

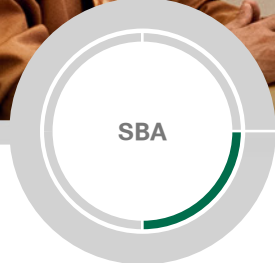


# Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to <http://www.cisco.com/go/sba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





# Teleworking—VPN Phone Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 Series

# Preface

## Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

## Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

**month year** Series

For example, the series of guides that we released in August 2012 are the “August 2012 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

## How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). 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 shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100  
100 100 100
```

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 [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

# Table of Contents

<b>What's In This SBA Guide</b> .....	<b>1</b>	<b>Deployment Details</b> .....	<b>3</b>
Cisco SBA Solutions.....	1	Configuring Cisco ASA.....	3
Route to Success.....	1	Configuring Cisco UCM.....	5
About This Guide.....	1	Configuring the IP Phone.....	9
<b>Introduction</b> .....	<b>2</b>	<b>Appendix A: Product List</b> .....	<b>12</b>
Business Overview.....	2	<b>Appendix B: Changes</b> .....	<b>14</b>
Technology Overview.....	2		

# What's In This SBA Guide

## Cisco SBA Solutions

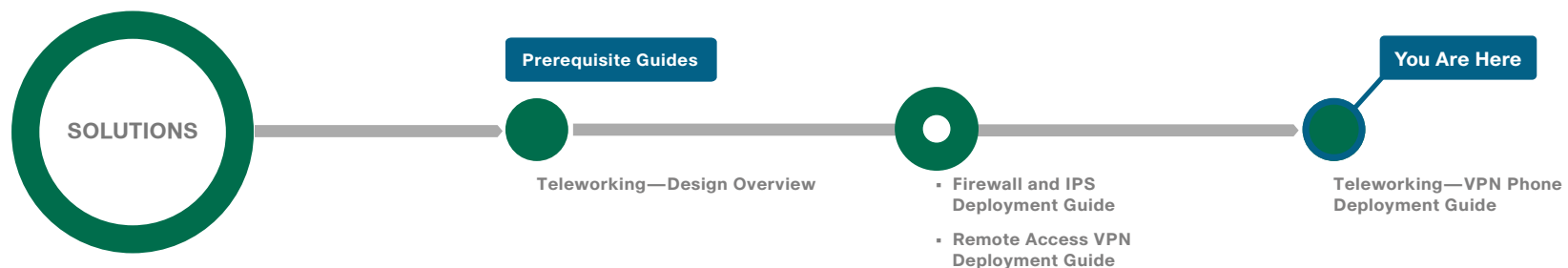
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

## Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



## About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>



# Introduction

## Business Overview

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.

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.

## Technology 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 *Cisco SBA—Borderless Networks Remote Access VPN Deployment 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. The Cisco VPN Client is:

- **Easy to Deploy**—You configure all settings via Cisco Unified Communications Manager (UCM) 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**—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 users' Microsoft Active Directory (AD) username and password.

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, and 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 *Cisco SBA—Borderless Networks Remote Access VPN Deployment Guide*.

## Procedure 1 Create the identity certificate

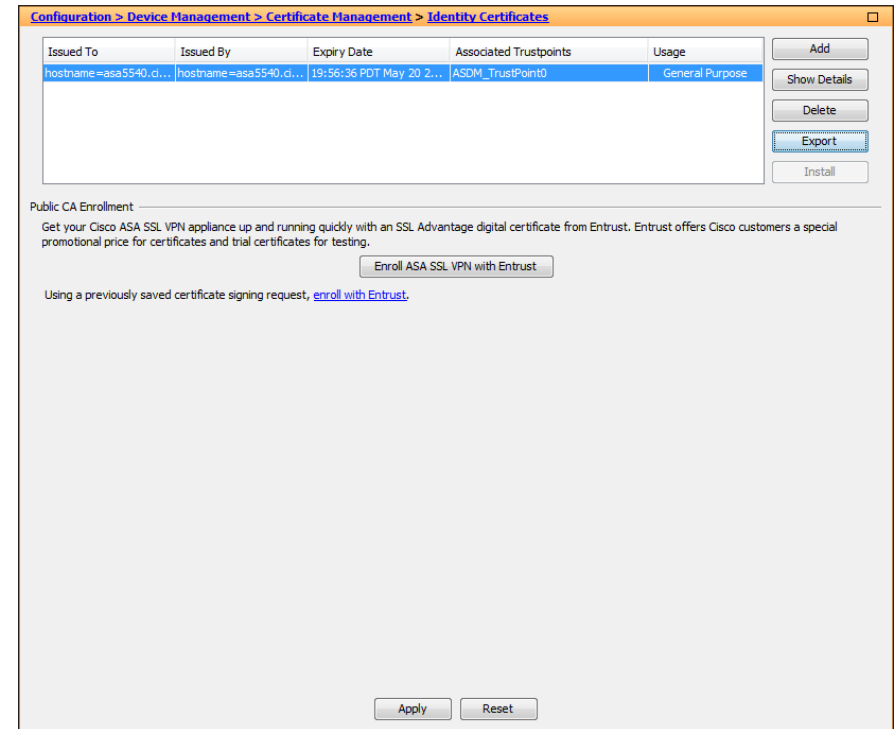
To attach to Cisco ASA from an IP phone, you must import a copy of the appliance's identity certificate, which can be self-signed, into Cisco Unified Communications Manager (UCM).

**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)

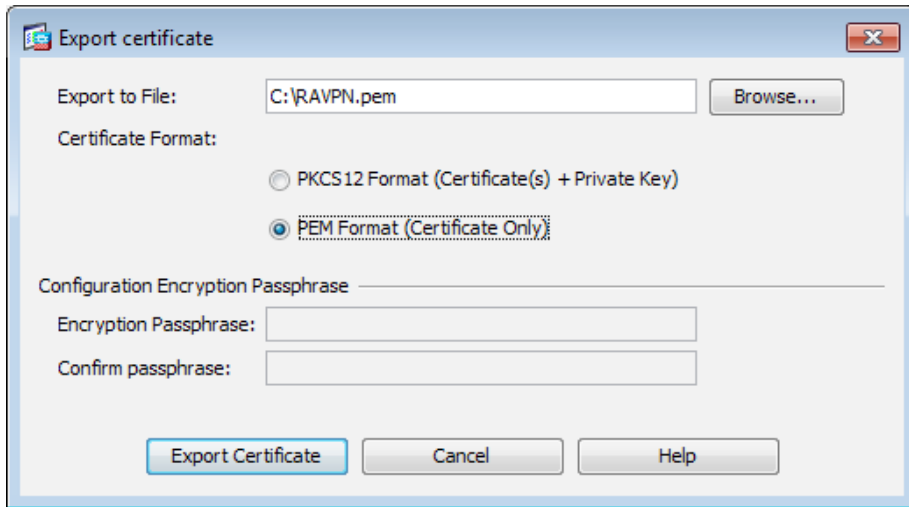
**Step 4:** Click **Export**.



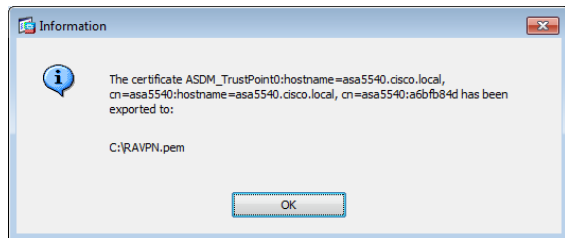
