CHAPTER 39

シングル サインオン

シングル サインオン機能を使用すると、エンド ユーザは Windows ドメインの Windows クライアント マシンにログインし、再度サインオンすることなく特定の Cisco Unified Communications Manager アプリケーションを使用できます。

シングル サインオン機能の詳細については、シスコのホワイト ペーパー「*A complete guide for installation, configuration and integration of CUCM8.5 with Open Access Manager and Active Directory for SSO*」を参照してください。

この章では、Cisco Unified Communications Manager のシングル サインオン機能について説明します。この章では、次のトピックについて取り上げます。

シングル サインオンの設定チェックリスト

シングル サインオン機能を使用すると、エンド ユーザは Windows クライアント マシンにログインし、再度サインオンすることなく特定の Cisco Unified Communications Manager アプリケーションを使用できます。

表 39-1 は、ネットワークで シングル サインオンを設定するためのチェックリストです。表 39-1 と「関連項目」（P.39-10）を併せて参照してください。

Cisco Unified Communication Interface for Microsoft Office Communicator でのシングル サインオンの設定については、Cisco Unified Communication Interface for Microsoft Office Communicator のマニュアルを参照してください。

表 39-1　シングル サインオンの設定チェックリスト

設定ステップ		関連項目と資料
ステップ 1	ご使用の環境が、「シングル サインオンのシステム要件」（P.39-3）で説明する要件を満たしていることを確認します。	
ステップ 2	Active Directory で OpenAM サーバをプロビジョニングし、keytab ファイルを生成します。 **（注）** ご使用の Windows バージョンに keytab ファイルを生成するための ktpass ツールが含まれていない場合は、そのツールを別途入手する必要があります。	Microsoft Active Directory のマニュアル
ステップ 3	OpenAM サーバ証明書を Cisco Unified Communications Manager tomcat 信頼ストアにインポートします。 **（注）** SSO を有効にする場合、OpenAM サーバ証明書をインポートしない場合、Web アプリケーションにアクセスできません。	「Cisco Unified Communications Manager への OpenAM 証明書のインポート」（P.39-4）
ステップ 4	Active Directory および OpenAM に Windows シングル サインオンを設定します。	「Active Directory および OpenAM への Windows シングル サインオンの設定」（P.39-4）
ステップ 5	（Cisco Unified Administration のみ） ユーザが Active Directory でプロビジョニングされることを確認します。	Microsoft Active Directory マニュアル。『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「**End User Configuration**」の項も参照してください。
ステップ 6	（Cisco Unified Administration のみ） DirSync サービスを使用して、ユーザ データを Cisco Unified Communications Manager データベースと同期化します。	『*Cisco Unified Communications Manager システム ガイド*』の「**DirSync Service**」の項。
ステップ 7	（Cisco Unified Administration のみ） ユーザを CCM Super Users グループに追加して、Cisco Unified Administration へのアクセスを有効にします。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「**Adding Users to a User Group**」の項。
ステップ 8	シングル サインオンに対応するようにクライアントのブラウザを設定します。	「シングル サインオンに対応するためのクライアントのブラウザの設定」（P.39-5）
ステップ 9	Cisco Unified Communications Manager でシングル サインオンを有効にします。	「シングル サインオン用の CLI コマンドの実行」（P.39-7）

Cisco Unified Communications Manager用のシングル サインオンの概要

シングル サインオン機能を使用すると、エンド ユーザは Windows にログインし、再度サインオンすることなく次の Cisco Unified Communications Manager アプリケーションを使用できます。

- ユーザ オプション
- Cisco Unified Communications Manager の管理
- Real-Time Monitoring Tool（RTMT; リアルタイム監視ツール）の管理
- Cisco Unified Communication Interface for Microsoft Office Communicator

シングル サインオンのシステム要件

Cisco Unified Communications Manager には、次のシングル サインオン システム要件があります。

- クラスタ内の各サーバの Cisco Unified Communications Manager リリース 8.5(1)。

この機能には、次のサードパーティ アプリケーションが必要です。

- Microsoft Windows Server 2003 または Microsoft Windows Server 2008
- Microsoft Active Directory
- ForgeRock Open Access Manager（OpenAM）バージョン 9.0

