



## Credential Policy

---

Cisco Unified Communications Manager authenticates user login credentials before allowing system access. To help secure user accounts, administrators specify settings for failed logon attempts, lockout durations, password expirations, and password requirements in Cisco Unified Communications Manager Administration. These authentication rules form a credential policy.

Credential policies apply to application users and end users. Administrators assign a password policy to end users and application users and a PIN policy to end users. The Credential Policy Default Configuration lists the policy assignments for these groups.

At installation, Cisco Unified Communications Manager assigns a static Default Credential Policy to user groups. It does not provide default credentials. The Credential Policy Default Configuration window in Cisco Unified Communications Manager Administration provides options to assign new default policies and to configure new default credentials and credential requirements for users.

**Note**

---

The system does not support empty (null) credentials. If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins will fail.

---

When you add a new user to the Cisco Unified Communications Manager database, the system assigns the default policy. You can change the assigned policy and manage user authentication events with the Edit Credentials button in the user configuration window. See the [“Credential Management” section on page 21-3](#) for more information.

This chapter includes the following topics:

- [Credential Policy and Authentication, page 22-2](#)
- [Credential Caching, page 22-2](#)
- [BAT Administration, page 22-2](#)
- [JTAPI/TAPI Support, page 22-3](#)
- [Credential History, page 22-3](#)
- [Authentication Events, page 22-3](#)
- [Data Migration Assistant, page 22-4](#)
- [Credential Policy Configuration Checklist, page 22-4](#)
- [Where to Find More Information, page 22-5](#)

# Credential Policy and Authentication

The authentication function in Cisco Unified Communications Manager authenticates users, updates credential information, tracks and logs user events and errors, records credential change histories, and encodes/decodes or encrypts/decrypts user credentials for data storage.

The system always authenticates application user passwords and end user PINs against the Cisco Unified Communications Manager database. The system can authenticate end user passwords against the corporate directory or the Cisco Unified Communications Manager database.

If your system is synchronized with the corporate directory, either the authentication function in Cisco Unified Communications Manager or LDAP can authenticate the password.

- With LDAP authentication enabled, user passwords and credential policies that are configured in Cisco Unified Communications Manager Administration do not apply. These defaults get applied to users that are created with directory synchronization (DirSync service).
- When LDAP authentication is disabled, the system authenticates user credentials against the Cisco Unified Communications Manager database. With this option, administrators can assign credential policies, manage authentication events, and administer passwords. End users can change passwords and PINs at the phone user pages.

Refer to [“Understanding the Directory” section on page 20-1](#) chapter for more information about LDAP authentication.

Credential policies do not apply to OS users or CLI users. These administrators use standard password verification procedures that the OS supports. Refer to the *Cisco Unified Communications Operating System Administration Guide* for information about OS login procedures.

## Credential Caching

To improve performance, administrators can configure the enterprise parameter “Enable Caching” to True. The parameter enables Cisco Unified Communications Manager to use cached credentials for up to 2 minutes. This eliminates the need for Cisco Unified Communications Manager to perform a database lookup or invoke a stored procedure for every single login request, thereby increasing system efficiency. An associated credential policy does not get enforced until the caching duration expires.

This setting applies to all Java applications that invoke user authentication. Setting the enterprise parameter to False turns off caching, so the system does not use cached credentials for authentication. The system ignores this setting for LDAP authentication. Credential caching requires a minimal amount of additional memory per user.

## BAT Administration

The Bulk Administration Tool (BAT) allows administrators to define common credential parameters, such as passwords and PINs, for a group of users in the BAT User Template. When you first create a user template, all the users get assigned the static Default Credential Policy. Refer to the *Cisco Unified Communications Manager Bulk Administration Guide* for more information.

## JTAPI/TAPI Support

Because Cisco Unified Communications Manager Java Telephony Applications Programming Interface (JTAPI) and Telephony Applications Programming Interface (TAPI) support the credential policies that are assigned to application users, developers must create applications that react to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Applications use an API to authenticate with the database or corporate directory, regardless of the authentication model that an application uses.

