Cisco Virtual Office Express Deployment Guide

Contents

Scope of Document

This document provides a deployment guide for the Cisco® Virtual Office Express solution.

For additional information about related solutions, architectures, and components, please refer to http://www.cisco.com/go/cvo.

Introduction

Cisco® Virtual Office Express is a solution that provides secure, rich network services to workers at locations outside the traditional corporate office, including part-time teleworkers, workers in small offices, and mobile workers. Compared to Cisco Virtual Office, Cisco Virtual Office Express has a simplified headend and management architecture, thus enabling faster deployment of the virtual office solution. It can be deployed rapidly at both the headend and the spoke side without compromising either feature richness or security.

Cisco Virtual Office Express

Cisco Virtual Office Express uses the Cisco Enhanced Easy VPN technology, which can push VPN policies from the server to the remote side when the remote side comes online, simplifying the remote router VPN configuration. Cisco Virtual Office Express, like Cisco Virtual Office, enables zero-touch deployment by using Cisco Secure Device Provisioning (SDP). SDP can securely, over the Internet, install a configuration file and a public key infrastructure (PKI) certificate without any administrator intervention. From the end user's perspective, the full provisioning is accomplished in a few minutes, after the Cisco Virtual Office Express router is connected to the Internet. In terms of headend and remote-site platform support, Cisco Virtual Office Express supports the same devices as Cisco Virtual Office. Cisco Configuration Engine may be added to facilitate the ongoing configuration updates and Cisco IOS® Software upgrades of the Cisco Virtual Office Express router. This document is divided into two main sections. The first section discusses in detail how standard Cisco Virtual Office Express is deployed. The second section shows how to add components for advanced management tasks and high-availability options for redundancy.

Platforms and Images

Please refer to the "Cisco Virtual Office Supported Hardware and Software" at http://www.cisco.com/go/cvo for image and platform recommendations for Cisco Virtual Office Express.

Identity Management

End users and devices should be authenticated before access to corporate resources is permitted. Both headend and remote routers query an authentication, authorization, and accounting (AAA) server for this purpose. Cisco Virtual Office Express can use an existing corporate AAA server, as long as it supports RADIUS with respective attribute-value pairs. Cisco Secure Access Control Server (ACS) 5.0 can be deployed as the AAA server. Cisco Virtual Office Express uses the AAA server for initial deployment (the SDP process) as well as for authentication and authorization of users and devices for PKI-AAA, wireless, IEEE 802.1x, and authentication proxy.

Deployment Components

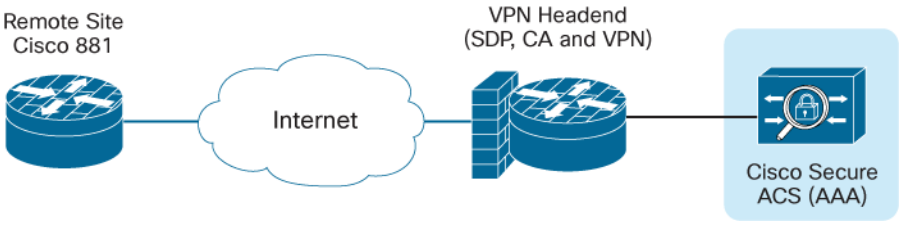
The components required to deploy Cisco Virtual Office Express are as follows:

- Headend site
  - VPN headend router: This router is responsible for SDP, and it acts as the certificate authority (CA) and VPN gateway where remote-site tunnels are terminated. It has the corporate network behind it.
  - An AAA server is required for authentication of the various components of the Cisco Virtual Office Express solution, as explained previously. The AAA server is hosted on the management network of the corporate office.
- Teleworker site or small office

- For the recommended platforms, please refer to the “Cisco Virtual Office Supported Hardware and Software” at http://www.cisco.com/go/cvo

Figure 1 shows the components of the Cisco Virtual Office Express solution.

Figure 1. Cisco Virtual Office Express Design



Cisco Virtual Office Express Deployment Steps

Headend and Management Side

1. Assign an Internet-facing IP address to the VPN gateway.
2. Open ports on the corporate firewall.

   Headends need to send and receive Internet Key Exchange (IKE) and IP Security (IPsec) packets. User Datagram Protocol (UDP) ports 500 and 4500 and Encapsulated Security Payload (ESP) port (IP 50) should be opened.

