



# 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.





SBA

ENTERPRISE

BORDERLESS  
NETWORKS

# Teleworking Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

February 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 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.

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 2011 are the “August 2011 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  
100 100 100
```

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 forum at the bottom of one of the following sites:

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

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

An RSS feed is available if you would like to be notified when new comments are posted.

# Table of Contents

<b>What's In This SBA Guide</b> .....	<b>1</b>
About SBA.....	1
About This Guide .....	1
<b>Introduction</b> .....	<b>2</b>
<b>AnyConnect PC and Phone</b> .....	<b>3</b>
Business Overview.....	3
Technology Overview.....	3
Deployment Details .....	4
Configuring Cisco ASA .....	4
Configuring Cisco UCM.....	5
Configuring the IP Phone .....	9
<b>Cisco ASA 5505</b> .....	<b>12</b>
Business Overview.....	12
Technology Overview.....	12

Deployment Details .....	12
Configuring Internet Edge ASA for Teleworker VPN.....	13
Configuring Teleworker Cisco ASA 5505 Endpoints.....	19
<b>Cisco OfficeExtend</b> .....	<b>22</b>
Business Overview.....	22
Technology Overview.....	22
Deployment Details .....	23
Configuring the Internet Edge.....	23
Configuring the Cisco ACS .....	28
Configuring the LAN Distribution Switch .....	32
Configuring the WLC .....	33
Configuring Voice and Data Connectivity .....	39
Configuring WLC Resiliency .....	47
Configuring the 600 Series Office Extend Access Point .....	48

<b>Cisco Virtual Office .....</b>	<b>50</b>
Business Overview.....	50
Technology Overview.....	50
Deployment Details .....	51
Configuring the DMVPN Aggregation Router .....	52
Configuring the WAN Distribution Switch .....	61
Configuring the Internet Edge.....	62
Configuring the Cisco ACS .....	66
Configuring ArcanaNetworks MEVO .....	71

<b>Appendix A: Product List .....</b>	<b>85</b>
<b>Appendix B: Resilient DMVPN Template.....</b>	<b>87</b>
<b>Appendix C: Configuration Files .....</b>	<b>89</b>
IE-ASA5540.....	89
CVO Aggregation Router.....	99

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.

# What's In This SBA Guide

## About SBA

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.

For more information, see the *How to Get Started with Cisco SBA* document:

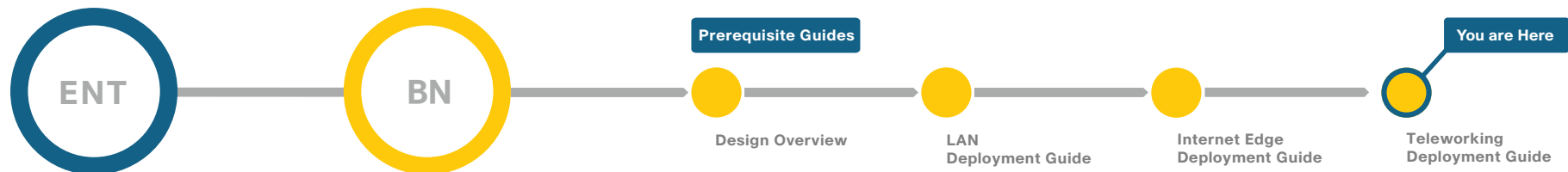
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless\\_Networks/Smart\\_Business\\_Architecture/SBA\\_Getting\\_Started.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf)

## About This Guide

This *additional deployment guide* includes the following sections:

- **Business Overview**—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.



## Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: <http://www.cisco.com/go/sba>  
For partner access: <http://www.cisco.com/go/sbachannel>

# Introduction

The concept of teleworking, also known as telecommuting, is not new. In 2010, IDC estimated that there were over 30 million teleworkers worldwide. Teleworkers differ from mobile workers in that they require a more office-like environment and typically work from a single semi-permanent location, in most cases their houses. These workers may have an informal arrangement with their supervisors, or the work arrangement may be more formalized with a written policy and enrollment.

Today, teleworkers are becoming more productive and connected, enabling companies to recruit the best talent, regardless of their location. At the same time, teleworking allows the workers to find the optimal life-work balance and job satisfaction while maintaining productivity and business continuity.

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 to sitting in a cubicle or office in the organization's facility. Additionally, solutions must support a wide range of teleworking employees with varying skill sets, making it critical to have a streamlined and simplified way to implement devices that allow for access to the corporate environment.

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. The introduction of cloud-based services requires IT to help ensure that employees have access to these services while minimizing the risk of viruses or attacks by providing secure Internet access. Because operational expenses are a constant consideration, IT must implement a cost-effective solution that provides investment protection without sacrificing quality or functionality.

The needs of teleworkers vary depending on the frequency and type of information they use to perform their jobs. There is no "one size fits all" technology solution for telework. To optimize teleworker solutions, organizations must understand the unique requirements of individual end users while providing a consistent, secure operating environment for all users, regardless of location.

Cisco offers a suite of teleworking solutions that provides options for all types of teleworkers. The Cisco teleworking solutions include:

- Cisco® AnyConnect PC and Phone.
- Cisco Adaptive Security Appliances (ASA) Series 5505.
- Cisco OfficeExtend.
- Cisco Virtual Office (CVO).

This document has been divided into multiple sections, each covering one of the teleworking solutions. To help decide which teleworking solution is the best fit for your organization, use the following table to identify your requirements and the solutions that support them.

**Table 1 - Teleworking requirements and the solutions that support them**

Your requirement	AnyConnect PC + Phone	ASA 5505	OfficeExtend	CVO
Wireless	X <sup>1</sup>		X	X
Wired	X <sup>1</sup>	X	X <sup>2</sup>	X
Efficient Intrasite Communication <sup>3</sup>		X		X
Advanced Technology Support (Multicast, Medianet)				X
Provisioning Complexity	Medium	High	Low	Low
Resiliency	Medium	Medium	Low	High
Recommended Scale in this Deployment	500	50	500	900

Notes:

1. Every device must support Cisco AnyConnect natively.
2. The Cisco OfficeExtend 600 Series AP supports one physical LAN connection and up to four MAC addresses.
3. Defined as traffic not having to leave the site to communicate between devices.

# AnyConnect PC and Phone

## 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 sitting in a cubicle or office in the organization's facility. However, many employees already have a personal network set up at their homes, and integrating another network in parallel might 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 only require data and voice access.

The solution builds upon the remote access VPN solution in the *Cisco SBA for Enterprise Organizations—Borderless Networks Internet Edge Deployment Guide*. That solution can be used both for the mobile user and the teleworker at the same time without modification.

Because the worker might 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 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) user name and password.

This Cisco VPN Client configuration requires that the phone be preprovisioned and that it establish the initial connection inside of the corporate network to retrieve the phone configuration, then 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

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the solution. These parameters are listed in the following table.

Table 2 - Universal design parameters

Network service	IP address
Domain name	cisco.local
Active Directory, DNS Server, DHCP Server	10.4.48.10
Authentication Control System (ACS)	10.4.48.15
Network Time Protocol (NTP) Server	10.4.48.17

### Process

Configuring Cisco ASA

1. Create the Identity Certificate

This guide assumes that the Cisco ASA has already been configured for remote access VPN. Only the procedures required to support the integration of VPN IP phones into the deployment are included. For more information on Cisco ASA configuration, see the *Internet Edge Deployment Guide*.

### Procedure 1 Create the Identity Certificate

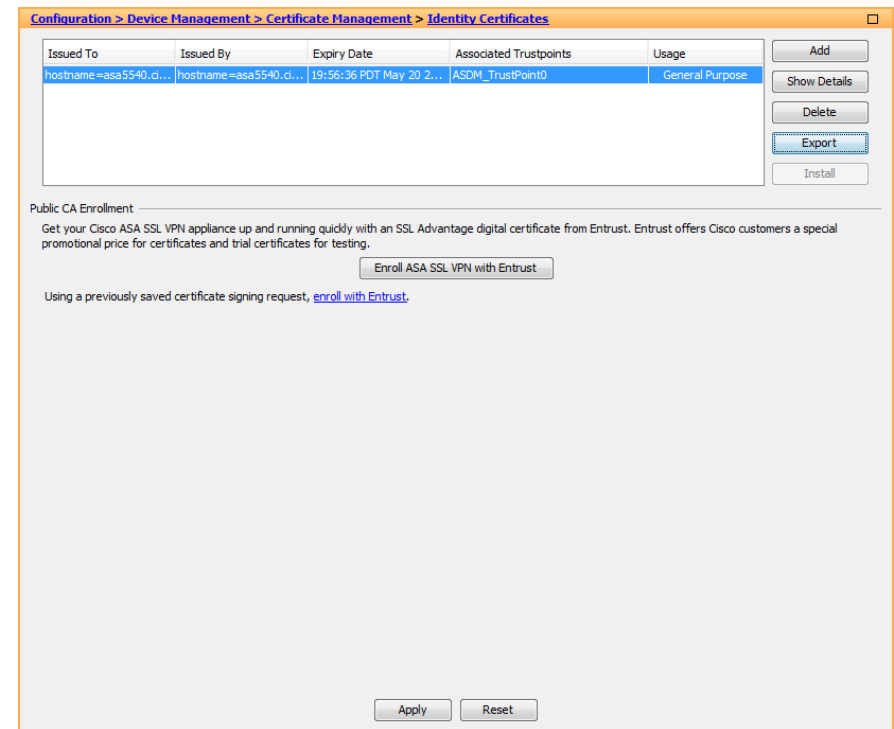
To be able to attach to Cisco ASA from an IP phone, you must import a copy of the appliance's identity certificate, which can be self-signed, into Cisco Unified Communications Manager.

**Step 1:** Launch the ASA Security Device Manager.

**Step 2:** In **Configuration > Device Management > Certificate Management**, click **Identity Certificates**.

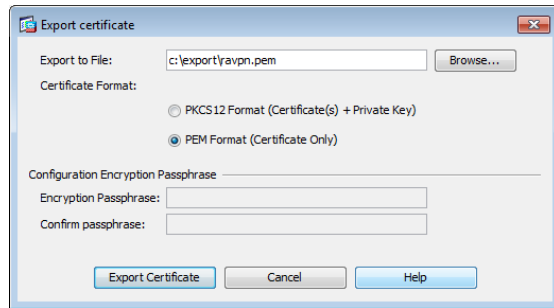
**Step 3:** From the list of identity certificates, select the identity certificate used for remote access VPN. (Example: ASDM\_TrustPoint0)

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

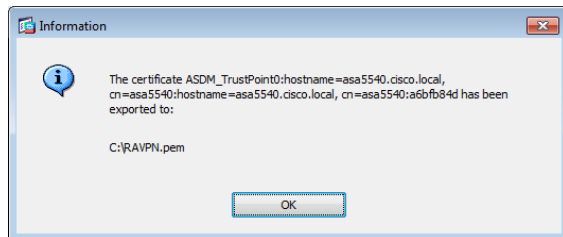


**Step 5:** In the **Export certificate** dialog box, enter a file name for the certificate. (Example: C:\RAVPN.pem)

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



The Information dialog box shows the certificate has been exported.



**Step 7:** Click OK, and then click Apply.

## 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

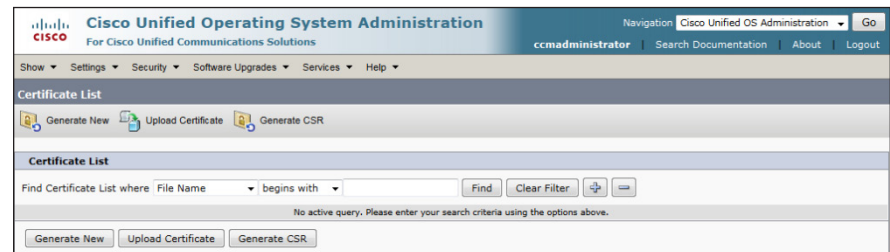
## Procedure 1

## Import Cisco ASA Certificate

**Step 1:** Navigate to the Cisco Unified Operating Systems Administration page. (Example: <https://cucm.cisco.local/cmplatform/>)



**Step 2:** In Security > Certificate Management, click Upload Certificate.



**Step 3:** On the Upload Certificate page, for the Certificate Name, choose Phone-VPN-trust.

**Step 4:** In the Upload File box, enter the certificate file name from 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: In Advanced Features > VPN > VPN Gateway, click Add New.

Step 3: On the VPN Gateway Configuration page, enter a name for the VPN Gateway. (Example: RAVPN-ASA5520-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://172.16.130.124/AnyConnect/)

Step 5: In the **VPN Gateway Certificates** pane, move the certificate from the truststore to the location by selecting it and 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://172.17.130.124/AnyConnect/)

### Procedure 3 Configure the VPN Group

**Step 1:** In Advanced Features > VPN > VPN Group, 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 Available VPN Gateway list to the Selected VPN Gateway 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 Available VPN Gateway list to the Selected VPN Gateway list by selecting the gateway and then clicking the down arrow.

**Step 5:** Click Save.

### Procedure 4 Configure the VPN Profile

**Step 1:** In Advanced Features > VPN > VPN Profile, 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 has a navigation bar at the top with 'Cisco Unified CM Administration' and 'CCMAdministrator'. Below the navigation bar, there are tabs for 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'VPN Profile Configuration' tab is selected. The page contains several sections: 'Status' (Ready), 'VPN Profile Information' (Name: RAVPN-ASAs, Description: , Enable Auto Network Detect: ), 'Tunnel Parameters' (MTU: 1290, Fail to Connect: 30, Enable Host ID Check: ), and 'Client Authentication' (Client Authentication Method: User and Password, Enable Password Persistence: ). At the bottom, there are buttons for 'Save', 'Delete', 'Copy', and 'Add New'.

## Procedure 5

## Configure the VPN Feature

**Step 1:** In **Advanced > VPN**, 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 the Cisco Unified CM Administration interface. The page has a navigation bar at the top with 'Cisco Unified CM Administration' and 'CCMAdministrator'. Below the navigation bar, there are tabs for 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'VPN Feature Configuration' tab is selected. The page contains several sections: 'Status' (Ready), 'VPN Parameters' (a table of parameters), and buttons for 'Save' and 'Set to Default'. The 'VPN Parameters' table lists parameters such as 'Enable Auto Network Detect', 'MTU', 'Keep Alive', 'Fail to Connect', 'Client Authentication Method', 'Enable Password Persistence', and 'Enable Host ID Check'. The 'Enable Host ID Check' parameter is set to 'False'. At the bottom, there are buttons for 'Save' and 'Set to Default'.

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

## Procedure 6 Configure a Common Phone Profile

**Step 1:** In **Device > Device Settings > Common Phone Profile**, click **Add New**.

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

**Step 3:** In the VPN information pane, choose the **VPN Group** created in Procedure 3. (Example: RA-VPN)

**Step 4:** In the **VPN Information** pane, choose the **VPN Profile** created 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 the 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.

The following procedures 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:** In **System > Region**, click **Add New**.

**Step 2:** Enter a name for the region, and then click **Save**. (Example: Teleworkers)

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

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

**Step 5:** In the **Link Loss Type** list choose **Lossy**, and then click **Save**.

The screenshot shows the 'Region Configuration' page in the Cisco Unified CM Administration console. The 'Status' section indicates a successful update. The 'Region Information' section shows the 'Name' as 'Teleworkers'. The 'Region Relationships' section shows a table with columns: Region, Max Audio Bit Rate, Max Video Call Bit Rate (Includes Audio), and Link Loss Type. The 'Modify Relationship to other Regions' section shows a table with columns: Regions, Max Audio Bit Rate, Max Video Call Bit Rate (Includes Audio), and Link Loss Type. The 'Link Loss Type' is set to 'Lossy'.

**Step 6:** In **System > Device Pool**, 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: CG\_1)

**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 created in Step 2, and then click **Save**. (Example: Teleworkers)

The screenshot shows the 'Device Pool Configuration' page in the Cisco Unified CM Administration console. The 'Status' section indicates the device pool is 'Ready'. The 'Device Pool Information' section shows the 'Device Pool' as 'New'. The 'Device Pool Settings' section shows the 'Device Pool Name' as 'Teleworker\_DP', 'Cisco Unified Communications Manager Group' as 'CG\_1', 'Calling Search Space for Auto-registration' as '< None >', 'Adjacent CSS' as '< None >', 'Reverted Call Focus Priority' as 'Default', 'Local Route Group' as '< None >', and 'Intercompany Media Services Enrolled Group' as '< None >'. The 'Roaming Sensitive Settings' section shows the 'Date/Time Group' as 'Pacific' and the 'Region' as 'Teleworkers'.

## Procedure 2

## Register and Configure the Device

**Step 1:** In **Device > Phone**, enter the name of the device in the search text box.

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

**Step 3:** To open the Phone Configuration page, in the **Device Name** column, click the name of the device.

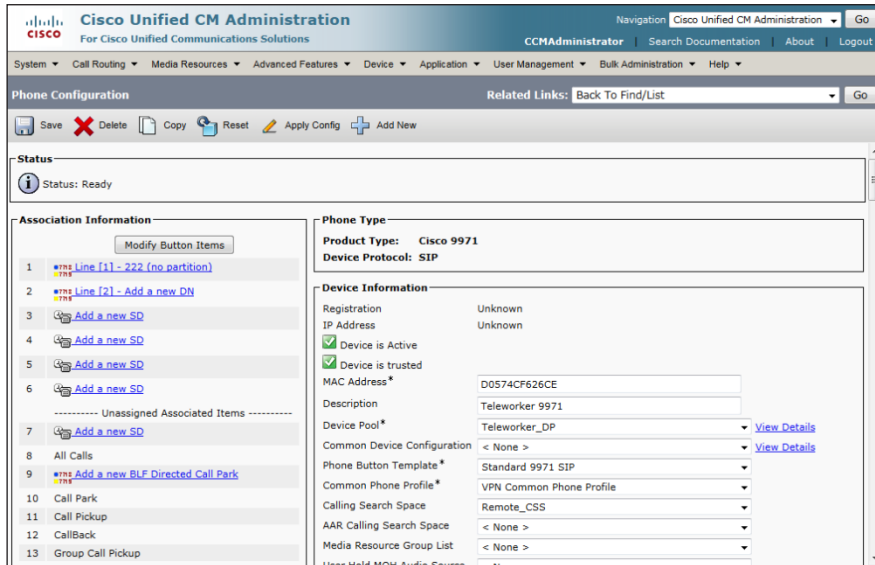
The screenshot shows the 'Find and List Phones' page in the Cisco Unified CM Administration console. The 'Status' section indicates 1 record was found. The 'Phone (1 - 1 of 1)' section shows a table with columns: Device Name, Description, Device Pool, Device Protocol, Status, IP Address, Copy, and Super Copy. The search results show a phone with the name 'SEP0574CF626CE', Description 'Teleworker 9971', Device Pool 'Teleworker\_DP', Device Protocol 'SIP', Status 'Unknown', and IP Address 'Unknown'.

**Step 4:** On the Phone Configuration page, choose the **Device Pool** created in Procedure 1 Step 6. (Example: Teleworker\_DP)

**Step 5:** Choose the **Common Phone Profile** created in Procedure 6. (Example: VPN Common Phone Profile)

**Step 6:** Choose the **Calling Search Space**, and then click **Save**. (Example: Remote\_CSS)

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



### Procedure 3 Connect the IP Phone

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

**Step 2:** To connect the phone to the organization over VPN, select **Applications > VPN**.



**Step 3:** For **VPN Enabled**, select **On**.

**Step 4:** Enter the user ID and password.

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



# Cisco ASA 5505

## Business Overview

Many organizations face increasing need to offer a telecommuter solution to their employees. Employees perceive that commuting and water-cooler chatter are time they spend at work, and renting or buying office space and fixtures and even deploying network infrastructure to host the work force adds up to a substantial sum of capital and operating expense.

Providing an office-like work environment at the teleworker's home requires:

- A phone that is accessible as an extension on the organization's phone system.
- An unobtrusive, quiet, low-power solution to provide multiple Ethernet connections for one or more IP phones or other desktop collaboration resources.
- One or more Ethernet connections for computers that will access the organization's network, as well as Ethernet connectivity for other network-connected devices, such as printers and IP video surveillance equipment.

Employees don't need wireless connectivity at the telework site because all of the telework resources connect with wired Ethernet.

## Technology Overview

Cisco ASA 5505 offers a low-cost option to provide teleworker connectivity to the organization's headquarters (HQ). Cisco ASA 5505 provides secure connectivity for data and collaboration end points in a compact, fanless form factor, minimizing noise and space requirements.

The Cisco ASA 5505 teleworker solution integrates with the Internet Edge portion of the Cisco SBA Midsize or Enterprise design. The teleworker's connection terminates at resilient Cisco ASA firewalls at the HQ or a secondary location, such as a regional office or business-continuation site. Some of the configuration re-uses portions of the Remote Access Virtual Private

Network (RAVPN) configuration, although it may be configured to be completely independent of the RAVPN resources. Addition of the head-end's support for Cisco ASA 5505 teleworker termination does not affect RAVPN connectivity, and the configuration can be applied without the imposition of a service outage.

The Cisco ASA 5505 teleworker solution provides access for endpoint devices such as laptop and desktop computers, IP phones, printers, and other devices that connect to the network via wired Ethernet connections. Two of the Cisco ASA 5505's ports provide Power over Ethernet to support IP Phones, IP Video Surveillance, and other endpoints without cluttering the teleworker's office with additional cables and "wall wart" power supplies.

The ASA 5505 teleworker solution offers:

- **Low cost**—The combination of a Cisco ASA 5505, a Cisco IP Phone, and the necessary license on the HQ Internet Edge ASAs.
- **Flexible connectivity**—The Cisco ASA 5505's integrated Ethernet switch can accommodate multiple endpoint devices, including two interfaces that can provide PoE.
- **Simple deployment**—The Cisco ASA 5505 can be configured quickly with a brief text-file configuration.
- **Security**—Deactivation of the teleworker site's credentials on the HQ appliance can terminate the teleworker's connectivity.

Ideally, the Cisco ASA 5505 teleworker device will be preconfigured and then sent home with the teleworker user. A newly-provisioned or existing desktop IP phone can be taken home, as well, and will register to the Call Manager server over the VPN.

## Deployment Details

Configuration of remote-access connectivity consists of two phases. In the first phase, you'll configure the resilient Internet Edge appliance pair at the HQ site to receive VPN connections from teleworkers' 5505 appliances. In the second phase, you'll deploy configuration on the teleworkers' 5505 hardware clients.

## Process

### Configuring Internet Edge ASA for Teleworker VPN

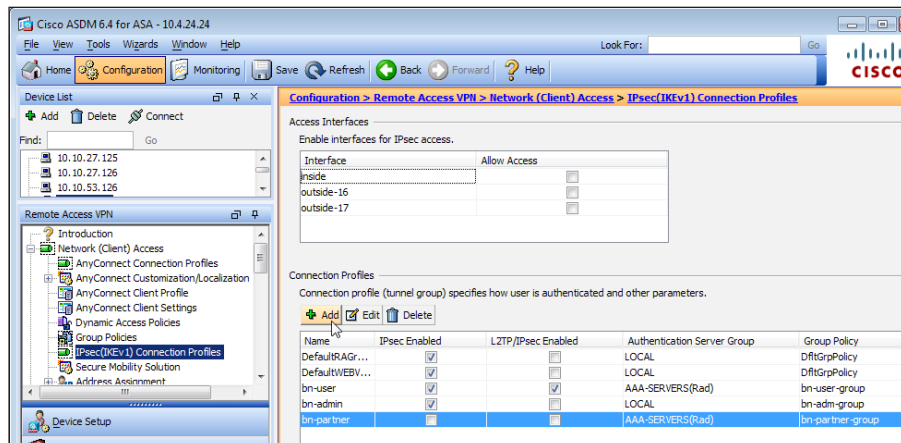
1. Configure IPsec(IKEv1) Connection Profile
2. Configure NAT Exemption
3. Configure Route Advertisement

As a rule, the HQ Internet Edge Cisco ASA configuration for Cisco ASA 5505 Teleworker VPN is self-contained. A few aspects rely on configuration from the Internet Edge Foundation, so you need to have followed the configuration steps for Cisco ASA-based Remote Access VPN in the *SBA for Enterprise Organizations—Borderless Networks Internet Edge Foundation Deployment Guide*.

## Procedure 1 Configure IPsec(IKEv1) Connection Profile

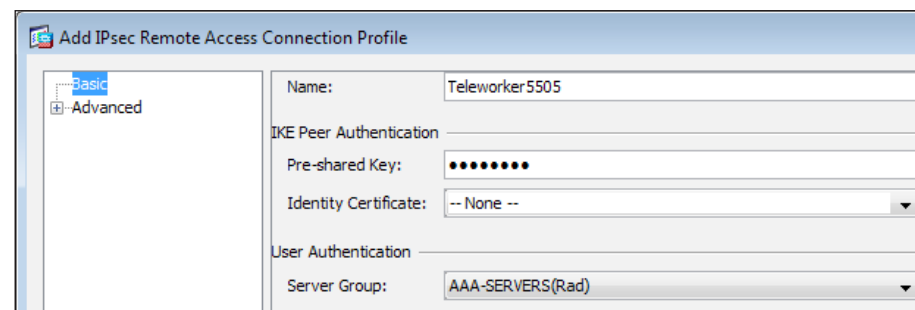
The IPsec Connection Profile carries the bulk of the configuration that sets the behavior for VPN client connections, so you must apply a number of steps in this procedure to complete the central configuration.

**Step 1:** Navigate to the **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1)Connection Profiles** tab, and in the right panel under **Connection Profiles**, click the **Add** button.

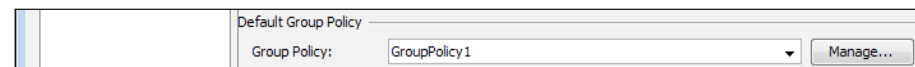


**Step 2:** In the **Add IPsec Remote Access Connection Profile** dialog box, enter the following details. This configuration affects the behavior of the 5505 teleworker device, as described:

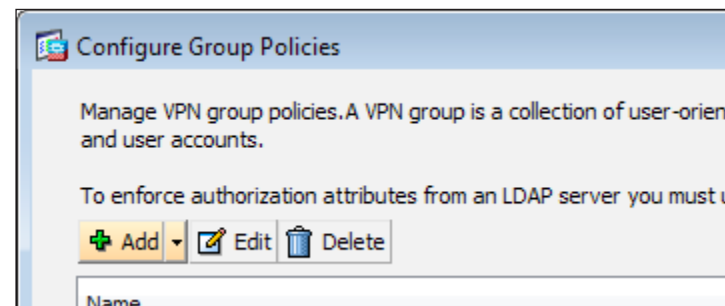
- Name—**Teleworker5505**  
This entry is the name of the VPN group that will be reflected in the 5505 Easy VPN Client configuration.
- IKE Peer Authentication Pre-Shared Key—**[IKE Group Key]**  
This entry is the group key that must be duplicated in the 5505 Easy VPN Client configuration.
- Server Group—Select **AAA-RADIUS**  
This entry selects the RADIUS server that authenticates user names and passwords that are presented to open the Easy VPN Client tunnel.



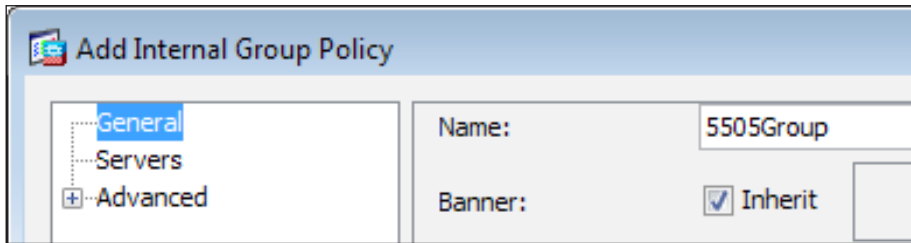
**Step 3:** On the right side of the Group Policy list, click **Manage**.



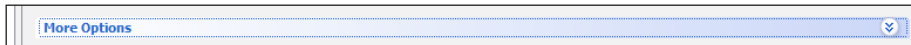
**Step 4:** In the **Configure Group Policies** dialog box, click **Add**.



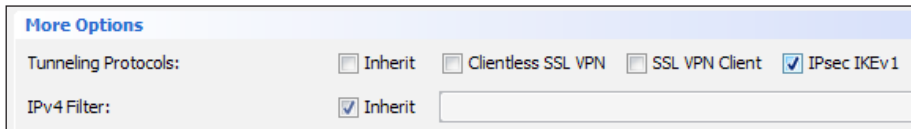
**Step 5:** In the **Add Internal Group Policy** dialog box, select **General**, and then in the Name box, enter **5505Group**.



**Step 6:** To expand the options panel, click **More Options**.

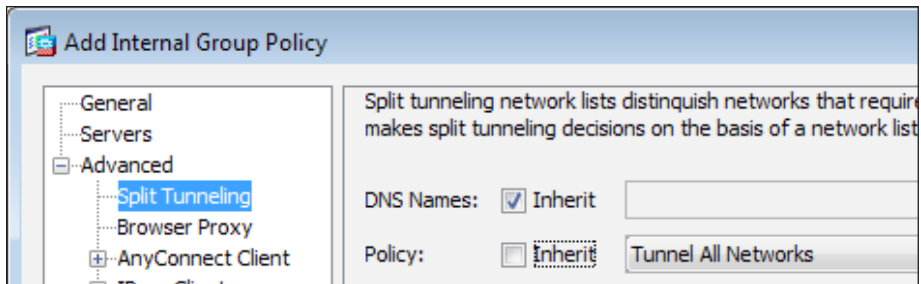


**Step 7:** Next to **Tunneling Protocols**, clear **Inherit**, and then select **IPsec IKEv1**.

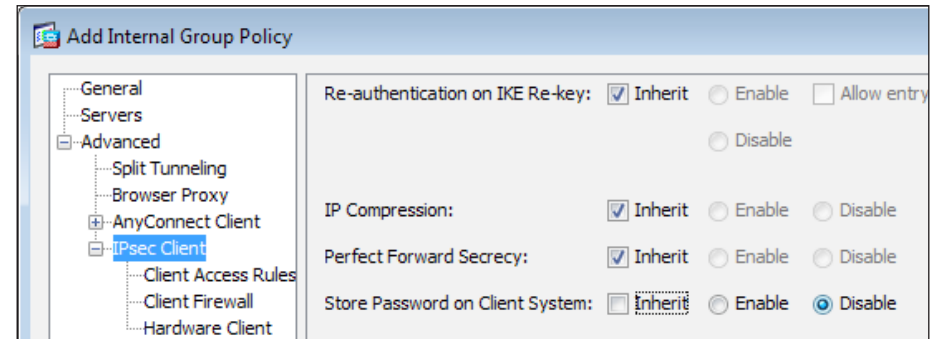


**Step 8:** Navigate to **Advanced > Split Tunneling**, and in the right panel, next to **Policy**, clear **Inherit**.

**Step 9:** In the **Policy** box, ensure that **Tunnel All Networks** is selected.

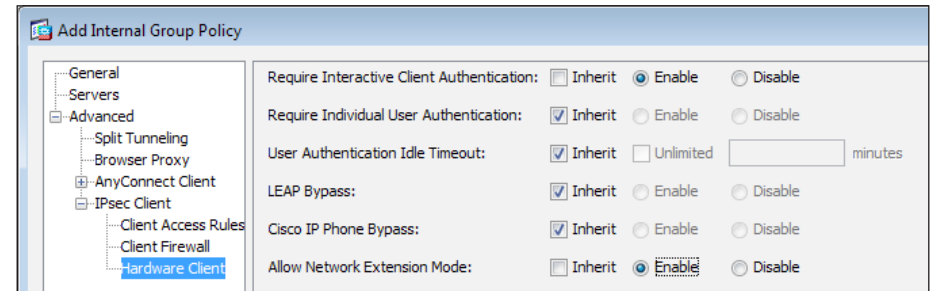


**Step 10:** Navigate to **Advanced > IPsec Client**, and next to **Store Password on Client System**, clear **Inherit**. Ensure that **Disable** is selected.



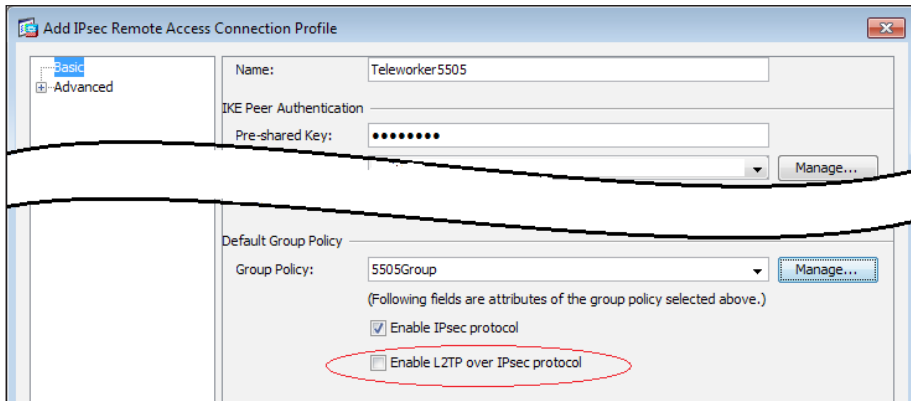
**Step 11:** Navigate to **Advanced > IPsec Client > Hardware Client**, and do the following:

- Next to **Require Interactive Client Authentication**, clear **Inherit**, and ensure that **Enable** is selected.
- Next to **Allow Network Extension Mode**, clear **Inherit**, and ensure that **Enable** is selected.
- Click **OK**.

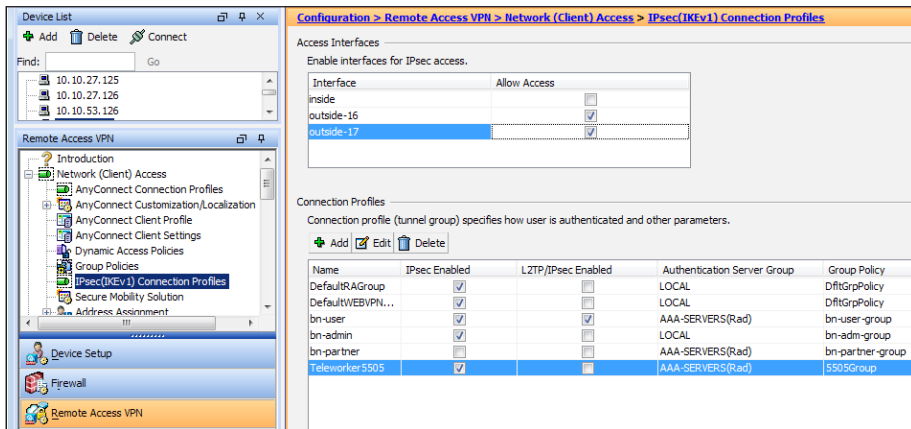


**Step 12:** In the **Configure Group Policies** dialog box, click **OK**.

**Step 13:** In the Add IPsec Remote Access Connection Profile dialog box, clear **Enable L2TP over IPsec protocol**, and then click OK.



**Step 14:** In the Connection Profiles window, navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1)**. Under **Access Interfaces**, next to the appliance's outside interface(s), select **Allow Access**.



**Step 15:** Under **Connection Profiles**, verify that the new Teleworker5505 profile appears, and then click **Apply**.

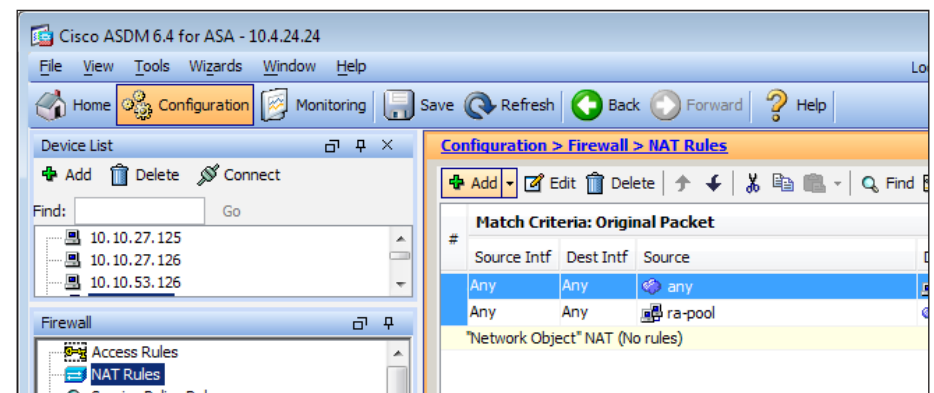
The steps above apply the following configuration:

