Identity Management

User Security Overview

User Access

User Security consists of the platforms which protect our users, endpoints, and their online activity to more efficiently correlate threats. As users are increasingly logging in to networks through their personal devices, securing personal devices are as important as securing company owned devices.

For more information on Users and Security, see **Configure End Users** in System Configuration Guide for Cisco Unified Communications Manager and **Manage Security** in Administration Guide for Cisco Unified Communications Manager.

Assign end users to Access Control Groups associated to Roles to manage User Access in Unified Communications Manager.

Access Control essentially allows the right people to access your network while simultaneously blocking those people who shouldn't be. Access Control refers to the visibility of who and what is accessing your network. It ensures that the right people are using the right devices, to access the right resources. Access Control regulates the spread of information and prevents unwanted visitors gaining access to your data.

Roles and Access Control Groups provide multiple levels of security to Unified Communications Manager. Each role defines a set of permissions for a specific resource within Unified Communications Manager. End Users get access permissions defined by the role when you assign roles and then assign end users to an access control group.

Upon installation, Unified Communications Manager comes with predefined default roles assigned to predefined default access control groups. You can assign end users to the default access control groups, or you can customize access settings by setting up new access control groups and roles.

For more information on Users and Access Control, see **Configure End Users** in System Configuration Guide for Cisco Unified Communications Manager and **Manage Users** in Administration Guide for Cisco Unified Communications Manager.

Identity Management

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications after signing into one of those applications. SAML describes the exchange of security-related information between trusted business partners. It's an authentication protocol used by service providers (such as Cisco Unified Communications Manager) to authenticate a user. With SAML, an identity provider and a service provider exchanges security authentication information. This feature provides secure mechanisms to use common credentials and relevant information across various applications. For more information on Identity management, see Manage SAML Single Sign-On in Administration Guide for Cisco Unified Communications Manager.

Contact Search Authentication

Contact Search Authentication requires you to authenticate yourselves before searching the directory for other users. Navigate to the following topics for more information on Contact Search Authentication.

1. Confirm Phone Support for Contact Search Authentication
2. Enable Contact Search Authentication
3. Configure Secure Directory Server for Contact Search

Identity Management Overview

Identity Management is an essential component of your Cisco Collaboration deployment. Because Identity is often the main target for hackers, it’s essential to configure secure authentication and authorization services in order to secure your system. Cisco Unified Communications Manager provides a number of options for managing identity, authentication and authorization for services.

- SAML SSO Deployment with Third-Party Identity Provider
- LDAP authentication
- Local DB Authentication

SAML SSO Deployment

SAML SSO improves your enterprise security, while improving productivity at the same time. Using the SAML 2.0 protocol, SAML SSO connects your Cisco Collaboration infrastructure to a third-party Identity Provider for secure login and authentication services for administrator and client logins across domains and across products. Worker productivity is improved as the Identity Provider stores a single login—once you login successfully to one of your Collaboration applications, you can access any of them without having to login again.

SAML SSO provides the following benefits to your Identity Framework:

- Reduces password fatigue by removing the need for entering different user name and password combinations.
- Transfers the authentication from your system that hosts the applications to a third party system.
- Protects and secures authentication information. SAML SSO provides encryption functions to protect authentication information passed between the IdP, service provider, and user. SAML SSO can also hide authentication messages passed between the IdP and the service provider from any external user.

- Improves productivity because you spend less time re-entering credentials for the same identity.
- Reduces costs as fewer help desk calls are made for password reset, thereby leading to more savings.

Trust Relationship with IdP

SAML SSO Deployments rely on the creation of a trust relationship between a Service Provider (Cisco Unified Communications Manager) and the third-party Identity Provider. You can configure a SAML SSO relationships using one of two SSO modes:

- Per Node agreement—The UC metadata zip file contains separate XML files for each node
- Per Cluster agreement—A single metadata file for the cluster

This trust relationship is created through an initial exchange of metadata files. The Cisco UC metadata file is an XML file which contains the following information:

- A unique identifier
- Organization
- Expiration time for this information
- Caching period
- XML signature of this information
- Contact persons
- Unique identifier of the entity (entity ID)
- Description of SAML role of this SAML instance (identity provider, service provider, and so forth)

Authorization

Once authentication is provided by the IdP, user access to Cisco Unified Communications Manager resources is determined by locally configured access control groups and the role permissions that those groups provide.

SAML SSO Configuration and Identity Provider Requirements

For more detailed information on SAML SSO, including configuration information and requirements for Identity Providers, see the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.

LDAP Authentication

If you have not deployed SAML SSO, and you have users synced against a company LDAP Directory, LDAP Authentication lets you authenticate user passwords against the credentials that are stored in the company LDAP directory. This option enables the Identity Management System (IMS) library on Cisco Unified Communications Manager to use the company LDAP directory to authenticate user passwords for LDAP synchronized users.

When end users login to the Self-Care Portal, they enter their company password (for example, their AD password), as configured in the company LDAP directory.

