



## Accessing the Cisco Unity Administrator

---

The Cisco Unity Administrator is a website that you use to do most administrative tasks. Administrative tasks include determining system schedules, specifying settings for individual subscribers (or for a group of subscribers by using a subscriber template), and implementing a call management plan.

See the following sections in this chapter for more information:

- [Accessing and Exiting the Cisco Unity Administrator, page 2-1](#)—This section explains how to access and exit the Cisco Unity Administrator.
- [Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator, page 2-3](#)—When multiple Cisco Unity servers are networked together, you can access the Cisco Unity Administrator on another Cisco Unity server.
- [About Cisco Unity Administrator Authentication, page 2-4](#)—This section explains the authentication methods that you can use with the Cisco Unity Administrator.
- [Cisco Unity Administrator Accounts, page 2-8](#)—This section describes the type of accounts that you can use to access the Cisco Unity Administrator, and the ways in which you create additional accounts or grant administrative rights to existing accounts so that they can be used to administer Cisco Unity. In addition, this section describes the account policy options available for Cisco Unity Administrator logons, passwords, and lockouts.

## Accessing and Exiting the Cisco Unity Administrator

To learn about accessing and exiting the Cisco Unity Administrator, see the following sections:

- [Logging On to the Cisco Unity Administrator, page 2-1](#)
- [Exiting the Cisco Unity Administrator, page 2-3](#)

## Logging On to the Cisco Unity Administrator

Although the way in which you log on to the Cisco Unity Administrator depends on the type of authentication that it uses, the account that you use to log on remains the same: you can use either the administration account that was selected when Cisco Unity was installed, or you can use an appropriate Windows domain account. For information on which accounts can be used to access the Cisco Unity Administrator, see the [“About the Accounts That Can Be Used to Administer Cisco Unity”](#) section on page 2-9.

**Note**

Until you create a Cisco Unity subscriber account for the purpose of administering Cisco Unity, you must use the Windows credentials associated with the administration account to log on to the Cisco Unity Administrator.

There are potential security risks if your system is configured so that you are not prompted for a name and password when you access the Cisco Unity Administrator, and if all of the following conditions exist:

- The Cisco Unity Administrator uses the Integrated Windows authentication method
- Internet Explorer is not configured to prompt for user name and password
- You logged on to Windows in a trusted domain by using either the administration account, or an appropriate Windows domain account

In this situation, it is recommended that you increase security by configuring the browser to prompt for a user name and password, or by locking the workstation when it is unattended.

The length of time that the browser can be left unattended before Cisco Unity automatically logs you off is governed by the Session Timeout limit specified in IIS. When the browser session times out, you must refresh the browser, and log on to the Cisco Unity Administrator again. If the Cisco Unity Administrator uses the Anonymous authentication method, you can set the session timeout value for IIS (see the [“Authentication Settings” section on page 28-11](#) for details). When the Cisco Unity Administrator uses the Integrated Windows authentication method, you must set session limits directly in IIS.

To log on to the Cisco Unity Administrator, use the applicable procedure in this section. Note that Cisco Unity does not permit more than five administrators to access the Cisco Unity Administrator at the same time.

#### To Log On to the Cisco Unity Administrator When It Uses Integrated Windows Authentication

- 
- Step 1** Log on to Windows on the Cisco Unity server (or a remote computer) by using either the administration account that was selected when Cisco Unity was installed or an appropriate Windows domain account.
- Step 2** If you logged on to the Cisco Unity Administrator on the Cisco Unity server, right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Launch System Admin**.
- If you logged on to the Cisco Unity Administrator on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/web/sa**.
- Step 3** If Internet Explorer prompts you, enter either the user name, password, and domain for the administration account that was selected when Cisco Unity was installed or an appropriate Windows domain account.
- 

#### To Log On to the Cisco Unity Administrator When It Uses Anonymous Authentication

- 
- Step 1** Log on to Windows on the Cisco Unity server (or a remote computer) by using any domain account that has the right to log on locally.
- Step 2** If you logged on to the Cisco Unity Administrator on the Cisco Unity server, right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Launch System Admin**.
- If you logged on to the Cisco Unity Administrator on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/web/sa**.

- Step 3** On the Cisco Unity Log On page, enter either the user name, password, and domain for the administration account that was selected when Cisco Unity was installed or an appropriate Windows domain account, and click **Log On**.
- 

## Exiting the Cisco Unity Administrator

### To Exit the Cisco Unity Administrator

---

- Step 1** Click the **Log Off** button on the lower left area of the Cisco Unity Administrator page.
- Step 2** Exit Internet Explorer.
- 

## Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator

Each Cisco Unity Administrator provides links to the Cisco Unity Administrator websites on other networked Cisco Unity servers. By clicking the links, you can access subscriber accounts and other Cisco Unity objects on another Cisco Unity server simply by browsing to the Cisco Unity Administrator on the Cisco Unity server on which those accounts and objects were created.