```
group-policy 5505Group internal
group-policy 5505Group attributes
password-storage disable
vpn-tunnel-protocol ikev1
split-tunnel-policy tunnelall
secure-unit-authentication enable
nem enable
tunnel-group Teleworker5505 type remote-access
tunnel-group Teleworker5505 general-attributes
default-group-policy 5505Group
authentication-server-group AAA-SERVERS (Rad)
tunnel-group Teleworker5505 ipsec-attributes
ikev1 pre-shared-key [cisco123]
```

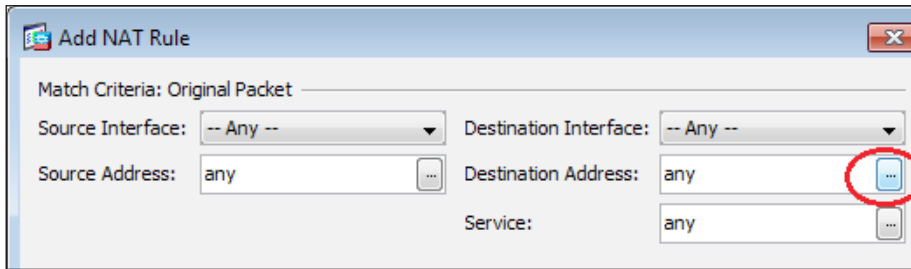
## Procedure 2 Configure NAT Exemption

The Internet Edge appliances must not apply network address translation (NAT) on traffic between the organization's private network and the IP subnet that encompasses teleworkers' remote addresses. You must configure a policy that prevents the Internet Edge appliance from applying NAT.

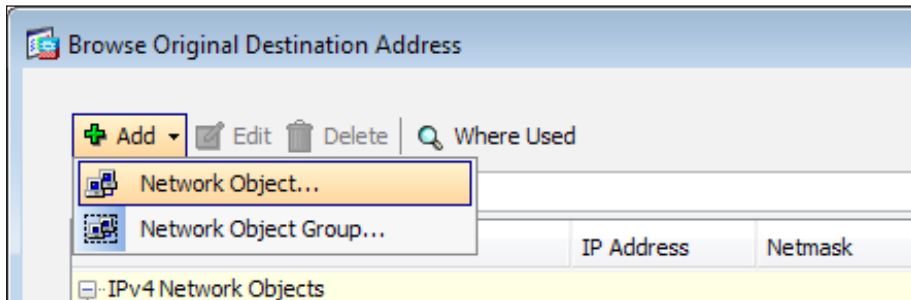
**Step 1:** Navigate to **Configuration > Firewall > NAT Rules**, and then click **Add**.



**Step 2:** In the Add NAT Rule dialog box, under **Match Criteria: Original Packet**, in the **Destination Address** box, click the ellipsis (...).

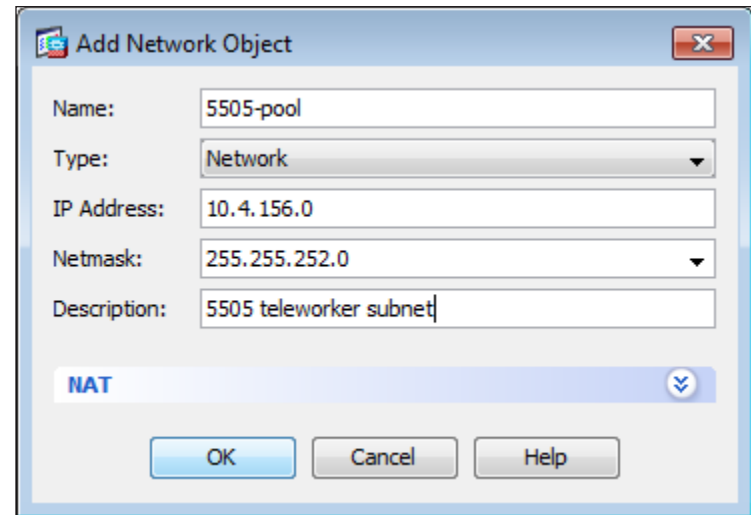


**Step 3:** In the Browse Original Destination Address dialog box, click **Add**, and then click **Network Object**.

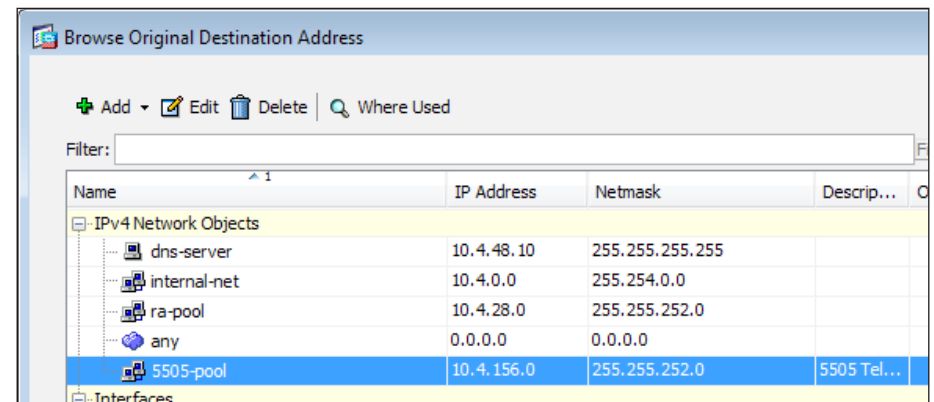


**Step 4:** In the Add Network Object dialog box, enter the following values, and then click **OK**.

- Name—**5505-pool**
- Type—**Network**
- IP Address—**[10.4.156.0]**
- Netmask—**[255.255.252.0]**
- Description—**5505 Teleworker Subnet**



**Step 5:** In the Browse Original Destination Address dialog box, expand the **IPv4 Network Objects** list, double-click **5505-pool**, and then click **OK**. Double-clicking **5505-pool** selects the 5505 teleworker subnet as the original destination address.



**Step 6:** In the Add NAT Rule dialog box, in the **Match Criteria: Original Packet > Destination Address** field, verify that the value is **5505-pool**.

**Step 7:** Under **Options**, ensure that **Enable Rule** is selected and that the indicated direction is **Both**, and then click **OK**.

**Step 8:** Review the configuration, and then click **Apply**.

Source Intf	Dest Intf	Source	Destination	Service
Any	Any	any	ra-pool	any
Any	Any	any	5505-pool	any
Any	Any	5505-pool	any	any

Cisco ASDM applies this configuration:

```
object network 5505-pool
  subnet 10.4.156.0 255.255.252.0
  description 5505 teleworker subnet
  nat (any,any) source static any any destination static 5505-
  pool 5505-pool
```

### Procedure 3

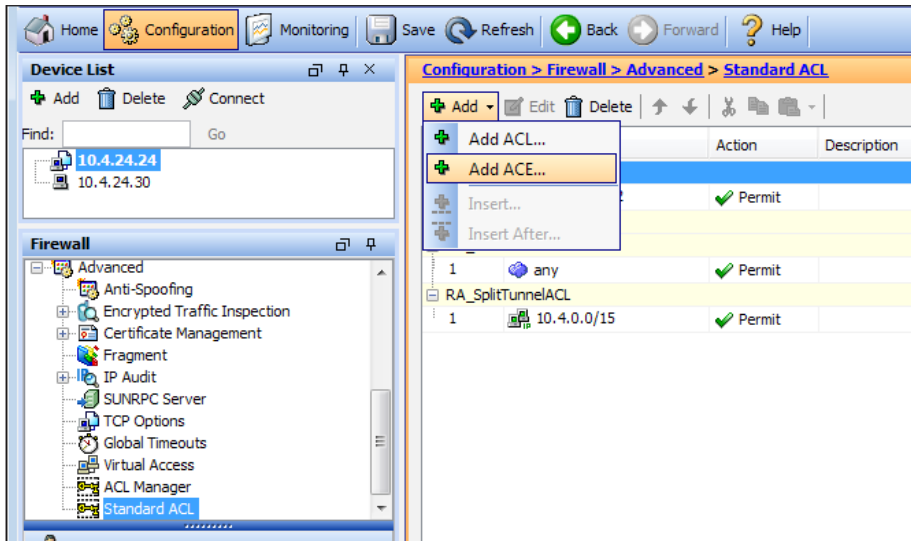
### Configure Route Advertisement

The Internet Edge appliances must advertise the teleworker sites' networks to the HQ LAN. RAVPN address pools are advertised as host routes by reverse route injection (RRI) and summarized on the Internet Edge distribution switch. Teleworker subnets are advertised by RRI, as well, but without summarization; the teleworker subnets remain intact as eight-number (/29) subnets advertised to the rest of the network.

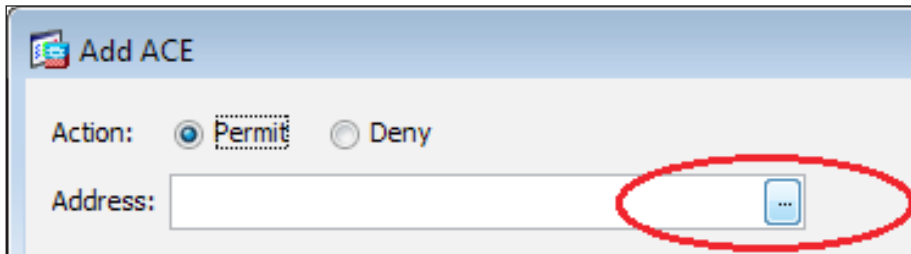
**Step 1:** In the **Configuration > Device Setup > Routing > EIGRP > Redistribution** panel, locate the static routing redistribution configuration, and verify that a route-map is defined in the static route redistribution for Enhanced Interior Gateway Routing Protocol (EIGRP). You may need to scroll the window to the far right (in the figure below, the Route Map column was moved). If no route-map is configured, you should review and apply the RAVPN-pool advertisement steps in the Remote Access VPN Configuration section of the *Internet Edge Deployment Guide*.

EIGRP Process	Protocol	Route Map	Bandwidth	Delay	Reliability
100	Static	redistribute...			

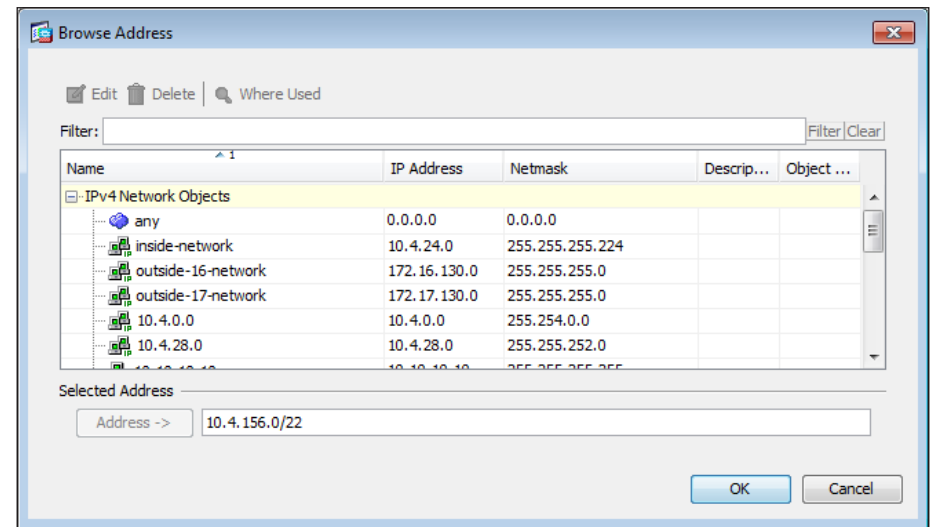
**Step 2:** Navigate to **Configuration > Firewall > Advanced > Standard ACL** and add the 5505 teleworker's subnet to the route-map's access-list by selecting the **redistribute-list** entry in the ACL list, clicking **Add**, and clicking **Add ACE**.



**Step 3:** In the Add ACE window, next to the Address box, click the ellipsis (...).

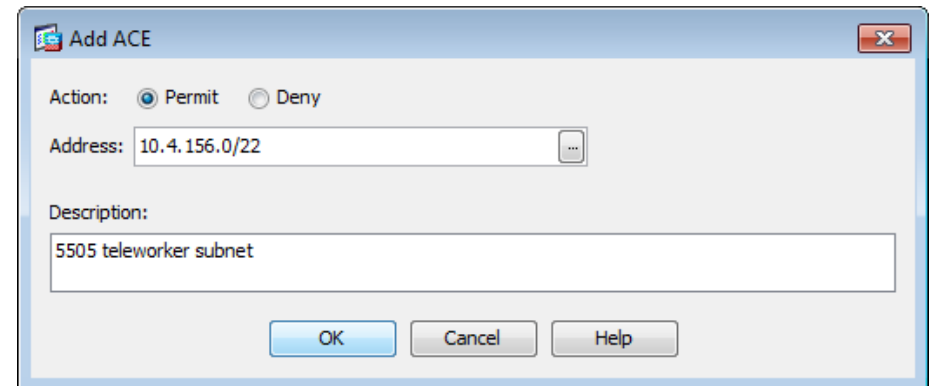


**Step 4:** In the Browse Address window, in the Address box, type **10.4.156.0/22** and click **OK**.

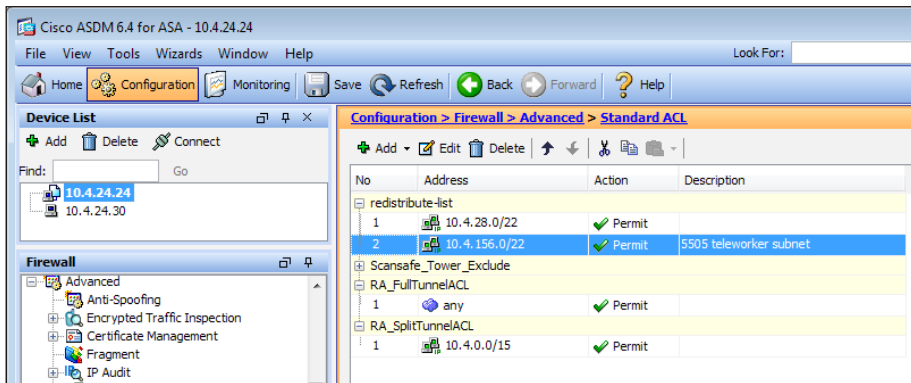


**Step 5:** Verify that **Permit** is selected and that **10.4.156.0/22** is the value for Address.

**Step 6:** In Description, enter **5505 teleworker subnet** and click **OK**.



**Step 7:** In the Standard ACL panel, click **Apply**.



ASDM applies this configuration:

```
access-list redistribute-list remark 5505 teleworker subnet
access-list redistribute-list standard permit 10.4.156.0
255.255.252.0
```

## Process

Configuring Teleworker Cisco ASA 5505 Endpoints

1. Define Global Device Configuration
2. Configure Outside VLAN and Switch Port
3. Configure Inside VLAN and Switch Ports
4. Configure Cisco ASA 5505 DHCP Server
5. Configure Cisco ASA 5505 Easy VPN Client

Each teleworker's Cisco ASA 5505 endpoint must be configured to connect to connect to the resilient Internet Edge appliance deployed at the HQ site. Because this configuration is likely to be deployed on multiple devices, the configuration is shown only in the command-line interface to streamline deployment. All 5505 teleworker sites connect using Network Extension

Mode, which allows teleworker-site endpoints to connect freely to the organization's LAN. Connecting in Network Extension Mode is particularly critical for endpoints such as IP phones and video surveillance cameras that might be susceptible to NAT's modification of data traffic.

Each site must use a unique inside IP subnet. Otherwise, all configuration is identical between sites. To avoid conflicting address assignments, Cisco recommends that you maintain a spreadsheet of subnet assignments for the various users that will be issued Cisco ASA 5505 telecommuter equipment.

User name	Subnet	ASA 5505 LAN address	Hostname
Employee1	10.4.156.0/29	10.4.156.1	5505site1

## Procedure 1

## Define Global Device Configuration

**Step 1:** Configure the Cisco ASA 5055's hostname and domain name.

```
hostname 5505site1
domain-name cisco.local
```

**Step 2:** Define a local administrative username.

```
username [admin] password [cisco123] privilege 15
```

**Step 3:** Set the enable password.

```
enable password [cisco123]
```

**Step 4:** Define the management configuration.

```
http server enable
http 10.0.0.0 255.0.0.0 inside
ssh 10.0.0.0 255.0.0.0 inside
management-access inside
```

**Step 5:** Define authentication servers for management access.

```
aaa-server AAA-SERVERS protocol tacacs+
aaa-server AAA-SERVERS (inside) host 10.4.48.15
key *****
aaa authentication http console AAA-SERVERS LOCAL
aaa authentication ssh console AAA-SERVERS LOCAL
```

## Procedure 2 Configure Outside VLAN and Switch Port

**Step 1:** Configure a VLAN interface to receive an IP address via DHCP from the teleworker's Internet gateway device.

```
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
```

**Step 2:** Associate the Cisco ASA 5505's Ethernet 0/0 interface with VLAN 2, and instruct the teleworker to connect Ethernet 0/0 to their Internet Gateway Device.

```
interface Ethernet0/0
 switchport access vlan 2
```

## Procedure 3 Configure Inside VLAN and Switch Ports

Each 5505 teleworker site needs a unique inside subnet, which you should track in the spreadsheet recommended in the introduction to this process.

**Step 1:** Configure the VLAN 1 interface for the teleworker site's LAN.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.4.156.1 255.255.255.248
```

**Step 2:** Associate the Cisco ASA 5505's Ethernet 0/1 through Ethernet 0/7 interfaces with VLAN 1, and instruct the teleworker to connect Power over Ethernet (PoE)-enabled devices to the Ethernet 0/6 and 0/7 ports.

```
interface Ethernet0/1
 switchport access vlan 1
...
interface Ethernet0/7
 switchport access vlan 1
```

## Procedure 4 Configure Cisco ASA 5505 DHCP Server

The Cisco ASA 5505 must be configured to provide IP addresses for the teleworker endpoints, such as computers, phones, printers, and video surveillance devices. Each site must use a unique subnet, which should be tracked in the spreadsheet described in the introduction of this process.

**Step 1:** Define the DHCP scope address range. The DHCP scope must be in the same subnet as the inside (VLAN 1) interface.

```
dhcpd address [10.4.156.2-10.4.156.6] inside
```

**Step 2:** Configure the DNS and domain-name values that will be distributed to clients.

```
dhcpd dns 10.4.48.10 interface inside
dhcpd domain cisco.local interface inside
```

**Step 3:** Define DHCP option 150 to provide the Cisco Unified Call Manager Server address for Cisco IP Phones.

```
dhcpd option 150 ip 10.4.48.20
```

**Step 4:** Enable the DHCP scope.

```
dhcpd enable inside
```

## Procedure 5

### Configure Cisco ASA 5505 Easy VPN Client

Cisco ASA 5505 uses Easy VPN network-extension mode to negotiate the VPN connectivity to the HQ site's Cisco ASA Remote Access server.

**Step 1:** Apply the Easy VPN client configuration for the remote Cisco ASA 5505: The vpngrp and password values must match the IPsec Remote Access Connection Profile that you configured on the HQ appliance.

```
vpnclient server 172.16.130.122
```

**Step 2:** Set network-extension mode:

```
vpnclient mode network-extension-mode
```

**Step 3:** Define the Easy VPN client connection attributes. The vpngrp and password values must match the IPsec Remote Access Connection Profile that you configured on the HQ appliance.

```
vpnclient vpngrp Teleworker5505 password [cisco123]
```

**Step 4:** Enable the Cisco ASA 5505's Easy VPN client:

```
vpnclient enable
```

The teleworker must manually initiate their VPN connection; when the user employs a web browser to access web content on the HQ's network, Cisco ASA 5505 intercepts the connection and provides an interactive login prompt. The user must provide login credentials, at which point the VPN connection is negotiated with the provided username and password.



#### Tech Tip

The IP Phone connected to the Cisco ASA 5505 can't place or receive calls if the user's VPN connection is not active.

In the event that a teleworker's VPN access must be revoked, the authentication server should deny the teleworker's access.

## Notes

# Cisco OfficeExtend

## 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 sitting in a cubicle or office in the organization's facility. However, residential and urban environments tend to have many potential sources of congestion found on the commonly used 2.4-GHz wireless band. Potential sources of interference include cordless handsets, personal home laptops, iPhones or iPods, baby monitors, and many more. Additionally, solutions must support a wide range of teleworking employees with varying skill sets, making it critical to have a streamlined and simplified way to implement devices that allow for access to the corporate environment.

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

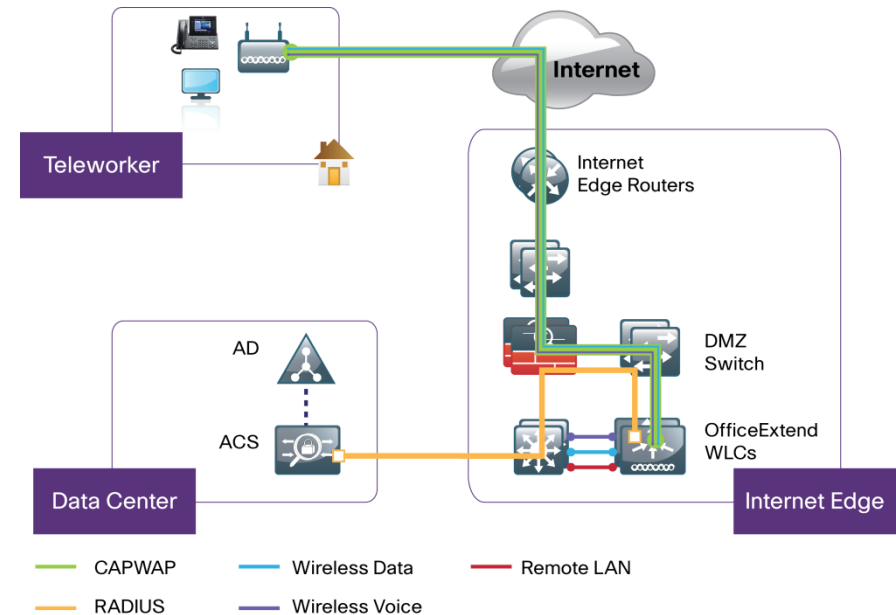
The Cisco OfficeExtend solution is specifically designed for the teleworker that primarily uses wireless devices; the solution consists of the following components:

- Cisco Aironet 600 Series OfficeExtend Access Point
- Cisco 5500 Series Wireless LAN Controller

The Cisco OfficeExtend solution configuration, management, and troubleshooting are centrally managed at the Cisco Wireless LAN Controller (WLC). Each Cisco 5500 Series Wireless LAN Controller supports up to 500 OfficeExtend Access Points.

This deployment guide uses two Cisco WLCs. The first is the primary WLC, and all of the access points will be configured to register to it. The second WLC provides resiliency in case the primary WLC or Internet connection fails. Under normal operation no Cisco 600 Series OfficeExtend access points are registered to the resilient WLC. Cisco recommends connecting devices that are exposed to the Internet in a DMZ.

Figure 1 - Cisco OfficeExtend architecture



To allow users to connect their endpoint devices to either the organization's on-site wireless network or their at-home teleworking wireless networks without reconfiguration, the Cisco OfficeExtend teleworking solution offers the same wireless Service Set Identifiers (SSIDs) at teleworkers' homes as those that support data and voice inside the organization.

Cisco OfficeExtend delivers full 802.11n wireless performance and avoids congestion caused by residential devices because it operates simultaneously in the 2.4-GHz and the 5-GHz radio frequency bands. The OfficeExtend solution uses the same quality of service (QoS) and security policy as the network core, so there is no overlay network to manage.

For the initial setup at a home office, the remote worker plugs the access point into the home router that is connected to or integrated with the worker's broadband modem. The Cisco Aironet 600 Series OfficeExtend Access Point can be provisioned in advance or by the user and will set up a secure tunnel to the Cisco wireless controller at the corporate HQ.

The OfficeExtend Access Point uses a centralized architecture built on control and provisioning using CAPWAP, an industry standard, to provide a secure, high-performance Datagram Transport Layer Security (DTLS) connection between the access point and the controller in the corporate network. This connection allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

## Deployment Details

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the solution. These parameters are listed in the following table.

*Table 3 - Universal design parameters*

Network service	IP address
Domain name	cisco.local
Active Directory, DNS Server, DHCP Server	10.4.48.10
Authentication Control System (ACS)	10.4.48.15
Network Time Protocol (NTP) Server	10.4.48.17

## Process

### Configuring the Internet Edge

1. Configure the Firewall DMZ Interface
2. Configure NAT
3. Configure Security Policy
4. Configure the DMZ Switch

## Procedure 1

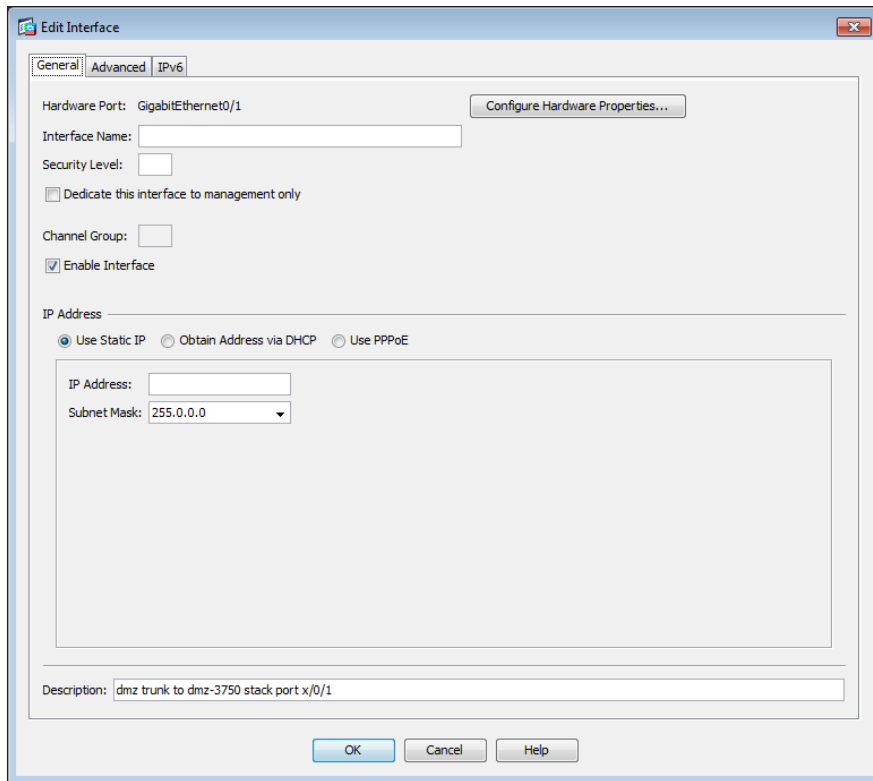
### Configure the Firewall DMZ Interface

The firewall DMZ is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The various DMZ networks are connected to Cisco ASA on the appliance's GigabitEthernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

**Step 1:** In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch (example: GigabitEthernet0/1), and then click **Edit**.

**Step 2:** Select **Enable Interface**, and then click **OK**.



**Step 3:** In the **Interface** pane, click **Add > Interface**.

**Step 4:** In the **Hardware Port** list, choose the interface that you configured in Step 1. (Example: GigabitEthernet0/1)

**Step 5:** In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

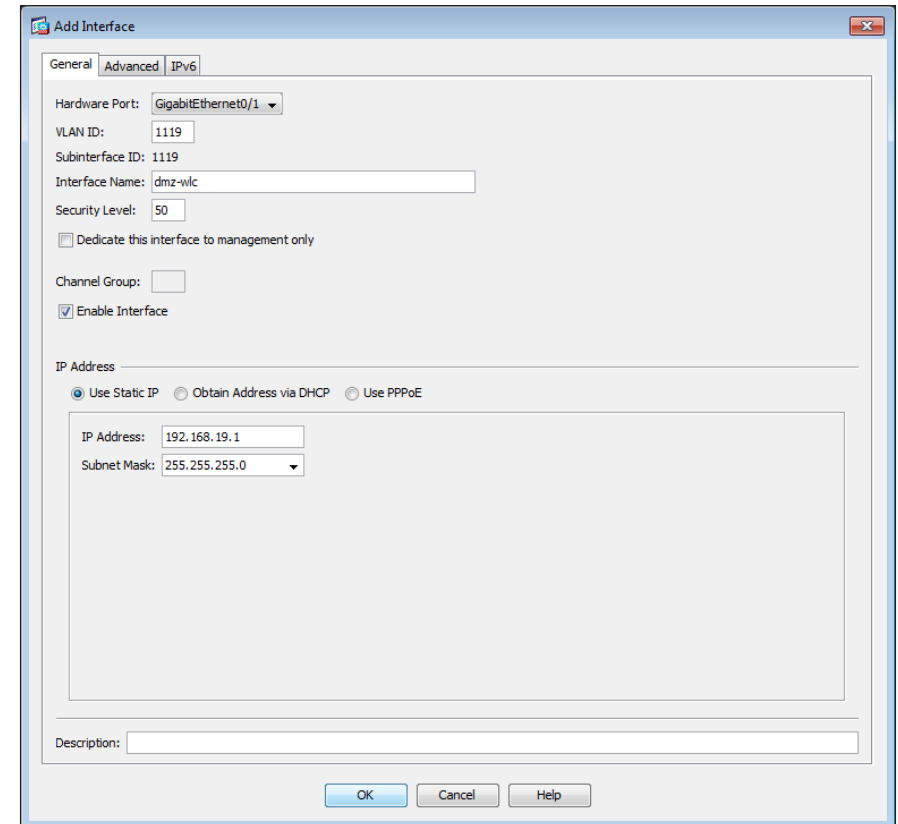
**Step 6:** In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

**Step 7:** Enter an **Interface Name**. (Example: dmz-wlc)

**Step 8:** In the **Security Level** box, enter a value of 50.

**Step 9:** Enter the interface **IP Address**. (Example: 192.168.19.1)

**Step 10:** Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)



## Procedure 2

## Configure NAT

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of the WLC to an outside public address. For resiliency, the primary and resilient WLCs are translated to separate ISPs. The example DMZ address to public IP address mapping is shown in the following table.

WLC DMZ address	WLC public address (externally routable after NAT)
192.168.19.20	172.16.130.20 (ISP-A)
192.168.19.21	172.17.130.20 (ISP-B)

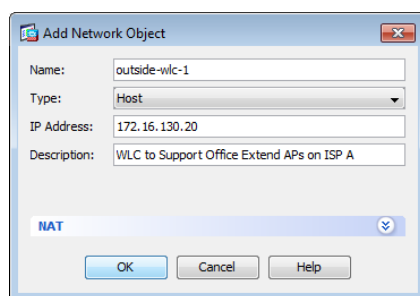
**Step 1:** Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

First, add a network object for the public address of the WLC

**Step 2:** Click **Add > Network Object**.

**Step 3:** On the Add Network Object dialog box, in the **Name** box, enter a description for the primary WLC's public IP address. (Example: outside-wlc-1)

**Step 4:** In the **IP Address** box, enter the primary WLC's public IP address, and then click **OK**. (Example: 172.16.130.20)



Next, you add a network object for the private DMZ address of the WLC.

