VPN Phone

TECHNOLOGY DESIGN GUIDE

August 2013

VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **IP Phone with VPN Client for Teleworker**—Organizations want a teleworker solution that is easy to deploy and manage and provides secure signaling and media. Their employees need a solution that is simple to use.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Unified communications applications, such as IP telephony
- Telephony call agent
- IP telephones
- Virtual private networks
- Security device manager

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices
- **CCNP Voice**—3 to 5 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks

Related CVD Guides

Remote Access VPN Technology Design Guide

Telephony Using Cisco UCM Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

Introduction

Providing employees access to networked business services from a residential environment poses challenges for both the end-user and IT operations. For the home-based teleworker, it is critical that access to business services be reliable and consistent, providing an experience that is as similar as possible to sitting in a cubicle or office in the organization's facility. However, many employees already have a personal network set up in their homes, and integrating another network in parallel may be impractical because of a lack of Ethernet wiring or congestion in the 2.4GHz wireless band.

Technology Use Case

IT operations have a different set of challenges when it comes to implementing a teleworking solution, including properly securing, maintaining, and managing the teleworker environment from a centralized location. Because operational expenses are a constant consideration, IT must implement a cost-effective solution that provides investment protection without sacrificing quality or functionality.

Use Case: IP Phone with VPN Client for Teleworker

Organizations want a teleworker solution that is easy to deploy and manage, and they want the telephony signaling and media to be secure from prying eyes on the Internet. Their users want a solution that is simple to use.

This design guide enables the following capabilities:

- Easy to deploy—You configure all settings via the centralized Cisco Unified Communications Manager (Unified CM) administration. Using the existing VPN Group configuration on the Cisco Adaptive Security Appliance (ASA), the phone establishes a VPN connection to the same Cisco ASA pair as the Cisco AnyConnect PC clients.
- Easy to use—After you configure the phone within the enterprise, the user can take it home and plug it into a broadband router for instant connectivity without any difficult menus to configure. Also, if you provide a Cisco Unified IP Phone 9971 and a laptop with a wireless card, this solution does not require the home office to be wired.
- Easy to manage—Phones can receive firmware updates and configuration changes remotely.
- Secure—The VPN tunnel only applies to traffic originating from the phone itself. A PC connected to the PC port is responsible for authenticating and establishing its own tunnel with VPN client software. As it is with the Cisco AnyConnect PC clients, authentication for the phone requires the user's Microsoft Active Directory (AD) username and password.

Design Overview

The Cisco VPN Client for Cisco Unified IP Phones, working in conjunction with the Cisco AnyConnect Client for PCs and laptops, provides a solution for organizations with remote telecommuters who require only data and voice access.

The solution builds upon the remote access VPN solution in the Remote Access VPN Design Guide. That solution can be used both for the mobile user and the teleworker at the same time, without modification.

Because the worker may be teleworking full-time, and to make the solution a more office-like environment, a physical phone is used instead of a soft phone running on the PC. To connect the phone back into the organization, the solution uses Cisco VPN Client for Cisco Unified IP Phones.

This Cisco VPN Client configuration requires that the phone is pre-provisioned and that it establishes the initial connection inside of the corporate network to retrieve the phone configuration. After that, subsequent connections can be made using VPN, as the configuration is retrieved on the phone.

The following Cisco Unified IP Phones are currently supported:

- 7942
- 7962
- 7945
- 7965
- 7975
- 8900 series
- 9900 series

Deployment Details

PROCESS

Configuring Cisco ASA

1. Create the identity certificate

Before you continue, ensure that Cisco ASA is configured for remote access VPN. Only the procedures required to support the integration of VPN IP phones into the deployment are included in this guide. For more information on Cisco ASA configuration, see the Remote Access VPN Design Guide.

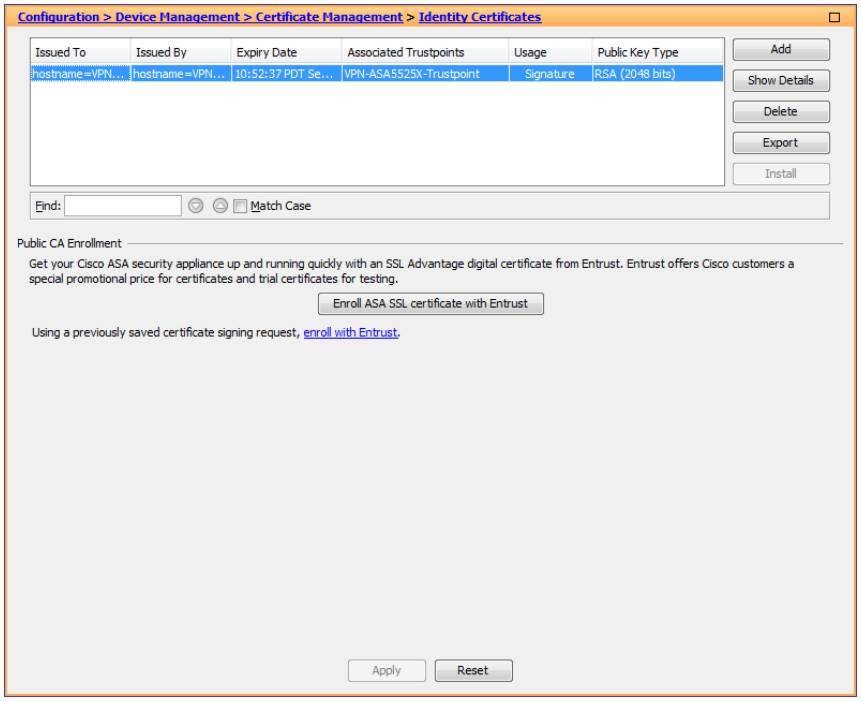
Procedure 1 Create the identity certificate