   The SDP server needs HTTPS (TCP 443) and HTTP (port 80 can be used, but using an alternate port, such as TCP 8000, is better).

3. Reserve an IP address pool for the Cisco Easy VPN connections.

   Every time a CPE device connects to the VPN server, an IP address from the pool will be pushed to that device. This pool should be routable companywide.

4. Install the VPN headend.

   The headend acts as the SDP server, CA, and VPN gateway. The SDP server pushes a template-based configuration to the remote site and installs a PKI certificate. In the case of Cisco Virtual Office Express, the full configuration is pushed to the client.

   To set up the server as a CA, configure the hostname, domain name, time zone, and Network Time Protocol (NTP) server for clock synchronization (if the router does not have a built-in hardware clock). In addition, the HTTP server should be enabled on the server to allow clients to perform Simple Certificate Enrollment Protocol (SCEP) enrollment. Set up the router as a VPN gateway to terminate tunnels. All these aspects are shown in the configuration samples in the section “VPN Server”.

5. Create the spoke template configuration.

   This configuration will be pushed to the client. It can be stored in the headend router flash memory or NVRAM, on an FTP network server, on an HTTP and HTTPS server, or on a network server that supports Secure Shell (SSH) Protocol. Please refer to the sample configuration in the section “Spoke Template Configuration.” Additionally, the SDP templates should also be customized and stored in any of the locations mentioned previously.

   Features such as IEEE 802.1x, authentication proxy, wireless access, and quality of service (QoS) can enhance the capabilities of the VPN as well as provide additional security. Sample configurations can be found in the section “Configuration of Additional Features”.

6. Set up the AAA server.

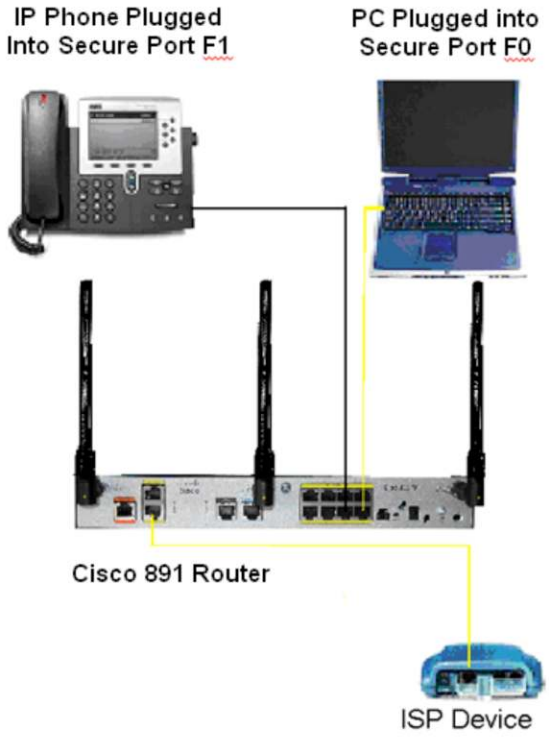
   Create a profile in the Cisco ACS, or set up the corporate AAA server for user authentication for the initial provisioning.

End-User Side

1. Connect to the Internet.

   Routers ordered with the Cisco Virtual Office option come from the factory with Dynamic Host Configuration Protocol (DHCP) enabled on the WAN side. This configuration accounts for about 92 percent of use cases, based on a Cisco internal survey. If connecting from home using a static address or PPPoE, use Cisco Configuration Professional on the client to connect to the Internet. Set up the router as shown in Figure 2.

