



# Configuring Software on the Server, and Installing a Service Release

In this chapter, you configure Cisco Unity Connection software or voice-recognition software, install a service release (if applicable), and test the phone system integration. If antivirus software is installed on the server, you also exclude selected directories from scanning. When you are finished with this chapter, return to “[Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System.](#)”



## Note

The tasks in the list reference detailed instructions in the *Cisco Unity Connection Installation Guide* and in other Cisco Unity Connection documentation. Follow the documentation for a successful installation.

The chapter contains the following sections:

- [Configuring Cisco Unity Connection Software \(Connection Server Only\)](#), page 5-1
- [Configuring Voice-Recognition Software \(Separate Voice-Recognition Server Only\)](#), page 5-3
- [Installing a Service Release \(If Applicable\)](#), page 5-5
- [Testing the Phone System Integration \(Connection Server Only\)](#), page 5-6
- [Excluding Selected Directories from Virus Scanning](#), page 5-6

## Configuring Cisco Unity Connection Software (Connection Server Only)

Do the following procedure on the Cisco Unity Connection server to specify passwords, install license files, and configure Connection for the phone system.

### To Configure Cisco Unity Connection Software (Connection Server Only)

- Step 1** Log on to Windows by using an account that is a member of the local Administrators group.  
The Cisco Unity Connection Configuration Assistant starts automatically. Note that it may require a few minutes to appear.
- Step 2** If a message box appears explaining that Internet Explorer Enhanced Security Configuration is enabled, check the **In the Future, Do Not Show This Message** check box, and click **OK**.
- Step 3** On the Welcome to the Cisco Unity Connection Configuration Assistant page, click **Next**.

**Step 4** On the Set Alias and Password for Default Administrator page, in the Alias field, enter the alias for the first (default) Cisco Unity Connection Administration account. You use this alias to log on to Connection Administration for the first time.

**Step 5** In the Password and Confirm Password fields, enter and confirm a password for the first Cisco Unity Connection Administration account. You use this password to log on to Connection Administration for the first time.

**Caution**

If you forget the value you enter for Alias or Password, you will have to uninstall and reinstall Cisco Unity Connection software.

Enter a password that meets the following criteria:

- Is at least <minimum password length> characters long.
- Includes at least three of the following characters:
  - An upper-case letter
  - A lower-case letter
  - A number
  - A symbol: ~ ! @ # \$ % ^ \* ' , . : ; ? - \_ ( ) [ ] < > { } + = / \ |
- Does not consecutively repeat any character more than three times. (For example, aaaB1C9 is invalid.)

**Step 6** Click **Next**.

**Step 7** On the Set Web Application Password and Voice Mail Password for Default User Template page, enter and confirm the password that users whose accounts will be created with the default user template will use to log on to the Cisco Personal Communications Assistant (PCA).

Enter a password that meets the following criteria:

- Is at least <minimum password length> characters long.
- Includes at least three of the following characters:
  - An upper-case letter
  - A lower-case letter
  - A number
  - A symbol: ~ ! @ # \$ % ^ \* ' , . : ; ? - \_ ( ) [ ] < > { } + = / \ |
- Does not consecutively repeat any character more than three times. (For example, aaaB1C9 is invalid.)

(The Cisco PCA website provides access to the web tools that users use to manage messages and personal preferences with Cisco Unity Connection.)

**Step 8** Enter and confirm the password that users whose accounts will be created with the default user template will use to log on to Cisco Unity Connection by phone.

Enter a password that meets the following criteria:

- Is at least <minimum password length> digits long.
- Contains three or more different numbers. (For example, 122112 is invalid.)
- Does not consecutively repeat any number more than twice. (For example, 333479 is invalid.)
- Does not contain groups of repeated digits. (For example, 408408 and 113377 are invalid.)

- Does not use a series of digits that all appear in a straight line on the phone keypad. (For example, 147 and 2580 are invalid.)
- Does not consist entirely of ascending or descending numbers. (For example, 123456 and 654321 are invalid.)

**Step 9** Click **Next**.

**Step 10** If Cisco Unity Connection license files are saved on a removable media, for example, a diskette or CD, insert the media into the drive on the Connection server.

**Step 11** Install the license file(s):

- a. On the Install Cisco Unity Connection License Files page, click **Browse**.
- b. In the Open File dialog box, browse to the location of the Cisco Unity Connection license file.
- c. Double-click the name of the file.
- d. On the Install Cisco Unity Connection License Files page, click **Add Selected**.

