



Configuring Cisco Unity Failover



Caution

Configure Cisco Unity failover only after you have installed both the primary and secondary servers according to instructions in the *Cisco Unity Installation Guide*, and after you have programmed the phone system and configured Cisco Unity according to instructions in the applicable Cisco Unity integration guide.

In this chapter, you do the following tasks in the order listed to configure failover correctly:

1. Configure failover on the primary and secondary servers. See the [“Configuring Failover on the Primary and Secondary Servers”](#) section on page 1-2.
2. On the secondary server, run the Cisco Unity Telephony Integration Manager to configure the voice messaging ports. See the [“Configuring the Voice Messaging Ports on the Secondary Server”](#) section on page 1-3.
3. *If the Cisco Unity system is integrated with a circuit-switched phone system, or with Cisco CallManager 3.2(1) or earlier:* Create a new routing rule so that subscribers will have easy message access when failover occurs. See the [“Creating a Routing Rule That Enables Subscriber Logon by Phone After Failover”](#) section on page 1-4.
4. Set up automatic daily resynchronization of MWIs. See the [“Setting Up Automatic Daily Resynchronization of MWIs”](#) section on page 1-5.
5. Set up notification of when failover occurs. See the [“Setting Up Notification of When Failover Occurs”](#) section on page 1-5.
6. Set up scheduled backups of the Cisco Unity system. See the [“Setting Up Scheduled Backups of Cisco Unity”](#) section on page 1-9.
7. Test Cisco Unity failover. See the [“Testing Cisco Unity Failover”](#) section on page 1-9.
8. *Optional:* Adjust the failover and failback settings. See the [“Customizing Failover and Failback Settings for the Cisco Unity System \(Optional\)”](#) section on page 1-12.
9. *Optional:* Disable failover initiation when calls are unanswered on the primary server. See the [“Disabling Failover Initiation When Calls Are Unanswered on the Primary Server \(Optional\)”](#) section on page 1-13.

If you are installing a new system, return to the “Overview of Mandatory Tasks for Installing Cisco Unity” in the *Cisco Unity Installation Guide* when you are finished with the failover configuration tasks, to continue installing the system correctly.

**Note**

The task list contains tasks that reference instructions in Cisco Unity documentation other than the *Cisco Unity Installation Guide*, so if you do not use the list, the installation will not be successful.

Configuring Failover on the Primary and Secondary Servers

The Configure Cisco Unity Failover wizard configures default settings for failover and failback on the Cisco Unity system. (For information on the default settings, see [Table 1-2 on page 1-12](#).) You can adjust the settings later in the configuration process—the *Cisco Unity Failover Configuration and Administration Guide* alerts you when to do the procedure.

**Caution**

The Computer Browser service for both primary and secondary servers must have the startup type set to Automatic and must be running. Otherwise, the Configure Cisco Unity Failover wizard cannot locate the other server in the failover pair.

Do the following two procedures in the order listed.

To Configure Failover on the Primary Server

- Step 1** In Windows Explorer, browse to the **CommServer** directory.
- Step 2** Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 3** On the Welcome page, click **Next**.
- Step 4** On the Specify Server Role page, click **Primary Server**, and click **Next**.
- Step 5** On the Enter the Name of Your Server page, click **Browse**, select the name of the secondary server, and click **OK**. The IP address for the secondary server is filled in automatically.
- Step 6** Click **Next**.
- Step 7** On the Enter Failover Account Information page, click **Browse**, and double-click the name of the messaging account. This account will own the failover service.

The account you select must have the right to act as part of the operating system and to log on as a service, and must be a member of the Local Administrators group.

**Caution**

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

- Step 8** In the Password field, enter the password for the account that owns the failover service, and click **Next**.
- Step 9** On the Begin Configuring Your Server page, 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 10** On the Completing page, click **Finish**.

