CHAPTER 7

Cisco Unity Connection でのシングル サインオン

Cisco Unity Connection 9.x はシングル サインオン機能をサポートしており、ユーザは 1 度ログインすれば次の Cisco Unity Connection アプリケーションに再ログインなしでアクセスできます。

- Cisco Personal Communications Assistant
- Web Inbox
- Cisco Unity Connection の管理
- Cisco Unity Connection Serviceability
- Cisco Unity ConnectionREST API

（注） Cisco Unity Connection 9.1(1) では、シングル サインオン機能が VmRest API をサポートしています。

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 the installation, configuration and integration of Open Access Manager 9.0 with CUCM 8.5, 8.6 /CUC 8.6 and Active Directory for SSO*』を参照してください。このガイドは、https://supportforums.cisco.com/docs/DOC-14462 から入手可能です。

次の項を参照してください。

- 「シングル サインオンの設定チェックリスト」（P.7-1）
- 「シングル サインオンのシステム要件」（P.7-2）
- 「シングル サインオンの設定」（P.7-3）

シングル サインオンの設定チェックリスト

この項では、ネットワーク内のシングル サインオン機能を設定するためのチェックリストを示します。

表 7-1　シングル サインオン設定チェックリスト

設定手順		関連項目およびマニュアル
ステップ 1	使用環境が「シングル サインオンのシステム要件」（P.7-2）で説明されてい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 の 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）　使用している Windows のバージョンに 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、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	Cisco Unity Connection の OpenAM サーバを設定します。	「OpenAM サーバの設定」（P.7-3）
ステップ 4	OpenAM のサーバ証明書を Cisco Unified Communications Manager tomcat 信頼ストアにインポートします。	https://supportforums.cisco.com/docs/DOC-14462
ステップ 5	Active Directory および OpenAM を使用して Windows シングル サインオンを設定します。	https://supportforums.cisco.com/docs/DOC-14462
ステップ 6	シングル サインオンのクライアント ブラウザを設定します。	https://supportforums.cisco.com/docs/DOC-14462
ステップ 7	Cisco Unified Communications Manager のシングル サインオンをイネーブルにします。	「シングル サインオンの CLI コマンドの実行」（P.7-4）

シングル サインオンのシステム要件

Cisco Unity Connection のシングル サインオンのシステム要件を次に示します。

- クラスタ内の各サーバで Cisco Unity Connection リリース 9.x。

この機能は、シングル サインオン機能を設定するために次のサードパーティ製アプリケーションが必要です。

- Active Directory を導入するための Microsoft Windows Server 2003 SP1/SP2 または Microsoft Windows Server 2008 SP2。
- Microsoft Active Directory サーバ（任意のバージョン）。
- ForgeRock Open Access Manager（OpenAM）バージョン 9.0。
- Apache Tomcat 7.0.0

シングル サインオン機能は、Active Directory および OpenAM を同時に使用し、クライアント アプリケーションにシングル サインオン アクセスを提供します。

シングル サインオン機能に必要なサードパーティ製アプリケーションは、次の設定要件を満たしている必要があります。

- Active Directory は、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される必要があります。
- OpenAM サーバは、ネットワーク上において Connection サーバ、すべてのクライアント システム、および Active Directory サーバから名前でアクセスできなければなりません。
- OpenAM サーバは、Microsoft Windows 2003 サーバまたは RedHat Enterprise Linux（RHEL）サーバにインストールできます。
- Active Directory（ドメイン コントローラ）サーバ、Windows クライアント、Cisco Unity Connection、および OpenAM 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。
- シングル サインオン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。

シングル サインオンの設定

シングル サインオンのための Connection および OpenAM サーバの設定手順の詳細については、シスコのホワイト ペーパー『*A complete guide for the installation, configuration and integration of Open Access Manager 9.0 with CUCM 8.5, 8.6 /CUC 8.6 and Active Directory for SSO*』を参照してください。このガイドは、https://supportforums.cisco.com/docs/DOC-14462 から入手可能です。

この項では、Connection 固有の設定に従う必要がある重要なステップや手順について説明します。しかし、シングル サインオンの設定を初めて行う場合は、シスコのホワイト ペーパーに記載されている詳細な手順に従うことを強く推奨します。

- 「OpenAM サーバの設定」（P.7-3）
- 「シングル サインオンの CLI コマンドの実行」（P.7-4）

OpenAM サーバの設定

OpenAM サーバを設定するには、次の手順を実行する必要があります。

OpenAM サーバ上のポリシーを設定するには、OpenAM にログインして [アクセス コントロール（Access Control）] タブを選択する必要があります。[トップ レベル レルム（Top Level Realm）] オプションをクリックし、[ポリシー（Policies）] タブを選択して新しいポリシーを作成します。新しいポリシーを作成するには、シスコ ホワイト ペーパー（https://supportforums.cisco.com/docs/DOC-14462）に記載されている手順に従います。また、ホワイト ペーパーの手順に従うと同時に、次のような Connection 固有の情報を持つポリシーを作成してください。