Figure 2. Cisco Virtual Office Express Setup



2. Start the automatic provisioning of the new router.

   Connect a PC to the Cisco 881 or 891 router port FE0, and the Cisco 881 router FastEthernet4 WAN interface (FE8 for the 891) to the Internet (modem or Network Address Translation [NAT] router). Then follow these steps:

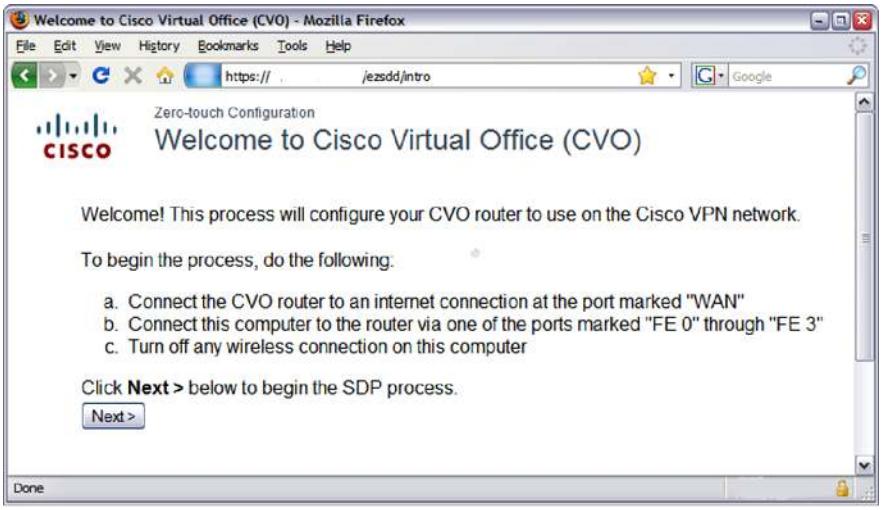
   a. Click the web link provided in the email received from your Cisco Virtual Office Express administrator.

   b. Enter your credentials in the pop-up username and password dialog box (Figure 3).

Figure 3. Authentication

c. Click Next to start the installation of the configuration in the router (Figure 4).

Figure 4. Cisco Virtual Office Welcome Window

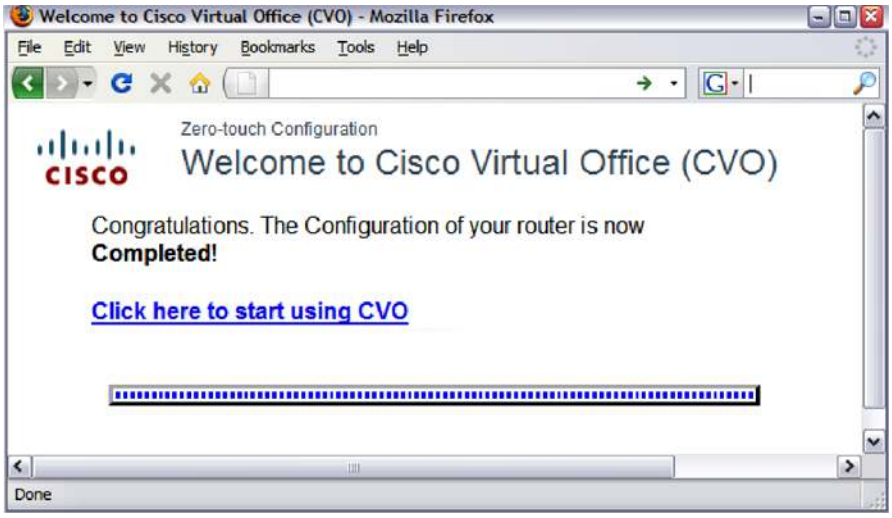


The remote router will be automatically configured from the server (Figure 5).

Figure 5. Automatic Configuration of Remote Router

The user will be informed when the router is ready (Figure 6).

Figure 6. Router Configuration Complete



Ongoing Management

This section outlines the tasks of the Cisco Virtual Office Express administrator when adding or removing users and updating the Cisco IOS Software configuration.

Adding a New User

There are two ways to add a new user to the VPN:

- Allow all users with valid corporate credentials to join the VPN (nothing needs to be done; all corporate users are automatically allowed).

  Note that you can still add a PKI-AAA authorization list to the VPN headend PKI trust point so that only devices that have valid profiles in the AAA server can build IPsec tunnels. Refer to the discussion of PKI-AAA in the Cisco Virtual Office - AAA Deployment guide for details.
- Add users in the SDP (simply add usernames and passwords to the Cisco IOS Software command line).

Removing a User

Revoke the PKI certificate by following these steps:

Note: These commands are supported in Cisco IOS Software Release 12.4(20)T and later only.

