Teleworking—Cisco Virtual Office Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

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

month year Series

For example, the series of guides that we released in February 2013 is the "February 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 SBA feedback form.

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

Table of Contents

What's In This SBA Guide

Cisco SBA Solutions

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

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

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

Route to Success

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

About This Guide

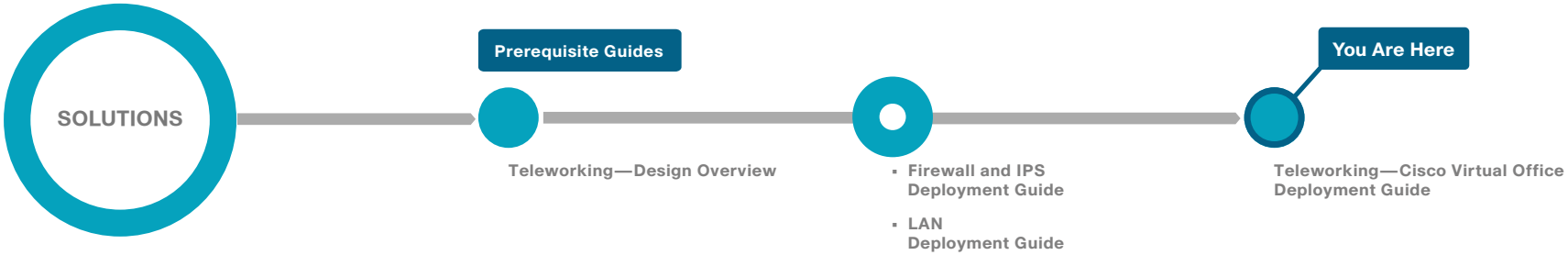
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

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

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

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

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



Introduction

Business Overview

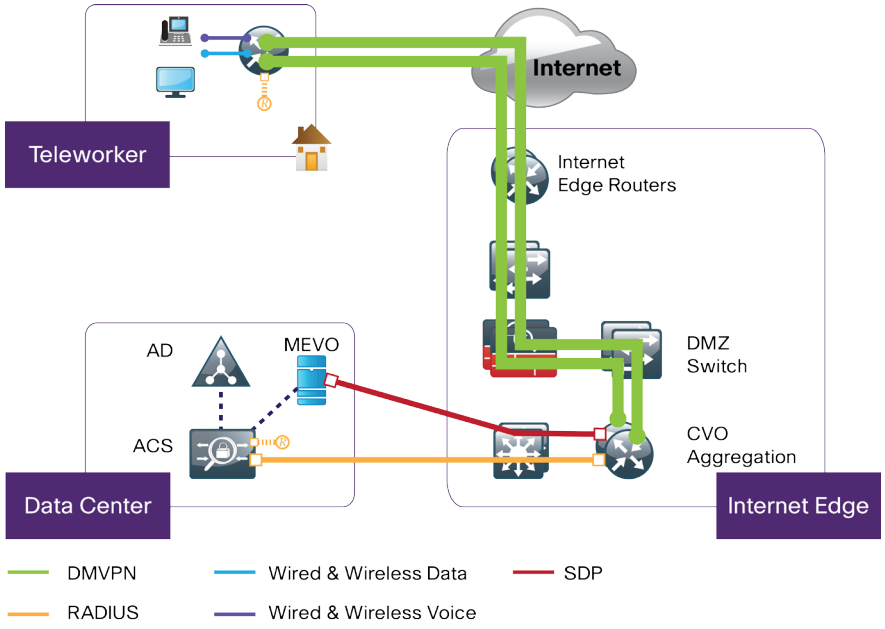
Providing end users access to networked business services from their residential environment, poses challenges for both the end user and IT operations. For the home-based teleworker, it is critical that access to business services be reliable and consistent, providing an experience that is as familiar as sitting in a cubicle or office in the organization's facility. Employees who work from home regularly can require a wide array of devices that need to connect to the network. These employees 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 who needs the highest level of resiliency and advanced technology support. The Cisco Virtual Office (CVO) Solution supports both wired and wireless users at the CVO remote site (home) and allows for direct communication between the devices without their having to traverse the Internet.

Figure 1 - Cisco Virtual Office architecture



Components of the CVO Solution include:

- Dynamic Multipoint VPN (DMVPN) aggregation router serving as the VPN termination point
- PKI 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 ManageExpress Virtual Office (MEVO) on a Microsoft Windows 2003 or 2008 server for Cisco Virtual Office management and provisioning
- On the remote-site (the teleworker's home), a Cisco 800 Series Router 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 as 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.

The benefits of PKI integration include:

- 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 certificate revocation list (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 Cisco 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.

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 1 - Universal design parameters

Network service	IP address
Domain name	cisco.local
Active Directory, Domain Name System (DNS) server, Dynamic Host Configuration Protocol (DHCP server	10.4.48.10
Access Control System (ACS)	10.4.48.15
Network Time Protocol (NTP) Server	10.4.48.17

Process

Configuring the Distribution Switch

1. Connect to the DMVPN aggregation router
2. Configure EIGRP on the distribution switch

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 SBA—Borderless Networks LAN Deployment Guide*.

Procedure 1 Connect to the DMVPN aggregation router

Table 2 - 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
 description CVOAGG-3945E-1
 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 GigabitEthernet1/0/13
 description CVOAGG-3945E-1 Gig0/0
!
interface GigabitEthernet2/0/13
 description CVOAGG-3945E-1 Gig0/1
!
interface range GigabitEthernet1/0/13, GigabitEthernet2/0/13
 no switchport
 no ip address
 channel-group 30 mode on
 macro apply EgressQoS
 logging event link-status
 logging event bundle-status
 carrier-delay msec 0
 no shutdown
```

Procedure 2 Configure EIGRP on the distribution switch

Step 1: Enable Enhanced Interior Gateway Routing Protocol (EIGRP) to form a neighbor relationship with the aggregation router.

```
router eigrp 100
 no passive-interface Port-channel30
```

Step 2: If 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 DMVPN Aggregation Router

1. Finish WAN router universal configuration
2. Configure connectivity to the LAN
3. Configure VRF Lite
4. Connect to the Internet DMZ
5. Configure CA and SDP servers
6. Configure ISAKMP and IPsec
7. Configure the mGRE tunnel
8. Configure EIGRP on the aggregation router
9. Configure QoS
10. Repeat the process for secondary router

The CVO aggregation includes two routers that terminate DMVPN traffic. Each aggregation router is configured as a unique DMVPN cloud and tied, through Network Address Translation (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 under most conditions.

Table 3 - 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 the local login and password.

The local login account and password provide basic access authentication to a router, which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plaintext passwords when viewing configuration files. By default, HTTPS access to the router will use the enable password for authentication.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 3: If you want to configure centralized user authentication, perform this step.

As networks scale in the number of devices to maintain, the operational burden to maintain local user accounts on every device also scales. A centralized AAA service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Reader Tip

The AAA server used in this architecture is the Cisco Access Control System. For details about ACS configuration, see the *Cisco SBA—Borderless Networks Device Management Using ACS 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 in Step 2 on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
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 device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) Protocol 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.

The use of the SSH and HTTPS protocols enables secure management of the network device. Both protocols are encrypted for privacy, and the unsecure protocols—Telnet and HTTP—are turned off.

Specify the **transport preferred none** command on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the DNS server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

When synchronous logging of unsolicited messages and debug output are 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
```

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 5: If network operational support is centralized in your organization, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Tech Tip

If you configure an access list on the vty interface, you may lose the ability to use SSH to log in from one router to the next for hop-by-hop troubleshooting.

Step 6: 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
```

Step 7: 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 later 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
```

Step 8: Configure IP unicast routing.

EIGRP is configured facing the LAN distribution or core layer. In this design, the port-channel interface and the loopback must be EIGRP interfaces. The loopback may remain a passive interface. The network range must include both interface IP addresses, either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
  network 10.4.0.0 0.1.255.255
  no auto-summary
  passive-interface default
  eigrp router-id 10.4.32.246
```

Step 9: Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP telephony Music on Hold (MOH) and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as a rendezvous point (RP) to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

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

```
ip multicast-routing
```

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.

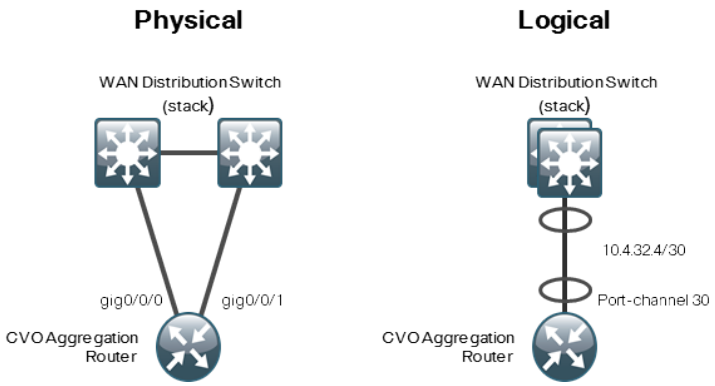
```
ip pim sparse-mode
```

Procedure 2 Configure connectivity to the LAN

The DMVPN hub routers connect to a resilient switching device in the distribution layer and in the demilitarized zone (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.

Figure 2 - Connecting to the distribution switch



Step 1: Configure the port-channel interface, and assign an 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
 ip address 10.4.32.6 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

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

```
interface GigabitEthernet0/0
 description WAN-D3750X Gig1/0/13
!
interface GigabitEthernet0/1
 description WAN-D3750X Gig2/0/13
!
interface range GigabitEthernet 0/0, GigabitEthernet 0/1
 no ip address
 channel-group 30
 no shutdown
```

Step 3: Enable EIGRP neighbor relationships across this interface.

```
router eigrp 100
 no passive-interface Port-channel 30
```

Procedure 3 Configure VRF Lite

Virtual Route 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.

Step 1: Configure VRF Lite.

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

Tech 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.

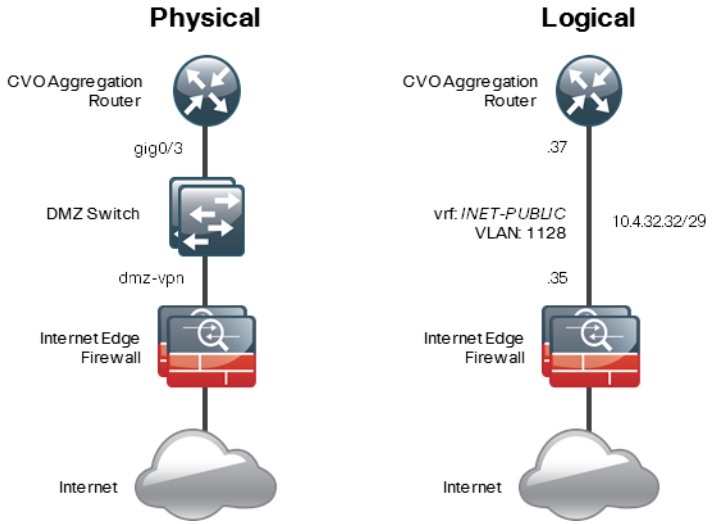
32-bit IP address: your 16-bit number

For example, 192.168.122.15:1.

Procedure 4 Connect to the Internet DMZ

The DMVPN aggregation router requires a connection to the Internet. In this deployment, the DMVPN aggregation router is connected through a Cisco ASA 5500 Adaptive Security Appliance using a DMZ interface specifically created and configured for all DMVPN termination routers.

Figure 3 - 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 ASA 5500 to translate the router IP address to a routable IP address.

This design assumes that the Cisco ASA 5500 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 Procedure 3.

```
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 Cisco ASA 5500 DMZ interface IP address.

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

Procedure 5 Configure CA and SDP servers

Perform this procedure only on the primary aggregation router.

Use this procedure to configure the aggregation components of Cisco Virtual Office for the CA server and the 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 Simple Certificate Enrollment Protocol (SCEP) and SDP.

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

Step 2: Configure the Cisco IOS CA.

```
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.

