Authentication Management

User Authentication

When signing in to the user interfaces, the credentials of the user can be authenticated based on user credentials in:

- The internal system database
- An LDAP-based external authentication server
- A SAML-based identity management server

Administrator users are users that are able to sign in to the administrator interface. Presence of an administrator interface means that a system user instance exists.

Subscribers are system users that have, and are linked to, user accounts in one or more UC applications. Subscriber management supports the management of UC application user accounts that in turn may also be configured for local, LDAP or SAML authentication.

API users are system users that connect directly to Cisco Unified Communications Domain Manager 10.6(x) using the API. The system controls access to its service through HTTP basic authentication. The technique is defined in section 11.1 of RFC1945.

Credential Policies

Cisco Unified Communications Domain Manager helps secure user accounts by authenticating user sign-in credentials before allowing system access. Administrators can specify settings for, among other things, failed sign-in attempts, lockout durations, password reset questions, and so on. The number of questions in the Password Reset Question Pool must be equal to (or more than) the number set in the **Number of Questions Asked During Password Reset** field. Collectively, these rules form a credential policy, which can be applied at any hierarchy level, and determine user sign-in behavior at that specific level.

A credential policy is not mandatory at specific levels in the hierarchy. However, a default credential policy is provided at the sys.hcs level. Administrators at lower levels can copy and edit this default policy if necessary. Administrators can also save it at their own hierarchy level so that it can be applied to the associated users at that level. If the administrators at the various levels do not create a credential policy at their level, it is inherited from the closest level above them. If a Provider Administrator has defined a credential policy, but a Customer Administrator has not, the customer automatically inherits the credential policy from the Provider. A different credential policy can also be defined for each user.

For each administrator user where IP address throttling (sign-in Limiting per Source) is required, manually create and assign a credential policy. The credential policy must have IP address, and username and email throttling enabled.

The default credential policy is defined at the sys.hcs level.

Note Credential Policies are not applicable for SSO authenticated users. For LDAP Synched users, only the session timeouts are applicable.

System User

The authentication method of a system user is specified when creating a user. the following authentications methods are available Cisco Unified Communications Domain Manager 10.6(x)in:

- Standard sign-in (Cisco Unified Communications Domain Manager 10.6(x)user authentication or proxy authentication)
- LDAP (LDAP authentication)
- SSO (using a SAML-based identity management server)

Standard Users and Sign-in

When creating a system user that uses the standard authorization method, the password is stored in the internal system database. Cisco Unified Communications Domain Manager 10.6(x) uses the PBKDF2 algorithm with an SHA256 hash, a key stretching mechanism recommended by the National Institute of Standards Technology (NIST), Computer Security Resource Center (CSRC).

When signing in as a standard user, go to the URL:

```
http://{hostname}/login
```

A sign-in page theme can be applied to the sign-in page during the log in process by adding the suffix '?theme={theme_name} where {theme_name} is an available theme. For example: http://{hostname}/login/?theme=default

When signing in, the username can be entered in either of the following formats:

```
{username}@hierarchy or {email address}
```

The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

The hierarchy on the log in form is prefixed with `sys`.

For example: `johndoe@sys.VS-OPS.VS-Corp.Chicago`

LDAP Users and Sign-in

When creating a system user using the LDAP authorization method, specify the LDAP server and the LDAP username. The LDAP username corresponds to the sign-in Attribute Name specified in the LDAP network connection.

When signing in as an LDAP user, go to the URL:

```
http://{host name}/login
```

Regardless of the sign-in Attribute Name specified in the LDAP network connection, the user email address can be used to log in.

When signing in with LDAP credentials, the username is in the format:

```
{user ID}[@hierarchy]
```

Note:

- `@hierarchy` is not required when the user ID corresponds to the user's email address.
- `{user ID}` corresponds to the sign-in attribute name (for example email address, user principal name, sAMaccountName). The sign-in attribute name is configured in the Authentication attribute of the LDAP device connection associated with this hierarchy.
- The hierarchy is in dot notation and corresponds with the hierarchy to which the user belongs. The hierarchy level is the level at which the user is created.

SSO Users and Login

When creating a system user using the SSO authorization method, the SSO Identity Provider must be specified and the SSO username.

When signing in as an SSO user, go to the URL:

```
http://{host name}/sso/{SSO login URI}/login
```

For example:

```
http://host.Agency1.CustomerA.com/sso/CustomerA/Agency1/login
```

Log in using the relevant SSO identity provider credentials.