1. On the certificate server, use the following command to obtain the certificate serial number for user user1.domain-name.com:

```
show crypto pki server <server-name> certificates | include
user1.domain-name.com
```

Sample output:

```
server#show crypto pki server pki-ca certificates | inc user1.cisco.com
```

```
     11      21:33:26 PDT Mar 24 2009 21:33:26 PDT May 23 2009
serialNumber=FTX0917A02E+
           hostname = user1.cisco.com
```

2. Revoke the certificate using the following command:

```
crypto pki server <server-name> revoke <Serial Number in Hexadecimal>
```

3. (Optional) If PKI-AAA is used, delete the AAA profile for the router (it will be username.domainname.com). Look in the Cisco Virtual Office-AAA Deployment guide at http://www.cisco.com/go/cvo for more information.

Performing Basic Cisco IOS Software Configuration Updates

In the absence of the configuration engine, you can push a configuration URL through a mode-configuration exchange. This feature allows any configuration change to be pushed to any number of Cisco IOS Easy VPN clients. It also provides zero-touch provisioning of any feature, including voice and routing. The following example shows how this feature works by configuring a Cisco IOS firewall policy on the Cisco Easy VPN remote:

1. Create the policy in a text file named vpn.cfg and place it in the corporate network; for example, TFTP server 172.16.30.2**.**

vpn.cfg

```
ip inspect name DEFAULT100 cuseeme
ip inspect name DEFAULT100 ftp audit-trail on timeout 3600
ip inspect name DEFAULT100 h323 timeout 3600
ip inspect name DEFAULT100 icmp
ip inspect name DEFAULT100 netshow
ip inspect name DEFAULT100 rcmd
ip inspect name DEFAULT100 realaudio
ip inspect name DEFAULT100 rtsp
ip inspect name DEFAULT100 esmtp
ip inspect name DEFAULT100 sqlnet
ip inspect name DEFAULT100 streamworks
ip inspect name DEFAULT100 tftp
ip inspect name DEFAULT100 tcp
ip inspect name DEFAULT100 udp
ip inspect name DEFAULT100 vdolive

access-list 101 permit esp any any
access-list 101 permit udp any any eq isakmp
access-list 101 deny   ip any any

interface f 0/0
ip access-group 101 in
ip inspect DEFAULT100 out
```

2. To successfully update the configuration, configure the version number on the server to a number higher than the one used on the client. For example, if the configuration version on the client is 10, the following server configuration would be valid:

```
 crypto isakmp client configuration group vpn
```

```
key vpnkey
domain cisco.com
pool vpn pool
save-password
configuration url tftp://172.16.30.2/vpn.cfg
configuration version 11
```

3. To apply the additional firewall configuration to Cisco Easy VPN Remote, renegotiate the IPsec security association.

   This renegotiation can be done either by clearing the security association using the **clear crypto sa** command on either the Cisco Easy VPN Remote or server, or by reloading the remote spoke router.

4. To check whether the configuration update has been pushed, you can use show commands on both the server and the remote site.

   a. On the server, enter the **show crypto isakmp peers config** command to display either the detail for a single remote router or the data for all the remote routers.

```
Server# show crypto isakmp peers config

Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.206; Client-
Group=vpn; Client-User=vpn; Client-Hostname=spoke; Client-Platform=Cisco 1841;
Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11; Client-
Flash=33292284; Client-Available-Flash=10202680; Client-Memory=95969280; Client-
Free-Memory=14992140; Client-Image=flash:c1841-advsecurityk9-mz
```

   b. On the remote side, use the following command:

```
spoke #show crypto ipsec client ezvpn

Easy VPN Remote Phase: 5
Tunnel name : vpn
Inside interface list: Vlan1
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 172.16.1.206
Mask: 255.255.255.255
Default Domain: cisco.com
Save Password: Allowed
Configuration URL [version]: tftp://172.16.30.2/vpn.cfg [11]
Config status: applied, Last successfully applied version: 11
Current EzVPN Peer: 192.168.10.1
```

Hence, the configuration is successfully updated.

Sample VPN Configurations

In the fields listed in the sample configurations, please substitute the values appropriate for your scenario.

The sample template shown includes configuration of the Cisco Easy VPN client with a basic firewall Port Address Translation (PAT) for the translation of the hosts on the local LAN. Three separate VLANS are defined in the configuration: one for devices that have access to the corporate network, a second for family or guests without corporate access, and a third for phones (voice VLAN). The samples do not have split tunneling enabled.