```
radius server RADIUS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
aaa group server radius RADIUS-SERVERS
 server name RADIUS-SERVER-1
aaa authentication login sdp-acs group RADIUS-SERVERS
aaa authorization network sdp-acs group RADIUS-SERVERS
ip radius source-interface Loopback0
```

Step 4: Configure the SDP Registrar and templates.

```
crypto provisioning registrar
 pki-server cvo-cs
 template config http://10.4.48.29/mevo/Configs/$n_Bootstrap.cfg
 template http welcome http://10.4.48.29/mevo/sdp/2-sdp_welcome.html
 template http completion http://10.4.48.29/mevo/sdp/4-sdp_completion.html
 template http introduction http://10.4.48.29/mevo/sdp/3-sdp_introduction.html
 template http start http://10.4.48.29/mevo/sdp/1-sdp_start.html
 template http error http://10.4.48.29/mevo/sdp/sdp_error.html
 template username Administrator password 0 Cisco123
 authentication list sdp-acs
 authorization list sdp-acs
```

Tech Tip

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

Procedure 6 Configure ISAKMP and IPsec

All virtual-office 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: Enable the AAA server for SDP user authentication on the secondary aggregation router. If configuring the primary aggregation router, you may proceed to the next step as this portion was previously completed.

```
radius server RADIUS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
aaa group server radius RADIUS-SERVERS
 server name RADIUS-SERVER-1
aaa authentication login sdp-acs group RADIUS-SERVERS
aaa authorization network sdp-acs group RADIUS-SERVERS
ip radius source-interface Loopback0
```

Step 2: 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-acs
 auto-enroll 75
```

Step 3: Authenticate and enroll the certificate.

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

Step 4: Configure the certificate map.

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

Step 5: Create the Internet Security Association and Key Management Protocol (ISAKMP) profile.

The ISAKMP profile creates an association with an IP Security (IPsec) peer that presents a certificate that matches one that uses the certificate map defined in the previous step.

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

Step 6: 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 7: 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 (hash-based message authentication code [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 8: 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

Table 4 - 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

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 **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 Front Door VRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in Procedure 6.

```
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 hold time should be configured to 600 seconds.

EIGRP (configured in the following procedure, Procedure 8) 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; the notification may be required for DMVPN spoke-to-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: Enable Protocol Independent Multicast (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.

Tech Tip

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

```
interface Tunnel10
 ip pim sparse-mode
 ip pim nbma-mode
```

Step 5: 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. The advertisement of these routes would normally be prevented by split horizon; you can override this by using the **no ip split-horizon eigrp** command.

Increase the EIGRP hello interval to 20 seconds, and the EIGRP hold time to 60 seconds. This accommodates 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 on the aggregation router

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 Cisco 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 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.

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 Tunnel10
 eigrp router-id 10.4.32.246
 no auto-summary
```

Step 2: 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 withdrawn 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 routing 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 5 - 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 Tunnel10
 set tag 65520
!
router eigrp 100
 redistribute eigrp 202 route-map SET-ROUTE-TAG-DMVPN
!
router eigrp 202
 redistribute eigrp 100
```

Procedure 9 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 ISP 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
```

Procedure 10 Repeat the process for secondary router

Step 1: Repeat the steps in the Configuring the DMVPN Aggregation Router process on the secondary CVO aggregation router. Be sure to use values associated with the secondary router.

Process

Configuring the Internet Edge

1. Configure the DMZ switch
2. Configure the firewall DMZ interface
3. Configure NAT
4. Configure security policy

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 *Cisco SBA—Borderless Networks Internet Edge Deployment Guide*.

