CHAPTER 7

Single Sign-On in Cisco Unity Connection 8.6 and Later

Revised August 2, 2011

Cisco Unity Connection 8.6 and later versions support the single sign-on feature that allows end users to log in once and gain access to use the following Cisco Unity Connection applications without signing on again:

- Cisco Personal Communications Assistant
- Web Inbox
- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability

For more information about the single sign-on feature, see the Cisco white paper, *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* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

See the following sections:

- Configuration Checklist for Single Sign-On, page 7-37
- System Requirements for Single Sign-On, page 7-38
- Configuring Single Sign-On, page 7-39

Configuration Checklist for Single Sign-On

This section provides a checklist for configuring the single sign-on feature in the network.

Table 7-1 Single Sign-On Configuration Checklist

Configuration Steps		Related Topics and Documentation
Step 1	Ensure that your environment meets the requirements described in the System Requirements for Single Sign-On, page 7-38	—
Step 2	Provision the OpenAM server in Active Directory, and then generate keytab files. **Note** If your Windows version does not include the ktpass tool for generating keytab files, then you must obtain it separately.	Microsoft Active Directory documentation
Step 3	Configure the OpenAM server for Cisco Unity Connection.	Configuring OpenAM Server, page 7-39
Step 4	Import the OpenAM server certificate into the Cisco Unified Communications Manager tomcat-trust store.	http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf
Step 5	Configure Windows single sign-on with Active Directory and OpenAM.	http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf
Step 6	Configure client browsers for single sign-on.	http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf
Step 7	Enable single sign-on in Cisco Unified Communications Manager.	Running CLI Commands for Single Sign-On, page 7-40

System Requirements for Single Sign-On

The following single sign-on system requirements exist for Cisco Unity Connection:

- Cisco Unity Connection release 8.6(1) or higher on each server in a cluster.

The feature requires the following third-party applications for configuring the single sign-on feature:

- Microsoft Windows Server 2003 with SP1/SP2 or Microsoft Windows Server 2008 with SP2 for deploying Active Directory
- Microsoft Active Directory server (any version)
- ForgeRock Open Access Manager (OpenAM) version 9.0
- Apache Tomcat 7.0.0

The single sign-on feature uses Active Directory and OpenAM simultaneously to provide single sign-on access to client applications.

The third-party applications required for the single sign-on feature must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible by name on the network to Connection server, all client systems, and the Active Directory server.
- The OpenAM server can be installed on Microsoft Windows 2003 server or RedHat Enterprise Linux (RHEL) server.

- The Active Directory (Domain Controller) server, Windows clients, Cisco Unity Connection, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- The clocks of all the entities participating in single sign-on must be synchronized.

See the third-party product documentation for more information about those products.

Configuring Single Sign-On

The complete set of instructions to configure Connection and OpenAM server for single sign-on are given in the Cisco white paper, *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* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf. This section outlines the key steps and/or instructions that must be followed for Connection-specific configuration. However, if you are configuring single sign-on for the first time, it is strongly recommended to follow the detailed instructions given in the Cisco white paper.

- Configuring OpenAM Server, page 7-39
- Running CLI Commands for Single Sign-On, page 7-40

Configuring OpenAM Server

To configure OpenAM server, you must perform the following steps:

Step 1: Configure Policies on OpenAM Server

To configure policies on OpenAM server, you must log in to OpenAM and select the Access Control tab. Click the Top Level Realm option, select the Policies tab, and then create a new policy. Follow the steps as given in the Cisco white paper, http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf, for creating a new policy. While following the instructions given in the white paper, make sure to create policies with the below mentioned Connection-specific information:

- Ensure the following points while adding rules to the policy:
  - Each rule should be of the URL Policy Agent service type
  - Make sure to check the GET and POST checkbox for each rule
  - Create a rule for each of the following resources, where 'fqdn' is the fully qualified domain name of your Connection server:

    https://<fqdn>:8443/*

    https://<fqdn>:8443/*?*

    https://<fqdn>/*

    https://<fqdn>/*?*

    http://<fqdn>/*

    http://<fqdn>/*?*
- Ensure the following points while adding a subject to the policy:
  - Make sure that the Subject Type field is Authenticated Users.
  - Specify a subject name

  - Do not check the Exclusive check box.
- Ensure the following points while adding a condition to the policy:
  - Mention the Condition type as Active Session Time
  - Specify a condition name
  - Configure active session timeout as 120 minutes and select 'No' for the Terminate Session option.

Step 2: Configure a Windows Desktop SSO login module instance

Follow the instructions for configuring Windows Desktop as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462.

Step 3: Configure a J2EE Agent Profile for Policy Agent 3.0

Follow the instructions to create a new J2EE agent as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462 with the below mentioned Connection-specific settings:

- The name mentioned as agent profile name is the name that you need to enter when enabling SSO on the Connection server, when it prompts as "Enter the name of the profile configured for this policy agent".
- The agent password entered here is the password that is entered on the Connection server when it prompts as "Enter the password of the profile name".
- Make sure to add the following URIs to the Login Form URI section on the Application tab:
  - /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
- Under the Application tab, add the following URI in the Not Enforced URI Processing session:
  - /inbox/gadgets/msg/msg-gadget.xml

In addition to above Connection-specific configuration, ensure the following points:

- Import users from LDAP to Connection. Users must be configured with the appropriate roles to log in to Cisco Unity Connection Administration, or Cisco Unity Connection Serviceability.
- Upload the OpenAM certificate into Connection as described in the Configuring SSO on Cisco Unified Communications Manager 8.6 section of the Cisco white paper, http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

Running CLI Commands for Single Sign-On

The following sections describe the CLI commands that configure single sign-on:

- utils sso enable
- utils sso disable
- utils sso status

For more information, see the Cisco white paper, .

- **utils sso enable**

The utils sso command enables and configures SSO-based authentication. Make sure to run the command on every node in the cluster.

Caution When you enable or disable single sign-on the Cisco Unity Connection, web server (Tomcat) restarts.

Command syntax

utils sso enable

Parameters

enable -Enables SSO-based authentication. This command starts the single sign-on configuration wizard.

- **utils sso disable**

This command disables SSO-based authentication. This command lists the web applications for which SSO is enabled. Enter Yes when prompted to disable single sign-on for the specified application. You must run this command on all nodes in a cluster.

Command syntax

utils sso disable

- **utils sso status**

This command displays the status and configuration parameters of single sign-on.

Command Syntax

utils sso status