



The Cisco Unity Administrator

Overview: The Cisco Unity Administrator

The Cisco Unity Administrator is a website that you use to perform most administration 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 2-5](#)—This section explains the authentication methods that you can use with the Cisco Unity Administrator.
- [Cisco Unity Administrator Accounts, page 2-9](#)—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.
- [Using the Cisco Unity Administrator, page 2-14](#)—This section describes how to use the Cisco Unity Administrator to modify settings, find records, access online Help, and record greetings and names.
- [Exiting and Starting the Cisco Unity Software and Server, page 2-19](#)—This sections explains how to exit and start the Cisco Unity software and server.

Accessing and Exiting the Cisco Unity Administrator

See the following sections:

- [Logging On to the Cisco Unity Administrator, page 2-2](#)—This section includes procedures for logging on to the Cisco Unity Administrator according to the authentication method used by the Cisco Unity Administrator.
- [Exiting the Cisco Unity Administrator, page 2-3](#)—This section includes the procedure for logging off of the Cisco Unity Administrator.

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 either use 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 2-10.



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.

Consider the circumstance that you are not prompted for a name and password when you access the Cisco Unity Administrator (and when 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 26-11 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 the administration account 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 for a user name and password, enter the user name, password, and domain for the administration account 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 the user name, password, and domain for the administration account 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 user name, password, and domain for a Windows domain account that is associated with a Cisco Unity subscriber account which has class of service (COS) rights to access the Cisco Unity Administrator on the Cisco Unity server that you want to access.

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 a Cisco Unity subscriber account that has COS rights to 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 in order to use the Cisco Unity Administrator on your local Cisco Unity server to search for a particular subscriber account among all 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 name, alias, or extension. 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.



Note When you perform wildcard (*) searches, Cisco Unity may take several minutes to display results in the Cisco Unity Administrator. This is particularly true if your site has a large number of subscribers (approximately 1000 users or more) and/or dozens of servers. For this reason, it is important that you narrow the scope of wildcard searches.

- 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 to 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](#) lists the advantages and disadvantages of using Integrated Windows authentication with the Cisco Unity Administrator.

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

Advantages	Disadvantages
<ul style="list-style-type: none"> • User credentials are not sent across the network. Instead, Internet Explorer and Windows use a challenge/response mechanism to authenticate the user. • By default, IIS is already set up so that the Cisco Unity Administrator uses the Integrated Windows authentication method. 	<ul style="list-style-type: none"> • Windows cannot validate the identity of a user when the user is logged on to an untrusted domain. To mitigate this problem, configure each subscriber browser to prompt for a user name and password so that subscribers can enter the applicable credentials for the domain that the Cisco Unity server is in. Alternatively, you can establish trusts across domains. • When subscribers log on to the Cisco Unity Administrator from another domain, they are 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.

Table 2-2 lists the advantages and disadvantages of using Anonymous authentication with the Cisco Unity Administrator.

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

Advantages	Disadvantages
<ul style="list-style-type: none"> 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. 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. 	<ul style="list-style-type: none"> When a subscriber enters Windows domain account credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. To mitigate this problem, you can set up Cisco Unity to use SSL. By default, IIS is not set up for the Cisco Unity Administrator to use the Anonymous authentication method. You must configure it.

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 more 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, 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 5-7](#).

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:

- A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
- Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
- 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 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 sends IIS an encrypted message regarding the Windows domain account based on the credentials that the subscriber entered to log on to Windows.

In both scenarios, the user password—or any representation of the password—is not sent across the network because authentication relies on Windows challenge/response.

5. If Windows can confirm the identity of the Windows domain user, then 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 were entered in the dialog box. 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.
7. If a 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 that indicates 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.

- 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, they can enter tcampbell or they can enter the full path tcampbell@<domain name> .) If subscribers enter the full path for their alias, 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 for their alias in the User Name field. If that is the case, subscribers can leave this field blank.

- Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To mitigate this security problem, you can set up Cisco Unity to use SSL.)
- Cisco Unity requests authentication of the credentials from Windows.
- 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 COS rights to access the Cisco Unity Administrator. The process continues with Step 9.

If the credentials cannot be authenticated, Cisco Unity presents a web page indicating that the subscriber does not have permission to view the Cisco Unity Administrator website.

- 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.

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 procedure, [To configure IIS so that the Cisco Unity Administrator uses Integrated Windows authentication, page 2-9](#).

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** Double-click <System-name> to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Properties dialog box, click the **Directory Security** tab.
- Step 5** Under Anonymous Access and Authentication Control, click **Edit**.

- Step 6** 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 Default Web Site 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** Double-click <System-name> to expand it.
 - Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
 - Step 4** In the Properties dialog box, click the **Directory Security** tab.
 - Step 5** Under Anonymous Access and Authentication Control, click **Edit**.
 - Step 6** 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 Default Web Site 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 2-10](#)—This section describes the types of accounts that can be used to administer Cisco Unity.
- [Creating Subscriber Accounts that Can Be Used To Access the Cisco Unity Administrator, page 2-11](#)—This section outlines how you create the Cisco Unity subscriber account(s) that will be used to access the Cisco Unity Administrator.
- [Defining Subscriber Account Policies for Logons, Passwords, and Lockouts, page 2-12](#)—This section describes the options available if you want to define an account policy that applies when subscribers access the Cisco Unity Administrator.
- [Granting Administrative Rights to Other Cisco Unity Servers, page 2-12](#)—This section describes how you can use the GrantUnityAccess utility to grant one or more Windows domain accounts access to the Cisco Unity Administrator on one or more Cisco Unity servers.

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.
A Windows domain account associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator	<p>In order for administrators to be able 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>



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.

Consider using an alternative to the administrative 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 can be used to access the Cisco Unity Administrator must have the appropriate COS rights. COS rights specify which tasks, if any, administrators can perform in the Cisco Unity Administrator. For example, some subscriber accounts can be associated with a COS which denies access to the Cisco Unity Administrator altogether, while other accounts can be associated with a COS that provides read-only access, or restricts administrators from access to 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 12-5.)

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

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 that Can Be Used To Access the Cisco Unity Administrator”](#) section on page 2-11. However, if you prefer not to create an additional subscriber account for each administrator that 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 2-12.

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. 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 (only 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**. Administrators appears in the bottom list.
 - 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 (only 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** tab.
 - Step 6** Click **Add**.

- Step 7** In the Select Groups dialog box, in the top list, double-click **Domain Admins**. The name appears in the bottom list.
- Step 8** Click **OK** to close the Select Groups dialog box.
- Step 9** Click **OK** to close the Properties dialog box.
-

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, however, 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 26-11](#).

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 a Windows domain account 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 used by the Cisco Unity Administrator). In this way, Cisco Unity can determine whether to permit someone who is not a Cisco Unity subscriber to access 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 2-11](#) 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 another subscriber account that you create on each Cisco Unity server—one that has more limited COS rights to access the Cisco Unity Administrator. 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 12-5](#).)

- 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. For example, someone who administers Cisco Unity can be associated with two (or more) separate subscriber accounts: one for administration and one for personal use.

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 2-13](#) for an example of how this utility can be used.

To use the GrantUnityAccess utility

-
- Step 1** Log on to Windows on the Cisco Unity server by using the administration account 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>
```

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 -?
```

