco Unified CM IM and Presence の管理	`/cupadmin/WEB-INF/pages/logon.jsp`
Cisco Unified IM and Presence サービスアビリティ	`/ccmservice/WEB-INF/pages/logon.jsp`
Cisco Unified IM and Presence のレポート	`/cucreports/WEB-INF/pages/logon.jsp`
Cisco Unified IM and Presence OS の管理	`/cmplatform/WEB-INF/pages/logon.jsp`
IM and Presence のディザスタ リカバリ システム	`/drf/WEB-INF/pages/logon.jsp`

アプリケーション	サンプル値
Real Time Monitoring Tool（RTMT）	`/ast/WEB-INF/pages/logon.jsp`
Cisco Client Profile Agent	`/ssoservlet/WEB-INF/pages/logon.html`

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [Access Control（アクセス コントロール）] タブで、[/（Top Level Realm）（/（最上位領域））] をクリックします。

ステップ 3 [Agents（エージェント）] タブから、[J2EE（J2EE）] タブを選択します。

ステップ 4 [Agents（エージェント）] セクションで、[New（新規）] をクリックします。

ステップ 5 J2EE セットアップ パラメータを入力します。

ステップ 6 [Create（作成）] をクリックします。
<hostname-j2ee-agent> の名前で J2EE エージェントが作成されます。

ステップ 7 作成した J2EE エージェントを選択します。

ステップ 8 [Login Processing（ログイン処理）] セクションの下の [Application（アプリケーション）] タブで、IM and Presence Service の各 Web GUI アプリケーションの ログイン フォームの URI を追加します。

ステップ 9 [Save（保存）] をクリックします。

ステップ 10 [OpenAM Services（OpenAM サービス）] タブで、`https://<OpenAM FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>` のように OpenSSO のログイン URL を追加します。

ヒント 入力する *<SSO_Module>* 値が SSO モジュール インスタンスをセットアップするときに入力した値に一致する必要があります。 たとえば、`https://server1.cisco.com:8443/opensso/UI/Login?module=IMPKRB` です。

ステップ 11 テキスト領域で、ログイン URL 以外のすべての URL を削除します。 前のステップで指定したログイン URL のみがテキスト領域にリストされている必要があります。

ステップ 12 [Save（保存）] をクリックします。

ステップ 13 [Back to Main Page（メイン ページに戻る）] をクリックします。

ステップ 14 SSO 用に有効にするその他すべての IM and Presence Service ノードの J2EE プロファイル エージェントを作成するために、ステップ 4 から ステップ 13 を繰り返します。

関連トピック

GUI を使用した シングル サインオンの有効化, （35 ページ）

OpenAM セッション タイムアウトの設定

OpenAM セッション タイムアウトは、IM and Presence サービス ノードにセットされるセッション タイムアウト パラメータよりも大きい値に設定する必要があります。 IM and Presence サービス ノードのセッション タイムアウト値を決定するには、CLI を使用して次のコマンドを入力してください。

show webapp session timeout

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。
ステップ 2 [Configuration（設定）] タブで、[Global（グローバル）] を選択します。
ステップ 3 [Session（セッション）] をクリックします。
ステップ 4 [Dynamic Attributes（ダイナミック属性）] をクリックします。
ステップ 5 [Maximum Idle Time（最大アイドル時間）] フィールドに値を入力します。
ステップ 6 [Save（保存）] をクリックします。

IM and Presence サービスへの OpenAM 証明書のインポート

SSO の IM and Presence サービス ノードは、暗号化されたチャネル経由の OpenAM サーバと通信します。 暗号化された通信チャネルの確立は、OpenAM サーバによって提示されるセキュリティ証明書を信頼するために、SSO を有する各 IM and Presence サービス ノードが必要です。 IM and Presence サービス ノードは tomcat-trust の信頼ストアに必要なセキュリティ証明書をインポートすることで、セキュリティ証明書を信頼します。

必要な手順は、OpenAM サーバの Java キーストアの作成時に使用するセキュリティ設定によって異なります。

- OpenAM/Tomcat インスタンスの自己署名セキュリティ証明書を使用します。
- OpenAM/Tomcat インスタンスの CA 署名付きセキュリティ証明書を使用します。

注意 OpenAM 証明書のインポートはサービスに影響し、メンテナンス時間帯に OpenAM 証明書をインポートすることを強く推奨します。

（注） 証明書のインポートの詳細については、『*Cisco Unified System Maintenance Guide for IM and Presence*』を参照してください。

