Passwords, PINs, and Authentication Rule Management

In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. We recommend that you define Unity Connection authentication rules as follows:

- To require that users change their PINs and passwords often.
- To require that user PINs and passwords be unique and not easy to guess.

Well thought out authentication rules can also thwart unauthorized access to Unity Connection applications, such as Cisco Personal Communication Assistant (Cisco PCA) and Cisco Unity Connection Survivable Remote Site Voicemail, by locking out users who enter invalid PINs or passwords too many times.

In this chapter, you find information on completing the above tasks and on other issues related to PIN and password security. To help you understand the scope of Cisco Unity Connection password management, the first section in this chapter describes the different passwords required to access the Cisco Personal Communications Assistant (PCA), the Unity Connection conversation, Cisco Unity Connection Administration, and other administrative web applications. Each of the sections that follow offer information on actions you need to take; recommendations that help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

For information that guides you through the process of securing Unity Connection passwords and defining authentication rules, see the following sections.

• Passwords, PINs, and Authentication Rule Management, on page 1

Passwords, PINs, and Authentication Rule Management

In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. We recommend that you define Unity Connection authentication rules as follows:

- To require that users change their PINs and passwords often.
- To require that user PINs and passwords be unique and not easy to guess.

Well thought out authentication rules can also thwart unauthorized access to Unity Connection applications, such as Cisco Personal Communication Assistant (Cisco PCA) and Cisco Unity Connection Survivable Remote Site Voicemail, by locking out users who enter invalid PINs or passwords too many times.

In this chapter, you find information on completing the above tasks and on other issues related to PIN and password security. To help you understand the scope of Cisco Unity Connection password management, the first section in this chapter describes the different passwords required to access the Cisco Personal Communications Assistant (PCA), the Unity Connection conversation, Cisco Unity Connection Administration, and other administrative web applications. Each of the sections that follow offer information on actions you need to take; recommendations that help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

For information that guides you through the process of securing Unity Connection passwords and defining authentication rules, see the following sections.

About the PINs and Passwords Users Use to Access Unity Connection Applications

Cisco Unity Connection users use different PINs and passwords to access various Unity Connection applications. Knowing which passwords are required for each application is important in understanding the scope of Unity Connection password management.

Phone PINs

Users use a phone PIN to sign in to the Cisco Unity Connection conversation by phone. Users use the phone keypad to enter a PIN (which consists entirely of digits), or can say the PIN if enabled for voice recognition.

Web Application (Cisco PCA) Passwords

A user who is assigned to an administrative role may also use the web application password to sign in to the following Unity Connection applications:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability
- Real-Time Monitoring Tool
- Cisco Unity Connection SRSV Administration

Note If you are using Cisco Unified Communications Manager Business Edition (CMBE) or LDAP authentication, users must use their Cisco Unified CMBE or LDAP account passwords to access Unity Connection web applications. Ensuring That Users Are Initially Assigned Unique and Secure PINs and Passwords in Cisco Unity Connection.

To help protect Cisco Unity Connection from unauthorized access and toll fraud, every user should be assigned a unique phone PIN and web application (Cisco PCA) password.

When you add users to Unity Connection, the phone PIN and web application password are determined by the template that is used to create the user account. By default, user templates are assigned randomly generated strings for the phone PIN and web password. All users created from a template are assigned the same PIN and password.

Consider the following options to ensure that each user is assigned a unique and secure PIN and password at the time that you create the account, or immediately thereafter:

- If you are creating a small number of user accounts, after you have used Cisco Unity Connection Administration to create the accounts, change the phone PIN and web password for each user on the Users > Users > Change Password page. Alternatively, instruct users to sign in as soon as possible to change their PINs and passwords (if you choose this option, also ensure that the User Must Change at Next Sign-In check box is checked on the Edit Password page of the template you used to create the accounts).
- If you are creating multiple user accounts, use the Bulk Password Edit tool to assign unique passwords and PINs to Unity Connection end user accounts (users with mailboxes) after they have been created. You use the Bulk Password Edit tool along with a CSV file that contains unique strings for the passwords and PINs to apply the passwords/PINs in bulk.

