



Changing Passwords

This chapter contains the following sections:

- [Changing Passwords for the Cisco Unity Service Accounts \(Without Failover\)](#), page 8-1
- [Changing Passwords for the Cisco Unity Service Accounts \(With Failover Configured\)](#), page 8-3
- [Changing the Active Directory Password for the Unity_<servername> and EAdmin Accounts](#), page 8-6
- [Changing the Notes Password on the Cisco Unity Server \(Without Failover\)](#), page 8-6
- [Changing the Notes Password on the Cisco Unity Server \(With Failover Configured\)](#), page 8-7

Changing Passwords for the Cisco Unity Service Accounts (Without Failover)



Note

If failover is configured, see the [“Changing Passwords for the Cisco Unity Service Accounts \(With Failover Configured\)”](#) section on page 8-3 instead.

To change passwords on the accounts that Cisco Unity services log on as, you determine the Active Directory accounts that the services log on as, change the password on each account, and then change the password on the Cisco Unity services.

Note that you use Active Directory Users and Computers in the procedure [“To Change the Password for an Active Directory Account That Cisco Unity Services Log On As.”](#) If the program is not installed on the Cisco Unity server, you can install it (refer to Windows 2000 Server Help), or you can use a computer in the domain that includes the Cisco Unity server (for example, the domain controller) on which Active Directory Users and Computers is already installed.

Do the following four procedures in the order listed.

To Determine the Active Directory Accounts That Cisco Unity Services Log On As

- Step 1** See [Table B-3](#) in [Appendix B, “Cisco Unity 4.x Services,”](#) which lists the Cisco Unity services and the Active Directory accounts that they log on as.
- Step 2** For each of the Cisco Unity services that log on as an account other than Local System, note:
- The name of the service.

- The name of the Active Directory account in the Logs On As column.

Ignore services that log on as the Local System account.

To Change the Password for an Active Directory Account That Cisco Unity Services Log On As

- Step 1** Log on to the server by using an account that has permission to change passwords (for example, a domain administrator account).
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.
- Step 3** In the left pane, click **Users** or the organizational unit in which the Active Directory account whose password you are changing was created.
- Step 4** In the right pane, right-click the name of the account, and click **Reset Password**.
- Step 5** Enter and confirm the new password, and click **OK**.
- Step 6** If you are changing the password on more than one account, repeat [Step 4](#) and [Step 5](#) for each account.
-

To Change the Password for Cisco Unity Services

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** In the right pane, right-click the name of the first service that you identified in the procedure “[To Determine the Active Directory Accounts That Cisco Unity Services Log On As](#).”
- Step 3** Click **Properties**.
- Step 4** Click the **Log On** tab.
- Step 5** In the Password box and in the Confirm Password box, enter the same new password that you used for the account that the service logs on as.
- Step 6** Click **OK**.
- Step 7** Repeat [Step 2](#) through [Step 6](#) for each of the remaining Cisco Unity services that you identified in the procedure “[To Determine the Active Directory Accounts That Cisco Unity Services Log On As](#).”
- Step 8** Shut down and restart the Cisco Unity server.
-

To Confirm That Cisco Unity Services Restarted After Password Changes

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** For each service for which you changed the password, confirm that the value in the Status column is **Started**.
- Step 3** If all services started, close the Services MMC, and skip the rest of this procedure.
If one or more services failed to start, on the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.

- Step 4** In the left pane, click **System Log**.
- Step 5** Look for one or more errors similar to the following description:
The <CiscoUnityServiceName> service failed to start due to the following error: The service did not start due to a logon failure.
- Step 6** If you find one or more such errors, confirm that the passwords for the specified services and for the corresponding accounts were changed to the same values.
- Step 7** If you change any passwords again while troubleshooting, shut down and restart the Cisco Unity server, and repeat this procedure.

Changing Passwords for the Cisco Unity Service Accounts (With Failover Configured)



Note

If failover is not configured, see the [“Changing Passwords for the Cisco Unity Service Accounts \(Without Failover\)”](#) section on page 8-1 instead.

To change passwords on the accounts that Cisco Unity services log on as, you determine the Active Directory accounts that the services log on as, change the password on each account, and then change the password on the Cisco Unity services.

Note that you use Active Directory Users and Computers in the procedure [“To Change the Password for an Active Directory Account That Cisco Unity Services Log On As.”](#) If the program is not installed on the Cisco Unity server, you can install it (refer to Windows 2000 Server Help), or you can use a computer in the domain that includes the Cisco Unity server (for example, the domain controller) on which Active Directory Users and Computers is already installed.

Do the following seven procedures in the order listed.

To Determine the Active Directory Accounts That Cisco Unity Services Log On As

- Step 1** See the [“Cisco Unity 4.x Services When Domino Is the Message Store”](#) section on page B-1 for a list of the Cisco Unity services and the Active Directory accounts that they log on as.
- Step 2** For each of the Cisco Unity services that log on as an account other than Local System, note:
- The name of the service.
 - The name of the Active Directory account in the Logs On As column.
- Ignore services that log on as the Local System account.

