



Administering the Cisco Voice Provisioning Tool

This chapter provides step-by-step procedures for configuring the main administrative components of the Cisco Voice Provisioning Tool. These procedures allow you to configure the Cisco Unity and Cisco CallManager product systems on which provisioning actions will occur, and to provide (and limit) role-based access to multiple administrative users.

If you are unfamiliar with the general concepts that this chapter discusses, you should first read the “[Cisco Voice Provisioning Tool System Overview](#)” chapter, then review the following sections before beginning to configure the tool:

- [Adding and Managing Product Systems, page 3-1](#)
- [Adding and Managing Roles, page 3-11](#)
- [Adding and Managing Administrators, page 3-12](#)

Adding and Managing Product Systems

The Cisco Voice Provisioning Tool automatically includes plug-ins for Cisco CallManager version 4.1(3) and Cisco Unity version 4.0(5). To configure VPT to allow provisioning on a Cisco CallManager or Cisco Unity server, you must configure the server as a product system. See the appropriate section for details:

- [Adding a Cisco CallManager Server, page 3-1](#)
- [Adding a Cisco Unity Server, page 3-3](#)
- [Modifying a Product System, page 3-9](#)
- [Deleting a Product System, page 3-10](#)

Adding a Cisco CallManager Server

Use the task list that follows to add a Cisco CallManager system to the Cisco Voice Provisioning Tool.

1. Set up the Cisco CallManager server or cluster. For information on installing and setting up the Cisco CallManager server(s), refer to the Cisco CallManager installation/upgrade documents, the *Cisco CallManager System Guide*, and the *Cisco CallManager Administration Guide*.
2. Set up an administrative account on the Cisco CallManager server to be used by VPT to authenticate with the product system. See the “[Setting Up a Provisioning Account on the Cisco CallManager Server](#)” section on page 3-2.

3. Add the Cisco CallManager system to VPT as a new product system. See the “Adding a New Cisco CallManager Product System to the Cisco Voice Provisioning Tool” section on page 3-2.
4. Test the product system connection. See the “Testing the Product System Connection” section on page 3-3.

Setting Up a Provisioning Account on the Cisco CallManager Server

You must configure the Cisco Voice Provisioning Tool with an account that has full access rights for provisioning Cisco CallManager.

You can use an existing account; however, we recommend creating an account specifically for VPT. If you have Multilevel Administration Access (MLA) enabled on the system, you can use the CCMAAdministrator account, or any account with super user privileges, or create a new account and add it to the SuperUserGroup. If MLA is not enabled, create or use an existing local NT administrator account. Be sure to let other administrators know if you have created a new account, so they do not inadvertently delete it.

Refer to the *Cisco CallManager Administration Guide* for details on setting up users and access rights.

Adding a New Cisco CallManager Product System to the Cisco Voice Provisioning Tool

For each Cisco CallManager cluster, you configure a product system in VPT to represent the publisher server (if there is only one Cisco CallManager server acting as publisher and subscriber, you configure that server as the product system). To add the server as a product system in VPT, perform the following procedure.



Note

To add a product system, your administrator account must belong to a role that has Product Systems Management Add permissions for the VPT application. If you do not see the VPT Administration > Product Systems > Add New Product System option in the VPT navigation menu, your account does not have the applicable permissions.

To Add a New Cisco CallManager Product System

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Add New Product System**.

The Add New Product System window displays.

- Step 2** From the Product System Type drop-down list, choose **CCM-4.1.3**.



Note

The options that are available when a new product system is added depend on the product system type that you choose in this step.

- Step 3** Enter the Product System Name.

- Step 4** Optionally, enter the URL for the Cisco CallManager CCMAdmin interface.

This allows administrators with sufficient permissions to click the Product SA URL link from the Manage Product Systems window to easily browse to this URL to carry out any additional configuration activities.

This URL is typically **https://<Server Name or IP Address>/CCMAdmin/main.asp**.

- Step 5** Optionally, enter a description for the product system.
- Step 6** Enter the CCM Publisher IP Address/Hostname.
- Step 7** Enter the CCM Publisher AXL Port.
VPT uses this port to communicate with the Cisco CallManager provisioning API (AXL). For most installations, this typically means port 80. However, if the port on which IIS is running on the Cisco CallManager server has been changed from the default, enter that port number here.
- Step 8** Enter the CCM Publisher Login ID and Password and confirm the password.
This information must match the provisioning account on the Cisco CallManager server.
- Step 9** Click **Save**.
-

Testing the Product System Connection

When the product system setup is complete, you should test it by using the check that the tool provides.