To attach to Cisco ASA from an IP phone, you must import a copy of the appliance's identity certificate, which can be self-signed, into Unified CM.

Step 1: Launch the Cisco ASA Security Device Manager.

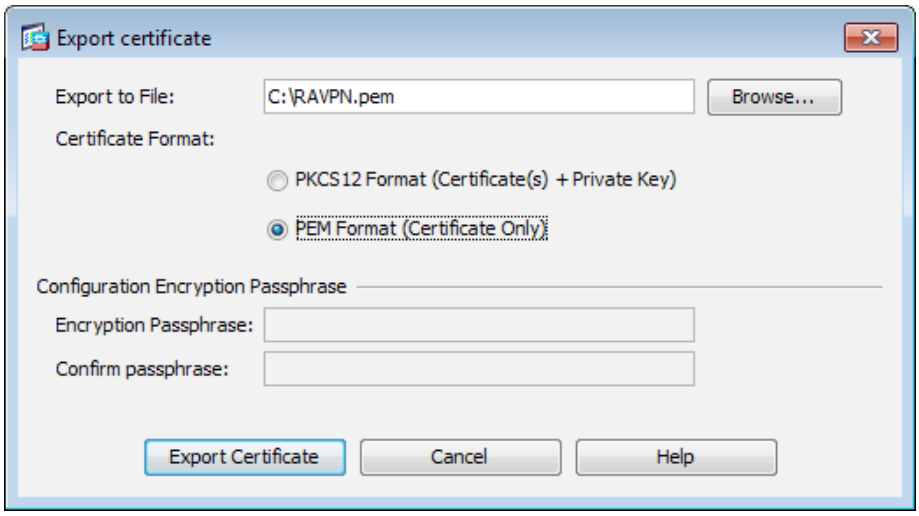
Step 2: Navigate to **Configuration > Device Management > Certificate Management**, and then click **Identity Certificates.**

Step 3: In the list of identity certificates, select the identity certificate used for remote access VPN (Example: ASDM_TrustPoint0), and then click **Export**.

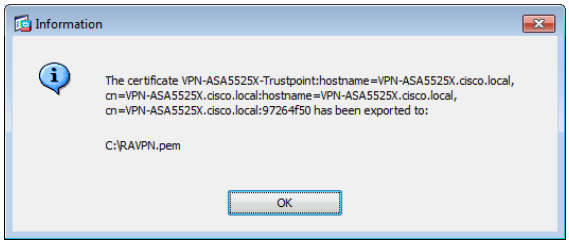


Step 4: On the Export certificate dialog box, enter a filename for the certificate. (Example: C:\RAVPN.pem)

Step 5: Select **PEM Format (Certificate Only)**, and then click **Export Certificate.**



The Information dialog box shows the certificate has been exported.



Step 6: On the Information dialog box, click **OK**, and then click **Apply**.

PROCESS

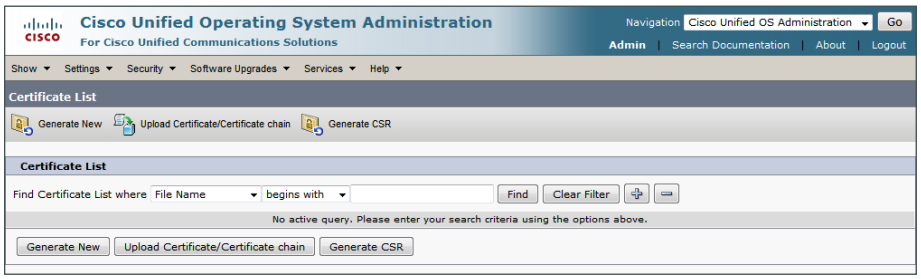
Configuring Cisco Unified CM

1. Import Cisco ASA certificate
2. Configure the VPN gateways
3. Configure the VPN group
4. Configure the VPN profile
5. Configure the VPN feature
6. Configure a common phone profile

Procedure 1 Import Cisco ASA certificate

Step 1: Navigate to the Cisco Unified Operating Systems Administration page on the publisher. (Example: https://cucm-pub1.cisco.local/cmplatform/)

