



CHAPTER 10

Setting Up Authentication for the Cisco Unity Administrator

In this chapter, you do the following tasks in the order listed:

1. Determine the authentication method that you want to use for the Cisco Unity Administrator. See the [“Determining the Authentication Method to Use for the Cisco Unity Administrator”](#) section on page 10-1.
2. Configure IIS so that the Cisco Unity Administrator and Status Monitor use the Anonymous authentication method, if applicable. See the [“Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication”](#) section on page 10-5.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining the Authentication Method to Use for the Cisco Unity Administrator

The Cisco Unity Administrator is the website used to do most administration tasks, including: 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.

To access the Cisco Unity Administrator, Cisco Unity requires that the identity of the administrator is authenticated by a name and password. You can choose which IIS authentication method that you want to use for the Cisco Unity Administrator. (Note that the authentication method you choose also applies to the Cisco Unity Status Monitor.)



Note

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

The following three subsections discuss the available authentication methods and how they work:

- [Authentication Methods Available for the Cisco Unity Administrator, page 10-2](#)

- [How Integrated Windows Authentication Works with the Cisco Unity Administrator, page 10-3](#)
- [How Anonymous Authentication Works with the Cisco Unity Administrator, page 10-4](#)

Authentication Methods Available for the Cisco Unity Administrator

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. If you prefer, you can configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method instead.

To determine which authentication method to use, first discuss it with the network administrator to confirm that the method you choose aligns with the existing authentication scheme in the organization and addresses security concerns for the site. In addition, consider the advantages and disadvantages of using each authentication method with the Cisco Unity Administrator, as shown in [Table 10-1](#) and [Table 10-2](#).

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

[Table 10-1](#) lists the advantages and disadvantages of using Integrated Windows authentication with the Cisco Unity Administrator.

Table 10-1 *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 solve 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 10-2 lists the advantages and disadvantages of using Anonymous authentication with the Cisco Unity Administrator.

Table 10-2 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 solve this problem, set up Cisco Unity to use SSL. By default, IIS is not set up so that the Cisco Unity Administrator uses the Anonymous authentication method. You must configure it.

How Integrated Windows Authentication Works with the Cisco Unity Administrator

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.

- 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.
- 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. Once 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.

- 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 Works with the Cisco Unity Administrator

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.

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 for Anonymous authentication by default.)
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 10-3](#).

Table 10-3 Cisco Unity Log On Page for Windows Credentials

Field Name	Description
User Name	Subscribers must 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 must enter the password for their Windows domain account.
Domain	Subscribers must 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 the field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To solve this security problem, 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 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 that indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

9. 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, which indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication

**Note**

If you decided that the Cisco Unity Administrator will use the Integrated Windows authentication method, skip this section.

This section contains two procedures. Do the applicable procedure, depending on whether the Cisco Unity server is running Windows Server 2003 or Windows 2000 Server.

To Configure IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows Server 2003)

- Step 1** On the Windows Start menu, click **Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the left pane, right-click **Application Pools**, and click **Properties**.
- Step 3** In the Application Pools Properties dialog box, click the **Identity** tab.
- Step 4** In the Predefined list, click **Local System**.
- Step 5** Click **OK** to close the Application Pools Properties dialog box.
- Step 6** In the IIS Manager message box, click **Yes** to confirm that you want to run this application pool as Local System.
- Step 7** In the left pane of Internet Information Services (IIS) Manager, expand **Web Sites > Default Web Site**.
- Step 8** Right-click **SAWeb**, and click **Properties**.
- Step 9** In the SaWeb Properties dialog box, click the **Directory Security** tab.
- Step 10** In the Authentication and Access Control section, click **Edit**.
- Step 11** In the Authentication Methods dialog box, check the **Enable Anonymous Access** check box.
- Step 12** Uncheck the **Integrated Windows Authentication** check box.
- Step 13** Click **OK** to close the Authentication Methods dialog box.
- Step 14** Click **OK** to close the SaWeb Properties dialog box.
- Step 15** Repeat [Step 8](#) through [Step 14](#) for the following virtual directories:
 - Status
 - StatusXml
 - Web
- Step 16** In the left pane, click **StatusXml**.
- Step 17** In the right pane, right-click **AvXml.dll**, and click **Properties**.

- Step 18** In the AvXml.dll Properties dialog box, click the **File Security** tab.
 - Step 19** In the Authentication and Access Control section, click **Edit**.
 - Step 20** In the Authentication Methods dialog box, check the **Enable Anonymous Access** check box.
 - Step 21** Uncheck the **Integrated Windows Authentication** check box.
 - Step 22** Click **OK** to close the Authentication Methods dialog box.
 - Step 23** Click **OK** to close the AvXml.dll Properties dialog box.
 - Step 24** Close Internet Information Services (IIS) Manager.
-

To Configure IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows 2000 Server)

- 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 Properties dialog box, set the authentication method for the Web directory:
 - a. Click the **Directory Security** tab.
 - b. Under Anonymous Access and Authentication Control, click **Edit**.
 - c. In the Authentication Methods dialog box, check the **Anonymous Access** check box.
 - d. Uncheck the **Integrated Windows Authentication** check box.
 - e. Click **OK** to close the Authentication Methods dialog box.
 - f. Click **OK** to close the Properties dialog box.
 - Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
 - Step 6** Repeat [Step 4](#) to set the authentication method for the SAWeb directory.
 - Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
 - Step 8** Repeat [Step 4](#) to set the authentication method for the Status directory.
 - Step 9** Under Default Web Site, click **AvXML**.
 - Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
 - Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.dll.
 - Step 12** Close the Internet Information Services window.
-