Note

To test product system connections, your administrator account must belong to a role that has Product System Connection Test permissions for the product system. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Test the Product System Connection

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.
The Manage Product Systems window displays a list of configured product systems.
- Step 2** In the Test Connection column of the product system that you want to test, click **Test**. If the test is successful, you should see a PASSED result for all tests.
-

Adding a Cisco Unity Server

Use the task list that follows to add a Cisco Unity system to the Cisco Voice Provisioning Tool.

1. Set up the Cisco Unity server or failover pair. Refer to the appropriate *Installation Guide for Cisco Unity* for your configuration.
2. Set up an administrative account on the Cisco Unity server to be used by VPT to authenticate with the product system. See the [“Setting Up a Provisioning Account on the Cisco Unity Server”](#) section on page 3-4.
3. Add the Cisco Unity system to VPT as a new product system. See the [“Adding a New Cisco Unity Product System to the Cisco Voice Provisioning Tool”](#) section on page 3-4.
4. If SSL has been configured on the Cisco Unity server(s), continue with the SSL configuration on the Cisco Voice Provisioning Tool server. See the [“Completing the SSL Configuration on the Cisco Voice Provisioning Tool Server”](#) section on page 3-5.

5. Test the product system connection. See the “Testing the Product System Connection” section on page 3-9.

Setting Up a Provisioning Account on the Cisco Unity Server

You must configure the Cisco Voice Provisioning Tool with an account that has full access rights to the Cisco Unity System Administrator.

You can use an existing subscriber account that can log in to the Cisco Unity System Administrator and that belongs to a Class of Service with permissions to add and delete subscribers. However, we recommend that you set up a separate subscriber specifically for use with VPT and notify other administrators that the subscriber should not be deleted. You can also give the new subscriber a display name that indicates the purpose of the account and specifies that it should not be removed from the system. You may also want to hide the new subscriber from the directory, so that other subscribers do not inadvertently address messages to it. Refer to the *Cisco Unity System Administration Guide* for details on setting up subscribers.

Adding a New Cisco Unity Product System to the Cisco Voice Provisioning Tool

For each Cisco Unity server on which subscribers are homed, you configure a product system in VPT. (If failover is in use, you add the failover pair as a single product system, and configure the product system with information about both the primary and the secondary server.) To add a Cisco Unity server as a new product system in VPT, perform the following procedure.



Note

To add a product system, your administrator account must belong to a role that has Product Systems Management Add permissions for the VPT application. If you do not see the VPT Administration > Product Systems > Add New Product System option in the VPT navigation menu, your account does not have the applicable permissions.

To Add a New Cisco Unity Product System

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Add New Product System**.

The Add New Product System window displays.

- Step 2** Choose **UNITY-4.0.5** from the Product System Type drop-down list.



Note

The options available when adding a new product system depend on the product system type that you choose in this step.

- Step 3** Enter the Product System Name.

- Step 4** Optionally, enter the URL for the Cisco Unity System Administrator interface.

This allows administrators with sufficient permissions to click the Product SA URL link from the Manage Product Systems window to easily browse to this URL to carry out any additional configuration activities.

This URL is typically **https://<Server Name or IP Address>/web/sa**.

- Step 5** Optionally, enter a description for the product system.

- Step 6** Enter the Cisco Unity IP Address/Hostname.

If Cisco Unity is configured for failover, enter the primary server IP address or hostname.

Step 7 Enter the Unity CUAL Port.

VPT uses this port to communicate with the Cisco Unity provisioning API. For most installations, this is typically port 80 if SSL is disabled or port 443 if SSL is enabled. However, if the port on which IIS is running on the Cisco Unity server has been changed from the default, enter that port number here.

Step 8 If Cisco Unity is configured for failover, enter the secondary server IP address or hostname and CUAL port in the Failover IP Address/Hostname and Failover CUAL Port fields.

Step 9 In the Security drop-down menu, specify whether SSL is enabled or disabled (no security) on the Cisco Unity System Administrator.

If failover is in use, this setting applies to both the primary and the secondary Cisco Unity server. If SSL is configured on the primary server, it must also be configured on the secondary server for VPT to communicate with the secondary server if the primary server is unavailable.