Procedure 1 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 to correctly trust the classification of packets that arrive from 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
```

Procedure 2 Configure the firewall DMZ interface

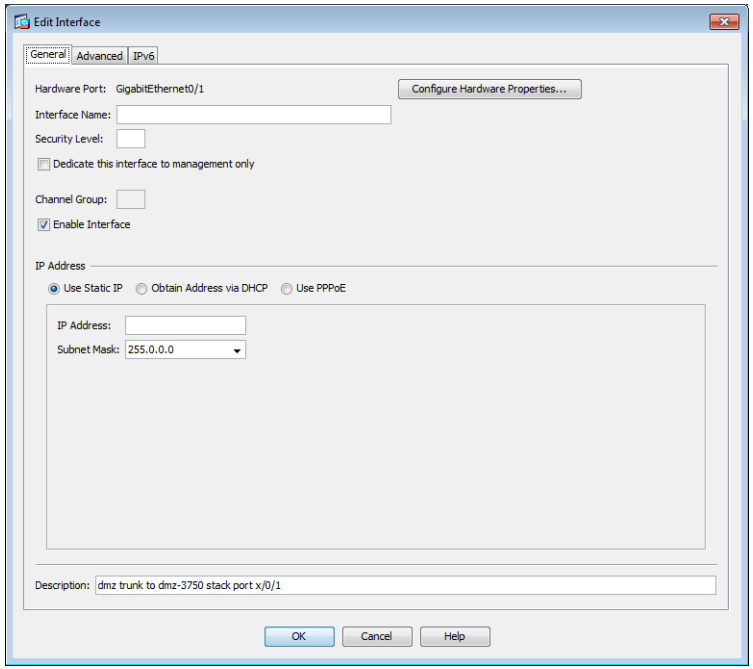
The firewall DMZ is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except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

The various DMZ networks are connected to 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 VLAN interface on the DMZ switch 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**.



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)

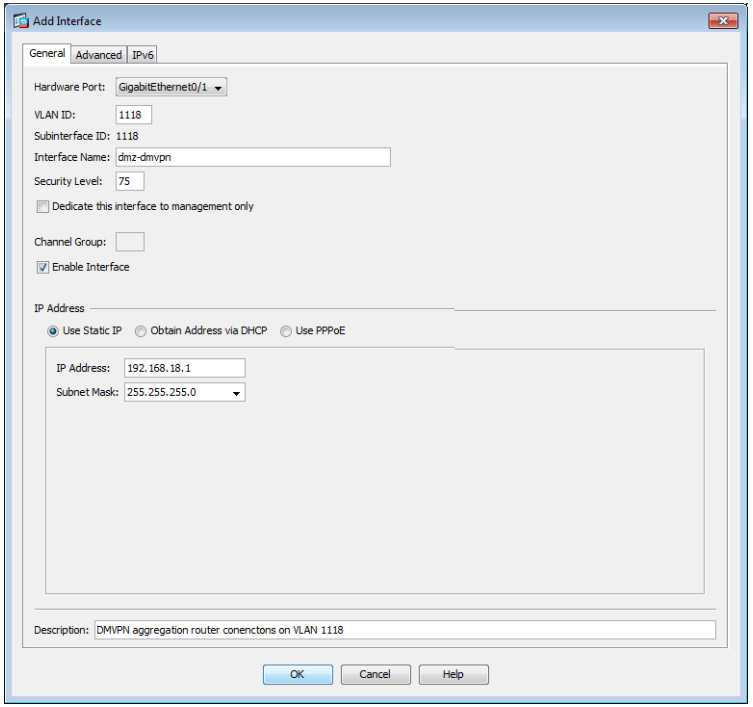
Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

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)



Procedure 3 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 6 - Example DMZ address to public IP address mapping

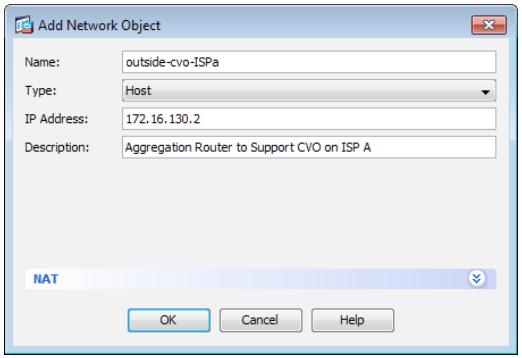
CVO router DMZ address	CVO router public address (externally routable after NAT)
192.168.18.20	172.16.130.2 (ISP-A)
192.168.18.21	172.17.130.2 (ISP-B)

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

Step 2: Click **Add > Network Object**. This adds a network object for the public address of the CVO aggregation router.

Step 3: On 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-ISPa)

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: Click **Add > Network Object**. This adds a network object for the private DMZ address of the CVO aggregation router.

Step 6: On 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)

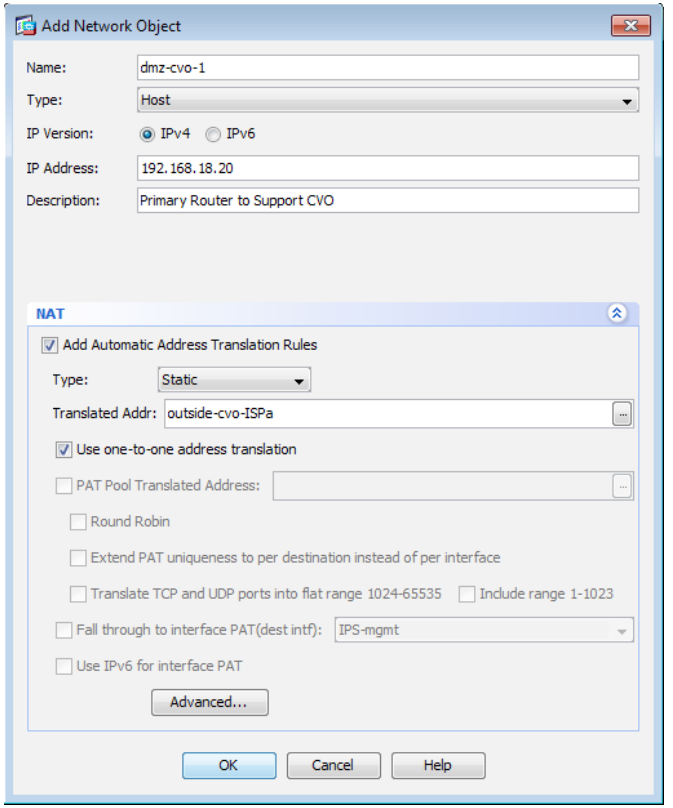
Step 7: In the **IP Address** box, enter the private DMZ IP address of the primary CVO aggregation router. (Example: 192.168.18.20)

Step 8: Click the two down arrows.

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

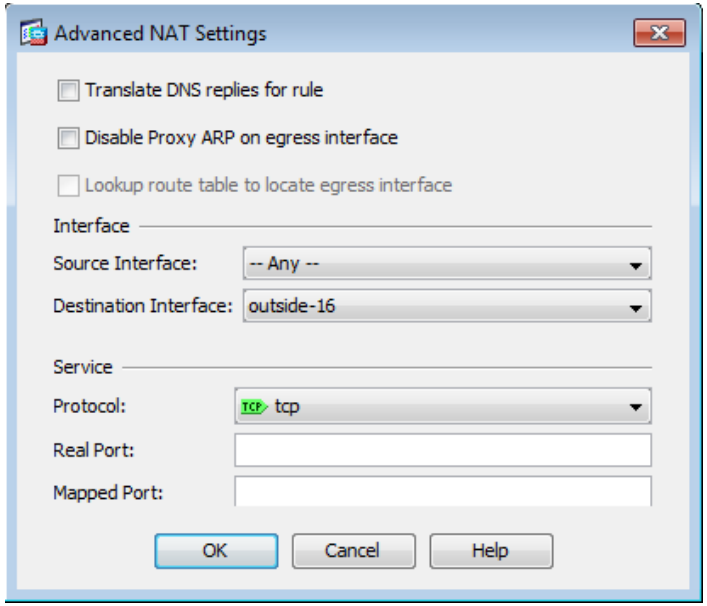
Step 10: In the **Translated Addr** list, choose the network object created in Step 2.

Step 11: Select **Use one-to-one address translation**.



Step 12: Click **Advanced**.

Step 13: In the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



Step 14: Repeat Step 1 through Step 13 for the resilient CVO aggregation router.

Procedure 4 Configure security policy

Security policy should suit the policy and management requirements of your organization. Use the examples here as a basis for configuring 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 7 - 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

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.

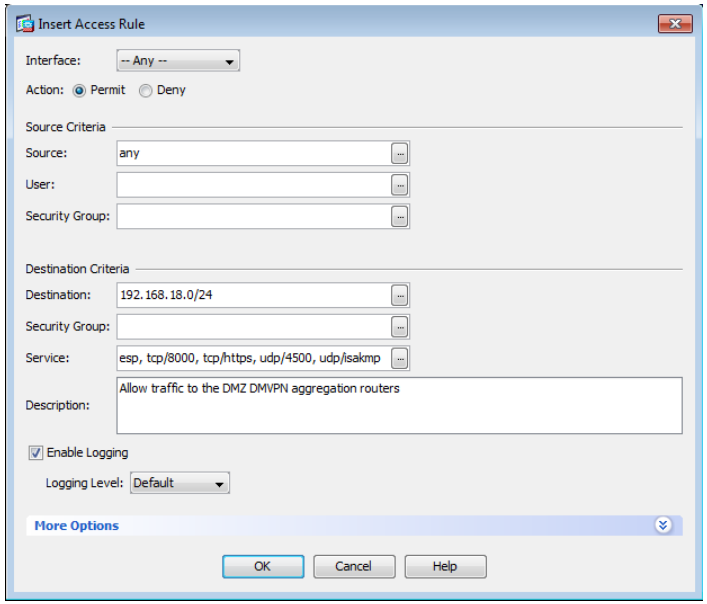
Step 3: Click **Add** > **Insert**.

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

Step 5: Next to **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** box, enter **esp, tcp/8000, tcp/https, udp/4500, udp/isakmp**, and then click **OK**.



Step 8: Click **Apply**.

Process

Configuring the Cisco ACS

1. Configure 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. Enable 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 SBA—Borderless Networks Device Management Using ACS 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 PKI authentication of routers.

Procedure 1 Configure the MEVO account

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

Step 2: Click **Create**.

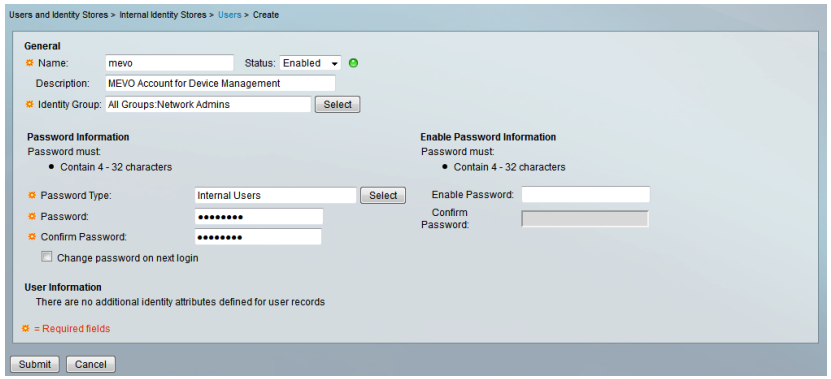
Step 3: In the **Name** box, enter a username for the account. (Example: mevo)

Step 4: Enter and confirm a password.

Step 5: Click **Select** next to the Identity Group field. The Identity Groups window opens. Next, you associate the account to the identity group that defines network administrators.

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

Step 7: Click **Submit**. This applies the changes.



Procedure 2 Enable the default network device

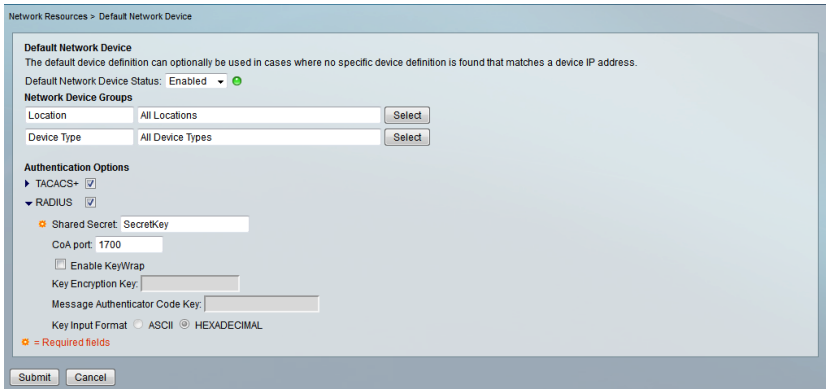
There are many devices deployed in a CVO solution, primarily CVO remote routers and autonomous access points, and tracking their assigned IP addresses can be difficult. So instead of creating a unique network device entry in ACS for each CVO remote device, enable the default network device, which can 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 **RADUIS**.

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 organization's 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 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**.

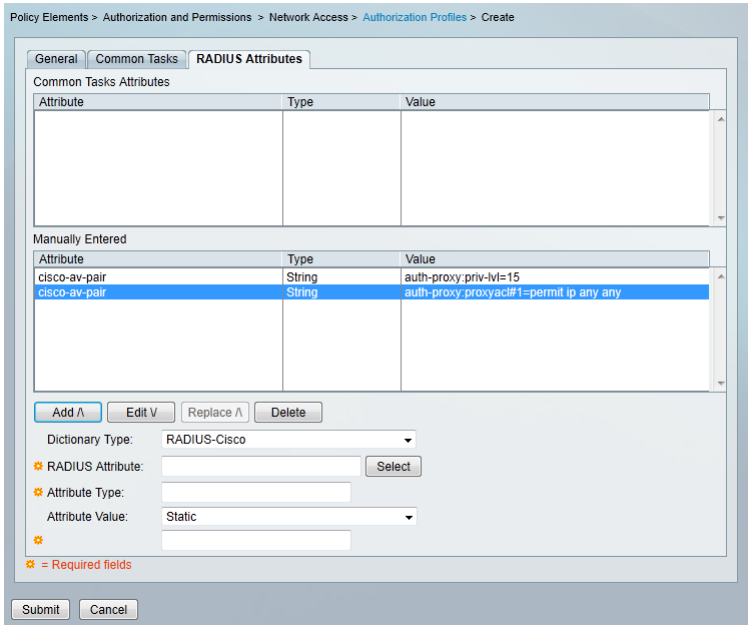
Step 5: In the **Attribute Value** box, enter **auth-proxy:priv-lvl=15**, and then click **Add**.

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**.

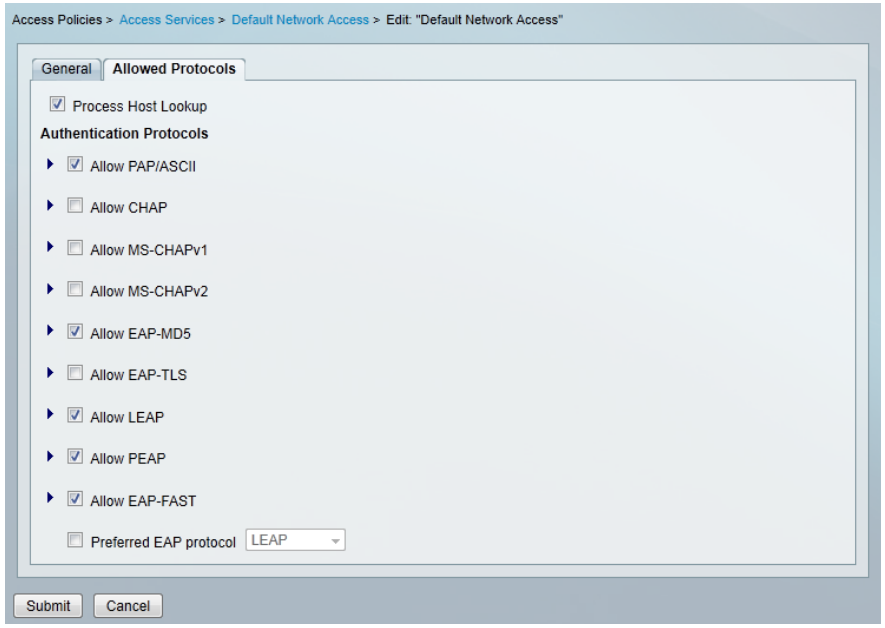


Procedure 4 Enable CVO user authentication

First you must disable the ACS from accepting the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) protocol.

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

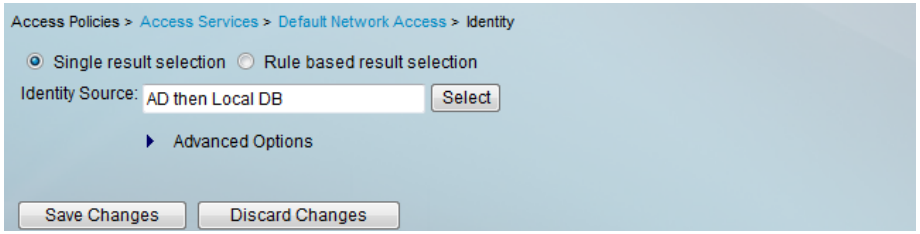
Step 2: On the Allowed Protocols tab, clear **Allow EAP-TLS**, and then click **Submit**.



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

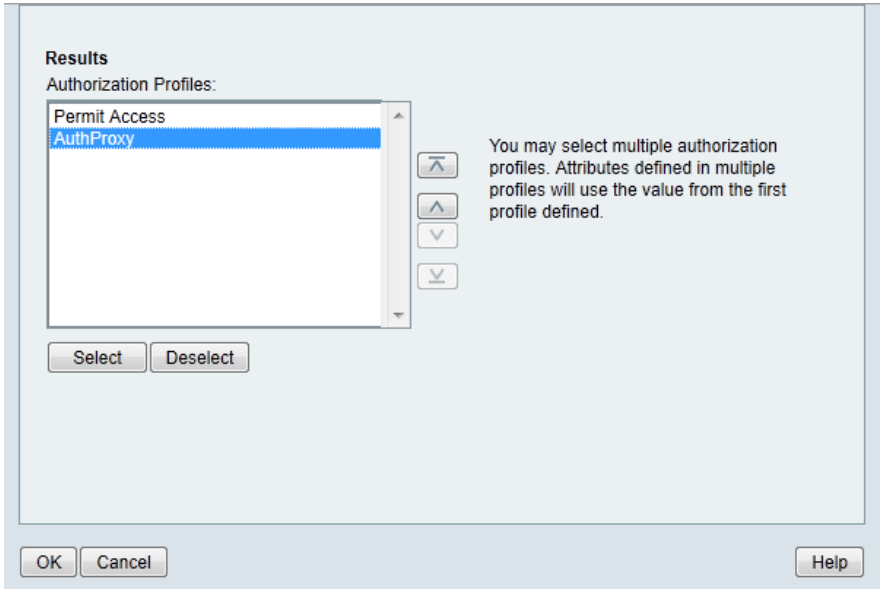
Step 3: Navigate to **Access Policies > Default Network Access > Identity**.

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

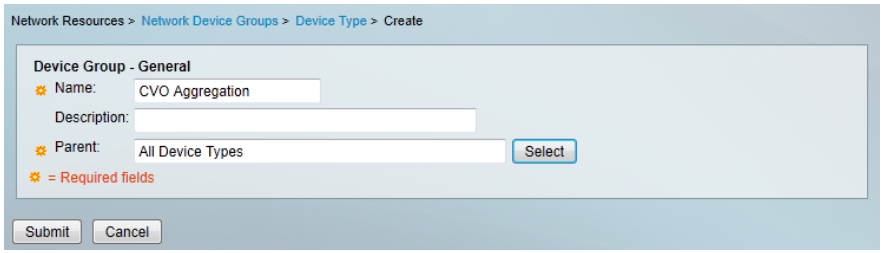
Procedure 5 Create the CVO groups and AAA clients

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)

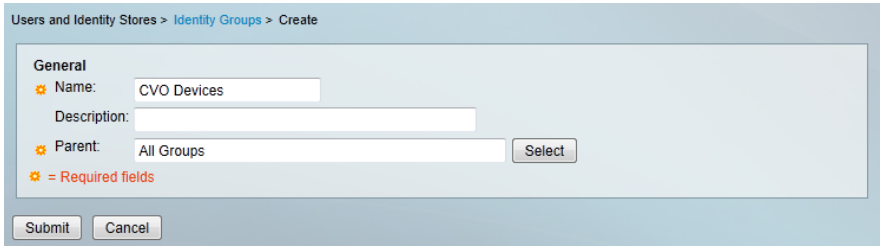
Step 3: In the **Parent** box, select **All Device Types**, and then click **Submit**.



Next, create an identity group to contain the CVO remote 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 router accounts.

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

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

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