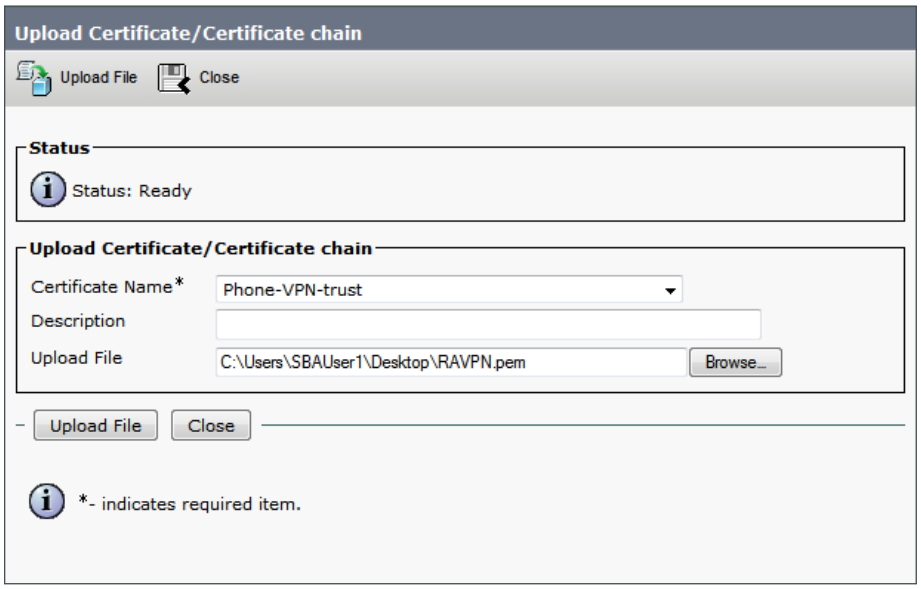
Step 2: Navigate to **Security > Certificate Management**, and then click **Upload Certificate/Certificate Chain**.



Step 3: On the Upload Certificate/Certificate chain page, in the **Certificate Name** list, choose **Phone-VPN-trust**.

Step 4: In the **Upload File** box, enter the certificate filename that you configured in Procedure 1, Step 5.

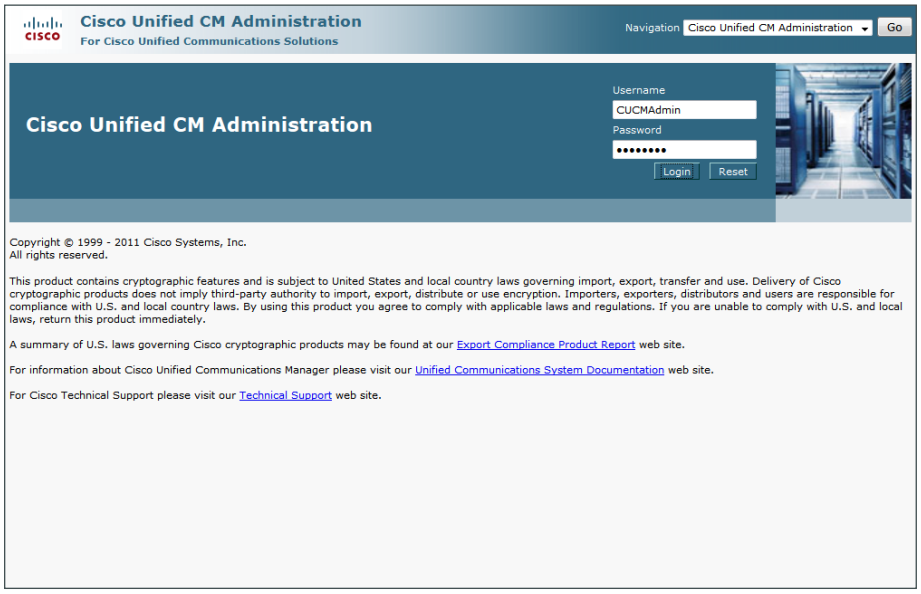
Step 5: Click **Upload File**.



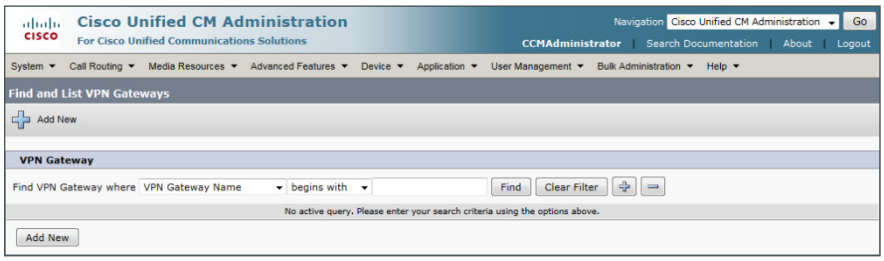
When the upload is complete, the Status pane shows **Success: Certificate Uploaded**.

Procedure 2 Configure the VPN gateways

Step 1: In the **Navigation** list, choose **Cisco Unified CM Administration**, and then click **Go**.



Step 2: Navigate to **Advanced Features > VPN > VPN Gateway**, and then click **Add New**.