Refer to the *Cisco Unified Communications Manager JTAPI Developers Guide* and the *Cisco Unified Communications Manager TAPI Developers Guide* for new error strings that support credential policy and authentication.

## Credential History

After a user is configured in the database, the system stores a history of user credentials in the database to prevent a user from entering previous credentials when the user is prompted to change credentials.

## Authentication Events

You can monitor and manage authentication activity for a user at the user Credential Configuration page, which is accessed with the **Edit Credentials** button in the user configuration windows. The system shows the most current authentication results, such as last hack attempt time, and counts for failed logon attempts.

See “[Managing End User Credential Information](#)” and “[Managing Application User Credential Information](#)” in the *Cisco Unified Communications Manager Administration Guide* for more information.

The system generates log file entries for the following credential policy events:

- Authentication success
- Authentication failure (bad password or unknown)
- Authentication failure due to
  - Administrative lock
  - Hack lock (failed logon lockouts)
  - Expired soft lock (expired credential)
  - Inactive lock (credential not used for some time)
  - User must change (credential set to user must change)
  - LDAP inactive (switching to LDAP authentication and LDAP not active)
- Successful user credential updates
- Failed user credential updates

**Note**

If you use LDAP authentication for end user passwords, LDAP tracks only authentication successes and failures.

All event messages contain the string “ims-auth” and the userid that is attempting authentication.

You can view log files with the Cisco Unified Cisco Unified Real-Time Monitoring Tool. You can also collect captured events into reports. See the *Cisco Unified Real-Time Monitoring Tool Administration Guide* and the *CDR Analysis and Reporting Administration Guide* for more information.

## Data Migration Assistant

The Cisco Unified Communications Manager Data Migration Assistant (DMA) provides conversion of Cisco Unified Communications Manager data to a format that is compatible with later releases of Cisco Unified Communications Manager:

- Upgrades from 5.x releases automatically migrate end user passwords and PINs. The system applies the application password that you configured at installation to all application users.
- Upgrades from 4.x releases reset end user credentials. During installation, the system queries for a default end user password and PIN and applies the credentials to all end users. The system applies the application password that you configured at installation to all application users.

For details on obtaining, installing, and using DMA, refer to the Cisco Unified Communications Manager *Data Migration Assistant User Guide*.

## Credential Policy Configuration Checklist

Table 22-1 lists the general steps and guidelines for configuring credential policies.

Table 22-1 Credential Policy Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Use the Credential Policy Configuration windows to configure a credential policy other than the default policy.	<a href="#">Credential Policy Configuration</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
Step 2	Use the Credential Policy Default windows to assign a new credential policy and configure a common password for an account type.	<a href="#">Credential Policy Default Configuration</a> , <i>Cisco Unified Communications Manager Administration Guide</i> <i>Cisco Unified Communications Manager Bulk Administration Guide</i>
Step 3	To manage or monitor the credential configuration for individual users, click the Edit Credential link in the user configuration window.	<a href="#">Managing End User Credential Information</a> , <i>Cisco Unified Communications Manager Administration Guide</i> <a href="#">Managing Application User Credential Information</a> , <i>Cisco Unified Communications Manager Administration Guide</i>

# Where to Find More Information

## Related Topics

- [Understanding the Directory](#), page 20-1
- [Application Users and End Users](#), page 21-1
- [Managing End User Credential Information](#), *Cisco Unified Communications Manager Administration Guide*
- [Managing Application User Credential Information](#), *Cisco Unified Communications Manager Administration Guide*
- [Credential Policy Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Credential Policy Default Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [LDAP System Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [LDAP Directory Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [LDAP Authentication Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Application User Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [End User Configuration](#), *Cisco Unified Communications Manager Administration Guide*

## Additional Cisco Documentation

- *Installing Cisco Unified Communications Manager Release 7.0(1)*
- *Cisco Unified Communications Operating System Administration Guide*
- *Data Migration Assistant User Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *CDR Analysis and Reporting Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Communications Manager Security Guide*
- Cisco Unified IP Phone user documentation and release notes (all models)

