



Setting Up Authentication for the Cisco Unity Administrator

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

1. Determine which 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 10-2.
2. Configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method, if applicable. See the [“Configuring IIS So That the Cisco Unity Administrator Uses Anonymous Authentication”](#) section on page 10-9.

When you are finished with this chapter, return to the applicable task list for your platform type to continue installing the Cisco Unity system correctly:

- [Task List for Installing Cisco Unity on a Qualified Server, page 1-2](#)
- [Task List for Installing Cisco Unity in the Cisco ICS 7750, page 1-7](#)



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 to use 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 to log on to the Cisco Unity Administrator.

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

- [Authentication Methods Available for the Cisco Unity Administrator, page 10-3](#)
- [How Integrated Windows Authentication for the Cisco Unity Administrator Works, page 10-5](#)
- [How Anonymous Authentication for the Cisco Unity Administrator Works, page 10-6](#)

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"> • Subscribers can choose whether to enter their Domino or Windows credentials on the Cisco Unity Log On page. If subscribers use their Domino credentials, they do not need to have Windows domain accounts created for them. However, if subscribers have Windows domain accounts, they can use their Windows credentials to access the Cisco Unity Administrator if the Domino server goes down, for example. • 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 Domino 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. • 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, you can 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 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.

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. 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.

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.

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. By default, the Log On page prompts subscribers to enter the Domino credentials, as shown in [Table 10-3](#). However, subscribers can click the Log On Using Windows Authentication link provided on the Log On page to browse to another Log On page (as shown in [Table 10-4](#)) on which they can enter their Windows domain account credentials.

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

Field Name	Description
Full Name	Subscribers must enter the full Lotus Notes user name that is associated with their Cisco Unity subscriber account. The full name consists of the user name, any organizational units that the Domino Person document resides in, and the IBM Domino certifier domain. (For example, subscribers can enter Terry Campbell/Sales/Cisco.)
Password	Subscribers must enter the Internet password for their Domino user account.

Table 10-4 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, you can set up Cisco Unity to use SSL.)
7. When the subscriber has entered Domino credentials on the Log On page, Cisco Unity searches the Domino Address Book for a Person document associated with the user name that the subscriber entered on the Log On page.

Once the user name is found, Cisco Unity retrieves the encrypted password from the Person document and compares it with the password that the subscriber entered on the Log On page. The process continues with Step 9.

(Note that by default, the connection between the Cisco Unity server and the Domino server is not encrypted. Refer to the Domino documentation for details on encrypting network data on a server port. It is also a good idea to discuss potential performance issues with the Domino administrator for the organization before enabling encryption on the Domino server.)

8. When the subscriber has entered Windows credentials on the Log On page, Cisco Unity requests authentication of the credentials from Windows. The process continues with Step 10.
9. If Cisco Unity can authenticate the Domino credentials, Cisco Unity confirms that there is a subscriber account associated with the Domino Person document used to authenticate the subscriber, and that the subscriber account has the proper COS rights. The process continues with Step 11.

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.

10. 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 11.

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.

11. 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 Uses Anonymous Authentication

Do the following procedure to configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method.

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.
-

■ Configuring IIS So That the Cisco Unity Administrator Uses Anonymous Authentication