手順

ステップ 1 SSO 対応の IM and Presence データベース パブリッシャ ノードの Cisco Unified CM IM and Presence の管理にログインします。

ステップ 2 [System（システム）] > [Security（セキュリティ）] > [Certificate Import Tool（証明書のインポート ツール）] を選択します。

ステップ 3 証明書信頼ストアとして [Tomcat Trust（Tomcat 信頼）] を選択します。

ステップ 4 [Peer Server（ピア サーバ）] として OpenAM サーバの完全修飾ドメイン名を入力します。

ステップ 5 [Peer Server Port（ピア サーバ ポート）] として 8443 を入力します。

ステップ 6 [Submit（送信）] をクリックします。
証明書インポート ツールは 2 種類のテストを実行します。

- [Verify reachability of the specified certificate server （pingable）（指定した証明書サーバ（ping が可能）の到達可能性の確認）] : OpenAM サーバが、この IM and Presence のノードに到達可能なことを確認します。 このテストに失敗する場合は、ping 操作をブロックする OpenAM ベースの Windows システム ファイアウォールが原因である可能性があります。 Windows ファイアウォールで ping を許可する IM and Presence サービスへの OpenAM 証明書のインポートに関連するトピックを参照してください。
- [Verify SSL connectivity to the specified certificate server（指定した証明書サーバへの SSL 接続の確認）] : この IM and Presence ノードが OpenAM サーバに安全に接続することが可能かどうかを確認します。 このテストが「証明書の欠落」によって失敗する場合は、必要な証明書が見つからず、セキュアな接続を確立できません。 このテストが失敗した場合は、次の手順に進みます。 このテストに成功した場合、ステップ 15 に進みます。

  （注） このテストが「トラブルシュータで内部エラーが発生しました」のメッセージが表示されて失敗する場合、次のステップに進む前に、証明書の障害をトラブルシューティングします。

ステップ 7 [Configure（設定）] をクリックして証明書ビューアを開きます。 証明書ビューアは、TLS 接続ハンドシェイク中に OpenAM から提示される証明書チェーンを視覚的に表示します。 これは、この IM and Presence サービス ノードにインポートされる必要がある証明書を表示します。

ステップ 8 チェーンの証明書を検査し、発行者が信頼できることを確認します。

ステップ 9 [Accept Certificate Chain（証明書チェーンを許可する）] のチェックボックスをオンにし、[Save（保存）] をクリックします。
チェーンから必要な証明書が、この IM and Presence サービス ノードの tomcat-trust の信頼ストアに今すぐインポートされます。

ステップ 10 [Close（閉じる）] をクリックします。
証明書のインポート ツールは「証明書が検証に成功」と報告します。

ステップ 11 次の CLI コマンドを使用して、このノードのCisco Intercluster Sync Agent サービスを再起動します。**utils service restart Cisco Intercluster Sync Agent**

ステップ 12 次の CLI コマンドを使用して、このノードで Tomcat サービスを再起動します。 **utils service restart Cisco Tomcat**

ステップ 13 このクラスタの各 IM and Presence サービス サブスクライバ ノードのステップ 11 と 12 を繰り返します。

ステップ 14 このクラスタの各サブスクライバ ノードの証明書のインポート ツールを使用して、セキュアな接続を確認します。

a) SSO が設定されている IM and Presence サービス サブスクライバ ノードの Cisco Unified CM IM and Presence の管理にログインします。
b) [System（システム）]>[Security（セキュリティ）]>[Certificate Import Tool（証明書のインポート ツール）] を選択します。
c) 証明書信頼ストアとして [Tomcat Trust（Tomcat 信頼）] を選択します。
d) [Peer Server（ピア サーバ）] として OpenAM サーバの FQDN を入力します。
e) [Peer Server Port（ピア サーバ ポート）] として 8443 を入力します。

ステップ 15 SSO が有効なすべての IM and Presence サービス クラスタのための、この手順を繰り返します。

関連トピック

シングル サインオンの設定前の重要な情報, （6 ページ）
証明書エラー

シングル サインオンのアクティブ化

SSO を有効にする場合は、ここに示す順序で次のタスクを実行する必要があります。

注意 SSO を有効にするとサービスに影響を与えます。そのため、メンテナンス時に、SSO を有効にすることを推奨します。

SSO 有効化前のアクセス権限の設定

SSO の有効化前および有効化後に設定されている必要があるユーザ アクセス権限を理解することが重要です。 権限を理解することで、IM and Presence Service アプリケーションにアクセスするときにユーザの権限が誤っているという状況を避けることができます。

