



Configuring Cisco Unity Failover

Configure Cisco Unity failover only after you have installed both the primary and secondary servers according to instructions in the *Cisco Unity Installation Guide*. Use the task list to configure failover correctly.

This chapter contains the following sections:

- [Task List for Configuring Cisco Unity Failover, page 1-1](#)
- [Setting Up the Cisco Unity Failover Account \(Optional\), page 1-3](#)
- [Configuring Failover on the Primary and Secondary Servers, page 1-5](#)
- [Enabling Direct Subscriber Logon to the Secondary Server After Failover, page 1-8](#)

Task List for Configuring Cisco Unity Failover

1. Confirm that the system keys are connected to the correct servers. See the [“Verifying the System Keys” section on page 1-2](#).
2. Create the Cisco Unity failover account, if applicable, and set the necessary rights. See the [“Setting Up the Cisco Unity Failover Account \(Optional\)” section on page 1-3](#).
3. Configure failover on the primary and secondary servers. See the [“Configuring Failover on the Primary and Secondary Servers” section on page 1-5](#).

4. If the Cisco Unity system is integrated with Cisco CallManager 3.1(x) or with Cisco CallManager 3.2(2) and later, skip to Task 5.
Otherwise, create a new routing rule so that subscribers have easy message access after failover. See the [“Enabling Direct Subscriber Logon to the Secondary Server After Failover”](#) section on page 1-8.
5. Adjust the failover and failback settings, if applicable. See the [“Customizing Failover and Failback for the Cisco Unity System”](#) section on page 2-2.

Verifying the System Keys

The system key contains the information that designates primary and secondary servers. Confirm that the system key for the primary server is attached to the machine that you want to use as the primary server, and that the system key for the secondary server is attached to the machine that you want to use as the secondary server.



Caution

If the failover servers are not identical and if you configure failover with the system keys attached to the wrong servers, you will need to reinstall all software to correct the problem.

To confirm that the system keys are connected to the correct servers

- Step 1 On the primary Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Key Dump**.
- Step 2 In the Features section, confirm that the **Failover Backup Server** check box is unchecked.
If the check box is checked, the key for the secondary server is attached to the primary server. Switch the keys between the servers.

Setting Up the Cisco Unity Failover Account (Optional)

When you configure failover, you are prompted to specify the account that owns the Node Manager service (AvCsNodeMgr.exe) and the file shares for file replication between the primary and secondary servers. By default, the Node Manager service is owned by the account with which you are logged on when you configure failover.

If your organization requires the use of a different failover account, do the following three procedures in the order listed to create the Cisco Unity failover account and to set the necessary rights.

To create the Cisco Unity failover account

- Step 1 Log on to Windows by using an account that is a member of the Domain Admins group.
 - Step 2 On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers**.
 - Step 3 In the left pane, right-click **Users** or the organizational unit where you want to create the failover account, and click **New > Users**.
 - Step 4 Follow the on-screen prompts. Do not create an Exchange mailbox.
 - Step 5 Close Active Directory Users and Computers.
-

To add the failover account to the Local Administrators group on both servers

- Step 1 On one Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
- Step 2 In the left pane of the Computer Management MMC, expand **System Tools > Local Users and Groups**.
- Step 3 In the left pane, click **Groups**.
- Step 4 In the right pane, double-click **Administrators**.
- Step 5 In the Administrators Properties dialog box, click **Add**.

■ Setting Up the Cisco Unity Failover Account (Optional)

- Step 6 In the Select Users or Groups dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.
 - Step 7 In the top list, double-click the name of the failover account. The name appears in the bottom list.
 - Step 8 Click **OK** to close the Select Users or Groups dialog box.
 - Step 9 Click **OK** to close the Administrators Properties dialog box.
 - Step 10 Close the Computer Management MMC.
 - Step 11 Repeat Steps 1 through 10 on the other server.
-

To grant the failover account the rights to act as a part of the operating system and to log on as a service on both servers

- Step 1 On one Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Local Security Policy**.
- Step 2 In the Local Security Settings MMC, in the left pane, expand **Local Policies**.
- Step 3 In the left pane, click **User Rights Assignment**.
- Step 4 In the right pane, double-click **Act as a Part of the Operating System**.
- Step 5 In the Local Security Policy Setting dialog box, click **Add**.
- Step 6 In the Select Users or Groups dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.
- Step 7 In the top list, double-click the name of the failover account. The name appears in the bottom list.
- Step 8 Click **OK** to close the Select Users or Groups.
- Step 9 Click **OK** to close the Local Security Policy Setting dialog box.
- Step 10 In the right pane, double-click **Log On as a Service**.
- Step 11 In the Local Security Policy Setting dialog box, click **Add**.
- Step 12 In the Select Users or Groups dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.
- Step 13 In the top list, double-click the name of the failover account. The name appears in the bottom list.
- Step 14 Click **OK** to close the Select Users or Groups dialog box.

- Step 15 Click **OK** to close the Local Security Policy Setting dialog box.
 - Step 16 Close the Local Security Settings MMC.
 - Step 17 Repeat Steps 1 through 16 on the other server.
-

Configuring Failover on the Primary and Secondary Servers

The Configure Cisco Unity Failover wizard configures default settings for failover on the Cisco Unity system. (For information on the default settings, see [Table 2-1 on page 2-3](#).)

Do the following two procedures in the order listed.

