



## **Cisco Voice Provisioning Tool System Management and Security Guide**

Release 1.0(1)

### **Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-7755-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

*Cisco Voice Provisioning Tool System Management and Security Guide*  
Copyright © 2005 Cisco Systems, Inc. All rights reserved.



## **Preface** i

Purpose	i
Audience	ii
Organization	ii
Related Documentation	iii
Conventions	iii
Obtaining Documentation	v
Cisco.com	v
Ordering Documentation	v
Documentation Feedback	v
Obtaining Technical Assistance	vi
Cisco Technical Support Website	vi
Submitting a Service Request	vi
Definitions of Service Request Severity	vii
Obtaining Additional Publications and Information	vii

---

## **CHAPTER 1**

### **Cisco Voice Provisioning Tool System Overview** 1-1

Understanding the Cisco Voice Provisioning Tool Components	1-1
VPT Graphical User Interface (GUI)	1-1
Administrators	1-2
Roles	1-2
Product Systems	1-3
Plug-Ins	1-4
Voice Provisioning	1-4
VPT Database	1-5
Audit Logging	1-5
VPT System Configuration Checklist	1-5

---

## **CHAPTER 2**

### **Accessing the Cisco Voice Provisioning Tool** 2-1

Cisco Voice Provisioning Tool Web Address	2-1
Logging In, Changing Your Password, and Logging Out	2-2
Considerations for Using the Graphical User Interface	2-2
Determining the Cisco Voice Provisioning Tool Version	2-3

Using Online Help 2-3

Accessing Product System Administrative Interfaces from the Cisco Voice Provisioning Tool 2-3

Changing the Session Timeout Length 2-4

Modifying the Number of Search Results That the Cisco Voice Provisioning Tool Returns 2-4

Disabling Administrator Access to the Cisco Voice Provisioning Tool Website 2-5

Changing the HTTP Port Number After Installation 2-6

**CHAPTER 3**

**Administering the Cisco Voice Provisioning Tool 3-1**

Adding and Managing Product Systems 3-1

    Adding a Cisco CallManager Server 3-1

    Adding a Cisco Unity Server 3-3

    Modifying a Product System 3-9

    Deleting a Product System 3-10

Adding and Managing Roles 3-11

Adding and Managing Administrators 3-12

**CHAPTER 4**

**Configuring System Security 4-1**

Configuring Browser Security 4-1

    Configuring SSL for the Cisco Voice Provisioning Tool Web Application After Installation 4-2

    Removing SSL from the Cisco Voice Provisioning Tool Web Application After Installation 4-4

Configuring Secure Communication with Product Systems 4-4

    SSL 4-4

    IPSec 4-12

Password Security 4-12

    Password Security Features Provided by the Cisco Voice Provisioning Tool 4-12

    Actions You Should Take to Ensure Password Security 4-13

**CHAPTER 5**

**Database Management 5-1**

VPT Database Design 5-1

Backing Up the VPT Database 5-1

Restoring the VPT Database 5-2

**CHAPTER 6**

**Audit Logging 6-1**

Audit Log Information 6-1

Audit Log File Storage 6-3

Configuring Audit Log Settings 6-3

Accessing Audit Logs 6-4

---

**CHAPTER 7****Monitoring the VPT System 7-1**

Monitoring the VPT Application via the Windows Event Log 7-1

Using the Audit Logs to Monitor the VPT Application 7-1

---

**INDEX**





## Preface

---

This preface describes the purpose, audience, organization, and conventions for this guide and provides information on how to obtain related documentation:

- [Purpose, page i](#)
- [Audience, page ii](#)
- [Organization, page ii](#)
- [Related Documentation, page iii](#)
- [Conventions, page iii](#)
- [Obtaining Documentation, page v](#)
- [Documentation Feedback, page v](#)
- [Obtaining Technical Assistance, page vi](#)
- [Obtaining Additional Publications and Information, page vii](#)

## Purpose

This *Cisco Voice Provisioning Tool System Management and Security Guide* provides information on the following topics:

- Overview of components of the VPT system and how they fit together
- Procedures for setting up and managing administrators, roles, and product systems for use in provisioning multiple Cisco CallManager and/or Cisco Unity systems
- Procedures and tips for setting up system security, managing the VPT database, and using audit logging to track changes
- Information about monitoring the VPT system.



**Tip**

---

For more information on the topics that this guide provides, see the [““Organization” section on page ii.](#)

---

## Audience

The *Cisco Voice Provisioning Tool System Management and Security Guide*, which is written for system administrators and information systems professionals, serves as a guide for managing and maintaining the Cisco Voice Provisioning Tool software and hardware.

You can perform all the procedures in this guide that involve actions taken on the Cisco Voice Provisioning Tool website by using the superadmin account that was created during installation. Other administrator accounts may or may not have appropriate permissions to perform a given procedure; where necessary, a note appears before each procedure or set of procedures describing these permissions.

## Organization

Table 1 provides a list of chapters and chapter descriptions for this guide.

**Table 1**      **Chapters for Guide**

Chapter	Description
Chapter 1, “Cisco Voice Provisioning Tool System Overview”	Provides a basic overview of the components of the Cisco Voice Provisioning Tool (VPT).
Chapter 2, “Accessing the Cisco Voice Provisioning Tool”	Provides information about accessing the VPT interface; also includes information about navigational aids within the interface.
Chapter 3, “Administering the Cisco Voice Provisioning Tool”	Provides step-by-step procedures for configuring the main administrative components of the tool.
Chapter 4, “Configuring System Security”	Discusses procedures for configuring browser security, securing the communications between the VPT system and the individual product systems, and securing passwords
Chapter 5, “Database Management”	Describes the types of information that are stored in the VPT database; also provides procedures for backing up and restoring the database by using OSQL commands.
Chapter 6, “Audit Logging”	Describes how to configure and access the VPT audit logs, which provide a record of actions taken on the system, when they were performed, and who performed them.
Chapter 7, “Monitoring the VPT System”	Discusses different approaches for monitoring the health and activity of the VPT system.



# Related Documentation

Refer to the following documents for more information on the Cisco Voice Provisioning Tool, Cisco CallManager, and Cisco Unity:

- *Cisco Voice Provisioning Tool Installation and Upgrade Guide*  
This document describes how to install and upgrade the Cisco Voice Provisioning Tool.
- *Cisco Voice Provisioning Tool User and Phone Management Guide*  
This document provides information on how to provision users, phones, and device profiles for Cisco CallManager and Cisco Unity.
- *Cisco Voice Provisioning Tool Release Notes*  
This document describes bugs that are categorized as severity 1, 2, and 3.
- *Cisco CallManager Documentation Guide for Release 4.1(x)*  
This document provides a list of Cisco CallManager documents that are available with the 4.1(x) release (for example, the 4.1(3) release). The document also provides a URL for each document, so you can locate the document on the web. To obtain this documentation guide, click the following URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/4\\_1/doc\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/doc_gd/index.htm)
- *Cisco Unity Documentation Guide*  
This document provides a list of Cisco Unity documents that are available with the 4.0(x) release (for example, the 4.0(5) release). The document also provides a URL for each document, so you can locate the document on the web. To obtain this documentation guide, click the following URL:  
[http://www.cisco.com/en/US/products/sw/voicew/ps2237/products\\_documentation\\_roadmaps\\_list.html](http://www.cisco.com/en/US/products/sw/voicew/ps2237/products_documentation_roadmaps_list.html)

# Conventions

This section contains conventions for the Cisco Voice Provisioning Tool graphical user interface and the documentation.

## Graphical User Interface

Consider the following information as you perform tasks in the Cisco Voice Provisioning Tool. Use the information in conjunction with the descriptions and procedures that this guide discusses.

The Cisco Voice Provisioning Tool uses popup windows. Ensure that your browser is configured to accept popup windows.

The Refresh button that displays in your browser does not refresh the contents in the current configuration window in the Cisco Voice Provisioning Tool. Instead, clicking the Refresh button in your browser takes you to the Cisco Voice Provisioning Tool home page. To refresh the contents in the current window, click the current node in the navigation pane.