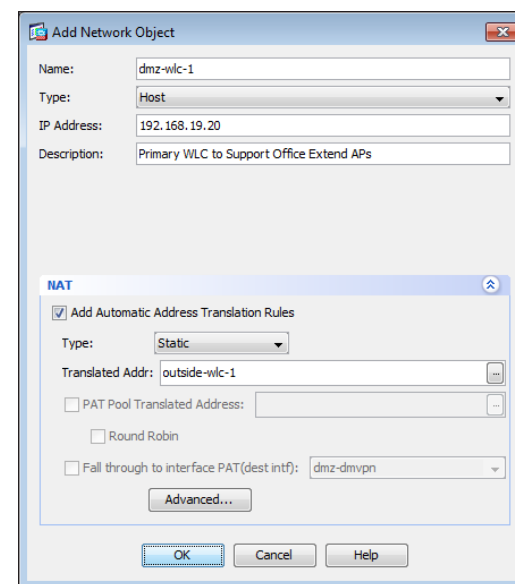
**Step 5:** In the **Add Network Object** dialog box, in the **Name** box, enter a description for the primary WLC's private DMZ IP address. (Example: dmz-wlc-1)

**Step 6:** In the **IP Address** box, enter the primary WLC's private DMZ IP address. (Example: 192.168.19.20)

**Step 7:** Click the two down arrows. The NAT pane expands.

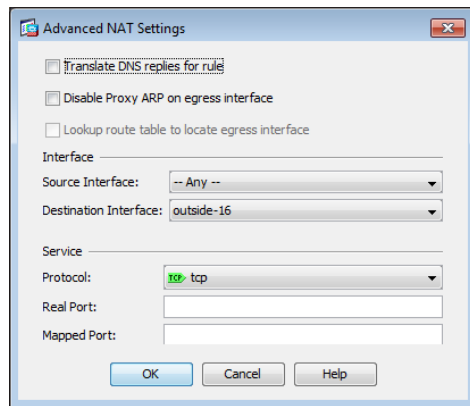
**Step 8:** Select **Add Automatic Address Translation Rules**.

**Step 9:** In the **Translated Addr** list, choose the network object created in Step 2.



**Step 10:** Click **Advanced**.

**Step 11:** In the **Destination Interface** list choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



**Step 12:** Repeat Step 1 through Step 11 through for the resilient Wireless LAN Controller.

**Step 13:** To ease the configuration of the security policy by creating a network object group that contains the private DMZ address of every Wireless LAN Controller in the DMZ, click **Add > Network Object Group**.

**Step 14:** In the **Add Network Object Group** dialog box, enter a name for the group in the **Group Name** box. (Example: dmz-wlcs)

**Step 15:** Choose the primary WLC from the **Existing Network Objects/Groups** pane, and then click **Add >>**.

**Step 16:** Choose the resilient WLC from the **Existing Network Objects/Groups** pane, click **Add >>**, and then click **OK**.

Next, you will insert a new rule above the rule you selected that enables the WLCs in the DMZ to communicate with the AAA server in the data center for management and user authentication.

**Step 3:** Click **Add > Insert**.

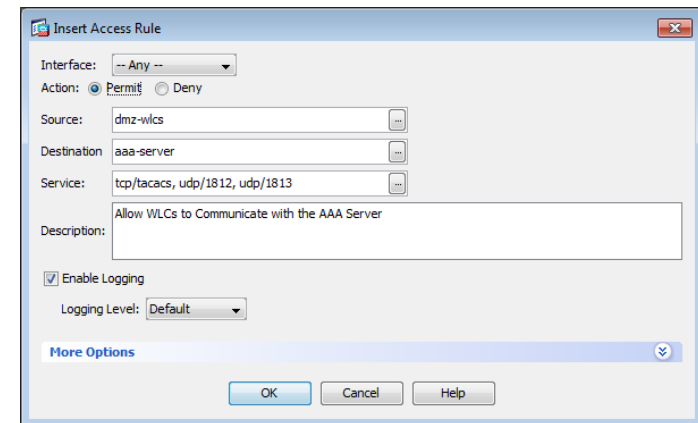
**Step 4:** In the **Internet Access Rule** dialog box, in the **Interface** list, select **—Any—**.

**Step 5:** For **Action**, select **Permit**.

**Step 6:** In the **Source** list, choose the network object group created in Procedure 2, Step 14. (Example: dmz-wlcs)

**Step 7:** In the **Destination** list, choose the network object for the AAA Server. (Example: aaa-server)

**Step 8:** In the **Service** list, enter **tcp/tacacs, udp/1812, udp/1813**, and then click **OK**.



Next, you must enable the WLCs in the DMZ to synchronize their time with the NTP server in the data center.

**Step 9:** Click **Add > Insert**.

**Step 10:** In the **Internet Access Rule** dialog box, in the **Interface** list, select **—Any—**.

**Step 11:** For **Action**, select **Permit**.

### Procedure 3 Configure Security Policy

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**.

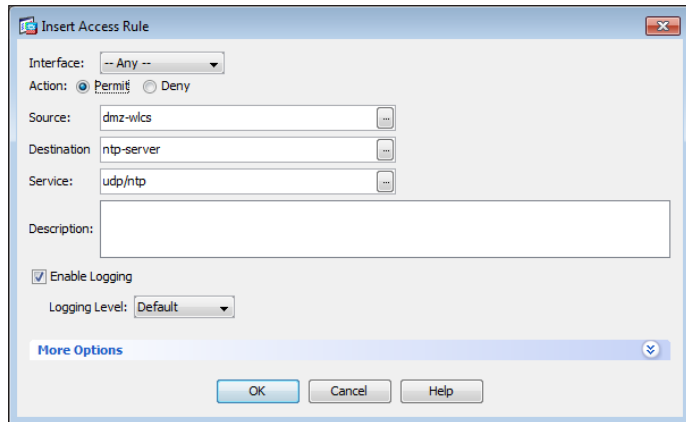
**Step 2:** Click the rule that denies traffic from the DMZ toward other networks.



**Step 12:** In the **Source** list, choose the network object group created in Procedure 2, Step 14. (Example: dmz-wlcs)

**Step 13:** In the **Destination** list, choose the network object for the NTP Server. (Example: ntp-server)

**Step 14:** In the **Service** list, enter **udp/ntp**, and then click **OK**.



Next, you enable the WLCs in the DMZ to be able to download new software via FTP.

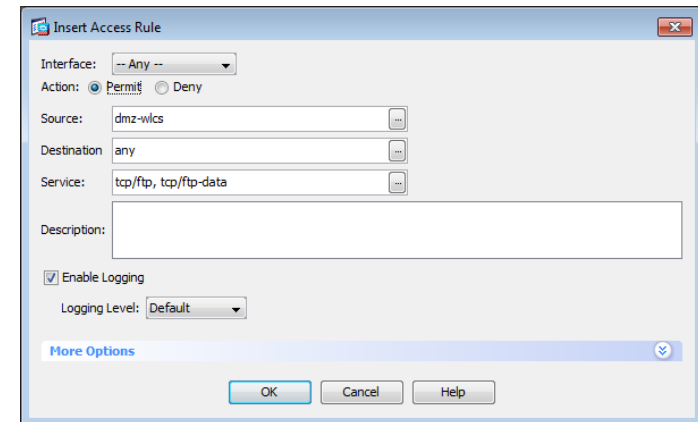
**Step 15:** Click **Add > Insert**.

**Step 16:** In the **Internet Access Rule** dialog box, in the **Interface** list, select **—Any—**.

**Step 17:** For **Action**, select **Permit**.

**Step 18:** In the **Source** list, choose the network object group created in Procedure 2, Step 14. (Example: dmz-wlcs)

**Step 19:** In the **Service** list, enter **tcp/ftp, tcp/ftp-data**, and then click **OK**.



Now you enable the 600 Series OfficeExtend Access Points to communicate with the WLCs in the DMZ using CAPWAP.

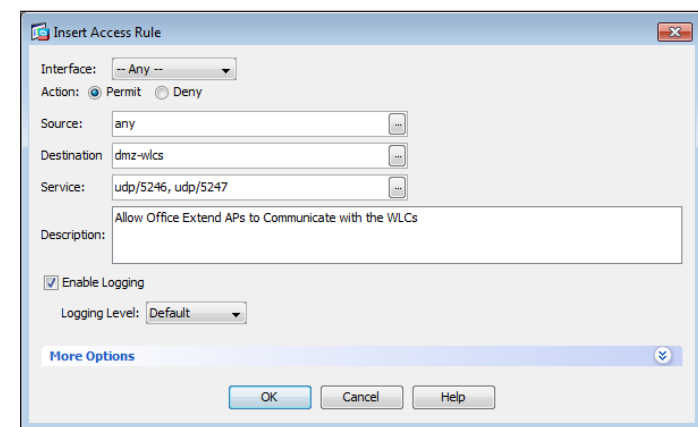
**Step 20:** Click **Add > Insert**.

**Step 21:** In the **Internet Access Rule** dialog box, in the **Interface** list, select **—Any—**.

**Step 22:** For **Action**, select **Permit**.

**Step 23:** In the **Destination** list, choose the network object group created in Procedure 2, Step 14. (Example: dmz-wlcs)

**Step 24:** In the **Service** list, enter **udp/5246, udp/5247**, and then click **OK**.



**Step 25:** Click **Apply**.

## Procedure 4 Configure the DMZ Switch

**Step 1:** Set the DMZ switch to be the spanning tree root for the VLAN that contains the WLCs.

```
vlan 1119
spanning-tree vlan 1119 root primary
```

**Step 2:** Configure the interfaces that are connected to the appliances as a trunk.

```
interface GigabitEthernet1/0/24
description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1119
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

**Step 3:** Configure the interfaces that are connected to the primary and resilient WLCs' management port.

```
interface GigabitEthernet1/0/5
description OEAP WLC-1 Management Port
!
interface GigabitEthernet2/0/5
description OEAP WLC-2 Management Port
!
interface range GigabitEthernet1/0/5, GigabitEthernet2/0/5
switchport access vlan 1119
switchport host
macro apply EgressQoS
logging event link-status
no shutdown
```

## Process

Configuring the Cisco ACS

1. Create the Wireless Device Type Group
2. Create the TACACS+ Shell Profile
3. Modify the Device Admin Access Policy
4. Modify the Network Access Policy
5. Create the Network Device

This guide assumes that Cisco ACS has already been configured. Only the procedures required to support the integration of wireless into the deployment are included. Full details on Cisco ACS configuration are included in the *Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations Network Device Authentication and Authorization Deployment Guide*.

## Procedure 1 Create the Wireless Device Type Group

**Step 1:** In **Network Resources > Network Device Groups > Device Type**, click **Create**.

**Step 2:** In the **Name** box, enter a name for the group. (Example: WLC)

**Step 3:** In the **Parent** box, select **All Device Types:All Devices**, and then click **Submit**.

The screenshot shows the 'Network Resources > Network Device Groups > Device Type > Create' page. It contains a form titled 'Device Group - General' with the following fields:

- Name:** A text box containing 'WLC'.
- Description:** An empty text box.
- Parent:** A dropdown menu showing 'All Device Types:All Devices' with a 'Select' button next to it.

Below the form, there is a legend indicating that orange asterisks (\*) denote required fields. At the bottom of the form are 'Submit' and 'Cancel' buttons.

## Procedure 2 Create the TACACS+ Shell Profile

You must create a shell profile for the WLCs that contains a custom attribute that assigns users full administrative rights when they log on to the WLC.

**Step 1:** In **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, click **Create**.

**Step 2:** In the **Name** box, enter a name for the wireless shell profile.  
(Example: WLC Shell)

**Step 3:** On the **Custom Attributes** tab, in the **Attribute** box, enter **role1**.

**Step 4:** In the **Requirement** list, choose **Mandatory**.

**Step 5:** In the **Value** box, enter **ALL**, click **Add**, and then click **Submit**.

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "WLC Shell"

General Common Tasks Custom Attributes

Common Tasks Attributes

Attribute	Requirement	Value
role1	Mandatory	ALL

Manually Entered

Attribute	Requirement	Value
role1	Mandatory	ALL

Add A Edit V Replace A Delete

Attribute:

Requirement: Mandatory

Value:

\* = Required fields

Submit Cancel

## Procedure 3 Modify the Device Admin Access Policy

First, you must exclude WLCs from the existing authorization rule.

**Step 1:** In **Access Policies > Default Device Admin > Authorization**, click the **Network Admin** rule.

**Step 2:** Select the **NDG:Device Type** condition, and from the filter list, choose **not in**.

**Step 3:** In the box, select **All Device Types:All Devices:WLC**, and then click **OK**.

General

Name: Network Admin Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☒ Identity Group: in All Groups:Network Admins Select

☐ NDG:Location: -ANY-

☒ NDG:Device Type: not in All Device Types:All Devices:WLC Select

☐ Time And Date: -ANY-

Results

Shell Profile: Level 15 Select

OK Cancel Help

Next, create a WLC authorization rule.

**Step 4:** In **Access Policies > Default Device Admin > Authorization**, click **Create**.

**Step 5:** In the **Name** box, enter a name for the rule. (Example: WLC Admin)

**Step 6:** Select the **Identity Group** condition, and in the box, select **Network Admins**.

**Step 7:** Select the **NDG:Device Type** condition and in the box select **All Device Types:All Devices:WLC**

**Step 8:** In the **Shell Profile** box, select **WLC Shell**, and then click **OK**.

**Step 9:** Click **Save Changes**.

The screenshot shows the 'General' tab of a policy rule configuration window. The 'Name' field is set to 'WLC Admin' and the 'Status' is 'Enabled'. A help icon and text explain that the 'Customize' button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules. Under the 'Conditions' section, 'Identity Group' is selected with a value of 'in' and 'All Groups:Network Admins'. 'NDG:Location' is set to '-ANY-'. 'NDG:Device Type' is selected with a value of 'in' and 'All Device Types:All Devices:WLC'. 'Time And Date' is set to '-ANY-'. Under the 'Results' section, 'Shell Profile' is set to 'WLC Shell'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

## Procedure 4

## Modify the Network Access Policy

First you must disable the ACS from accepting the EAP-TLS protocol.

**Step 1:** In **Access Policies**, click **Default Network Access**.

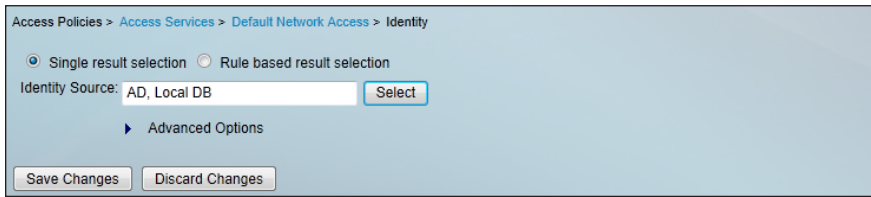
**Step 2:** On the **Allowed Protocols** tab, clear **Allow EAP-TLS**, and then click **Submit**.

The screenshot shows the 'Allowed Protocols' tab of the 'Default Network Access' configuration window. The 'Process Host Lookup' checkbox is checked. Under 'Authentication Protocols', 'Allow PAP/ASCII', 'Allow CHAP', 'Allow MS-CHAPv1', 'Allow MS-CHAPv2', 'Allow EAP-MD5', 'Allow EAP-TLS', 'Allow LEAP', 'Allow PEAP', and 'Allow EAP-FAST' are all checked. The 'Preferred EAP protocol' dropdown is set to 'LEAP'. At the bottom are 'Submit' and 'Cancel' buttons.

Next create an authorization rule to allow the WLCs to authenticate clients using RADIUS.

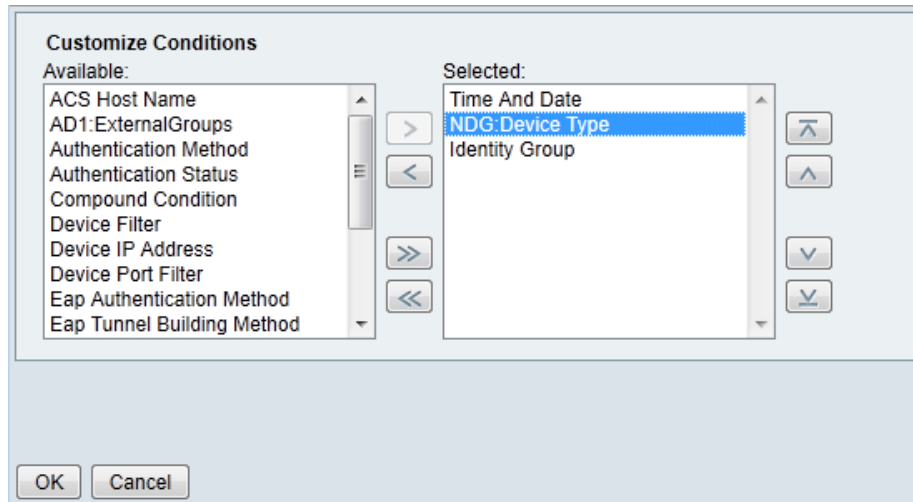
**Step 3:** Navigate to **Access Policies > Default Network Access > Identity**.

**Step 4:** In the **Identity Source** box select **AD, Local DB**, and then click **Save Changes**.



**Step 5:** In **Access Policies > Access Services > Device Network Access > Authorization**, click **Customize**.

**Step 6:** Move **NDG:Device Type** into the **Selected** pane, and then click **OK**.

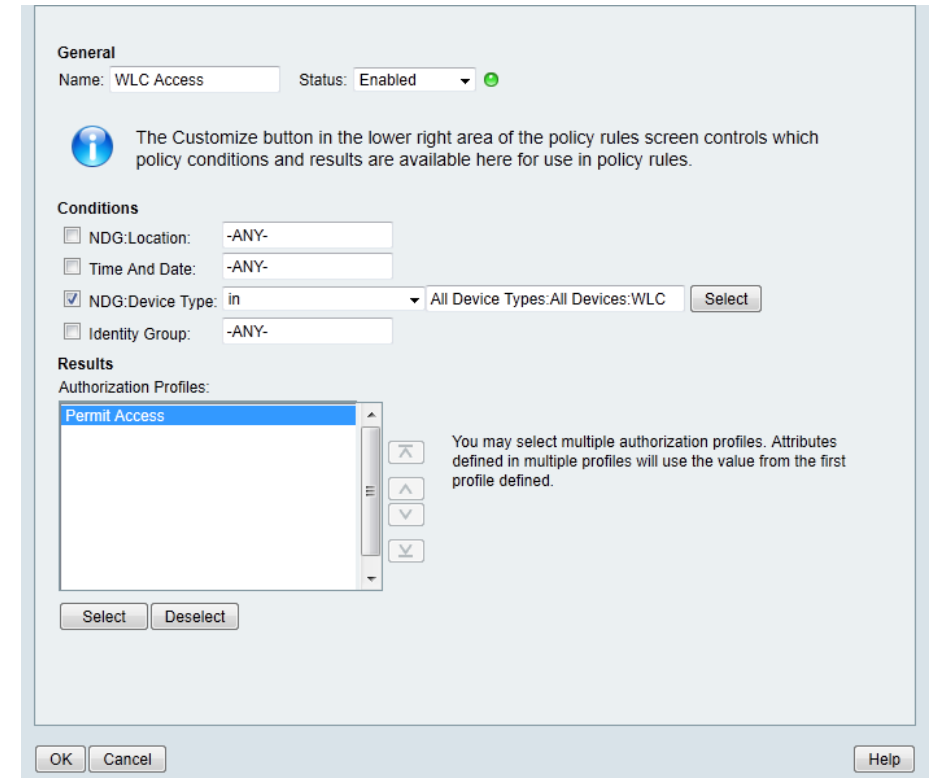


**Step 7:** In **Access Policies > Default Network Access > Authorization**, click **Create**.

**Step 8:** In the **Name** box, enter a name for the rule. (Example: WLC Access)

**Step 9:** Select the **NDG:Device Type** condition, and in the box, select **All DeviceTypes:All Devices:WLC**.

**Step 10:** In the **Authorization Profiles** box, select **Permit Access**, and then click **OK**.



**Step 11:** Click **Save Changes**.

## Procedure 5 Create the Network Device

For each WLC in the organization, create a network device entry in the ACS.

**Step 1:** In **Network Resources > Network Devices and AAA Clients**, click **Create**.

**Step 2:** In the **Name** box, enter the device hostname. (Example: WLC-OEAP-1)

**Step 3:** In the **Device Type** box, select **All Device Types:All Devices:WLC**.

**Step 4:** In the **IP** box, enter the WLCs management interface IP address. (Example: 192.168.19.20)

**Step 5:** Select **TACACS+**.

**Step 6:** Enter the TACACS+ shared secret key. (Example: SecretKey)

**Step 7:** Select **RADIUS**.

**Step 8:** Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)

Network Resources > Network Devices and AAA Clients > Create

Name: WLC-OEAP-1  
Description:

Network Device Groups  
Location: All Locations [Select]  
Device Type: All Device Types:All Devices:WLC [Select]

IP Address  
☒ Single IP Address ☐ IP Range(s)  
IP: 10.4.27.20

Authentication Options  
▼ TACACS+ ☒  
Shared Secret: SecretKey  
☐ Single Connect Device  
☒ Legacy TACACS+ Single Connect Support  
☐ TACACS+ Draft Compliant Single Connect Support  
▼ RADIUS ☒  
Shared Secret: SecretKey  
CoA port: 1700  
☐ Enable KeyWrap  
Key Encryption Key:  
Message Authenticator Code Key:  
Key Input Format ☐ ASCII ☒ HEXADECIMAL

\* = Required fields

Submit Cancel

## Process

Configuring the LAN Distribution Switch

1. Configuring the LAN Distribution Switch

## Procedure 1

### Configuring the LAN Distribution Switch

The VLANs used in the following configuration examples are:

- Wireless data—**VLAN 244, IP: 10.4.144.0/22**
- Wireless voice—**VLAN 248, IP 10.4.148.0/22**
- Remote LAN—**VLAN 252, IP 10.4.152.0/24**

**Step 1:** For Layer 2 configuration, set the distribution layer switch to be the spanning tree root for the wireless VLANs that you are connecting to the distribution switch.

```
vlan 244,248,252
spanning-tree vlan 244,248,252 root primary
```

**Step 2:** For Layer 3 configuration, configure a VLAN interface (SVI) for each VLAN so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan244
description OEAP Wireless Data Network
ip address 10.4.144.1 255.255.252.0
no shutdown
!
interface Vlan248
description OEAP Wireless Voice Network
ip address 10.4.148.1 255.255.252.0
no shutdown
!
interface Vlan252
description OEAP Remote LAN Data Network
ip address 10.4.152.1 255.255.252.0
no shutdown
```

**Step 3:** For interface configuration, an 802.1Q trunk is used for the connection to the WLCs. This allows the distribution switch to provide the Layer 3 services to all the networks defined on the WLC. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the WLC.

```
interface range [interface type] [number], [interface type]
[number]
description To WLC-OEAP
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 244,248,252
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

## Process

### Configuring the WLC

1. Configure the WLC Platform
2. Configure the WLC for NAT
3. Configure Time Zone
4. Configure SNMP
5. Configure Wireless User Authentication
6. Configure Management Authentication

## Procedure 1

## Configure the WLC Platform

After the WLC is physically installed and powered up, you will see the following on the console:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: YES
```

**Step 1:** Enter a system name. (Example: WLC-OEAP-1)

```
System Name [Cisco_7e:8e:43] (31 characters max): WLC-OEAP-1
```

**Step 2:** Enter an administrator username and password.



### Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits or special characters .

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
```

**Step 3:** Use DHCP for the service port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

**Step 4:** Disable link aggregation so clients can attach directly to the LAN distribution switch and not have to traverse the firewall.

```
Enable Link Aggregation (LAG) [yes][NO]: NO
```

**Step 5:** Enter the IP address and subnet mask for the management interface.

