



# CHAPTER 7

## Securing Accounts

---

In this chapter, you will find descriptions of potential security issues related to securing accounts; information on any actions you need to take; recommendations that will help you make decisions; ramifications of the decisions you make; and in many cases, best practices.

See the following sections:

- [Understanding Accounts, page 7-1](#)
- [Best Practices for Accounts That Are Used to Access the Cisco Unity Administrator, page 7-2](#)
- [Best Practices for Accounts That Are Used to Access the Cisco Unity Server, page 7-3](#)
- [Best Practices When Deleting Cisco Unity Subscriber Accounts, page 7-4](#)
- [Securing the Account That Was Used to Install Cisco Unity, page 7-4](#)
- [Securing the Directory Services and Message Store Services Accounts, page 7-4](#)
- [Best Practices for Securing Default Accounts, page 7-5](#)

For the latest requirements for Cisco Unity service accounts and permissions, see the applicable Cisco Unity installation guide, available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html).

## Understanding Accounts

Each Cisco Unity subscriber account has a corresponding Active Directory domain account. Depending on the method you use to create Cisco Unity subscriber accounts, the Active Directory account may be created automatically.

If the Active Directory account for a subscriber has been disabled, the subscriber:

- Cannot access the Cisco Personal Communications Assistant (PCA).
- Cannot access the Cisco Unity Administrator.
- Cannot use the phone as a recording and playback device for the Media Master.

### Best Practices

- On Cisco Unity systems that are configured for Voice Messaging, if you do not want subscribers to have access to the Cisco PCA, the Cisco Unity Administrator, or the Media Master, we recommend that you disable Active Directory accounts for the subscribers.

**Note**

If you have Cisco Unity create Active Directory accounts at the same time that you create Cisco Unity subscribers, you can configure Cisco Unity so the Active Directory accounts are created disabled. For more information, in Cisco Unity Tools Depot, run the Advanced Settings Tool, and review the help for the setting “Administration - Disable AD accounts created by Unity.”

- Depending on how subscriber accounts are created, all of the corresponding Active Directory domain accounts may be created with the same default password. We recommend that you change these passwords immediately—before subscribers start to use Cisco Unity—to prevent subscribers from accessing accounts other than their own.

For information on Active Directory passwords, see the “[Ensuring That Subscribers Are Initially Assigned Unique and Secure Windows Passwords](#)” section on page 9-4.

## Best Practices for Accounts That Are Used to Access the Cisco Unity Administrator

The Cisco Unity Administrator is a website that you use to do most administrative tasks. Depending on the associated class of service rights, accounts that can be used to access the Cisco Unity Administrator can offer access to settings used to define how Cisco Unity works for individual subscribers (or for a group of subscribers), system schedules, call management options, and other important data. If your site is comprised of multiple Cisco Unity servers, an account used to access one Cisco Unity Administrator may be able to gain access to the other Cisco Unity Administrators as well. To secure access to the Cisco Unity Administrator, consider the following best practices.

### Best Practice: Limit the Use of the Administration Account

Until you create a Cisco Unity subscriber account specifically for the purpose of administering Cisco Unity, you log on to the Cisco Unity Administrator by using the Active Directory credentials that are associated with the administration account that was selected when Cisco Unity was installed. The administration account is automatically associated with a class of service that offers 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. For this reason, you should limit the use of this highly privileged account to only one or to very few individuals.

As an alternative to the administration account, you can create additional accounts that have class of service rights to access the Cisco Unity Administrator, but offer fewer privileges. If your organization depends on more than person to administer Cisco Unity, you can modify the class of service rights for each account so that access to the Cisco Unity Administrator is appropriate to the administrative tasks that each person performs. By creating additional accounts, you also ensure that additional accounts are available to access the Cisco Unity Administrator in the event that the administration account is deleted or corrupted.

To learn about the ways in which you create additional accounts or grant administrative rights to existing accounts so that they can be used to access the Cisco Unity Administrator, see the “About the Accounts That Can Be Used to Administer Cisco Unity” section in the “Managing Cisco Unity Administrator Accounts” chapter of the *System Administration Guide for Cisco Unity*. The guide is available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html).