シングル サインオン機能は、Active Directory および OpenAM を併用して、クライアント アプリケーションへのシングル サインオン 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構成に配置する必要があります。
- 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 サーバが OpenAM サーバに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、Cisco Unified Communications Manager、および OpenAM は、同じドメインに存在する必要があります。
- ドメインで DNS を有効にする必要があります。
- Cisco Unified Communications Manager サーバには、サード パーティ製品をインストールしません。
- SSO に参加するすべてのエンティティのクロックを同期する必要があります。

サード パーティ製品の詳細については、それぞれのマニュアルを参照してください。

シングル サインオンのインストールとアクティブ化

Cisco Unified Communications Manager 8.6(1) のインストール後、必要な設定作業を実行すると、ネットワークでシングル サインオンをサポートできます。実行する必要がある設定作業については、「シングル サインオンの設定チェックリスト」（P.39-1）を参照してください。

シングル サインオンの設定

この項では、次のトピックについて取り上げます。

ヒント　シングル サインオンを設定する前に、「シングル サインオンの設定チェックリスト」（P.39-1）を参照してください。

OpenAM の設定

OpenAM を使用して、次のタスクを実行します。

- OpenAM に次のものに関するポリシーを設定します。
  - CUCM ユーザおよび UDS Web アプリケーション
  - クエリー パラメータ
- Policy Agent 3.0 用の J2EE Agent Profile を設定します。
- Windows Desktop SSO ログイン モジュール インスタンスを設定します。
- PA 用の「Login Form URI」および「OpenAM Login URL」を設定します。
- ローカル ユーザ プロファイルを無効にします。

Cisco Unified Communications Manager への OpenAM 証明書のインポート

Cisco Unified Communications Manager と OpenAM 間の通信がセキュアであるため、OpenAM セキュリティ証明書を入手して Cisco Unified Communications Manager tomcat 信頼ストアにインポートする必要があります。5 年間有効になるように OpenAM 証明書を設定します。

証明書のインポートについては、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

Active Directory および OpenAM への Windows シングル サインオンの設定

この項では、Active Directory および OpenAM に Windows シングル サインオンを設定する方法について説明します。この手順に従うと、Cisco Unified Communications Manager を Active Directory で認証できます。

手順

ステップ 1　Active Directory で、OpenAM Enterprise ホスト名（ドメイン名なし）をユーザ ID（ログイン名）として、新規にユーザを作成します。

ステップ 2　Active Directory サーバに keytab ファイルを作成します。

ステップ 3　作成した keytab ファイルを OpenAM システムにエクスポートします。

ステップ 4　OpenAM で、次の設定で新規に認証モジュールのインスタンスを作成します。

- タイプは、Windows Desktop SSO です。
- レルムのアトリビュートは次のように設定します。
  - [Service Principal]：keytab ファイルを作成するときに使用したプリンシパル名を入力します。
  - [Keytab File Name]：keytab ファイルのインポート先のパスを入力します。
  - [Kerberos Realm]：ドメイン名を入力します。
  - [Kerberos Server Name]：Active Directory サーバの FQDN を入力します。
  - [Authentication level]：**22** を入力します。

シングル サインオンに対応するためのクライアントのブラウザの設定

ブラウザベースのクライアント アプリケーションでシングル サインオンを使用するには、Web ブラウザを設定する必要があります。

次の各項では、シングル サインオンを使用するようにクライアントのブラウザを設定する方法について説明します。

- 「シングル サインオンに対応するための Internet Explorer の設定」（P.39-5）
- 「シングル サインオンに対応するための Firefox の設定」（P.39-6）

シングル サインオンに対応するための Internet Explorer の設定

シングル サインオン機能は、Internet Explorer バージョン 6.0 以降を実行している Windows クライアントをサポートします。シングル サインオンを使用するように Internet Explorer を設定するには、次のタスクを実行します。

- 統合 Windows 認証オプションを選択します。
- 次のように設定したカスタムのセキュリティ レベルを作成します。
  - [ローカル イントラネット (Intranet Zone)] オプションで [イントラネット ゾーンでのみ自動的にログオンする (Automatic Logon Only)] を選択します。
  - サイトに関するオプションをすべて選択します。
  - OpenAM をローカル ゾーンにまだ追加していない場合は追加します。
- Windows 7 で Internet Explorer 8.0 を実行している場合には、次のタスクを実行します。
  - 保護モードを無効にします。
  - レジストリ キー HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥LSA¥ で、DWORD 値として SuppressExtendedProtection - 0x02 を追加します。