The sample template configuration shown is for the Cisco 881 platform. For the Cisco 891 platform, please use WAN interface F8 and port range F0–F7.

The VPN headend configuration has the SDP server, certificate server, and Cisco Enhanced Easy VPN configured on the same box. The parts of the configuration relevant to these components are shown in the form of comments. The configuration provided applies to the Cisco 3945 Integrated Services Router.

Spoke Template Configuration (Cisco 881)

Note: The sample template configurations contain expansion variables (e.g., "$n") that are replaced by the Cisco IOS SDP registrar or Petitioner. More information can be found in the Secure Device Provisioning Guide.

```
username <username> privilege 15 secret 0 <password>
enable secret 0 <enable-password>
vlan 20
state active
vlan 11
state active
vlan 10
state active
int vlan20
int vlan 1
 exit
!
service password-encryption
password encryption aes
!
!!! Use your timezone here
clock timezone PST -8
clock summer-time PDT recurring
!
ip domain name <domain>
ntp server <ntp-server-ip>
!
hostname $n
aaa new-model

aaa authentication login default local
aaa authorization exec default local

no ip http access-class 23

crypto pki trustpoint $l
```

```
 enrollment url http://<CA-server-ip-address>:8000
 rsakeypair $k $s
 serial-number
 !!! The OU field MUST be set to the ezvpn group name.
 subject-name OU= easyvpn-group
 revocation-check none
 password none
 ip-address none
 auto-enroll 70

$c

crypto isakmp keepalive 20 5
crypto isakmp nat keepalive 20

aaa session-id common

interface Virtual-Template1 type tunnel
 description Management Virtual-Tunnel
 no ip address
 tunnel mode ipsec ipv4

ip cef
no ip dhcp use vrf connected

!! Easy VPN client config !!
crypto ipsec client ezvpn vpnserver
 connect auto
 mode client
 peer <vpn-server-ip>
 virtual-interface 1

!! Corporate address pool !!
no ip dhcp pool sdm-pool
ip dhcp pool client
   import all
   network 10.10.10.0 255.255.255.0
   dns-server <dns-server-ip>
   domain-name <domain>
   default-router 10.10.10.1
   option 150 ip <corporate-tftpserver-for-callManager>

!! Guest address pool !!
ip dhcp pool guest
   import all
   network 192.168.20.0 255.255.255.0
```

```
   default-router 192.168.20.1
   dns-server <guest-dns-ip>

!! Voice VLAN address pool!!
ip dhcp pool voice
   import all
   network 10.20.20.0 255.255.255.248
   dns-server <dns-server-ip>
   default-router 10.20.20.1
   option 150 ip <corporate-tftpserver-for-callManager>

!! Firewall Rules!!
!
no ip inspect name DEFAULT100
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall realaudio
ip inspect name firewall rtsp
ip inspect name firewall tftp
ip inspect name firewall ftp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall streamworks
ip inspect name firewall esmtp
ip inspect name firewall sip
ip inspect name firewall skinny
ip inspect name firewall sip-tls

cdp run

ip access-list extended allow_skinny_acl
 permit udp any any range bootps bootpc
 permit udp any any eq domain
 permit udp any any eq tftp
 permit tcp any any eq 2000
 permit udp any any range 24576 24656
 permit udp any any eq 5445
 permit udp any any range 2326 2373
 permit tcp any host <Directory-services-ip> eq www
 permit tcp any host <other-phone-services> eq www
 .
 .

 deny   ip any any log

interface FastEthernet0
```

```
 spanning-tree portfast
 switchport access vlan 10
 switchport voice vlan 11
 cdp enable
!
interface FastEthernet1
 spanning-tree portfast
 switchport access vlan 10
 switchport voice vlan 11
 cdp enable
!
interface FastEthernet2
 spanning-tree portfast
 switchport access vlan 20
 switchport voice vlan 11
 cdp enable
!
interface FastEthernet3
 switchport access vlan 20
 spanning-tree portfast
 switchport voice vlan 11
 cdp enable

interface FastEthernet4
description *** Outside - WAN side – Interface***
!! enter here the correct ISP ip address if not using dhcp !!
 ip nat outside
 ip access-group fw_acl in
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto ipsec client ezvpn vpnserver outside


!! Guest Vlan !!
interface Vlan20
 description Guest Access
 ip address 192.168.20.1 255.255.255.0
 ip inspect firewall in
 no ip access in
 no autostate
 ip nat inside

!!! Inspection for the voice Vlan
ip inspect name voice skinny
ip inspect name voice sip
ip inspect name voice sip-tls
```

```
ip inspect name voice h323
ip inspect name voice tft
ip inspect name voice dns

!!Voice Vlan!!
interface Vlan11
 description Voice VLAN
 ip address 10.20.20.1 255.255.255.0
 ip access-group allow_skinny_acl in
 ip inspect voice in
 ip nbar protocol-discovery
 no autostate
 crypto ipsec client ezvpn vpnserver inside

!!Corporate Vlan!!
 interface vlan10
 description Corporate Access
 ip address 10.10.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip proxy-arp
 ip nbar protocol-discovery
 ip nat inside
 ip inspect firewall in
 ip virtual-reassembly
 ip tcp adjust-mss 1360
 crypto ipsec client ezvpn vpnserver inside

no access 1
no access 23
no access 100
no access 101

!
ip access-list extended nat_acl
 permit ip 192.168.20.0 0.0.0.255 any

no ip nat inside source list 1 interface FastEthernet4 overload
 ip nat inside source list nat_acl interface FastEthernet4 overload
!
ip access-list extended fw_acl
 permit esp any any
 permit udp any any eq isakmp
 permit udp any eq isakmp any
 permit udp any eq non500-isakmp any
 permit udp host <NTP-server-IP> eq ntp any
 permit udp any any eq bootpc
```

```
 permit udp any any eq domain
 permit icmp any any
 permit tcp host <CA-server-ip> any
 deny ip any any

!! Policy-based routing configured to support guest vlan !!
ip access-list extended guest_acl
 permit ip 192.168.20.0 0.0.0.255 any

route-map policy_route_map permit 10
 match ip address guest_acl
 set ip next-hop dynamic dhcp

int vlan 20
 ip policy route-map policy_route_map


ip tftp source-interface vlan10
!
crypto pki enroll $l
end
```