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, 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
```

Using the Cisco Unity Administrator

See the following sections:

- [Cisco Unity Administrator User Interface, page 2-14](#)
- [Cisco Unity Data, page 2-14](#)
- [Navigation, page 2-15](#)
- [Using the Online Help, page 2-15](#)
- [Command Icons, page 2-16](#)
- [Saving Data, page 2-16](#)
- [Finding Records, page 2-17](#)
- [Adding Records, page 2-17](#)
- [Recording Greetings and Names, page 2-18](#)

Cisco Unity Administrator User Interface

The Cisco Unity Administrator interface is divided into three areas.

Navigation bar	Located along the left side of the interface; contains links to categories of data pages.
Page	Where Cisco Unity data is entered and displayed. The page name is highlighted at the top of the page.
Title bar	Displays the name of the record or of the group of settings that appears on the page. The title bar also features command icons that initiate actions such as saving and finding records.

Cisco Unity Data

The Cisco Unity Administrator features links from the main navigation bar to five groupings of data, representing the subscribers and other Cisco Unity entities that you create on your local Cisco Unity server. The Cisco Unity Administrator does not allow you to view or modify the accounts of subscribers or other entities that were created on another Cisco Unity server.

The data groupings available from the Cisco Unity Administrator include:

Subscribers

These pages are used to enter data related to individual subscriber records. Also included are subscriber template pages, which contain settings that are applied to groups of subscribers. Settings include schedules, passwords, account permissions, call processing and transfer options, and distribution lists.

Call management

These pages are used to set how Cisco Unity answers, routes, transfers, and records calls. Settings include call routing, prerecorded caller interviews, call recording, and allowing or blocking certain dial strings.

Reports

These pages are used to generate reports on subscriber-based and system-based data. Reports can be generated for any of the data stored in the system, such as subscriber message activity, distribution lists, phone logs, disk storage, administration access, and port usage.

Network

These pages are used to add and view information about other Cisco Unity locations and to specify AMIS and/or Cisco Unity Bridge settings. Note that the network data pages are only available if Digital Networking, AMIS, and/or the Cisco Unity Bridge are installed.

System

These pages are used to customize and view numerous system features, including business schedules, annual holidays, recording settings, and languages.

Navigation

There are two levels of navigation in the Cisco Unity Administrator.

- At the first level, the navigation bar displays the data categories and provides links to each group of pages within those categories.
- At the second level, the navigation bar provides a link to each page within a selected group. Once a page is displayed, you can access individual records of that page type by clicking the Find icon. For more information, see the [“Finding Records” section on page 2-17](#).

Always use the Cisco Unity navigation bar, rather than the Internet Explorer navigation buttons, to move between pages. Otherwise, incorrect data will be displayed.

Using the Online Help

The Cisco Unity Administrator includes two types of context-sensitive online Help:

Online Documentation	Displays Help for the current page in the Cisco Unity Administrator.
Field Help	Displays descriptions for individual fields in the Cisco Unity Administrator.

To display Online Documentation

-
- Step 1** Click the **Online Documentation** icon in the upper right corner of the Cisco Unity Administrator. Cisco Unity displays the relevant page from the *Cisco Unity System Administration Guide* in a separate window.
- Step 2** If desired, click a link included in the displayed topic or listed in the Contents to browse to another topic.
-








To display Field Help

-
- Step 1** Click the **Field Help** icon in the upper right corner of the Cisco Unity Administrator. Cisco Unity displays a question mark next to each field for which Help is available.

- Step 2** For help on a field, click the question mark next to that field.
- Step 3** To turn Field Help off, click the **Field Help** icon in the upper right corner of the Cisco Unity Administrator.

Command Icons

The command icons are located in the title bar, which is in the upper-right area of each Cisco Unity Administrator page.

	Save icon	Saves data that you have entered. Available only when you have changed the record.
	Find icon	Opens the Find window, where you search for existing records in the displayed category.
	Add icon	Opens the Add window, where you enter information to create a new record in the displayed category.