**Best Practices: Use Class of Service to Restrict Access to the Cisco Unity Administrator**

When modifying class of service settings and assignments to secure access to the Cisco Unity Administrator, consider the following best practices:

- Do not modify the system access settings for the Default Administrator class of service. Instead, reassign subscriber accounts to a new class of service that offers an appropriate level of access to the Cisco Unity Administrator. For example, you may want to associate an account with a class of service that offers read-only access to the Cisco Unity Administrator, or only offers access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords.
- Verify that at least one subscriber account is assigned to the Default Administrator class of service. If you do not have at least one Active Directory account with class of service rights to access the Cisco Unity Administrator, you may lose the ability to administer Cisco Unity, and be required to reinstall.
- By default, the Default Subscriber class of service prohibits access to the Cisco Unity Administrator, and should not be changed to allow it. Instead, use it to offer access to Cisco Unity features and applications that are more appropriate to end users.

To learn how to create and modify classes of service, see the “Managing Classes of Service” chapter of the *System Administration Guide for Cisco Unity*. The guide is available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html).

**Best Practice: Do Not Use Other Accounts to Access the Cisco Unity Administrator**

Cisco Unity administrators should not use the same account to access the Cisco Unity Administrator that they use to log on to the Cisco Personal Communications Assistant (PCA). In addition, administrators should not use Cisco Unity service accounts to access the Cisco Unity Administrator.

## Best Practices for Accounts That Are Used to Access the Cisco Unity Server

When you install Cisco Unity, you can choose the drive and directory where it is installed. By default, it is installed in the CommServer directory.

By default, the Active Directory accounts that Cisco Unity services log on as have Full Control access to the CommServer directory because they belong either to the local Administrators group (when the Cisco Unity server is a member server) or the Domain Admins group (when the Cisco Unity server is a domain controller). However, we recommend that you not use these accounts as administration accounts. Instead, we recommend that you designate a highly privileged account for use by a system administrator, and grant Full Control permissions to the Cisco Unity directories and files so that the account can be used for administration and troubleshooting.

**Best Practice**

Verify that other domain accounts used by Cisco Unity system administrators are restricted to read-only access, and verify that all Cisco Unity subscribers and any other domain accounts and groups have no access rights to the directories or files on the Cisco Unity server. To restrict access, exclude the System Group Everyone from the default user permissions for C:\ or the root of any other drive on the Cisco Unity server. Instead, as applicable, assign authenticated users. Finally, verify that no explicitly privileged assignments have been made to individual groups or accounts.

# Best Practices When Deleting Cisco Unity Subscriber Accounts

Deleting the Cisco Unity subscriber account does not delete the Active Directory account (if there is one) or the Exchange mailbox for that subscriber. You can delete the Active Directory account and Exchange mailbox separately after you delete the subscriber account in the Cisco Unity Administrator.

## Securing the Account That Was Used to Install Cisco Unity

Cisco Unity Setup creates a variety of objects in Active Directory and also creates mailboxes in Exchange. As a result, the account that is used to install Cisco Unity requires a broad range of user rights, group memberships, and Active Directory permissions. If you are concerned that an account with so many permissions will be available after the Cisco Unity installation is complete, you can disable the account in Active Directory Users and Computers.

We recommend that you not delete the account because when you upgrade to a later version of Cisco Unity you will again need an installation account with the same permissions. If you delete the current account, you will have to create another, re-run the Cisco Unity Permissions wizard to set the required permissions, and manually delegate Exchange administrative control to the account.

For more information on the permissions set by the Permissions wizard, see the *Permissions Granted by the Cisco Unity 5.0(1)+ Permissions Wizard* Help. The Help file is available at [http://www.ciscounitytools.com/App\\_PW\\_501.htm](http://www.ciscounitytools.com/App_PW_501.htm).

## Securing the Directory Services and Message Store Services Accounts

**Added October 23, 2008**

The Permissions wizard adds the directory services and message store services accounts to the local Administrators group. Cisco Unity requires most of the permissions that are associated with being a member of the local Administrators group, and denying these permissions will prevent Cisco Unity from functioning properly. However, if you want, you can deny the accounts the right to log on locally. Do the following procedure.