表 7: シングル サインオンを有効化するための前提条件

アプリケーション	注意

Cisco Unified CM IM and Presence の管理 • Cisco Unified CM IM and Presence の管理 • IM and Presence サービスアビリティ • IM and Presence のレポート	

SSOを有効にする前に、管理アクセスを容易にするために必要なユーザ グループのメンバーであるエンド ユーザが存在していることを確認します。

インストール時に作成されたデフォルトの管理者アプリケーション ユーザには次が必要です。

グループ：

- 標準監査ユーザ
- 標準 CCM スーパー ユーザ

権限：

- Standard AXL API Access
- 標準 Admin Rep Tool Admin
- 標準監査ログ管理
- Standard CCM Admin Users
- Standard CCMADMIN Administration
- 標準 CUReporting
- 標準 EM 認証プロキシ権
- Standard SERVICEABILITY Administration
- 標準 SSO 設定管理

これらの役割を持つ上記のユーザ グループのメンバーであるユーザには、デフォルトの管理者と同様に、IM and Presence Service への完全なアクセス権があります。

IM and Presence Service のデフォルトのアプリケーション ユーザを表示するには、[Cisco Unified CM Administration（Cisco Unified CM の管理）] > [User Management（ユーザ管理）] > [Application User（アプリケーション ユーザ）] > [Find（検索）] を選択します。詳細を表示するには、デフォルトのアプリケーション ユーザ（インストール時に作成されたユーザ）を選択します。

IM and Presence Service のこれらのグループにエンドユーザを追加するには、[Cisco Unified CM Administration（Cisco Unified CM の管理）] > [User Management（ユーザ管理）] > [User Settings（ユーザ設定）] > [Access Control Group（アクセス制御グループ）] > [Find（検索）] を選択します。 グループを選択し、[Add End Users（エンドユーザの追加）] をクリックします。 目的のエンドユーザを検索してそのユーザを選択し、[Add End Users

	to Group（グループへのエンドユーザの追加）] をクリックします。
Cisco Unified IM and Presence オペレーティング システムの管理 • IM and Presence オペレーティング システムの管理 • IM and Presence のディザスタ リカバリ システム	通常、デフォルトの管理者アプリケーション ユーザはこれらの Web アプリケーションにアクセスできません。これらの Web アプリケーションには、Cisco Unified IM and Presence オペレーティング システムの管理者のみがアクセスできます。 この管理者は、これらの Web アプリケーションに加え、管理 CLI にアクセスできます。 これらのアプリケーションに対して SSO が有効になった後は、デフォルトの管理者アプリケーション ユーザと同じ権限があるエンド ユーザがアプリケーションにアクセスできます。
リアルタイム監視ツール	SSO を有効にする前に、リアルタイム監視ツールへの管理アクセスを許可するために必要なユーザ グループのメンバーであるエンド ユーザが存在することを確認します。 上記の Cisco Unified CM IM and Presence の管理の注記を参照してください。

GUI を使用した シングル サインオンの有効化

この Cisco Unified IM and Presence オペレーティング システムの管理アプリケーションは、3 個のコンポーネントに分割されます。

- ステータス
- サーバの設定
- アプリケーションの選択

ステータス

SSO 設定の変更によって、Tomcat が再起動することを示す警告メッセージが表示されます。

SSO アプリケーションを有効にすると、次のエラー メッセージが表示されることがあります。

- 無効な Open Access Manager（OpenAM）サーバの URL（Invalid Open Access Manager (OpenAM) server URL）：無効な OpenAM サーバ URL を入力すると、このエラー メッセージが表示されます。
- 無効なプロファイル クレデンシャル（Invalid profile credentials）：間違ったプロファイル名または間違ったプロファイル パスワードあるいは両方を入力すると、このエラー メッセージが表示されます。

- セキュリティ信頼エラー：この IM and Presence サービス ノードが OpenAM server によって提示される証明書チェーンを信頼しない場合、このエラー メッセージが表示されます。