The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html.

Unity Connection SRSV Passwords and Shared Secrets

All the requests initiated from the central Unity Connection server to the Unity Connection SRSV server use administrator credentials of Unity Connection SRSV for communication whereas the requests from Unity Connection SRSV to Unity Connection use secret tokens for authentication.

The central Unity Connection server uses the administrator username and password of Unity Connection SRSV to authenticate access to the server. The username and password of Unity Connection SRSV get stored in the Connection database as you create a new branch on the central Unity Connection server.

During each provisioning cycle with Unity Connection SRSV, the central Unity Connection server generates a secret token and shares the token with Unity Connection SRSV. After the provisioning is completed from the Unity Connection SRSV site, it notifies the central Unity Connection server using the same token. Then this token is removed from both the central Unity Connection and Unity Connection SRSV servers as soon as the provisioning cycle is completed. This concept of runtime token keys is known as shared secrets.

For more information on Unity Connection SRSV, refer to the Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) Release 15 at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/srsv/guide/b_15cucsrsvx.html.

Changing Web Application Passwords

You can change the web application (Cisco PCA) password for an individual user on the Users > Users > Change Password page in Cisco Unity Connection Administration at any time.

When passwords expire, users and administrators is required to enter a new password when they next attempt to sign in to the Cisco PCA or Connection Administration.

Users can also change their Cisco PCA passwords in the Unity Connection Messaging Assistant.

To change passwords for multiple end user accounts (users with mailboxes), you can use the Bulk Password Edit tool to assign unique new passwords to the accounts. You use the Bulk Password Edit tool along with a CSV file that contains unique strings for the passwords to apply the passwords in bulk. The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at X http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html. You can also use the Cisco Unity Connection Bulk Administration Tool (BAT) to change multiple user passwords at one time.

For users who are able to access voice messages in an IMAP client, make sure that they understand that whenever they change their Cisco PCA password in the Messaging Assistant, they also must update the password in their IMAP client. Passwords are not synchronized between IMAP clients and the Cisco PCA.

Best Practice:

Specify a long—eight or more characters—and non-trivial password. Encourage users to follow the same practice whenever they change their passwords, or assign them to an authentication rule that requires them to do so. Cisco PCA passwords should be changed every six months.

Changing Phone PINs

You can change the phone PIN for an individual user on the Users > Users > Change Password page in Cisco Unity Connection Administration at any time.

Users can use the Unity Connection phone conversation or the Unity Connection Messaging Assistant to change their phone PINs.

To change PINs for multiple end user accounts (users with mailboxes), you can use the Bulk Password Edit tool to assign unique new PINs to the accounts. You use the Bulk Password Edit tool along with a CSV file that contains unique strings for the PINs to apply the PINs in bulk. The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html. You can also use the Cisco Unity Connection Bulk Administration Tool (BAT) to change multiple user PINs at one time.

When PINs expire, users are required to enter a new PIN when they next attempt to sign in to the Unity Connection conversation.

Because users can use the Messaging Assistant to change their phone PINs, they can help ensure the security of their PINs by taking appropriate measures also to keep their web application (Cisco PCA) passwords secure.

Users need to understand that the phone PIN and Cisco PCA password are not synchronized. While first-time enrollment prompts them to change their initial phone PIN, it does not let them change the password that they use to sign in to the Cisco PCA website.

Best Practice:

Each user should be assigned a unique PIN that is six or more digits long and non-trivial. Encourage users to follow the same practice or assign them to an authentication rule that requires them to do so.

Defining Authentication Rules to Specify Password, PIN, and Lockout Policies

Note Cisco Unity Connection authentication rules are not applicable to managing user passwords in Cisco Unified Communications Manager Business Edition (CMBE), or when LDAP authentication is enabled, because authentication is not handled by Unity Connection in those cases.