### To Deny the Directory Services and Message Store Services Accounts the Right to Log On Locally

- 
- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Local Security Policy**.
  - Step 2** In the left pane of the Local Security Policy MMC, expand **Local Policies**, and click **User Rights Assignment**.
  - Step 3** In the right pane, right-click **Deny Log on Locally**, and click **Properties**.
  - Step 4** In the Deny Logon Locally Properties dialog box, on the Local Security Settings tab, click **Add User or Group**, select the directory services and message store services accounts, and click **OK**.
  - Step 5** In the Deny Logon Locally Properties dialog box, click the names of the two accounts that you selected in **Step 4**, and click **OK**.

In the right pane of the Local Security Policy MMC, the Deny Log on Locally policy now lists the two accounts in the Security Setting column.

---

# Best Practices for Securing Default Accounts

Table 7-1 lists the Active Directory accounts and Exchange mailboxes that are created by Cisco Unity, when they are created, and best practices for securing them.

**Table 7-1** Considerations for Securing Default Cisco Unity Accounts, Active Directory Accounts, or Exchange Mailboxes

Cisco Unity Subscriber Account	Active Directory Account and Exchange Mailbox	When Created	Best Practice
Example Administrator	EAdministrator	At installation	<p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Administrator template, which is used to create the Example Administrator account and the corresponding Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the Active Directory Example Administrator account may still have the default password. This account is created in a disabled state.</p> <p>For systems that were upgraded from Cisco Unity 4.0(3) or earlier:</p> <ul style="list-style-type: none"> <li>• Change the Active Directory password.</li> <li>• Change the phone password.</li> <li>• Change the class of service to remove administration rights.</li> </ul> <p>Optionally, you can disable (but not delete) this account.</p>
Example Subscriber	ESubscriber	At installation (for Cisco Unity version 4.0(2) and earlier only)	If present, delete this subscriber account and the associated Active Directory account and Exchange mailbox.
Unity Messaging System (not visible in the Cisco Unity Administrator)	Unity_<servername>	At installation	<p>For systems that were upgraded from a version prior to Cisco Unity 4.0(5), change the Active Directory password.</p> <p>Optionally, you can disable (but not delete) this account. This account is created in a disabled state when you install Cisco Unity.</p>

**Table 7-1** Considerations for Securing Default Cisco Unity Accounts, Active Directory Accounts, or Exchange Mailboxes (continued)

Cisco Unity Subscriber Account	Active Directory Account and Exchange Mailbox	When Created	Best Practice
None	UAmis_<servername>	When configuring AMIS	<p>If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the UAmis account may have a default password. This account is disabled by default.</p> <p>For systems that were upgraded from Cisco Unity 4.0(5) or earlier, change the Active Directory password.</p> <p>Optionally, you can disable this account. Do not hide this account from the Exchange address book if using the Voice Connector for Exchange 2000 or Exchange 2003 version 11.0(2) or earlier. Doing so may prevent AMIS networking from working properly. Do not delete this account, even if AMIS is no longer in use.</p>
None	UOmni_<servername>	When configuring the Cisco Unity Bridge	<p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the UOmni Active Directory account. If the system was upgraded from Cisco Unity version 4.0(3) or earlier, the UOmni account may still have a default password. By default, this account is disabled, hidden from the Exchange address book, and configured to appear in AD Advanced View only.</p> <p>For Cisco Unity systems that were upgraded from version 4.0(3) or earlier, change the Active Directory password.</p> <p>Optionally, you can disable this account. Do not hide this account from the Exchange address book if using the Cisco Unity Voice Connector for Microsoft Exchange 2000 or Exchange 2003 version 11.0(2) or earlier. Doing so may prevent Bridge networking from working properly. Do not delete this account, even if Bridge Networking is no longer in use.</p>

**Table 7-1** *Considerations for Securing Default Cisco Unity Accounts, Active Directory Accounts, or Exchange Mailboxes (continued)*

Cisco Unity Subscriber Account	Active Directory Account and Exchange Mailbox	When Created	Best Practice
None	USbms_<servername>	At installation	<p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the account. By default, this account is disabled, hidden from the Exchange address book, and configured to appear in AD Advanced View only.</p> <p>Do not delete this account, even if broadcast messaging is not in use.</p>
None	UVpim_<servername>	When configuring VPIM	<p>The Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the account. By default, this account is disabled, hidden from the Exchange address book, and configured to appear in AD Advanced View only.</p> <p>Do not delete this account, even if VPIM is no longer in use.</p>

