Securing Administration and Services Accounts

Securing Administration and Services Accounts

Introduction

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

Understanding Cisco Unity Connection Administration Accounts

A Cisco Unity Connection server has two types of administration accounts. Table 1: Administration Accounts on a Unity Connection Server summarizes the purposes for and the differences between the two types of accounts.

Table 1: Administration Accounts on a Unity Connection Server

	Operating System Administration Account	Application Administration Account
The account is used to access	• Cisco Unified Operating System Administration • Disaster Recovery System • Command line interface	• Cisco Unity Connection Administration • Cisco Unified Serviceability • Cisco Unity Connection Serviceability • Real-Time Monitoring Tool
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

	Operating System Administration Account	Application Administration Account
How to change the account name	Not supported	Using Cisco Unity Connection Administration. **Caution** Do not change the account name using the **utils reset_ui_administrator_name** command, or Unity Connection does not function properly.
How to change the account password	Using the **set password** CLI command	• Using Cisco Unity Connection Administration • Using the **utils cuc reset password** CLI command **Caution** Do not change the account name using the **utils reset_ui_administrator_passwo** command, or Unity Connection do not function properly.
How to create additional accounts	Using the **set account** CLI command	Using Cisco Unity Connection Administration **Caution** Do not create additional accounts using the **set account** command, or Unity Connection does not function properly.
How to delete accounts other than the first account	Using the **delete account** CLI command	Using Cisco Unity Connection Administration **Caution** Do not delete accounts using the **delete account** command, or Unity Connection does not function properly.
How to list administrator accounts	Using the **show account** CLI command.	Using Cisco Unity Connection Administration
Can be integrated with an LDAP user account	No	Yes

Best Practices for Accounts Used to Access Cisco Unity Connection Administration

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 Unity Connection user account specifically for the purpose of administering Unity Connection, you sign in to Cisco Unity Connection Administration 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 generate an error:

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

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 is 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 11.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.

Ensuring File Integrity

Unity Connection provides enhanced security by allowing the administrator to ensure the integrity of the files that can be downloaded from various interfaces, such as Cisco Unity Connection Administration and Cisco Unity Connection Serviceability of Cisco Unity Connection. To verify the file integrity, Unity Connection offers the SHA-512 checksum value for all download files. For example, the SHA-512 checksum value for Cisco Unified Real-Time Monitoring Tool plugin appears in the **Description** field of the Search Plugin page.

For ensuring the integrity of the file, administrator can download the file and generate the checksum for the file by using any external tool available online. Now, compare the displayed checksum with the checksum of

the downloaded file. If both the checksums of the file are same, it means there is no error in the download file.