VPN Server Configuration

```
hostname vpn_hub
!
enable secret 0 <enable-password>
!
ip http server
aaa new-model
!
aaa authentication login default local
aaa authorization network default local
!
interface GigabitEthernet0/0
 description *** Outside - WAN side – Interface***
 ip address <<WAN-ip-address> <netmask>
 no shut
 ip virtual-reassembly
 duplex auto
 speed auto
 no ip access-group in
!
ip route 0.0.0.0 0.0.0.0 <default-gateway>
!
no ip http access-class

!!! Use your timezone here
```

```
clock timezone PST -8
clock summer-time PDT recurring
!
ntp server <NTP-server-ip>
!
!
crypto pki trustpoint hub_cert
 enrollment url http://<WAN-ip-address>:8000
 serial-number
 ip-address none
 password none
 rsakeypair ca-server 1024
!

ip domain name <domain>
!
username <username> privilege 15 password <password>
!
service password-encryption
password encryption aes

!! SDP Server config !!
crypto provisioning registrar
 pki-server sdp-server
 template http welcome <sdp-template-page-locations>
 .
 .
 template config <location of template config>
 authentication list default
 authorization list default
!
crypto isakmp policy 1
 encr aes 256
 group 2
crypto isakmp keepalive 10
!
!! VPN Server config !!
crypto isakmp client configuration group easyvpn-group
 dns <dns-server>
 domain <domain>
 pool easyvpn-pool

crypto isakmp profile prof
   ca trust-point hub_cert
   match identity group easyvpn-group
   isakmp authorization list default
```

```
   client configuration address respond
   virtual-template 1
!
!
crypto ipsec transform-set ipsec-xform esp-aes 256 esp-sha-hmac
!
crypto ipsec profile ipsec-profile
 set transform-set ipsec-xform
!
interface Virtual-Template1 type tunnel
 description Corporate data-traffic Virtual-Tunnel
 ip unnumbered GigabitEthernet 0/0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile
!
!
ip local pool easyvpn-pool <corporate-routable-address-range>
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!Please issue a "sh ntp status" command at this point. Wait    !!!
!!!until the output shows "Clock is synchronized” and then       !!!
!!!proceed                                                       !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!! CA Server config !!
crypto pki server ca-server
database archive pkcs12 password abc12345
database level complete
grant auto trustpoint hub_cert
auto-rollover 3
issuer-name cn=test, o=cisco
no shut

!!! Please wait for the server to get enabled !!!
ip http secure-server
ip http port 8000
ip http secure-trustpoint hub_cert

crypto pki authenticate hub_cert
yes
!
crypto pki enroll hub_cert
!
end
```