When you want to find a subscriber account, but do not know on which Cisco Unity server in the network the account was created, you can search for it from any subscriber page in the Cisco Unity Administrator on your local Cisco Unity server by using the Find icon.

When the Cisco Unity Administrator uses the Integrated Windows authentication method, you are not required to re-enter your Windows domain account credentials when you browse to another Cisco Unity Administrator website from your local Cisco Unity server. Note that this is true only if you log on to the Cisco Unity Administrator on your local server by using the credentials of a Windows domain account that is associated with a Cisco Unity subscriber account that has appropriate class of service (COS) rights on the remote Cisco Unity server.



### Note

COS rights specify which tasks, if any, administrators can do in the Cisco Unity Administrator. For example, some subscriber accounts can be associated with a COS that provides read-only access, or restricts administrators to access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords. (For more information, see the [“Class of Service System Access Settings”](#) section on page 14-5.)

---

However, when the Cisco Unity Administrator uses the Anonymous authentication method, you are prompted to enter authentication credentials regardless of the account you used to log on to the Cisco Unity Administrator on your local server. In this case, simply enter the appropriate credentials for the Cisco Unity Administrator website that you want to access.

---

### To Browse to Another Cisco Unity Administrator on a Networked Cisco Unity Server

- Step 1** Near the bottom of the navigation bar on the left side of the Cisco Unity Administrator interface, click **Unity Servers**. The Server Chooser page appears.
- Step 2** From the list, click the server that you want to access.
- Step 3** If prompted, enter the appropriate credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server that you selected.

---

Do the following procedure to use the Cisco Unity Administrator on your local Cisco Unity server to search for subscriber accounts on other Cisco Unity servers in the network.

### To Search for Subscriber Accounts Created on a Cisco Unity Server Other than Your Local Cisco Unity Server

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.
- Step 2** Click the **Find** icon.
- Step 3** Indicate whether to search by alias, extension, first name, or last name.
- Step 4** Enter the appropriate alias, extension, or name. You also can enter \* to display a list of all subscribers, or enter one or more characters or values followed by \* to narrow your search.
- Step 5** Check the **Search All Cisco Unity Servers** check box.
- Step 6** Click **Find**.
- Step 7** On the list of matches, click the name of the subscriber to display the record.
- Step 8** If prompted, enter the appropriate credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server on which the subscriber account was created. The subscriber profile page is displayed in the new browser window.

---

## About Cisco Unity Administrator Authentication

By default, IIS is configured so that the Cisco Unity Administrator uses the Integrated Windows authentication method (formerly called NTLM or Windows NT Challenge/Response authentication) to authenticate the user name and password. During installation, the installer determines whether to configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method instead.

Regardless of how the installer configured IIS, you can change the authentication method that the Cisco Unity Administrator currently uses at any time. (Note that the authentication method you choose to use also applies when accessing the Cisco Unity Status Monitor.) Before you make a change, however, first discuss it with the network administrator to confirm that the method you choose aligns with the

existing authentication scheme in your organization and that it addresses security concerns for your site. In addition, consider the advantages and disadvantages of using each authentication method with the Cisco Unity Administrator, as shown in [Table 2-1](#) and [Table 2-2](#).

Refer to the Microsoft website for general information on the strengths and weaknesses of Integrated Windows and Anonymous authentication.

**Table 2-1 Using Integrated Windows Authentication with the Cisco Unity Administrator**

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• User credentials are not sent across the network. Instead, Internet Explorer and Windows use a challenge/response mechanism to authenticate the user.</li> <li>• Integrated Windows authentication is the default in IIS; therefore, no additional setup is required.</li> </ul>	<ul style="list-style-type: none"> <li>• Windows cannot validate the identity of a user when the user is logged on to an untrusted domain, and therefore, denies the user access to the Cisco Unity Administrator. To mitigate this problem, configure each subscriber browser to prompt for a user name and password, allowing subscribers to enter the applicable credentials for the domain that the Cisco Unity server is in. Alternatively, you can establish trusts across domains.</li> <li>• When subscribers log on to the Cisco Unity Administrator from another domain, they will be prompted to re-enter their credentials every time that they want to use the phone as a recording and playback device for the Media Master.</li> </ul>