Step 10 Enter the Cisco Unity Login ID and Password and confirm the password.

This information must match the provisioning account on the Cisco Unity server. If the Cisco Unity account that you plan to use is a Windows domain account that overlaps with a local account by the same name on the Cisco Unity server (such as Administrator), you should specify the domain as well as the account name in the Login ID field (for example, UMdom\Administrator).

Step 11 Click **Save**.

Step 12 If SSL is configured for the product system, continue with the [“Completing the SSL Configuration on the Cisco Voice Provisioning Tool Server”](#) section on page 3-5. Otherwise, skip to the [“Testing the Product System Connection”](#) section on page 3-9.

Completing the SSL Configuration on the Cisco Voice Provisioning Tool Server

The Cisco Unity provisioning API (CUAL) and the Cisco Voice Provisioning Tool plug-in for Cisco Unity 4.0(5) support the configuration of Secure Sockets Layer (SSL) communications. When you configure the Cisco Unity web applications (the Cisco Unity Administrator, Status Monitor, and Cisco Personal Communications Assistant) to use SSL, the CUAL interface that VPT uses to communicate with Cisco Unity will also be secured with SSL.

After SSL has been configured on the Cisco Unity system, and a certificate has been procured or generated for the system, do the following tasks to set up secure communication with the system on the VPT server:

1. If you do not already have access to a copy of the server certificate(s), export a copy. See either the [“To Export a Certificate Generated by a Certificate Authority \(CA\)”](#) procedure on page 3-6 or the [“To Export Self-Signed Certificates”](#) procedure on page 3-6.
2. Copy the certificate(s) to the VPT server. See the [“To Copy Certificates to the VPT Server”](#) procedure on page 3-7.
3. Add the product system certificate(s) to a keystore on the VPT server. See the [“To Add Certificates to a Keystore by Using Keytool”](#) procedure on page 3-7.
4. If you have not already done so, configure the keystore properties in the Cisco Voice Provisioning Tool. See the [“To Configure Keystore Information in the Cisco Voice Provisioning Tool”](#) procedure on page 3-9.

To Export a Certificate Generated by a Certificate Authority (CA)

- Step 1** On the CA server, on the Windows Start menu, choose **Programs > Administrative Tools > Certification Authority**.
 - Step 2** In the left pane of the Certification Authority window, right-click the <Root Certification Authority name>, and click **Properties**.
 - Step 3** Click **View Certificate**.
 - Step 4** Click the **Details** tab.
 - Step 5** In the Show list, choose **All** and click **Copy to File**.
 - Step 6** On the Certificate Export wizard welcome window, click **Next**.
 - Step 7** Click **Base-64 Encoded X.509 (.CER)** and click **Next**.
 - Step 8** Specify a file name and a location and click **Next**.
 - Step 9** Verify the settings and click **Finish**.
 - Step 10** To close the Certificate Details dialog box, click **OK**.
 - Step 11** To close the Properties dialog box for the Root Certification Authority, click **OK**.
 - Step 12** Close the **Certification Authority** window.
-

To Export Self-Signed Certificates

- Step 1** On the Cisco Unity server, on the Windows Start menu, choose **Programs > Administrative Tools > Internet Services Manager**. (If failover is in use, begin this procedure on the primary Cisco Unity server and repeat the procedure on the secondary server.)
- Step 2** To expand the Cisco Unity server, double-click the name of the Cisco Unity server.
- Step 3** Right-click **Default Web Site** and click **Properties**.
- Step 4** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 5** Click **View Certificate**.
- Step 6** Click the **Details** tab.
- Step 7** In the Show list, choose **All** and click **Copy to File**.
- Step 8** On the Certificate Export wizard welcome window, click **Next**.
- Step 9** Click **No, Do Not Export the Private Key** and click **Next**.
- Step 10** Click **Base-64 Encoded X.509 (.CER)** and click **Next**.
- Step 11** Specify a file name and a location and click **Next**.
- Step 12** Verify the settings, and click **Finish**.
- Step 13** To close the Certificate Details dialog box, click **OK**.
- Step 14** To close the Properties dialog box for the Root Certification Authority, click **OK**.
- Step 15** To close the Certificate window, click **OK**.
- Step 16** To close the Default Web Site Properties window, click **OK**.
- Step 17** Close the **Internet Information Services** window.