When you want to move backward or forward in the Cisco Voice Provisioning Tool, particularly in a wizard, do not click the browser Forward or Back buttons. In fact, we recommend that you do not use these buttons when you perform any tasks in the Cisco Voice Provisioning Tool.

Clicking the Stop button on your browser does not stop the task that is occurring on the Cisco Voice Provisioning Tool server. The Stop button only controls the browser, not the server. Be aware that task results will not display in the browser if you click the Stop button.

You can navigate to pages via the navigation pane or via the hyperlinks that display in the configuration windows themselves. Likewise, the Cisco Voice Provisioning Tool may provide buttons that allow you to navigate throughout the tool.

If you cannot perform certain tasks because you do not have the appropriate RBAC permissions, you will find that most often, the configuration options that are associated with the tasks—including the buttons, menus, hyperlinks, and so on—do not display in the graphical user interface (GUI). If the option displays for some reason and you do not have the appropriate RBAC permissions, the GUI displays a message that insufficient privileges exist and informs you that the tool does not permit the action. For example, if you have the appropriate RBAC permissions to delete users on one product system and not another system, the delete button displays. However, the Cisco Voice Provisioning Tool will only allow you to delete the users for the systems where you have the appropriate RBAC permissions.

If a single configuration option relies on other configuration options, the single option appears disabled until you configure the related configuration options.

### Documentation

Procedures in this guide that specify doing a step in the Cisco Voice Provisioning Tool should be performed by logging in to the graphical user interface with a supported web browser. Procedures that specify doing a step on the VPT server require access to an account that can log in to the Windows 2000 operating system and access files or applications on the server on which the Cisco Voice Provisioning Tool is installed.

Consider the following documentation conventions as you use this guide.

**Table 2**      **Documentation Conventions**

Convention	Description
<b>boldface</b> screen font	Information that you must enter displays in <b>boldface</b> screen font.
<a href="#">blue text</a>	Information acts as a hyperlink; click the blue text to go to the step, URL, chapter section, and so on.

Notes use the following convention:



#### Note

Means take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following convention:



#### Timesaver

Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following convention:



#### Tip

Means the information contains useful tips.

Cautions use the following convention:



**Caution**

---

Means be careful. In this situation, you might do something that could result in equipment damage or loss of data.

---

Warnings use the following convention:



**Warning**

---

**Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

---

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>



# Cisco Voice Provisioning Tool System Overview

---

To begin setting up and using the Cisco Voice Provisioning Tool, you should understand the various parts of the system and how they fit together, as well as how you can customize each piece to the needs of your deployment. This chapter provides background information, in the following sections:

- [Understanding the Cisco Voice Provisioning Tool Components, page 1-1](#)
- [VPT System Configuration Checklist, page 1-5](#)

## Understanding the Cisco Voice Provisioning Tool Components

The Cisco Voice Provisioning Tool is a web-based application for use in performing frequent move/add/change operations within a Cisco IP Telephony deployment. The VPT installation process automatically sets up plug-ins that allow for the provisioning and management of user profiles and Cisco IP Phones in Cisco CallManager, and subscribers in Cisco Unity. Because the tool provides one single graphical interface to both types of systems and can be configured to provision multiple Cisco CallManager clusters and Cisco Unity server instances at once, it can simplify adding, locating, and managing end users and their associated phones and messaging accounts.

The following sections provide further detail on the main VPT system components:

- [VPT Graphical User Interface \(GUI\), page 1-1](#)
- [Administrators, page 1-2](#)
- [Roles, page 1-2](#)
- [Product Systems, page 1-3](#)
- [Plug-Ins, page 1-4](#)
- [Voice Provisioning, page 1-4](#)
- [VPT Database, page 1-5](#)
- [Audit Logging, page 1-5](#)

## VPT Graphical User Interface (GUI)

You can use the Cisco Voice Provisioning Tool from any supported host/browser that has access to the VPT server.

When an administrator logs in to VPT, the GUI provides dual-pane navigation: a tree control task list pane on the left for finding and choosing tasks, and a task pane on the right for following the steps that are required to accomplish a task. Provisioning tasks (such as adding phones and users) display in the task list under Voice Provisioning. VPT management tasks (such as adding product systems) appear under VPT Administration. With the VPT role-based authorization approach, an administrator typically sees only the options that are available to the roles to which the account belongs.

## Administrators

VPT administrators comprise all individuals who have accounts with permission to access the Cisco Voice Provisioning Tool. Although VPT administrative accounts may be created for the same people who administer Cisco Unity and Cisco CallManager within an organization, no requirement exists for this. VPT maintains its own administrative account information and role-based permissions, which allow the creation of administrative accounts that only permit specific tasks to be performed on specific systems or types of systems. See the [“Adding and Managing Administrators” section on page 3-12](#) for related procedures.

## Roles

VPT uses a Role-Based Access Control (RBAC) approach for authorization. At the lowest level, privileges (for example, the ability to add users) combine with the product system(s) to which they can be applied (for example, a particular Cisco CallManager server) to define a permission. Sets of permissions are grouped into roles, and access to perform a given set of tasks on a given set of resources goes to administrators who have been assigned the associated role. An administrator can be assigned to more than one role.

The plug-ins that are installed in the system define the list of privileges that are available for use in creating roles. (By default, Cisco CallManager version 4.1(3) and Cisco Unity version 4.0(5) plug-ins are installed.) For example, the Cisco CallManager plug-in defines privileges to add, view, modify, and delete phones and to add, view, modify, and delete users.

The product systems that have been configured to use a particular plug-in define the list of resources or servers on which a privilege can be granted. For example, the privilege to view phones can be granted on a particular Cisco CallManager server (which uses the Cisco CallManager plug-in).

Besides granting permissions to an individual product system resource, a predefined All <Product System Type> resource automatically applies any privileges granted for it to all currently configured product systems of a given type (that is, product systems that all use the same plug-in). As new product systems of that type are added, they automatically are included.

In addition to specifying provisioning permissions for product systems, with VPT roles you can grant or deny permissions for configuring and monitoring the VPT application itself (for example, a role could include the ability to add product systems or to configure audit log settings and view audit logs).

## Predefined Roles

When VPT is installed, three predefined roles are created automatically. Each default role includes a name and description that cannot be modified. You cannot delete a default role. See [Table 1-1](#) for information about these predefined roles.



**Table 1-1** Predefined Roles

Role Name	Default Associated Accounts	Description
Super Admin	superadmin	This role includes all provisioning privileges on all product systems and all VPT administration privileges.  Although this role cannot be modified, additional administrator accounts can be assigned to this role.
Full Provisioning	None	This role includes all provisioning privileges on all product systems but does not include VPT administration privileges.  Although the role name and description for this role cannot be modified, the permissions can be modified, and administrator accounts can be assigned to this role.
View-only Provisioning	None	This role has view-only provisioning privileges for all product systems but no VPT administration privileges.  Although the role name and description for this role cannot be modified, the permissions can be modified, and administrator accounts can be added to this role.

If a new product plug-in is added to the Cisco Voice Provisioning Tool, each predefined role automatically is updated to include the appropriate privileges on all product systems that use that plug-in (for example, an administrator that is associated only with the View-only Provisioning role would automatically be able to view, but not modify, any objects on any product systems that use the new plug-in). Similarly, when a plug-in is removed, the corresponding privileges are removed from each predefined role.

## User-Defined Roles

In addition to the predefined roles, administrators with sufficient permissions can add, modify, or delete custom roles. Custom roles are not automatically updated when new product plug-ins are installed, but administrators with appropriate privileges can modify them to include permissions for newly added systems. See the [“Adding and Managing Roles” section on page 3-11](#) for related procedures.

## Product Systems

A product system represents a Cisco IP Telephony product with a distinct set of provisioning data (for example, a Cisco CallManager cluster or a Cisco Unity failover pair). You can use VPT to administer multiple product systems of the same type.

For each Cisco CallManager cluster, you configure a product system in VPT to represent the publisher server (if only one Cisco CallManager server acts as publisher and subscriber, you configure that server as the product system representative). For Cisco Unity servers, you configure a product system for each Cisco Unity system that has a unique set of subscribers. In a failover pair, you can specify information in the product system configuration for both the primary and secondary servers, and VPT will communicate with whichever server is currently active.

