



CHAPTER 2

Managing Cisco Unity Administrator Accounts

See the following sections in this chapter:

- [About the Accounts That Can Be Used to Administer Cisco Unity, page 2-1](#)
- [Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator, page 2-2](#)
- [Granting Administrative Rights to Other Cisco Unity Servers, page 2-3](#)

About the Accounts That Can Be Used to Administer Cisco Unity

To access the Cisco Unity Administrator, administrators can use one of the following accounts:

Administration account	This is the account that was selected during installation to administer Cisco Unity. The administration account is automatically associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator
The Active Directory account associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator	<p>In order for administrators to log on to the Cisco Unity Administrator on the Cisco Unity server, this account must be a member of one of the following Admins groups, as applicable:</p> <ul style="list-style-type: none">• Domain Admins group (when the Cisco Unity server is a domain controller)• Local Administrators group (when the Cisco Unity server is a member server) <p>Otherwise, the account must at least have the right to log on locally so that administrators can log on to the Cisco Unity Administrator from a computer other than the Cisco Unity server</p>

Until you create a Cisco Unity subscriber account specifically for the purpose of administering Cisco Unity, you must use the Active Directory credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

Consider using an alternative to the administration account, if you want to do the following:

- Limit the use of the administration account. The COS assigned to the administration account has full system access rights to the Cisco Unity Administrator. This means that not only can the administration account access all pages in the Cisco Unity Administrator, but it also has read, edit, add, and delete privileges for all Cisco Unity Administrator pages.

- Ensure that there are additional accounts available that can be used to access the Cisco Unity Administrator if the administration account is deleted or corrupted.

The Cisco Unity subscriber accounts that are used to access the Cisco Unity Administrator must have the appropriate COS rights. COS rights specify which tasks, if any, administrators can do in the Cisco Unity Administrator. For example, some subscriber accounts that are used for administrator access can be associated with a COS that provides read-only access, or that restricts administrators to access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords.

In addition to COS rights, subscriber accounts that are used to access the Cisco Unity Administrator must be associated with an Active Directory account that is enabled.

To create additional subscriber accounts for the purposes of accessing the Cisco Unity Administrator, complete the procedures in the [“Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator”](#) section on page 2-2. If you prefer not to create a specific subscriber account for each administrator who needs to access the Cisco Unity Administrator, you can use the GrantUnityAccess utility to associate one or more Active Directory accounts with a single subscriber account. For more information about using the GrantUnityAccess utility, see the [“Granting Administrative Rights to Other Cisco Unity Servers”](#) section on page 2-3.


Note

As a best practice, we recommend that Cisco Unity Administrators not use the same subscriber account to log on to the Cisco Unity Administrator that they use to log on to the Cisco PCA to manage their own Cisco Unity accounts. In addition, they should not use Unity service accounts to administer Cisco Unity.

Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator

To create additional subscriber accounts for the purposes of accessing the Cisco Unity Administrator, you use the same procedures that you use for creating regular subscriber accounts (as detailed in the [“Managing Subscriber Accounts”](#) chapter. However, if you want administrators to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you will also need to add their Active Directory accounts either to the local Administrators group—when the Cisco Unity server is a member server—or to the Domain Admins group—when the Cisco Unity server is a domain controller. You can do the applicable procedures in this section either before or after you create subscriber accounts. Until this is done, administrators can access the Cisco Unity Administrator only from another computer.

To Add the Active Directory Account to the Local Administrators Group (When the Cisco Unity Server Is a Member Server)

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
- Step 2** In the left pane of the Computer Management MMC, expand **System Tools > Local Users and Groups**.
- Step 3** In the left pane, click **Users**.
- Step 4** In the right pane, double-click the administration account.
- Step 5** In the Properties dialog box, click the **Member Of** tab.
- Step 6** Click **Add**.
- Step 7** In the Select Groups dialog box, in the top list, double-click **Administrators**.