Use authentication rules to customize the sign-in, password, and lockout policies that Cisco Unity Connection applies when users access Unity Connection by phone, and how users access Cisco Unity Connection Administration, the Cisco PCA, and other applications such as IMAP clients.

The settings that you specify on the Edit Authentication Rule page in Connection Administration determine:

- The number of failed sign-in attempts to the Unity Connection phone interface, the Cisco PCA, or Connection Administration that are allowed before an account is locked.
- The number of minutes an account remains locked before it is reset.
- Whether a locked account must be unlocked manually by an administrator.
- The minimum length allowed for passwords and PINs.
- The number of days before a password or PIN expires.

Best Practices:

For increased security, we recommend the following best practices when defining authentication rules:

- Require that users change their Unity Connection passwords and PINs at least once every six months.
- Require web application passwords to be eight or more characters and non-trivial.
- Require voicemail PINs to be six or more characters and non-trivial.

For greater security, establish authentication rules that prevent PINs and passwords from being easy to guess and from being used for a long time. At the same time, is also best to avoid requiring PINs and passwords that are so complicated or that must be changed so often that users have to write them down to remember them.

In addition, use the following guidelines as you specify authentication rules in the following fields:

Failed Sign-In __ Attempts:

Use this field to indicate how Unity Connection handles situations when a user repeatedly enters an incorrect PIN or password. We recommend that you set the field to lock user accounts after three failed sign-in attempts.

Reset Failed Sign-In Attempts Every __ Minutes:

Use this field to specify the number of minutes after which Unity Connection clear the count of failed sign-in attempts (unless the failed sign-in limit is already reached and the account is locked). We recommend that you set the field to clear the count of failed sign-in attempts after 30 minutes.

Lockout Duration:

Use this field to specify the length of time that a user who is locked out must wait before attempting to sign in again.

For even tighter security, you can check the Administrator Must Unlock check box, which prevents users from accessing their accounts until an administrator unlocks them on the applicable User > Password Settings page. Check the Administrator Must Unlock check box only if an administrator is readily available to assist users or if the system is prone to unauthorized access and toll fraud.

Credential Expires After __ Days:

As a best practice, do not enable the Never Expires option. Instead, confirm that this field has a value greater than zero so that users are prompted to change their passwords every X days (X is the value specified in the Credential Expires After field).

We recommend that you configure web passwords to expire after 120 days and phone PINs to expire after 180 days.

Minimum Credential Length:

As a best practice, set this field to six or higher.

For authentication rules that are used for web application passwords, we recommend that you require users to use passwords that are eight or more characters in length.

For authentication rules that are used for phone PINs, we recommend that you require users to use PINs that are six or more digits in length.

When you change the minimum credential length, users are required to use the new length the next time that they change their PINs and passwords.

Minimum Number of Character Changes between Successive Credentials:

Use this field to specify the number of characters that a user must change while updating the web application password.(not applicable for PIN)

The value of this field should be less than or equal to the value of Minimum Credential Length.

By default, the value of this field is set to 1, which means that the user must change at least one character between old password and new password.

Stored Number of Previous Credentials:

As a best practice, specify a number in this field. By doing so, you enable Unity Connection to enforce password uniqueness by storing a specified number of previous passwords or PINs for each user. When users change passwords and PINs, Unity Connection compares the new password or PIN with those stored in the credential history. Unity Connection rejects any password or PIN that matches a password or PIN stored in the history.

By default, Unity Connection stores 5 passwords or PINs in credential history.

Check For Trivial Passwords:

As a best practice, confirm that this field is enabled so that users must use non-trivial PINs and passwords.