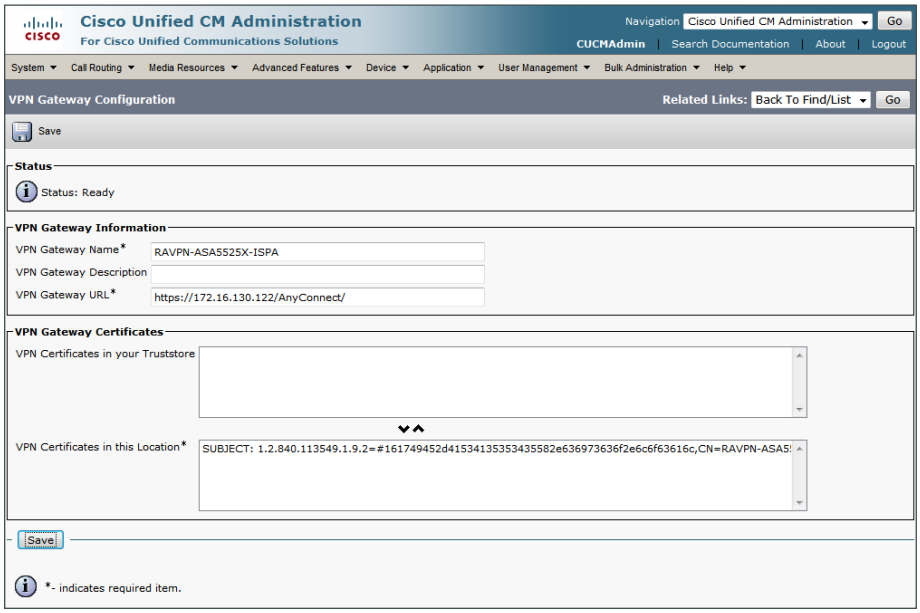


Step 3: On the VPN Gateway Configuration page, enter a name for the VPN Gateway. (Example: RAVPN-ASA5525X-ISPA)

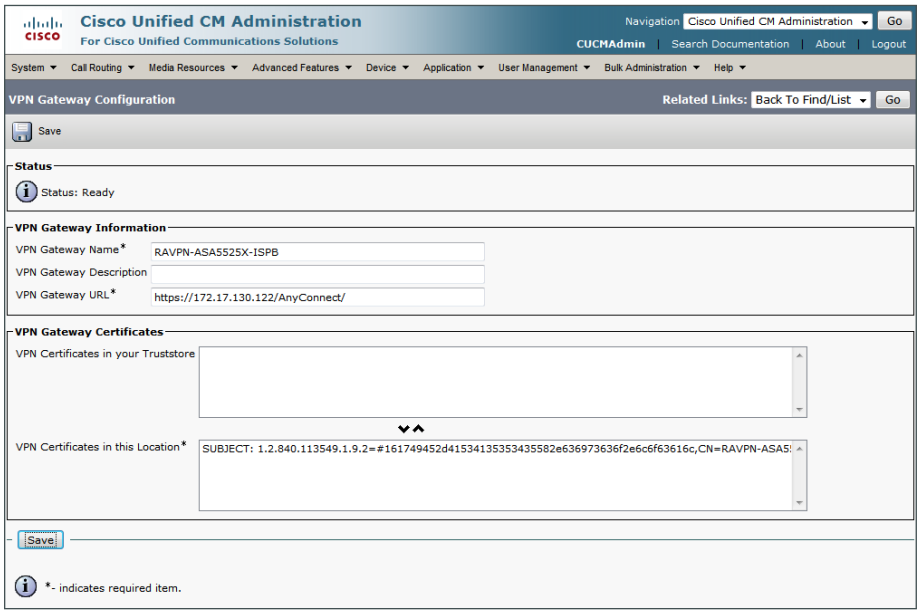
Step 4: In the **VPN Gateway URL** box, enter the URL for the VPN group on Cisco ASA's primary Internet connection. (Example: https://172.16.130.122/AnyConnect/)

Step 5: In the **VPN Gateway Certificates** pane, move the certificate from the **VPN Certificates in your Truststore** list to the **VPN Certificates in this Location** list by selecting it, and then clicking the **down arrow**.

Step 6: Click **Save**.



Step 7: If you have a second Internet connection, repeat Step 2 through Step 6 to add a second VPN gateway using the URL for the VPN group on Cisco ASA's second interface. (Example: https://172.17.130.122/AnyConnect/)