**Table 2-2 Using Anonymous Authentication with the Cisco Unity Administrator**

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• When subscribers log on to the Cisco Unity Administrator from another domain, they can enter the applicable credentials on the Cisco Unity Log On page for the domain that the Cisco Unity server is in. Thus, you do not need to configure each subscriber browser to prompt for a user name and password, nor do you need to establish trusts across domains.</li> <li>• When subscribers log on to the Cisco Unity Administrator from another domain, they are not prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master.</li> </ul>	<ul style="list-style-type: none"> <li>• When a subscriber enters credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. To solve this problem, you can set up Cisco Unity to use SSL.</li> <li>• Because Integrated Windows authentication is the IIS default, you must configure the system to use Anonymous authentication.</li> </ul>

If you decide to change the authentication method that is currently used by the Cisco Unity Administrator, see the [“Changing the Authentication Method Used by the Cisco Unity Administrator” section on page 2-8](#). For additional information on Cisco Unity authentication, see the following sections in this chapter:

- [How Integrated Windows Authentication for the Cisco Unity Administrator Works, page 2-6](#)—This section offers a high-level summary of the authentication process performed by Windows.
- [How Anonymous Authentication for the Cisco Unity Administrator Works, page 2-7](#)—This section offers a high-level summary of the authentication process performed by Cisco Unity, including a description of the credentials required by the Cisco Unity Log On page.

In addition, you may want to review the following related sections in other chapters:

- For information on using SSL to protect user credentials and subscriber data, see the [“Setting Up Cisco Unity to Use SSL”](#) chapter.
- For information on how authentication works with the Cisco Personal Communications Assistant (PCA), see the [“About Cisco Personal Communications Assistant Authentication”](#) section on page 7-7.

## How Integrated Windows Authentication for the Cisco Unity Administrator Works

When IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication, Cisco Unity does not authenticate the subscriber. Instead, the identity of the user is verified by Windows, as follows:

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS indicates that it cannot authenticate the user.
4. When Internet Explorer is configured to prompt for a user name and password, it displays a dialog box and waits for the subscriber to enter the Windows domain account credentials. When the subscriber enters the credentials, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it also sends IIS an encrypted message regarding the Windows domain account (based on the credentials that the subscriber entered in the dialog box).

When Internet Explorer is not configured to prompt for a user name and password, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it also sends IIS an encrypted message regarding the Windows domain account (based on the credentials that the subscriber had previously entered to log on to Windows).

In neither scenario is the user password—or any representation of the password—sent across the network, because authentication relies on Windows challenge/response.

5. If Windows can confirm the identity of the Windows domain user, IIS sends the user and domain name to Cisco Unity, and the process continues with Step 6.

If Windows cannot validate the identity of the Windows domain user (as would be the case if the subscriber logged on to an untrusted domain), Internet Explorer prompts the subscriber for a user name and password. Once again, the credentials are not sent across the network; instead, Internet Explorer sends IIS an encrypted message regarding the Windows domain account based on the credentials that are entered in the dialog box.

If authentication occurs, the process continues with Step 6. However, if Windows still cannot authenticate the user, Internet Explorer displays a message indicating that access to the website is denied because the domain account is unknown.

6. Cisco Unity checks to see that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber, and that the subscriber account has COS rights to access the Cisco Unity Administrator.

If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

## How Anonymous Authentication for the Cisco Unity Administrator Works

When IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, Cisco Unity authenticates the credentials that subscribers enter on the Cisco Unity Log On page, as follows:

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR\_<computer name> account. (This is the anonymous account that IIS uses by default for Anonymous authentication.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. The Log On page prompts subscribers to enter their Windows domain account credentials, as shown in [Table 2-3](#).

**Table 2-3 Cisco Unity Log On Page for Windows Credentials**

Field Name	Description
User Name	Subscribers enter the alias for the Windows domain account that is associated with their Cisco Unity subscriber account. (For example, a subscriber can enter <b>tcampbell</b> , or can enter the full path <b>tcampbell@&lt;domain name&gt;</b> .) If subscribers enter the full path, they do not need to complete the Domain field.
Password	Subscribers enter the password for their Windows domain account.
Domain	Subscribers enter the name of the domain in which their Windows domain account resides, unless they entered a full path in the User Name field, in which case they leave this field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To mitigate this security risk, you can set up Cisco Unity to use SSL.)
7. Cisco Unity requests authentication of the credentials from Windows.
8. If Cisco Unity can authenticate the Windows credentials, Cisco Unity then confirms that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber, and that the subscriber account has the proper COS rights. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the Windows credentials cannot be authenticated, or if the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

## Changing the Authentication Method Used by the Cisco Unity Administrator

Use the following procedure to configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method. Alternatively, if you want to change back to the Integrated Windows authentication method (which is the default), do the [“To Configure IIS so That the Cisco Unity Administrator Uses Integrated Windows Authentication”](#) procedure that follows.