- Step 18** If failover is in use, repeat [Step 1](#) through [Step 17](#) on the secondary Cisco Unity server.
-

To Copy Certificates to the VPT Server

- Step 1** Copy the certificate(s) to the VPT server by doing the applicable steps:
- Recommended—By using a floppy disk. Continue with [Step 2](#).
 - For secure networks—By using a network share. Skip to [Step 3](#).
- Step 2** If you are using a floppy disk to copy the certificate, do the following substeps:
- a. Insert an empty formatted floppy disk in the floppy drive of the Cisco Unity or CA server.
 - b. Browse to the directory that contains the certificate (.CER) file(s).
 - c. Copy the certificate file(s) to the floppy disk.
 - d. Remove the floppy disk from the Cisco Unity or CA server.
 - e. Insert the floppy disk in the floppy drive of a VPT server.
 - f. Copy the certificate file(s) on the floppy disk to a directory on the VPT server.
 - g. For security, delete the certificate file(s) on the floppy disk.
- Step 3** If you are using a secure network share to copy the certificate(s), do the following substeps:
- a. On the Cisco Unity or CA server, browse to the directory that contains the certificate.
 - b. Select the certificate file, and press **Ctrl-C**.
 - c. Open a network share to the VPT server and log on.
 - d. Browse to or create a directory on the VPT server in which to store certificates.
 - e. To paste the certificate file, press **Ctrl-V**.
-

To configure VPT to communicate with product systems that are using SSL, you must use the keytool application, which is included as part of the Sun Microsystems Java Development Kit (JDK) when you install the Cisco Voice Provisioning Tool.

The keytool application creates a keystore (by default, the keystore is stored as a file). You can store multiple certificates in a keystore; the keystore is created automatically when you add the first certificate by using the keytool application. For more information on the keytool command, refer to the Sun Microsystems Java Development Kit documentation.

To Add Certificates to a Keystore by Using Keytool

- Step 1** On the VPT server, check to make sure that the PATH environment variable on the system includes the path to the bin directory of the JDK that is installed with VPT:
- a. On the Windows Start menu, choose **Settings > Control Panel > System**.
 - b. Click the **Advanced** tab.
 - c. Click **Environment Variables**.
 - d. In the System Variables list, find and click the **Path** variable and click **Edit**.

- e. If it is not already present in the path, add the full path to the bin directory of the JDK that is installed with VPT. Make sure that a semicolon (;) separates the new entry from any other entries. For example, if the JDK was installed in C:\j2sdk1.4.2_03, add the following to the end of the path:
;C:\j2sdk1.4.2_03\bin
- f. Click **OK**.
- g. Close the System Properties and Control Panel windows.

Step 2 Verify that the JDK tools are available by using the path specified in [Step 1](#):

- a. On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.
- b. In the command prompt window, enter **javac**. If the path is set correctly, usage information for the javac command displays.

Step 3 In the command prompt window that opened in [Step 2](#), change to the directory where the Cisco Voice Provisioning Tool is installed. For example, enter:
cd C:\Program Files\Cisco Systems\Voice Provisioning Tool
and press **Enter**.

Step 4 Enter
keytool -import -alias <Name of Server the Certificate was Obtained From> -storepass <Password> -File <Certificate File> -keystore <Keystore File>
and press **Enter**.

We recommend that you use the name of the product system or certificate authority from which the certificate was obtained for the alias. For example, if a self-signed certificate file from server c-unity1 is stored in C:\certificates\c-unity1-cert.CER, you might enter: `keytool -import -alias c-unity1 -storepass pa$$w0rd! -File C:\certificates\c-unity1-cert.CER -keystore C:\VPTProdSysKeystore`



Note The `-keystore` parameter specifies a file that holds the keystore. If you do not specify a full path, the file is created in the directory in which you run the `keytool` command. You will need to know the full path to the keystore file to configure the VPT security settings in the next procedure.

Step 5 When prompted to trust the certificate, enter **yes** and press **Enter**.

Step 6 To verify that the import was successful, enter
keytool -list -keystore <Keystore File>
and press **Enter**.

Step 7 Repeat [Step 4](#) through [Step 6](#) for each certificate. If Cisco Unity is configured for failover, add the certificates for both the primary and secondary servers.