Procedure 3 Configure the VPN group

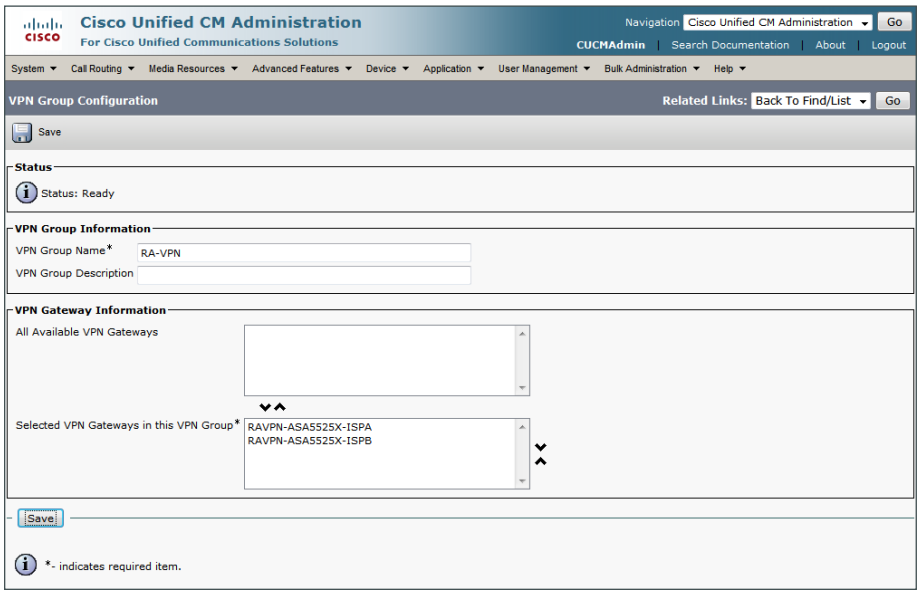
Step 1: Navigate to **Advanced Features > VPN > VPN Group**, and then click **Add New**.

Step 2: On the VPN Group Configuration page, enter a VPN Group Name. (Example RA-VPN)

Step 3: Move the primary VPN gateway from the **All Available VPN Gateways** list to the **Selected VPN Gateways in this VPN Group** list by selecting the gateway, and then clicking the **down arrow**.

Step 4: If you have a second Internet connection, move the secondary VPN gateway from the **All Available VPN Gateways** list to the **Selected VPN Gateways in this VPN Group** list by selecting the gateway, and then clicking the **down arrow**.

Step 5: Click **Save**.



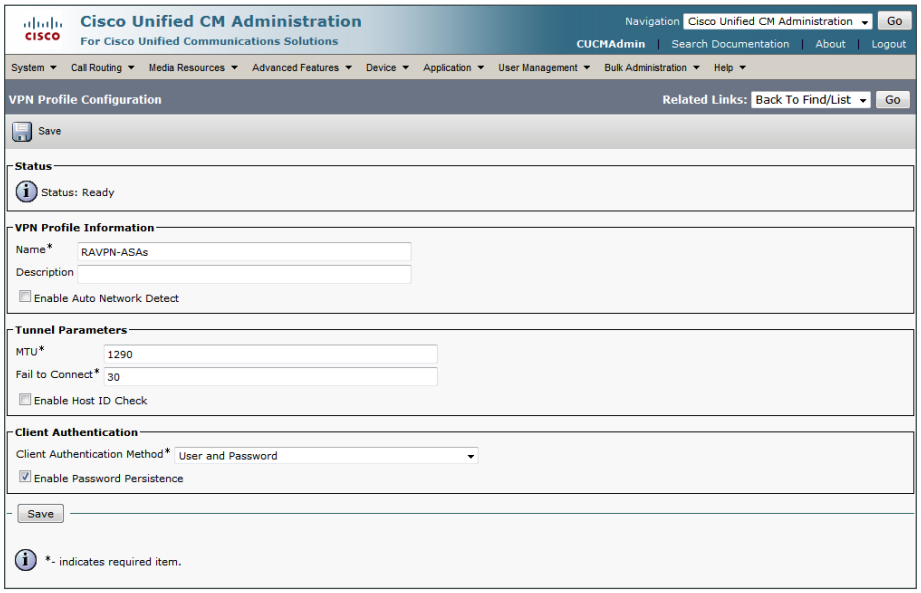
Procedure 4 Configure the VPN profile

Step 1: Navigate to **Advanced Features > VPN > VPN Profile**, and then click **Add New**.

Step 2: On the VPN Profile Configuration page, enter a name. (Example: RAVPN-ASAs)

Step 3: Because the Cisco ASA's identity certificate has been self-signed, clear **Enable Host ID Check**.

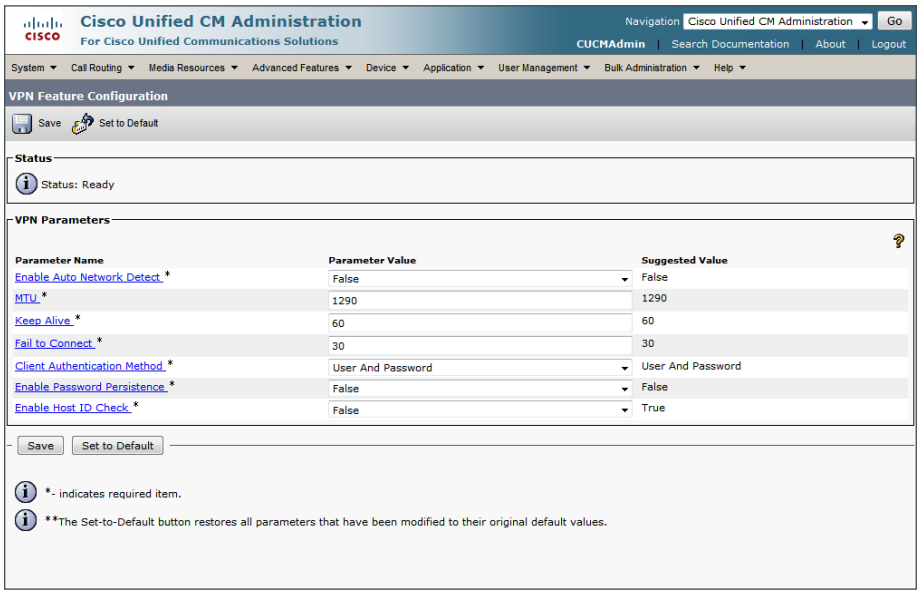
Step 4: Select **Enable Password Persistence**, and then click **Save**.