A non-trivial phone PIN has the following attributes:

- The PIN cannot match the numeric representation of the first or last name of the user.
- The PIN cannot contain the primary extension or alternate extensions of the user.
- The PIN cannot contain the reverse of the primary extension or alternate extensions of the user.
- The PIN cannot contain groups of repeated digits, such as “408408” or “123123.”
- The PIN cannot contain only two different digits, such as “121212.”
- A digit cannot be used more than two times consecutively (for example, “28883”).
- The PIN cannot be an ascending or descending group of digits (for example, “012345” or “987654”).
- The PIN cannot contain a group of numbers that are dialed in a straight line on the keypad when the group of digits equals the minimum credential length that is allowed (for example, if 3 digits is allowed, the user could not use “123,” “456,” or “789” as a PIN).

A non-trivial web application password has the following attributes:

- The password must contain at least three of the following four characters: an uppercase character, a lowercase character, a number, or a symbol.
- The password cannot contain the user alias or its reverse.
- The password cannot contain the primary extension or any alternate extensions.

- A character cannot be used more than three times consecutively (for example, !Cooool).
- The characters cannot all be consecutive, in ascending or descending order (for example, abcdef or fedcba).

Changing the Unity Connection SRSV User PIN

If you want to change the PIN of a Unity Connection SRSV user, you can do it through the Cisco Unity Connection Administration interface. After changing the PIN of the selected user, you need to provision the associated branch to update the user information in the Unity Connection SRSV database.

Note You cannot change the PIN of an SRSV user through Cisco Unity Connection SRSV Administration interface.

Restricting the Maximum Concurrent Sessions

With release 11.5(1) and later, Unity Connection provides enhanced security by allowing the administrator to restrict the maximum concurrent sessions that a user can have on the following interfaces:

- **Telephony Interface**: On telephony interface, if a user attempts a new session beyond the configured maximum limit, the call gets disconnected.
- **Visual Voicemail Interface** *(PIN Based Authentication)*: On visual voicemail interface, if a user attempts a new session beyond the configured maximum limit, the user is not allowed to login to the interface.

  Telephony or visual voicemail sessions includes calling from both primary extension as well as alternate extension. To enable the feature on both the interfaces, login to Cisco Unity Connection Administration, navigate to **System Settings** > **Advanced** > **Conversations** and enter a value for the maximum concurrent sessions in the **Maximum Concurrent Sessions for Telephony Interface (Per User)** field.

- **IMAP Interface**: On IMAP interface, if a user tries to login to an IMAP account beyond the configured limit, the login attempt fails. To enable the feature on IMAP interface, login to Cisco Unity Connection Administration, navigate to **System Settings** > **Advanced** > **Messaging** and enter a value for the maximum concurrent sessions in the **Maximum Concurrent Sessions for IMAP Interface (Per User)** field.

By default, the value of **Maximum Concurrent Sessions for Telephony Interface (Per User)** and **Maximum Concurrent Sessions for IMAP Interface (Per User)** field is set to zero, which means that the feature is disabled.

Note In case of Outlook 2010, the recommended minimum value for the field is 4 and for Outlook 2013, the recommended value is 2.

Configuring Inactivity Timeout

With release 11.5(1) and later, Unity Connection provides a new feature for enhanced security by allowing administrator to configure the number of days for user inactivity timeout. If a user does not login to the voicemail account from any of the Unity Connection interface, such as TUI or Web Inbox for configured numbers of days, the account is disabled and further access is denied.

To enable this feature, login to Cisco Unity Connection Administration, navigate to **System Settings** > **Advanced** > **Connection Administration** and enter a value for the inactivity timeout in the **User Inactivity Timeout (in Days)** field.

Note By default, the value of **User Inactivity Timeout (in Days)** field is set to zero, which means that the feature is disabled.

When the feature is enabled the following settings are applicable to Unity Connection:

- You can search the inactive users by limiting the search criterion to **Inactive Users** at **Users** > **Search Users** page of Cisco Unity Connection Administration.
- You can update the **VoiceMail Application Access** for the user to **Active** or **Inactive** at **Users** > **Edit User Basics** page of Cisco Unity Connection Administration.
- The **Check Inactive Users** sysagent task can be scheduled to run at configured intervals and mark a user inactive if the user has not logged in for more than configured number of days.