シングル サインオンに対応するための Firefox の設定

シングル サインオン機能は、Firefox バージョン 3.0 以降を実行している Windows クライアントをサポートします。

シングル サインオンを使用するように Firefox を設定するには、ブラウザと SPNEGO 認証の連動を許可する信頼できるドメインと URL を network.negotiate-auth.trusted-uris プリファレンスに入力します。

SSO アプリケーションの設定

SSO を設定するには、[Cisco Unified OS Administration] > [セキュリティ (Security)] > [シングルサインオン (Single Sign On)] をクリックします。

このアプリケーションは、次の 3 つのコンポーネントに分割されます。

- [ステータス (Status)]
- [アプリケーションの選択 (Select Applications)]
- [サーバの設定 (Server Settings)]

[ステータス (Status)]

SSO 設定の変更により Tomcat が再起動され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場合、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 Manger(Open AM) サーバ URL(Invalid Open Access Manger (Open AM) server URL)] : このエラー メッセージは、無効な OpenAM サーバ URL を提供した場合に表示されます。
- [無効なプロファイル証明書 (Invalid profile credentials)] : このエラー メッセージは、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、あるいはこれらの両方を提供した場合に表示されます。
- [セキュリティトラストエラー (Security trust error)] : このエラー メッセージは、OpenAM 証明書がインポートされていない場合に表示されます。

SSO を有効にした状態で上記のいずれかのメッセージが表示される場合、ステータスが上記のエラーに変わります。

[アプリケーションの選択 (Select Applications)]

特定のアプリケーションの SSO を有効または無効にするアプリケーションを選択または選択解除します。

次のアプリケーションを使用できます。

- Cisco Unified CM Administration : Cisco Unified CM Administration、Cisco Unified Serviceability、および Cisco Unified Reporting の SSO を有効にします。
- Cisco Unified CM User Options : Cisco Unified CM ユーザ オプションの SSO を有効にします。
- Cisco Unified Operating System Administration : Cisco Unified Operating System Administration およびディザスタ リカバリ システムの SSO を有効にします。
- Cisco Unified Data Service : Cisco UC Integration for Microsoft Office Communicator の SSO を有効にします。
- RTMT : Real-Time Monitoring Tool の Web アプリケーションを有効にします。

[サーバの設定(Server Settings)]

サーバ設定は、すべてのアプリケーションで SSO が無効な場合のみ編集できます。

次の手順を実行します。

手順

ステップ 1　Open Access Manager（OpenAM）サーバの次の URL を入力します。
http://opensso.sample.com:443/opensso

ステップ 2　Policy Agent の配置先となる相対パスを入力します。相対パスは、英数字で入力する必要があります。

ステップ 3　このポリシー エージェントに設定されているプロファイルの名前を入力します。

ステップ 4　プロファイル名のパスワードを入力します。

ステップ 5　Windows Desktop SSO に設定されるログイン モジュール インスタンス名を入力します。

ステップ 6　[保存(Save)] をクリックします。

ステップ 7　確認ダイアログボックスの [OK] をクリックして、Tomcat を再起動します。

シングル サインオン用の CLI コマンドの実行

次の各項では、シングル サインオンを設定する CLI コマンドについて説明します。

- 「utils sso enable」（P.39-7）
- 「utils sso disable」（P.39-9）
- 「utils sso status」（P.39-9）

utils sso enable

utils sso enable コマンドを使用すると、SSO ベースの認証を有効および設定、SSO を無効、または SSO ベースの認証のステータスおよび設定パラメータを表示できます。

注意　シングル サインオンを有効または無効にすると、Cisco Unified Communications Manager Web サーバ（Tomcat）が再起動します。