```
Management Interface IP Address: 192.168.19.20
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 192.168.19.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
```

**Step 6:** Enter the default DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: **10.4.48.10**

**Step 7:** The WLC uses the virtual interface for Mobility DHCP relay and inter-controller communication. (Example: 192.0.2.1)

Virtual Gateway IP Address: **192.0.2.1**

**Step 8:** Enter a name that will be used as the default mobility and RF group. (Example: OEAP-1)

Mobility/RF Group Name: **OEAP-1**

**Step 9:** Enter an SSID for the WLAN SSID that supports data traffic. You will be able to leverage this later in the deployment process.

Network Name (SSID): **WLAN-Data**

Configure DHCP Bridging Mode [yes][no]: **NO**

**Step 10:** For increased resiliency during a WLC failure, disable DHCP snooping.

Allow Static IP Addresses {YES}[no]: **YES**

**Step 11:** The RADIUS Server will be configured later using the graphical user interface (GUI).

Configure a RADIUS Server now? [YES][no]: **NO**

**Step 12:** Enter the correct country code for the country where you are deploying the WLC.

Enter Country Code list (enter 'help' for a list of countries)  
[US]: **US**

**Step 13:** Enable all wireless networks.

Enable 802.11b network [YES][no]: **YES**

Enable 802.11a network [YES][no]: **YES**

Enable 802.11g network [YES][no]: **YES**

**Step 14:** To help you keep your network up and operational, enable the radio resource management (RRM) auto RF feature.

Enable Auto-RF [YES][no]: **YES**

**Step 15:** Synchronize the WLC clock to the organizations NTP server.

Configure a NTP server now? [YES][no]: **YES**

Enter the NTP server's IP address: **10.4.48.17**

Enter a polling interval between 3600 and 604800 secs: **86400**

**Step 16:** Save the configuration. If you respond with **no** the system will restart without saving the configuration and this procedure must be completed again.

Configuration correct? If yes, system will save it and reset.

[yes][NO]: **YES**

Configuration saved!

Resetting system with new configuration

**Step 17:** Once the WLC has reset, login to the Cisco Wireless LAN Controller Administration page using the credentials defined in Step 2. (Example: <https://wlc-oeap-1.cisco.local/>)

## Procedure 2

## Configure the WLC for NAT

The Internet edge firewall is translating the IP address of the WLC management interface in the DMZ to a publicly reachable IP address so 600 Series OfficeExtend Access Points at telework locations can reach the WLC. However, in order for the 600 Series OfficeExtend Access Points to be able to communicate with the WLC, the publicly reachable address must also be configured on the WLC management interface.

**Step 1:** In **Controller > Interfaces**, click the **management** interface.

**Step 2:** Select **Enable NAT Address**.

**Step 3:** Enter the publicly reachable IP address in the **NAT IP Address** box. (Example: 172.16.130.20)

Step 4: Click Apply.

The screenshot shows the Cisco OfficeExtend Controller configuration page for the 'management' interface. The left sidebar contains a navigation menu with options like General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > Edit' and has '< Back' and 'Apply' buttons. It is divided into several sections: General Information (Interface Name: management, MAC Address: d0:d0:fd:1f:59:e0), Configuration (Quarantine checkbox, Quarantine Vlan Id: 0), NAT Address (Enable NAT Address checkbox, NAT IP Address: 172.16.130.20), Interface Address (VLAN Identifier: 0, IP Address: 192.168.19.20, Netmask: 255.255.255.0, Gateway: 192.168.19.1), Physical Information (Port Number: 1, Backup Port: 0, Active Port: 1, Enable Dynamic AP Management checkbox), DHCP Information (Primary DHCP Server: 10.4.48.10, Secondary DHCP Server: 0.0.0.0), and Access Control List (ACL Name: none). A note at the bottom states: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

### Procedure 3

### Configure Time Zone

Step 1: Navigate to Commands > Set Time.

Step 2: In the Location list choose the time zone that corresponds to the location of the WLC.

Step 3: Click Set Timezone.

The screenshot shows the Cisco OfficeExtend Controller 'Commands > Set Time' page. The left sidebar contains a 'Commands' menu with options like Download File, Upload File, Reboot, Config Boot, Scheduled Reboot, Reset to Factory Default, Set Time, and Login Banner. The main content area is titled 'Set Time' and has 'Set Date and Time' and 'Set Timezone' buttons. It displays the 'Current Time' as 'Tue May 31 11:07:38 2011'. The 'Date' section has dropdowns for Month (May), Day (31), and Year (2011). The 'Time' section has dropdowns for Hour (11), Minutes (7), and Seconds (38). The 'Timezone' section has a 'Delta' section with 'hours' (0) and 'mins' (0) dropdowns, and a 'Location' dropdown menu showing '(GMT -8:00) Pacific Time (US and Canada)'. A 'Foot Notes' section at the bottom states: '1. Automatically sets daylight savings time where used.'

## Procedure 4 Configure SNMP

Step 1: In **Management > SNMP > Communities**, click **New**.

Step 2: Enter the **Community Name**. (Example: cisco)

Step 3: Enter the **IP Address**. (Example: 0.0.0.0)

Step 4: Enter the **IP Mask**. (Example: 0.0.0.0)

Step 5: In the **Status** list choose **Enable**.

Step 6: Click **Apply**.

The screenshot shows the Cisco Management console interface. The left sidebar contains a navigation menu with categories like Summary, SNMP, HTTP-HTTPS, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, Software Activation, and Tech Support. The main content area is titled 'SNMP v1 / v2c Community > New'. It contains a form with the following fields: 'Community Name' (cisco), 'IP Address' (0.0.0.0), 'IP Mask' (0.0.0.0), 'Access Mode' (Read Only), and 'Status' (Enable). There are 'Back' and 'Apply' buttons at the top right of the form.

Step 7: In **Management > SNMP > Communities**, click **New**.

Step 8: Enter the **Community Name**. (Example: cisco123)

Step 9: Enter the **IP Address**. (Example: 0.0.0.0)

Step 10: Enter the **IP Mask**. (Example: 0.0.0.0)

Step 11: In the **Access Mode** list, choose **Read/Write**.

Step 12: In the **Status** list, choose **Enable**.

Step 13: Click **Apply**.

The screenshot shows the Cisco Management console interface. The left sidebar contains a navigation menu with categories like Summary, SNMP, HTTP-HTTPS, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, Software Activation, and Tech Support. The main content area is titled 'SNMP v1 / v2c Community > New'. It contains a form with the following fields: 'Community Name' (cisco123), 'IP Address' (0.0.0.0), 'IP Mask' (0.0.0.0), 'Access Mode' (Read/Write), and 'Status' (Enable). There are 'Back' and 'Apply' buttons at the top right of the form.

Step 14: Navigate to **Management > SNMP > Communities**.

Step 15: Point to the blue box for the **public** community, and then click **Remove**.

Community Name	IP Address	IP Mask	Access Mode	Status	
public	0.0.0.0	0.0.0.0	Read-Only	Enable	Remove
private	0.0.0.0	0.0.0.0	Read-Write	Enable	Remove
cisco	0.0.0.0	0.0.0.0	Read-Only	Enable	Remove
cisco123	0.0.0.0	0.0.0.0	Read-Write	Enable	Remove

**Step 16:** In the message box asking “Are you sure you want to delete?”, click OK.

**Step 17:** Repeat Step 15 and Step 16 for the **private** community.

## Procedure 5 Configure Wireless User Authentication

**Step 1:** In Security > AAA > Radius > Authentication, click New.

**Step 2:** Enter the **Server IP Address**. (Example: 10.4.48.15)

**Step 3:** Enter and confirm the **Shared Secret**. (Example: SecretKey)

**Step 4:** Clear the **Management** box.

**Step 5:** Click **Apply**.

The screenshot shows the Cisco configuration interface for RADIUS Authentication Servers. The left sidebar lists the navigation menu with 'AAA' expanded, showing 'General', 'RADIUS', 'Authentication', 'Accounting', 'Fallback', 'TACACS+', 'LDAP', 'Local Net Users', 'MAC Filtering', 'Disabled Clients', 'User Login Policies', 'AP Policies', and 'Password Policies'. The 'RADIUS' section is selected. The main area is titled 'RADIUS Authentication Servers > New' and contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User: ☒ Enable
- Management: ☐ Enable
- IPSec: ☐ Enable

**Step 6:** In Security > AAA > Radius > Accounting, click **New**.

**Step 7:** Enter the **Server IP Address**. (Example: 10.4.48.15)

**Step 8:** Enter and confirm the **Shared Secret**. (Example: SecretKey)

**Step 9:** Click **Apply**.

The screenshot shows the Cisco configuration interface for RADIUS Accounting Servers. The left sidebar is the same as the previous screenshot. The main area is titled 'RADIUS Accounting Servers > New' and contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Port Number: 1813
- Server Status: Enabled
- Server Timeout: 2 seconds
- Network User: ☒ Enable
- IPSec: ☐ Enable

## Procedure 6 Configure Management Authentication

**Step 1:** In Security > AAA > TACACS+ > Authentication, click New.

**Step 2:** Enter the Server IP Address. (Example: 10.4.48.15)

**Step 3:** Enter and confirm the Shared Secret. (Example: SecretKey), and then click Apply.

The screenshot shows the Cisco configuration interface for TACACS+ Authentication Servers. The left sidebar shows the navigation tree with 'TACACS+ > Authentication' selected. The main panel is titled 'TACACS+ Authentication Servers > New'. The form contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: SecretKey
- Confirm Shared Secret: SecretKey
- Port Number: 49
- Server Status: Enabled
- Server Timeout: 5 seconds

Buttons for '< Back' and 'Apply' are at the top right of the form.

**Step 4:** In Security > AAA > TACACS+ > Accounting, click New.

**Step 5:** Enter the Server IP Address. (Example: 10.4.48.15)

**Step 6:** Enter and confirm the Shared Secret. (Example: SecretKey), and then click Apply.

The screenshot shows the Cisco configuration interface for TACACS+ Accounting Servers. The left sidebar shows the navigation tree with 'TACACS+ > Accounting' selected. The main panel is titled 'TACACS+ Accounting Servers > New'. The form contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: SecretKey
- Confirm Shared Secret: SecretKey
- Port Number: 49
- Server Status: Enabled
- Server Timeout: 5 seconds

Buttons for '< Back' and 'Apply' are at the top right of the form.

**Step 7:** In Security > AAA > TACACS+ > Authorization, click New.

**Step 8:** Enter the Server IP Address. (Example: 10.4.48.15)

**Step 9:** Enter and confirm the Shared Secret. (Example: SecretKey), and then click Apply.

The screenshot shows the Cisco configuration interface for TACACS+ Authorization Servers. The left sidebar shows the navigation tree with 'TACACS+ > Authorization' selected. The main panel is titled 'TACACS+ Authorization Servers > New'. The form contains the following fields:

- Server Index (Priority): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: SecretKey
- Confirm Shared Secret: SecretKey
- Port Number: 49
- Server Status: Enabled
- Server Timeout: 5 seconds

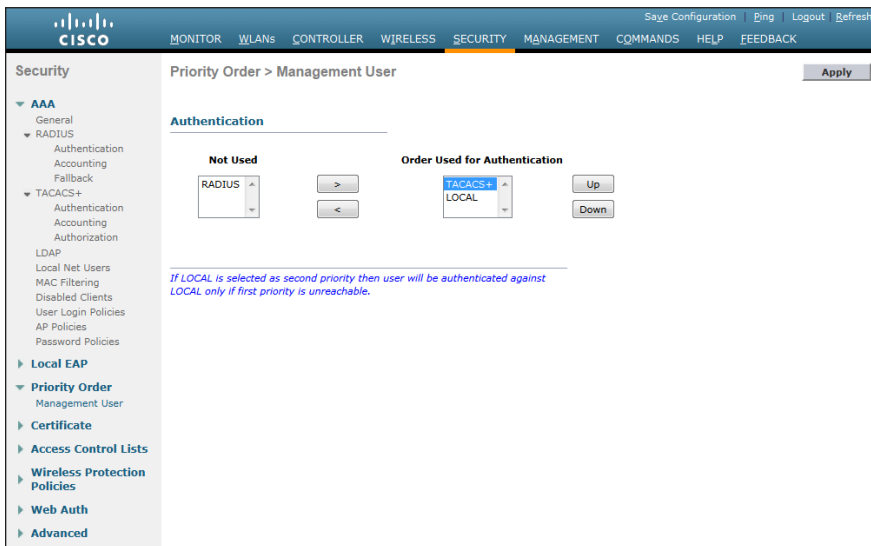
Buttons for '< Back' and 'Apply' are at the top right of the form.

**Step 10:** Navigate to **Security > Priority Order > Management User**

**Step 11:** Using the arrow buttons, move TACACS+ from the **Not Used** list to the **Used for Authentication** list.

**Step 12:** Using the **Up** and **Down** buttons, move TACACS+ to be the first in the **Order Used for Authentication** list.

**Step 13:** Move RADIUS to the **Not Used** list, and then click **Apply**



## Process

### Configuring Voice and Data Connectivity

1. Create Wireless LAN Data Interface
2. Create Wireless LAN Voice Interface
3. Create Remote LAN Interface
4. Configure Data Wireless LAN
5. Configure Voice Wireless LAN
6. Configure Remote LAN

The 600 Series OfficeExtend Access Point supports a maximum of two wireless LANs and one Remote LAN. Configure the SSIDs to separate voice and data traffic, which is essential in any good network design in order to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing.

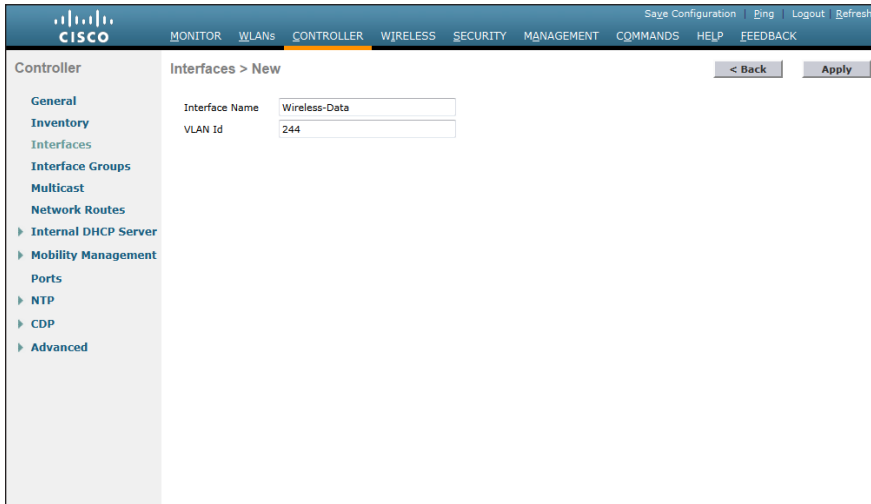
## Procedure 1

### Create Wireless LAN Data Interface

**Step 1:** To add an interface that allows devices on the wireless data network to communicate with the rest of the organization, in **Controller>Interfaces**, click **New**.

**Step 2:** Enter the **Interface Name**. (Example: Wireless-Data)

**Step 3:** Enter the **VLAN identifier**, and then click **Apply**. (Example: 244)



The screenshot shows the Cisco Controller configuration page. The left sidebar has a menu with options like General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main area is titled 'Interfaces > New'. It contains two input fields: 'Interface Name' with the value 'Wireless-Data' and 'VLAN Id' with the value '244'. There are '< Back' and 'Apply' buttons at the top right of the form.

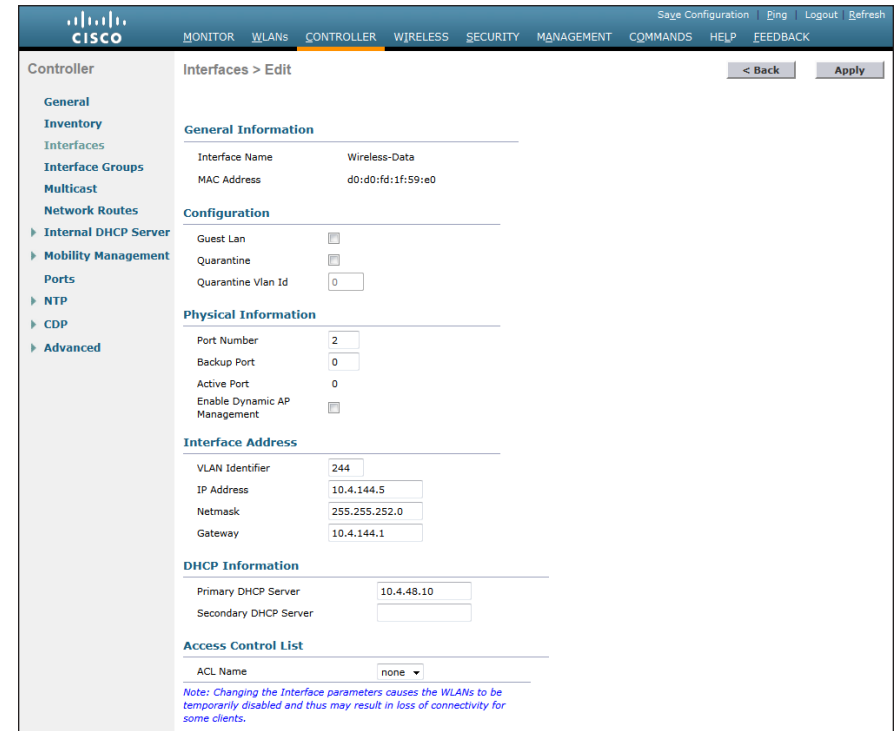
**Step 4:** In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

**Step 5:** In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.144.5)

**Step 6:** Enter the **Netmask**. (Example: 255.255.252.0)

**Step 7:** In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1, Step 2. (Example: 10.4.144.1)

**Step 8:** In the **Primary DHCP Server**, enter the IP address of the organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)



The screenshot shows the Cisco Controller configuration page for 'Interfaces > Edit'. The left sidebar is the same as in Step 3. The main area is titled 'Interfaces > Edit'. It contains several sections: 'General Information' with 'Interface Name' (Wireless-Data) and 'MAC Address' (d0:d0:fd:1f:59:e0); 'Configuration' with checkboxes for 'Guest Lan', 'Quarantine', and 'Quarantine Vlan Id' (0); 'Physical Information' with 'Port Number' (2), 'Backup Port' (0), 'Active Port' (0), and 'Enable Dynamic AP Management' (checkbox); 'Interface Address' with 'VLAN Identifier' (244), 'IP Address' (10.4.144.5), 'Netmask' (255.255.252.0), and 'Gateway' (10.4.144.1); 'DHCP Information' with 'Primary DHCP Server' (10.4.48.10) and 'Secondary DHCP Server'; and 'Access Control List' with 'ACL Name' (none). There are '< Back' and 'Apply' buttons at the top right. A note at the bottom states: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

## Procedure 2

## Create Wireless LAN Voice Interface

You must add an interface that allows devices on the wireless voice network to communicate with the rest of the organization.

**Step 1:** In **Controller>Interfaces**, click **New**.

**Step 2:** Enter the **Interface Name**. (Example: Wireless-Voice)

**Step 3:** Enter the **VLAN identifier**, and then click **Apply**. (Example: 248)

The screenshot shows the Cisco Controller configuration page for a new interface. The left sidebar contains a navigation menu with options: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New'. It contains two input fields: 'Interface Name' with the value 'Wireless-Voice' and 'VLAN Id' with the value '248'. At the top right of the main area are buttons for '< Back' and 'Apply'.

**Step 4:** In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

**Step 5:** In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.148.5)

**Step 6:** Enter the **Netmask**. (Example: 255.255.252.0)

**Step 7:** In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1, Step 2. (Example: 10.4.148.1)

**Step 8:** In the **Primary DHCP Server** box, enter the IP address of the organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)

The screenshot shows the Cisco Controller configuration page for an existing interface. The left sidebar is the same as in Step 3. The main content area is titled 'Interfaces > Edit'. It contains several sections: 'General Information' with 'Interface Name' as 'wireless-voice' and 'MAC Address' as 'd0:d0:fd:1f:59:e0'; 'Configuration' with checkboxes for 'Guest Lan', 'Quarantine', and 'Quarantine Vlan Id' (set to 0); 'Physical Information' with 'Port Number' (2), 'Backup Port' (0), 'Active Port' (0), and 'Enable Dynamic AP Management' (checked); 'Interface Address' with 'VLAN Identifier' (248), 'IP Address' (10.4.148.5), 'Netmask' (255.255.252.0), and 'Gateway' (10.4.148.1); 'DHCP Information' with 'Primary DHCP Server' (10.4.48.10) and an empty 'Secondary DHCP Server' field; and 'Access Control List' with 'ACL Name' set to 'none'. At the bottom, a note states: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.' Buttons for '< Back' and 'Apply' are at the top right.

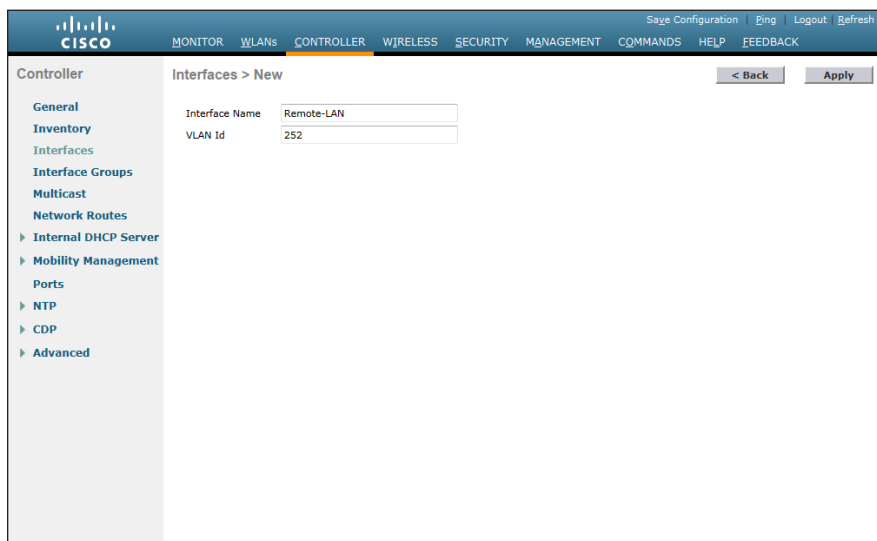
### Procedure 3 Create Remote LAN Interface

Next, you add an interface that allows devices on the remote LAN network to communicate with the rest of the organization.

**Step 1:** In **Controller>Interfaces**, click **New**.

**Step 2:** Enter the **Interface Name**. (Example: Remote-LAN)

**Step 3:** Enter the **VLAN identifier**, and then click **Apply**. (Example: 252)



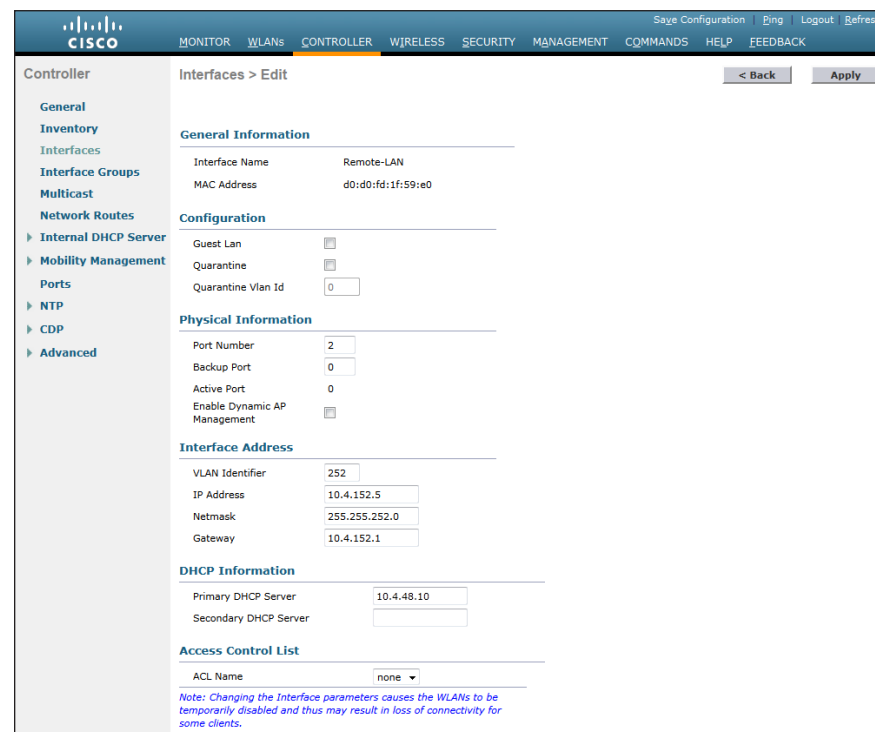
**Step 4:** In the **Port Number** box, enter the WLC interface that connects to the LAN distribution switch. (Example: 2)

**Step 5:** In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.152.5)

**Step 6:** Enter the **Netmask**. (Example: 255.255.252.0)

**Step 7:** In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1, Step 2. (Example: 10.4.152.1)

**Step 8:** In the **Primary DHCP Server** box, enter the IP address of the organization's DHCP server and then click **Apply**. (Example: 10.4.48.10)

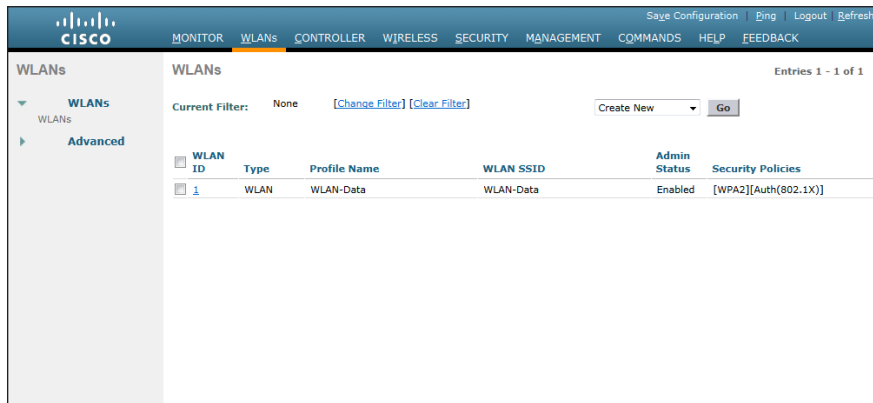


### Procedure 4 Configure Data Wireless LAN

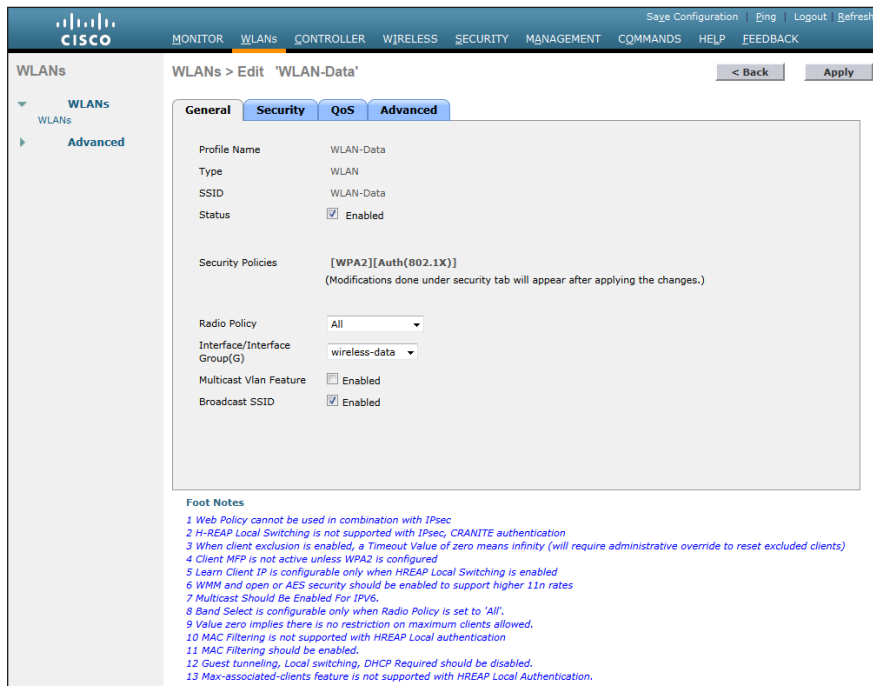
Wireless data traffic is unique to voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. For the data wireless LAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

**Step 1:** Navigate to **WLANS**.

**Step 2:** Click the **WLAN ID** of the SSID created during platform setup.

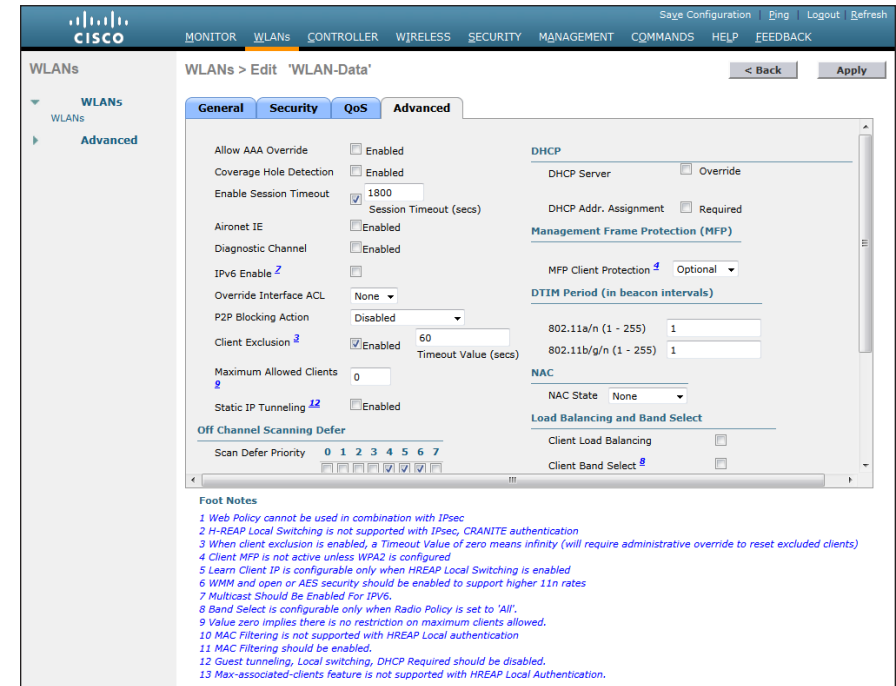


**Step 3:** On the General tab, in the **Interface** list, choose the interface created in Procedure 1. (Example: Wireless-Data)



**Step 4:** On the Advanced tab, clear **Coverage Hole Detection**.

**Step 5:** Clear **Aironet IE**., and then click **Apply**.



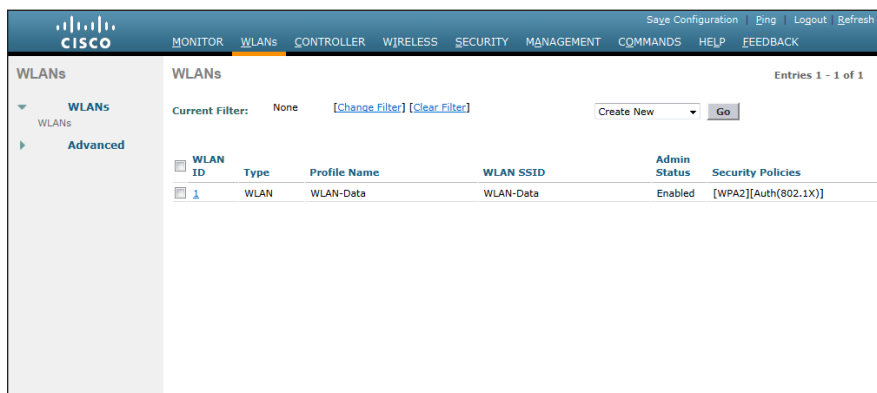
## Procedure 5

## Configure Voice Wireless LAN

Wireless voice traffic is unique to data traffic in that it cannot effectively handle delay and jitter as well as packet loss. To configure the voice wireless LAN change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

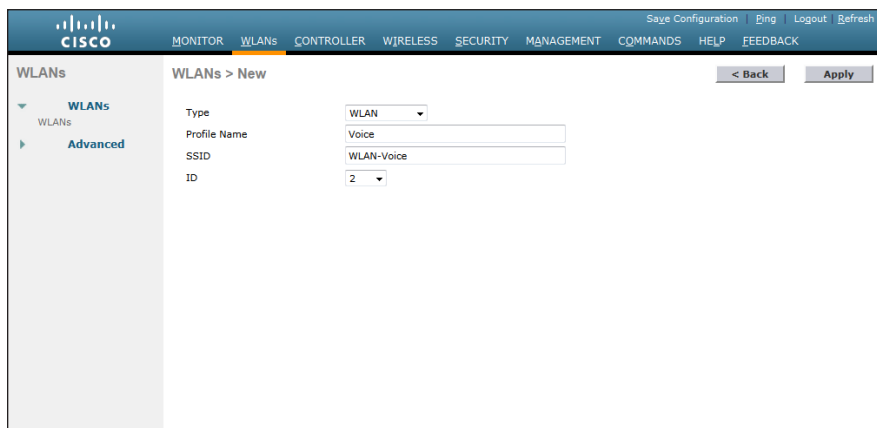
**Step 1:** Navigate to WLANs.

**Step 2:** Select **Create New** in the drop-down list, and then click **Go**.



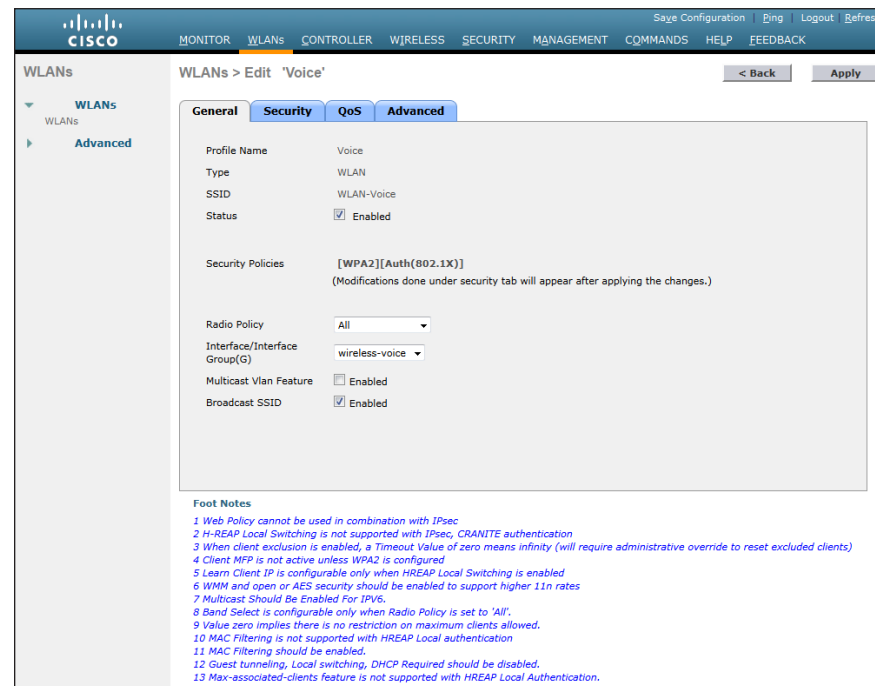
**Step 3:** Enter the **Profile Name**. (Example: Voice)

**Step 4:** Enter the voice WLAN name in the **SSID** box, and then click **Apply**. (Example: WLAN-Voice)



**Step 5:** On the **General** tab, for **Status** select **Enabled**.

**Step 6:** In the **Interface** list, choose the interface created in Procedure 2. (Example: Wireless-Voice)



**Step 7:** On the QoS tab, in the Quality of Service (QoS) list, choose Platinum.

WLANs > Edit 'Voice'

General Security QoS Advanced

Quality of Service (QoS) Platinum (voice)

WMM

WMM Policy	Allowed
7920 AP CAC	<input checked="" type="checkbox"/> Enabled
7920 Client CAC	<input checked="" type="checkbox"/> Enabled

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPv6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.

**Step 8:** On the Advanced tab, clear Coverage Hole Detection.

**Step 9:** Clear Aironet IE., and then click Apply.

WLANs > Edit 'Voice'

General Security QoS Advanced

Allow AAA Override ☐ Enabled

Coverage Hole Detection ☐ Enabled

Enable Session Timeout ☒ 1800

Aironet IE ☐ Enabled

Diagnostic Channel ☐ Enabled

IPv6 Enable ☒

Override Interface ACL None

P2P Blocking Action Disabled

Client Exclusion ☒ Enabled

Maximum Allowed Clients 0

Static IP Tunneling ☒ Enabled

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)

MFP Client Protection ☐ Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

Load Balancing and Band Select

Client Load Balancing ☐

Client Band Select ☐

Foot Notes

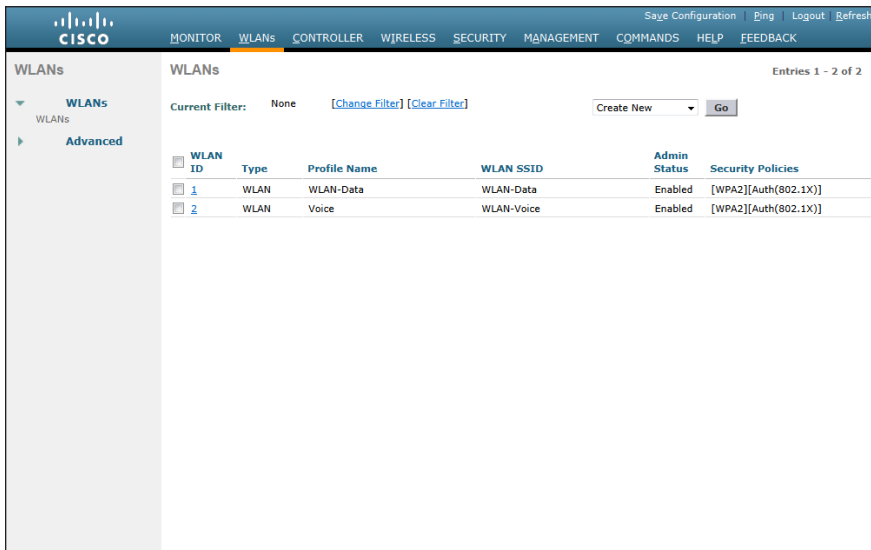
- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPv6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.

## Procedure 6 Configure Remote LAN

A remote LAN is similar to a WLAN except it is mapped to one of the Ethernet ports on the back of the 600 Series OfficeExtend Access Point.

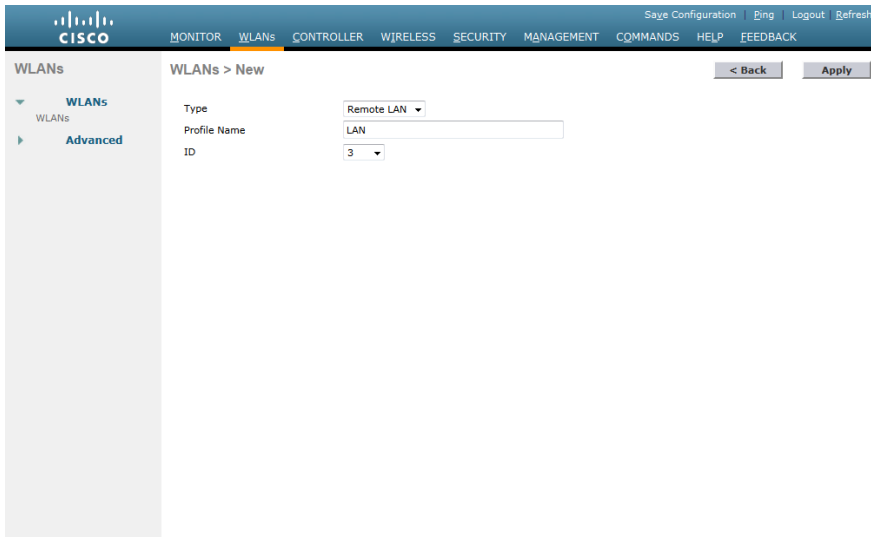
**Step 1:** Navigate to WLANs.

**Step 2:** Select **Create New** in the drop-down list, and then click **Go**.



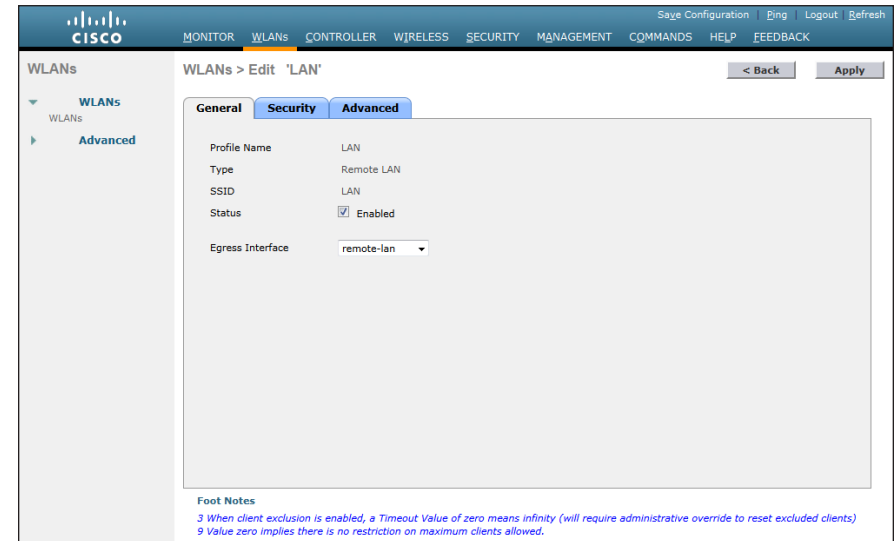
**Step 3:** In the **Type** list, choose **Remote LAN**.

**Step 4:** Enter the **Profile Name**, and then click **Apply**. (Example: LAN)



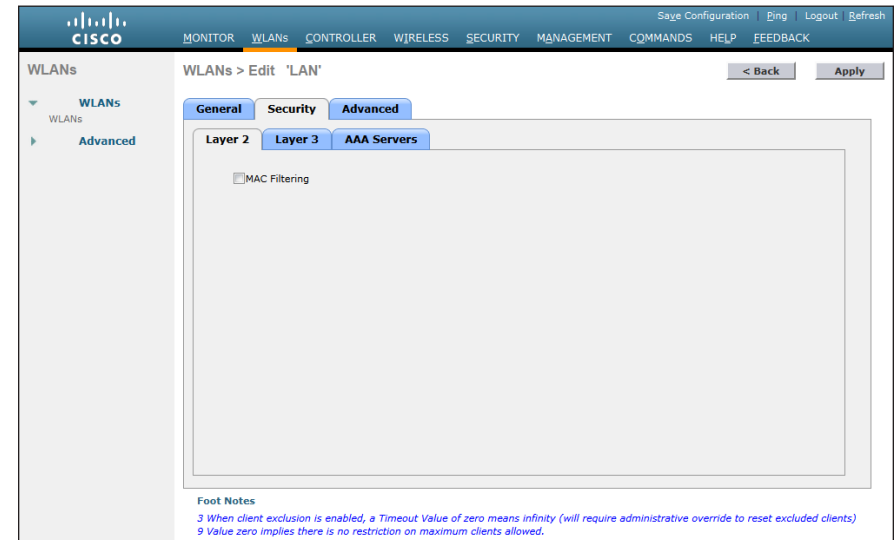
**Step 5:** On the **General** tab, for **Status** select **Enabled**.

**Step 6:** In the **Interface** list, choose the interface created in Procedure 3. (Example: Remote-LAN)



**Step 7:** Click the **Security** tab.

**Step 8:** On the **Layer 2** tab, clear **MAC Filtering**, and then click **Apply**.



## Process

### Configuring WLC Resiliency

1. Configure the resilient WLC
2. Configure APs for Resiliency

This design uses two WLCs. The first is the primary WLC, and in this process, you configure all of the 600 Series OfficeExtend Access Points will be configured to register to it.

The second WLC provides resiliency in case the primary WLC or Internet connection fails. Under normal operation there will not be any 600 Series OfficeExtend Access Points registered to this WLC.

### Procedure 1 Configure the resilient WLC

Repeat the *Configuring the WLC* and *Configuring Voice and Data Connectivity* processes for the second WLC.

### Procedure 2 Configure APs for Resiliency

**Step 1:** On the primary WLC, navigate to **Wireless** and select the desired 600 Series OfficeExtend Access Point.

**Step 2:** Click the **High Availability** tab.

**Step 3:** In the **Primary Controller** box, enter the name and management IP address of the primary WLC. (Example: WLC-OEAP-1 / 172.16.130.20)

**Step 4:** In the **Secondary Controller** box, enter the name and management IP address of the resilient WLC, and then click **Apply**. (Example: WLC-OEAP-2 / 172.17.130.20)

The screenshot shows the Cisco Wireless Controller configuration page for High Availability. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled 'All APs > Details for APE05F.B9DC.FC30'. The 'High Availability' tab is active, showing a table for configuring controllers. The table has columns for 'Name' and 'Management IP Address'. The 'Primary Controller' is configured with 'WLC-OEAP-1' and '172.16.130.20'. The 'Secondary Controller' is configured with 'WLC-OEAP-2' and '172.17.130.20'. The 'Tertiary Controller' is currently empty. Below the table, the 'AP Failover Priority' is set to 'Low'. At the bottom, there is a 'Foot Notes' section with a note: '1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.'

	Name	Management IP Address
Primary Controller	WLC-OEAP-1	172.16.130.20
Secondary Controller	WLC-OEAP-2	172.17.130.20
Tertiary Controller		

AP Failover Priority: Low

**Foot Notes**  
1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.

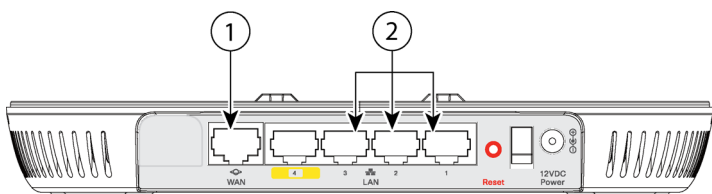
## Process

Configuring the 600 Series Office Extend Access Point

1. Configure the OfficeExtend AP

### Procedure 1

#### Configure the OfficeExtend AP



**Step 1:** Connect the WAN port on the back of the 600 Series OfficeExtend Access Point to your home router/gateway. The 600 Series OfficeExtend Access Point will get an IP address from the home router/gateway.



#### Tech Tip

The 600 Series Office Extend Access Point is not designed to replace the functionality of a home router, and it should not be connected directly to the service provider gateway.

**Step 2:** After the 600 Series OfficeExtend Access Point has started, connect a computer to Ethernet port 1, 2, or 3. The computer gets an IP address from the default DHCP address pool of 10.0.0.0/24.

**Step 3:** Navigate to the 600 Series OfficeExtend Access Point by using its default IP address: <https://10.0.0.1/>

**Step 4:** Log in to the Administration page by using the default credentials: **admin/admin**.

**Step 5:** On the 600 Series OfficeExtend Access Point Welcome page, click **Enter**. The Summary page appears.

**Home: Summary**

**General Information**

Ap Name	APE05F.B9DC.FC30
AP IP Address	192.168.1.100
AP Mode	Local
AP MAC Address	E0:5F:B9:DC:FC:30
AP Uptime	1 minutes, 28 seconds
AP Software Version	7.0.112.53

**AP Statistics**

Radio	Admin Status	Freq/Chan	Tx Power	Pkts In/Out	Bytes In/Out
Radio-802.11G	up	2.4 GHz/6	18.50dBm	0/0	0/0
Radio-802.11A	up	5 GHz/36	12.50dBm	0/0	0/0

**Association**

Client MAC	Association Time	Bytes In/Out	Duplicate/Retries	Decrypt Failed
------------	------------------	--------------	-------------------	----------------

To edit 'Personal SSID' association and settings, click on [Configuration](#)

©2010 Cisco Systems Inc. All rights reserved.

**Step 6:** Navigate to **Configuration > WAN**.

**Step 7:** Enter the outside IP address of the primary WLC in the **Primary Controller IP Address** field, and then click **Apply**. (Example: 172.16.130.20)

The screenshot shows the Cisco OfficeExtend configuration interface. The top navigation bar includes links for HOME, CONFIGURATION, EVENT\_LOG, and HELP. The CONFIGURATION tab is active. Below the navigation bar, there are tabs for System, SSID, DHCP, and WAN. The Primary Controller section is expanded, showing the IP Address field set to 172.16.130.20. Below this, the Uplink IP Configuration section is visible, showing fields for Static IP, Domain Name, IP Address, Subnet Mask, Default Gateway, and DNS Server. The IP Address field is set to 192.168.1.100, Subnet Mask to 255.255.255.0, Default Gateway to 192.168.1.1, and DNS Server to 171.68.226.120. An Apply button is located at the top right of the configuration area.

System	SSID	DHCP	WAN
<b>Primary Controller</b>			
IP Address		172.16.130.20	
<b>Uplink IP Configuration</b>			
Static IP		<input type="checkbox"/>	
Domain Name		cisco.com	
IP Address		192.168.1.100	
Subnet Mask:		255.255.255.0	
Default Gateway		192.168.1.1	
DNS Server		171.68.226.120	

©2010 Cisco Systems Inc. All rights reserved.

**Step 8:** The screen switches to a verification screen. Click **Continue** when it appears.

**Step 9:** The 600 Series OfficeExtend Access Point connects to the controller and downloads the current software image. Allow 5 minutes for the device to download and reboot with the new code and configuration.



### Tech Tip

After a connection is made to the WLC the Status LED on the top of the access point flashes. The Status LED continues flashing until the download is complete. When the download is complete, your access point restarts. Once connected to the controller, the Status LED displays a solid blue or purple.

## Notes

# Cisco Virtual Office

## Business Overview

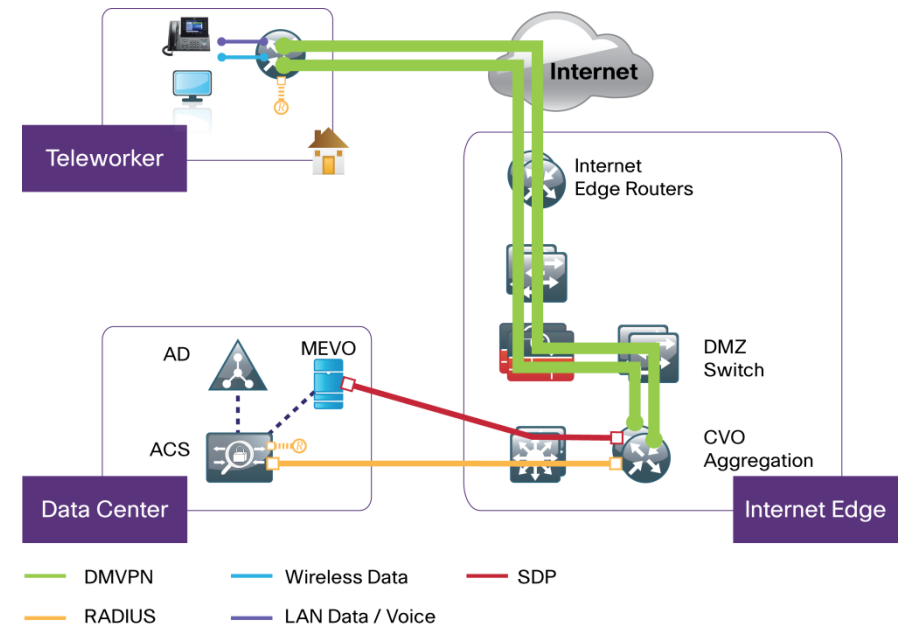
Providing employees access to networked business services from a residential environment poses challenges for both the end user and IT operations. For the home-based teleworker, it is critical that access to business services be reliable and consistent, providing an experience that is as similar as sitting in a cubicle or office in the organization's facility. Employees who work from their home regularly can require a wide array of devices that need to connect to the network. Employees who work from their home regularly might also require support of advanced collaboration technologies like video and call centers.

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 Virtual Office Solution is specifically designed for the teleworker that needs the highest level of resiliency, and advanced technology support. The Cisco Virtual Office Solution supports both wired and wireless users at the CVO remote site (home) and allows for direct communication between the devices without having to traverse the Internet.

Figure 2 - Cisco Virtual Office architecture



Components on the CVO Solution include:

- Dynamic Multipoint VPN (DMVPN) aggregation router serving as the VPN termination point
- Certificate authority (CA) server to issue certificates for both remote and aggregation routers
- Secure device provisioning (SDP) server for provisioning the remote routers
- Authentication, authorization, and accounting (AAA) server for device and user authentication: typically a Cisco Secure Access Control Server (ACS)
- ArcanaNetworks MEVO on a Microsoft Windows 2003 or 2008 server for Cisco Virtual Office management and provisioning
- On the remote-end side, a Cisco 800 Series Router is needed, with an optional IP phone depending on the needs of the customer.

This deployment guide uses two DMVPN aggregation routers for resiliency. The primary VPN aggregation router also hosts the SDP server and the CA server.

## DMVPN Overview

Dynamic Multipoint VPN (DMVPN) is a solution for building scalable site-to-site VPNs that support a variety of applications. DMVPN is widely used for encrypted site-to-site connectivity over public or private IP networks.

DMVPN was selected for the encryption solution for the CVO solution because it supports on-demand full mesh connectivity with a simple hub-and-spoke configuration and a zero-touch hub deployment model for adding remote sites. DMVPN also supports spoke routers that have dynamically assigned IP addresses.

DMVPN makes use of multipoint Generic Route Encapsulation tunnels (mGRE) to interconnect the hub to all of the spoke routers. These mGRE tunnels are also sometimes referred to as DMVPN clouds in this context. This technology combination supports unicast, multicast, and broadcast IP, including the ability to run routing protocols within the tunnels.

## PKI Overview

Public key infrastructure (PKI) provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Each device participating in the secure communication is enrolled, a process by which the entity generates a Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key), and a trusted entity (also known as a CA) validates its identity.

After each entity enrolls in a PKI it is granted a digital certificate that has been issued by the CA. When peers must negotiate a secured communication session, they exchange their digital certificates. Using the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

### Benefits of PKI Integration

- PKI integration reduces the need for complex management of preshared keys for Cisco Virtual Office routers.
- Security of the Cisco Virtual Office router can be increased by the use of RSA keys that are nonexportable and CRL checking to prevent sessions from unauthorized devices.
- PKI integration with AAA protects Cisco Virtual Office hubs with even more security.

## ACS Overview

The Cisco Secure ACS is required for different components of the Cisco Virtual Office solution, namely network device management, end user authentication through the IOS Authentication Proxy (AuthProxy), end user wireless authentication, and PKI-AAA authentication of CVO routers.

## MEVO Overview

ArcanaNetworks MEVO, a Microsoft Windows-based management platform, provides the management component of the Cisco Virtual Office solution.

## CVO Remote

On the remote-end side, a Cisco 800 Series Router, Cisco 1900 Series ISR, or Cisco 2900 Series ISR (the platform is determined by the number of hosts that need to connect) is needed, with an optional IP phone depending on the needs of the customer.

## Deployment Details

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the CVO Solution. These parameters are listed in the following table.

*Table 4 - Universal design parameters*

Network Service	IP Address
Domain name	cisco.local
Active Directory, DNS Server, DHCP Server	10.4.48.10
Authentication Control System (ACS)	10.4.48.15
Network Time Protocol (NTP) Server	10.4.48.17

## Process

Configuring the DMVPN Aggregation Router

1. Finish WAN Router Universal Configuration
2. Connect to the Distribution Switch
3. Configure VRF Lite
4. Connect to Internet DMZ
5. CA and SDP Server Configuration
6. Configure ISAKMP and IPsec
7. Configure the mGRE Tunnel
8. Configure EIGRP
9. Configure IP Multicast Routing
10. Configure QoS

The CVO aggregation includes two routers that terminate DMVPN traffic. Each aggregation router is configured as a unique DMVPN cloud and tied through NAT to a unique ISP.

The deployment of the dual DMVPN clouds is specifically tuned to behave in an active/standby manner. This type of configuration provides symmetric routing, with traffic flowing along the same path in both directions. Symmetric routing simplifies troubleshooting because bidirectional traffic flows always traverse the same links.

The design assumes that one of the DMVPN WAN transports is designated as the primary transport, which is the preferred path in most conditions.

*Table 5 - Example router IP addressing*

Device	Loopback IP address	Port-channel IP address	DMZ IP address
CVOAGG-3945E-1	10.4.32.246/32	10.4.32.6/30	192.168.18.20/24
CVOAGG-3945E-2	10.4.32.247/32	10.4.32.14/30	192.168.18.21/24

## Procedure 1

### Finish WAN Router Universal Configuration

**Step 1:** Configure the device host name to make it easy to identify the device.