Procedure 5 Configure the VPN feature

Step 1: Navigate to **Advanced Features > VPN**, and then click **VPN Feature Configuration**.

Step 2: Because the Cisco ASA's identity certificate has been self-signed, in the **Enable Host ID Check** field, choose **False**, and then click **Save**.



Procedure 6 Configure a common phone profile

Step 1: Navigate to **Device > Device Settings > Common Phone Profile**, and then click **Add New**.

Step 2: On the Common Phone Profile Configuration page, enter a name. (Example: VPN Common Phone Profile)

Step 3: In the VPN Information pane, in the **VPN Group** list, choose the VPN group that you configured in Procedure 3. (Example: RA-VPN)

Step 4: In the **VPN Profile** list, choose the VPN profile that you configured in Procedure 4. (Example: RAVPN-ASAs)

Step 5: Click **Save**.

PROCESS

Configuring the IP Phone

1. Create the teleworker device pool
2. Register and configure the device
3. Connect the IP phone

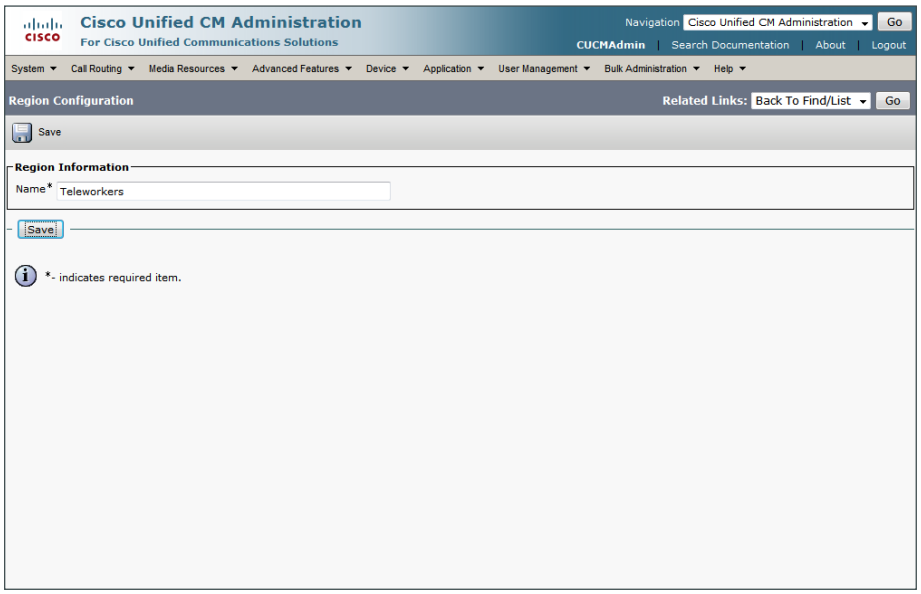
The phone must register to Cisco Unified CM from inside the organization's network before the end-user can use it over VPN. The registration process upgrades the phone's firmware and downloads the phone's configuration, including the VPN settings.

In the following procedures, you can configure a registered device with the VPN information so that an end-user can deploy it outside the organization's network.

Procedure 1 Create the teleworker device pool

Step 1: Navigate to **System > Region Information > Region**, and then click **Add New**.

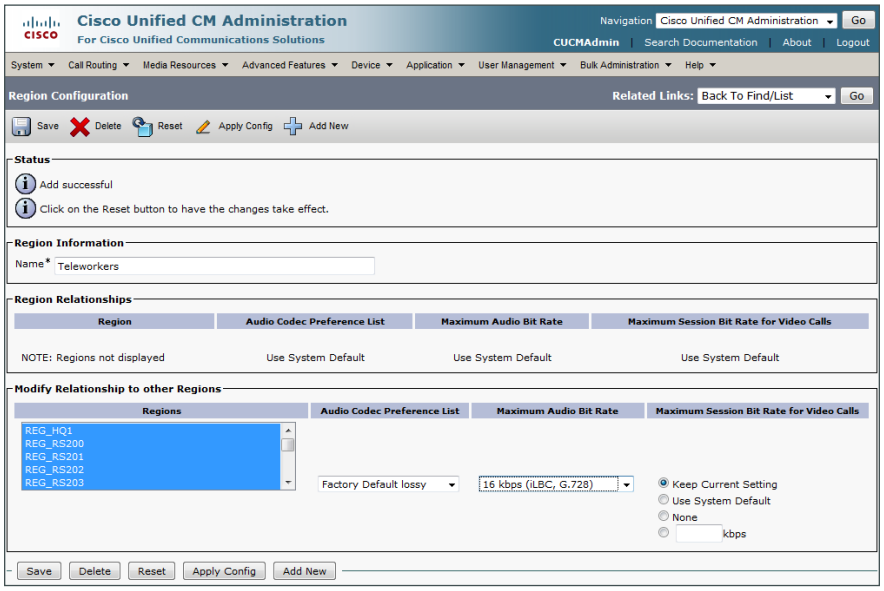
Step 2: In the Region Information pane, in the **Name** box, enter a name for the region, and then click **Save**. (Example: Teleworkers)