To Configure Failover on the Secondary Server

- Step 1** On the Windows taskbar, double-click the system clock. The Date/Time Properties dialog box appears.
- Step 2** Set the time to the same hour and minute as shown on the primary server, and click **OK**.
- Step 3** In Windows Explorer, browse to the **CommServer** directory.
- Step 4** Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 5** On the Welcome page, click **Next**.
- Step 6** On the Specify Server Role page, click **Secondary Server**, and click **Next**.
- Step 7** On the Enter the Name of Your Server page, click **Browse**, select the name of the primary server, and click **OK**. The IP address for the primary server is filled in automatically.
- Step 8** Click **Next**.
- Step 9** On the Enter Failover Account Information page, click **Browse**, and double-click the name of the messaging account. This account will own the failover service.

The account you select must have the right to act as part of the operating system and to log on as a service, and must be a member of the Local Administrators group.



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

- Step 10** In the Password field, enter the password for the account that owns the failover service, and click **Next**.
- Step 11** On the Begin Configuring Your Server page, 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 12** On the Completing page, click **Finish**.
-

Configuring the Voice Messaging Ports on the Secondary Server

After running the failover configuration wizard on the secondary server, you must enter settings for the voice messaging ports (for example, set the ports for Answer Calls, Dialout MWIs).

To Configure the Voice Messaging Ports on the Secondary Server

- Step 1** After the secondary server restarts, on the Windows Start menu, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.
- Step 2** In the left pane of the UTIM window, click the phone system integration you are creating.
- Step 3** In the right pane of the UTIM window, click the **Ports** tab.

- Step 4** Enter the port settings. For details on the settings needed by the phone system, refer to the applicable Cisco Unity integration guide. (Integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.)



Caution When programming the phone system, do not forward calls to voice messaging ports in Cisco Unity that cannot answer calls (voice messaging ports that are not set to Answer Calls). For example, if a voice messaging port is set only to Dialout MWI, do not forward calls to it.

- Step 5** Click **Save**.

- Step 6** Exit UTIM.

Creating a Routing Rule That Enables Subscriber Logon by Phone After Failover



Note If the Cisco Unity system is integrated with a SIP proxy server or with Cisco CallManager version 3.2(2) or later, skip this section because the phone system automatically forwards calls to the secondary server when it becomes active.

The routing rule for failover allows subscribers to use the phone to log on to Cisco Unity on the secondary server after failover occurs. With the rule, when subscribers dial the internal Cisco Unity phone number that they normally use to access their messages, Cisco Unity automatically routes the call to the secondary server, and subscribers hear the subscriber logon conversation instead of the external caller greeting.

Create the routing rule only after you have run the failover configuration wizard on both the primary and secondary servers. Do the procedure in this section only on the primary server when it is active.

To Create a Routing Rule That Enables Subscriber Logon by Phone After Failover

- Step 1** On the primary server, open the Cisco Unity Administrator.
- Step 2** Go to the **Call Management > Call Routing > Forwarded Calls** page.
- 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 corresponding values in the following 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.
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:
- Manually initiate failover. See [“Manually Initiating Failover or Failback” section on page 3-2.](#)
 - 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.

Setting Up Automatic Daily Resynchronization of MWIs

We recommend that you set up the primary and secondary servers to resynchronize MWIs every day.

To Set Up Automatic Daily Resynchronization of MWIs

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Manage Integrations**.
- Step 2** In the left pane of the UTIM window, click the **Properties** node for the phone system integration.
- Step 3** Under MWI Synchronization, check the **Resynchronize** check box.
- Step 4** Select a time when network traffic is at its lowest.
- Step 5** Click **Save**.
- Step 6** Exit UTIM.
- Step 7** On the secondary server, repeat [Step 1](#) through [Step 6](#).

Setting Up Notification of When Failover Occurs

We recommend that you set up the Event Monitoring service (EMS) to notify system administrators when failover occurs. The EMS monitors the Windows Event logs and can send notification when the secondary server becomes active. You choose the message type(s) that the EMS uses to notify system administrators.

[Table 1-1](#) describes the available message types; the procedure to set up notification follows the table.