```
hostname CVOAGG-3945E-1
```

**Step 2:** Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

**Step 3:** Configure secure user authentication.

Enable authentication, authorization, and accounting (AAA) for access control. AAA controls all management access to the network infrastructure devices (SSH and HTTPS).



## Reader Tip

The AAA server used in this architecture is the Cisco Authentication Control System. For details about ACS configuration, see the *Cisco SBA for Enterprise Organizations—Borderless Networks Network Device Authentication and Authorization Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
!
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

## Step 4: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
  logging synchronous
```

## Step 5: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the IP address block that the distribution switch summarizes to the rest of the network.

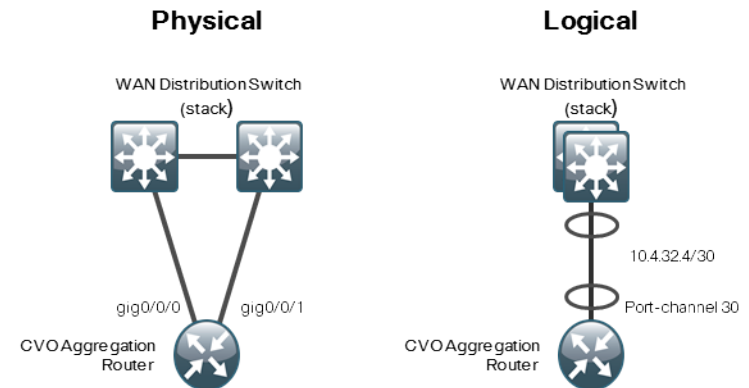
```
interface Loopback0
  ip address 10.4.32.246 255.255.255.255
  ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in the process.

Bind the SNMP and SSH processes to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback 0
ip ssh source-interface Loopback 0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

Figure 3 - Connecting to the distribution switch



**Step 1:** Configure the port-channel interface, and assign an IP address.

## Procedure 2 Connect to the Distribution Switch

The DMVPN hub routers connect to a resilient switching device in the distribution layer and in the DMZ. The DMVPN routers use EtherChannel connections consisting of two port bundles. This design provides both resiliency and additional forwarding performance. Additional forwarding performance can be accomplished by increasing the number of physical links within an EtherChannel.

A Layer 3 port-channel interface connects to the WAN distribution switch. The following configuration creates an EtherChannel link between the router and switch, with two channel-group members.

## Tech Tip

As a best practice, use the same channel numbering on both sides of the link where possible.

```
interface Port-channel 30
  ip address 10.4.32.6 255.255.255.252
```

**Step 2:** Enable the port channel group members and assign the appropriate channel group.

```
interface range GigabitEthernet 0/0, GigabitEthernet 0/1
  no ip address
  channel-group 30
  no shutdown
```

## Procedure 3 Configure VRF Lite

Virtual Routing and Forwarding (VRF) is a technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting

with each other. Often in a multiprotocol label switching (MPLS) context, VRF is also defined as VPN Routing and Forwarding.

VRF may be implemented in a network device by having distinct routing tables, also known as forwarding information bases (FIBs), one per VRF. Alternatively, a network device may have the ability to configure different virtual routers, where each one has its own FIB that is not accessible to any other virtual router instance on the same device.

The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment on a peer-by-peer basis. VRF Lite configurations are only locally significant.

An Internet-facing VRF is created to support Front Door VRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. An associated route distinguisher (RD) must also be configured to make the VRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This deployment uses VRF Lite so the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

```
ip vrf INET-PUBLIC
rd 65520:1
```



### Reader Tip

Command reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

*16-bit autonomous-system-number:your 32-bit number*

For example, 65520:1.

*32-bit IP address: your 16-bit number*

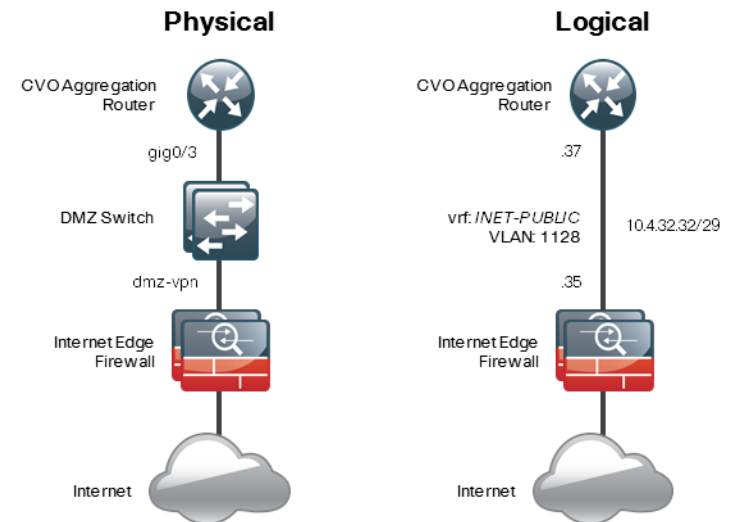
For example, 192.168.122.15:1.

## Procedure 4

## Connect to Internet DMZ

The DMVPN aggregation router requires a connection to the Internet, and in this deployment the DMVPN aggregation router is connected through a Cisco ASA5500 Adaptive Security Appliance using a DMZ interface specifically created and configured for all DMVPN termination routers.

Figure 4 - Connecting to Internet DMZ



**Step 1:** Enable the interface, select the VRF, and assign the IP address.

The IP address used for the Internet-facing interface of the DMVPN aggregation router must be an Internet routable address. There are two possible methods to accomplish this task:

- Assign a routable IP address directly to the router
- Assign a non-routable RFC-1918 address directly to the router and use a static NAT on the Cisco ASA5500 to translate the router IP address to a routable IP address.

This design assumes that the Cisco ASA5500 is configured for static NAT for the DMVPN aggregation router.

The DMVPN design is using Front Door VRF, so this interface must be placed into the VRF configured in the previous procedure.

```
interface GigabitEthernet 0/3
 ip vrf forwarding INET-PUBLIC
 ip address 192.168.18.20 255.255.255.0
 no cdp enable
 no shutdown
```

**Step 2:** Configure the VRF specific default routing.

The VRF created for Front Door VRF must have its own default route to the Internet. This default route points to the ASA5500 DMZ interface IP address.

```
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
```

## Procedure 5 CA and SDP Server Configuration

### Primary Aggregation Router Only

This section presents the configurations for the aggregation components of Cisco Virtual Office for the CA server, and SDP server. The CA and SDP servers can be configured on dedicated routers or co-resident with other features. In this deployment the CA and SDP servers are configured on the primary CVO DMVPN aggregation router.

A CA server manages certificate requests and issues certificates to participating network devices. These services provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

**Step 1:** Configure the HTTP and HTTPS server required for SCEP and SDP.

```
ip http server
ip http port 8000
```

**Step 2:** Configure the IOS Certificate Authority.

```
crypto pki server cvo-cs
 database level complete
 database archive pkcs12 password cisco123
```

```
issuer-name cn=cvo-cs,ou=cvo
auto-rollover
grant auto
no shut
```

**Step 3:** Enable the AAA server for SDP user authentication.

```
aaa group server radius acs
 server-private 10.4.48.15 auth-port 1812 acct-port 1813 key
 SecretKey
aaa authentication login sdp-acs group acs
aaa authorization network sdp-acs group acs
ip radius source-interface Loopback0
```

**Step 4:** Configure SDP Registrar and templates.

```
ip host OpsXML 10.4.48.29
ip host cvo-cs 10.4.32.246
crypto provisioning registrar
 pki-server cvo-cs
 template config http://OpsXML/mevo/Configs/$n_Bootstrap.cfg
 template http welcome http://OpsXML/mevo/sdp/2-sdp_welcome.
 html
 template http completion http://OpsXML/mevo/sdp/4-sdp_
 completion.html
 template http introduction http://OpsXML/mevo/sdp/3-sdp_
 introduction.html
 template http start http://OpsXML/mevo/sdp/1-sdp_start.html
 template http error http://OpsXML/mevo/sdp/sdp_error.html
 template username Administrator password 0 cisco123
 authentication list sdp-acs
 authorization list sdp-acs
```



### Tech Tip

The template user name and password are the Windows administrator credentials on the MEVO server.

## Procedure 6

## Configure ISAKMP and IPsec

All remote-site traffic must be encrypted when transported over public IP networks such as the Internet. The primary goal of encryption is to provide data confidentiality, integrity, and authenticity by encrypting IP packets as the data travels across a network.

**Step 1:** Configure the CA server.

```
ip host cvo-cs 10.4.32.246
crypto pki trustpoint cvo-pki
  enrollment url http://cvo-cs:8000
  serial-number
  ip-address none
  password none
  revocation-check crl
  authorization list sdp-acis
  auto-enroll 75
```

**Step 2:** Authenticate and enroll the certificate.

```
crypto pki authenticate cvo-pki
!!! Type YES if prompted to accept the certificate
crypto pki enroll cvo-pki
```

**Step 3:** Configure the certificate map.

```
crypto pki certificate map DMVPN 10
  issuer-name co cvo-cs
  unstructured-subject-name co cisco.local
```

**Step 4:** Create the Internet Security Association and Key Management Protocol (ISAKMP) profile.

The ISAKMP profile creates an association with an IPsec peer that presents a certificate that matches one using the certificate map defined in previous step.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
  match certificate DMVPN
```

**Step 5:** Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
  encr aes 256
  hash sha
  group 2
```

**Step 6:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN aggregation router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
  esp-sha-hmac
  mode transport
```

**Step 7:** Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

## Procedure 7 Configure the mGRE Tunnel

**Step 1:** Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth of the respective primary or secondary carrier.

The IP maximum transmission unit (MTU) should be configured to 1400 and the **ip tcp adjust-mss** should be configured to 1360. There is a 40 byte difference that corresponds to the combined IP and TCP header length.

```
interface Tunnel 10
  bandwidth 10000
  ip address 10.4.160.1 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

**Step 2:** Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface used in Procedure 4 to connect to the Internet. The **tunnel vrf** command should be set to the VRF defined previously for Front Door VRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel 10
  tunnel source GigabitEthernet0/3
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC
  tunnel key 10
  tunnel protection ipsec profile DMVPN-PROFILE
```

**Step 3:** Configure Next Hop Resolution Protocol (NHRP).

The DMVPN aggregation router acts in the role of NHRP server for all of the spokes. Remote routers use NHRP to determine the tunnel destinations for peers attached to the mGRE tunnel.

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

EIGRP (configured in the following procedure) relies on a multicast transport, and requires NHRP to automatically add routers to the multicast NHRP mappings.

The **ip nhrp redirect** command allows the DMVPN aggregation to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-spoke direct communications.

```
interface Tunnel 10
  ip nhrp authentication cisco123
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp redirect
```

**Step 4:** Configure EIGRP on the tunnel.

EIGRP is configured in the following procedure but has some specific requirements for the mGRE tunnel interface.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This limitation requires that the DMVPN aggregation router advertise routes from other spokes on the same network. This advertisement of these routes would normally be prevented by split horizon, and can be overridden by the **no ip split-horizon eigrp** command.

The EIGRP hello interval is increased to 20 seconds, and the EIGRP hold time is increased to 60 seconds to accommodate up to 900 remote sites on a single DMVPN cloud.

```
interface Tunnel 10
  ip hello-interval eigrp 202 20
  ip hold-time eigrp 202 60
  no ip split-horizon eigrp 202
```

## Procedure 8

## Configure EIGRP

The DMVPN hub routers must have sufficient IP-routing information to provide end-to-end reachability. Maintaining this routing information typically requires a routing protocol. EIGRP is used for this purpose. Multiple separate EIGRP processes are used, one for internal routing on the LAN (EIGRP-100) and one for the DMVPNs (EIGRP-202). The primary reason for the separate EIGRP processes is to ensure compatibility with the route selection process at the WAN-aggregation site when deploying other SBA WAN designs. This method ensures DMVPN learned routes appear as EIGRP external routes after they are redistributed into the EIGRP-100 process used on the campus LAN.

### Step 1: Enable EIGRP-100 for internal routing.

EIGRP-100 is configured facing the LAN distribution. In this deployment, the port-channel interface and the loopback are EIGRP interfaces, with EIGRP neighbor relationships being formed only across the port-channel interface. The network range must include both interface IP addresses either in a single network statement or in multiple network statements. The tunnel interface address should not be included in the network range. It may be helpful to explicitly list all of the relevant networks rather than include them in a single statement. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
 network 10.4.32.6 0.0.0.3
 network 10.4.32.246 0.0.0.0
 passive-interface default
 no passive-interface Port-channel130
 eigrp router-id 10.4.32.246
 no auto-summary
```

### Step 2: Enable an additional EIGRP process for DMVPN.

EIGRP-202 is configured for the DMVPN mGRE interface. Routes from the other EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required. The primary DMVPN cloud is cloud 1.

Table 6 - DMVPN interface parameters

DMVPN cloud	IP address	Tunnel number and key	NHRP network ID
Primary	10.4.160.1/23	10	101
Secondary	10.4.162.1/23	11	102

The tunnel interface is the only EIGRP interface, and its network range should be explicitly listed.

```
router eigrp 202
 network 10.4.160.0 0.0.1.255
 passive-interface default
 no passive-interface Tunnel110
 eigrp router-id 10.4.32.246
 no auto-summary
```

### Step 3: Tag and redistribute the routes.

This design uses mutual route redistribution. DMVPN Routes from the EIGRP-202 process are redistributed into EIGRP-100 and other learned routes from EIGRP-100 are redistributed into EIGRP-202. Because the routing protocol is the same, no default metric is required.

It is important to tightly control how routing information is shared between different routing protocols when this mutual route redistribution is used; otherwise, it is possible to experience route flapping, where certain routes are repeatedly installed and with-drawn from the device routing tables. Proper route control ensures the stability of the routing table.

An inbound distribute-list is used on WAN routers in other SBA WAN deployment guides to limit which routes are accepted for installation into the route table. These routers are configured to only accept routes that do not originate from other WAN sources. Accomplishing this task requires that the DMVPN aggregation routers explicitly tag the DMVPN learned WAN routes during the route redistribution process. The specific route tags in use are shown in the following table.

Table 7 - Route tag information

Tag	Route source	Method
65401	MPLS A	implicit
65402	MPLS B	implicit
65512	DMVPN aggregation routers	Explicit
65520	CVO aggregation routers	Explicit

This example includes all WAN route sources in the reference designs. Depending on the actual design of your network, you may need to use more tags.

```
route-map SET-ROUTE-TAG-DMVPN permit 10
  match interface Tunnel110
  set tag 65520
!
router eigrp 100
  redistribute eigrp 202 route-map SET-ROUTE-TAG-DMVPN
!
router eigrp 202
  redistribute eigrp 100
```

## Procedure 9 Configure IP Multicast Routing

This procedure applies to all DMVPN aggregation routers.

**Step 1:** Enable IP multicast routing.

Enable IP multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

**Step 2:** Configure Protocol Independent Multicast (PIM), RP and scoping.

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.



### Tech Tip

Do not enable PIM on the Internet DMZ interface because no multicast traffic should be requested from this interface.

```
interface range Loopback0, Port-Channel130, Tunnel110
  ip pim sparse-mode
```

**Step 3:** Enable PIM non-broadcast multiple access (NBMA) mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP multicast.

To resolve this issue requires a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
interface Tunnel 10
  ip pim nbma-mode
```

## Procedure 10 Configure QoS

When configuring the WAN-edge QoS, you are defining how traffic will egress your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering to ensure consistent QoS treatment end to end.

**Step 1:** Create the class maps to identify traffic for QoS.

```
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
!
class-map match-any VOICE
  match dscp ef
```

```

!
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
!
class-map match-any CRITICAL-DATA
  match dscp af31 cs3
!
class-map match-any DATA
  match dscp af21
!
class-map match-any SCAVENGER
  match dscp af11 cs1
!
class-map match-any NETWORK-CRITICAL
  match dscp cs6 cs2
  match access-group name ISAKMP

```

**Step 2:** Create the policy map that defines the queuing behavior along with the maximum guaranteed bandwidth allocated to each class

```

policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect

```

**Step 3:** Apply the policy map to the Internet facing interface.

```

interface GigabitEthernet0/3
  service-policy output WAN

```

## Process

Configuring the WAN Distribution Switch

1. Connect to DMVPN Aggregation Router
2. Configure EIGRP

This guide assumes that the WAN distribution switch has already been configured. The guide includes only the procedures required to complete the connections of the DMVPN aggregation router and summarize routes toward the core devices. Full details on distribution layer switch configuration are included in the *Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide*.

## Procedure 1

## Connect to DMVPN Aggregation Router

Table 8 - EtherChannel information

Port-channel number	Port-channel IP address
30	10.4.32.5/30
31	10.4.32.13/30

The port-channel interface connects to a DMVPN aggregation router. This connection is a Layer 3 port-channel. The following configuration creates an EtherChannel link between the switch and router, with two channel-group members.

**Step 1:** Configure the port-channel interface and assign the IP address.



### Tech Tip

As a best practice, use the same channel numbering on both sides of the link where possible.

```
interface Port-channel 30
  no switchport
  ip address 10.4.32.5 255.255.255.252
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
```

**Step 2:** Enable the port-channel group members, and assign the appropriate channel group.

```
interface range GigabitEthernet1/0/13, GigabitEthernet2/0/13
  description CVOAGG-3945E-1
  no switchport
  no ip address
  channel-group 30 mode on
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  carrier-delay msec 0
  no shutdown
```

## Procedure 2 Configure EIGRP

**Step 1:** Enable EIGRP to form a neighbor relationship with the aggregation router.

```
router eigrp 100
  no passive-interface Port-channel130
```

**Step 2:** When the distribution switch connects to a core layer, configure the WAN switch to generate IP route summaries for the CVO sites. After the summaries have been configured, EIGRP suppresses the advertisement of more specific routes within the summary ranges.

```
interface range TenGigabitEthernet2/1/1,
TenGigabitEthernet1/1/1
  ip summary-address eigrp 100 10.4.160.0 255.255.252.0
  ip summary-address eigrp 100 10.4.128.0 255.255.240.0
```

## Process

Configuring the Internet Edge

1. Configure the Firewall DMZ Interface
2. Configure NAT
3. Configure Security Policy
4. Configure the DMZ Switch

This guide assumes that the Internet Edge firewall has already been configured. The guide includes only the procedures required to complete the connections to the DMVPN aggregation routers. Full details on Internet Edge firewall configuration are included in the *Internet Edge Deployment Guide*.

## Procedure 1 Configure the Firewall DMZ Interface

The firewall DMZ (De-Militarized Zone) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The various DMZ networks are connected to the Cisco ASAs on the ASAs' GigabitEthernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the Cisco ASA is the default gateway for that DMZ subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

**Step 1:** In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

**Step 2:** Click **Edit**.

**Step 3:** Select **Enable Interface**, and then click **OK**.

**Edit Interface**

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/1 Configure Hardware Properties...

Interface Name:

Security Level:

☐ Dedicate this interface to management only

Channel Group:

☒ Enable Interface

IP Address

☒ Use Static IP ☐ Obtain Address via DHCP ☐ Use PPPoE

IP Address:

Subnet Mask: 255.0.0.0

Description: dmz trunk to dmz-3750 stack port x/0/1

OK Cancel Help

**Step 4:** On the Interface pane, click **Add > Interface**.

**Step 5:** In the **Hardware Port** list, choose the interface configured in Step 1. (Example: GigabitEthernet0/1)

**Step 6:** In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

**Step 7:** In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

**Step 8:** Enter an **Interface Name**. (Example: dmz-dmvpn)

**Step 9:** In the **Security Level** box, enter a value of **75**.

**Step 10:** Enter the interface IP address. (Example: 192.168.18.1)

**Step 11:** Enter the interface subnet mask, and then click **OK**. (Example: 255.255.255.0)

**Add Interface**

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/1

VLAN ID: 1118

Subinterface ID: 1118

Interface Name: dmz-dmvpn

Security Level: 75

☐ Dedicate this interface to management only

Channel Group:

☒ Enable Interface

IP Address

☒ Use Static IP ☐ Obtain Address via DHCP ☐ Use PPPoE

IP Address: 192.168.18.1

Subnet Mask: 255.255.255.0

Description: DMVPN aggregation router connections on VLAN 1118

OK Cancel Help

## Procedure 2 Configure NAT

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of the CVO aggregation router to an outside public address. For resiliency, the primary and resilient CVO aggregation routers will be translated to separate ISPs.

*Table 9 - Example DMZ address to public IP address mapping*

CVO router DMZ address	CVO router public address (externally routable after NAT)
192.168.18.20	172.16.130.2 (ISP-A)
192.168.18.21	172.17.130.2 (ISP-B)

**Step 1:** Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

**Step 2:** To add a network object for the public address of the CVO aggregation router, click **Add > Network Object**.

**Step 3:** In the **Add Network Object** dialog box, in the **Name** box, enter a description for the public IP address of the primary CVO aggregation router. (Example: outside-cvo-1)

**Step 4:** In the **IP Address** box, enter the public IP address of the primary CVO aggregation router, and then click **OK**. (Example: 172.16.130.2)

**Step 5:** To add a network object for the private DMZ address of the CVO aggregation router, click **Add > Network Object**.

**Step 6:** In the **Add Network Object** dialog box, in the **Name** box, enter a description for the private DMZ IP address of the primary CVO aggregation router. (Example: dmz-cvo-1)

**Step 7:** In the **IP Address** box, enter the private DMZ IP address of the primary CVO aggregation router. (Example: 192.168.18.20)

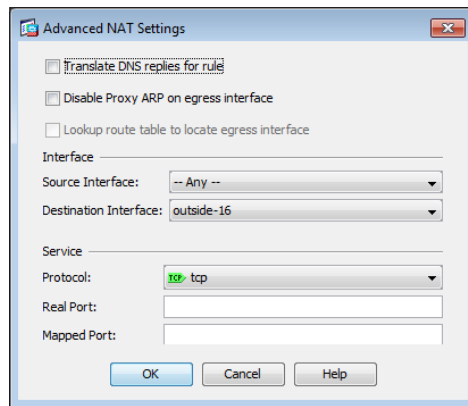
**Step 8:** To expand the NAT pane, click the two down arrows.

**Step 9:** Select **Add Automatic Address Translation Rules**.

**Step 10:** In the **Translated Addr** list, choose the network object created in Step 2.

**Step 11:** Click **Advanced**.

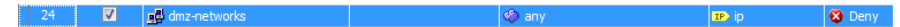
**Step 12:** In the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



**Step 13:** Repeat Step 1 through Step 12 for the resilient CVO aggregation router.

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**.

**Step 2:** Click the rule that denies traffic from the DMZ toward other networks.



Next, you will insert a new rule above the rule you selected that enables the CVO remote routers to communicate with the CVO aggregation routers in the DMZ.

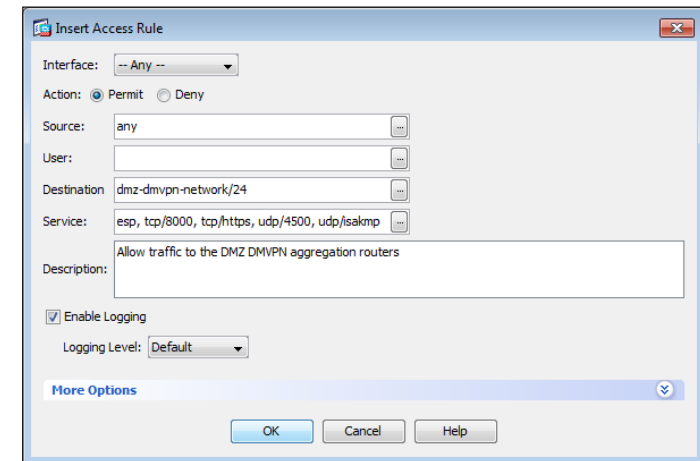
**Step 3:** Click **Add > Insert**.