When this option is configured:

- End user passwords of users imported from LDAP are authenticated against the corporate directory by a simple bind operation.
- End user passwords for local users are authenticated against the Unified CM database.
- Application user passwords are authenticated against the Unified CM database.
- End user PINs are authenticated against the Unified CM database.

Configure LDAP Authentication

Use this procedure to enable LDAP Authentication for end user passwords. You can add LDAP Authentication to an existing LDAP Directory sync.

Before you begin

This procedure assumes you already have an existing LDAP Directory sync configured. If you have not yet configured an LDAP Directory sync, refer to the System Configuration Guide for Cisco Unified Communications Manager to set one up.

Step 1 From Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Authentication**.

Step 2 Check the **Use LDAP Authentication for End Users** check box.

Step 3 For the **LDAP Manager Distinguished Name**, enter the user ID of the LDAP Manager who is an administrative user that has access rights to the LDAP directory in question.

Step 4 Enter the **Password** and **Confirm the Password**.

Step 5 Enter the LDAP Directory server address information.

Step 6 Complete the remaining fields in the **LDAP Authentication Configuration** window.

Step 7 Click **Save**.

Local Database Authentication

Local Authentication against the Cisco Unified Communications Manager database is required for end users if you are not deploying SAML SSO with a third-party Identity provider, or if you do not have LDAP Authentication configured. With this option, user passwords are stored in the local database and are managed via the End User Configuration.

For both application users and end user PINs, local database authentication is always used to manage authentication. The following table highlights the three main password types and how they are managed.

Table 1:

Password Types	Credential Management
End User Passwords	If you are not using SAML SSO or LDAP authentication, end user passwords are managed locally in the End User Configuration window for individual end users. All passwords can be updated via the End User Configuration. End users can edit their own passwords via the Self-Care Portal.

Password Types	Credential Management
End User PINs	Irrespective of whether you have SAML SSO or LDAP Authentication deployed, end user PINs are always managed in End User Configuration window of Cisco Unified CM Administration. As administrator, you can edit existing end user PINs via the End User Configuration window.
Application User Passwords	Irrespective of whether you have SAML SSO or LDAP Authentication deployed, application user passwords are stored in the local database and are managed in the Application User Configuration window of Cisco Unified CM Administration.

Note All local passwords and PINs are stored in the database in an encrypted format.

OAuth Framework

The OAuth Authorization Framework is defined by IETF under RFC 6749. The OAuth 2.0 authorization protocol lets a resource owner (for example, Cisco Unified Communications Manager) authorize a third-party application to obtain limited access to an HTTP service. With Cisco Unified Communications Manager, the OAuth framework uses access tokens to provide access and refresh tokens to provide access to resources over the life of the token. OAuth eliminates the need for web sites to ask for passwords when you are attempting to access information. With OAuth, the resource owner authorizes a client to access resources on a server.

Cisco Jabber clients use OAuth Refresh Logins to obtain access to resources from Cisco Unified Communications Manager. After an initial login, OAuth access tokens and refresh tokens provide seamless access to resources over the life of the tokens.

OAuth Refresh Logins

With OAuth Refresh Logins, short-lived access tokens let Jabber authenticate, providing access while the token is valid the life of the token (the default lifespan for an access token is 60 minutes). The longer-lived refresh tokens provide Jabber with new access tokens as the old access tokens expire. So long as the refresh token is valid (the default life is 60 days) the Jabber client can obtain new access tokens dynamically, thereby providing seamless acess, without the user having to reauthenticate.

Every time when the OAuth token reaches 75% of its lifespan, the enduser application requests for new access token and CUCM will provide new access token to authorize the end user. If the refresh token reaches 100% of its lifespan, they will need to reauthenticate before they can generate new access tokens.

Important This feature is applicable from Release 15 onwards and for Webex clients only.

Whenever Webex clients request the renewal of their access tokens, Cisco Unified Communications Manager checks whether the refresh token renewal feature has been enabled on Cisco Unified CM and Webex clients, as well as whether the refresh token's lifetime has reached 50% of its expiry time. When both the conditions are met, then the refresh tokens will be automatically renewed during the process of renewing access tokens, ensuring seamless access without the need for reauthentication.

SIP OAuth Mode

SIP OAuth Mode enhances the OAuth framework, enabling the usage of OAuth access tokens and refresh tokens for SIP lines, thereby removing the need to install LSC certificates on Jabber clients. SIP OAuth Mode allows for secure signing and media for Jabber without CAPF. Token validation is completed during SIP registration. In this mode, Jabber can perform media and signaling encryption without an LSC, and without the need to enable mixed-mode on Unified CM.

Regenerating Keys for OAuth

If you believe the keys that are used for signing and encrypting OAuth tokens have been compromised, use the following CLI commands to generate new keys. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

- `set key regen authz encryption`
- `set key regen authz signing`

Note When OAuth keys are regenerated, you must restart the Cisco XCP Authentication Service on all IM and Presence nodes for Jabber OAuth login to work.

Configure SIP OAuth Mode

For detailed procedures on how to configure SIP OAuth Mode so that you can use OAuth Refresh Logins for SIP lines, refer to the "SIP OAuth Mode" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager.*

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.