The screenshot shows the Cisco ASA Security Device Manager interface for Identity Certificates. The breadcrumb navigation is Configuration > Device Management > Certificate Management > Identity Certificates. A table lists identity certificates with columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, and Usage. One certificate is listed: hostname=asa5540.c... | hostname=asa5540.c... | 19:56:36 PDT May 20 2... | ASDM\_TrustPoint0 | General Purpose. To the right of the table are buttons: Add, Show Details, Delete, Export (highlighted), and Install. Below the table is a section for Public CA Enrollment with a button 'Enroll ASA SSL VPN with Entrust' and a link 'enroll with Entrust'. At the bottom are 'Apply' and 'Reset' buttons.

**Step 5:** On the Export certificate dialog box, enter a filename for the certificate. (Example: C:\RAVPN.pem)

**Step 6:** Select **PEM Format (Certificate Only)**, and then click **Export Certificate**.



The Information dialog box shows the certificate has been exported.



**Step 7:** On the Information dialog box, click **OK**, and then click **Apply**.

## Notes



## Process

### Configuring Cisco UCM

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/>)

**Cisco Unified Operating System Administration**

Navigation: Cisco Unified OS Administration Go

Status  
Ligon failed. Please try again.

Username  
Admin

Password  
\*\*\*\*\*

Login Reset

Copyright © 1999 - 2011 Cisco Systems, Inc. All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

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

**Cisco Unified Operating System Administration**

Navigation: Cisco Unified OS Administration Go

Show Settings Security Software Upgrades Services Help

Certificate List

Generate New Upload Certificate/Certificate chain Generate CSR

Certificate List

Find Certificate List where File Name begins with Find Clear Filter

No active query. Please enter your search criteria using the options above.

Generate New Upload Certificate/Certificate chain Generate CSR

**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.

**Upload Certificate/Certificate chain**

Upload File Close

Status  
Status: Ready

**Upload Certificate/Certificate chain**

Certificate Name\* Phone-VPN-trust

Description

Upload File C:\Users\SBAUser1\Desktop\RAVPN.pem Browse...

Upload File Close

\* - indicates required item.

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

Status  
Success: Certificate Uploaded

## Procedure 2

## Configure the VPN gateways

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

The screenshot shows the Cisco Unified CM Administration login page. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below this, there is a "Navigation" dropdown menu set to "Cisco Unified CM Administration" and a "Go" button. The main content area features a large blue header with the text "Cisco Unified CM Administration". Below the header, there is a login form with fields for "Username" (containing "CUCMAdmin") and "Password" (masked with dots). There are "Login" and "Reset" buttons. At the bottom of the page, there is a copyright notice: "Copyright © 1999 - 2011 Cisco Systems, Inc. All rights reserved." and several paragraphs of legal disclaimers regarding cryptographic features and U.S. laws.

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