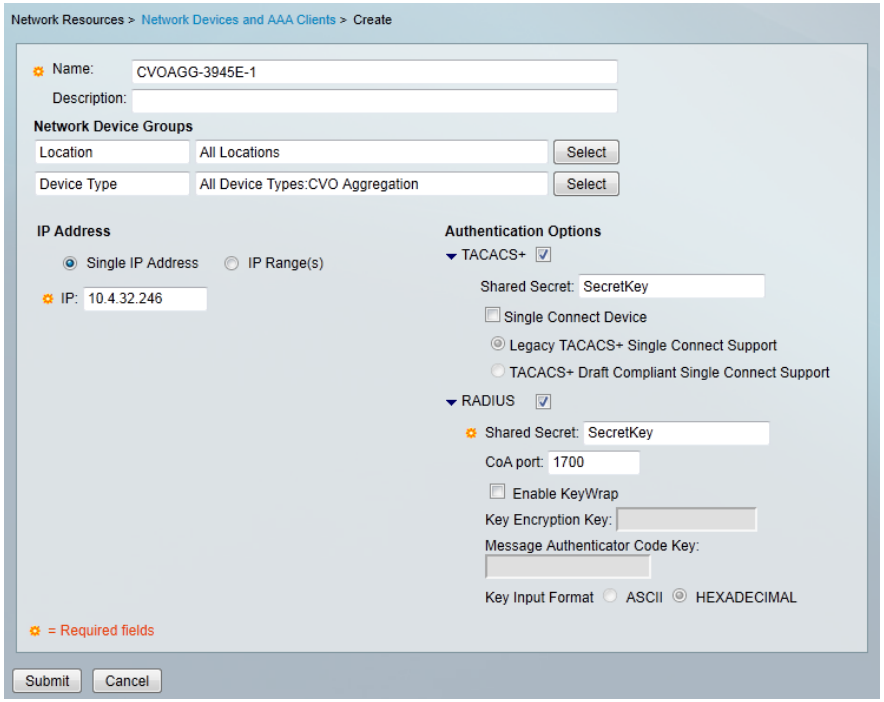
Step 9: In the **IP** box, enter the router's loopback IP address. (Example: 10.4.32.246)

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)



Step 14: Repeat this procedure for the secondary CVO aggregation router.

Procedure 6 Enable 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**.

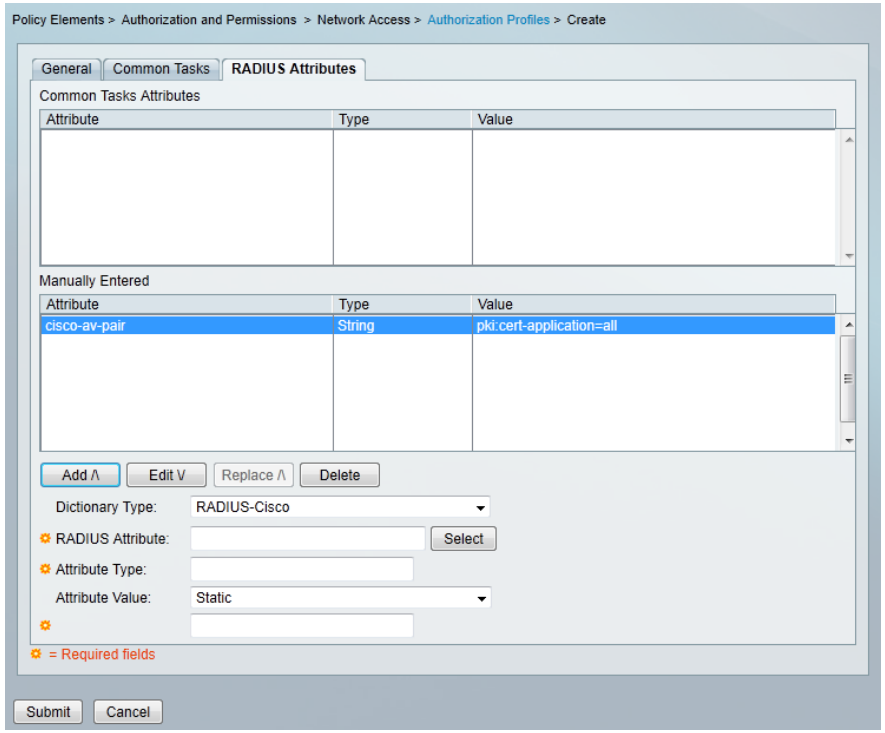
Step 2: Enter a name. (Example: PKI-AAA)

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

Step 6: Click **Submit**.



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

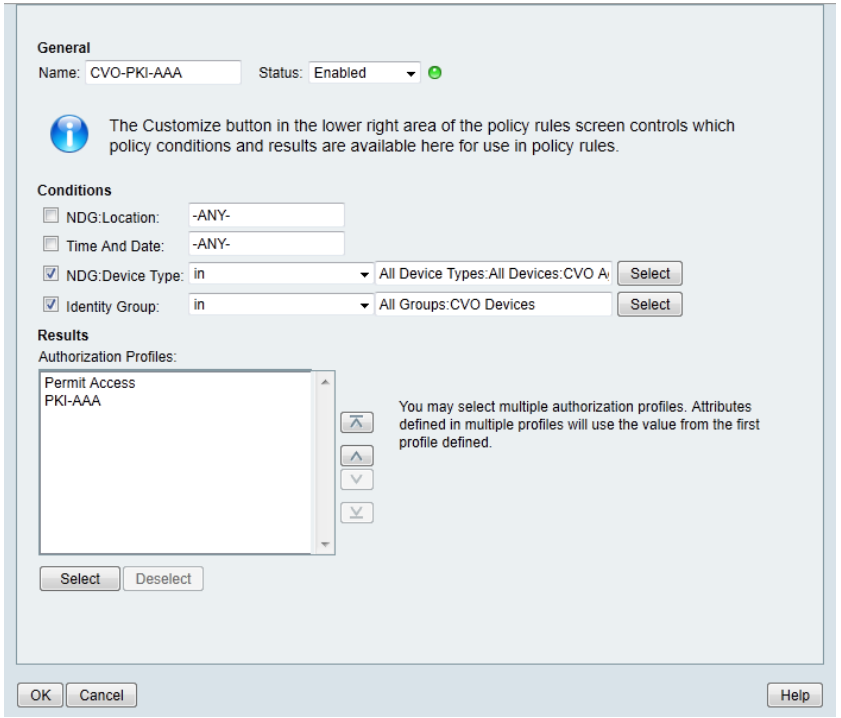
Step 8: Enter a name. (Example: CVO-PKI-AAA)

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**.



Process

Configuring ArcanaNetworks MEVO

1. Integrate MEVO into the SDP Registrar
2. Integrate the primary DMVPN cloud
3. Integrate the resilient DMVPN cloud
4. Integrate MEVO into the Cisco ACS
5. Configure variables for the remote site
6. Configure authentication server
7. Configure subnet blocks
8. Activate CVO remote templates
9. Configure the email server
10. Create end users
11. Provision end users
12. Deploy the 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, you should only need to use MEVO to manage user accounts.

Procedure 1 Integrate MEVO into the SDP Registrar

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 (username **mevoadmin** and password: **mevoadmin**).

Step 3: Navigate to **Configuration** > **Headend**.

Step 4: For the SDP Registrar 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 outside interface of the primary aggregation device. (Example: 172.16.130.2)

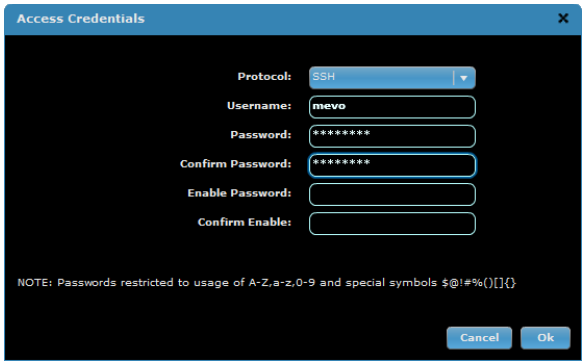
Step 7: Click the icon in the **Passwords** field. The Access Credentials window appears. Next, you enter the access credentials to the primary aggregation device.

Step 8: In the **Username** box, enter the username created in the ACS in Procedure 1 of the "Configuring the Cisco ACS" process. (Example: mevo)

Step 9: Enter and confirm the password, and then click **OK**.

Tech Tip

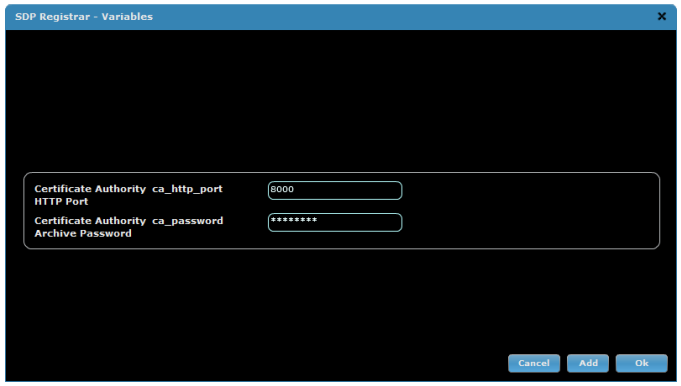
The account you created in ACS for MEVO to manage the aggregation devices is authorized at the enable prompt during login, so you don't have to enter a value in the Enable Password field.



Step 10: Click the icon in the **Variables** field. The SDP Registrar–Variables window appears.

Step 11: In the **Certificate Authority HTTP Port** box, enter **8000**, which is the HTTP port previously configured for SCEP in Step 1 of Procedure 5 in the "Configuring the DMVPN Aggregation Router" process.

Step 12: In the **Certification Authority Archive Password** box, enter the PKI server archive password configured previously on the SDP server in Step 2 of Procedure 5 in the "Configuring the DMVPN Aggregation Router" process, and then click **OK**. (Example: cisco123)



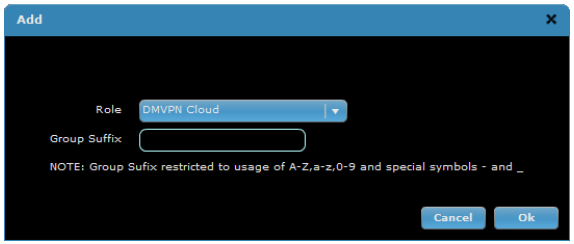
Step 13: Click **Save Changes**. The Task Details window appears, and the Status field shows Passed.

Step 14: Close the Task Details window.

Procedure 2 Integrate the primary DMVPN cloud

Step 1: Click **Add**. The Add dialog box appears. Next, you add a new DMVPN cloud.

Step 2: In the **Role** list, choose **DMVPN Cloud**, and then click **OK**.

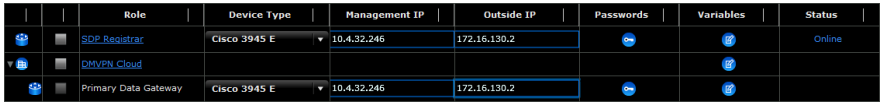


Step 3: Select **Secondary Data Gateway**, and then click **Delete**.

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 outside interface of the primary aggregation device. (Example: 172.16.130.2)



Next, enter the access credentials to the primary aggregation device.

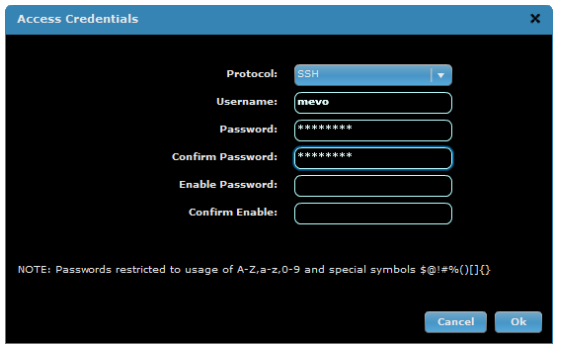
Step 7: Click the icon in the **Passwords** field. The Access Credentials dialog box appears.

Step 8: In the **Username** box, enter the username created in the ACS in Procedure 1 of the "Configuring the Cisco ACS" process. (Example: mevo)

Step 9: Enter and confirm the password, and then click **OK**.

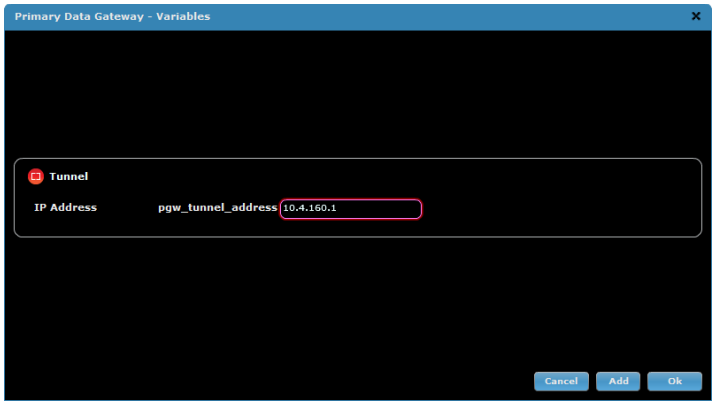
Tech Tip

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 router's tunnel interface, and then click **OK**. (Example: 10.4.160.1)



Step 12: For the DMVPN Cloud, click the icon in the **Variables** field. The DMVPN Cloud–Variables window appears. MEVO assigns an address to each CVO remote router tunnel interface from the tunnel network address.

Step 13: In the **Tunnel Network Address** box, enter the network address for the tunnel interfaces. (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)

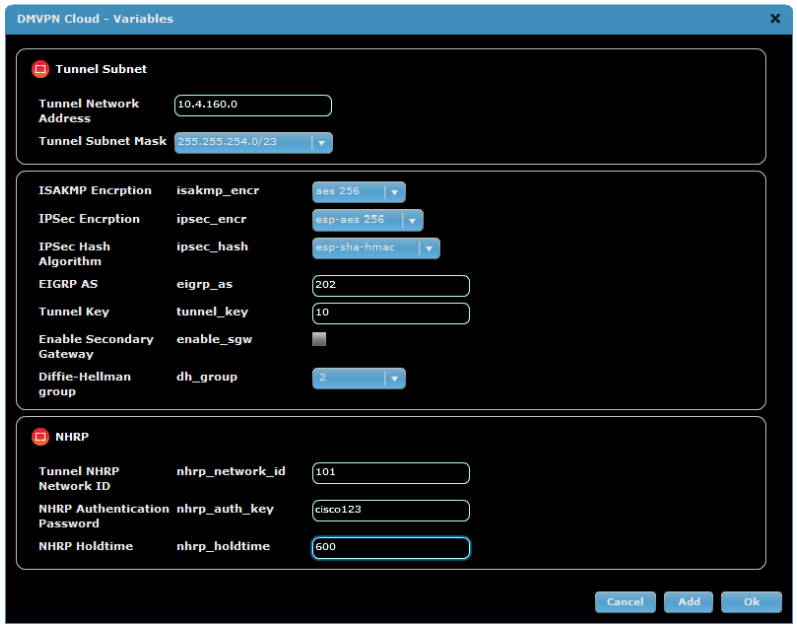
Step 16: In the **Tunnel Key** box, enter the key. (Example: 10)

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**.



Step 21: Click **Save Changes**. The Task Details window appears, and the Status field shows Passed.

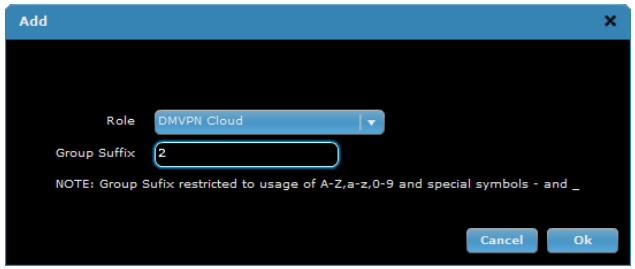
Step 22: Close the Task Details window.

Procedure 3 Integrate the resilient DMVPN cloud

Step 1: Click **Add**. A new DMVPN cloud is added.

Step 2: In the **Role** list, choose **DMVPN Cloud**.

Step 3: In the **Group Suffix** box, enter **2**, and then click **OK**.

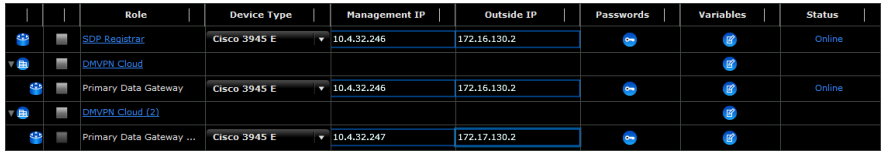


Step 4: Under DMVPN Cloud (2), select **Secondary Data Gateway**, and then click **Delete**.

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 outside interface of the resilient aggregation device. (Example: 172.17.130.2)



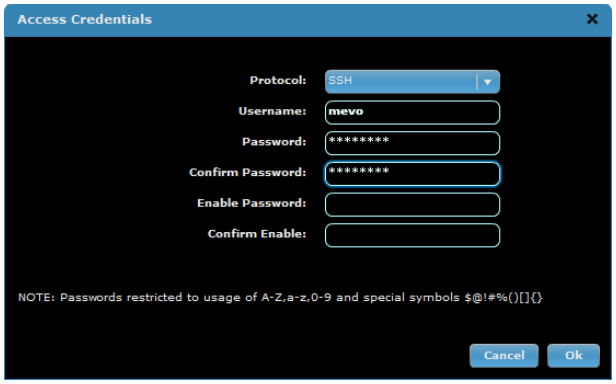
Step 8: Click the icon in the **Passwords** field. The Access Credentials window appears. Next, you enter the access credentials to the resilient aggregation device.

Step 9: In the **Username** box, enter the username created in the ACS in Procedure 1 of the "Configuring Cisco ACS" process. (Example: mevo)

Step 10: Enter and confirm the password, and then click **OK**.

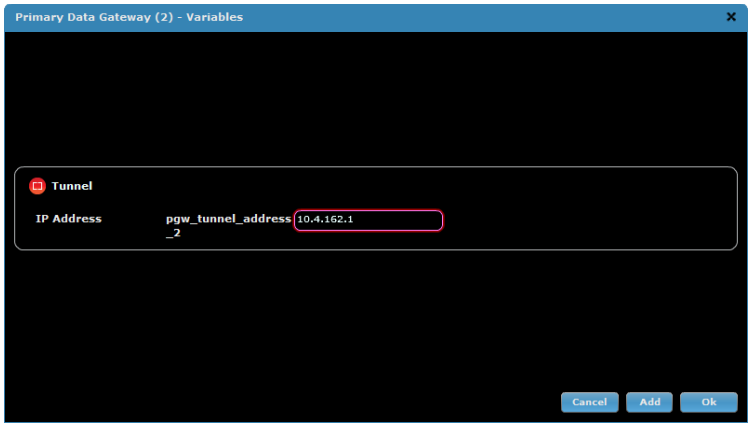