**Step 12** If you have more than one license file, repeat **Step 11** until you have installed all license files.

**Step 13** Click **Next**.

**Step 14** Beginning on the Select Phone System Manufacturer page, follow the on-screen prompts to configure Cisco Unity Connection for the integration with the phone system. Refer to the applicable Cisco Unity Connection integration guide for information on the values to specify. Integration guides are available at [http://www.cisco.com/en/US/products/ps6509/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html).

**Step 15** On the Cisco Unity Connection Configuration Complete page, click the link to start Cisco Unity Connection Administration, or close the browser.

## Configuring Voice-Recognition Software (Separate Voice-Recognition Server Only)



### Note

If you are not installing a separate voice-recognition server, skip this section. When you installed Cisco Unity Connection software on the Connection server, the voice-recognition software was also installed and automatically configured for that server.

This section contains four procedures. Do the procedures in the order listed after you have installed software on both the Cisco Unity Connection server and the voice-recognition server.

### To Configure the Voice-Recognition Server in Cisco Unity Connection Administration

**Step 1** On the Cisco Unity Connection server, log on to Windows by using an account that is a member of the local Administrators group.

**Step 2** In Cisco Unity Connection Administration, expand **System Settings**, then click **Voice Recognition Server**.

**Step 3** On the Search Voice Recognition Server page, click **Local Voice Recognition Server**.

- Step 4** On the New Voice Recognition Server page, in the Display Name field, change the name for the server, if applicable.
  - Step 5** In the IP Address field, enter the IP address of the voice-recognition server.
  - Step 6** Click **Save**.
  - Step 7** Close Cisco Unity Connection Administration.
- 

#### To Disable the Nuance Watcher Daemon Service and Restart the CuVrt Service on the Connection Server

---

- Step 1** On the Cisco Unity Connection server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2** In the right pane, right-click the **Nuance Watcher Daemon** service, and click **Stop**.
  - Step 3** When the Nuance service has stopped, double-click the **Nuance Watcher Daemon** service.
  - Step 4** On the General tab of the Nuance Watcher Daemon Properties dialog box, in the Startup Type list, click **Disabled**.
  - Step 5** Click **OK** to close the dialog box.
  - Step 6** In the right pane, right-click the **CuVrt** service, and click **Restart**.
  - Step 7** Close the Services MMC.
- 

#### To Restart the Nuance Watcher Daemon Service on the Voice-Recognition Server

---

- Step 1** On the voice-recognition server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2** In the right pane, right-click the **Nuance Watcher Daemon** service, and click **Stop**.
  - Step 3** When the Nuance service has stopped, right-click the **Nuance Watcher Daemon** service, and click **Start**.
  - Step 4** Close the Services MMC.
- 

#### To Secure the Connection Between the Cisco Unity Connection Server and the Voice-Recognition Server

---

- Step 1** On the Cisco Unity Connection server, browse to the directory **G:\Cisco Systems\Cisco Unity Connection\TechTools**, and run **NetworkSecurityWizard.exe**.
- Step 2** On the Overview page, click **Next**.
- Step 3** On the Windows Firewall Configuration page, click **Next** to accept the default configuration.
- Step 4** On the IPSec Configuration page, check the **Configure IPSec for Speech Recognition Traffic** check box.
- Step 5** In the IP Address of the Speech Recognition Server field, enter the IP address of the voice-recognition server.

- Step 6** In the Pre-shared Key or Passphrase for Speech Recognition IPSec Authentication field, enter a 15-character or greater key or passphrase. This value will be used to encrypt network traffic between the Connection server and the voice-recognition server.
- Write down the key or passphrase that you specify. You will need it again later in this procedure because the Connection server and the voice-recognition server must use the same value to encrypt and decrypt traffic.
- Step 7** In the Confirm Pre-shared Key field, re-enter the value that you entered in [Step 6](#).
- Step 8** Click **Next**.
- Step 9** On the Confirmation page, click **Configure**.
- Step 10** On the Execute Configuration page, click **Next**.
- Step 11** On the Completion page, click **Finish**.
- Step 12** On the voice-recognition server, browse to the directory **G:\Cisco Systems\Cisco Unity Connection\TechTools**, and run **NetworkSecurityWizard.exe**.
- Step 13** On the Overview page, click **Next**.
- Step 14** On the Windows Firewall Configuration page, click **Next** to accept the default configuration.
- Step 15** On the IPSec Configuration page, check the **Configure IPSec for Cisco Unity Connection Traffic** check box.
- Step 16** In the IP Address of the Cisco Unity Connection Server field, enter the IP address of the Cisco Unity Connection server.
- Step 17** In the Pre-shared Key or Passphrase for Cisco Unity Connection IPSec Authentication field, enter the same 15-character or greater key or passphrase that you entered in [Step 6](#).
- Step 18** In the Confirm Pre-shared Key field, re-enter the value that you entered in [Step 6](#).
- Step 19** Click **Next**.
- Step 20** On the Confirmation page, click **Configure**.
- Step 21** On the Execute Configuration page, click **Next**.
- Step 22** On the Completion page, click **Finish**.
- 

