



Securing Accounts

Introduction

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 6-1](#)
 - [Best Practices for Accounts That Are Used to Access the Cisco Unity Administrator, page 6-2](#)
 - [Best Practices for Accounts That Are Used to Access the Cisco Unity Server, page 6-3](#)
 - [Best Practices When Deleting Cisco Unity Subscriber Accounts, page 6-4](#)
 - [Securing the Account That Was Used to Install Cisco Unity, page 6-4](#)
 - [Best Practices for Securing Default Accounts, page 6-5](#)

For the latest requirements for Cisco Unity service accounts and permissions, refer to the applicable Cisco Unity installation guide, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Understanding Accounts

Each Cisco Unity subscriber account generally has a corresponding Active Directory domain account or a Windows NT user account:

When the partner Exchange server is running Exchange 2003 or Exchange 2000, every regular Cisco Unity subscriber account is associated with an Active Directory domain account.

When the partner Exchange server is running Exchange 5.5 and the Cisco Unity server is a member server or a domain controller in an Active Directory domain, every regular Cisco Unity subscriber is associated with an Active Directory domain account.

When the partner Exchange server is running Exchange 5.5 and the Cisco Unity server is a member server in a Windows NT domain, regular Cisco Unity subscribers may or may not have a Windows NT user account. (Exchange 5.5 allows a user to have a mailbox without having a corresponding Windows NT account.)

Depending on the method you use to create Cisco Unity subscriber accounts, the corresponding Active Directory or Windows NT account may be created automatically.

-
-
- Cannot use the phone as a recording and playback device for the Media Master.

**Note**

the Cisco Unity Inbox was known as the Visual Messaging Interface, or VMI.

Best Practices

- On Cisco Unity systems 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 or not create Windows NT accounts for the subscribers.
- 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 8-4.

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

Best Practice: Limit the Use of the Administration Account

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

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

-
-
-

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

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

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

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

account (if there is one) or the Exchange mailbox for that subscriber. You can delete the Active Directory or Windows NT 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 (if the Cisco Unity server is a member server or domain controller in an Active Directory domain) or in Windows NT (if the Cisco Unity server is a member server in a Windows NT domain), 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 or Windows NT 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 (for an Active Directory account) or in User Manager for Domains (for a Windows NT account).

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 give the account Exchange Administrator permission (if the partner server is running Exchange 2003 or Exchange 2000) or Services Account Administration permission (if the partner Exchange server is running Exchange 5.5).

For more information on the permissions set by the Permissions wizard, refer to the *Permissions Set by Permissions Wizard*

Table 6-1 *Considerations for Securing Default Cisco Unity Accounts, Active Directory or Windows NT Accounts, or Exchange Mailboxes*

Cisco Unity Subscriber Account	Active Directory or Windows NT Account, and Exchange Mailbox	When Created	Best Practice
			<ul style="list-style-type: none"> • • •
	Unity_<servername>	At installation	<p>For versions of Cisco Unity prior to 4.0(5), or for systems that were upgraded from a version prior to 4.0(5), change the Active Directory or Windows NT 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 version 4.0(5).</p>

Exchange Mailboxes (continued)

None	UAmis_<servername>	When configuring AMIS	<p>In Cisco Unity 4.0(3) and earlier, there was a default password for this account. In Cisco Unity 4.0(4) and later, the Cisco Unity Installation and Configuration Assistant prompts for a password for the Default Subscriber template, which is used to create the UAmis Active Directory or Windows NT account. If a Cisco Unity 4.0(4) or later system was upgraded from version 4.0(3) or earlier, the UAmis account may still have the default password. Beginning with Cisco Unity 4.0(5), this account is disabled by default.</p> <p>For versions of Cisco Unity prior to 4.0(5), or for systems that were upgraded from a version prior to 4.0(5), change the Active Directory or Windows NT 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 5.5. 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 (shipped with Cisco Unity 4.0(4) 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>
------	--------------------	-----------------------	---

Table 6-1 *Considerations for Securing Default Cisco Unity Accounts, Active Directory or Windows NT Accounts, or Exchange Mailboxes (continued)*