To configure failover on the primary server

- Step 1 In Windows Explorer, browse to the directory where Cisco Unity is installed (the default directory is C:\CommServer).
- Step 2 Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 3 Click **Next**.
- Step 4 Click **Browse**, select the name of the secondary server, and click **OK**. The IP address for the secondary server is filled in automatically.
- Step 5 If the system is running Cisco Unity 3.1(2), skip to Step 6.

If the system is running Cisco Unity 3.1(3) or later, and you want the switch file for the selected phone system to replicate during the wizard, check the **Copy Switch Files from Primary Server to Secondary Server** check box.



Note

The switch file is replicated only during the failover configuration wizard. If you select a different phone system after you run the wizard, the new switch file is not replicated to the secondary server. In addition, changes to phone system settings

are not replicated between the primary and secondary servers. If you change phone system settings after you run the failover configuration wizard, you must manually change values on both servers.

Step 6 Click **Next**.

Step 7 If you did not create a Cisco Unity failover account, skip to Step 8.

If you created a Cisco Unity failover account, click **Browse**, and double-click the name of the account.



Caution

You must specify the same account on the both the primary and the secondary servers.

Step 8 Enter the password for the account that owns the failover service.

Step 9 Click **Next**.

Step 10 Click **Configure**. The wizard verifies settings and configures failover on the primary server.

If the wizard does not finish the configuration successfully, an error message explains why the wizard failed. Exit the wizard, correct the problem, and click **Configure** again.

Step 11 Click **Finish**.

Step 12 Exit and restart the Cisco Unity software. For more information, see [Appendix A, “Exiting and Starting the Cisco Unity Software and Server.”](#)

To configure failover on the secondary server

Step 1 In Windows Explorer, browse to the directory where Cisco Unity is installed (the default directory is C:\CommServer).

Step 2 Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.

Step 3 Click **Next**.

Step 4 Click **Browse**, select the name of the primary server, and click **OK**. The IP address for the primary server is filled in automatically.

- Step 5** If the system is running Cisco Unity 3.1(2), skip to Step 6.
- If the system is running Cisco Unity 3.1(3) or later, and you want the switch file for the selected phone system to replicate during the wizard, check the **Copy Switch Files from Primary Server to Secondary Server** check box.

**Note**

The switch file is replicated only during the failover configuration wizard. If you select a different phone system after you run the wizard, the new switch file is not replicated to the secondary server. In addition, changes to phone system settings are not replicated between the primary and secondary servers. If you change phone system settings after you run the failover configuration wizard, you must manually change values on both servers.

- Step 6** Click **Next**.
- Step 7** If you created a Cisco Unity failover account, click **Browse**, and double-click the name of the account.
- Otherwise, skip to Step 8.

**Caution**

You must specify the same account on both the primary and the secondary servers.

- Step 8** Enter the password for the account that owns the failover service.
- Step 9** Click **Next**.
- Step 10** Click **Configure**. The wizard verifies settings and configures failover on the secondary server.
- If the wizard does not finish the configuration successfully, an error message explains why the wizard failed. Exit the wizard, correct the problem, and click **Configure** again.
- Step 11** Click **Finish**.
- Step 12** Exit and restart the Cisco Unity software. For more information, see [Appendix A, “Exiting and Starting the Cisco Unity Software and Server.”](#)
-

Enabling Direct Subscriber Logon to the Secondary Server After Failover



Note

If the Cisco Unity system is integrated with Cisco CallManager 3.1(x) or with Cisco CallManager 3.2(2) and later, skip this section.

This section describes how to create a new routing rule for failover, so that subscribers can directly log on to Cisco Unity on the secondary server after failover. When subscribers press the phone button to listen to messages, they hear the subscriber logon conversation instead of the external caller greeting.

Do the following procedure on the applicable server, depending on the Cisco Unity version installed:

- | | |
|------------------------------------|---|
| Cisco Unity 3.1(3) or later | Do the procedure only after you have run the failover configuration wizard on both servers, and only on the primary server when it is active. |
| Cisco Unity 3.1(2) | Do the procedure only after you have run the failover configuration wizard on both servers, and only on the secondary server when it is active. |

To enable direct subscriber logon to the secondary server after failover

- Step 1 On the applicable server, open the Cisco Unity Administrator.
- Step 2 Go to **Call Management > Call Routing > Forwarded Calls**.
- Step 3 Click the **Add** icon to add a new routing rule.
- Step 4 Enter a name for the rule, and click **Add**.
- Step 5 Enter the following values in the applicable fields:

Status	Enabled
Call Type	Both

Dialed Number (DNIS)	<The pilot number for the voice messaging ports used by the primary server> Typically, the pilot number is the extension of the first voice messaging port. (For example, if the voice messaging ports are numbered from 7000 to 7047, the pilot number is 7000.)
Send Call To	Attempt Sign-in

- Step 6** Click the **Save** icon. Do not change the order of the rules.
With Cisco Unity version 3.1(3) or later, the new routing rule is stored in the SQL Server database and replicated to the secondary server.
- Step 7** Exit and restart the Cisco Unity software on the primary server, then on the secondary server. For more information, see [Appendix A, “Exiting and Starting the Cisco Unity Software and Server.”](#)
- Step 8** Confirm that the rule is in effect by manually failing over to the secondary server and doing the following:
- Press the messages button on a phone that is associated with a subscriber. Cisco Unity should play the subscriber logon conversation.
 - Press the messages button on a phone that is not associated with a subscriber. Cisco Unity should play the external caller greeting.
-

■ Enabling Direct Subscriber Logon to the Secondary Server After Failover