The screenshot shows the "Find and List VPN Gateways" page in the Cisco Unified CM Administration interface. The navigation bar at the top includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area has a "Find and List VPN Gateways" header with an "Add New" button. Below this, there is a search form with a dropdown for "VPN Gateway Name" and a "begins with" dropdown. There are "Find", "Clear Filter", and "Add New" buttons. A message at the bottom of the search area reads: "No active query. Please enter your search criteria using the options above."

**Step 3:** On the VPN Gateway Configuration page, enter a name for the VPN Gateway. (Example: RAVPN-ASA525X-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.

The screenshot shows the "VPN Gateway Configuration" page in the Cisco Unified CM Administration interface. The navigation bar at the top includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area has a "VPN Gateway Configuration" header with a "Save" button and "Related Links: Back To Find/List" and "Go" buttons. Below this, there is a "Status" section showing "Status: Ready". The "VPN Gateway Information" section contains fields for "VPN Gateway Name\*" (RAVPN-ASA525X-ISPA), "VPN Gateway Description", and "VPN Gateway URL\*" (https://172.16.130.122/AnyConnect/). The "VPN Gateway Certificates" section has two lists: "VPN Certificates in your Truststore" and "VPN Certificates in this Location\*". The "VPN Certificates in this Location\*" list shows a certificate with the subject "SUBJECT: 1.2.840.113549.1.9.2=#161749452d41534135353435582e636973636f2e6c6f63616c,CN=RAVPN-ASAS:". There is a "Save" button at the bottom of the form and a note: "\* - indicates required item."

**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/)

The screenshot shows the "VPN Gateway Configuration" page in the Cisco Unified CM Administration interface, similar to the previous screenshot but with a different VPN Gateway Name and URL. The "VPN Gateway Information" section contains fields for "VPN Gateway Name\*" (RAVPN-ASA525X-ISP8), "VPN Gateway Description", and "VPN Gateway URL\*" (https://172.17.130.122/AnyConnect/). The "VPN Certificates" section has two lists: "VPN Certificates in your Truststore" and "VPN Certificates in this Location\*". The "VPN Certificates in this Location\*" list shows a certificate with the subject "SUBJECT: 1.2.840.113549.1.9.2=#161749452d41534135353435582e636973636f2e6c6f63616c,CN=RAVPN-ASAS:". There is a "Save" button at the bottom of the form and a note: "\* - indicates required item."

### 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**.

The screenshot shows the 'VPN Group Configuration' page in the Cisco Unified CM Administration interface. The page includes a navigation menu at the top with options like System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is divided into several sections: 'Status' (Ready), 'VPN Group Information' (Name: RA-VPN, Description: ), and 'VPN Gateway Information'. The 'VPN Gateway Information' section contains two lists: 'All Available VPN Gateways' (empty) and 'Selected VPN Gateways in this VPN Group' (containing RAVPN-ASA5525X-1SPA and RAVPN-ASA5525X-1SPB). A 'Save' button is located at the bottom left, and a note indicates that asterisks denote required items.