	Delete icon	Deletes the displayed record.
	Run icon	Generates a report. Available only on Reports pages.
	Online Documentation icon	Provides in-depth descriptions and conceptual Help and includes an index and glossary.
	Field Help icon	Displays question marks next to fields and buttons for which Help is available.

Saving Data

Save newly entered data by clicking the Save icon. Cisco Unity requires you to save new data before moving to another record or to another part of the Cisco Unity Administrator. The following cues remind you when the displayed record contains unsaved data:

- The Save icon is enabled.
- An asterisk is displayed on the title bar next to the record name.
- If you attempt to leave a changed record without saving it, Cisco Unity prompts you to save the record.

Finding Records

A record is the group of settings or collection of data for an individual subscriber, class of service (COS), or other Cisco Unity entity. For example, a subscriber record contains the subscriber account data.

To find a subscriber record

- 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 name, alias, or extension. 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.



Note When you perform wildcard (*) searches, Cisco Unity may take several minutes to display results in the Cisco Unity Administrator. This is particularly true if your site has a large number of subscribers (approximately 1000 users or more) and/or dozens of servers. For this reason, it is important that you narrow the scope of wildcard searches.

- Step 5** Click **Find**.
 - Step 6** On the list of matches, click the name of the subscriber to display the record.
-

To find other types of records

- Step 1** In the Cisco Unity Administrator, go to any page of the appropriate record type.
 - Step 2** Click the **Find** icon.
 - Step 3** Enter the appropriate name. You also can enter * to display a list of all records, or enter one or more characters followed by * to narrow your search.
 - Step 4** Click **Find**.
 - Step 5** On the displayed list, double-click the appropriate record.
-

Adding Records

Always enter information for a new record in an Add window. Entering new record information on an existing page will change the displayed record rather than create a new record.

To add a record

- Step 1** Click the **Add** icon from any page of the appropriate record type.
- Step 2** In the window that is displayed, enter basic identifying information, such as the name of the record.
- Step 3** Indicate whether this record is new or based on an existing one. If based on an existing record, click the name of that record on the list.

Step 4 Click **Add**.

Recording Greetings and Names

You can record names for subscribers, public distribution lists, private lists, and call handlers (including interview handlers and directory handlers), and greetings for subscribers and call handlers, from pages within the Cisco Unity Administrator. You can also record greetings for call handlers by using the Cisco Unity phone conversation.

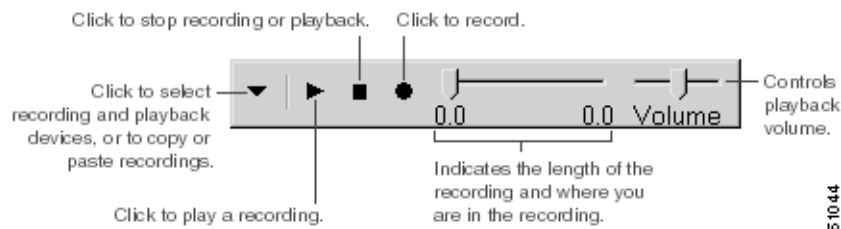
Subscribers can also record their own names and personal greetings by accessing the Cisco Unity conversation by phone, or the Cisco Unity Assistant website. (Note that in version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA.) For more information on setting up subscribers to record, see the [“Setting Up Recording and Playback Devices”](#) section on page 5-9.

Before you begin recording subscriber and call handler names and greetings, consider the following:

- Who will record the greetings? For example, do you want to hire a professional to record the call handler greetings?
- What will the greetings say? Write detailed scripts for the greeting of each call handler greeting before beginning to record.
- Will you use the phone or a computer microphone to make and play your recordings? The phone offers the best sound quality for recordings.

The Media Master control bar appears on each page of the Cisco Unity Administrator where recordings can be made. It allows you to make and play recordings, either with a phone or with your computer microphone and speakers, by clicking the Media Master controls. The Media Master control bar relies on DCOM (Distributed Component Object Model), and does not work through a firewall. It also requires that your browser is able to download and run ActiveX controls.

Figure 2-1 Media Master Control Bar



When determining the recording and playback device that you want to use to manage greetings and subscriber names in the Cisco Unity Administrator, consider the following:

- The phone serves as the default recording and playback device for the Media Master.
- In order to use the phone as a recording and playback device, Cisco Unity must have at least one port designated TRAP Connection per session on the System > Ports page. See the [“Voice Messaging Port Settings”](#) section on page 26-13 for more information.