Tech Tip

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)

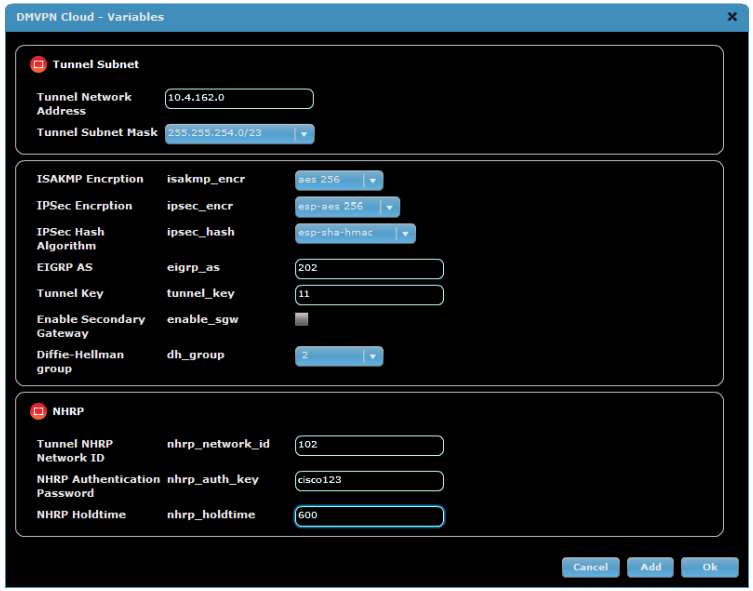
Step 17: Enter the tunnel key. (Example: 11)

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**.



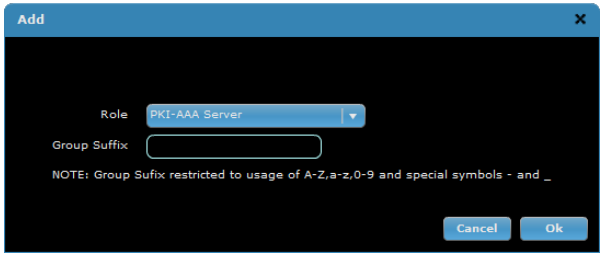
Step 22: Click **Save Changes**. The Task Details window appears, and the Status field shows Online.

Step 23: Close the Task Details window.

Procedure 4 Integrate MEVO into the Cisco ACS

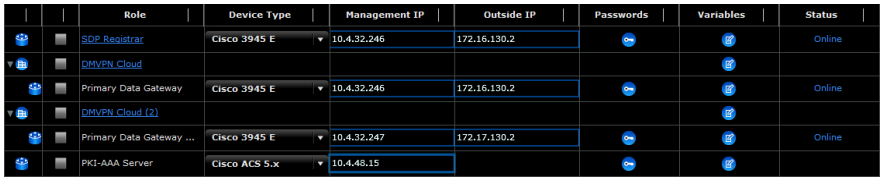
Step 1: Click **Add**. The **Add** dialog box appears.

Step 2: In the **Role** list, choose **PKI-AAA Server**, and then click **OK**.



Step 3: For the PKI-AAA Server in the **Device Type** list, choose **Cisco ACS 5.3**.

Step 4: In the **Management IP** box, enter the IP address of the ACS server. (Example 10.4.48.15)



Next, you enter the access credentials for the ACS server.

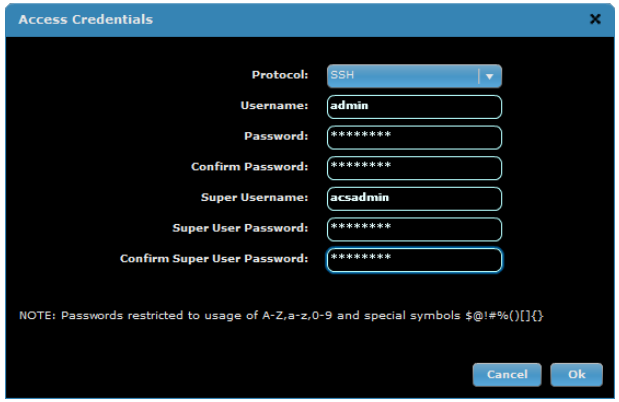
Step 5: Click the icon in the **Passwords** field. The Access Credentials dialog box appears.

Step 6: In the **Username** box, enter the platform username for ACS. (Example: admin)

Step 7: Enter and confirm the password.

Step 8: In the **Super Username** box, enter the web username for ACS. (Example: acsadmin)

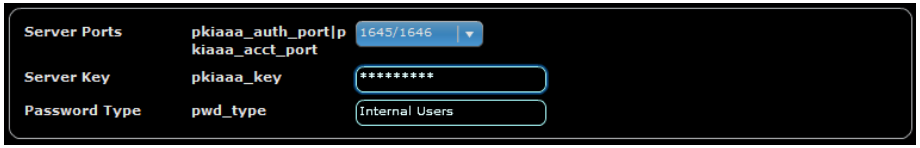
Step 9: Enter and confirm the password, and then click **OK**.



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 **1645/1646**.

Step 12: In the **Server Key** box, enter the RADIUS secret key, and then click **OK**. (Example SecretKey)



Step 13: Click **Save Changes**. The Task Details window appears, and the Status field shows Online.

Step 14: Close the Task Details window.

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**.

Step 17: Click **Save Changes**. The Task Details window appears, and the Status field shows Inventory Success.

Step 18: Close the Task Details window.

Procedure 5 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 username. (Example: admin)

Step 3: In the **Management Password** box, enter a password for the user. (Example: cisco123)

Step 4: In the **Enable Secret** box, enter a password. This allows users to escalate their privilege levels on the CVO remote router,

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)

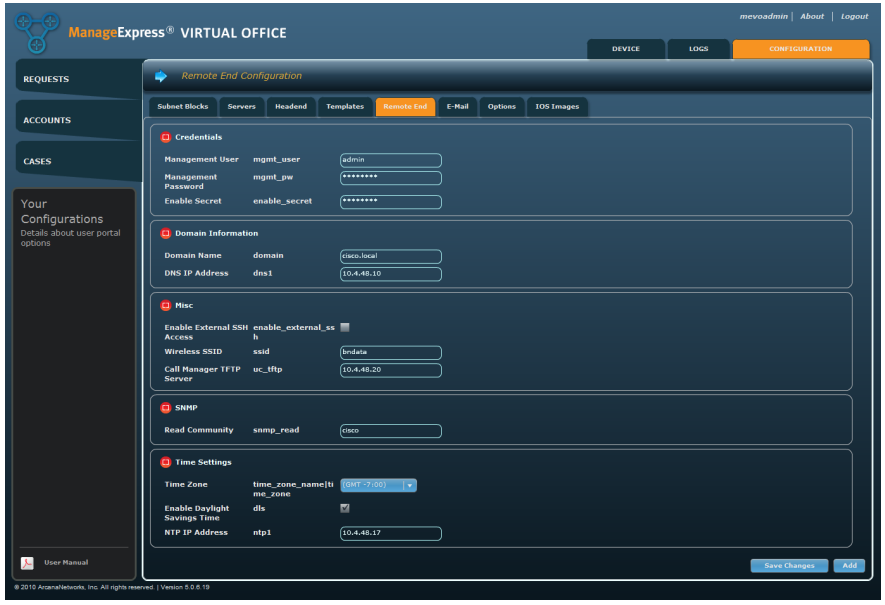
Step 8: In the **Call Manager TFTP Server** box, enter the IP address of the organization's Cisco UCM TFTP Server. (Example: 10.4.48.120)

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: In the **NTP IP Address** box, enter the IP address of the NTP server, and then click **Save Changes**. (Example: 10.4.48.17)



Procedure 6 Configure authentication server

Step 1: Navigate to **Configuration** > **Servers**.

Step 2: For the Authentication Server in the **Device Type** list, choose **RADIUS Server**.

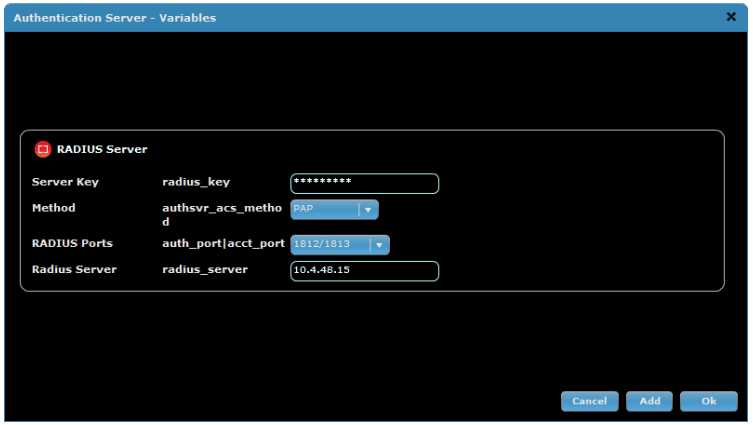
Step 3: In the **Hostname/IP** box, enter the IP address of the organizations AAA server. (Example: 10.4.48.15)

Step 4: Click the icon in the Variables field. The Authentication Server – Variables window appears.

Step 5: In the **Server Key** box, enter the shared secret for the AAA server. (Example: SecretKey)

Step 6: In the **Method** list, choose **PAP**.

Step 7: In the **RADIUS Ports** list, choose **1645/1646**, and then click **OK**.



Step 8: On the Servers Configuration pane, click **Save Changes**.

Procedure 7 Configure subnet blocks

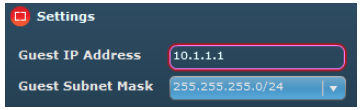
Configure support for users who are connecting to the Internet via the CVO remote router but who aren't employees of the organization.

Step 1: In **Configuration** > **Subnet Blocks**, in the **Settings** pane, in the **Guest IP Address** box, enter a network address. (Example: 10.1.1.1)

Step 2: In the **Guest Subnet Mask** list, choose the subnet size. (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 NAT.



Now you define the network range from which to assign unique remote LAN networks for each CVO remote router.

Step 3: In **Configuration > Subnet Blocks,** click **Add**.

Step 4: In the **Name** box, enter the name of the network. (Example: Remote LAN)

Step 5: In the **Description** box, enter a summary of the network. (Example: LAN)

Step 6: In the **Type** list, choose **LAN**.

Step 7: In the **LAN Type** list, choose Default.

Next, define the network range from which to assign remote subnets.

Step 8: In the **Network Address** box, enter an IP address. (Example: 10.4.128.0)

Step 9: 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 10: Select the subnet size from the **LAN subnet mask** list, and then click **OK**. (Example: 255.255.255.248/29)

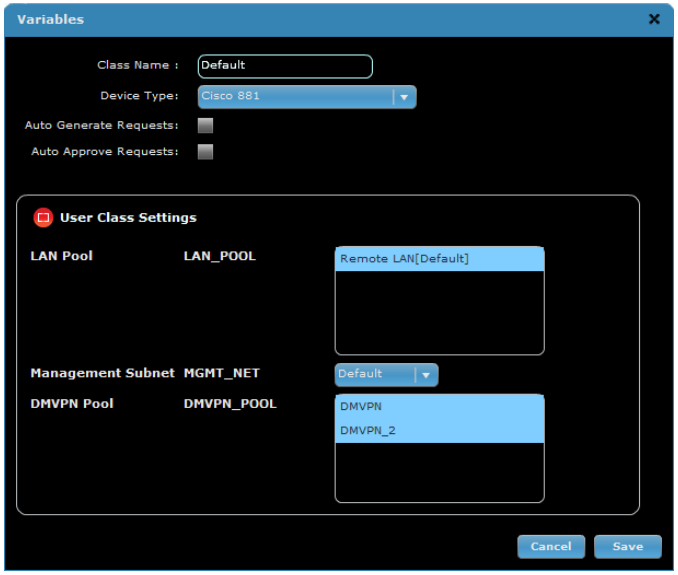
Step 11: In the confirmation window, click **Add**. The Add New User Class dialog box appears.

Next, you define the type of device used for the CVO remote routers,

Step 12: In the **Device Type** list, choose **Cisco 881**.

Step 13: In the **LAN Pool** pane, select **Remote LAN[Default]**.

Step 14: In the **DMVPN Pool** pane, select both **DMVPN** and **DMVPN_2**, and then click **OK**.



Procedure 8 Activate CVO remote templates

Add the resilient DMVPN cloud template from Appendix B into MEVO, edit the firewall configuration, and select the appropriate templates.

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: Click **Browse**.

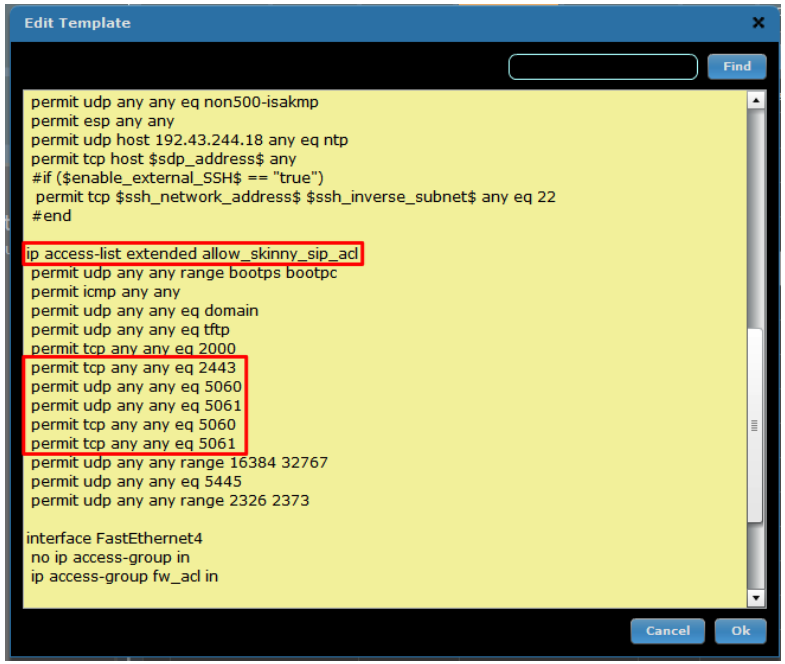
Step 7: In the **Template File** box, select the file you created in Step 1, and then click **Import**.

Step 8: Click the **Edit** icon next to **Firewall Configuration**.

Step 9: Find the **allow_skinny_acl** access list and edit the title to **allow_skinny_sip_acl** to better reflect its new purpose.

Step 10: Add the following rules to the **allow_skinny_sip_acl** to allow additional standard voice protocols.