While the VPT administrators do not need to have accounts on the Cisco CallManager or Cisco Unity servers that they manage, each product system must have a system account that is configured, so that the VPT server can authenticate and communicate with the product system. You must configure VPT to use the correct credentials for this account when it connects to the product system.

See the [“Adding and Managing Product Systems” section on page 3-1](#) for step-by-step procedures for configuring and adding a product system to VPT.

## Plug-Ins

Plug-ins define the provisioning actions that are available to VPT for a particular type (and version) of product system. They also define the individual permissions that can be granted to manage the associated 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). Plug-ins provide the core extensibility of the VPT system. As new plug-ins are developed, you can dynamically add them to the VPT system to extend the provisioning capabilities to cover additional types of systems and provisioning actions.

## Voice Provisioning

The Cisco Voice Provisioning Tool unifies the most common elements of end-user move/add/change operations by providing a single interface to provision users and phones across Cisco CallManager and Cisco Unity. To further aid in provisioning tasks, the provisioning interface provides unified template and bulk import/export support.

## Templates

The Cisco Voice Provisioning Tool allows administrators to configure and store templates that include default data for creating users on a Cisco CallManager system, a Cisco Unity system, or on both systems simultaneously. The tool also allows you to set up templates for provisioning phones on a Cisco CallManager system. You can enter as much or as little data as you want in a template. In addition, you can enter a subset of the information that is required for a given field; for example, you can enter a partial MAC address for a phone and fill in the rest of the MAC address when you apply the template to create a phone.

In addition to using templates to add a user or phone, you can apply templates to existing users or phones either individually or in bulk. If a value is specified in a given field in the template, it overwrites any existing information in the field for the user or phone (however, in the case of bulk adds or updates, if a different value is specified for the field in the CSV file, the value in the CSV file takes precedence over the template value).

## Bulk Provisioning

The bulk provisioning functionality allows administrators to schedule and run bulk add, bulk update, and bulk export tasks on large sets of users or phones at one time. You can access information about scheduled, queued, running, and completed jobs and the associated input or output file and log file from the Manage Bulk Tasks window. You can modify or cancel tasks that are scheduled or queued, cancel in-progress tasks, and rerun tasks that have completed or remove them from the list of saved tasks.

## VPT Database

The VPT database contains data that the VPT application uses to facilitate provisioning of product systems—details about the product systems and how to communicate with them; information about administrator accounts, roles, and permissions; security settings; and the templates that are used in provisioning users and phones. The VPT database does not store data that is related to individual users and phones. This data resides in the databases of the individual product systems to which the users and phones have been added.

You can back up and restore the VPT database by using OSQL commands. See the “[Database Management](#)” chapter for details.

## Audit Logging

The VPT audit logs provide a record of activity on the system, including information about who performed an action and when the action occurred. Audit log entries are generated for login and logout attempts, provisioning operations, configuration changes, and the startup and shutdown of the VPT application. See the “[Audit Logging](#)” chapter for details on configuring and accessing the audit logs.

# VPT System Configuration Checklist

[Table 1-2](#) describes the tasks that you perform after the Cisco Voice Provisioning Tool is installed to set up the system to perform provisioning actions.

**Table 1-2** VPT System Configuration Checklist

Configuration Steps		Related procedures and topics
<b>Step 1</b>	Review the descriptive information on the components of the Cisco Voice Provisioning Tool. This information provides you with an understanding of how the various configuration elements relate to one another.	<ul style="list-style-type: none"> <li>• <a href="#">Understanding the Cisco Voice Provisioning Tool Components, page 1-1</a></li> </ul>
<b>Step 2</b>	Log in to the VPT GUI, and familiarize yourself with the interface and how you can customize it.	<ul style="list-style-type: none"> <li>• <a href="#">Chapter 2, “Accessing the Cisco Voice Provisioning Tool”</a></li> </ul>
<b>Step 3</b>	Add Cisco CallManager and/or Cisco Unity servers as new product systems.	<ul style="list-style-type: none"> <li>• <a href="#">Adding a Cisco CallManager Server, page 3-1</a></li> <li>• <a href="#">Adding a Cisco Unity Server, page 3-3</a></li> </ul>
<b>Step 4</b>	Decide whether you will use the default roles or add new roles to provide the specific permissions that are desired for your environment.	<ul style="list-style-type: none"> <li>• <a href="#">Adding and Managing Roles, page 3-11</a></li> </ul>
<b>Step 5</b>	Add additional administrator accounts.	<ul style="list-style-type: none"> <li>• <a href="#">Adding and Managing Administrators, page 3-12</a></li> </ul>

Table 1-2 VPT System Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
<b>Step 6</b>	Review VPT security recommendations and take action on any that apply to your environment.	<ul style="list-style-type: none"> <li>Chapter 4, “Configuring System Security”</li> </ul>
<b>Step 7</b>	Review the descriptive information on the VPT database and review how to back it up and restore it.	<ul style="list-style-type: none"> <li>Chapter 5, “Database Management”</li> </ul>
<b>Step 8</b>	Review the audit logging settings and familiarize yourself with the contents of the logs. Also, understand which information is written to the logs and which information is written to the Windows application event log.	<ul style="list-style-type: none"> <li>Chapter 6, “Audit Logging”</li> <li>Chapter 7, “Monitoring the VPT System”</li> </ul>
<b>Step 9</b>	Tell administrators how to access the tool and point them to information on using the tool for provisioning users and phones.	<i>Cisco Voice Provisioning Tool User and Phone Management Guide</i>



## Accessing the Cisco Voice Provisioning Tool

---

For all product system provisioning activities and most VPT configuration activities, you use a web browser to access the Cisco Voice Provisioning Tool website. You can modify how the website is accessed and the behavior that you or other administrators experience when accessing the site. The following sections provide additional details:

- [Cisco Voice Provisioning Tool Web Address, page 2-1](#)
- [Logging In, Changing Your Password, and Logging Out, page 2-2](#)
- [Considerations for Using the Graphical User Interface, page 2-2](#)
- [Determining the Cisco Voice Provisioning Tool Version, page 2-3](#)
- [Using Online Help, page 2-3](#)
- [Accessing Product System Administrative Interfaces from the Cisco Voice Provisioning Tool, page 2-3](#)
- [Changing the Session Timeout Length, page 2-4](#)
- [Modifying the Number of Search Results That the Cisco Voice Provisioning Tool Returns, page 2-4](#)
- [Disabling Administrator Access to the Cisco Voice Provisioning Tool Website, page 2-5](#)
- [Changing the HTTP Port Number After Installation, page 2-6](#)

### Cisco Voice Provisioning Tool Web Address

The URL that you use to access the tool depends on whether SSL is configured and the HTTP port number that was chosen during installation:

- If SSL is enabled, the URL is `https://<server name or IP address>:<port number>/vpt`, and the default port is 8443.
- If SSL is not enabled, the URL is `http://<server name or IP address>:<port number>/vpt`, and the default port is 8080.



**Note**

The Cisco Voice Provisioning Tool website uses popup windows. If you have popup blocker software installed, configure it to enable popups for this site.

---

# Logging In, Changing Your Password, and Logging Out

You can log in to the Cisco Voice Provisioning Tool website either by using the desktop shortcut that was added during installation on the Cisco Voice Provisioning Tool server or by browsing to the site by using a supported web browser on any computer with a network connection to the VPT server.

When you access the main URL for the website, a prompt tells you to log in with an Admin ID and password.

After you have successfully logged in to the system, if you are logging in for the first time or your password has been changed by another administrator since your last login, you automatically are prompted to change your password.

In addition, you can change your password at any time after logging in by clicking **Change Password** at the upper right side of the browser window.

You can log yourself out of the VPT interface by clicking **Log Out**, which also appears at the upper right corner of the window. If you do not request any pages or perform any actions for a period exceeding the session timeout (this period defaults to 15 minutes but is configurable), you automatically are logged out of the system and are prompted to log in again as soon as you request a page or attempt to perform an action.

## Considerations for Using the Graphical User Interface

Consider the following information as you perform tasks in the Cisco Voice Provisioning Tool. Use the information in conjunction with the descriptions and procedures that this guide discusses.