**Step 4:** In the **Internet Access Rule** dialog box, in the **Interface** list, select **—Any—**.

**Step 5:** For **Action**, select **Permit**.

**Step 6:** In the **Destination** list, choose the automatically created network object for the DMZ. (Example: dmz-dmvpn-network/24)

**Step 7:** In the **Service** list box, enter **esp, tcp/8000, tcp/https, udp/4500, udp/isakmp**, and then click **OK**.



**Step 8:** Click **Apply**.

### Procedure 3 Configure Security Policy

Security policy configuration is fairly arbitrary to suit the policy and management requirements of an organization. Thus, use the examples here as a basis for your network-security requirements.

The VPN DMZ provides an additional layer of protection to lower the likelihood that certain types of misconfiguration on the CVO routers will expose the business network to the Internet. A filter allows only CVO related traffic to reach the CVO routers.

**Table 10 - Required DMVPN protocols (aggregation router)**

Name	Protocol	Usage
sdp	HTTPS / TCP 8000	SDP
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

## Procedure 4 Configure the DMZ Switch

You should connect each CVO aggregation router to a different switch in the DMZ switch stack for resiliency. The CVO aggregation routers are connected to a VLAN that is dedicated to routers that aggregate DMVPN connections from the Internet. QoS policies are applied even though the traffic crosses the Internet to correctly trust the classification of packets that occurred at the CVO remote site.

**Step 1:** Set the DMZ switch to be the spanning tree root for the VLAN that contains the CVO aggregation routers.

```
vlan 1118
spanning-tree vlan 1118 root primary
```

**Step 2:** Configure the interfaces that are connected to the appliances as a trunk.

```
interface GigabitEthernet1/0/24
description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1118
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

**Step 3:** Configure the interfaces that are connected to the CVO aggregation routers.

```
interface GigabitEthernet1/0/9
description CVOAGG-3945E-1 Gig0/3
!
interface GigabitEthernet2/0/9
description CVOAGG-3945E-2 Gig0/3
```