Note Ensure all product system keys are stored in the same keystore for the Cisco Voice Provisioning Tool to access them. Make sure you use the correct syntax for the keystore value each time that you enter a new certificate.

Step 8 Close the command prompt window.

**Note**

To configure keystore settings, your administrator account must belong to a role that has VPT Configuration Modify permissions for the VPT application. If you do not see the VPT Administration > Configuration option in the VPT navigation menu, your account does not have the applicable permissions.

To Configure Keystore Information in the Cisco Voice Provisioning Tool

-
- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**. The Configuration window displays.
- Step 2** In the Security settings section, enter the full path of the keystore and the password that you specified in [Step 4](#) of the “[To Add Certificates to a Keystore by Using Keytool](#)” procedure on page 3-7.
- Step 3** Click **Save**.
- Step 4** For the changes to take effect, you must restart the Tomcat service. On the Windows Start menu, choose **Programs > Administrative Tools > Services**. In the right pane, locate **VPT Tomcat**, right-click it, and click **Restart**.
-

Testing the Product System Connection

When the product system setup is complete, you should test it by using the check that the tool provides.

**Note**

To test product system connections, your administrator account must belong to a role that has Product System Connection Test permissions for the product system. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Test the Product System Connection

-
- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**. The Manage Product Systems window displays a list of configured product systems.
- Step 2** Click the Test button in the Test Connection column of the product system that you want to test. If the test is successful, you should see a PASSED result for all tests.
-

Modifying a Product System

From the Manage Product Systems window, you can choose a product system and modify some of the settings after a product system has been created. However, once a product system has been created, you cannot modify the product system type or name. You must delete the product system and re-add it if you want to change these values.

Use the procedure that follows to change the product description, system administration URL, or account details. To change the security settings on a Cisco Unity product system, see the [“Configuring Secure Communication with Product Systems”](#) section on page 4-4.

**Note**

To modify a product system, your administrator account must belong to a role that has Product Systems Management View and Modify permissions for the VPT application. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Modify a Product System

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.

The Manage Product Systems window displays.

Step 2 Click the name of the product system that you want to modify.

Step 3 Modify the product description, URL, connection details, or account details as desired.

**Note**

After a product system is created, you cannot modify the product system type or name. You must delete the product system and re-add it if you want to change these values.

Step 4 Click **Save**.

**Tip**

After modifying a product system, use the Test button on the Manage Product Systems window to verify that the Cisco Voice Provisioning Tool can still connect to the product system.

Deleting a Product System

**Note**

To delete a product system, your administrator account must belong to a role that has Product Systems Management View and Delete permissions for the VPT application. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Delete a Product System

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.

The Manage Product Systems window displays.

Step 2 Click the check box to the left of the product system name for each product system that you want to delete.

To choose all product systems for deletion, click the check box at the top left corner of the table.

Step 3 Click **Delete**.

Adding and Managing Roles

In addition to the predefined roles, administrators with sufficient permissions can add, modify, or delete custom roles.

When creating a custom role, be aware that many of the individual permissions that you can grant require other permissions to be granted in order for the action that is being permitted to be visible to the administrator. For example, if you grant to a role only the bulk provisioning permissions for the VPT Application, an administrator who is assigned to that role cannot perform bulk actions on any product systems, unless provisioning permissions are explicitly granted on this or another role to which the administrator is also assigned.



Note

Only the superadmin and other administrators who are assigned to the predefined Super Admin role can add, modify, or delete roles.

To Add a New Role

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Roles > Add New Role**.
The Add New Role window displays.
- Step 2** Enter a Role Name and Role Description.
Enter no more than 80 characters in the role name field and no more than 256 characters in the role description field. The system validates the name and description and displays an error message in the GUI if a problem exists.
- Step 3** In the Permissions table, find the row corresponding to the Product System Name for which you want to add privileges and click **Modify**.
- Step 4** Click the check box for each permission that you want to add or check **All Permissions** to apply all permissions that are available to the product system.
- Step 5** Click **Save**.
- Step 6** Repeat [Step 3](#) through [Step 5](#) for each product system for which you want to grant permissions.
- Step 7** When all permissions are granted, on the Add New Role window, click **Save**.
-

To Modify a Role

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Roles > Manage Roles**.
The Manage Roles window displays.
- Step 2** Click the name of the role that you want to modify.