- The Cisco Voice Provisioning Tool uses popup windows. Ensure that your browser is configured to accept popup windows.
- The Refresh button that displays in your browser does not refresh the contents in the current configuration window in the Cisco Voice Provisioning Tool. Instead, clicking the Refresh button in your browser takes you to the Cisco Voice Provisioning Tool home page. To refresh the contents in the current window, click the current node in the navigation pane.
- When you want to move to backward or forward in the Cisco Voice Provisioning Tool, particularly in a wizard, do not click the browser Forward or Back buttons. In fact, we recommend that you do not use these buttons when you perform any tasks in the Cisco Voice Provisioning Tool.
- Clicking the Stop button on your browser does not stop the task that is occurring on the Cisco Voice Provisioning Tool server. The Stop button only controls the browser, not the server. Be aware that task results will not display in the browser if you click the Stop button.
- You can navigate to windows via the navigation pane or via the hyperlinks that display in the configuration windows themselves. Likewise, the Cisco Voice Provisioning Tool may provide buttons that allow you to navigate throughout the tool.
- If you cannot perform certain tasks because you do not have the appropriate RBAC permissions, you will find that most often, the configuration options that are associated with the tasks—including the buttons, menus, hyperlinks, and so on—do not display in the graphical user interface (GUI). If the option displays for some reason and you do not have the appropriate RBAC permissions, the GUI displays a message that insufficient privileges exist and informs you that the tool does not permit the action. For example, if you have the appropriate RBAC permissions to delete users on one product system and not another system, the delete button displays. However, the Cisco Voice Provisioning Tool will only allow you to delete the users for the systems where you have the appropriate RBAC permissions.

- If a single configuration option relies on other configuration options, the single option appears disabled until you configure the related configuration options.

## Determining the Cisco Voice Provisioning Tool Version

To determine the version of VPT software in use, log in to the tool and click **About**.

## Using Online Help

When you navigate to any provisioning or administration window in the Cisco Voice Provisioning Tool, a Help menu displays at the top of the window. The Help menu provides links to online versions of the *Cisco Voice Provisioning Tool User and Phone Management Guide* and the *Cisco Voice Provisioning Tool System Management and Security Guide*. These online guides comprise an indexed, searchable help system that was installed with the VPT software.

**Note**

---

For the most up-to-date version of the information in these guides, refer to the Cisco website. You can access the most current Cisco documentation at this URL:  
<http://www.cisco.com/univercd/home/home.htm>

---

## Accessing Product System Administrative Interfaces from the Cisco Voice Provisioning Tool

When configuring product systems in the Cisco Voice Provisioning Tool, you can optionally specify the URL of the individual product system administrative GUI. This allows any administrator with sufficient permissions to click on a link from within the tool to easily browse to the product system GUI to carry out any additional configuration activities that can only be performed on the native product system administrative interface.

To access the product system administrative interface from the link, the VPT administrator also needs an account with sufficient privileges on the product system itself. In most cases, the administrator will be prompted to enter a user name and password to log in to the product system GUI, unless the GUI is configured for Integrated Windows Authentication, and the user identity can be verified based on the Windows login credentials of the administrator.

Also note that following the link from within the Cisco Voice Provisioning Tool will cause the product system GUI to open in another window in the same browser you are using to access the tool; however, the individual product system administrative interfaces may not support all of the web browsers that are supported by VPT.

If the criteria mentioned above are met, and the URL has been configured, you can access the product system administrative interface from VPT by using the following procedure:

**Note**

---

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

---

**To Access Product System Administrative Interfaces from the Cisco Voice Provisioning Tool**

- 
- 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 button in the Product SA URL column of the product system GUI that you want to launch.
- 

## Changing the Session Timeout Length

As a security feature, the Cisco Voice Provisioning Tool automatically logs any administrator out after 15 minutes of inactivity. After the session timeout is reached, if you attempt to navigate to another window or choose an action on a window (such as Save or Cancel), the tool will indicate that your session has expired, and prompt you to log in again.

The session timeout represents a global value that applies to all administrator accounts. You can change the number of minutes before an idle session times out by using the following procedure.

**Note**

To configure security 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 Change the Session Timeout Length**

- 
- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**.
- The Configuration window displays.
- Step 2** In the Security section, enter a new value between 5 and 1440 for the Session Timeout.
- Step 3** Click **Save**.
- 

## Modifying the Number of Search Results That the Cisco Voice Provisioning Tool Returns

When it is performing searches on large quantities of provisioning data, the Cisco Voice Provisioning Tool automatically limits the number of search results that are returned to ensure that the amount of memory used by the search results does not overburden the system.

By default, up to 500 records are returned per product system for any individual search query; if the result set for a product system is larger than 500, the tool returns an error message.

You can change the search result limit by using the following procedure.



**Note**

To configure search results 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 Change the Number of Search Results That the Cisco Voice Provisioning Tool Returns**

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**.  
The Configuration window displays.
- Step 2** In the Search Results section, enter a new value between 0 and 5000 for the Result Limit.
- Step 3** Click **Save**.

## Disabling Administrator Access to the Cisco Voice Provisioning Tool Website

If your administrator account has sufficient privileges, you can lock out other administrator accounts without removing the accounts from the system. You can re-enable the disabled accounts at a later time.

If the administrator is active at the time his or her account is disabled, any operations that have been submitted and are in progress will complete, but as soon as the administrator attempts to perform an additional action or navigate to a new window, he or she will receive a message that indicates that the session is no longer valid, and the administrator will be logged out.

You can disable one or more administrator accounts at once by using the following procedure:

**Note**

Only the superadmin and other administrators who belong to the predefined Super Admin role can disable administrator accounts. You cannot disable the predefined superadmin account, or the account that you use to perform this procedure.

**To Disable Administrator Access to the Cisco Voice Provisioning Tool Website**

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Administrators > Manage Administrators**.  
The Manage Administrators window displays a list of configured administrators.
- Step 2** Choose **Disable** in the Status column of each administrator that you want to disable.

**Caution**

The change takes effect immediately. If the administrator that you are disabling is logged in and has entered data on a window but has not yet submitted it, the data may be lost.

# Changing the HTTP Port Number After Installation

The Tomcat HTTP port number that is used to access the Cisco Voice Provisioning Tool is specified during installation. If you later need to change the port number to correct an error or to accommodate another service, perform the following procedure.

## To Change the HTTP Port Number After Installation

---

- Step 1** Ensure that the **VPT Tomcat** service is stopped.
- On the VPT server, on the Windows Start menu, choose **Programs > Administrative Tools > Services**.
  - In the right pane, locate **VPT Tomcat**, right-click it, and click **Stop**.
- Step 2** Browse to the <VPT Installation Root>\tomcat\conf directory.
- Step 3** Use a text editor to open **server.xml**.
- Step 4** In the text that displays, locate the **Coyote HTTP Connector Port**.
- Step 5** Delete the port number for the Coyote HTTP connector port and enter a port that is not in use.
- Step 6** Save the file.
- Step 7** Start the **VPT Tomcat** service.
- On the Windows Start menu, choose **Programs > Administrative Tools > Services**.
  - In the right pane, locate **VPT Tomcat**, right-click it, and click **Start**.
-



# 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 CCMAAdmin 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>/CCMAAdmin/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.

---





## Configuring System Security

---

You can use the Cisco Voice Provisioning Tool to provide administrators a central point of access to sensitive provisioning information (such as user passwords and other information) on multiple product systems in different locations. For this reason, you should ensure that both the connection between the administrator and the tool and the connections between the tool and the product systems are secure. If any of these connections takes place across the boundaries of a secure network, you must take additional steps to ensure that these connections are secured. This chapter explains those steps, as well as additional steps that you should take to ensure that the passwords that are used to restrict access to the tool are secure at all times.

This chapter covers the following topics:

- [Configuring Browser Security, page 4-1](#)
- [Configuring Secure Communication with Product Systems, page 4-4](#)
- [Password Security, page 4-12](#)

### Configuring Browser Security

You can use the Secure Sockets Layer (SSL) to provide an authenticated, encrypted connection between the web clients that administrators use and the Cisco Voice Provisioning Tool. Without SSL in place, passwords and other potentially sensitive provisioning information may be passed in plain text across the network.