To Change the Password for an Active Directory Account That Cisco Unity Services Log On As

- Step 1** Log on to the server by using an account that has permission to change passwords (for example, a domain administrator account).
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.

- Step 3 In the left pane, click **Users** or the organizational unit in which the Active Directory account whose password you are changing was created.
 - Step 4 In the right pane, right-click the name of the account, and click **Reset Password**.
 - Step 5 Enter and confirm the new password, and click **OK**.
 - Step 6 If you are changing the password on more than one account, repeat [Step 4](#) and [Step 5](#) for each account.
-

To Change the Password for Cisco Unity Services on the Secondary Server

- Step 1 On the secondary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2 In the right pane, right-click the name of the first service that you identified in the procedure “[To Determine the Active Directory Accounts That Cisco Unity Services Log On As](#).”
 - Step 3 Click **Properties**.
 - Step 4 Click the **Log On** tab.
 - Step 5 In the Password box and in the Confirm Password box, enter the same new password that you used for the account that the service logs on as.
 - Step 6 Click **OK**.
 - Step 7 Repeat [Step 2](#) through [Step 6](#) for each of the remaining Cisco Unity services that you identified in the procedure “[To Determine the Active Directory Accounts That Cisco Unity Services Log On As](#).”
 - Step 8 Shut down and restart the secondary server.
-

To Confirm That Cisco Unity Services on the Secondary Server Restarted After Password Changes

- Step 1 On the secondary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2 For each service for which you changed the password, confirm that the value in the Status column is **Started**.
 - Step 3 If all services started, close the Services MMC, and skip the rest of this procedure.
If one or more services failed to start, on the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.
 - Step 4 In the left pane, click **System Log**.
 - Step 5 Look for one or more errors similar to the following description:
The <CiscoUnityServiceName> service failed to start due to the following error: The service did not start due to a logon failure.
 - Step 6 If you find one or more such errors, confirm that the passwords for the specified services and for the corresponding accounts were changed to the same values.
 - Step 7 If you change any passwords again while troubleshooting, shut down and restart the secondary server, and repeat this procedure.
-

To Manually Initiate Failover to the Secondary Server

- Step 1 On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
 - Step 2 Click **Failover**.
 - Step 3 Click **OK** to confirm that you want to fail over to the secondary server. The primary server becomes inactive, and the secondary server becomes active.
-

To Change the Password for Cisco Unity Services on the Primary Server

- Step 1 On the primary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2 In the right pane, right-click the name of the first service that you identified in the procedure “[To Determine the Active Directory Accounts That Cisco Unity Services Log On As](#).”
 - Step 3 Click **Properties**.
 - Step 4 Click the **Log On** tab.
 - Step 5 In the Password box and in the Confirm Password box, enter the same new password that you used for the account that the service logs on as.
 - Step 6 Click **OK**.
 - Step 7 Repeat [Step 2](#) through [Step 6](#) for each of the remaining Cisco Unity services that you identified in the procedure “[To Determine the Active Directory Accounts That Cisco Unity Services Log On As](#).”
 - Step 8 Shut down and restart the primary server.
-

To Confirm That Cisco Unity Services on the Primary Server Restarted After Password Changes

- Step 1 On the primary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2 For each service for which you changed the password, confirm that the value in the Status column is **Started**.
 - Step 3 If all services started, close the Services MMC, and skip the rest of this procedure.
If one or more services failed to start, on the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.
 - Step 4 In the left pane, click **System Log**.
 - Step 5 Look for one or more errors similar to the following description:
The <CiscoUnityServiceName> service failed to start due to the following error: The service did not start due to a logon failure.
 - Step 6 If you find one or more such errors, confirm that the passwords for the specified services and for the corresponding accounts were changed to the same values.
 - Step 7 If you change any passwords again while troubleshooting, shut down and restart the primary server, and repeat this procedure.
-

Changing the Active Directory Password for the Unity_<servername> and EAdmin Accounts

When Cisco Unity is installed, two Active Directory accounts are automatically created: Unity_<servername> and EAdmin<8_alphanumeric_characters>. Prior to Cisco Unity 4.0(4), the default passwords on these accounts were long strings of random, alphanumeric characters. Beginning with Cisco Unity 4.0(4), the passwords are specified in the Password Hardening wizard, during installation.

Because the accounts are used only by Cisco Unity, you can change a password at any time by using the applicable Windows application. For Active Directory accounts, use Active Directory Users and Computers; for Windows NT accounts, use User Manager for Domains. For more information, refer to Help for the application.



Note

To secure the accounts more effectively, you can disable (not delete) the accounts by using the same application that you use to change a password.

Changing the Notes Password on the Cisco Unity Server (Without Failover)

The password for Notes on the Cisco Unity server appears in two places. If you want to change the password, you need to change it in both places:

- When you installed Cisco Unity, you registered a Domino user. The password that you specified was included, in encrypted format, in the resulting .id file. When you installed Notes, the .id file was copied to the Cisco Unity server. To change the password in the .id file, you use Notes. See the “[To Change the Password in the .id File](#)” procedure below.
- When you installed Cisco Unity, the encrypted password in the .id file was copied to the Windows registry on the Cisco Unity server to facilitate communication with Domino. To change the password in the registry, you use the Change Notes Password utility in the Cisco Unity Tools Depot. See the “[To Change the Password in the Registry](#)” procedure on page 8-7.