```
!
interface range GigabitEthernet1/0/9, GigabitEthernet2/0/9
switchport access vlan 1118
switchport host
macro apply EgressQoS
logging event link-status
no shutdown
```

## Process

Configuring the Cisco ACS

1. Configuring the MEVO account
2. Enable the Default Network Device
3. Create an AuthProxy Authorization Profile
4. Enable CVO User Authentication
5. Create the CVO Groups and AAA Clients
6. Enabled Support for PKI-AAA

This guide assumes that Cisco ACS has already been configured. The guide includes only the procedures required to support the integration of CVO into the deployment. Full details on Cisco ACS configuration are included in the *Cisco Smart Business Architecture—Borderless Networks for Enterprise Organizations Network Device Authentication and Authorization Deployment Guide*.

An access control server is required for different components of the Cisco Virtual Office solution, namely network device management authentication, authentication proxy for end users, wireless authentication, and public key infrastructure authentication of routers.

## Procedure 1 Configuring the MEVO account

**Step 1:** Navigate to Users and Identity Stores > Internal Identity Stores > Users.

**Step 2:** Click **Create**.

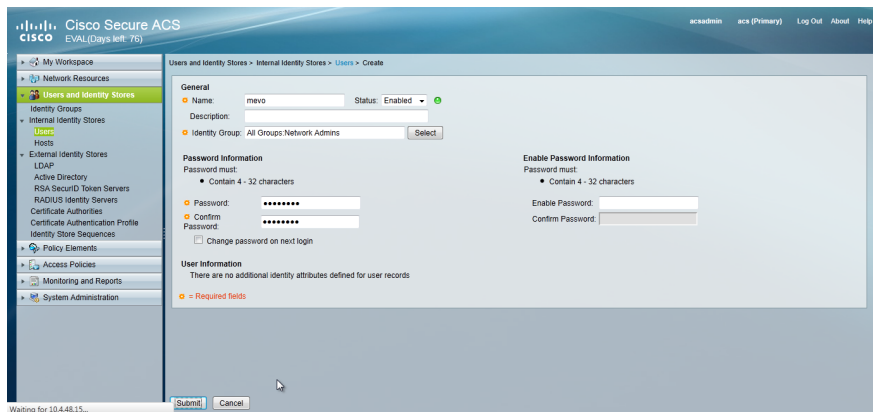
**Step 3:** Enter a user name for the account in the **Name** box. (Example: mevo)

**Step 4:** Enter and confirm the password.

**Step 5:** To associate the account to the identity group that defines network administrators, click **Select**. The **Identity Groups** window opens.

**Step 6:** Select the appropriate identity group, and then click **OK**. (Example: All Groups:Network Admins)

**Step 7:** To apply the changes, click **Submit**.



## Procedure 2 Enable the Default Network Device

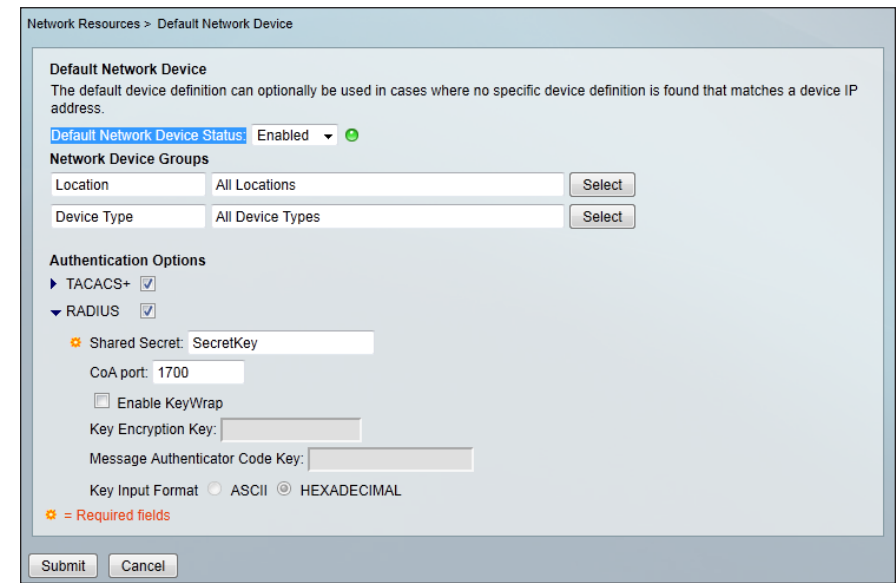
There are many devices deployed in a CVO solution, primarily CVO remote routers and autonomous APs, and tracking their assigned IP addresses can be difficult. So instead of creating a unique network device entry in ACS for each CVO remote device, enable the default network device, which can be used by any device on the network as long as it has the correct shared secret key.

**Step 1:** Navigate to **Network Resources > Default Network Device**.

**Step 2:** In the **Default Network Device Status** list, choose **Enabled**.

**Step 3:** Select **RADIUS**.

**Step 4:** Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)



## Procedure 3 Create an AuthProxy Authorization Profile

The Authentication Proxy (AuthProxy) feature is used for CVO end-user authentication. The CVO user is allowed access to the organizations internal network only if the user provides valid credentials. The ACS server must verify the credentials. Upon verification of the credentials, access control entries are downloaded and applied on the CVO remote site router, giving the user the appropriate level of access.

**Step 1:** In **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, click **Create**.

**Step 2:** Enter a **Name**. (Example: AuthProxy)

**Step 3:** On the **Radius Attributes** tab, in the **Dictionary Type** list, choose **RADIUS-Cisco**.

**Step 4:** In the **RADIUS Attribute** box, select **cisco-av-pair**.

**Step 5:** In the **Attribute Value** box, enter **auth-proxy:priv-lvl=15**, and then click **Add**.

**Step 6:** On the **RADIUS Attributes** tab, in the **Dictionary Type** list, choose **RADIUS-Cisco**.

**Step 7:** In the **RADIUS Attribute** box, select **cisco-av-pair**.

**Step 8:** In the **Attribute Value** box, enter **auth-proxy:proxyacl#1=permit ip any any**, and then click **Add**.

**Step 9:** Click **Submit**.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	auth-proxy:priv-lvl=15
cisco-av-pair	String	auth-proxy:proxyacl#1=permit ip any any

Add A Edit V Replace A Delete

Dictionary Type: RADIUS-Cisco

RADIUS Attribute: Select

Attribute Type:

Attribute Value: Static

Submit Cancel

## Procedure 4

## Enable CVO User Authentication

First you must disable the ACS from accepting the EAP-TLS protocol.

**Step 1:** In **Access Policies**, click **Default Network Access**.

**Step 2:** On the **Allowed Protocols** tab, clear **Allow EAP-TLS**, and then click **Submit**.

Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"

General **Allowed Protocols**

☒ Process Host Lookup

**Authentication Protocols**

- ☒ Allow PAP/ASCII
- ☐ Allow CHAP
- ☐ Allow MS-CHAPv1
- ☐ Allow MS-CHAPv2
- ☒ Allow EAP-MD5
- ☐ Allow EAP-TLS
- ☒ Allow LEAP
- ☒ Allow PEAP
- ☒ Allow EAP-FAST

☐ Preferred EAP protocol LEAP

Submit Cancel

Next create an authorization rule to allow the CVO devices to authenticate clients using RADIUS.

**Step 3:** Navigate to **Access Policies > Default Network Access > Identity**.

**Step 4:** In the **Identity Source** box, select **AD, Local DB**, and then click **Save Changes**.

Access Policies > Access Services > Default Network Access > Identity

☒ Single result selection ☐ Rule based result selection

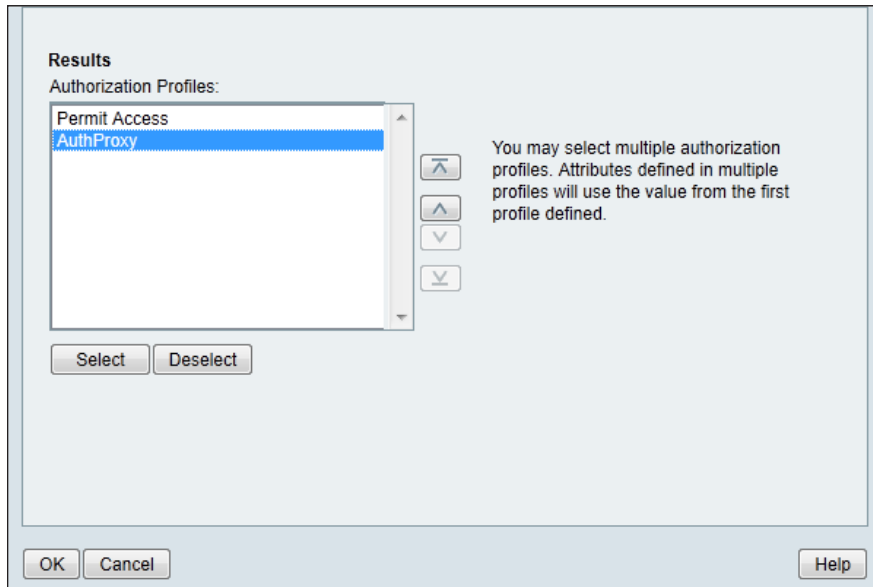
Identity Source: AD, Local DB Select

Advanced Options

Save Changes Discard Changes

**Step 5:** In **Access Policies > Default Network Access > Authorization**, click the **Default** rule.

**Step 6:** In the **Authorization Profiles** box, select **Permit Access** and the profile created in Procedure 3, and then click **OK**.



**Step 7:** Click **Save Changes**.

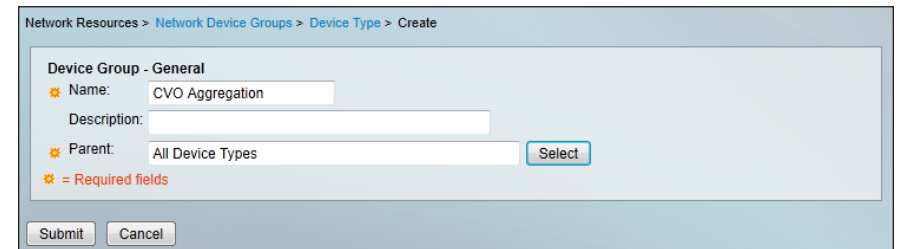
### Procedure 5 Create the CVO Groups and AAA Clients

First, you must create a network device group to contain the CVO aggregation routers.

**Step 1:** In **Network Resources > Network Device Groups > Device Type**, click **Create**.

**Step 2:** In the **Name** box, enter a name for the group. (Example: CVO Aggregation)

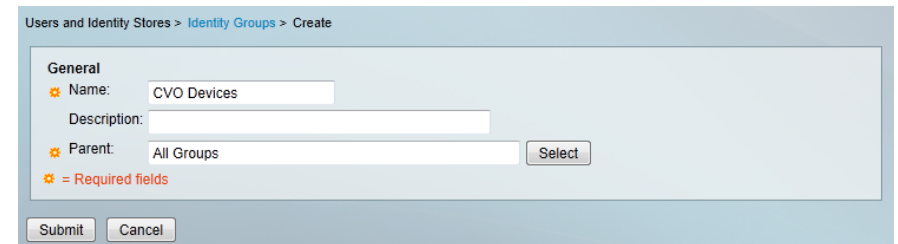
**Step 3:** In the **Parent** box, select **All Device Types**, and then click **Submit**.



Next, create an identity group to contain the CVO remote site routers.

**Step 4:** In **Users and Identity Stores > Identity Groups**, click **Create**.

**Step 5:** In the **Name** box, enter a name for the group, and then click **Submit**. (Example: CVO Devices)



Next, for the primary and resilient CVO aggregation routers, create network device entries in the ACS. MEVO creates the CVO remote site router accounts.

**Step 6:** In **Network Resources > Network Devices and AAA Clients**, click **Create**.

**Step 7:** In the **Name** box, enter the device hostname. (Example: CVOAGG-3945E-1 )

**Step 8:** In the **Device Type** box, select **All Device Types:CVO Aggregation**.

**Step 9:** In the **IP** box, enter the router's loopback IP address. (Example: 10.4.32.246)

**Step 10:** Select **TACACS+**.

**Step 11:** Enter the TACACS+ shared secret key. (Example: SecretKey)

**Step 12:** Select **RADIUS**.

**Step 13:** Enter the RADIUS shared secret key, and then click **Submit**.  
(Example SecretKey)

Network Resources > Network Devices and AAA Clients > Create

Name: CVOAGG-3945E-1  
Description:

Network Device Groups  
Location: All Locations [Select]  
Device Type: All Device Types:CVO Aggregation [Select]

IP Address  
☒ Single IP Address ☐ IP Range(s)  
IP: 10.4.32.246

Authentication Options  
▼ TACACS+ ☒  
Shared Secret: SecretKey  
☐ Single Connect Device  
☒ Legacy TACACS+ Single Connect Support  
☐ TACACS+ Draft Compliant Single Connect Support  
▼ RADIUS ☒  
Shared Secret: SecretKey  
CoA port: 1700  
☐ Enable KeyWrap  
Key Encryption Key:  
Message Authenticator Code Key:  
Key Input Format ☐ ASCII ☒ HEXADECIMAL

★ = Required fields

Submit Cancel

**Step 5:** In the **Attribute Value** box, enter **pki:cert-application=all**, and then click **Add**.

**Step 6:** Click **Submit**.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General Common Tasks RADIUS Attributes

Common Tasks Attributes

Attribute	Type	Value
-----------	------	-------

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	pki:cert-application=all

Add Edit Replace Delete

Dictionary Type: RADIUS-Cisco

RADIUS Attribute: [Select]  
Attribute Type: [Select]  
Attribute Value: Static

★ = Required fields

Submit Cancel

## Procedure 6 Enabled Support for PKI-AAA

PKI-AAA authentication is used for device authentication to check the validity of CVO remote routers as part of the secure session setup.

**Step 1:** In **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, click **Create**.

**Step 2:** Enter a **Name**. (Example: PKI-AAA)

**Step 3:** On the **Radius Attributes** tab, in the **Dictionary Type** list choose **RADIUS-Cisco**.

**Step 4:** In the **RADIUS Attribute** box, select **cisco-av-pair**.

**Step 7:** In **Access Policies > Default Network Access > Authorization**, click **Create**.

**Step 8:** Enter a **Name**. (Example: CVO-PKI-AAA)

**Step 9:** Select the **NDG:Device Type** condition, and in the box, select the group created in Procedure 5, Step 1. (Example: All Device Types:CVO Aggregation)

**Step 10:** Select the **Identity Group** condition and in the box select the group created in Procedure 5, Step 4. (Example: All Groups:CVO Devices)

**Step 11:** In the **Authorization Profiles** box select **Permit Access** and the profile created in Step 1, and then click **OK**. (Example: PKI-AAA)

## Step 12: Click Save Changes.

The screenshot shows the 'General' tab of a policy rule configuration window. The 'Name' field is 'CVO-PKI-AAA' and the 'Status' is 'Enabled' with a green checkmark. An information icon and text state: 'The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.' Under the 'Conditions' section, 'NDG:Location' and 'Time And Date' are set to '-ANY-'. 'NDG:Device Type' is set to 'in' with a dropdown menu showing 'All Device Types:All Devices:CVO A' and a 'Select' button. 'Identity Group' is set to 'in' with a dropdown menu showing 'All Groups:CVO Devices' and a 'Select' button. Under the 'Results' section, 'Authorization Profiles' shows a list with 'Permit Access' and 'PKI-AAA'. To the right of the list, text says: 'You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.' Below the list are 'Select' and 'Deselect' buttons. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

## Process

### Configuring ArcanaNetworks MEVO

1. Configure Subnet Blocks
2. Integrate MEVO into the SDP Registrar
3. Integrate the Primary DMVPN Cloud
4. Integrating the Resilient DMVPN Cloud
5. Integrating MEVO into the Cisco ACS
6. Configure Variables for the Remote Site
7. Activate CVO Remote Templates
8. Configure the Email Server
9. Create End Users
10. Provision End Users
11. Deploying Authentication Proxy

This process describes the procedures needed to configure a newly installed instance of ArcanaNetworks MEVO for Cisco Virtual Office. Many of the administrator tasks need to be performed only once. After the initial configuration, the administrator should need to do little except manage user accounts.

## Procedure 1

### Configure Subnet Blocks


**Step 1:** Navigate to the ArcanaNetworks MEVO Administration page.  
(Example: <http://mevo.cisco.local/mevo/login.php>)

**Step 2:** Log in using the default credentials (user name and password: **mevoadmin** and **mevoadmin**).

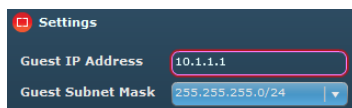
Next, you configure support for users who are connecting to the Internet via the CVO remote router but who aren't employees of the organization.

**Step 3:** In **Configuration > Subnet Blocks**, in the **Settings** pane, enter a network address in the **Guest IP Address** box. (Example: 10.1.1.1)

**Step 4:** Choose the subnet size from the **Guest Subnet Mask** list. (Example: 255.255.255.0/24)

**Tech Tip**

The guest network information is the same for all CVO routers. Guest traffic will be sent directly to the Internet using Network Address Translation (NAT)



Now you define the network range from which to assign unique remote LAN networks for each CVO remote router.

**Step 5:** In **Configuration > Subnet Blocks**, click **Add**.

**Step 6:** In the **Name** box, enter the name of the network. (Example: Remote LAN)

**Step 7:** In the **Description** box, enter a summary of the network. (Example: LAN)

**Step 8:** In **Type** list, choose **LAN**.

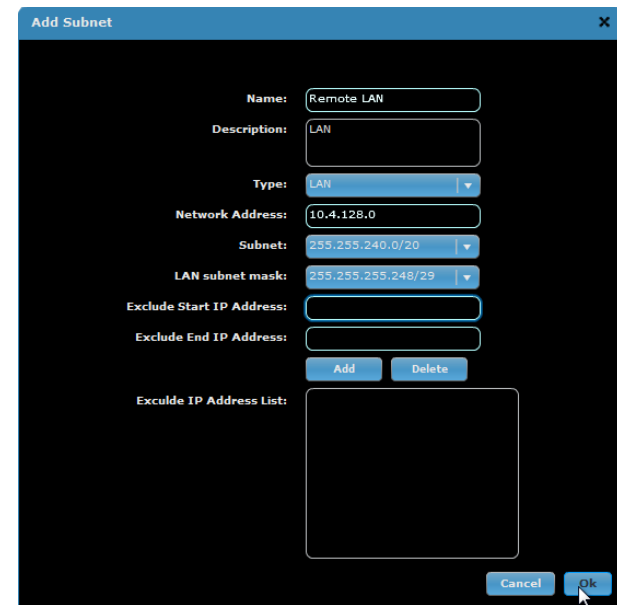
Next, define the network range from which to assign remote subnets.

**Step 9:** In the **Network Address** box, enter an IP address. (Example: 10.4.128.0)

**Step 10:** From the **Subnet** list, choose the subnet size. (Example: 255.255.240.0/20)

Now you define the size of the subnet assigned to each CVO remote router.

**Step 11:** Select the subnet size from the **LAN subnet mask** list, and then click **OK**. (Example: 255.255.255.248/29)

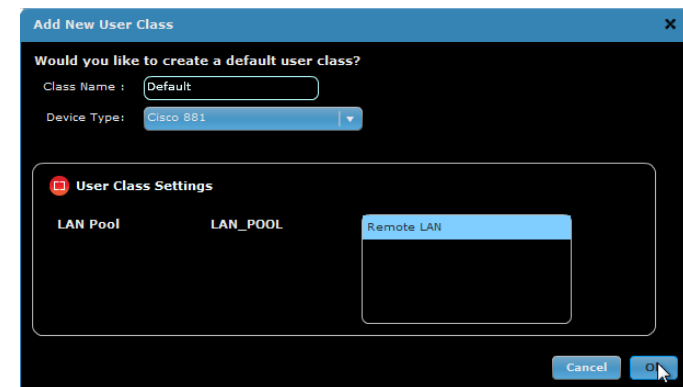


**Step 12:** In the confirmation window, click **Add**. The **Add New User Class** dialog box appears.

Next, you define the type of device used for the CVO remote routers.

**Step 13:** In the **Device Type** list, choose **Cisco 881**, and then click **OK**.

**Step 14:** Click **Save**.



## Procedure 2






## Integrate MEVO into the SDP Registrar

**Step 1:** To integrate MEVO into the SDP registrar, navigate to **Configuration > Headend**.

**Step 2:** For the SDP registrar in the **Device Type** list, choose the model of the primary aggregation device. (Example: Cisco 3945 E)

**Step 3:** In the **Management IP** box, enter the loopback IP address of the primary aggregation device. (Example: 10.4.32.246)

**Step 4:** In the **Outside IP** box, enter the IP address of the primary aggregation device's outside interface. (Example: 172.16.130.2)

		Role	Device Type	Management IP	Outside IP	Passwords	Variables	Status
		SDP Registrar	Cisco 3945 E	10.4.32.246	172.16.130.2			

**Step 5:** To enter the access credentials to the primary aggregation device, click the icon in the **Passwords** field. The **Access Credentials** window appears.

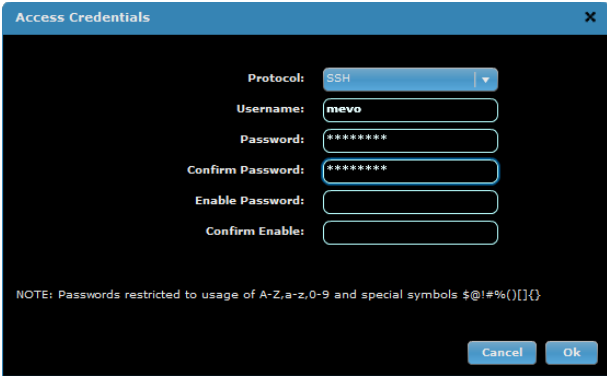
**Step 6:** In the **Username** box, enter the user name created in the ACS in "Configuring the Cisco ACS."

**Step 7:** Enter and confirm the password, and then click **OK**.



### Tech Tip

The account you created in ACS for MEVO to manage the aggregation devices is authorized at the enable prompt during login, so you don't have to enter a value in the enable password field.



The **Access Credentials** dialog box is shown with the following fields:

- Protocol:** SSH (dropdown menu)
- Username:** mevo
- Password:** (masked with asterisks)
- Confirm Password:** (masked with asterisks)
- Enable Password:** (empty field)
- Confirm Enable:** (empty field)

NOTE: Passwords restricted to usage of A-Z,a-z,0-9 and special symbols \$@!#%(){}.

Buttons: **Cancel** and **Ok**.

**Step 8:** Click the icon in the **Variables** field. The **SDP Registrar-Variables** window appears.

**Step 9:** In the **Certificate Authority HTTP Port** box, enter **8000**, which is the HTTP port previously configured for SCEP.

**Step 10:** In the **Certification Authority Archive Password** box, enter the PKI server archive password, configured previously on the SDP server. (Example: cisco123)

**Step 11:** In the **RADIUS IP Address** box, enter the IP address of the RADIUS server. (Example: 10.4.48.15) RADIUS is used for user authentication at the start of SDP processing.

**Step 12:** In the **RADIUS Ports** list, choose **1812/1813**. This step configures the RADIUS port pair for authentication and accounting.

**Step 13:** In the **RADIUS Server Key** box, enter the shared secret as configured on the RADIUS server, and then click **OK**. (Example: SecretKey)

**Step 14:** Click **Save Changes**. The **Task Details** window appears, and the **Status** field shows **Passed**.

**Step 15:** Close the **Task Details** window.

### Procedure 3 Integrate the Primary DMVPN Cloud

**Step 1:** To add a new DMVPN cloud, click **Add**. The **Add** dialog box appears.

**Step 2:** In the **Role** list, choose **DMVPN Cloud**, and then click **OK**.

**Step 3:** Select the **Secondary Data Gateway**, and then click **Delete**.

**Step 4:** For the Primary Data Gateway in the **Device Type** list, choose the model of the primary aggregation device. (Example: Cisco 3945 E)

**Step 5:** In the **Management IP** box, enter the loopback IP address of the primary aggregation device. (Example: 10.4.32.246)

**Step 6:** In the **Outside IP** box, enter the IP address of the primary aggregation device's outside interface. (Example: 172.16.130.2)

	Role	Device Type	Management IP	Outside IP	Passwords	Variables	Status
	SDP Registrar	Cisco 3945 E	10.4.32.246	172.16.130.2			Online
	DMVPN Cloud						
	Primary Data Gateway	Cisco 3945 E	10.4.32.246	172.16.130.2			

Next, enter the access credentials to the primary aggregation device.

**Step 7:** Click the icon in the **Passwords** field. The **Access Credentials** dialog box appears.

**Step 8:** In the **Username** box, enter the user name created in the ACS in "Configuring the Cisco ACS."

**Step 9:** Enter and confirm the password, and then click **OK**.

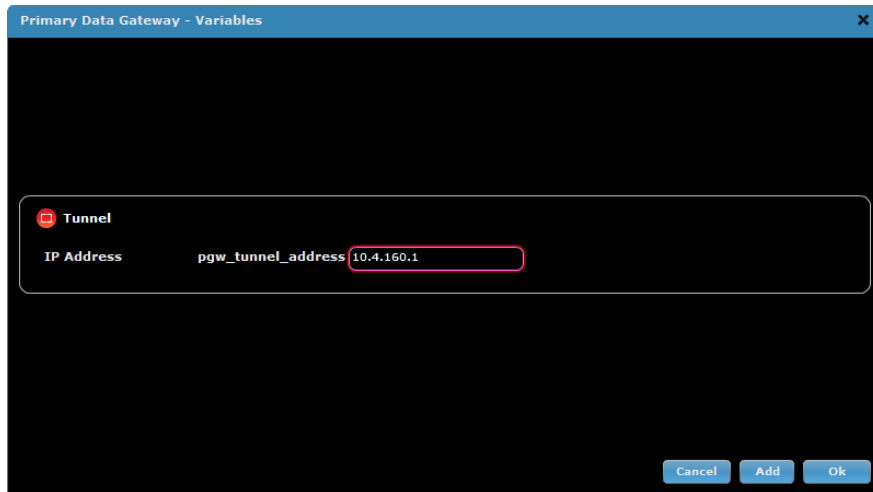


### Tech Tip

The account you created in ACS for MEVO to manage the aggregation devices is authorized at the enable prompt during login, so you don't have to enter a value in the enable password field.

**Step 10:** Click the icon in the **Variables** field. The **Primary Data Gateway–Variables** window appears.

**Step 11:** In the **IP Address** box, enter the IP address of the routers tunnel interface, and then click **OK**. (Example: 10.4.160.1)

The screenshot shows the 'Primary Data Gateway - Variables' window. It has a dark blue header with the title and a close button. The main area is dark gray. On the left, there's a sidebar with a red icon and the label 'Tunnel'. The main content area shows a table with one row: 'IP Address' with the value 'pgw\_tunnel\_address 10.4.160.1'. The value '10.4.160.1' is highlighted with a red border. At the bottom right, there are three buttons: 'Cancel', 'Add', and 'Ok'.

**Step 12:** For the **DMVPN Cloud**, click the icon in the **Variables** field. The **DMVPN Cloud–Variables** window appears.

**Step 13:** MEVO assigns an address to each CVO remote router tunnel interface from the tunnel network address. Enter the network address for the tunnel interfaces in the **Tunnel Network Address** box. (Example: 10.4.160.0)

**Step 14:** In the **Tunnel Subnet Mask** list, choose 255.255.254.0/23.

**Step 15:** In the **EIGRP AS** box, enter the EIGRP number of the DMVPN cloud. (Example: 202)

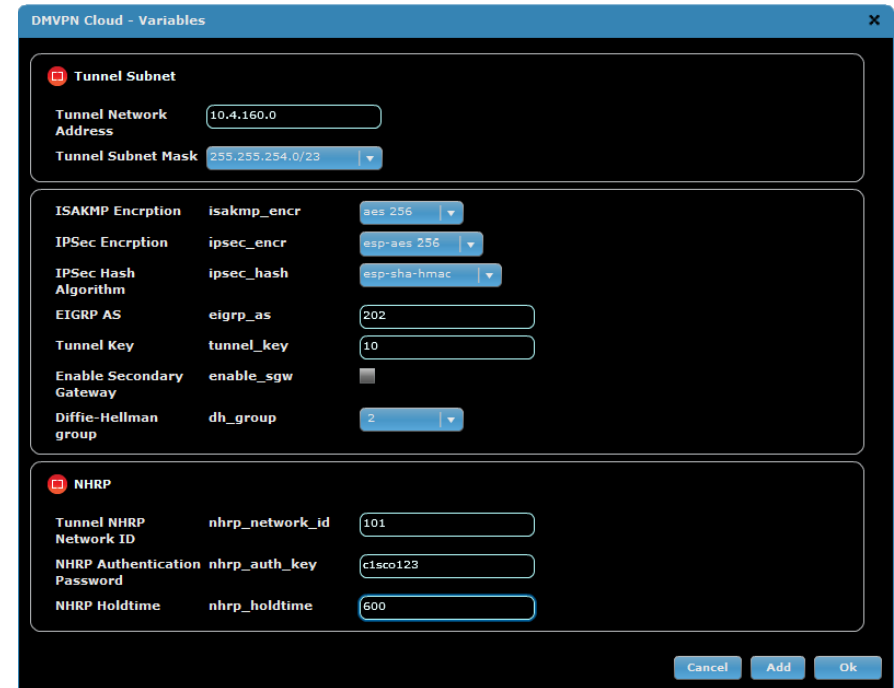
**Step 16:** In the **Tunnel Key** box, enter the key. (Example: 10)

**Step 17:** In the **Diffie-Hellman group** list, choose 2.

**Step 18:** In the **Tunnel NHRP Network ID** box, enter the NHRP ID. (Example: 101)

**Step 19:** In the **NHRP Authentication Password** box, enter the password. (Example: cisco123)

**Step 20:** In the **NHRP Holdtime** box, enter 600, and then click **OK**.

The screenshot shows the 'DMVPN Cloud - Variables' window. It has a dark blue header with the title and a close button. The main area is dark gray. On the left, there's a sidebar with a red icon and the label 'Tunnel Subnet'. The main content area is divided into two sections. The top section, 'Tunnel Subnet', has fields for 'Tunnel Network Address' (10.4.160.0) and 'Tunnel Subnet Mask' (255.255.254.0/23). The bottom section, 'NHRP', has fields for 'Tunnel NHRP Network ID' (101), 'NHRP Authentication Password' (cisco123), and 'NHRP Holdtime' (600). There are also fields for 'ISAKMP Encryption' (aes 256), 'IPSec Encryption' (esp-aes 256), 'IPSec Hash Algorithm' (esp-sha-hmac), 'EIGRP AS' (202), 'Tunnel Key' (10), 'Enable Secondary Gateway' (checkbox), and 'Diffie-Hellman group' (2). At the bottom right, there are three buttons: 'Cancel', 'Add', and 'Ok'.

**Step 21:** Click **Save Changes**. The **Task Details** window appears and the **Status** field shows as **Passed**.

**Step 22:** Close the **Task Details** window.

## Procedure 4

## Integrating the Resilient DMVPN Cloud

**Step 1:** Add a new DMVPN cloud. Click **Add**.

**Step 2:** In the **Role** list, choose **DMVPN Cloud**.

**Step 3:** Enter **2** in the **Group Suffix** box, and then click **OK**.

**Step 4:** Under **DMVPN Cloud (2)**, select the **Secondary Data Gateway**, and then click **Delete**.

**Step 5:** Under **DMVPN Cloud (2)**, for the Primary Data Gateway in the **Device Type** list, choose the model of the primary aggregation device. (Example: Cisco 3945 E)

**Step 6:** In the **Management IP** box, enter the loopback IP address of the resilient aggregation device. (Example: 10.4.32.247)

**Step 7:** In the **Outside IP** box, enter the IP address of the resilient aggregation device's outside interface. (Example: 172.17.130.2)

		Role	Device Type	Management IP	Outside IP	Passwords	Variables	Status
		SDP Registrar	Cisco 3945 E	10.4.32.246	172.16.130.2			Online
		DMVPN Cloud						
		Primary Data Gateway	Cisco 3945 E	10.4.32.246	172.16.130.2			Online
		DMVPN Cloud (2)						
		Primary Data Gateway ...	Cisco 3945 E	10.4.32.247	172.17.130.2			

**Step 8:** To enter the access credentials to the resilient aggregation device, click the icon in the **Passwords** field. The **Access Credentials** window appears.

**Step 9:** In the **Username** box, enter the username created in the ACS in "Configuring Cisco ACS."

**Step 10:** Enter and confirm the password, and then click **OK**.

### Tech Tip

The account you created in ACS for MEVO to manage the aggregation device is authorized at the enable prompt during login, so you don't have to enter a value in the enable password field.

**Step 11:** Click the icon in the **Variables** field. The **Primary Data Gateway-Variables** dialog box appears.

**Step 12:** In the **IP Address** box, enter the IP address of the tunnel interface, and then click **OK**. (Example 10.4.162.1)

**Step 13:** For the **DMVPN Cloud (2)**, click the icon in the **Variables** field. The **DMVPN Cloud–Variables** dialog box appears.

**Step 14:** In the **Tunnel Network Address** box, enter the network address of the tunnel. (Example: 10.4.162.0)

**Step 15:** In the **Tunnel Subnet Mask** list, choose **255.255.254.0/23**.

**Step 16:** In the **EIGRP AS** box, enter the EIGRP process number of the DMVPN cloud. (Example: 202)

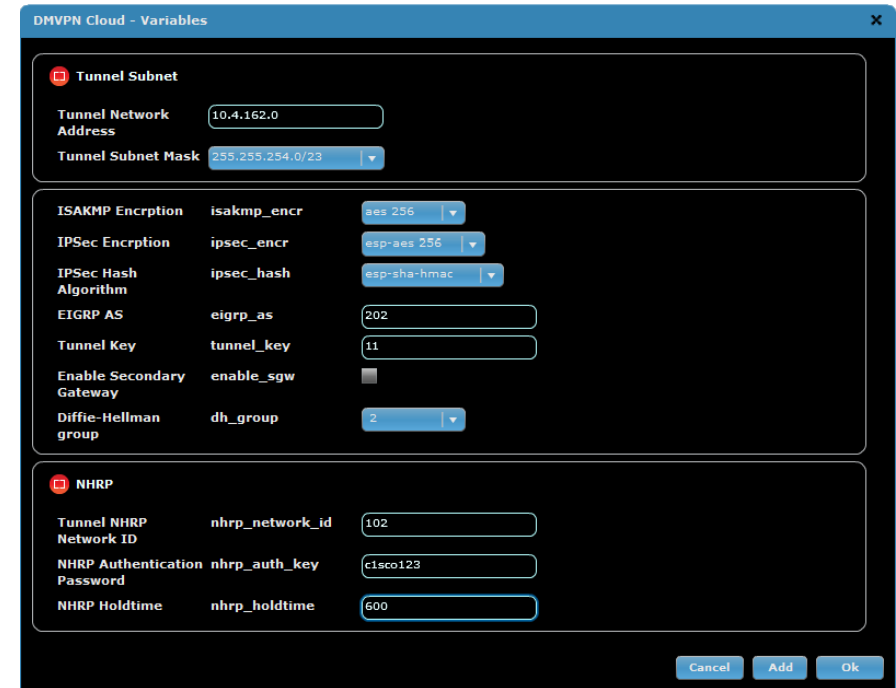
**Step 17:** Enter the tunnel key. (Example: 11)

**Step 18:** In the **Diffie-Hellman group** list, choose **2**.

**Step 19:** In the **Tunnel NHRP Network ID** box, enter the NHRP ID. (Example: 102)

**Step 20:** In the **NHRP Authentication Password** box, enter the password. (Example: cisco123)

**Step 21:** In the **NHRP Holdtime** box, enter **600**, and then click **OK**.



The image shows the 'DMVPN Cloud - Variables' dialog box. It is divided into two main sections: 'Tunnel Subnet' and 'NHRP'. The 'Tunnel Subnet' section contains fields for 'Tunnel Network Address' (10.4.162.0) and 'Tunnel Subnet Mask' (255.255.254.0/23). Below these are several encryption and algorithm settings: 'ISAKMP Encryption' (aes 256), 'IPSec Encryption' (esp-aes 256), 'IPSec Hash Algorithm' (esp-sha-hmac), 'EIGRP AS' (202), 'Tunnel Key' (11), 'Enable Secondary Gateway' (unchecked), and 'Diffie-Hellman group' (2). The 'NHRP' section contains fields for 'Tunnel NHRP Network ID' (102), 'NHRP Authentication Password' (cisco123), and 'NHRP Holdtime' (600). At the bottom right, there are three buttons: 'Cancel', 'Add', and 'Ok'.

Section	Variable	Value
Tunnel Subnet	Tunnel Network Address	10.4.162.0
	Tunnel Subnet Mask	255.255.254.0/23
	ISAKMP Encryption	aes 256
	IPSec Encryption	esp-aes 256
	IPSec Hash Algorithm	esp-sha-hmac
	EIGRP AS	202
	Tunnel Key	11
	Diffie-Hellman group	2
NHRP	Tunnel NHRP Network ID	102
	NHRP Authentication Password	cisco123
	NHRP Holdtime	600
	Enable Secondary Gateway	<input type="checkbox"/>

**Step 22:** Click **Save Changes**. The **Task Details** window appears, and the **Status** field shows **Passed**.

**Step 23:** Close the **Task Details** window.

## Procedure 5 Integrating MEVO into the Cisco ACS

**Step 1:** To integrate MEVO to ACS, click **Add**. The **Add** dialog box appears.

**Step 2:** In the **Role** list, choose **PKI-AAA Server**, and then click **OK**.

The **Add** dialog box has a title bar with a close button. It contains a **Role** dropdown menu set to **PKI-AAA Server** and a **Group Suffix** text input field. Below the input field is a note: "NOTE: Group Suffix restricted to usage of A-Z,a-z,0-9 and special symbols - and \_". At the bottom are **Cancel** and **Ok** buttons.

**Step 3:** For the PKI-AAA Server in the **Device Type** list, choose **Cisco ACS 5.x**.

**Step 4:** In the **Management IP** box, enter the IP address of the ACS server. (Example 10.4.48.15)

	Role	Device Type	Management IP	Outside IP	Passwords	Variables	Status
	SDP Registrar	Cisco 3945 E	10.4.32.246	172.16.130.2			Online
	DMVPN Cloud						
	Primary Data Gateway	Cisco 3945 E	10.4.32.246	172.16.130.2			Online
	DMVPN Cloud (2)						
	Primary Data Gateway ...	Cisco 3945 E	10.4.32.247	172.17.130.2			Online
	PKI-AAA Server	Cisco ACS 5.x	10.4.48.15				

Next, you enter the access credentials for the ACS server

**Step 5:** Click the icon in the **Passwords** field. The **Access Credentials** dialog box appears.

**Step 6:** In the **Username** box, enter the platform user name for ACS. (Example: admin)

**Step 7:** Enter and confirm the password.

**Step 8:** In the **Super Username** box, enter the web user name for ACS. (Example: acsadmin)

**Step 9:** Enter and confirm the password, and then click **OK**.

The **Access Credentials** dialog box has a title bar with a close button. It contains several fields: **Protocol** (SSH), **Username** (admin), **Password** (masked), **Confirm Password** (masked), **Super Username** (acsadmin), **Super User Password** (masked), and **Confirm Super User Password** (masked). At the bottom is a note: "NOTE: Passwords restricted to usage of A-Z,a-z,0-9 and special symbols \$@!#%()[]{}". At the bottom right are **Cancel** and **Ok** buttons.

**Step 10:** Click the icon in the **Variables** field. The **PKI-AAA Server-Variables** dialog box appears.

**Step 11:** In the **Server Ports** list, choose **1812/1813**.

**Step 12:** In the **Server Key** box, enter the RADIUS secret key, and then click **OK**. (Example SecretKey)

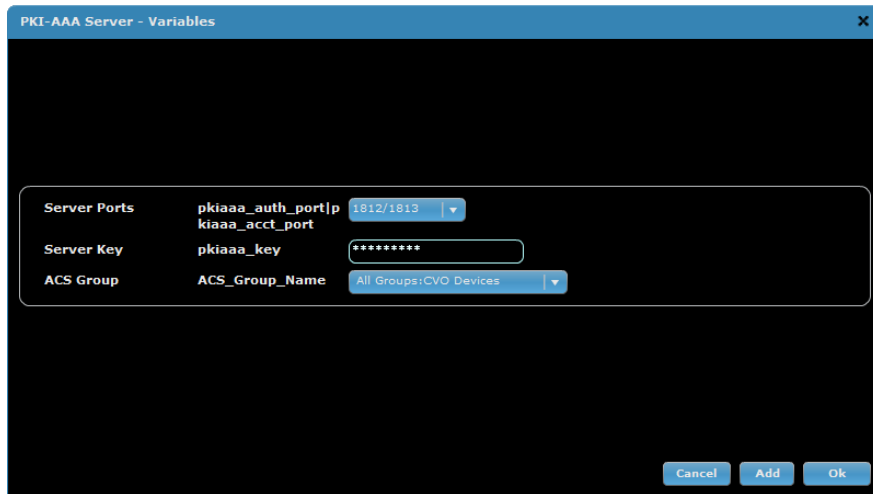
The **PKI-AAA Server - Variables** dialog box has a title bar with a close button. It contains two sections: **Server Ports** with a dropdown menu showing **pkiaaa\_auth\_port/pkiaaa\_acct\_port** and **1812/1813**, and **Server Key** with a text input field containing **pkiaaa\_key** and a masked password field. At the bottom right are **Cancel**, **Add**, and **Ok** buttons.

**Step 13:** Click **Save Changes**. The **Task Details** window appears, and the **Status** field shows **Passed**.

**Step 14:** Close the **Task Details** window closes.

**Step 15:** Click the icon in the **Variables** field. The **PKI-AAA Server-Variables** window appears.

**Step 16:** In the **ACS Group** list, choose **All Groups:CVO Devices**, and then click **OK**.

A screenshot of the 'PKI-AAA Server - Variables' window. It has a blue header bar with the title and a close button. The main area is dark gray with a white border around the configuration fields. There are four rows of fields: 'Server Ports' with 'pkiaaa\_auth\_port/p' set to '1812/1813' and 'kiaaa\_acct\_port' empty; 'Server Key' with 'pkiaaa\_key' set to '\*\*\*\*\*'; and 'ACS Group' with 'ACS\_Group\_Name' set to 'All Groups:CVO Devices'. At the bottom are 'Cancel', 'Add', and 'Ok' buttons.

**Step 17:** Click **Save Changes**. The **Task Details** window will appear and the **Status** field shows **Passed**.

**Step 18:** Close the **Task Details** window.

## Procedure 6 Configure Variables for the Remote Site

**Step 1:** Navigate to **Configuration > Remote End**.

Here, you define the local access credentials on the CVO remote router.

**Step 2:** In the **Management User** box, enter a user name. (Example: admin)

**Step 3:** In the **Management Password** box, enter a password for the user. (Example: cisco123)

**Step 4:** If you want to allow users to escalate their privilege levels on the CVO remote router, in the **Enable Secret** box, enter a password.

**Step 5:** In the **Domain Name** box, enter the organization's DNS domain. (Example: cisco.local)

**Step 6:** In the **DNS IP Address** box, enter the organization's primary DNS server IP address. (Example: 10.4.48.10)

**Step 7:** In the **Wireless SSID** box, enter the name of the organization's wireless LAN that supports data. (Example: WLAN-Data)

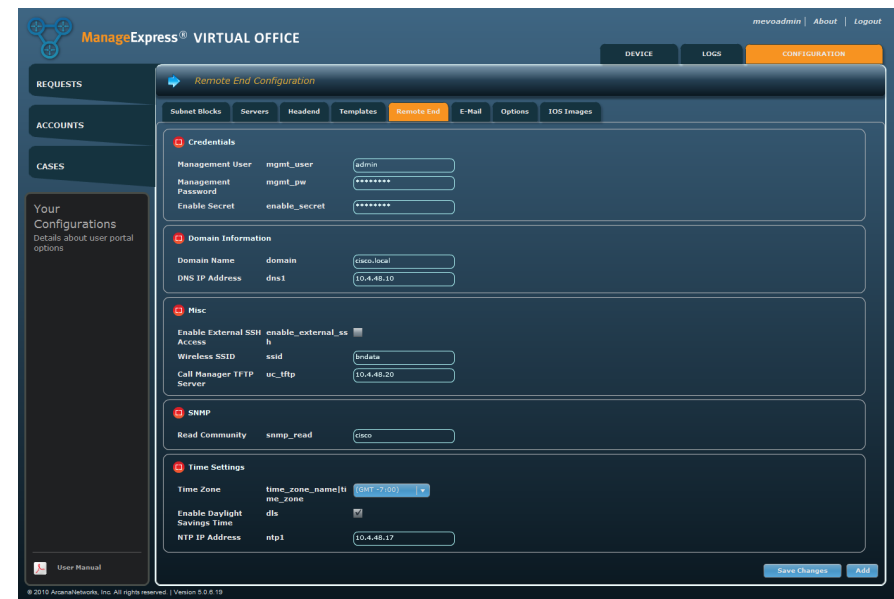
**Step 8:** In the **Call Manager TFTP Server** box, enter the IP address of the organization's Cisco UCM TFTP Server. (Example: 10.4.48.20)

**Step 9:** In the **Read Community** box, enter the read-only SNMP community string. (Example: cisco)

**Step 10:** In the **Time Zone** list, choose **(GMT -8:00)**.

**Step 11:** Select **Enable Daylight Savings Time**.

**Step 12:** Enter the NTP server IP address in the **NTP IP Address** box, and then click **Save Changes**. (Example: 10.4.48.17)

A screenshot of the 'ManageExpress VIRTUAL OFFICE' web interface. The 'Remote End Configuration' window is open, showing various configuration sections. The 'Credentials' section has fields for 'Management User' (mgmt\_user), 'Management Password' (mgmt\_pw), and 'Enable Secret' (enable\_secret). The 'Domain Information' section has 'Domain Name' (domain) and 'DNS IP Address' (dns1). The 'Misc' section has 'Enable External SSH Access' (enable\_external\_ssh), 'Wireless SSID' (ssid), and 'Call Manager TFTP Server' (uc\_http). The 'SNMP' section has 'Read Community' (snmp\_read). The 'Time Settings' section has 'Time Zone' (time\_zone\_name), 'Enable Daylight Savings Time' (dls), and 'NTP IP Address' (ntp1). At the bottom are 'Save Changes' and 'Add' buttons.

## Procedure 7 Activate CVO Remote Templates

First, add the resilient DMVPN cloud template into MEVO from Appendix B.

**Step 1:** Save the CLI from Appendix B as a file on your local machine.

**Step 2:** Navigate to **Configuration > Templates**.

**Step 3:** In the **Filter by Router Type** list, choose **Cisco 881**, and then click **Add**.

**Step 4:** In the **Type** list, choose **DMVPN Configuration**.

**Step 5:** In the **Device Type** list, choose **Cisco 881**.

**Step 6:** In the **Template File** box, select the file you created in Step 1, and then click **OK**.

**Step 7:** Select **Active** for the Wireless, Firewall, QoS, and DMVPN Configuration template you added in Step 6, and then click **Save**.

	Type	Device Type	Filename	Access Point	Active	Edit
<input type="checkbox"/>	Base Configuration	Cisco 881	1-step-881.cfg	No	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Wireless Configuration	Cisco 881	wireless-881.cfg	Yes	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	EEM Configuration	Cisco 881	EEM-881.cfg	No	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Authproxy Configuration	Cisco 881	authproxy-881.cfg	No	<input type="checkbox"/>	
<input type="checkbox"/>	Firewall Configuration	Cisco 881	classicfw-881.cfg	No	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Dot1x Configuration	Cisco 881	dot1x-881.cfg	No	<input type="checkbox"/>	
<input type="checkbox"/>	QOS Configuration	Cisco 881	qos-881.cfg	No	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	DMVPN Configuration	Cisco 881	New DMVPN Configuration	No	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	DMVPN Configuration	Cisco 881	dmvpn-881.cfg	No	<input type="checkbox"/>	

**Step 8:** In the confirmation window, click **Save**.

## Procedure 8 Configure the Email Server

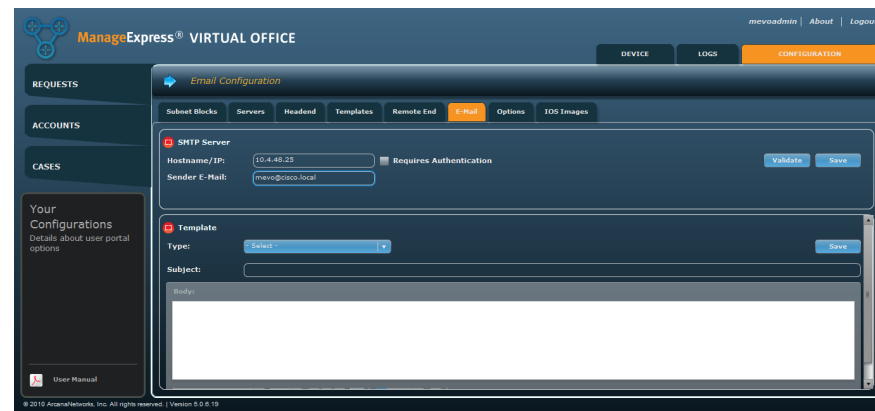
To ease the approval and deployment of CVO, ArcanaNetworks MEVO automatically generates email messages for CVO approvers and users during the provisioning process.

Configure the SMTP server to send mail.

**Step 1:** Navigate to **Configuration > E-mail**.

**Step 2:** In the **Hostname/IP** box, enter the hostname or IP address of the organization's SMTP server. (Example: 10.4.48.25)

**Step 3:** In the **Sender E-Mail** box, enter the email address that automated MEVO messages should be sent from, and then click **Save**. (Example: mevo@cisco.local)



## Procedure 9 Create End Users

Four roles are included in the typical Cisco Virtual Office deployment with ArcanaNetworks MEVO:

- **Administrator**—This role configures and maintains ArcanaNetworks MEVO. This role may also manage users and ArcanaNetworks MEVO accounts. If the Administrator requests Cisco Virtual Office service on behalf of the user, a manager approval is not required.
- **End user**—This role includes the teleworker.
- **Manager or approver**—This role approves or declines an end user's request for Cisco Virtual Office in the typical Cisco Virtual Office deployment workflow.
- **Requestor**—This role requests Cisco Virtual Office service on behalf of the end user but does not have ArcanaNetworks MEVO administrator privileges. This role is optional; end users can request their own services if corporate policies permit.

All end users must have a manager attached to their accounts.

**Step 1:** Navigate to the **Accounts** tab, and then click **Create User**.

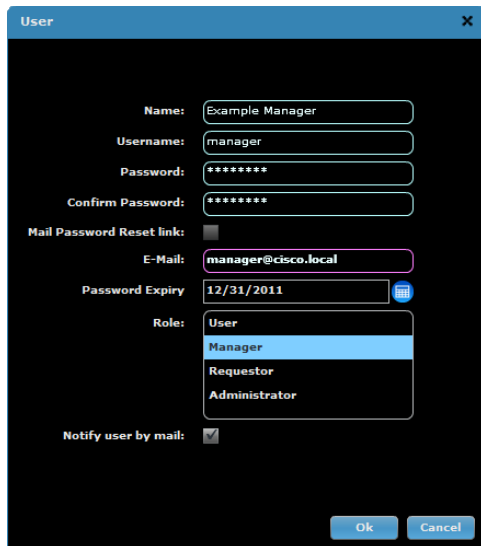
**Step 2:** Enter the manager's name. (Example: Example Manager)

**Step 3:** Enter the manager's user name. (Example: manager)

**Step 4:** Enter and confirm the password.

**Step 5:** Enter the manager's email address. (Example: manager@cisco.local)

**Step 6:** In the **Role** list choose **Manager**, and then click **OK**.



Next, create an end user for CVO provisioning.

**Step 7:** Click **Create User**.

**Step 8:** Enter the user's name. (Example: Employee One)

**Step 9:** Enter the user's user name. (Example: employee1)

**Step 10:** Enter and confirm the password.

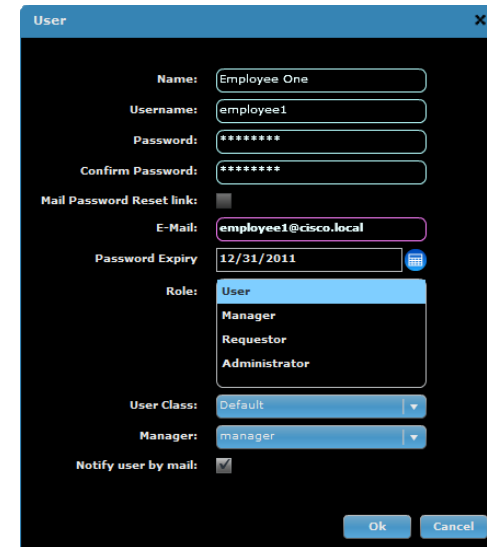
**Step 11:** Enter the user's email address. (Example: employee1@cisco.local)

**Step 12:** In the **Role** list, choose **User**.

**Step 13:** In the **User Class** list, choose **Default**.

**Step 14:** In the **Manager** list, choose the user name created in Step 3. (Example: manager)

**Step 15:** If you want to send the user an email with instructions on how to start the Secure Device Provisioning (SDP) after that user is provisioned, select **Notify user by mail**, and then click **OK**.



## Procedure 10

## Provision End Users

This procedure describes the SDP process from the end-user's perspective and shows what needs to be done after the user receives the router at the remote location. Typically, the end user receives a router with factory-default settings, instructions for setup, and an email to access the provisioning page (described in more detail in the steps that follow).

The steps presented here assume that the user has an Internet connection with DHCP. Variations such as connection through DSL or a static IP address are also possible with a few modifications, but the basic steps that the end-user performs remain the same.

The MEVO administrator can create a provisioning request on behalf of the end user.

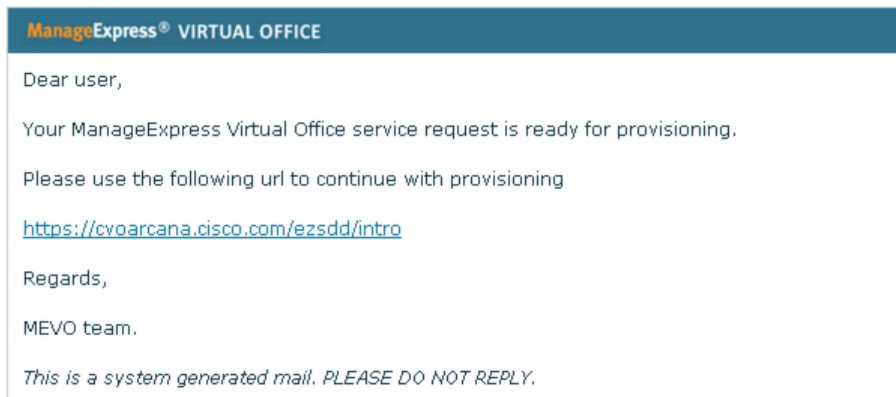
**Step 1:** Navigate to the **Accounts** tab.

**Step 2:** Select the user for which you want to provision a CVO remote router, and then click **New Request**.

**Step 3:** On the **ISP Information** panel, in the **Technology** list, choose the correct Internet connection method for CVO remote. (Example: Cable)

**Step 4:** To enable proper prioritization of voice traffic as it leaves the remote site, in the **Upload Speed** list, choose the correct uplink speed for CVO remote. (Example: 1Mbps)

**Step 5:** After the configuration is generated on ArcanaNetworks MEVO, the end user will get an email similar to the one shown below with a link to start the SDP process. Click the link to continue.



**Step 6:** When the pop-up screen asks for user credentials, enter the appropriate AAA credentials.

**Step 7:** Click **Next** on the welcome screen.



ArcanaNetworks MEVO connects to the router to begin configuration.

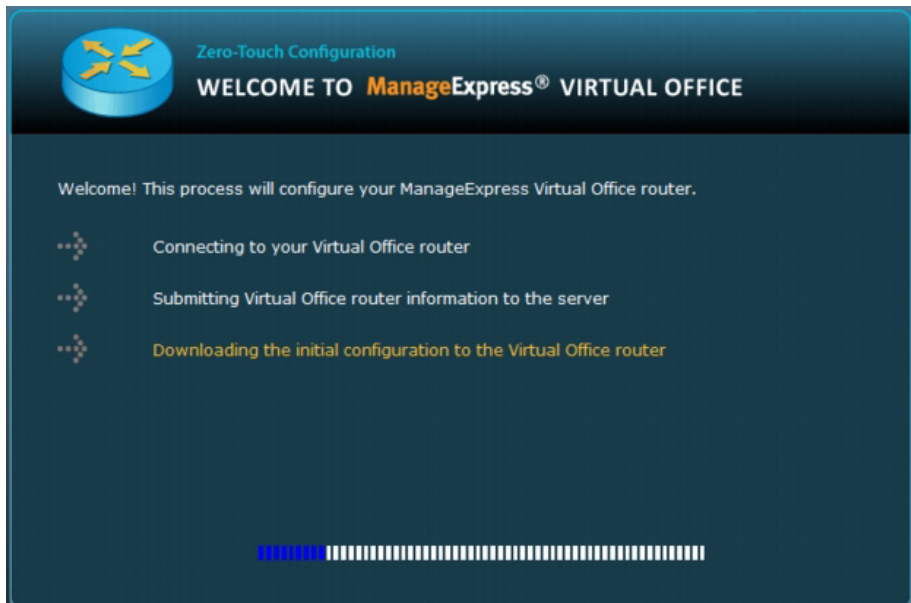




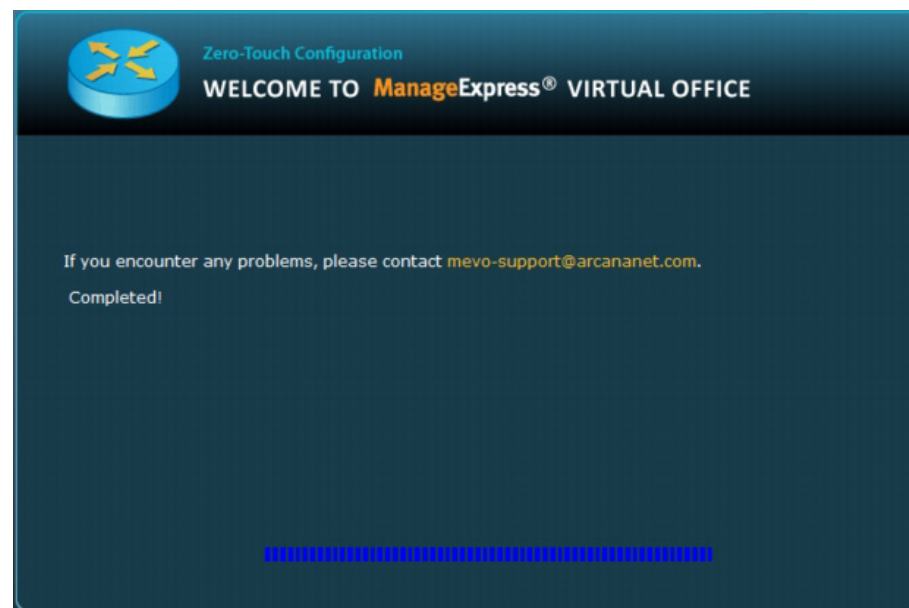
## Tech Tip

Enter the user name **cisco** and the password **cisco** if you are asked for the router login credentials.

The configuration is downloaded automatically to the router.



When the process is finished, the router is fully configured with access to the corporate network.



## Procedure 11

## Deploying Authentication Proxy

**Step 1:** Navigate to the **Device** tab.

**Step 2:** Click the portion of the graph labeled **Online**.

**Step 3:** In the list of devices, select the CVO remote site that was just provisioned.

**Step 4:** At the bottom of the page in the action list, choose **Apply Templates**, and then click **Go**.

**Step 5:** Select **Authproxy Configuration**, and then click **Next**.

Apply Templates				X
	Type	Device Type	Filename	Post SDP
<input type="checkbox"/>	Base Configuration	Cisco 881	1-step-881.cfg	No
<input type="checkbox"/>	Wireless Configuration	Cisco 881	wireless-881.cfg	Yes
<input type="checkbox"/>	EEM Configuration	Cisco 881	EEM-881.cfg	No
<input checked="" type="checkbox"/>	Authproxy Configuration	Cisco 881	authproxy-881.cfg	No
<input type="checkbox"/>	Firewall Configuration	Cisco 881	classicfw-881.cfg	No
<input type="checkbox"/>	Dot1x Configuration	Cisco 881	dot1x-881.cfg	No
<input type="checkbox"/>	QOS Configuration	Cisco 881	qos-881.cfg	No
<input type="checkbox"/>	DMVPN Configuration	Cisco 881	New DMVPN Configuration.txt	No
<input type="checkbox"/>	DMVPN Configuration	Cisco 881	dmpvpn-881.cfg	No
				Close Next

**Step 6:** Select **Start Immediately**, and then click **Next**. The template is deployed when the Status field shows **Passed**.

**Step 7: Click Close.**

## Notes

# Appendix A: Product List

The following products and software versions have been validated for the Cisco Smart Business Architecture.

Functional area	Product	Part numbers	Software version
Internet Edge Firewall	Adaptive Security Appliance ASA 5540 with the SSM-40 IPS Module ASA 5520 with the SSM-20 IPS Module ASA 5510 with the SSM-10 IPS Module	ASA5540-AIP40-K9 L-ASA-AC-PH-5540= ASA5520-AIP20-K9 L-ASA-AC-PH-5520= ASA5510-AIP10-K9 L-ASA-AC-PH-5510=	8.4.2 7.0.(5a)E4
Remote Site Appliance	Adaptive Security Appliance 5505	ASA5505-BUN-K9	8.4.2
OfficeExtend	5508 Wireless LAN Controller	AIR-CT5508-100-K9 5508 Wireless LAN Controller with 100 AP license	7.1.91.0
OfficeExtend	600 Series AP	AIR-OEAP602I-A-K9	7.1.91.0
DMZ Switch	Catalyst 3750X	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image	15.0(1)SE1
Distribution Layer	Catalyst 3750X Stackable 12 Port SFP	WS-C3750X-12S-S Catalyst 3750 12 SFP + IPS Image	15.0(1)SE1

Functional area	Product	Part numbers	Software version
Distribution Layer	Catalyst 4507R+E Dual Supervisors Dual Power Supplies	WS-C4507R+E Catalyst 4500 E-Series 7-Slot Chassis with 48Gbps per Slot WS-X45-SUP7-E Catalyst 4500 E-Series Supervisor, 848Gbps WS-X4624-SFP-E Catalyst 4500 E-Series 24-Port GE (SFP) WS-X4712-SFP+E Catalyst 4500 E-Series 12-Port 10GbE (SFP+)	15.0(2)SG1
Distribution Layer	Catalyst 6500 VSS	WS-C6506-E Catalyst 6500 E-Series 6-Slot Chassis VS-S2T-10G Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE WS-X6724-SFP Catalyst 6500 24-port GigE Mod (SFP) WS-X6816-10G-2T Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC4	15.0(1)SY
CVO Aggregation: DMVPN Hub Router	Cisco 3945E	CISCO3945E/K9 SL-39-DATA-K9 C3900-SPE250/K9 PWR-3900-AC	15.1(4)M2
CVO Management	ArcanaNetworks MEVO	L-SP-MESYSTEM= L-SP-MEBASE-B-100= L-SP-MEVO-100=	11.0.0.2
CVO Remote Site Router	Cisco 881W	CISCO881W-GN-A-K9 800-IL-PM-2 CVO800-CFG	15.1(4)M2

# Appendix B: Resilient DMVPN Template

```
ip pim autorp listener
!
ip route $pgw_outside_address$ 255.255.255.255 dhcp
#if ($enable_sgw$ == "true")
    ip route $sgw_outside_address$ 255.255.255.255 dhcp
#end

#if ($ADDR_SCHEME$ == "static")
    no ip route $pgw_outside_address$ 255.255.255.255 dhcp
    ip route $pgw_outside_address$ 255.255.255.255 $DEF_GW$
    #if ($enable_sgw$ == "true")
        no ip route $sgw_outside_address$ 255.255.255.255 dhcp
        ip route $sgw_outside_address$ 255.255.255.255 $DEF_GW$
    #end
#end

ip route $pgw_outside_address_2$ 255.255.255.255 dhcp
#if ($enable_sgw_2$ == "true")
    ip route $sgw_outside_address_2$ 255.255.255.255 dhcp
#end

#if ($ADDR_SCHEME$ == "static")
    no ip route $pgw_outside_address_2$ 255.255.255.255 dhcp
    ip route $pgw_outside_address_2$ 255.255.255.255 $DEF_GW$
    #if ($enable_sgw_2$ == "true")
        no ip route $sgw_outside_address_2$ 255.255.255.255 dhcp
        ip route $sgw_outside_address_2$ 255.255.255.255 $DEF_GW$
    #end
#end
```

```
crypto isakmp policy 1
    encr $isakmp_encr$
    group $dh_group$

crypto isakmp keepalive 10
crypto isakmp nat keepalive 10

crypto ipsec transform-set t1 $ipsec_encr$ $ipsec_hash$
    mode transport require

crypto ipsec profile cvo
    set transform-set t1

no ip igmp snooping
ip multicast-routing

interface Tunnel0
    description DMVPN phase 3
    bandwidth 1000
    ip address $TUNNEL_IP_ADDRESS$ $tunnel_subnet$
    no ip redirects
    ip mtu 1400
    ip pim sparse-mode
    ip pim dr-priority 0
    ip nhrp map multicast $pgw_outside_address$
    ip nhrp map $pgw_tunnel_address$ $pgw_outside_address$
    ip nhrp nhs $pgw_tunnel_address$
    #if ($enable_sgw$ == "true")
        ip nhrp map multicast $sgw_outside_address$
        ip nhrp map $sgw_tunnel_address$ $sgw_outside_address$
        ip nhrp nhs $sgw_tunnel_address$
    #end
    ip nhrp authentication $nhrp_auth_key$
    ip nhrp network-id $nhrp_network_id$
    ip nhrp holdtime $nhrp_holdtime$
    ip nhrp registration no-unique
    ip nhrp shortcut
```