```
permit tcp any any eq 2443
permit udp any any eq 5060
permit udp any any eq 5061
permit tcp any any eq 5060
permit tcp any any eq 5061
```



Step 11: Click **Ok** to accept the edits.

Step 12: To the right of Wireless Configuration, Firewall Configuration, QoS Configuration, and DMVPN Configuration for the template you added in Step 7, select **Active**, and then click **Save**.

Tech Tip

The default wireless configuration template does not broadcast the wireless SSID. Clients must be configured with the SSID to connect.

	Type	Device Type	Filename	Access Point	Active	Edit
☐	Base Configuration	Cisco 881	1-step-881.cfg	No	☑	
☐	Wireless Configuration	Cisco 881	wireless-881.cfg	Yes	☑	
☐	EEM Configuration	Cisco 881	EEM-881.cfg	No	☑	
☐	Authproxy Configuration	Cisco 881	authproxy-881.cfg	No	☐	
☐	Firewall Configuration	Cisco 881	classicfw-881.cfg	No	☑	
☐	Dot1x Configuration	Cisco 881	dot1x-881.cfg	No	☐	
☐	QOS Configuration	Cisco 881	qos-881.cfg	No	☑	
☐	DMVPN Configuration	Cisco 881	New DMVPN Configuratio	No	☑	
☐	DMVPN Configuration	Cisco 881	dmvpn-881.cfg	No	☐	

Step 13: In the confirmation window, click **Save**.

Procedure 9 Configure the email server

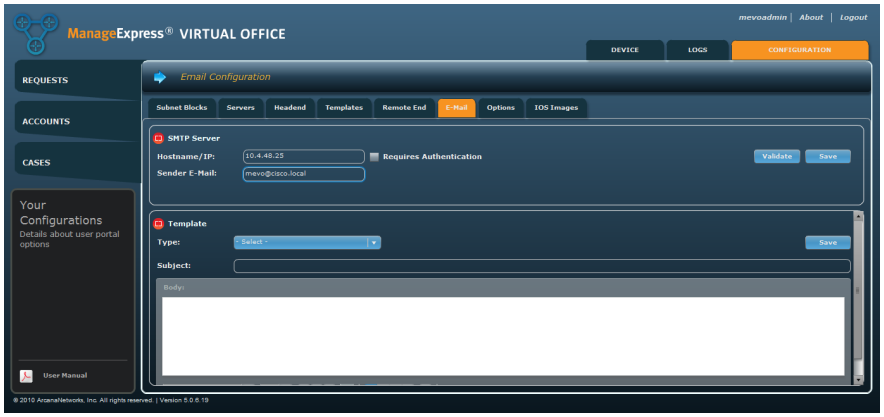
To ease the approval and deployment of CVO, ArcanaNetworks MEVO automatically generates email messages for CVO approvers and users during the provisioning process.

Configure the Simple Mail Transfer Protocol (SMTP) server to send mail.

Step 1: Navigate to **Configuration** > **E-mail**.

Step 2: In the **Hostname/IP** box, enter the host name 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 10 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's approval is not required.
- **Approver**—This role approves or declines an end user's request for Cisco Virtual Office in the typical Cisco Virtual Office deployment workflow.
- **End user**—This role includes the teleworker.
- **User administrator**— This role can manage user accounts, perform device operations, view logs, and handle support cases.

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)

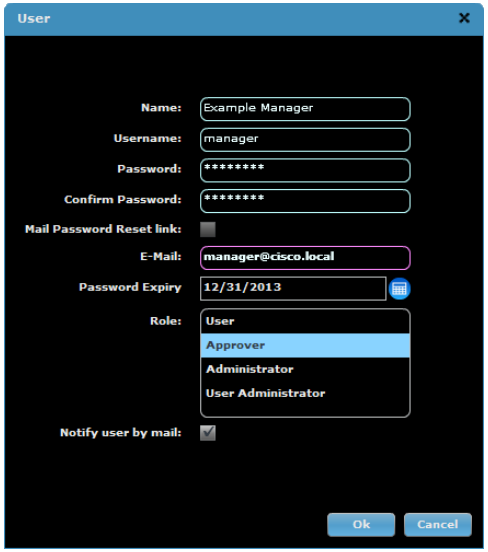
Step 3: Enter the manager's username. (Example: manager)

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 **Approver**.

Step 7: Select **Notify user by mail**, and then click **OK**.



Next, create an end user for CVO provisioning.

Step 8: Click **Create User**.

Step 9: Enter the user's name. (Example: Employee One)

Step 10: Enter the user's username. (Example: employee1)

Step 11: Enter and confirm the password.

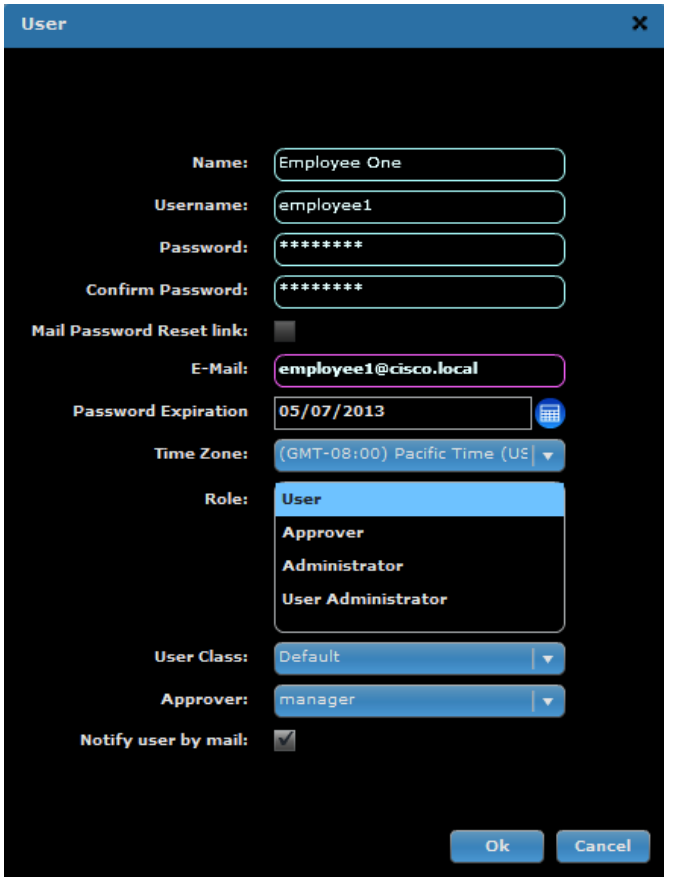
Step 12: Enter the user's email address. (Example: employee1@cisco.local)

Step 13: In the **Role** list, choose **User**.

Step 14: In the **User Class** list, choose **Default**.

Step 15: In the **Approver** list, choose the username created in Step 3. (Example: manager)

Step 16: If you want to send the user an email with instructions on how to start the SDP server after that user is provisioned, select **Notify user by mail**, and then click **OK**.



Tech Tip

Ensure the user added to MEVO has matching user data in Active Directory so that RADIUS AAA requests to ACS during the provisioning process can be authenticated properly. In this case *employee1* is a valid user ID in both MEVO and Active Directory.

Procedure 11 Provision end users

This procedure describes the SDP process from the end user's perspective and shows what needs to be done after the end 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.

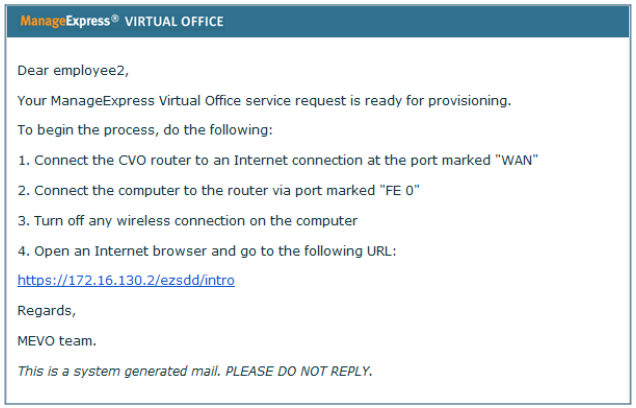
Step 1: Navigate to the **Accounts** tab.

Step 2: Select the user for whom 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: In the **Upload Speed** list, choose the correct uplink speed for CVO remote. (Example: 1Mbps) This enables proper prioritization of voice traffic as it leaves the remote site.

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.


ManageExpress® VIRTUAL OFFICE

Dear employee2,

Your ManageExpress Virtual Office service request is ready for provisioning.

To begin the process, do the following:

1. Connect the CVO router to an Internet connection at the port marked "WAN"
2. Connect the computer to the router via port marked "FE 0"
3. Turn off any wireless connection on the computer
4. Open an Internet browser and go to the following URL:

https://172.16.130.2/ezsdd/intro

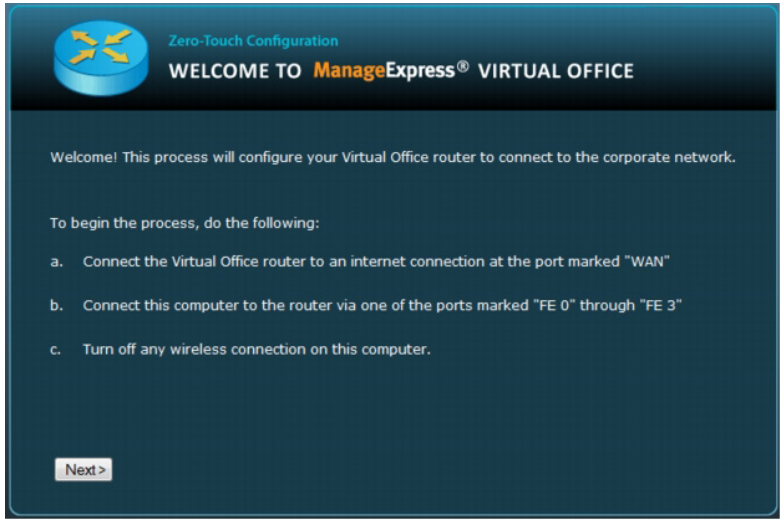
Regards,

MEVO team.

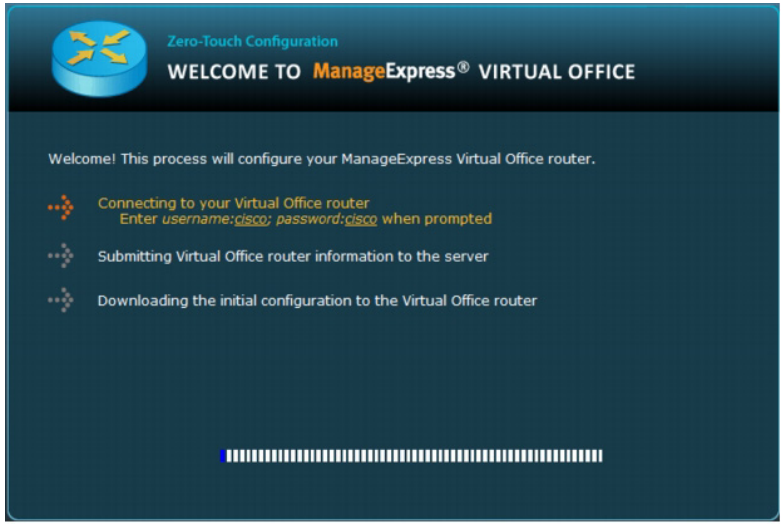
This is a system generated mail. PLEASE DO NOT REPLY.

Step 6: When the pop-up screen asks for user credentials, enter the appropriate AAA credentials.

Step 7: On the welcome screen, click **Next**.



ArcanaNetworks MEVO connects to the router to begin configuration.

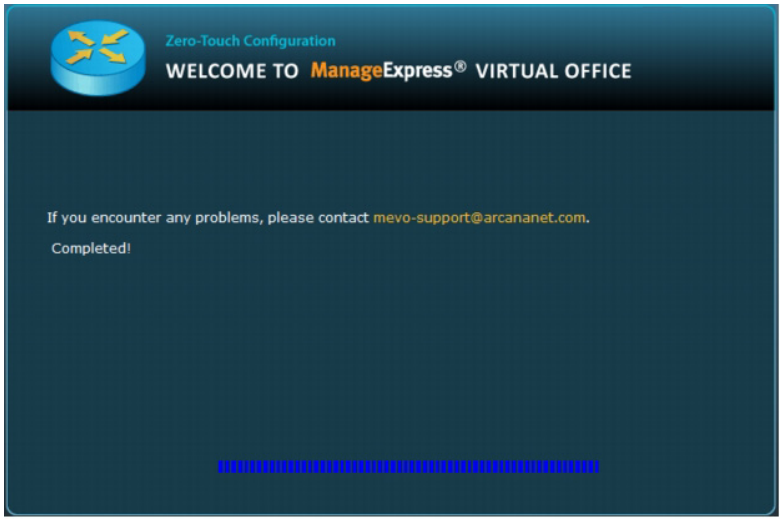


Tech Tip

Enter the username **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 12 Deploy the authentication proxy

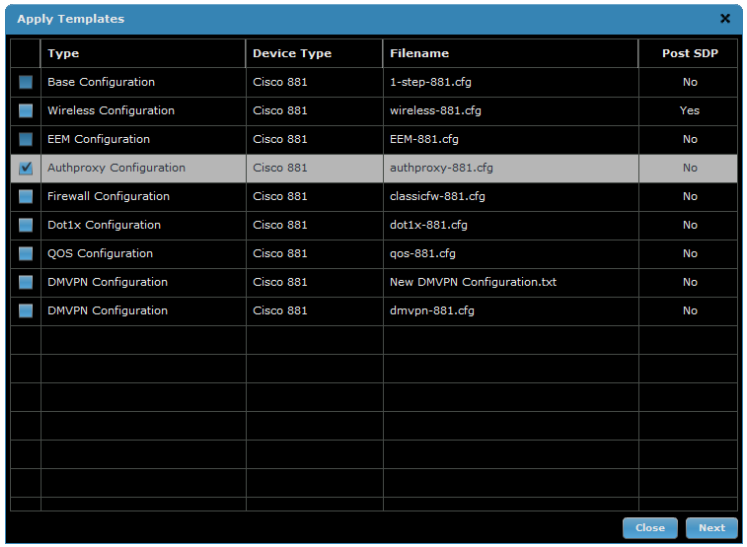
Step 1: Navigate to the **Device** tab.

Step 2: Click the portion of the graph labeled **Online**.

Step 3: In the list of devices, select the CVO remote router 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**.



Step 6: Select **Start Immediately**, and then click **Next**. The template is deployed when the Status field shows Passed.

Step 7: Click **Close**.

Appendix A: Product List

CVO

Functional Area	Product Description	Part Numbers	Software
CVO Aggregation	Cisco 3945E Security Bundle w/SEC license PAK	CISCO3945E-SEC/K9	15.1(4)M5 securityk9 license datak9 license
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
CVO Management	ArcanaNetworks System License	L-SP-MESYSTEM=	5.0.8.3(11.0.0.21)
	ArcanaNetworks Base License	L-SP-MEBASE-B-100=	
	ArcanaNetworks MEVO License	L-SP-MEVO-100=	
CVO Remote Router	Cisco 881 Ethernet Security Router with 802.11n FCC Compliant	C881W-A-K9	15.1(4)M5 Advanced IP Services license
	Cisco 880 Advanced IP Services License	SL-880-AIS	
	2 Port PoE Module for 880 Series Router	800G2-POE-2	
	Cisco Virtual Office config for Cisco 871/881	CVO800-CFG	

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Internet Edge

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

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE IP Base license

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

CVOAGG-3945E-1