（注） SSOを有効にするときに上記のいずれかのエラーメッセージが表示された場合は、ステータスが該当するエラーに変更します。

サーバの設定

SSOがすべてのアプリケーションで無効になっている場合にのみ、サーバの設定を編集できます。

アプリケーションの選択

次のアプリケーションのいずれかを使用して SSO を有効または無効にできます。

- Cisco Unified CM IM and Presence の管理：Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence のサービスアビリティ、および Cisco Unified IM and Presence のレポートに対して SSO を有効にします。
- Cisco Unified IM and Presence オペレーティング システムの管理：Cisco Unified IM and Presence オペレーティング システムの管理およびディザスタ リカバリ システムに対して SSO を有効にします。
- RTMT： Real-Time Monitoring Tool 用に Web アプリケーションを有効にします。
- Cisco UP Client Profile Agent：Cisco UP Client Profile Agent サービスの SSO を有効にします。このオプションは、共通アクセスカード（Common Access Card）（CAC） Sign-On を使用する顧客にのみ適用されます。

手順

ステップ 1 [Cisco Unified IM and Presence Operating SystemAdministration（Cisco Unified IM and Presence オペレーティングシステムの管理）] > [Security（セキュリティー）] > [Single Sign On（シングル サインオン）] を選択します。

ステップ 2 Open Access Manager（OpenAM）サーバの URL を入力します。

例：

```
https://server1.cisco.com:8443/opensso
```

ステップ 3 ポリシー エージェントを展開する相対パスを入力します。 相対パスは、英数字（*agentapp* など）にする必要があります。

ステップ 4 このポリシーエージェント用に設定されたプロファイルの名前（たとえば「cupnode01 j2ee エージェント」）を入力します。

ステップ 5 プロファイル名のパスワードを入力します。

ステップ 6 「IMPKRB」などの、Windows デスクトップ SSO 用に設定されたログイン モジュール インスタンス名を入力します。 詳細については、SSO のモジュール例のセットアップに関するトピックを参照してください。

ステップ 7 [Save（保存）] をクリックします。

ステップ 8 [Confirmation（確認）] ダイアログボックスで、[OK（OK）] をクリックして Tomcat を再起動します。

シングル サインオンの非アクティブ化

SSO を無効にするには、ここに示す順序で次のタスクを実行します。

SSO 無効化前のアクセス権限の設定

SSO が SSO をサポートする任意のIM and Availability Web アプリケーションに対して無効になっている場合は、そのアプリケーションにアクセスするすべてのユーザにユーザ名とパスワードを提供する必要があります。 IM and Presence Service 管理者が IM and Availability Web アプリケーションに対して SSO を無効にする場合は、SSO の無効化後にユーザがアプリケーションにアクセスできることを確認します。 この操作は、アクティブな IM and Presence Service 管理アカウントを誤ってロック アウトしないようにするために重要です。

表 *8*：シングル サインオン無効化の前提条件

アプリケーション	注意

Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence の管理、IM and Presence のサービスアビリティ、IM and Presence のレポート）	SSO を無効にする前に、既知のユーザ名およびパスワードを持つアプリケーション ユーザが存在し、このユーザが必要なユーザ グループのメンバーであることを確認します。 インストール時に作成されたデフォルトの管理者アプリケーション ユーザには次が必要です。 グループ： • 標準監査ユーザ • 標準 CCM スーパー ユーザ 権限： • Standard AXL API Access • 標準 Admin Rep Tool Admin • 標準監査ログ管理 • Standard CCM Admin Users • Standard CCMADMIN Administration • 標準 CUReporting • 標準 EM 認証プロキシ権 • Standard SERVICEABILITY Administration • 標準 SSO 設定管理 SSO が無効になっている場合は、これらの役割を持つ上記のユーザ グループのメンバーであるアプリケーション ユーザは IM and Presence Service に対する完全なアクセス権限を持つことになります。 IM and Presence のアプリケーション ユーザを表示するには、[Cisco Unified CM IM and Presence Administration（Cisco Unified CM IM and Presence の管理）] > [User Management（ユーザ管理）] > [Application User（アプリケーション ユーザ）] > [Find（検索）] を選択します。 ユーザを選択して詳細を表示します。
Cisco Unified IM and Presence オペレーティング システムの管理（IM and Presence オペレーティング システムの管理、 IM and Presence DRS）	SSO を無効にする前に、既知のユーザ名およびパスワードを持つ OS 管理ユーザが存在し、このユーザに Cisco Unified IM and Presence オペレーティングシステム管理 CLI へのアクセス権があることを確認します。 SSO を無効にした後に、このユーザには Cisco Unified IM and Presence オペレーティング システム管理 GUI へのアクセス権があります。

リアルタイム監視ツール	SSO を無効にする前に、既知のユーザ名およびパスワードを持つアプリケーション ユーザが存在しており、このユーザに Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence の管理、IM and Presence のサービスアビリティ、および IM and Presence のレポート）に指定されたユーザと同じアクセス権があることを確認します。