```

ip nhrp redirect
ip tcp adjust-mss 1360
load-interval 30
delay 1000
qos pre-classify
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key $tunnel_key$
tunnel protection ipsec profile cvo shared

interface Tunnel1
description DMVPN phase 3
bandwidth 1000
ip address $TUNNEL_IP_ADDRESS_2$ $tunnel_subnet_2$
no ip redirects
ip mtu 1400
ip pim sparse-mode
ip pim dr-priority 0
ip nhrp map multicast $pgw_outside_address_2$
ip nhrp map $pgw_tunnel_address_2$ $pgw_outside_address_2$
ip nhrp nhs $pgw_tunnel_address_2$
#if ($enable_sgw$ == "true")
    ip nhrp map multicast $sgw_outside_address_2$
    ip nhrp map $sgw_tunnel_address$ $sgw_outside_address_2$
    ip nhrp nhs $sgw_tunnel_address_2$
#end
ip nhrp authentication $nhrp_auth_key_2$
ip nhrp network-id $nhrp_network_id_2$
ip nhrp holdtime $nhrp_holdtime_2$
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
ip tcp adjust-mss 1360
load-interval 30
delay 1000
qos pre-classify
tunnel source FastEthernet4

```

```

tunnel mode gre multipoint
tunnel key $tunnel_key_2$
tunnel protection ipsec profile cvo shared

ip access-list standard dmvpn_acl
permit $LAN_IP_ADDRESS$ $LAN_INVERSE_SUBNET$

router eigrp $eigrp_as$
no auto-summary
network $TUNNEL_IP_ADDRESS$ 0.0.0.0
network $TUNNEL_IP_ADDRESS_2$ 0.0.0.0
network $LAN_IP_ADDRESS$ 0.0.0.0
distribute-list dmvpn_acl out

```

# Appendix C: Configuration Files

## IE-ASA5540

```
ASA Version 8.4(2)
!
terminal width 511
hostname IE-ASA5540
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
  summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
  description Trunk to DMZ-3750X GigabitEthernet X/0/24
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/1.1116
  description Web server DMZ connection on VLAN 1116
  vlan 1116
  nameif dmz-web
  security-level 50
  ip address 192.168.16.1 255.255.255.0 standby 192.168.16.2
!
```

```
interface GigabitEthernet0/1.1117
  description Email Security Appliance DMZ Connection on VLAN 1117
  vlan 1117
  nameif dmz-mail
  security-level 50
  ip address 192.168.17.1 255.255.255.0 standby 192.168.17.2
!
interface GigabitEthernet0/1.1118
  description DMVPN aggregation router conenctons on VLAN 1118
  vlan 1118
  nameif dmz-dmvpn
  security-level 75
  ip address 192.168.18.1 255.255.255.0 standby 192.168.18.2
!
interface GigabitEthernet0/1.1119
  vlan 1119
  nameif dmz-wlc
  security-level 50
  ip address 192.168.19.1 255.255.255.0
!
interface GigabitEthernet0/1.1123
  description Management DMZ connection on VLAN 1123
  vlan 1123
  nameif dmz-management
  security-level 50
  ip address 192.168.23.1 255.255.255.0 standby 192.168.23.2
!
interface GigabitEthernet0/1.1128
  vlan 1128
  nameif dmz-guest
  security-level 10
  ip address 192.168.28.1 255.255.252.0
!
interface GigabitEthernet0/2
  description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
```

```

description Trunk to OUT-2960S GigabitEthernet X/0/24
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3.16
description Primary Internet connection on VLAN 16
vlan 16
nameif outside-16
security-level 0
ip address 172.16.130.124 255.255.255.0 standby 172.16.130.123
!
interface GigabitEthernet0/3.17
description Resilient Internet connection on VLAN 17
vlan 17
nameif outside-17
security-level 0
ip address 172.17.130.124 255.255.255.0 standby 172.17.130.123
!
interface Management0/0
shutdown
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
domain-name cisco.local
same-security-traffic permit intra-interface
object network internal-network
subnet 10.4.0.0 255.254.0.0
description The organization's internal network range
object network dmz-networks
subnet 192.168.16.0 255.255.248.0

```

```

description The organization's DMZ network range
object network internal-network-ISPa
subnet 10.4.0.0 255.254.0.0
description PAT traffic from inside out the primary internet
connection
object network internal-network-ISPb
subnet 10.4.0.0 255.254.0.0
description PAT traffic from inside out the resilient internet
connection
object network outside-webserver-ISPa
host 172.16.130.100
description Webserver on ISP A
object network dmz-webserver-ISPa
host 192.168.16.100
description NAT the webserver in the DMZ to the outside address
on ISP A
object network dmz-webserver-ISPb
host 192.168.16.100
description NAT the webserver in the DMZ to the outside address
on ISP B
object network outside-webserver-ISPb
host 172.17.130.100
description Webserver on ISP B
object network NETWORK_OBJ_10.4.28.0_22
subnet 10.4.28.0 255.255.252.0
object network outside-esa-ISPa
host 172.16.130.25
description ESA on ISP A
object network dmz-esa-ISPa
host 192.168.17.25
description NAT the ESA in the DMZ to the outside address on ISP
A
object network internal-dns
host 10.4.48.10
description DNS in the internal data center
object network internal-exchange
host 10.4.48.25

```

```

description Exchange server in the internal data center
object network internal-ntp
  host 10.4.48.17
description NTP server in the internal data center
object network outside-dmvpn-ISPa
  host 172.16.130.1
description DMVPN aggregation router on ISP A
object network dmz-dmvpn-1
  host 192.168.18.10
description NAT the primary DMVPN aggregation router in the DMZ
to ISP A
object network dmz-dmvpn-2
  host 192.168.18.11
description NAT the resilient DMVPN aggregation router in the
DMZ to ISP B
object network outside-dmvpn-ISPB
  host 172.17.130.1
description Resilient DMVPN aggregation router on ISP B
object network dmz-guest-network-ISPa
  subnet 192.168.28.0 255.255.252.0
object network dmz-wlc-guest-1
  host 192.168.19.10
description Guest Anchor Wireless LAN Controller
object network internal-flex7500-1
  host 10.4.46.66
object network internal-flex7500-2
  host 10.4.46.67
object network internal-wlc-1
  host 10.4.46.64
object network internal-wlc-2
  host 10.4.46.65
object network internal-acs
  host 10.4.48.15
description Internal ACS server
object network dmz-wlc-1
  host 192.168.19.20
description Primary WLC to Support Office Extend APs

```

```

object network outside-wlc-1
  host 172.16.130.20
description WLC to support Office Extend APs on ISP A
object network dmz-cvo-1
  host 192.168.18.20
description Primary Router to Support CVO
object network outside-cvo-1
  host 172.16.130.2
description Aggregation Router to Support CVO on ISP A
object network 5505-pool
  subnet 10.4.156.0 255.255.252.0
description 5505 Teleworker Subnet
object-group service DM_INLINE_SERVICE_1
  service-object tcp destination eq ftp
  service-object tcp destination eq ftp-data
  service-object tcp destination eq tacacs
  service-object udp destination eq ntp
  service-object udp destination eq syslog
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_2
  service-object tcp destination eq domain
  service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_1
  network-object 10.0.0.0 255.0.0.0
  network-object 172.16.0.0 255.255.0.0
  network-object 192.168.0.0 255.255.0.0
object-group service DM_INLINE_SERVICE_3
  service-object esp
  service-object udp destination eq 4500
  service-object udp destination eq isakmp
object-group icmp-type DM_INLINE_ICMP_1
  icmp-object echo
  icmp-object echo-reply
object-group service DM_INLINE_TCP_2 tcp
  port-object eq www

```

```

port-object eq https
object-group service DM_INLINE_TCP_3 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_SERVICE_4
service-object tcp destination eq 1025
service-object tcp destination eq 135
service-object udp destination eq 389
service-object udp destination eq domain
service-object tcp destination eq 445
service-object tcp destination eq 49158
object-group service DM_INLINE_TCP_4 tcp
port-object eq www
port-object eq https
object-group network internal-wlcs
description All internal wireless LAN controllers
network-object object internal-flex7500-1
network-object object internal-flex7500-2
network-object object internal-wlc-1
network-object object internal-wlc-2
object-group service DM_INLINE_SERVICE_5
service-object tcp destination eq tacacs
service-object udp destination eq 1812
service-object udp destination eq 1813
object-group service DM_INLINE_SERVICE_6
service-object 97
service-object udp destination eq 16666
object-group service DM_INLINE_TCP_5 tcp
port-object eq ftp
port-object eq ftp-data
object-group network DM_INLINE_NETWORK_2
network-object object dmz-networks
network-object object internal-network
object-group service DM_INLINE_SERVICE_7
service-object tcp destination eq domain
service-object udp destination eq bootps
service-object udp destination eq domain

```

```

object-group service DM_INLINE_TCP_6 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_7 tcp
port-object eq 8080
port-object eq 8443
object-group service DM_INLINE_SERVICE_8
service-object tcp
service-object tcp destination eq tacacs
service-object udp destination eq 1812
service-object udp destination eq 1813
object-group service DM_INLINE_UDP_1 udp
port-object eq 5246
port-object eq 5247
object-group service DM_INLINE_SERVICE_9
service-object esp
service-object tcp destination eq https
service-object udp destination eq 4500
service-object udp destination eq isakmp
service-object tcp destination eq 3389
access-list global_access remark Permit management protocols from
the DMZ to the internal network
access-list global_access extended permit object-group DM_INLINE
SERVICE_1 192.168.23.0 255.255.255.0 object internal-network
access-list global_access remark Allow anyone to access the
webserver in the DMZ
access-list global_access extended permit tcp any 192.168.16.0
255.255.255.0 object-group DM_INLINE_TCP_1
access-list global_access remark Permit the mail DMZ to sync with
the internal NTP server
access-list global_access extended permit udp 192.168.17.0
255.255.255.0 object internal-ntp eq ntp
access-list global_access remark Permit the mail DMZ to do
lookups on the internal DNS
access-list global_access extended permit object-group DM_INLINE
SERVICE_2 192.168.17.0 255.255.255.0 object internal-dns
access-list global_access remark Permit the mail DMZ to send SMTP

```

```

to the internal exchange server
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 object internal-exchange eq smtp
access-list global_access remark Permit SMTP traffic into the
email DMZ
access-list global_access extended permit tcp any 192.168.17.0
255.255.255.0 eq smtp
access-list global_access remark Allow diagnostic traffic to the
DMVPN aggregation routers
access-list global_access extended permit icmp any 192.168.18.0
255.255.255.0 object-group DM_INLINE_ICMP_1
access-list global_access remark Allow traffic to the DMVPN
aggregation routers
access-list global_access extended permit object-group DM_INLINE
SERVICE_3 any 192.168.18.0 255.255.255.0
access-list global_access extended permit tcp 192.168.28.0
255.255.252.0 192.168.16.0 255.255.255.0 object-group DM_INLINE
TCP_6
access-list global_access extended permit object-group DM_INLINE
SERVICE_7 192.168.28.0 255.255.252.0 object internal-dns
access-list global_access remark Deny traffic for the guest
network to internal and dmz resources
access-list global_access extended deny ip 192.168.28.0
255.255.252.0 object-group DM_INLINE_NETWORK_2
access-list global_access remark Allow guest traffic to the
internet
access-list global_access extended permit ip 192.168.28.0
255.255.252.0 any
access-list global_access extended permit udp 192.168.19.0
255.255.255.0 object internal-dns eq bootps
access-list global_access extended permit object-group DM_INLINE
SERVICE_6 192.168.19.0 255.255.255.0 object-group internal-wlcs
access-list global_access remark Allow WLCs to download via FTP
from internal servers
access-list global_access extended permit tcp 192.168.19.0
255.255.255.0 object internal-network object-group DM_INLINE
TCP_5

```

```

access-list global_access remark Allow WLCs to communicate with
the internal NTP server
access-list global_access extended permit udp 192.168.19.0
255.255.255.0 object internal-ntp eq ntp
access-list global_access remark Allow WLCs to communicate with
the AAA server
access-list global_access extended permit object-group DM_INLINE
SERVICE_5 192.168.19.0 255.255.255.0 object internal-acs
access-list global_access remark Allow traffic to the DMZ DMVPN
aggregation routers
access-list global_access extended permit object-group DM_INLINE
SERVICE_9 any 192.168.18.0 255.255.255.0
access-list global_access remark Deny traffic from any DMZ
network
access-list global_access extended deny ip object dmz-networks
any
access-list global_access remark Deny the use of telnet from the
internal network to external networks
access-list global_access extended deny tcp object internal-
network any eq telnet
access-list global_access remark Permit IP traffic from the
internal network to external networks
access-list global_access extended permit ip object internal-
network any log disable
access-list global_access extended permit udp any object dmz-
wlc-1 object-group DM_INLINE_UDP_1
access-list global_mpc extended permit ip any any
access-list RA_PartnerACL remark Partners can access this
internal host only
access-list RA_PartnerACL standard permit host 10.4.48.35
access-list RA_SplitTunnelACL remark Internal networks
access-list RA_SplitTunnelACL standard permit 10.4.0.0
255.254.0.0
access-list RA_SplitTunnelACL remark DMZ networks
access-list RA_SplitTunnelACL standard permit 192.168.16.0
255.255.248.0
access-list WCCP_Redirect remark Do not WCCP redirect connections

```

```

to these addresses
access-list WCCP_Redirect extended deny ip any object-group DM
  INLINE_NETWORK_1
access-list WCCP_Redirect remark WCCP redirect all other IP
addresses
access-list WCCP_Redirect extended permit ip any any
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu dmz-web 1500
mtu dmz-mail 1500
mtu dmz-dmvpn 1500
mtu dmz-wlc 1500
mtu dmz-management 1500
mtu dmz-guest 1500
mtu outside-16 1500
mtu outside-17 1500
mtu management 1500
ip local pool RA-pool 10.4.28.1-10.4.31.255 mask 255.255.252.0
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.33 255.255.255.224 standby
10.4.24.34
monitor-interface dmz-web
monitor-interface dmz-mail
monitor-interface dmz-dmvpn
monitor-interface dmz-management
monitor-interface outside-16
monitor-interface outside-17

```

```

icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (inside,outside-16) source static any any destination static
  NETWORK OBJ 10.4.28.0 22 NETWORK OBJ 10.4.28.0 22 no-proxy-arp
route-lookup
nat (any,any) source static any any destination static 5505-pool
  5505-pool
!
object network internal-network-ISPa
  nat (any,outside-16) dynamic interface
object network internal-network-ISPb
  nat (any,outside-17) dynamic interface
object network dmz-webserver-ISPa
  nat (any,outside-16) static outside-webserver-ISPa
object network dmz-webserver-ISPb
  nat (any,outside-17) static outside-webserver-ISPb
object network dmz-esa-ISPa
  nat (any,outside-16) static outside-esa-ISPa
object network dmz-dmvpn-1
  nat (any,outside-16) static outside-dmvpn-ISPa
object network dmz-dmvpn-2
  nat (any,outside-17) static outside-dmvpn-ISPb
object network dmz-guest-network-ISPa
  nat (any,outside-16) dynamic interface
object network dmz-wlc-1
  nat (any,outside-16) static outside-wlc-1
object network dmz-cvo-1
  nat (any,outside-16) static outside-cvo-1
access-group global_access global
!
router eigrp 100
  no auto-summary
  network 10.4.24.0 255.255.252.0
  network 192.168.16.0 255.255.248.0
  passive-interface default
  no passive-interface inside

```

```

redistribute static
!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 128 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 254
route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15
key *****
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.4.48.15
timeout 5
key *****
user-identity default-domain LOCAL
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 192.168.1.0 255.255.255.0 management
http 10.4.0.0 255.254.0.0 inside
snmp-server host inside 10.4.48.35 community ***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown

```

```

coldstart warmstart
sla monitor 16
type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-
md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-
md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-
sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-
sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-
hmac
crypto dynamic-map SYSTEM DEFAULT CRYPTO MAP 65535 set ikev1
transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA
ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-
3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM
DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface outside-16
crypto map outside-17_map 65535 ipsec-isakmp dynamic SYSTEM
DEFAULT_CRYPTO_MAP
crypto map outside-17_map interface outside-17
crypto ca trustpoint ASDM_TrustPoint0
enrollment self
subject-name CN=IE-ASA5540.cisco.local
proxy-ldc-issuer
crl configure

```

```

crypto ca certificate chain ASDM_TrustPoint0
certificate e5035c4e
  3082026c 308201d5 a0030201 020204e5 035c4e30 0d06092a
864886f7 0d010105
  05003048 311f301d 06035504 03131649 452d4153 41353534
302e6369 73636f2e
  6c6f6361 6c312530 2306092a 864886f7 0d010902 16164945
2d415341 35353430
  2e636973 636f2e6c 6f63616c 301e170d 31313038 32393231
35313130 5a170d32
  31303832 36323135 3131305a 3048311f 301d0603 55040313
1649452d 41534135
  3534302e 63697363 6f2e6c6f 63616c31 25302306 092a8648
86f70d01 09021616
  49452d41 53413535 34302e63 6973636f 2e6c6f63 616c3081
9f300d06 092a8648
  86f70d01 01010500 03818d00 30818902 818100a7 fee67ff4
14768acb 30269b24
  53e09cce 9f7691f3 17b25250 67c7e892 6362af6a 3c7fb393
83209a44 947bb7cb
  2a5b4cdb 8ccd87c4 1890f5b9 8c247e7c f2835887 a2d266fd
262804a8 6c64270f
  4f6cf5a6 248208f7 9f60bc45 0ffcb8df 4806df1f 518e4b85
2aa39e44 88455de9
  acaee96b e0f69b5b 71aa8d70 8e86a0e4 b8989b02 03010001
a3633061 300f0603
  551d1301 01ff0405 30030101 ff300e06 03551d0f 0101ff04
04030201 86301f06
  03551d23 04183016 8014fa32 2185c193 c80b6bc1 d1b24051
fd6b7044 e673301d
  0603551d 0e041604 14fa3221 85c193c8 0b6bc1d1 b24051fd
6b7044e6 73300d06
  092a8648 86f70d01 01050500 03818100 19d5cf64 3416269f
934e5601 4e36df73
  14a8f44b 14ea0c96 70fda56d de559466 4d8fafb5 65a4bad8
a65fe039 2553b96b
  44c54065 7dac21a6 7950b619 a2361fc5 c63ce35a bccc30b2

```

```

4c10cb5c 7f761f31
  9b1679ef 0f69f210 a5268f88 0a09bb37 f094859a cc66d77f
e80d0df9 22c47631
  232993bc 7d0c8851 d84b7d78 076e6d07
quit
crypto ikev1 enable outside-16
crypto ikev1 enable outside-17
crypto ikev1 policy 10
  authentication crack
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 20
  authentication rsa-sig
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 30
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 40
  authentication crack
  encryption aes-192
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 50
  authentication rsa-sig
  encryption aes-192
  hash sha
  group 2
  lifetime 86400

```

```
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
```

```
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.0.0 255.254.0.0 inside
ssh timeout 5
ssh version 2
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
!
tls-proxy maximum-session 2000
!
threat-detection basic-threat
```

```

threat-detection statistics access-list
no threat-detection statistics tcp-intercept
wccp 90 redirect-list WCCP_Redirect
wccp interface inside 90 redirect in
ntp server 10.4.48.17
ssl trust-point ASDM_TrustPoint0 outside-16
ssl trust-point ASDM_TrustPoint0 outside-17
webvpn
    enable outside-16
    enable outside-17
    anyconnect image disk0:/anyconnect-linux-64-3.0.3054-k9.pkg 1
    anyconnect image disk0:/anyconnect-macosx-i386-3.0.3054-k9.pkg 2
    anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg 3
    anyconnect profiles ra_profile disk0:/ra_profile.xml
    anyconnect profiles web_security_profile disk0:/web_security
    profile.wsp
    anyconnect profiles web_security_profile.wso disk0:/web
    security_profile.wso
    anyconnect enable
    tunnel-group-list enable
group-policy 5505Group internal
group-policy 5505Group attributes
    vpn-tunnel-protocol ikev1
    password-storage disable
    split-tunnel-policy tunnelall
    secure-unit-authentication enable
    nem enable
group-policy GroupPolicy_AnyConnect internal
group-policy GroupPolicy_AnyConnect attributes
    wins-server none
    dns-server value 10.4.48.10
    vpn-tunnel-protocol ssl-client
    split-tunnel-policy excludespecified
    default-domain value cisco.local
    webvpn
        anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Administrators internal

```

```

group-policy GroupPolicy_Administrators attributes
    banner value Your access is via an unrestricted split tunnel.
    split-tunnel-policy tunnelspecified
    split-tunnel-network-list value RA_SplitTunnelACL
    webvpn
        anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
    banner value Your access is restricted to the partner server
    vpn-filter value RA_PartnerACL
    webvpn
        anyconnect profiles value ra_profile type user
username admin password w2Y.6Op4j7clVDk2 encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
    address-pool RA-pool
    authentication-server-group AAA-RADIUS
    default-group-policy GroupPolicy_AnyConnect
tunnel-group AnyConnect webvpn-attributes
    group-alias AnyConnect enable
    group-url https://172.16.130.124/AnyConnect enable
    group-url https://172.17.130.124/AnyConnect enable
tunnel-group Teleworker5505 type remote-access
tunnel-group Teleworker5505 general-attributes
    authentication-server-group AAA-RADIUS
    default-group-policy 5505Group
tunnel-group Teleworker5505 ipsec-attributes
    ikev1 pre-shared-key *****
!
class-map global-class
    match access-list global_mpc
class-map inspection_default
    match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
    parameters

```

```

message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
class global-class
ips inline fail-close
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:520104e0c6eb2938412c572758ee6c81
: end

```

## CVO Aggregation Router

```

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname CVOAGG-3945E-1
!

```

```

boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$aCns$7.1jixK6Q1QB8FDGemyli/
!
aaa new-model
!
!
aaa group server radius acs
server-private 10.4.48.15 auth-port 1812 acct-port 1813 key 7
0235015819031B0A4957
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authentication login sdp-acs group acs
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
aaa authorization network sdp-acs group acs
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
!
!
ip cef
!

```

```

ip vrf INET-PUBLIC
  rd 65520:1
!
ip multicast-routing
!
!
ip domain name cisco.local
ip host cvo-cs 10.4.32.246
ip host OpsXML 10.4.48.29
!
multilink bundle-name authenticated
!
!
!
crypto pki server cvo-cs
  database level complete
  database archive pkcs12 password 7 110A1016141D5A5E57
  issuer-name cn=cvo-cs,ou=cvo
  grant auto
  auto-rollover
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-526531848
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-526531848
  revocation-check none
  rsakeypair TP-self-signed-526531848
!
crypto pki trustpoint cvo-cs
  revocation-check crl
  rsakeypair cvo-cs
!
crypto pki trustpoint cvo-pki
  enrollment url http://cvo-cs:8000
  serial-number
  ip-address none
  password 7 082F43400C

```

```

revocation-check crl
authorization list sdp-acs
auto-enroll 75
!
!
!
crypto pki certificate map DMVPN 10
  issuer-name co cvo-cs
  unstructured-subject-name co cisco.local
!
crypto pki certificate chain TP-self-signed-526531848
  certificate self-signed 01
    30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274
    69666963 6174652D 35323635 33313834 38301E17 0D313131 31323832
32333833
    335A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403
1325494F
    532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3532
36353331
    38343830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
02818100
    DCB817F9 90FDCDE1 16BCBD2F BF26F0FD 224A1213 7E61FE77 9676AB68
DFD411DF
    0BE67687 71BFA66D A70D4BA9 85F5E718 809E5AB1 482BA738 B0477F15
8D455523
    0DF6557C 8785C3ED C5E0FA4F E6E40978 B2746BBC 860134A5 1CE49F22
E06408D5
    FBA13130 3FCA37F5 6BC28AB0 253450AD 3E078391 D83889B8 6970A6AF
B3535863
    02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
0603551D
    23041830 1680147F C0E85DF6 52CE197B 0F8FBFE2 A849B755 99D68030
1D060355
    1D0E0416 04147FC0 E85DF652 CE197B0F 8FBFE2A8 49B75599 D680300D

```

```

06092A86
  4886F70D 01010505 00038181 009F00F0 38F28B0F 57532DD8 D447D238
FF20E260
  96982CF7 1417D611 1AD5D949 565D0B3B 2B9275B4 9B95A7BE CB9EC112
963D27E4
  EC66AAB0 7A33C35F 0AFE7371 2EEC5C7A 03CFDB1A 41FD769D 18CBE808
1ED72E23
  0F33C109 10E15FFD 254402F4 D4A698C2 ADC3BBA3 EB325B99 43E73F6B
93D13521
  54F1329E 6163E702 2F88ABDC 33
quit
crypto pki certificate chain cvo-cs
certificate ca 01
  30820217 30820180 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  1F310C30 0A060355 040B1303 63766F31 0F300D06 03550403 13066376
6F2D6373
  301E170D 31313131 32383232 34303532 5A170D31 34313132 37323234
3035325A
  301F310C 300A0603 55040B13 0363766F 310F300D 06035504 03130663
766F2D63
  7330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100BD14
  41D2D72C A48938D5 8AB45971 EA66928E C0B620A4 EA8D7E36 E7BC6AE4
8F6BC17D
  3DDA8231 343F209C AC4AF4E2 7B4D1068 B2200F46 41E8BFFE 7B395522
7C588DDC
  341CF1EF 027D3BE8 C7C25CFC D657F75B 09A08C5D 1E60BC64 1ECF6452
12E49A67
  A9BF3E54 689CCE3F 022B0C5A DEBFD784 E013BE9F CF3F0ED2 7802B5F6
E1770203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603
551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 149C5E56 BD199D91
18CB3C6F
  CB31C3F8 CD99CA4A E9301D06 03551D0E 04160414 9C5E56BD 199D9118
CB3C6FCB

```

```

  31C3F8CD 99CA4AE9 300D0609 2A864886 F70D0101 04050003 81810020
76C42DBC
  8FFE9CDC C489B3E3 7D180E4B 46446BF3 E6D0588F 38FE9C70 6F1006ED
7AE60BAC
  6FE8EF17 D0864013 6E9F42FF 0DAA152A 39DEFA4F A3B99843 7EBF2A2E
100465FA
  AB1F8F63 B6EF6A8A DCA63CE5 8EF71D78 B37BFA7C 993F2C43 74155CE5
6C134B22
  018BC277 422BEC7E D4098747 2C327531 FCA7D4EE F9E33EC0 47CDD4
quit
crypto pki certificate chain cvo-pki
certificate 02
  308201DF 30820148 A0030201 02020102 300D0609 2A864886 F70D0101
05050030
  1F310C30 0A060355 040B1303 63766F31 0F300D06 03550403 13066376
6F2D6373
  301E170D 31313131 32383232 34323138 5A170D31 32313132 37323234
3231385A
  303F313D 30120603 55040513 0B465458 31343339 4148384E 30270609
2A864886
  F70D0109 02161A43 564F4147 472D3339 3435452D 312E6369 73636F2E
6C6F6361
  6C305C30 0D06092A 864886F7 0D010101 0500034B 00304802 4100BF3B
8438FA8F
  1FAE6BC5 C80F639B 795B68B3 EFDEED2F F895B4CD 532F9F79 B97278D8
90AA5C18
  5D03A50B BB5580CE 98A16E69 6CBB0796 CC863FDA 9D2242E5 FE530203
010001A3
  4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680
149C5E56
  BD199D91 18CB3C6F CB31C3F8 CD99CA4A E9301D06 03551D0E 04160414
ACC7E656
  8777D8DD EE546EFF 649BD4AD 51DBF392 300D0609 2A864886 F70D0101
05050003
  81810096 C73EB800 DA62AFB6 4844C481 D4726761 5192C054 68FCFB45
0E7BD2FA
  0FBBFF7A ECA1DD80 7735BE27 648ADB66 AB4CA67D B5B66D8B DAF669EB

```

```

1D560B38
 4F03FE3D D4305242 3DA9DA6D 448E4E13 44240E1B 974F279D 8D8DFF39
2CDA483C
 6453890F 3B104B0A 898CA3F1 30EF94B6 5B16AA62 DE36A7D0 599A7EBA
8821FF51 3998F3
quit
certificate ca 01
 30820217 30820180 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
 1F310C30 0A060355 040B1303 63766F31 0F300D06 03550403 13066376
6F2D6373
 301E170D 31313131 32383232 34303532 5A170D31 34313132 37323234
3035325A
 301F310C 300A0603 55040B13 0363766F 310F300D 06035504 03130663
766F2D63
 7330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100BD14
 41D2D72C A48938D5 8AB45971 EA66928E C0B620A4 EA8D7E36 E7BC6AE4
8F6BC17D
 3DDA8231 343F209C AC4AF4E2 7B4D1068 B2200F46 41E8BFFE 7B395522
7C588DDC
 341CF1EF 027D3BE8 C7C25CFC D657F75B 09A08C5D 1E60BC64 1ECF6452
12E49A67
 A9BF3E54 689CCE3F 022B0C5A DEBFD784 E013BE9F CF3F0ED2 7802B5F6
E1770203
 010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603
551D0F01
 01FF0404 03020186 301F0603 551D2304 18301680 149C5E56 BD199D91
18CB3C6F
 CB31C3F8 CD99CA4A E9301D06 03551D0E 04160414 9C5E56BD 199D9118
CB3C6FCB
 31C3F8CD 99CA4AE9 300D0609 2A864886 F70D0101 04050003 81810020
76C42DBC
 8FFE9CDC C489B3E3 7D180E4B 46446BF3 E6D0588F 38FE9C70 6F1006ED
7AE60BAC
 6FE8EF17 D0864013 6E9F42FF 0DAA152A 39DEFA4F A3B99843 7EBF2A2E
100465FA

```

```

AB1F8F63 B6EF6A8A DCA63CE5 8EF71D78 B37BFA7C 993F2C43 74155CE5
6C134B22
 018BC277 422BEC7E D4098747 2C327531 FCA7D4EE F9E33EC0 47CDD4
quit
license udi pid C3900-SPE250/K9 sn FOC14373A5X
!
!
username admin password 7 121A0C0411045D5679
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match dscp af21
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4 af41
class-map match-any CRITICAL-DATA
 match dscp cs3 af31
class-map match-any VOICE
 match dscp ef
class-map match-any SCAVENGER
 match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
 match dscp cs2 cs6
 match access-group name ISAKMP
!
!
policy-map WAN
 class VOICE
  police rate percent 10
  priority
 class INTERACTIVE-VIDEO

```

```

    police rate percent 23
class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
class DATA
    bandwidth percent 19
    random-detect dscp-based
class SCAVENGER
    bandwidth percent 5
class NETWORK-CRITICAL
    bandwidth percent 3
class class-default
    bandwidth percent 25
    random-detect
!
!
!
crypto provisioning registrar
    pki-server cvo-cs
    template http welcome http://OpsXML/mevo/sdp/2-sdp_welcome.html
    template http completion http://OpsXML/mevo/sdp/4-sdp_
completion.html
    template http introduction http://OpsXML/mevo/sdp/3-sdp_
introduction.html
    template http start http://OpsXML/mevo/sdp/1-sdp_start.html
    template http error http://OpsXML/mevo/sdp/sdp_error.html
    template config http://OpsXML/mevo/Configs/$n_Bootstrap.cfg
    template username Administrator password 7 130646010803557878
    authentication list sdp-acs
    authorization list sdp-acs
!
crypto isakmp policy 10
    encr aes 256
    group 2
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
    match certificate DMVPN
!

```

```

!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
    mode transport
!
crypto ipsec profile DMVPN-PROFILE
    set transform-set AES256/SHA/TRANSPORT
    set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
!
!
!
!
!
!
interface Loopback0
    ip address 10.4.32.246 255.255.255.252
    ip pim sparse-mode
!
interface Tunnel10
    bandwidth 10000
    ip address 10.4.160.1 255.255.254.0
    no ip redirects
    ip mtu 1400
    ip pim nbma-mode
    ip pim sparse-mode
    ip hello-interval eigrp 202 20
    ip hold-time eigrp 202 60
    ip nhrp authentication cisco123
    ip nhrp map multicast dynamic
    ip nhrp network-id 101
    ip nhrp holdtime 600
    ip nhrp redirect
    ip tcp adjust-mss 1360
    no ip split-horizon eigrp 202
    tunnel source GigabitEthernet0/3
    tunnel mode gre multipoint
    tunnel key 10

```

```

tunnel vrf INET-PUBLIC
tunnel protection ipsec profile DMVPN-PROFILE
!
interface Port-channel30
 ip address 10.4.32.6 255.255.255.252
 ip pim sparse-mode
 hold-queue 150 in
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 channel-group 30
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 channel-group 30
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 service-policy output WAN
!
interface GigabitEthernet0/3
 ip vrf forwarding INET-PUBLIC
 ip address 192.168.18.20 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
!
!
router eigrp 100
 network 10.4.32.4 0.0.0.3

```

```

network 10.4.32.246 0.0.0.0
 redistribute eigrp 202 route-map SET-ROUTE-TAG-DMVPN
 passive-interface default
 no passive-interface Port-channel30
 eigrp router-id 10.4.32.246
!
!
router eigrp 202
 network 10.4.160.0 0.0.1.255
 redistribute eigrp 100
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.4.32.246
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
ip http server
ip http port 3389
ip http authentication aaa
ip http secure-server
!
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
ip tacacs source-interface Loopback0
!
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
!
ip radius source-interface Loopback0
!
!
!
!
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65520

```

```
!  
!  
snmp-server community cisco R0  
snmp-server community cisco123 RW  
snmp-server trap-source Loopback0  
tacacs server TACACS-SERVER-1  
  address ipv4 10.4.48.15  
  key 7 15210E0F162F3F0F2D2A  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
  logging synchronous  
line aux 0  
line vty 0 4  
  transport input ssh  
line vty 5 15  
  transport input ssh  
!  
scheduler allocate 20000 1000  
ntp source Loopback0  
ntp update-calendar  
ntp server 10.4.48.17  
end
```

## Notes



## SMART BUSINESS ARCHITECTURE



**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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [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. (1005R)