When first installing the tool, you can choose whether to enable SSL on this connection. If you need to change the configuration after installation, use one of the following sections:

- [Configuring SSL for the Cisco Voice Provisioning Tool Web Application After Installation, page 4-2](#)
- [Removing SSL from the Cisco Voice Provisioning Tool Web Application After Installation, page 4-4](#)

## Configuring SSL for the Cisco Voice Provisioning Tool Web Application After Installation

To configure the Tomcat web server so that it communicates with the client web browser over a secure connection, perform the following procedure.

### To Configure SSL for the Cisco Voice Provisioning Tool Web Application

- 
- Step 1** On the VPT server, verify that the PATH environment variable on the system includes the path to the bin directory of the JDK that is installed with VPT:
- On the Windows Start menu, choose **Settings > Control Panel > System**.
  - Click the **Advanced** tab.
  - Click **Environment Variables**.
  - In the System Variables list, find and click the **Path** variable and click **Edit**.
  - 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**
  - Click **OK**.
  - 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](#):
- On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.
  - In the command prompt window, enter **javac**. If the path is set correctly, usage information for the javac command displays.
- Step 3** Add a root certificate to the keystore for the VPT server by doing the applicable steps:
- Create and add a self-signed certificate. Continue with [Step 4](#).
  - Install a certificate from a Certificate Authority. Skip to [Step 5](#).
- Step 4** If you are creating a self-signed certificate, do the following substeps:
- Enter  
**keytool -genkey -alias tomcat -keyalg RSA -keystore <keystore file name>**  
and press **Enter**.



---

**Note** The keystore file name should include the full path to the keystore file and must not contain any spaces.

---

- Follow the prompts to enter a keystore password, your name, organizational and location information, and a key password.



---

**Note** The keystore password and key password must match.

---

- Close the command prompt window. Skip to [Step 6](#).

**Step 5** If you have obtained a certificate from a Certificate Authority, do the following substeps:

- a. Enter **keytool -import -alias tomcat -keyalg RSA -keystore <keystore file name> -trustcacerts -file <certificate file name>** and press **Enter**.



**Note** The keystore file name must not contain any spaces. The certificate file name must be an absolute path to your certificate file and should not contain any spaces.

- b. Follow the prompt to enter the keystore password.



**Note** The keystore password must match the certificate password.

- c. If the password that you entered is correct, you will be presented with the information on the certificate that you are importing and asked whether you trust the certificate. Enter **y** and press **Enter** to trust the certificate. If the password that you entered is not correct, repeat Steps **a.** and **b.**
- d. Close the command prompt window.

**Step 6** Browse to the <VPT installation root>\tomcat\conf directory.

**Step 7** Use a text editor to open the **server.xml** file.

**Step 8** Find **non-SSL Coyote HTTP/1.1 Connector**. Replace all the text that begins with **<Connector** and ends with **/>** with the following:

```
<Connector port="8443" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true" URIEncoding="UTF-8"
useBodyEncodingForURI="true" acceptCount="100" debug="0" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="<keystore file name>"
keystorePass="<keystore password>" />
```



**Note** Port 8443 is the recommended port. If this port is already in use by another process, choose a different port.



**Note** The keystore file name and keystore password must match the values that you chose in [Step 4](#) or [Step 5](#).

**Step 9** Save and close the **server.xml** file.


**Step 10** For the changes to take effect, you must restart the VPT 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**.

**Step 11** To verify the changes, open a web browser and browse to **https://<server name or IP address>:<port number>/vpt**.

## Removing SSL from the Cisco Voice Provisioning Tool Web Application After Installation

To configure the Tomcat web server so that it communicates with the client web browser over a non-secure connection, perform the following procedure.

### To Remove SSL from the Cisco Voice Provisioning Tool Web Application

- 
- Step 1** On the VPT server, browse to the <VPT installation root>\tomcat\conf directory.
- Step 2** Use a text editor to open the **server.xml** file.
- Step 3** Find **SSL Coyote HTTP/1.1 Connector**. Replace all the text that begins with **<Connector** and ends with **/>** with the following:
- ```
<Connector port="8080" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100" debug="0"
connectionTimeout="20000" URIEncoding="UTF-8" useBodyEncodingForURI="true"
disableUploadTimeout="true" />
```
-  **Note** Port 8080 is the recommended port. If this port is already in use by another process, choose a different port.
- 
- Step 4** Save and close the **server.xml** file.
- Step 5** For the changes to take effect, you must restart the VPT 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**.
- Step 6** To verify the changes, open a web browser and browse to **http://<server name or IP address>:<port number>/vpt**.
- 

## Configuring Secure Communication with Product Systems

To implement security between the Cisco Voice Provisioning Tool and individual product systems, use one of the following mechanisms:

- Secure Sockets Layer (SSL) is recommended for use with Cisco Unity product systems. See the “[SSL](#)” section on page 4-4.
- IP Security (IPSec) provides a security alternative for use with Cisco CallManager systems that are separated from the VPT server by non-secure networks. See the “[IPSec](#)” section on page 4-12.

### SSL

You can implement security between the Cisco Voice Provisioning Tool and individual Cisco Unity product systems by using the Secure Sockets Layer (SSL) protocol. SSL provides secure transmission of data across the network through the use of public/private key encryption.

## Configuring a Product System for SSL

To configure SSL on the link between VPT and a product system, you must first configure SSL on the individual product system.

**Note**

As of the first release of the Cisco Voice Provisioning Tool, only the Cisco Unity 4.0(5) plug-in supports SSL. For information on configuring SSL on Cisco Unity, see the *Cisco Unity Security Guide*.

If failover is in use, and 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.

After SSL has been configured on the product system, and a certificate has been procured or generated for the product system, do the following tasks to set up secure communication with the product 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 the [“Exporting Certificates for Each Product System” section on page 4-5](#).
2. Copy certificates for each Cisco Unity product system to the VPT server. See the [“Copying Certificates for Each Product System” section on page 4-7](#).
3. Add the product system certificate(s) to a keystore on the VPT server. See the [“Entering Product System Certificates in the VPT Keystore” section on page 4-7](#).
4. Configure the keystore properties in the Cisco Voice Provisioning Tool. See the [“Configuring Keystore Information in the Cisco Voice Provisioning Tool” section on page 4-9](#).
5. Configure the product system settings to use SSL in the Cisco Voice Provisioning Tool. See the [“Configuring the Product Systems to use SSL in the Cisco Voice Provisioning Tool” section on page 4-9](#).
6. Test the product system. See the [“Testing the Product System” section on page 4-10](#).

### Exporting Certificates for Each Product System

Whether certificates were generated by using a Certificate Authority (CA) or were generated as self-signed certificates, you need to obtain a copy of the certificate to add to the VPT keystore. If self-signed certificates are used, you will need to export a copy of each server certificate (if failover is in use, you will need a copy from both the primary and secondary Cisco Unity servers). If your enterprise has a Certificate Authority, you generally will only need to obtain and add the CA root certificate to the keystore once.

Do one of the following procedures, depending on the mechanism that is used to generate the certificate(s):

- [To Export a Certificate Generated by a Certificate Authority \(CA\), page 4-5](#)
- [To Export Self-Signed Certificates, page 4-6](#)

#### 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** Double-click the name of the Cisco Unity server to expand it.
  - 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.
-

## Copying Certificates for Each Product System

Use the following procedure to copy certificates from each product system to the VPT server.

### To Copy Certificates for Each Product System

---

- 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. Choose 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**.
- 

## Entering Product System Certificates in the VPT Keystore

To configure VPT to communicate with product systems by using SSL, you must use the keytool application that 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 automatically is created 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 Key Store by Using Keytool

---

- Step 1** On the VPT server, verify 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 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 <Server Name> -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 product system certificate.




---

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

---

**Step 8** Close the command prompt window.

---



## Configuring Keystore Information in the Cisco Voice Provisioning Tool



**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 Key Store by Using Keytool](#)” procedure on page 4-7.
- Step 3** Click **Save**.
- Step 4** For the changes to take effect, you must restart the VPT 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**.

