



# Securing Administration and Services Accounts in Cisco Unity Connection

In this chapter, you will find descriptions of potential security issues related to securing accounts; information on any actions you need to take; recommendations that will help you make decisions; ramifications of the decisions you make; and in many cases, best practices.

See the following sections:

- [Understanding Cisco Unity Connection Administration Accounts, page 5-1](#)
- [Best Practices for Accounts That Are Used to Access Cisco Unity Connection Administration in Unity Connection, page 5-2](#)
- [Securing Unified Messaging Services Accounts, page 5-4](#)





## Understanding Cisco Unity Connection Administration Accounts

A Cisco Unity Connection server has two types of administration accounts. [Table 5-1](#) summarizes the purposes for and the differences between the two types of accounts.

**Table 5-1** Administration Accounts on a Unity Connection Server

	Operating System Administration Account	Application Administration Account
The account is used to access	<ul style="list-style-type: none"><li>• Cisco Unified Operating System Administration</li><li>• Disaster Recovery System</li><li>• Command line interface</li></ul>	<ul style="list-style-type: none"><li>• Cisco Unity Connection Administration</li><li>• Cisco Unified Serviceability</li><li>• Cisco Unity Connection Serviceability</li><li>• Real-Time Monitoring Tool</li></ul>
The first account is created	During installation, when you specify the Administrator ID and password	During installation, when you specify the application user name and password

Table 5-1 Administration Accounts on a Unity Connection Server (continued)

	Operating System Administration Account	Application Administration Account
How to change the account name	Not supported	By using Cisco Unity Connection Administration.   <b>Caution</b> Do not change the account name by using the <b>utils reset_ui_administrator_name</b> command, or Unity Connection will not function properly.
How to change the account password	By using the <b>set password</b> CLI command	<ul style="list-style-type: none"> <li>• By using Cisco Unity Connection Administration</li> <li>• By using the <b>utils cuc reset password</b> CLI command</li> </ul>  <b>Caution</b> Do not change the account name by using the <b>utils reset_ui_administrator_password</b> command, or Unity Connection will not function properly.
How to create additional accounts	By using the <b>set account</b> CLI command	By using Cisco Unity Connection Administration   <b>Caution</b> Do not create additional accounts by using the <b>set account</b> command, or Unity Connection will not function properly.
How to delete accounts other than the first account	By using the <b>delete account</b> CLI command	By using Cisco Unity Connection Administration   <b>Caution</b> Do not delete accounts by using the <b>delete account</b> command, or Unity Connection will not function properly.
How to list administrator accounts	By using the <b>show account</b> CLI command.	By using Cisco Unity Connection Administration
Can be integrated with an LDAP user account	No	Yes

## Best Practices for Accounts That Are Used to Access Cisco Unity Connection Administration in Unity Connection

Cisco Unity Connection Administration is a web application that you use to do most administrative tasks. An administrative account can be used to access Connection Administration to define how Cisco Unity Connection works for individual users (or for a group of users), to set system schedules, to set call management options, and to make changes to other important data, all depending on the roles to which the administrative account is assigned. If your site is comprised of multiple Unity Connection servers, an account that is used to access Connection Administration on one server may be able to authenticate and gain access to Connection Administration on the other networked servers as well. To secure access to Connection Administration, consider the following best practices.

**Best Practice: Limit the Use of the Application Administration Account**

Until you create a Cisco Unity Connection user account specifically for the purpose of administering Unity Connection, you sign in to Cisco Unity Connection Administration by using the credentials that are associated with the default administrator account. The default administrator account is created during the installation of Unity Connection with the application user username and password you specify during installation. The default administrator account is automatically assigned to the system administrator role, which offers full system access rights to Connection Administration. This means that not only can the administration account access all pages in Connection Administration, but it also has read, edit, create, delete and execute privileges for all Connection Administration pages. For this reason, you should limit the use of this highly privileged account to only one or to very few individuals.

As an alternative to the default administrator account, you can create additional administrative accounts that are assigned to roles that have fewer privileges based on what is appropriate to the administrative tasks that each person performs.

**Note**

- Make sure you do not use the following application usernames as this will generate an error:
  - CCMSysUser
  - WDSysUser
  - CCMQRTSysUser
  - IPMASysUser
  - WDSecureSysUser
  - CCMQRTSecureSysUser
  - IPMASecureSysUser
  - TabSyncSysUser
  - CUCService

[www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/10x/user\\_mac/guide/10xcucmacx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html).

**Best Practice: Use Roles to Provide Different Levels of Access to Cisco Unity Connection Administration**

When modifying role assignments to secure access to Cisco Unity Connection Administration, consider the following best practices:

- Do not modify the role assignment of the default administrator account. Instead, create additional administrative user accounts that offer the appropriate levels of access to Connection Administration. For example, you may want to assign an administrative user account to the User Administrator role, which allows the administrator to manage user account settings and access all user administration functions. Or you may want to assign an administrative user account to the Help Desk Administrator role, which allows the administrator to reset user passwords and PINs, unlock user accounts, and view user setting pages.
- Create additional administrative user templates that are assigned to roles that provide varying levels of access. By default, the Administrator user template is assigned to the System Administrator role. Any administrative user accounts that are created from the Administrator user template will be assigned to the System Administrator role, which gives administrators full access to all Unity Connection administrative functions. Use this Administrator template sparingly to create accounts for administrative users.

- By default, the Voicemail User Template is not assigned to any roles, and should not be assigned to any administrative roles. Instead, use this template to create accounts for end users with mailboxes. (The only role that should be assigned to an end user with a mailbox is the Greeting Administrator role; with this role, the only “administrative” function is to have access to the Cisco Unity Greetings Administrator, which allows users to manage the recorded greetings for call handlers by phone.)

**Best Practice: Use Different Accounts to Access a Voice Mailbox and Cisco Unity Connection Administration**

We recommend that Cisco Unity Connection administrators do not use the same account to access Cisco Unity Connection Administration that they use to sign in to the Cisco Personal Communications Assistant (PCA) or the phone interface.

## Securing Unified Messaging Services Accounts

When you configure unified messaging for Cisco Unity Connection 10.x, you create one or more Active Directory accounts that Unity Connection uses to communicate with Exchange. Like any Active Directory account that has the right to access Exchange mailboxes, this account allows anyone who knows the account name and password to read mail and listen to voice messages, and to send and delete messages. The account does not have broad rights in Exchange, so you could not use it to restart an Exchange server, for example.

To secure the account, we recommend that you give the account a long password (20 or more characters) that includes upper- and lower-case characters, numbers, and special characters. The password is encrypted with AES 128-bit encryption and stored in the Unity Connection database. The database is accessible only with root access, and root access is available only with assistance from Cisco TAC.

Do not disable the account, or Unity Connection cannot use it to access Exchange mailboxes.