Table 1-1 Message Types Used by the Event Monitoring Service

Message Type	Description
Voice message	<p>A recorded notification is sent to one or more subscribers or public distribution lists. With this option, you can use the default message, or you can record the message you want sent. The recording must be a WAV file and must be saved on the secondary server. You can use a recording and playback device on the active primary server to record the message.</p> <p>(For information on making recordings, refer to the “Using the Media Master to Record Greetings and Names” section in the “Cisco Unity Conversation” chapter of the <i>Cisco Unity System Administration Guide, Release 4.0(5)</i> at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag405/ex/index.htm.)</p>
E-mail message	A text message is sent to one or more subscribers or public distribution lists.
SMTP message	A text message is sent by using the SMTP server included with Microsoft Internet Information Services (IIS). This capability is useful when you want to send notification over the Internet to an e-mail address at another location. Because this method does not depend on Cisco Unity for the notification, it can be used to monitor events that indicate catastrophic failure of Cisco Unity.
SNMP trap	<p>SNMP trap notification works with the Remote Serviceability Kit (RSK) to allow you to configure SNMP notifications for monitored Windows Event log entries. You configure the SNMP destinations by using the SNMP Service properties in the Services configuration manager in Windows.</p> <p>(For information on setting up SNMP on the Cisco Unity server, refer to the “Setting Up SNMP Notification” section in the “Configuring Cisco Unity for Maintenance Tasks” chapter of the <i>Cisco Unity Maintenance Guide, Release 4.0(5)</i> at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/ex/index.htm.)</p>
Syslog	A Windows Event log entry is sent over the IP network to a syslog server.

To Set Up Notification of When Failover Occurs

- Step 1** On the secondary server, click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Tools Depot window, expand **Diagnostic Tools**, and double-click **Event Monitoring Service**.
- Step 3** If you are not starting the EMS for the first time, skip to [Step 4](#).
If you are starting the EMS for the first time, when prompted, enter the password for the account that the AvCsMgr service logs on as, and click **OK**.
- Step 4** On the File menu of the Event Monitoring Service window, click **New > Recipient**. The Create New Recipient dialog box appears.
- Step 5** In the Recipient Name field, enter a display name for the subscriber or distribution list that you want to receive notification.
- Step 6** If you do not want to add notification by voice message, skip to [Step 7](#).

To select the subscriber or list for notification by voice message:

- a. Click the **Voice Mail** tab.
- b. Click either **Subscriber** or **Distribution List**, depending on the recipient.
- c. Click **Select**.
- d. In the Search dialog box, click **Search**, click the name of the subscriber or list, and click **OK**.
- e. To add notification by another message type, continue with the applicable step:

E-mail message	Step 7
SMTP message	Step 8
SNMP Trap	Step 9
Syslog	Step 10

Otherwise, click **OK**, and skip to [Step 11](#).

Step 7 If you do not want to add notification by e-mail, skip to [Step 8](#).

To select the subscriber or list for notification by e-mail:

- a. Click the **E-Mail** tab.
- b. Click either **Subscriber** or **Distribution List**, depending on the recipient.
- c. Click **Select**.
- d. In the list, click the name of the subscriber or list, and click **OK**.
- e. To add notification by another message type, continue with the applicable step:

SMTP message	Step 8
SNMP Trap	Step 9
Syslog	Step 10

Otherwise, click **OK**, and skip to [Step 11](#).

Step 8 If you do not want to add notification by SMTP, skip to [Step 9](#).

To select the subscriber or list for notification by SMTP:

- a. Click the **SMTP** tab.
- b. In the **New SMTP Address** field, enter a fully qualified SMTP address for the subscriber or distribution list.
- c. Click **>>** to add the SMTP address to the SMTP Addresses list.
- d. Repeat [Step 8b.](#) and [Step 8c.](#) for each additional SMTP address you want to enter for the subscriber or list.

- e. To add notification by another message type, continue with the applicable step:

SNMP Trap	Step 9
Syslog	Step 10

Otherwise, click **OK**, and skip to [Step 11](#).