## Configuring the Product Systems to use SSL in the Cisco Voice Provisioning Tool

If you have not yet added the product system to the Cisco Voice Provisioning Tool, see the “[Adding a Cisco Unity Server](#)” section on page 3-3.

If the product system is already configured in the Cisco Voice Provisioning Tool, you can change the security settings from the Manage Product Systems window, as follows:



**Note** To configure product system settings, your administrator account must belong to a role that has Product Systems Management Modify and View 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 Configure a Product System to use SSL

- 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.



**Note** As of the first release of the Cisco Voice Provisioning Tool, only product systems of type UNITY-4.0.5 support SSL.

- Step 3** If the URL for the Cisco Unity Administrator changed because of the change in security settings, enter the new URL as the Product SA URL.

- Step 4** Change the Unity CUAL port. Typically, the port number for SSL is 443. If failover is configured, you must also change the failover CUAL port (for the secondary Cisco Unity server).
- Step 5** In the Security drop-down menu, choose **SSL**.
- Step 6** Click **Save**.
- 

## Testing the Product System

After you have configured the product system and the Cisco Voice Provisioning Tool to enable SSL on a product system connection, you should test the connection to verify that the setup is working correctly.



### 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.
- 

## Removing SSL from Product Systems

If SSL has been configured on a Cisco Unity product system and you want to remove it, do the following tasks:

1. Remove SSL from the product system server. Refer to the *Cisco Unity Security Guide* for instructions. If failover is in use, you must also remove SSL from the secondary Cisco Unity server.
2. Change the product system settings for the Cisco Unity server to reflect the removal of SSL. See the [“Removing SSL from the Product System Configuration in the Cisco Voice Provisioning Tool”](#) section on page 4-10.
3. Test the product system. See the [“Testing the Product System”](#) section on page 4-11.

## Removing SSL from the Product System Configuration in the Cisco Voice Provisioning Tool

If you have not yet added the product system to the Cisco Voice Provisioning Tool, see the [“Adding a Cisco Unity Server”](#) section on page 3-3.

If the product system is already configured in the Cisco Voice Provisioning Tool, you can change the security settings from the Manage Product Systems window, as follows.

**Note**

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

---

**To Remove SSL from 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** If the URL for the Cisco Unity Administrator changed because of the change in security settings, enter the new URL as the Product SA URL.
- Step 4** Change the Unity CUAL port. Typically, the port number when SSL is not enabled is 80. If failover is configured, you must also change the failover CUAL port (for the secondary Cisco Unity server).
- Step 5** In the Security drop-down menu, choose **No Security**.
- Step 6** Click **Save**.
- 

**Testing the Product System**

After you have configured the product system and the Cisco Voice Provisioning Tool to remove SSL from the product system connection, you should test the connection to verify that the setup is working correctly.

**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.
-

## IPSec

If the traffic between the Cisco Voice Provisioning Tool server and one or more Cisco CallManager product systems will traverse a non-secure network, you can implement IPSec to protect sensitive provisioning configuration data (such as user names, passwords, and PINs).

IPSec is a secure connection protocol that provides authentication and/or encryption at the IP layer between two hosts, or between a host and a security gateway (such as a firewall or router). For securing the connection between VPT and a Cisco CallManager server, we recommend that you implement IPSec between the VPT host and the network infrastructure for the Cisco CallManager server, rather than between the VPT host and the Cisco CallManager server.

You can enable IPSec on the VPT server by using Windows 2000 IPSec tunneling. Refer to the Microsoft Windows 2000 Help for IPSec tunneling configuration details.

For information on configuring the network infrastructure for the Cisco CallManager server, refer to the *Cisco CallManager Security Guide*.

## Password Security

The Cisco Voice Provisioning Tool provides built-in features to help you ensure password security. However, because access to and use of the tool involves other network and system components, external security factors can also affect the security of the passwords that are used by and for the tool. When implementing a security policy for VPT, you should understand the mechanisms that VPT provides, as well as the actions you can take to ensure password security.

### Password Security Features Provided by the Cisco Voice Provisioning Tool

The Cisco Voice Provisioning Tool provides the following password security features:

- The tool automatically validates all administrator passwords for security. All passwords require a minimum password length of 8 characters (and maximum of 80 characters). In addition, passwords must contain characters taken from at least three of the following character classes:
  - Symbols—for example, !"#%&'()\*+,-./
  - Numbers—0 to 9
  - Upper-case letters—A to Z
  - Lower-case letters—a to z
- The tool also checks all passwords for the following restrictions:
  - No character in the password can repeat more than three times consecutively.
  - The password cannot match the user name (Admin ID), either spelled forwards or backwards.
- The tool always prompts new administrators to change their passwords when they first log in to the system.
- Any time that an administrator password has been reset by another user, at the next login, the administrator will be prompted to change the new password.

- Administrators with sufficient permissions can disable other administrator accounts, which allows the administrator data to remain in the system while locking out the administrator. The change takes effect immediately (any operations already in progress by the administrator will complete, but at the next attempt to browse to another page or submit another action, the disabled administrator will be logged out of the system).

## Actions You Should Take to Ensure Password Security

After installing the Cisco Voice Provisioning Tool, you should take the following actions:

- Immediately log in as superadmin and change the superadmin password (the initial password that you set during the installation process is a temporary password; the first time you log in as superadmin you will be required to change it).
- Configure SSL on the VPT website and SSL or IPSec on the product system interfaces. When administrators log in to the Cisco Voice Provisioning Tool, their credentials are sent across the network to the tool in clear text, unless SSL is configured for the VPT website. In addition, the information that administrators enter on the windows of the tool is not encrypted unless secure communications mechanisms are in use on both the VPT website and the product system connections.
- Assign unique passwords to new administrator accounts as you create them (rather than repeatedly reusing the same default password).
- Encourage administrators to log in and change their passwords as quickly as possible after creating their accounts.
- Make sure that administrators use strong passwords in templates for end-user provisioning, and that end-user access points use secure methods to transmit passwords across the network. Refer to the *Cisco CallManager Security Guide* and the *Cisco Unity Security Guide* for further details.





## Database Management

---

In this chapter, you will find a description of the role of the VPT database, and procedures for manually backing up and restoring the database.

See the following sections:

- [VPT Database Design, page 5-1](#)
- [Backing Up the VPT Database, page 5-1](#)
- [Restoring the VPT Database, page 5-2](#)

### VPT Database Design

The VPT database contains data that the VPT application uses to facilitate provisioning of product systems—details about the product systems and how to communicate with them; information about administrator accounts, roles, and permissions; security settings; and the templates that are used in provisioning users and phones. The VPT database does not store data that is related to individual users and phones—this data resides in the databases of the individual product systems to which the users and phones have been added.

To maintain the data that the tool requires in the event of a loss of system functionality that requires reinstalling the application, you should back up the database on a regular basis. If such an outage occurs, you can reinstall VPT and then restore the database to regain functionality. You can perform both the backup and restore operations by using standard SQL tools.

### Backing Up the VPT Database

Run the following procedure on the VPT server to back up the VPT database to a file.

#### To Back Up the VPT Database

- Step 1** On the VPT server, on the Windows Start menu, choose **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter `osql -S localhost -E -Q "backup database usadb to disk='<File Name>' with init"` and press **Enter**.



**Note** The file name must end with the extension `.dat`.

**Step 3** When the backup is complete, close the Command Prompt window.



**Tip**

You can use the Windows AT command in conjunction with the osql command in [Step 2](#) to schedule a periodic backup of the database. For help with the AT command, enter AT /? in a Command Prompt window.

## Restoring the VPT Database

You can restore the VPT database from a file if you have removed the VPT database during an uninstall operation or if you otherwise need to recapture the data. Use one of the following procedures, as applicable to your situation:

- If the location where MSDE/SQL Server is installed has not changed since the backup was made, see the [“To Restore the Database to the Same MSDE Location” procedure on page 5-2](#).
- If the location where MSDE/SQL Server is installed has changed since the backup was made (for example, if you have uninstalled and reinstalled VPT, specifying a different install directory each time), see the [“To Restore the Database to a Different MSDE Location” procedure on page 5-2](#).