```
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 system flash0:/c3900e-universalk9-mz.SPA.151-4.M2.bin
boot-end-marker
!
!
enable secret 5 $1$4uvF$AkH1EQDz..P/oUzLGJM.m/
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa group server radius RADIUS-SERVERS
 server name RADIUS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authentication login sdp-acs group RADIUS-SERVERS
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
aaa authorization network sdp-acs group RADIUS-SERVERS
!
!
!
!
!
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 MEVO 10.4.48.29
ip host cvo-cs 10.4.32.246
!
multilink bundle-name authenticated
!
!
!
!
!
!
```

```
crypto pki server cvo-cs
 database level complete
 database archive pkcs12 password 7 045802150C2E1D1C5A
 issuer-name cn=cvo-cs,ou=cvo
 grant auto
 auto-rollover
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-3411892186
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3411892186
 revocation-check none
 rsakeypair TP-self-signed-3411892186
!
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 0608002F49
 revocation-check crl
 auto-enroll 75
 authorization list sdp-acs
!
!
!
crypto pki certificate map DMVPN 10
 issuer-name co cvo-cs
 unstructured-subject-name co cisco.local
!
crypto pki certificate chain TP-self-signed-3411892186
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 33343131 38393231 3836301E 170D3132 30363036
32313239
  31395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33
34313138
  39323138 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100DE69 4A3BCB1F 6AE008A4 31FF9BA8 0485498E 29135E54 D6F4ED55
EA3293B5
  0BD9A51F 3A6BEB56 390B6F25 AED6D35C 0282D2F3 888AC83A 24F4C32E
CC1F378A
  91C23231 71329683 F222C837 E3F691B8 A55FC623 5375412C 82AE4D75
E8A0FEA8
  6827FBE1 116F0464 9AA8560E 35E3D9EA CC1026D2 75F9450B D6119904
36664CB2
  46FF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 14BD4034 69861846 7FD7156C B9649EC1 6FC8071F
7E301D06
  03551D0E 04160414 BD403469 8618467F D7156CB9 649EC16F C8071F7E
300D0609
  2A864886 F70D0101 05050003 81810007 698A6CBF A2E6B8EB 8A858589
DCF5C42A
  AC516736 6397B0B0 E0ABB692 FAD0EDE4 F3006BA4 2CC87819 B25F29FA
143A019E
  5BF2C690 AC4D3C18 4AA33D08 8DDF6554 B4D2FC27 5C3DD3FE 3DEB68E1
C8BDA205
  D329CF07 0EEBE57F 5108D438 17112A29 EB2EC9AA 7754D60F 457FCE35
DC8736F4
  1CCF433F 2929DFBC 46BF74F4 5887F9
        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 31323036 30363231 33383433 5A170D31 35303630 36323133
3834335A
  301F310C 300A0603 55040B13 0363766F 310F300D 06035504 03130663
766F2D63
  7330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B8BB
  3BBE9A7E 7DCA8673 B6E906B7 A2DF2EEA 71FD2BC8 D41AF818 E0400FC1
51BFCE7C
  1063C5A9 672AF966 F4A3C42F AD83DBC2 4D721FC8 C9F9C099 3C07E1BB
0EC24632
  0341F8B7 25DF2811 5ED58247 DA3D233D 09D5FDEB A5BABA12 46337457
2B8996C5
  D87485A7 CF918AF9 6C2F8DF8 9603453C B4EB1781 1A5A255C 01E8B4F1
14630203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603
551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1411A486 282EB8C0
FA33810E
  9ADEB399 A7E8FB9E 12301D06 03551D0E 04160414 11A48628 2EB8C0FA
33810E9A
  DEB399A7 E8FB9E12 300D0609 2A864886 F70D0101 04050003 81810034
0131EBDE
  088A4EBB 53BA6403 951CC1D3 208542D1 EFC2F3CB 7F1CE416 D4368673
992E1510
  2CDBDBAF C3AE5453 786A2F0A BC72CB30 26504146 F18FDFE5 4307AD48
0423896E
  02866761 0926ABAD 442DF20C 034DB87D D006FFD7 B481DB27 7EBF8A1C
73E80A78
  FCAE7938 761A1762 AF3EAD00 DCAD9822 ABF4DD9B AEE0FC1D 6A6EF4
       quit
crypto pki certificate chain cvo-pki
 certificate 03
  308202A7 30820210 A0030201 02020103 300D0609 2A864886 F70D0101
05050030
  1F310C30 0A060355 040B1303 63766F31 0F300D06 03550403 13066376
6F2D6373
  301E170D 31323036 30363231 35343434 5A170D31 33303630 36323135
3434345A
  303F313D 30120603 55040513 0B46484B 31343037 46325157 30270609
2A864886
  F70D0109 02161A43 564F4147 472D3339 3435452D 312E6369 73636F2E
6C6F6361
  6C308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201
  0100A89B DC9969A9 EC31E3AA F21F0005 0961BC06 2512EAFE 35DCF976
23A764A0
  509D2F3E A6328A78 9E5399AB 9413601B 775C0BC3 11D6FA49 EEAF76F4
E0C44141
  EEB50A5E E559CAEE 67A37102 EEE34A53 941BF3A6 DA0B10B6 B0D46D1C
788ADB5C
  083F5189 F3967B90 C9699670 A29ABD4D A12ACF63 10D15C2A E3C6D432
43603FDE
  42379431 C429613F 41E8DAF1 256615F2 1DC8368D 18363069 0AEF89DD
D2CECF1A
  CAC01395 5B1D9A4F 68AFFC52 89222FAB 206775EC BF09A522 9079FFDA
FE643AFB
  B74CE110 D8E5F599 02572976 526F348F 47E83359 259C2C02 D40B2A4B
50BC6862
  7C63ED92 C1A5466D B36EB443 2C338E3D 3D33DC57 A5348E65 1C788161
3F99BD5D
  1FE70203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
551D2304
  18301680 1411A486 282EB8C0 FA33810E 9ADEB399 A7E8FB9E 12301D06
03551D0E
  04160414 68B2797C 5B1A838F C4EDEC87 AC00331D 62C4B2DD 300D0609
2A864886
  F70D0101 05050003 8181005F 4C789A35 D6245FC7 F3B4A9D8 4F76FA15
88EC1F30
  35BC79E3 CBF62DF1 EE6C4337 D3F9B434 E3DA849F 8EFF8EC1 755F2E62
89307FBC
  41980E82 68C6D523 EEE9EDE9 EA4B9DAD ABD88A12 55FD669F E181E543
```