コマンド構文

utils sso enable

パラメータ

- enable：SSO ベースの認証を有効にします。このコマンドは、シングル サインオン設定ウィザードを起動します。

次の表に、SSO を有効にするときに表示されるプロンプトの情報を示します。

パラメータ	説明
1. Cisco Unified CM Administration（Cisco Unified Administration、Cisco Unified Serviceability、Cisco Unified Reporting） **2.** Cisco Unified CM ユーザ オプション **3.** Cisco Unified Operating System Administration（Cisco Unified OS Administration、ディザスタ リカバリ システム） **4.** Cisco Unified Data Service（CUCiMOC） **5.** RTMT	Cisco Unified Administration、Cisco Unified Serviceability、Cisco Unified Reporting などの Unified CM Administration Web アプリケーションを有効にします。 Cisco Unified Communications Manager ユーザ オプション ページを有効にします。 Cisco Unified CM OS Administration、ディザスタ リカバリ システムで Cisco Unified Operating System Administration を有効にします。 Cisco UC Integration for Microsoft Office Communicator で Cisco Unified Data Service Web アプリケーションを有効にします。 Cisco Unified Real-Time Monitoring Tool を有効にします。 CLI により、示されている各 Web アプリケーションで SSO を有効にするよう応答を求めるプロンプトが表示されます。各 Web アプリケーションで、yes または no の値を入力し、SSO を有効または無効にします。
サーバ URL	Open SSO サーバに設定した URL。配置 URI *http://opensso.sample.com:443/opensso* を含める必要があります。
エージェント URL	ポリシー エージェントが配置される Cisco Unified Communications Manager の相対パス。例：*http://agent1.sample.com:1234/agentapp*
プロファイル名	Open SSO のこのポリシー エージェントに作成したプロファイルの名前。
パスワード	プロファイルのパスワード。
ログイン モジュール名	Open SSO に設定した Windows Desktop SSO 用のログイン モジュール インスタンスの名前。

例

```
admin:utils sso enable
***** W A R N I N G *****
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): yes
List of apps for which SSO can be enabled
1) Cisco Unified Administration (Cisco Unified Administration, Cisco Unified
Serviceability, Cisco Unified Reporting)
2) Cisco Unified User Options
3) Cisco Unified Operating System Administration (Cisco Unified OS Administration,
Disaster Recovery System)
```

```
4) Cisco Unified Data Service (CUCiMOC)
5) RTMT
Do you want to enable SSO for Cisco Unified Administration (Cisco Unified
Administration, Cisco Unified Serviceability, Cisco Unified Reporting) (yes/no): y
Do you want to enable SSO for Cisco Unified User Options (yes/no): n
Do you want to enable SSO for Cisco Unified Operating System Administration (Cisco
Unified OS Administration, Disaster Recovery System) (yes/no): n
Do you want to enable SSO for Cisco Unified Data Service (CUCiMOC) (yes/no): y
Do you want to enable SSO for RTMT (yes/no): n

Enter URL of the Open Access Manager (OpenAM) server:
https://blr-opensso.vrajoli.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: CUCMPA220
Enter the password of the profile name: *******
Enter the login module instance name configured for Windows Desktop SSO: Universal_SSO

Validating connectivity and profile with Open Access Manager (OpenAM) Server:
https://blr-opensso.vrajoli.com:8443/opensso
Valid profile
Enabling SSO ... This will take up to 5 minutes
SSO Enable Success
Please make sure to execute this command on all the nodes in the cluster.
```

utils sso disable

このコマンドは、SSO ベースの認証を無効にします。このコマンドは、SSO が有効な Web アプリケーションをリストします。指定アプリケーションのシングル サインオンを無効にするよう求めるプロンプトが表示された場合、**Yes** と入力します。

コマンド構文

utils sso disable

使用上のガイドライン

注意　シングル サインオンを無効にすると、Cisco Unified Communications Manager Web サーバ（Tomcat）が再起動されます。

このコマンドは、クラスタ内のすべてのノードで実行する必要があります。

utils sso status

このコマンドは、シングル サインオンのステータスおよび設定パラメータを表示します。

コマンド構文

utils sso status

関連項目

- 「シングル サインオンの設定チェックリスト」（P.39-1）
- 「Cisco Unified Communications Manager 用のシングル サインオンの概要」（P.39-3）
- 「シングル サインオンのシステム要件」（P.39-3）
- 「シングル サインオンのインストールとアクティブ化」（P.39-3）
- 「シングル サインオンの設定」（P.39-4）