### 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**.

The screenshot shows the 'VPN Profile Configuration' page in the Cisco Unified CM Administration interface. The page includes a navigation menu at the top with options like System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is divided into several sections: 'Status' (Ready), 'VPN Profile Information' (Name: RAVPN-ASAs, Description: ), 'Tunnel Parameters' (MTU: 1290, Fail to Connect: 30, Enable Host ID Check: unchecked), and 'Client Authentication' (Method: User and Password, Enable Password Persistence: checked). A 'Save' button is located at the bottom left, and a note indicates that asterisks denote required items.

### 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**.

The screenshot shows the 'VPN Feature Configuration' page in Cisco Unified CM Administration. The 'VPN Parameters' table is as follows:

Parameter Name	Parameter Value	Suggested Value
Enable Auto Network Detect *	False	False
MTU *	1290	1290
Keep Alive *	60	60
Fail to Connect *	30	30
Client Authentication Method *	User And Password	User And Password
Enable Password Persistence *	False	False
Enable Host ID Check *	False	True

Buttons for 'Save' and 'Set to Default' are visible at the bottom of the configuration area.

## 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)

The screenshot shows the 'VPN Information' section with the following values:

- VPN Group: RA-VPN
- VPN Profile: 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 UCM 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**, 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)

The screenshot shows the 'Region Configuration' page in Cisco Unified CM Administration. The 'Region Information' section has the following value:

- Name: Teleworkers

A 'Save' button is visible below the name field.

**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 **Link Loss Type** list, choose **Lossy**, and then click **Save**.

**Region Configuration**

Save Delete Reset Apply Config Add New

**Status**

Add successful  
Click on the Reset button to have the changes take effect.

**Region Information**

Name\* Teleworkers

**Region Relationships**

Region	Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)	Link Loss Type
NOTE: Region(s) not displayed	Use System Default	Use System Default	Use System Default

**Modify Relationship to other Regions**

Regions	Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)	Link Loss Type
REG_RS223 REG_RS230 REG_RS231 REG_RS232 Teleworkers	16 kbps (iLBC, G.728)	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None kbps	Lossy

Save Delete Reset Apply Config Add New

\*- indicates required item.

**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)

**Device Pool Configuration**

Save

**Status**

Status: Ready

**Device Pool Information**

Device Pool: New

**Device Pool Settings**

Device Pool Name\* Teleworker\_DP