- Step 9** If you do not want to add notification by SNMP, skip to [Step 10](#).
To select an SNMP community name for notification:
- Click the **SNMP Trap** tab.
 - Check the **SNMP Trap Enabled** check box.
 - To add a syslog server for notification, continue with [Step 10](#).
Otherwise, click **OK**, and skip to [Step 11](#).
- Step 10** If you do not want to add notification by syslog server, skip to [Step 11](#).
To select a syslog server for notification:
- Click the **Syslog** tab.
 - Check the **Enabled** check box.
 - In the Server field, enter the IP address of the syslog server that you want to receive the Event log message.
 - Click **OK**.
- Step 11** Repeat [Step 4](#) through [Step 10](#) for each additional subscriber or distribution list that you want to receive notification.
- Step 12** On the File menu, click **New > Event**. The Add New Event dialog box appears.
- Step 13** In the Source list, click **CiscoUnity_NodeMgr**. For Cisco Unity versions 4.0(2) and earlier, click **AvCsNodeMgr**.
- Step 14** Under ID, click **Specific Event ID**, and enter **1047**.
- Step 15** In the Type list, click **Errors**.
- Step 16** In the Notes field, enter **Failover** or another name to indicate what this event monitors.
- Step 17** If you did not add notification by voice message, skip to [Step 18](#).
To configure the voice message for notification by voice message:
- To the right of the Voice Mail File Name field, click **...**, browse to the WAV file you want to use as the voice message, and click **OK**. The EMS will send this recording as a voice message.
 - In the Voice Mail Priority list, click **Urgent** or another priority that you want.
 - To configure notification by e-mail or by SMTP, continue with [Step 18](#).
Otherwise, click **OK**, and skip to [Step 19](#).
- Step 18** If you did not add notification by e-mail or SMTP, skip to [Step 19](#).
To configure e-mail or SMTP content for notification by e-mail or by SMTP:
- In the E-Mail Subject field, enter the subject line for the e-mail or SMTP notification that the EMS will send. You can enter text or right-click to see a menu of insertion strings that the service provides. (For example, you can enter Cisco Unity Failover Occurred.)

- b. In the E-Mail Priority field, click **Urgent** or another priority that you want.
- c. In the E-Mail Body field, accept the default body text or enter customized body text for the e-mail or SMTP notification that the EMS will send. You can enter text or right-click to see a menu of insertion strings that the EMS provides.

For example, you can enter the following:

Cisco Unity Failover Occurred.

Date: <Date>

Time: <Time>

Event ID: <Event>

Event source: <Source>

- d. Click **OK**.

- Step 19** In the right pane of the Event Monitoring Service window, under Recipients, click the **Add Recipients** icon.
- Step 20** In the Edit Recipients for Event dialog box, check the **Active** check box for all recipients you created in [Step 4](#) to receive failover notification, and click **OK**.
- Step 21** Near the top of the right pane, check the **Active** check box, and click **Apply**.
- Step 22** Close the Event Monitoring Service window and the Tools Depot window.
-

Setting Up Scheduled Backups of Cisco Unity

To prevent loss of Cisco Unity data caused by the failure of hardware components on the primary and secondary servers, we recommend that you set up scheduled backups of Cisco Unity by using a supported third-party backup and restore application.

For information on backing up Cisco Unity, refer to the “Backing Up a Cisco Unity System” chapter of the *Cisco Unity Maintenance Guide, Release 4.0(5)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/ex/index.htm.

Testing Cisco Unity Failover

To test whether Cisco Unity failover and the integration with the secondary server function correctly, do the seven procedures in this section in the order listed.

The testing procedures require that:

- Failover is configured on the primary and secondary servers.
- The primary server is active, and the secondary server is inactive.
- Both servers are integrated with the phone system.

To Add a Test Subscriber with a Recorded Name

- Step 1** In the Cisco Unity Administrator on the primary server, go to the **Subscribers > Subscribers > Profile** page.
- Step 2** Click the **Add** icon.
- Step 3** Click **New Exchange Subscriber**.