## Installing a Service Release (If Applicable)

If you downloaded a Cisco Unity Connection service release in the “[Downloading Software for the Installation](#)” section on page 2-2, install it now. For installation instructions, see the following documentation, depending on the Connection version:

- For Connection 1.2(1) and later, refer to *Release Notes for Cisco Unity Connection <Version> Service Release <Number>* at [http://www.cisco.com/en/US/products/ps6509/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html).
- For Connection 1.1(1), refer to the “Cisco Unity Connection 1.1(1) Service Release 1” section under “New Support—Release 1.1(1)” in *Release Notes for Cisco Unity Connection Release 1.1(1)* at [http://www.cisco.com/en/US/products/ps6509/prod\\_release\\_note09186a008058bbd1.html](http://www.cisco.com/en/US/products/ps6509/prod_release_note09186a008058bbd1.html).

# Testing the Phone System Integration (Connection Server Only)

Test the integration with the phone system. Refer to the Cisco Unity Connection integration guide for the phone system.

Note that you use Cisco Unity Connection Administration for part of the integration test. Use the default administration account and the password that you specified when you ran the Cisco Unity Connection Configuration Assistant in the [“Configuring Cisco Unity Connection Software \(Connection Server Only\)”](#) section on page 5-1.

## Excluding Selected Directories from Virus Scanning

**Note**

---

If antivirus software is not installed on the Cisco Unity Connection server or on the voice-recognition server, skip this section.

---

You exclude selected directories from virus scanning so that Cisco Unity Connection Administration, the Cisco Unity Assistant web tool, and voice recognition will function properly.

This section contains two procedures. Do the applicable procedure for excluding the selected directories, depending on whether you installing the Connection server or the separate voice-recognition server.

### To Exclude Selected Directories on the Cisco Unity Connection Server from Virus Scanning

---

- Step 1** On the Cisco Unity Connection server, log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On the Windows desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 3** In the left pane of the Tools Depot, expand **Reporting Tools**.
- Step 4** Double-click **Gather Unity System Info**.
- Step 5** Start the administration interface for the antivirus software.
- Step 6** Exclude from virus scanning the directories associated with the following items (the directories are listed in Gather Unity System Info):
  - Logging Diagnostics and Data Files To
  - Storing Greeting and Voice Name Files To
  - Storing Message Attachment Wav Files To
  - Storing Mdf Database Files To

- Storing Ldf Database Files To
- The parent directory of the SMTP Server Drop directory. (For example, if the SMTP Server Drop directory is C:\Inetpub\mailroot\Drop, exclude C:\Inetpub\mailroot.)

**Caution**

Do not configure antivirus software to block WAV attachments, or voice messages will be stripped of their recordings. In addition, do not configure antivirus software to scan WAV files, .log files, or .tmp files. Finally, do not configure antivirus software to block TCP or UDP port traffic, or Cisco Unity Connection may not function properly.

Refer to the antivirus software Help for instructions on excluding directories from scanning.

**Step 7**

Exclude from virus scanning the following three directories:

- Nuance
- NuanceLogs
- The directory in which Cisco Unity Connection was installed, and all subdirectories under that directory.

Refer to the antivirus software Help for instructions on excluding directories from scanning.

---

**To Exclude Selected Directories on the Voice-Recognition Server from Virus Scanning****Step 1**

On the voice-recognition server, log on to Windows by using an account that is a member of the local Administrators group.

**Step 2**

Start the administration interface for the antivirus software.

**Step 3**

Exclude the following two directories from virus scanning:

- Nuance
- NuanceLogs

**Caution**

Do not configure antivirus software to block WAV attachments, or voice messages will be stripped of their recordings. In addition, do not configure antivirus software to scan WAV files, .log files, or .tmp files. Finally, do not configure antivirus software to block TCP or UDP port traffic, or Cisco Unity Connection may not function properly.

Refer to the antivirus software Help for instructions on excluding directories from scanning.