Because the CA server is not in auto-grant mode, you need to manually grant the certificate from the CA server:

```
vpn_hub#crypto pki server ca-server grant all
```

Configuration of Additional Features

Note: These sample configurations apply to the Cisco 881 platform. For other platforms, please make the appropriate modifications.

QoS

```
ip access-list extended isakmp_acl
 permit udp any any eq isakmp
!
ip access-list extended voice_acl
 permit udp any any range 24576 24656
!
ip access-list extended non_voip_traffic_acl
 permit ip any any
!
ip access-list extended video_acl
 permit udp any any eq 5445
 permit udp any any range 2326 2373
!

class-map match-any call-setup
 match ip dscp cs3
 match ip precedence 3
class-map match-any internetwork-control
 match access-group name isakmp_acl
 match ip precedence 6
 match ip precedence 7
class-map match-any voice
 match access-group name voice_acl
 match ip precedence 5
class-map match-any routing
 match protocol eigrp
class-map match-all discover_signaling
 match protocol skinny
class-map match-all discover_video
 match protocol rtp video
class-map match-all discover_voip
 match protocol rtp audio
class-map match-any video
 match access-group name video_acl
 match ip dscp af41
 match ip precedence 4
class-map match-all non_voip
 match access-group name non_voip_traffic_acl
```

```
policy-map mark_incoming_traffic
 class discover_signaling
  set dscp cs3
 class discover_video
  set dscp af41
 class discover_voip
  set dscp ef
 class non_voip
  set dscp default


policy-map voice_and_video
 class voice
  bandwidth 128
 class call-setup
  priority percent 5
 class internetwork-control
  priority percent 5
 class routing
  priority percent 5
 class video
  priority 384
 class class-default
  fair-queue
  random-detect
policy-map shaper
  class class-default
    shape average 750000 7500
    service-policy voice_and_video

 interface BVI1
 ip nbar protocol-discovery
 service-policy input mark_incoming_traffic

interface virtual-template1
 service-policy output shaper
!
end
```

IEEE 802.1x

Note: If 802.1x is enabled on all ports as shown in the following configuration, the **switchport access vlan** <*number*> command need not be configured for the Fast Ethernet interfaces in the template spoke configuration.

```
aaa new-model
!!! The ‘radius-key’ should match the key configured on the AAA server!!!
```

```
aaa group server radius <name>
 server-private <radius-ip-address> auth-port 1812 acct-port 1813 key <radius-
key>
aaa authentication login default local group <name>
aaa authorization network default group <name>
!
! Enable dot1x feature globally
dot1x system-auth-control

 interface FastEthernet0
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 20
 dot1x auth-fail vlan 20
 spanning-tree portfast
!
interface FastEthernet1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 20
 dot1x auth-fail vlan 20
 spanning-tree portfast
 !
interface FastEthernet2
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 20
 dot1x auth-fail vlan 20
 spanning-tree portfast
!

interface FastEthernet3
 switchport access vlan 20
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 20
 dot1x auth-fail vlan 20
 spanning-tree portfast
!
end
```

Wireless

Wireless on the Cisco 881 Integrated Services Router can be implemented in either autonomous (standalone) or lightweight (unified) mode. For more information and configuration guidelines, please refer to the Cisco Virtual Office-Secure Wireless guide at http://www.cisco.com/go/cvo.