シングル サイン オンの無効化

この手順で説明されているように、GUI または CLI を使用して SSO を無効にできます。 CLI を使用して SSO を無効にする方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』の utils sso disable コマンドを参照してください。

手順

ステップ 1 [Cisco Unified OS Administration（Cisco Unified OS の管理）] > [Security（セキュリティ）] > [Single Sign On（シングル サインオン）] を選択します。

ステップ 2 前に SSO 用に有効にしたすべてのアプリケーションを選択解除します。

ステップ 3 [Save（保存）] をクリックします。

ステップ 4 [Confirmation（確認）] ダイアログボックスで、[OK（OK）] をクリックして Tomcat を再起動します。

Windows での OpenAM のアンインストール

はじめる前に

OpenAM をアンインストールする前に、次の作業が完了していることを確認します。

- SSO を無効にする前に、アクセス権限を設定します。
- シングル サイン オンの無効化

手順

ステップ 1 OpenAM サーバの Windows デスクトップにアクセスし、[Start（開始）] > [All Program（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7] > [Configure Tomcat（Tomcat の設定）] を選択します。

（注） このメニュー パスは Tomcat 7. を使用していることを前提としています。

ステップ 2 OpenAM サーバ上で Tomcat サービスが動作している場合は、[General（全般）] タブで [Stop（停止）] をクリックし、サービスを停止します。

ステップ 3 OpenAM 設定データを削除します。 このデータは通常、Tomcat インスタンスを実行しているユーザのホームディレクトリにある 2 つのディレクトリに保存されています。 たとえば、`C:\opensso`（フォルダ名が、`opensso` などの OpenAM WAR ファイルの展開済みの URI と一致する場合）や、`C:\.openssocfg` などです。

ステップ 4 OpenAM/Tomcat インスタンスの `tomcat-dir\webapps` から、展開済みの OpenAM WAR ファイルと WAR ファイル自体を削除します。

例：
```
C:\Program Files\Apache Software Foundation\Tomcat 7\webapps
```
ヒント Tomcat ディレクトリ変数の説明については、Tomcat のインストールに関するトピックを参照してください。

ステップ 5 OpenAM サーバの Windows デスクトップにアクセスし、[Start（開始）] > [All Program（すべてのプログラム）] > [Apache Tomcat 7.0 Tomcat7] > [Configure Tomcat（Tomcat の設定）] を選択します。

ステップ 6 [General（全般）] タブで、[Start（開始）] をクリックして Tomcat サービスを起動します。

関連トピック

SSO 無効化前のアクセス権限の設定, （37 ページ）
シングル サイン オンの無効化, （39 ページ）
Tomcat のインストール, （17 ページ）

デバッグ レベルの設定

J2EE Policy Agent のログ レベルの設定に従い、IM and Presence サービス ノードの追加デバッグ情報を収集できます。 このコンポーネントのログ レベルは OpenAM サーバで設定されます。 デフォルトのログ レベルはエラーです。 追加デバッグ情報を提供するためにログ レベルをメッセージ（Message）に変更できます。 関連ログ ファイルが非常に大きくなる場合があるので、短期間だけメッセージ ログ レベルを使用することを推奨します。

手順

ステップ 1 Web ブラウザ（たとえば、Mozilla Firefox）から OpenAM（`https://<OpenAM FQDN>:8443/opensso`）にサインインします。

ステップ 2 [Access Control（アクセス コントロール）] メニューから、[Top Level Realm（トップ レベルのレルム）] > [Agents（エージェント）] > [J2EE] を選択します。

ステップ 3 [General（全般）] 見出しの下で、[Agent Debug Level（エージェントのデバッグ レベル）] を選択します。

ステップ 4 [Agent Debug Level（エージェントのデバッグ レベル）] を下で、目的のレベルを指定します（メッセージまたはエラー）。

ステップ 5 [Save（保存）] をクリックします。

ステップ 6 IM and Presence サービス ノードで Cisco Tomcat サービスを再起動します。

a) IM and Presence の管理 CLI にアクセスします。

b) 次のコマンドを実行します。**utils service restart Cisco Tomcat**

ステップ 7 SSO コンポーネントのログを参照およびダウンロードしてから、IM and Presence サービスのCisco Unified Real Time Monitoring Tool を使用してログを取得します。

（注） SSO が有効になっているときに問題が発生する場合は、SSO を無効にして、Cisco Unified Real Time Monitoring Tool から debug.out logs にアクセスするために SSO を再び有効にする必要があります。