### To Restore the Database to the Same MSDE Location

- 
- Step 1** Ensure that the **VPT Tomcat** service is stopped.
- a. On the VPT server, on the Windows Start menu, choose **Programs > Administrative Tools > Services**.
  - b. In the right pane, locate **VPT Tomcat**, right-click it, and click **Stop**.
- Step 2** On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.
- Step 3** In the Command Prompt window, enter `osql -S localhost -E -Q “restore database usadb from disk = ‘<File Name>”` and press **Enter**.
- Step 4** Close the Command Prompt window.
- Step 5** Start the **VPT Tomcat** service.
- a. On the Windows Start menu, choose **Programs > Administrative Tools > Services**.
  - b. In the right pane, locate **VPT Tomcat**, right-click it, and click **Start**.
- 

### To Restore the Database to a Different MSDE Location

- 
- Step 1** Ensure that the **VPT Tomcat** service is stopped.
- a. On the VPT server, on the Windows Start menu, choose **Programs > Administrative Tools > Services**.
  - b. In the right pane, locate **VPT Tomcat**, right-click it, and click **Stop**.
- Step 2** On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.



- Step 3** In the Command Prompt window, enter  
**osql -S localhost -E -Q “restore database usadb from disk = ‘<File Name>’ with move 'usadb' to '<New Path>\MSSQL\Data\usadb.mdf', move 'usadb\_log' to '<New Path>\MSSQL\Data\usadb\_log.LDF”**  
and press **Enter**.



---

**Note** Make sure that the new path that you enter in this command contains the MSSQL\Data directory.

---

- Step 4** Close the Command Prompt window.
- Step 5** Start the **VPT Tomcat** service.
- a. On the Windows Start menu, choose **Programs > Administrative Tools > Services**.
  - b. In the right pane, locate **VPT Tomcat**, right-click it, and click **Start**.
-





# Audit Logging

The VPT audit logs provide a record of activity on the system, including information about who performed an action and when he or she performed it. Audit log entries are generated for login and logout attempts, provisioning operations, configuration changes, and the startup and shutdown of the VPT application.

This chapter contains the following information:

- [Audit Log Information, page 6-1](#)
- [Audit Log File Storage, page 6-3](#)
- [Configuring Audit Log Settings, page 6-3](#)
- [Accessing Audit Logs, page 6-4](#)

## Audit Log Information

Each audit log file starts with a header row that contains a comma-separated list of field names, followed by a row for each audit entry. [Table 6-1](#) lists the fields that display in the log and a description of the content that is logged for each field.

**Table 6-1**      *Audit Log Field Descriptions*

| Field             | Description                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Task ID           | An alphanumeric identifier, which can be used to correlate multiple operations when a particular task (such as adding a new user) involves multiple back-end operations (such as adding the user profile on a Cisco CallManager server and adding the subscriber account on a Cisco Unity server). |
| Task Name         | The name of the high-level task to which the operation belongs (for example, Add User).                                                                                                                                                                                                            |
| Event ID          | An alphanumeric identifier, which can be used to correlate multiple audit log events, if a particular back-end operation generates multiple events before completing.                                                                                                                              |
| Date/Time         | The timestamp at which the audit record was generated.                                                                                                                                                                                                                                             |
| Event             | The name of the back-end operation or the type of the event being logged.                                                                                                                                                                                                                          |
| Product System(s) | The name(s) of the product system(s) on which the task was executed.                                                                                                                                                                                                                               |

**Table 6-1** Audit Log Field Descriptions (continued)

| Field    | Description                                                                                                                                                                                                                                                                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Outcome  | The outcome of the operation or event. The possible values follow: <ul style="list-style-type: none"> <li>Initiated—A back-end operation began execution.</li> <li>Completed—A back-end operation finished execution.</li> <li>Success—The event or operation completed successfully.</li> <li>Failure—The event or operation did not complete successfully.</li> </ul> |
| Severity | Indicates whether the event or outcome that occurred is normal (an expected event or outcome) or severe (an error condition). Severe events also are logged in the Windows application event log.                                                                                                                                                                       |
| Admin    | The admin ID of the administrator who requested or performed the operation.                                                                                                                                                                                                                                                                                             |
| Data     | A detailed listing of the data involved in an operation or event. This field usually contains a list of attribute-value pairs that are involved in the operation. Sensitive information such as passwords and PINs are not recorded. If no relevant data is involved, this field stays empty.                                                                           |
| Remarks  | Any additional information relevant to understanding the outcome of the operation—for example, when an “Add User” operation fails, this field may include further information, such as “Product System not responding.”                                                                                                                                                 |

In the following example, the superadmin adds a user with the alias kbader as a subscriber on the Cisco Unity server c-unity1 and as a user on the Cisco CallManager server c-callmanager1. In this example, you can see that the task ID, E97BEB7A-D04E-E5AB-3656-D931B92DF18A, remains the same throughout the Add User Task operation; however, the entire operation requires a series of individual steps on each product system, which can be linked together based on the event ID.

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,BB9655AB-107F-A888-9274-4E7A2BC06933,Thu Jun 09 12:51:03 EDT 2005,Get System
Dependent User Task Data,c-unity1,Initiated,Normal,superadmin,, ,
```

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,BB9655AB-107F-A888-9274-4E7A2BC06933,Thu Jun 09 12:51:04 EDT 2005,Get System
Dependent User Task Data,c-unity1,Success,Normal,superadmin,
[Message System = c-unity1], ,
```

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,BB9655AB-107F-A888-9274-4E7A2BC06933,Thu Jun 09 12:51:04 EDT 2005,Get System
Dependent User Task Data,c-unity1,Completed Successfully,Normal,superadmin,, ,
```

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:30 EDT 2005,Add
User,c-callmanager1;c-unity1,Initiated,Normal,superadmin,, ,
```

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:30 EDT 2005,Add
User,c-callmanager1,Success,Normal,superadmin,[First Name = Kelly]
[Locale = English UnitedStates] [Default Profile = ] [Telephone No. = ]
[User ID = kbader] [Last Name = Bader] [Primary Extension = ]
[Call Park Retrieval = false] [Calling Party Number Modification = false]
[Authentication Proxy = false] [Manager's User Id = ] [CTI Application Use = false]
[Dept. = Marketing] , ,
```

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
```

```
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:39 EDT 2005,Add
User,c-unity1,Success,Normal,superadmin,[Message Extension = 3003]
[First Name = Kelly] [Exchange Server = c-exch1] [Fax Id = ]
[Display name = Kelly Bader] [User ID = kbader] [Message System = c-unity1]
[Subscriber Type = unity_user_subscriberTypes_exchange] [Last Name = Bader] ,,
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:40 EDT 2005,Add
User,c-callmanager1;c-unity1,Completed Successfully,Normal,superadmin,,,
```

## Audit Log File Storage

The Cisco Voice Provisioning Tool automatically controls the size and number of audit log files that are stored for the tool based on configurable audit log settings. If your account has sufficient permissions, you can configure the location of the logs; you can also control the total amount of disk space that can be taken up by the logs and the number of backup log files that should be kept. The log files automatically roll over based on these two parameters.

For example, if you set the total disk space allowed for the logs to 5 MB, and you set the number of backup files to 4, then an individual audit log file will be written until it reaches 1 MB (5 MB divided by 5 possible files) in size; at that point, a new log file will be created, and the old file will be renamed AuditLog.csv.1. Each time the audit log reaches 1 MB, a new file will be opened, and the file names of the old logs will be renumbered from newest (.1) to oldest (.4). When four backup files are saved, and the total disk space taken up by the current file and the four backup files reaches 5MB, the oldest file is deleted, and once again, a new file will be opened, and the older backup files will be renumbered.

## Configuring Audit Log Settings

You can configure the parameters that control where and how audit logs are stored via the VPT administrative interface.



### Note

To configure audit log settings, your administrator account must belong to a role that has Audit Log 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 Audit Log Settings

- Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**.  
The Configuration window displays.
- Step 2** In the Audit section, enter the **Audit Log Location**.  
Specify the full path to the directory where audit logs will be stored. The directory must already exist and should reside on the VPT server (you should not specify a network drive or path to a directory on another server).
- Step 3** Enter the **Total Disk Space for Audit**.  
This total specifies the maximum disk space (in megabytes) that can be in use by all audit log files. When audit log information exceeds this size, the oldest audit log file is removed, and a new file is created.
- Step 4** Enter the **Number of Audit Backup Files**.