Use the following procedure to change the recording and playback device used by the Media Master.

To select a recording and playback device

-
- Step 1** Go to any Media Master control bar in the Cisco Unity Administrator.
- Step 2** From the Options menu, click **Playback Devices**.
- Step 3** Select the device that you want to use from the list.
- The <Use Preferred Device> option refers to the recording and playback devices that you have already selected for your computer (click Settings > Control Panel > Sounds and Multimedia on the Windows Start menu to set your preferred devices). See the Windows online Help for more information on preferred recording and playback devices.
- Step 4** From the Options menu, click **Recording Devices**, and repeat **Step 3**. The Options menu button is on the far left of the Media Master control bar. See [Figure 2-1](#).
-

Table 2-4 Media Master Control Bar Options Menu

Option	Meaning
New	Use this option to start a new recording.
Paste	Paste a copied voice message, name, or greeting recording into this recording. Use the Media Master Copy option to copy the recording that you want to paste.
Paste from file	Paste a WAV file that you have stored on your computer into this recording.
Copy	Copy this recording so that you can paste into another voice message, name, or greeting recording. Use the Media Master Paste option to paste the copied recording.
Copy to file	Save this recording as a WAV file to location that you specify on your computer.
Playback devices	Select the phone or the multimedia speakers used with your computer. If you select the phone, you must click Options on the Media Master Control Bar Options menu and enter an extension and server name.
Recording devices	Select the phone or the multimedia microphone used with your computer. Note that if you select the phone, you must click Options on the Media Master Control Bar Options menu and enter an extension and server name. Use the phone to get the best sound quality.
Options	Enter an extension and the Cisco Unity server name here when you want to use the phone as the playback and recording device for the Media Master. Note that you must manually change the server name field during failover and fallback. Refer to the <i>Cisco Unity Failover Configuration and Administration Guide</i> for details, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guide_books_list.html .

Exiting and Starting the Cisco Unity Software and Server

The following sections provide instructions on exiting the Cisco Unity software, shutting down and restarting the Cisco Unity server, and starting the Cisco Unity software.

Exiting the Cisco Unity Software

This section provides two procedures for exiting the software: from the Cisco Unity server and from another computer. (For details on the accounts that you use to log on to the Cisco Unity server and the Cisco Unity Status Monitor, see the [“About the Accounts that Can Be Used To Administer Cisco Unity” section on page 2-10.](#))



Caution

Do not use Kill av*.* to exit the Cisco Unity software. Kill av*.* does not stop all Cisco Unity services, and may cause problems with upgrades from Cisco Unity version 2.x.

To exit the Cisco Unity software from the Cisco Unity server

-
- Step 1** If the system uses the automated attendant, route all calls to the operator.
 - Step 2** Log on to Windows on the Cisco Unity server by using either the administration account or an appropriate Windows domain account.
 - Step 3** Right-click the **Cisco Unity** icon in the status area of the taskbar.
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click **AvCsTrayStatus.exe**.)
 - Step 4** Click **Stop Cisco Unity**. Cisco Unity stops running when all calls are finished, and an “X” appears in the Cisco Unity icon.
 - Step 5** Press **Ctrl-Alt-Delete**, then lock or log off Windows to prevent access by unauthorized users.
-

To exit the Cisco Unity software from another computer

-
- Step 1** If the system uses the automated attendant, route all calls to the operator.
 - Step 2** When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following sub-steps. Otherwise, proceed to [Step 3](#).
 - a.** Log on to Windows by using either the administration account or an appropriate Windows domain account.
 - b.** Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
 - c.** If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or an appropriate Windows domain account.
 - d.** Proceed to [Step 5](#).
 - Step 3** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following:
 - a.** Log on to Windows by using any domain account that has the right to log on locally.
 - b.** Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
 - Step 4** On the Cisco Unity Log On page, enter the user name, password, and domain for the administration account or an appropriate Windows domain account.