- ポリシーにルールを追加するときは、次の点を確認してください。
  - 各ルールは、URL ポリシー エージェント サービスのタイプである必要があります
  - 各ルールの GET および POST チェックボックスをオンにします
  - 次の各リソースに対してルールを作成します。「fqdn」は Connection サーバの完全修飾ドメイン名を示します。

    https://<fqdn>:8443/*
    https://<fqdn>:8443/*?*
    https://<fqdn>/*
    https://<fqdn>/*?*
    http://<fqdn>/*
    http://<fqdn>/*?*
- ポリシーにサブジェクトを追加するときは、次の点を確認してください。
  - [件名のタイプ（Subject Type）] フィールドが Authenticated Users であることを確認してください。
  - サブジェクト名を指定します

  - [排他的（Exclusive）] チェックボックスはオンにしないでください。
- ポリシーに条件を追加するときは、次の点を確認してください。
  - [条件（Condition）] のタイプを Active Session Time とします
  - 条件名を指定します
  - アクティブ セッション タイムアウトを 120 分に設定し、[セッション終了（Terminate Session）] オプションで [いいえ（No）] を選択します。

ステップ 2：Windows Desktop SSO ログイン モジュール インスタンスの設定

シスコ ホワイト ペーパー（ https://supportforums.cisco.com/docs/DOC-14462）の指示に従って、Windows デスクトップを設定します。

ステップ 3：Policy Agent 3.0 の J2EE Agent Profile の設定

シスコ ホワイト ペーパー（https://supportforums.cisco.com/docs/DOC-14462）の指示に従って、続く部分に示す Connection 固有の設定で新しい J2EE エージェントを作成します。

- エージェントのプロファイル名として示される名前は、Connection サーバ上で SSO がイネーブルである場合や、「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（Enter the name of the profile configured for this policy agent）」というメッセージが表示された場合に入力する必要があります。
- ここで入力されるエージェント パスワードは、Connection サーバ上で「プロファイル名のパスワードを入力（Enter the password of the profile name）」というメッセージが表示された場合にも入力する必要があります。
- [アプリケーション（Application）] タブ上の [ログイン フォーム URI（Login Form URI）] セクションに次の URI を追加します。
  - /cuadmin/WEB-INF/pages/logon.jsp
  - /cuservice/WEB-INF/pages/logon.jsp
  - /ciscopca/WEB-INF/pages/logon.jsp
  - /inbox/WEB-INF/pages/logon.jsp
  - /ccmservice/WEB-INF/pages/logon.jsp
  - /vmrest/WEB-INF/pages/logon.jsp
- [アプリケーション（Application）] タブの下の [URI 処理を強制しない（Not Enforced URI Processing）] セクションに、次の URI を追加します。
  - /inbox/gadgets/msg/msg-gadget.xml

上記の Connection 固有の設定の他に、次の点を確認してください。

- LDAP から Connection にユーザをインポートします。ユーザが Cisco Unity Connection Administration、または Cisco Unity Connection Serviceability にログインするには、適切な役割を設定されている必要があります。
- シスコ ホワイト ペーパー（https://supportforums.cisco.com/docs/DOC-14462）の 8.6 項「Configuring SSO on Cisco Unified Communications Manager」に従って、OpenAM 証明書を Connection にアップロードします。

シングル サインオンの 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
- utils sso disable
- utils sso status

詳細については、シスコのホワイト ペーパー（https://supportforums.cisco.com/docs/DOC-14462）を参照してください。

- **utils sso enable**

utils sso コマンドは、SSO-based 認証のイネーブル化と設定に使用します。クラスタ内のすべてのノード上でこのコマンドを実行してください。

注意　Cisco Unity Connection へのシングル サインオンをイネーブルまたはディセーブルにすると、Web サーバ（Tomcat）が再起動します。

コマンドの構文

utils sso enable

パラメータ

enable：SSO-based 認証をイネーブルにします。このコマンドにより、シングル サインオン設定ウィザードが開始されます。

- **utils sso disable**

このコマンドは、SSO-based 認証をディセーブルにします。また、SSO がイネーブルになっている Web アプリケーションをリスト表示します。指定されたアプリケーションのシングル サインオンをディセーブルにするよう求められた場合は、「Yes」と入力します。クラスタ内のすべてのノード上でこのコマンドを実行する必要があります。

コマンドの構文

utils sso disable

- **utils sso status**

このコマンドにより、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が表示されます。

コマンドの構文

utils sso status