This number specifies the maximum number of backup audit files to create. Enter a value from 1 to 99. An audit log will be written until it reaches a size equal to the total disk space for audit logs divided by the total possible number of audit files (the current log file plus the backup files). At this point, a new audit log file is created. When all audit log files are full, the oldest file is removed and a new file is created.

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

---

## Accessing Audit Logs

**Note**

To access audit logs through the VPT Administrator interface, your administrator account must belong to a role that has Audit Log Access permissions for the VPT application. If you do not see the VPT Administration > View Audit Log option in the VPT navigation menu, your account does not have the applicable permissions.

---

**To Access Audit Logs**

---

**Step 1** In the Cisco Voice Provisioning Tool, choose **VPT Administration > View Audit Log**.

The View Audit Log window displays a list of audit log files that are currently stored on the system, the time when each file was last updated, and the size of each file in bytes.

**Step 2** Click the name of the audit log that you want to view.

Depending on your browser settings, you may be prompted to open or save the file, or the browser may launch an external viewer. All audit logs are stored in comma-separated value (CSV) format. Using an external viewer or application, you can view, sort, or filter the audit log after downloading it.

---



## Monitoring the VPT System

---

This chapter discusses different approaches for monitoring the health and activity of the VPT system.

See the following sections:

- [Monitoring the VPT Application via the Windows Event Log, page 7-1](#)
- [Using the Audit Logs to Monitor the VPT Application, page 7-1](#)

### Monitoring the VPT Application via the Windows Event Log

The Cisco Voice Provisioning Tool includes an audit subsystem that tracks all changes that are made to the system, and any errors or warnings that are associated with them. All of this information is logged to the audit log. Each audit entry is marked with a severity level; entries that are marked normal are logged only to the audit log. Entries that are marked severe are logged both to the audit log and to the Windows application event log.

You can view application events by using the Windows Event Viewer (on the Windows Start menu, choose Programs > Administrative Tools > Event Viewer). For more information on Windows events, refer to the Windows Event Viewer Help.

### Using the Audit Logs to Monitor the VPT Application

The VPT audit logs provide a record of activity on the system, including information about who performed an action and when he or she performed it. Audit log entries are generated for login and logout attempts, provisioning operations, configuration changes, and the startup and shutdown of the VPT application. The audit logs also include information about warnings or errors that occur in the course of performing such operations.

Administrators with sufficient privileges can configure and access the audit logs. See the [“Audit Logging”](#) chapter for more information.







---

## A

about the Voice Provisioning Tool [2-3](#)

accessing

audit logs [6-4](#)

product system administrator websites [2-3](#)

the Voice Provisioning Tool website [2-1](#)

accounts

Cisco CallManager provisioning [3-2](#)

Cisco Unity provisioning [3-4](#)

adding

administrators [3-13](#)

product systems

Cisco CallManager [3-1](#)

Cisco Unity [3-3](#)

roles [3-11](#)

Secure Sockets Layer (SSL)

on the VPT web application [4-2](#)

with product systems [4-4](#)

administrators

adding [3-13](#)

deleting [3-14](#)

disabling access [2-5](#)

modifying [3-13](#)

overview [1-2](#)

audit logging

accessing audit logs [6-4](#)

configuring settings [6-3](#)

disk usage for storing log files [6-3](#)

information stored in logs [6-1](#)

overview [1-5](#)

---

## B

backing up the VPT database [5-1](#)

browser security [4-1](#)

---

## C

changing

HTTP port number used to access VPT [2-6](#)

number of search results returned by VPT [2-4](#)

password for another administrator account [3-13](#)

password for your own administrator account [2-2](#)

session timeout length [2-4](#)

Cisco CallManager

adding as a product system [3-1](#)

provisioning account [3-2](#)

using IPSec for securing the connection to [4-12](#)

Cisco Unity

adding as a product system [3-3](#)

provisioning account [3-4](#)

Secure Sockets Layer (SSL)

configuring [4-5](#)

removing [4-10](#)

Configuration window

Audit settings [6-3](#)

Search Results settings [2-4](#)

Security settings

keystore [4-9](#)

session timeout [2-4](#)

configuring

administrators [3-13](#)

audit log settings [6-3](#)

browser security [4-1](#)

product systems [3-1](#)  
 roles [3-11](#)  
 secure communication with product systems [4-4](#)

---

## D

database  
   backing up [5-1](#)  
   overview [1-5](#)  
   restoring [5-2](#)  
 deleting  
   administrators [3-14](#)  
   product systems [3-10](#)  
   roles [3-12](#)  
 disabling administrator access [2-5](#)

---

## F

Full Provisioning role [1-3](#)

---

## G

Graphical User Interface  
   accessing [2-1](#)  
   considerations for using [2-2](#)  
   overview [1-1](#)

---

## H

Help [2-3](#)  
 HTTP port number used to access VPT  
   changing [2-6](#)  
   determining [2-1](#)

---

## I

IP Security (IPSec) [4-12](#)

---

## L

logging in [2-2](#)  
 logging out [2-2](#)

---

## M

Manage Administrators window  
   deleting an administrator [3-14](#)  
   disabling administrator access [2-5](#)  
   modifying an administrator [3-13](#)  
 Manage Product Systems window  
   accessing a product system administrative interface  
     from [2-3](#)  
   modifying or deleting a product system [3-9](#)  
   testing a Cisco CallManager product system [3-3](#)  
   testing a Cisco Unity product system [3-9](#)  
 modifying  
   administrators [3-13](#)  
   product systems [3-9](#)  
   roles [3-11](#)  
 monitoring  
   via audit logs [7-1](#)  
   via Windows application event log [7-1](#)

---

## O

online Help [2-3](#)  
 overview  
   administrators [1-2](#)  
   audit logging [1-5](#)  
   database [1-5](#)  
   Graphical User Interface [1-1](#)  
   product systems [1-3](#)  
   roles [1-2](#)  
   voice provisioning [1-4](#)

---

**P**

passwords

- changing
  - after login [2-2](#)
  - on another administrator account [3-13](#)
- security [4-12](#)

plug-ins [1-4](#)

port number used to access VPT

- changing [2-6](#)
- determining [2-1](#)

Product SA URL [2-3](#)

product systems

- adding
  - Cisco CallManager [3-1](#)
  - Cisco Unity [3-3](#)
- deleting [3-10](#)
- modifying [3-9](#)
- overview [1-3](#)
- security [4-4](#)

---

**R**

removing

- administrators [3-14](#)
- product systems [3-10](#)
- roles [3-12](#)
- Secure Sockets Layer (SSL)
  - from Cisco Unity product systems [4-10](#)
  - from the VPT web application [4-4](#)

restoring the VPT database [5-2](#)

Role-Based Access Control (RBAC) overview [1-2](#)

roles

- adding [3-11](#)
- deleting [3-12](#)
- modifying [3-11](#)
- overview [1-2](#)

---

**S**

search results, changing number of [2-4](#)

Secure Sockets Layer (SSL)

- configuring for Cisco Unity product systems [4-4](#)
- configuring for the VPT web application [4-2](#)
- removing from Cisco Unity product systems [4-10](#)
- removing from the VPT web application [4-4](#)

security

- browser [4-2](#)
- IPSec [4-12](#)
- password [4-12](#)
- product system [4-4](#)

session timeout length [2-4](#)

Super Admin role [1-3](#)

---

**T**

testing

- Cisco CallManager product system, after adding [3-3](#)
- Cisco Unity product system
  - after adding [3-9](#)
  - after enabling SSL [4-10](#)

---

**U**

URL

- Product SA [2-3](#)
- VPT [2-1](#)

using online Help [2-3](#)

---

**V**

View Audit Log window [6-4](#)

View-only Provisioning role [1-3](#)

Voice Provisioning Tool

- determining the version of [2-3](#)
- web address [2-1](#)

---

**W**

Windows application event log [7-1](#)