Note The predefined Super Admin role allows all permissions on the VPT application and all product systems. The superadmin account is assigned to this role. You cannot modify or delete this role and you cannot remove the superadmin account from it. You can modify the permissions on the two other predefined roles (Full Provisioning and View-only Provisioning), but you cannot delete these roles from the system.

Step 3 Modify the Role Name, Role Description, and/or Permissions as desired.

Step 4 Click **Save**.



Note Changes to the role take effect immediately after they are saved. If an administrator associated with the role is currently logged in, any changes to the navigation options are reflected in the GUI after the administrator logs out and logs back in.

To Delete One or More Roles

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Roles > Manage Roles**.

The Manage Roles window displays.

Step 2 Click the check box to the left of the Role Name for each role that you want to delete.

To choose all user-defined roles for deletion, click the check box at the top left corner of the table.



Note You cannot delete the predefined roles (Super Admin, Full Provisioning, and View-only Provisioning) from the system.

Step 3 Click **Delete**.

Adding and Managing Administrators

Administrators with sufficient permissions can add, modify, or delete VPT administrator accounts. Although these account names can overlap with account names that are created in individual Cisco CallManager and Cisco Unity servers, the VPT accounts represent independent accounts with separate passwords and permissions. VPT administrator accounts do not have automatic access to the Cisco CallManager or Cisco Unity administrative interfaces.

When creating accounts for new administrators, be sure to let the new administrators know how to access the VPT website, and notify them of considerations for navigating the site. See the [“Considerations for Using the Graphical User Interface” section on page 2-2](#), or refer them to the preface of the *Cisco Voice Provisioning Tool User and Phone Management Guide*.






Note Only the superadmin and other administrators that are assigned to the predefined Super Admin role can add, modify, or delete administrators.

To Add a New Administrator

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Administrators > Add New Administrator**.
- The Add New Administrator window displays.
- Step 2** Enter a First Name and Last Name.
- Enter no more than 24 characters in each field.
- Step 3** From the Status drop-down menu, choose the account status.
- To enable the account for immediate use, choose **Enable**. To disable the account, so that the administrator cannot log in, choose **Disable**.
- Step 4** Enter an Admin ID.
- The Admin ID is used for logging in to the system. You cannot change the Admin ID after the administrator is created. Enter no more than 80 characters.
- Step 5** Enter a temporary Admin Password for the account and reenter the password to confirm it.
- The administrator is prompted to change the password when he or she logs in for the first time.
- Step 6** Click the check box to the left of the Role Name for each role to which the account should be assigned. To choose all roles, click the check box at the top left corner of the table.
- Step 7** Click **Save**.
-

To Modify an Administrator

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Administrators > Manage Administrators**.
- The Manage Administrators window displays.
- Step 2** Click the name of the administrator that you want to modify.
-  **Note** The superadmin account is predefined with all permissions on the VPT application and all product systems. Change the password on the account by logging in to VPT as superadmin and clicking the Change Password link. You cannot otherwise modify the account.
- Step 3** Modify the First Name and/or Last Name as desired.
-  **Note** After an administrator account is created, you cannot modify the AdminID field.
- Step 4** Modify the Status if desired. If you change the account status to disabled, the change takes effect as soon as you save your changes, and the account is disabled even if the administrator is currently logged in to the system.
-  **Note** You cannot disable the account with which you are currently logged in to the system.
- Step 5** If you want to reset the administrator password, click **Reset**. You will be prompted to enter and confirm a new password for the account.



Note When you change an administrator password from the Manage Administrators window, the administrator will be prompted to reset his or her password the next time he or she logs in.

Step 6 Click the check box to the left of the Role Name for each role to which the account should be assigned (or from which the account should be removed). To check all roles, click the check box at the top left corner of the table. To uncheck all roles, click the check box again.

Step 7 Click **Save**.

To Delete One or More Administrators

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Administrators > Manage Administrators**.

The Manage Administrators window displays.

Step 2 Click the check box to the left of the Admin ID for each administrator that you want to delete.

To choose all user-defined administrators for deletion, click the check box at the top left corner of the table.



Note You cannot delete the predefined superadmin account from the system.

Step 3 Click **Delete**.



Note If the administrator is logged in at the time his or her account is deleted, the current operation that he or she is performing will complete. Subsequent operations will result in a “Session Invalid” error message.