Caution

Do not run Notes on the Cisco Unity server while Cisco Unity is running, or Cisco Unity may stop functioning.

To Change the Password in the .id File

- Step 1 Stop Cisco Unity. (Right-click the **Cisco Unity** icon in the system tray, click **Stop Cisco Unity**, and then click **OK** on the confirmation dialog; if the Cisco Unity icon is not available, browse to the CommServer directory and double-click **AvCsTrayStatus.exe**.)
- Step 2 Stop the Cisco Unity services:
 - a. On the Windows Start menu, click **Run**.
 - b. Run **cmd**.
 - c. Change to the directory in which Cisco Unity is installed (the default is CommServer).

- d. Run the command **kill -f av*** to stop all Cisco Unity services, including the Windows tray icon. (The tray icon may continue to appear in the Windows taskbar, but if you move the mouse cursor over it, it disappears.)
 - e. Close the Command Prompt window.
- Step 3** On the Windows Start menu, click **Programs > Lotus Applications > Lotus Notes**.
- Step 4** On the Lotus Notes File menu, click **Tools > User ID**.
- Step 5** Click **Set Password**.
- Step 6** Follow the on-screen prompts.
- Step 7** When you are finished, close Lotus Notes.
-

To Change the Password in the Registry

- Step 1** On the Windows desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Cisco Unity Tools Depot, expand **Administration Tools**.
- Step 3** Double-click **Change Notes Password**.
- Step 4** Follow the on-screen prompts.
- Step 5** Restart the Cisco Unity server.
-

Changing the Notes Password on the Cisco Unity Server (With Failover Configured)

The password for Notes on the Cisco Unity server appears in two places on the primary Cisco Unity server and in two places on the secondary Cisco Unity server. If you want to change the password, you need to change it in both places on the two servers:

- When you installed Cisco Unity, you registered a Domino user. The password that you specified was included, in encrypted format, in the resulting .id file. When you installed Notes, the .id file was copied to the Cisco Unity servers. To change the password in the .id file, you use Notes. See [Step 1](#) through [Step 7](#) in the “[To Change the Notes Password](#)” procedure below.
- When you installed Cisco Unity, the encrypted password in the .id file was copied to the Windows registry on the Cisco Unity servers to facilitate communication with Domino. To change the password in the registry, you use the Change Notes Password utility in the Cisco Unity Tools Depot. See [Step 8](#) through [Step 12](#) in the “[To Change the Notes Password](#)” procedure below.



Caution

Do not run Notes on the Cisco Unity servers while Cisco Unity is running, or Cisco Unity may stop functioning. By stopping Cisco Unity on the primary server, the secondary server will become active and begin handling calls while you change the password on the primary server. After you manually failback to the primary server and it begins handling calls, you can change the password on the secondary server.

If Cisco Unity is configured for failover, do the procedure first on the primary Cisco Unity server. The procedure alerts you when to do it on the secondary Cisco Unity server.

To Change the Notes Password

-
- Step 1** Stop Cisco Unity. (Right-click the **Cisco Unity** icon in the system tray, click **Stop Cisco Unity**, and then click **OK** on the confirmation dialog; if the Cisco Unity icon is not available, browse to the CommServer directory and double-click **AvCsTrayStatus.exe**.)
- The secondary server will become active and begin handling calls, while the primary server will become inactive.
- Step 2** Stop the Cisco Unity services:
- On the Windows Start menu, click **Run**.
 - Run **cmd**.
 - Change to the directory in which Cisco Unity is installed (the default is CommServer).
 - Run the command **kill -f av*** to stop all Cisco Unity services, including the Windows tray icon. (The tray icon may continue to appear in the Windows taskbar, but if you move the mouse cursor over it, it disappears.)
 - Close the Command Prompt window.
- Step 3** On the Windows Start menu, click **Programs > Lotus Applications > Lotus Notes**.
- Step 4** On the Lotus Notes File menu, click **Tools > User ID**.
- Step 5** Click **Set Password**.
- Step 6** Follow the on-screen prompts.
- Step 7** When you are finished, close Lotus Notes.
- Step 8** On the Windows desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 9** In the left pane of the Cisco Unity Tools Depot, expand **Administration Tools**.
- Step 10** Double-click **Change Notes Password**.
- Step 11** Follow the on-screen prompts.
- Step 12** Restart the Cisco Unity server.
- Step 13** Manually fail back to the primary server:
- On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
 - Click **Failback**.
 - Click **OK** to confirm that you want to fail back to the primary server. The primary server become active, and the secondary server becomes inactive.
- The primary server will become active and begin handling calls, while the secondary server will become inactive.
- Step 14** Do [Step 1](#) through [Step 12](#) on the secondary Cisco Unity server.
- The primary server will remain active and continue handling calls.
-