Step 3: In the **Modify Relationship to other Regions** pane, in the **Regions** list, select every region.

Step 4: In the **Max Audio Bit Rate** list, choose **16 kbps (iLBC, G.728)**.

Step 5: In the **Audio Codec Preference List** list, choose **Factory Default lossy**, and then click **Save**.



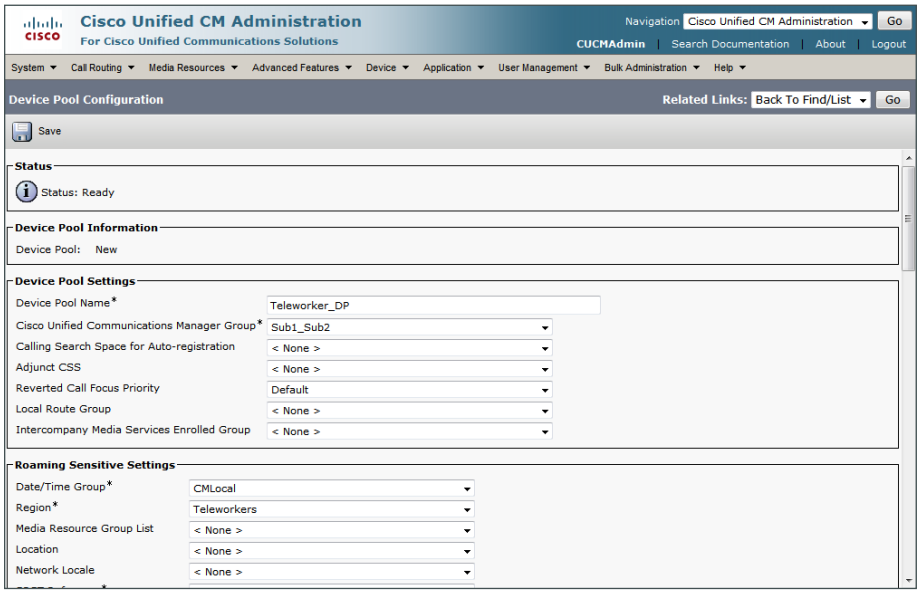
Step 6: Navigate to **System > Device Pool**, and then click **Add New**.

Step 7: In the **Device Pool Name** box, enter a name. (Example: Teleworker_DP)

Step 8: In the **Cisco Unified Communications Manager Group** list, choose the primary group. (Example: Sub1_Sub2)

Step 9: In the **Date/Time Group** list, choose the time zone for the teleworker devices. (Example: Pacific)

Step 10: In the **Region** list, choose the teleworker region that you configured in Step 2, and then click **Save**. (Example: Teleworkers)



Procedure 2 Register and configure the device

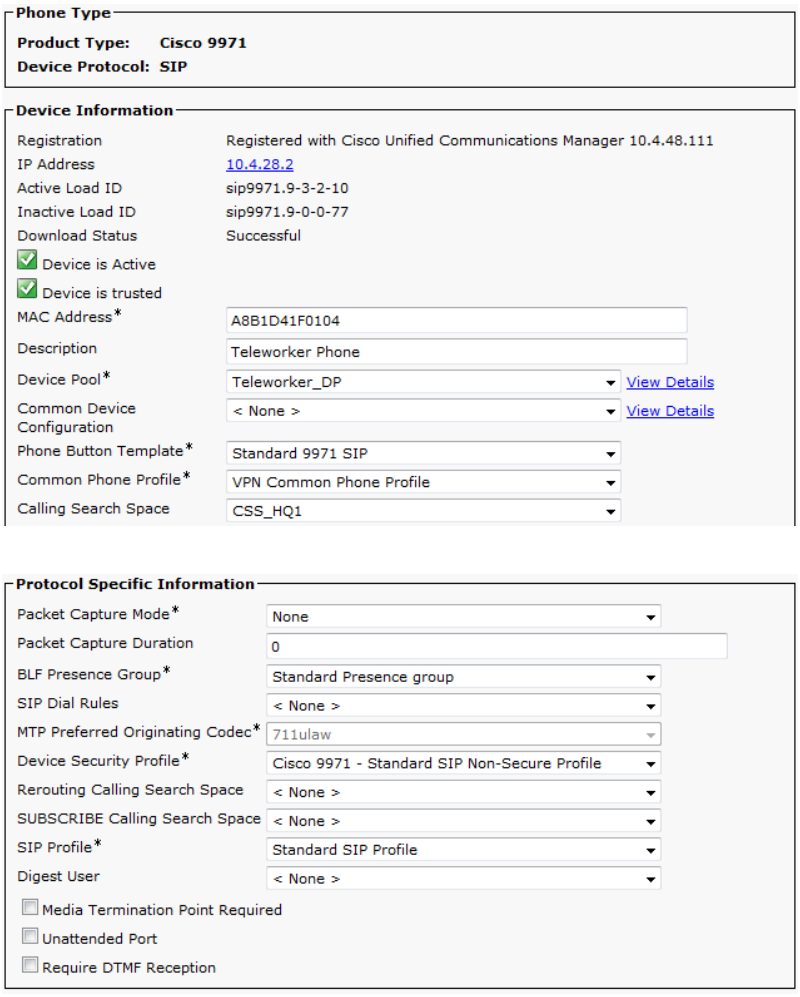
Step 1: On Unified CM, navigate to **Device > Phone**, and then click **Add New.**