- Step 4** Enter the applicable information on the Add Subscriber page.
 - Step 5** Click **Add**.
 - Step 6** Record the subscriber name by using the Media Master control bar.
 - Step 7** On the subscriber record, customize settings as applicable, then click the **Save** icon.
-

To Confirm That the Data Replication to the Secondary Server Occurred

- Step 1** In the Cisco Unity Administrator on the secondary server, go to the **Subscribers > Subscribers > Profile** page for the test subscriber. Seeing the test subscriber on the secondary server indicates that failover replicates the UnityDb SQL database.
 - Step 2** Confirm that the Media Master control bar shows that a recorded name exists (the length of the recording is greater than 0). Seeing the recorded name indicates that failover replicates recordings.
-

To Make the Secondary Server Active

- 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 initiate failover to the secondary server.
-

To Set Up the Integration Test for the Secondary Server

- Step 1** Set up two test extensions (Phone 1 and Phone 2) on the same phone system that the Cisco Unity servers are integrated with.
- Step 2** Set Phone 1 to forward calls to the Cisco Unity pilot number when calls are not answered.
- Step 3** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page for the test subscriber you created in the procedure [“To Add a Test Subscriber with a Recorded Name.”](#)
- Step 4** In the Extension field, enter the extension of Phone 1.
- Step 5** In the Active Schedule field, click **All Hours - All Days**.
- Step 6** Click the **Save** icon.
- Step 7** In the navigation bar, click **Call Transfer** to go to the Subscribers > Subscribers > Call Transfer page for the test subscriber.
- Step 8** Under Transfer Incoming Calls, click **Yes, Ring Subscriber’s Extension**, and confirm that the extension is for Phone 1.
- Step 9** Under Transfer Type, click **Release to Switch**.
- Step 10** Click the **Save** icon.
- Step 11** In the navigation bar, click **Messages** to go to the Subscribers > Subscribers > Messages page for the test subscriber.
- Step 12** Under Message Waiting Indicators (MWIs), check the **Use MWI for Message Notification** check box.

- Step 13** In the Extension field, enter x.
- Step 14** Click the **Save** icon.
-

To Test Recording a Message and Activating the MWI

- Step 1** From Phone 2, dial the extension for Phone 1.
- Step 2** Confirm that Phone 1 rings and that you hear a ringback tone on Phone 2. Do not answer Phone 1.
- Step 3** Confirm that after the number of rings that the phone system is set to wait, the call is forwarded to Cisco Unity and that you hear the greeting for the test subscriber. Hearing the greeting means that the phone system forwarded the unanswered call and the call-forward information to Cisco Unity, which correctly interpreted the information.
- Step 4** Leave a message for the test subscriber, and hang up Phone 2.
- Step 5** Confirm that the MWI on Phone 1 is activated. The activated MWI means that the phone system and the secondary server are successfully integrated for activating MWIs.
-

To Test Listening to a Message and Deactivating the MWI

- Step 1** From Phone 1, dial the internal pilot number for Cisco Unity.
- Step 2** When asked for your password, enter the password for the test subscriber. Hearing the request for your password means that the phone system sent the necessary call information to Cisco Unity, which correctly interpreted the information.
- Step 3** Confirm that you hear the recorded name for the test subscriber (if you did not record a name for the test subscriber, you will hear the extension for Phone 1). Hearing the recorded name means that Cisco Unity correctly identified the subscriber by the extension.
- Step 4** When asked whether you want to listen to your messages, press **1**.
- Step 5** After listening to the message, press **3** to delete the message.
- Step 6** Confirm that the MWI on Phone 1 is deactivated. The deactivated MWI means that the phone system and Cisco Unity are successfully integrated for deactivating MWIs.
- Step 7** Hang up Phone 1.
-

To Delete the Test Subscriber

- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile page**.
If the name of the test subscriber is not displayed, click the **Find** icon (the magnifying glass) in the title bar, then click **Find**, and click the name of the test subscriber in the list that appears.
- Step 2** In the title bar, click the **Delete Subscriber** icon (the X).
- Step 3** Click **Delete**.
-

Customizing Failover and Failback Settings for the Cisco Unity System (Optional)

You can customize the default settings for failover and failback that the failover configuration wizard gives the primary and secondary servers. (For example, you might want to increase the frequency of file replication.)

When you customize failover and failback, you can specify:

- The frequency with which the primary and secondary servers send keep-alive events (or “pings”) to one another, and the number of missed keep-alive events before the secondary server starts taking calls. The default setting is to send keep-alive events every second and to wait 30 keep-alive events before failing over.