- Step 8** Click **OK** to close the Select Groups dialog box.
 - Step 9** Click **OK** to close the Properties dialog box.
 - Step 10** Close the **Computer Management MMC**.
-

To Add the Active Directory Account to the Domain Admins Group (When the Cisco Unity Server Is a Domain Controller)

- Step 1** On the Cisco Unity server, log on to Windows by using an account that is a member of the Domain Admins group.
 - Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers** or click **Programs > Administrative Tools > Active Directory Users and Computers**.
 - Step 3** In the left pane, expand the domain, and click **Users**.
 - Step 4** In the right pane, double-click the name of the administration account.
 - Step 5** Click the **Members Of** tab.
 - Step 6** Click **Add**.
 - Step 7** In the Select Groups dialog box, in the top list, double-click **Domain Admins**.
 - Step 8** Click **OK** to close the Select Groups dialog box.
 - Step 9** Click **OK** to close the Properties dialog box.
 - Step 10** Close **Active Directory Users and Computers**.
-

Granting Administrative Rights to Other Cisco Unity Servers

Rather than create subscriber accounts on each server for each person who needs to administer Cisco Unity, you can use the GrantUnityAccess utility to associate any number of Active Directory accounts with a single Cisco Unity subscriber account. GrantUnityAccess maintains a table of the associated Active Directory accounts and Cisco Unity subscriber accounts that Cisco Unity references when someone tries to access the Cisco Unity Administrator (regardless of the authentication method used by the Cisco Unity Administrator). This table is used to determine whether to permit someone access to the Cisco Unity Administrator.

Before you use GrantUnityAccess, consider the following:

- The Active Directory account(s) that you want to associate with a subscriber account must either be in the same domain as the Cisco Unity server or in a trusted domain. In addition, if you want administrators to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you must add the Active Directory account to the applicable Admins group (see the [“Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator”](#) section on page 2-2 for a detailed procedure.) Otherwise, the account must at least have the right to log on locally so that administrators can log on to the Cisco Unity Administrator from a computer other than the Cisco Unity server.
- As a best practice, the Active Directory accounts that are associated with subscriber accounts should require strong passwords. Set your domain account policy in Active Directory to require them.
- You can associate multiple accounts with a single subscriber account.

- You can associate Active Directory account(s) with any subscriber account, as long as the subscriber account has COS rights to access the Cisco Unity Administrator. This includes the administration account that was selected when Cisco Unity was installed.
- Because the administration account is associated with a COS that offers unlimited access to the Cisco Unity Administrator, consider associating the Active Directory account(s) used by administrators with a different subscriber account that you create on each Cisco Unity server—one that has more limited COS rights. In this way, you can customize the level of access for the administrators in your organization.
- If there are several servers that the administrators need access to, you can create a batch file that contains the commands to grant access to the applicable servers. In this way, you can avoid entering the commands repeatedly.

Use the following procedure to run `GrantUnityAccess`. Note that you cannot run `GrantUnityAccess` remotely across a network, so you will need to run it on each Cisco Unity server that you want to make accessible, and for each account that you want to map. See the “[Sample GrantUnityAccess Arguments](#)” section on page 2-4 for an example of how this utility is used, and for argument syntax details.

To Use the GrantUnityAccess Utility

-
- Step 1** Log on to Windows on the Cisco Unity server by using either the administration account that was selected when Cisco Unity was installed or an Active Directory account that is a member of the local Administrators group on the Cisco Unity server.
- Step 2** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 3** In the left pane, expand **Diagnostic Tools**, and double-click **Grant Unity Access** to display a command prompt window.
- Step 4** To associate an Active Directory account with a Cisco Unity subscriber account, enter:

```
GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias>
```

Sample GrantUnityAccess Arguments

For example, assume that `JSmith` and `KChen` are the aliases of administrators who need access to the Cisco Unity Administrator on another Cisco Unity server, and that their Active Directory accounts are in a domain called `NewYorkDomain`. To associate their Active Directory accounts with the administration account that was selected when Cisco Unity was installed, run `GrantUnityAccess` two times as follows:

```
GrantUnityAccess -u NewYorkDomain\JSmith -s <UnitySubscriberAlias for administration account>
```

```
GrantUnityAccess -u NewYorkDomain\KChen -s <UnitySubscriberAlias for administration account>
```

Rather than specifying the administration account, you could associate the Active Directory account for Neil Jones with the subscriber account for Kelly Bader instead:

```
GrantUnityAccess -u NewYorkDomain\NJones -s KBader
```

To obtain a list of accounts that have been associated with Cisco Unity subscriber accounts, enter:

```
GrantUnityAccess -l
```

To delete an association made previously using `GrantUnityAccess`, enter:

```
GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias> -d
```

To display information about these and other arguments, enter:

```
GrantUnityAccess -?
```