### To Configure IIS so That the Cisco Unity Administrator Uses Anonymous Authentication

- 
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
  - Step 2** In the Internet Information Services window, double-click <System-name> to expand it.
  - Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
  - Step 4** In the Web Properties dialog box, click the **Directory Security** tab.
  - Step 5** Under Anonymous Access and Authentication Control, click **Edit**.
  - Step 6** In the Authentication Methods dialog box, check the **Anonymous Access** check box.
  - Step 7** Uncheck the **Integrated Windows Authentication** check box.
  - Step 8** Click **OK** to close the Authentication Methods dialog box.
  - Step 9** Click **OK** to close the Web Properties dialog box.
  - Step 10** Close the Internet Information Services window.
- 

### To Configure IIS so That the Cisco Unity Administrator Uses Integrated Windows Authentication

- 
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
  - Step 2** In the Internet Information Services window, double-click <System-name> to expand it.
  - Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
  - Step 4** In the Web Properties dialog box, click the **Directory Security** tab.
  - Step 5** Under Anonymous Access and Authentication Control, click **Edit**.
  - Step 6** In the Authentication Methods dialog box, uncheck the **Anonymous Access** check box.
  - Step 7** Check the **Integrated Windows Authentication** check box.
  - Step 8** Click **OK** to close the Authentication Methods dialog box.
  - Step 9** Click **OK** to close the Web Properties dialog box.
  - Step 10** Close the Internet Information Services window.
- 

## Cisco Unity Administrator Accounts

See the following sections:

- [About the Accounts That Can Be Used to Administer Cisco Unity, page 2-9](#)

- [Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator](#), page 2-10
- [Defining Subscriber Account Policies for Logons, Passwords, and Lockouts](#), page 2-11
- [Granting Administrative Rights to Other Cisco Unity Servers](#), page 2-11

## 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:

<b>Administration account</b>	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.
<b>A Windows domain account associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator</b>	<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"> <li>• Domain Admins group (when the Cisco Unity server is a domain controller)</li> <li>• Local Administrators group (when the Cisco Unity server is a member server)</li> </ul> <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 Windows credentials associated with the administration account 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, which 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 can be associated with a COS that provides read-only access, or restricts administrators to access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords. (For more information, see the [“Class of Service System Access Settings”](#) section on page 14-5.)

In addition to COS rights, subscriber accounts that are used to access the Cisco Unity Administrator must be associated with a Windows domain account.

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 2-10. 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 Windows domain 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 2-11.

As a best practice, it is recommended 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

If you choose to create additional subscriber accounts for the purposes of accessing the Cisco Unity Administrator, you can do so by completing the procedures in the [“Creating Subscriber Accounts”](#) chapter. Note that if you want administrators to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you need to add their Windows domain 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 Windows Domain 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 Windows Domain 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**.
- 

## Defining Subscriber Account Policies for Logons, Passwords, and Lockouts

When the Cisco Unity Administrator uses the Integrated Windows authentication method (which is the default), the account policy that is specified for each Windows domain account determines the following: how Windows handles situations when users attempt to log on to Windows and repeatedly enter incorrect passwords; the number of failed logon attempts that Windows allows before the user account cannot be used to access Windows; and the length of time that a user remains locked out.

If the Cisco Unity Administrator uses Anonymous authentication, you can use the settings on the Authentication page in the Cisco Unity Administrator to customize the logon, password, and lockout policies that Cisco Unity applies when subscribers use the Cisco Unity Administrator to access Cisco Unity. For details, see the [“Authentication Settings” section on page 28-11](#).

## 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 Windows domain accounts with a single Cisco Unity subscriber account. GrantUnityAccess maintains a table of the associated Windows domain accounts and Cisco Unity subscriber accounts, which 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 Windows domain 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 Windows domain account to the appropriate Admins group (see the [“Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator” section on page 2-10](#) for a detailed procedure.) Otherwise, the domain 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.
- You can associate multiple domain accounts with a single subscriber account.
- You can associate Windows domain 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 Windows domain 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. (For more information, see the “[Class of Service System Access Settings](#)” section on page 14-5.)
- 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 appropriate 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 2-12 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 a Windows domain 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 a Windows domain 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 Windows domain accounts are in a domain called NewYorkDomain. To associate their Windows domain 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 Windows domain 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 -?
```