```
0C14E7C1
  F7AFF8CC BFFA811B 65ADFEAB 3BBBCB4C 1D6E32C2 FDB3AC82 1F977059
0BDCB0C6
  39E8C629 BC2C4EE6 57971D
       quit
 certificate ca 01
  30820217 30820180 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  1F310C30 0A060355 040B1303 63766F31 0F300D06 03550403 13066376
6F2D6373
  301E170D 31323036 30363231 33383433 5A170D31 35303630 36323133
3834335A
  301F310C 300A0603 55040B13 0363766F 310F300D 06035504 03130663
766F2D63
  7330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B8BB
  3BBE9A7E 7DCA8673 B6E906B7 A2DF2EEA 71FD2BC8 D41AF818 E0400FC1
51BFCE7C
  1063C5A9 672AF966 F4A3C42F AD83DBC2 4D721FC8 C9F9C099 3C07E1BB
0EC24632
  0341F8B7 25DF2811 5ED58247 DA3D233D 09D5FDEB A5BABA12 46337457
2B8996C5
  D87485A7 CF918AF9 6C2F8DF8 9603453C B4EB1781 1A5A255C 01E8B4F1
14630203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603
551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1411A486 282EB8C0
FA33810E
  9ADEB399 A7E8FB9E 12301D06 03551D0E 04160414 11A48628 2EB8C0FA
33810E9A
  DEB399A7 E8FB9E12 300D0609 2A864886 F70D0101 04050003 81810034
0131EBDE
  088A4EBB 53BA6403 951CC1D3 208542D1 EFC2F3CB 7F1CE416 D4368673
992E1510
  2CDBDBAF C3AE5453 786A2F0A BC72CB30 26504146 F18FDFE5 4307AD48
0423896E
  02866761 0926ABAD 442DF20C 034DB87D D006FFD7 B481DB27 7EBF8A1C
73E80A78
  FCAE7938 761A1762 AF3EAD00 DCAD9822 ABF4DD9B AEE0FC1D 6A6EF4
       quit
voice-card 0
!
!
!
!
!
!
!
license udi pid C3900-SPE250/K9 sn FOC14034Z6F
!
!
username admin password 7 130646010803557878
!
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
  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
!
!
!
crypto provisioning registrar
 pki-server cvo-cs
 template http welcome http://10.4.48.29/mevo/sdp/2-sdp_welcome.
html
 template http completion http://10.4.48.29/mevo/sdp/4-sdp_
completion.html
 template http introduction http://10.4.48.29/mevo/sdp/3-sdp_
introduction.html
 template http start http://10.4.48.29/mevo/sdp/1-sdp_start.html
 template http error http://10.4.48.29/mevo/sdp/sdp_error.html
 template config http://10.4.48.29/mevo/Configs/$n_Bootstrap.cfg
 template username administrator password 7 0508571C22431F5B4A
 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 10.4.32.246 255.255.255.255
 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
 description WAN-D3750X Gig1/0/13
 no ip address
 duplex auto
 speed auto
 channel-group 30
!
interface GigabitEthernet0/1
 description WAN-D3750X Gig2/0/13
 no ip address
 duplex auto
 speed auto
 channel-group 30
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
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
 service-policy output WAN
!
!
!
router eigrp 100
 network 10.4.0.0 0.1.255.255
 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 8000
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
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65520
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 113A1C0605171F270133
!
radius server RADIUS-SERVER-1
 address ipv4 10.4.48.15 auth-port 1645 acct-port 1646
 key 7 01200307490E12242455
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
end
```

Appendix D: Changes

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

- We made minor changes to improve the technical accuracy and readability of this guide.
- We added a section describing the addition of voice protocols into the ACLs provisioned on teleworker routers.
- We updated the code version of the ISR G2 aggregation and teleworker routers.

Notes

Feedback

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

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.

B-0000305-1 2/13