Step 2: Enter the following values, and after each entry, click **Next**:

- Phone Type–**Cisco [Model]**
- Select the device protocol–**SIP**

Step 3: On the Phone Configuration page, enter the following values, and then click **Save**:

- MAC Address–**[MAC Address]**
- Description–**Teleworker Phone**
- Device Pool–**Teleworker_DP**
- Phone Button Template–**Standard [Model] SIP**
- Common Phone Profile–**VPN Common Phone Profile**
- Calling Search Space–**CSS_HQ1**
- Device Security Profile–**Cisco [Model] - Standard SIP Non-Secure Profile**
- SIP Profile–**Standard SIP Profile**



Step 4: On the Phone Configuration page, under Association Information, click **Line [1] - Add a new DN**.

Step 5: On the Directory Number Configuration page, enter the following values, and then click **Save**.

- Directory Number–**[DN]**
- Route Partition–**PAR_Base**
- Description–**Teleworker - [name]**
- Alerting Name–**[Alerting name]**
- ASCII Alerting Name–**[ASCII alerting name]**

Procedure 3 Connect the IP phone

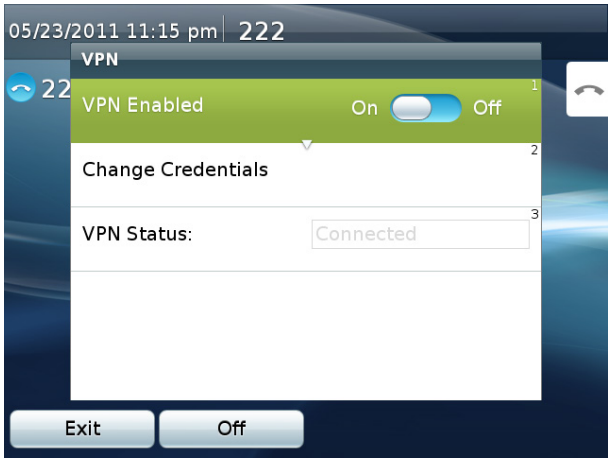
Step 1: Connect the phone to the user's home network.

Step 2: On the phone, select **Applications > VPN**. This connects the phone to the organization over VPN.

Step 3: In the **VPN Enabled** pane, select **On**.

Step 4: Enter the user ID and password.

Step 5: Press **Sign In**. The VPN Status shows **Connected**.



Appendix A: Product List

VPN Phone License

Functional Area	Product Description	Part Numbers	Software
SSL Software License for ASA	ASA 5500 SSL VPN 250 Premium User License	ASA5500-SSL-250	ASA 9.0(1)
	ASA 5500 SSL VPN 500 Premium User License	ASA5500-SSL-500	
AnyConnect VPN Phone License	AnyConnect VPN Phone License - ASA 5545-X (requires a Premium license)	L-ASA-AC-PH-5545=	ASA 9.0(1)
	AnyConnect VPN Phone License - ASA 5525-X (requires a Premium license)	L-ASA-AC-PH-5525=	
	AnyConnect VPN Phone License - ASA 5515-X (requires a Premium license)	L-ASA-AC-PH-5515=	
	AnyConnect VPN Phone License - ASA 5512-X (requires a Premium license)	L-ASA-AC-PH-5512=	

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(6)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	ASA 9.0(1)
	Cisco ASA 5525-X Firewall Edition - security appliance	ASA5525-K9	
	Cisco ASA 5515-X Firewall Edition - security appliance	ASA5515-K9	
	Cisco ASA 5512-X Firewall Edition - security appliance	ASA5512-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Data Center or Server Room

Functional Area	Product Description	Part Numbers	Software
Virtual Servers	Cisco UCS C240 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C240M3S	9.1(1a) ESXi 5.0
	Cisco UCS C220 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C220M3S	
	Cisco UCS C220 M3 for Business Edition 6000	UCSC-C220-M3SBE	

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000320-1 08/13