Cisco Unified Communications Manager Group\* Sub1\_Sub2

Calling Search Space for Auto-registration < None >

Adjunct CSS < None >

Reverted Call Focus Priority Default

Local Route Group < None >

Intercompany Media Services Enrolled Group < None >

**Roaming Sensitive Settings**

Date/Time Group\* CMLocal

Region\* Teleworkers

Media Resource Group List < None >

Location < None >

Network Locale < None >

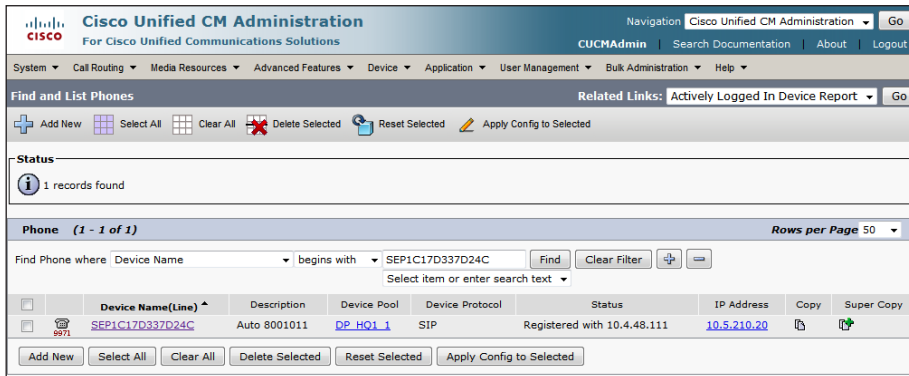
## Procedure 2

## Register and configure the device

**Step 1:** Navigate to **Device > Phone**, and then enter the name of the device in the search text box.

**Step 2:** Click **Find**.

**Step 3:** In the **Device Name** column, click the name of the device. The Phone Configuration page opens.

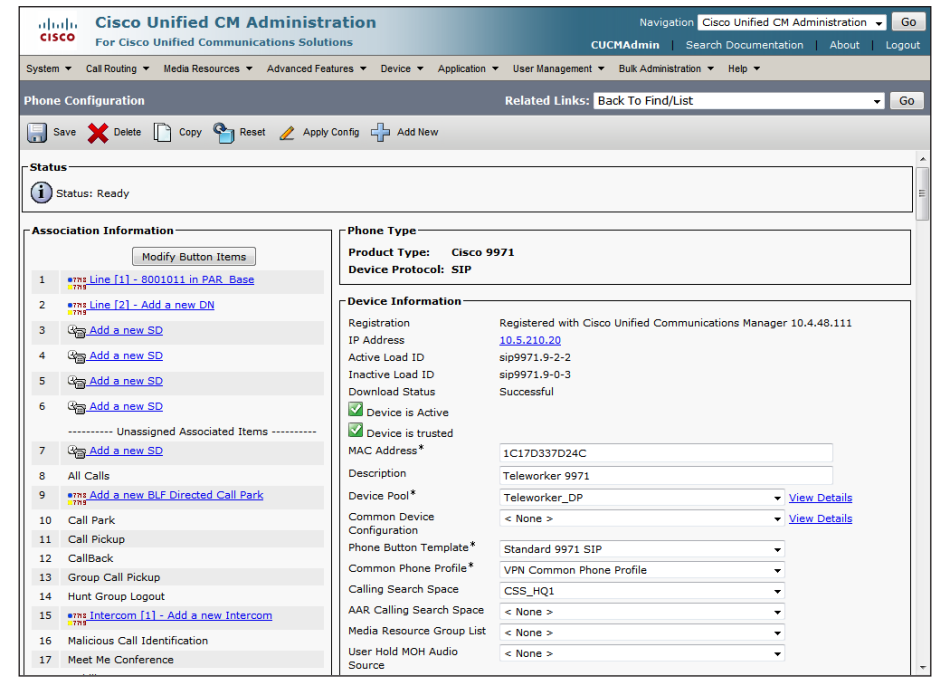


**Step 4:** On the Phone Configuration page, in the **Device Pool** list, choose the device pool that you configured in Procedure 1 Step 6. (Example: Teleworker\_DP)

**Step 5:** In the **Common Phone Profile** list, choose the profile that you configured in Procedure 6. (Example: VPN Common Phone Profile)

**Step 6:** In the **Calling Search Space** list, choose the calling search space, and then click **Save**. (Example: CSS\_HQ1)

**Step 7:** Click **Apply Config**.





### 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 500 Premium User License	ASA5500-SSL-500	8.6(1)1
	ASA 5500 SSL VPN 250 Premium User License	ASA5500-SSL-250	
AnyConnect VPN Phone License	AnyConnect VPN Phone License - ASA 5545-X (requires a Premium license)	L-ASA-AC-PH-5545=	8.6(1)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 8.6(1)1 IPS 7.1(4) 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	6.6.114
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	8.6(1)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 ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	6.6.114

## Telephony

Functional Area	Product Description	Part Numbers	Software
Call Control	Cisco Media Convergence Server 7845-I3 for Unified Communications Manager up to 10,000 users	MCS7845I3-K9-CMD3A	8.6(2a)SU1
	Cisco Media Convergence Server 7835-I3 for Unified Communications Manager up to 2500 users	MCS7835I3-K9-CMD3A	
Voice Messaging	Cisco Media Convergence Server 7845-I3 for Unity Connection up to 10,000 users	MCS7845I3-K9-UCC2	8.6(2a)SU1
	Cisco Media Convergence Server 7835-I3 for Unity Connection up to 2500 users	MCS7835I3-K9-UCC2	
Call Control Virtual Servers	Cisco UCS C210 M2 General-Purpose Rack-Mount Server for unified communications applications	UCS-C210M2-VCD2	8.6(2a)SU1 ESXi4.1
	Cisco UCS C200 M2 High-Density Rack-Mount Server for unified communications applications	UCS-C200M2-VCD2	
	Unified CMBE6K UCS C200M2 for Unified Communications Manager up to 500 users	UCS-C200M2-BE6K	

# Appendix B: Changes



This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We made minor changes to improve the readability of this guide.

## Notes

## Feedback

Click [here](#) to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



**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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)