- Step 5** In the Cisco Unity Status Monitor, under Shutting Down Cisco Unity, choose a method:
- Cisco Unity stops running after all calls are finished.
 - Cisco Unity interrupts calls in progress with a voice message, disconnects all calls, then stops running.
- Step 6** Click **Shut Down**.

Shutting Down or Restarting the Cisco Unity Server



Note

Restarting the Cisco Unity server may result in delayed message notification and message waiting indication until MAPI logon to all subscriber mailboxes has been completed. Depending on the size of the subscriber database, it could take several hours to complete the MAPI logon.

If the Cisco Unity system has an expansion chassis or is set up for failover, consider the following before shutting down or restarting the Cisco Unity server:

Expansion chassis connected to the Cisco Unity server	When both the expansion chassis and the Cisco Unity server are turned off, turn on the expansion chassis before you turn on the server. Otherwise, the server may not detect the voice cards in the expansion chassis.
Cisco Unity failover	<ul style="list-style-type: none"> • When both servers are running and the active server is shut down, the inactive server becomes active. • When neither server is running, the first server started becomes the active server. • When the secondary server is active and configured for automatic failback, and the primary server is also running, the secondary server attempts failback on the failback schedule.

To shut down or restart the Cisco Unity server

- Step 1** Exit the Cisco Unity software, if it is running, by using a procedure in the [“Exiting the Cisco Unity Software”](#) section on page 2-20.
- Step 2** On the Windows Start menu, click **Shut Down**.
- Step 3** Click **Shut Down** or **Restart**.

During a restart, the Cisco Unity software starts automatically.

When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon in the status area of the taskbar.

When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon in the status area of the taskbar.

Starting the Cisco Unity Software

This section provides two procedures for starting the software: from the Cisco Unity server and from another computer. (For details on the accounts that you use to log on to the Cisco Unity server and the Cisco Unity Status Monitor, see the [“About the Accounts that Can Be Used To Administer Cisco Unity” section on page 2-10.](#))

Cisco Unity is a Windows service that is configured to start automatically when you turn on or restart the server. Do one of the following procedures only if you exited the Cisco Unity software but did not restart the server.

Exchange must be running before you start the Cisco Unity software, whether or not Exchange is installed on the Cisco Unity server:

Exchange on another server	Exchange must be running on the Exchange server that Cisco Unity connects with.
Exchange on the Cisco Unity server	If you exited Exchange manually but did not restart the Cisco Unity server, start Exchange first. (Exchange starts automatically when you turn on or restart the server.)

If Exchange stops for any reason while Cisco Unity is running, Cisco Unity will continue to take messages.

To start the Cisco Unity software from the Cisco Unity server

-
- Step 1** Log on to Windows on the Cisco Unity server by using either the administration account or an appropriate Windows domain account.
- Step 2** Right-click the **Cisco Unity** icon in the status area of the taskbar.
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click **AvCsTrayStatus.exe**.)
- Step 3** Click **Start Cisco Unity**.
When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon.
When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon.
- Step 4** Press **Ctrl-Alt-Delete**, then lock or log off Windows to prevent access by unauthorized users.
- Step 5** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-

To start the Cisco Unity software from another computer

-
- Step 1** When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following sub-steps. Otherwise, proceed to [Step 2](#).
- a. Log on to Windows by using either the administration account or an appropriate Windows domain account.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.

- c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or an appropriate Windows domain account.
 - d. Proceed to [Step 4](#).
- Step 2** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following:
- a. Log on to Windows by using any domain account that has the right to log on locally.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** On the Cisco Unity Log On page, enter the user name, password, and domain for the administration account or an appropriate Windows domain account.
- Step 4** In the Cisco Unity Status Monitor, click the **System Status** icon (the first icon), at the top of the page.
- Step 5** Click **Start**.
- Step 6** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-