Note When the primary server is active but not receiving keep-alive events from the secondary server, failover will not occur because the secondary server may not be able to take calls. Similarly, when the secondary server is active but not receiving keep-alive events from the primary server, failback will not occur because the primary server may not be able to take calls.

- The frequency of file replication. The default setting is to replicate changed files every 10 minutes.
- Whether the secondary server initiates failback to the primary server during a certain time range each day. The default setting is for manual failback.
- Whether failover is initiated when a call is answered by a port on the secondary server. The default setting is to enable failover initiation.

You customize failover and failback on only one server. Changes to failover configuration are replicated to the other server.

To Customize Failover and Failback Settings

- Step 1** On either server (unless otherwise noted in [Table 1-2](#)), on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Configure**.
- Step 3** Using [Table 1-2](#), change the applicable values in the Failover Configuration dialog box.

Table 1-2 Failover and Failback Configuration Settings

Field	Value
Interval (ms)	Specify the amount of time that elapses between keep-alive events. <i>The default setting is 1,000 milliseconds (1 second).</i> Increasing the interval between keep-alive events decreases network traffic. However, it also increases the amount of time before the secondary server begins answering calls if the primary server fails.

Table 1-2 Failover and Failback Configuration Settings (continued)

Field	Value
Missed Events Before Failover	<p>Specify the number of keep-alive events from the primary server that the secondary server must miss before it becomes the active server. <i>The default is 30 keep-alive events.</i></p> <p>Decreasing the number of missed keep-alive events before failover may cause a network glitch or abnormally high traffic on the network to trigger an unnecessary failover. Increasing the number increases the amount of time before the secondary server begins answering calls if the primary server fails.</p> <p>Note that failover can also be initiated under other circumstances. Some errors are detected immediately (for example, if the Cisco Unity service—AvCsMgr.exe—stops running), and failover is initiated when the error is detected.</p>
File Replication Interval (In Minutes)	<p>Specify the amount of time that elapses before the active server replicates changed files to the inactive server. <i>The default is 10 minutes.</i></p> <p>Increasing the file replication interval causes the active server to replicate files to the inactive server less often, which decreases network traffic.</p>
Failback Type	<ul style="list-style-type: none"> • If you do not want to schedule the secondary server to initiate failback to the primary server, click Manual. The secondary server fails back only when you manually initiate failback by using the Failover Monitor. <i>The default is the Manual failback type.</i> • If you want to schedule when the secondary server initiates failback to the primary server, click Scheduled, and enter settings for the Scheduled Failback Start and Scheduled Failback End field. (You can manually initiate failback before the scheduled time in the Failover Monitor.)
Scheduled Failback Start and Scheduled Failback End	<p>If you chose Scheduled in the Failback Type field, enter the range of time in which the secondary server initiates failback. <i>The default is 3 a.m. to 6 a.m.</i></p>
Force Failover If Call Arrives on Inactive Secondary	<p>Set this field only on the secondary server. The setting does not replicate between servers.</p> <ul style="list-style-type: none"> • Check the check box to enable failover initiation when a call is not answered by a voice messaging port on the primary server, is forwarded to the secondary server, and then is answered by a port on the secondary server. <i>The default is to enable failover initiation.</i> • Uncheck the check box to disable failover initiation when a call is answered by a port on the secondary server.

Step 4 Click **OK** to close the Failover Configuration dialog box.

Step 5 Close the Failover Monitor.

Disabling Failover Initiation When Calls Are Unanswered on the Primary Server (Optional)

By default, failover is initiated when a call is not answered by a voice messaging port on the primary server, is forwarded to the secondary server, and then is answered by a port on the secondary server.

Do the following procedure if you want to disable the initiation of failover when calls are unanswered on the primary server.

To Disable Failover Initiation When Calls Are Unanswered on the Primary Server

- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Configure**.
- Step 3** Uncheck the **Force Failover If Call Arrives on Inactive Secondary** check box.
- Step 4** Click **OK**.
-