Authentication Proxy

```
aaa new-model

aaa group server radius <name>
 server-private <radius-ip-address> auth-port 1812 acct-port 1813 key
 <radius-key>
aaa authentication login default local group <name>
aaa authorization auth-proxy default group <name>
!
ip admission max-login-attempts 6
!
ip http server
ip http authentication aaa
no ip http secure-server
ip admission name pxy proxy http inactivity-time 1440 list auth_proxy_acl
!
ip radius source-interface BVI1
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
no ip access-list extended auth_proxy_acl
ip access-list extended auth_proxy_acl
remark --- Auth-Proxy ACL -----------
! Deny lines are used to bypass auth-proxy
 deny   tcp any host <ip address> eq www 443
 ! auth-proxy will intercept http access matching the below permit lines
 ! it is sufficient to use 'permit tcp any any eq www 443' when split
 ! tunneling is not enabled
 permit tcp any <network> <wildcard mask> eq www 443
 !
no ip access-list extended auth_proxy_inbound_acl
ip access-list extended auth_proxy_inbound_acl
 remark --- Auth-Proxy Inbound ACL -----------
! Allow access to certain protocols
 permit tcp 10.10.10.0 0.0.0.255 host 10.10.10.1
 permit udp any any eq domain
 permit udp any any eq netbios-ns
 permit udp any any eq netbios-dgm
 permit udp any any eq 5445
 permit tcp any any eq 5060
```

```
 permit tcp any any eq 5061
 permit tcp any any eq 2000
 permit tcp any any eq 2443
 permit udp any any eq tftp
! Block corporate subnets. If split tunneling is not enabled denying
! all traffic using
! "deny any any" is sufficient
 deny ip any <network> wildcard mask>

! if split tunneling is enabled
 permit ip any any
!
interface BVI1
 ip access-group auth_proxy_inbound_acl in
 ip admission pxy
end
```

Advanced Management and High-Availability Deployment Steps

This section shows how to add components to the management side for advanced configuration updates and Cisco IOS Software upgrades. It also shows how to add redundancy for the data VPN tunnels.

Multiple Data Headends for Failover

Data headends can be added as backups in case the primary data headend fails. For each backup headend, all that needs to added is an additional “peer” command for every new backup server. A sample configuration follows:

```
crypto ipsec client ezvpn data-vpn
connect auto
mode client
peer 172.20.20.1
peer 172.20.20.2
peer 172.20.20.3
virtual-interface 1
```

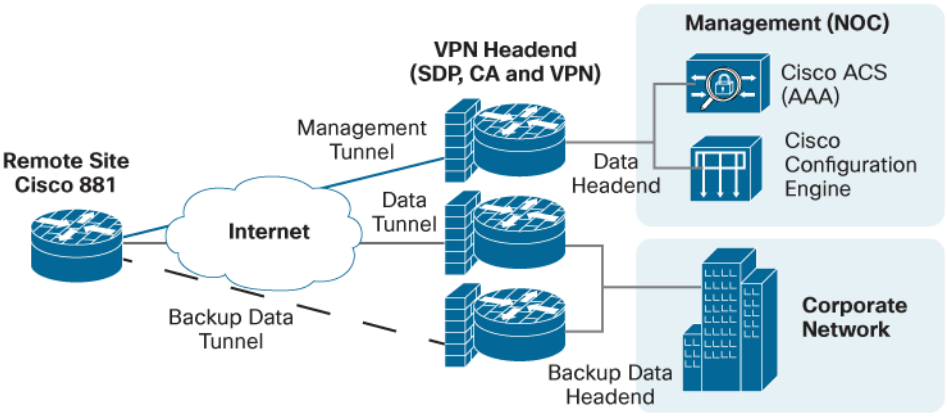
Cisco Configuration Engine

The Cisco Configuration Engine provides an automated and event-directed means of pushing predefined configuration files (or updates) to remote devices. It understands the Cisco Networking Services language and communicates with the spoke routers. It keeps track of all spokes connected to the corporate network. It can also run tasks to automatically upgrade Cisco IOS Software images for groups of devices.

Cisco Configuration Engine 3.5 is a software product that runs on a Red Hat Enterprise Linux Version 4.0. The installation details can be found at: http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/3.5/installation/guide/CE_3_ig_install.html.

The Cisco Virtual Office Express design with the additional components is shown in Figure 7.

Figure 7. Extended Cisco Virtual Office Express Design



Ongoing Management

Performing Advanced Cisco IOS Software Configuration and Image Updates

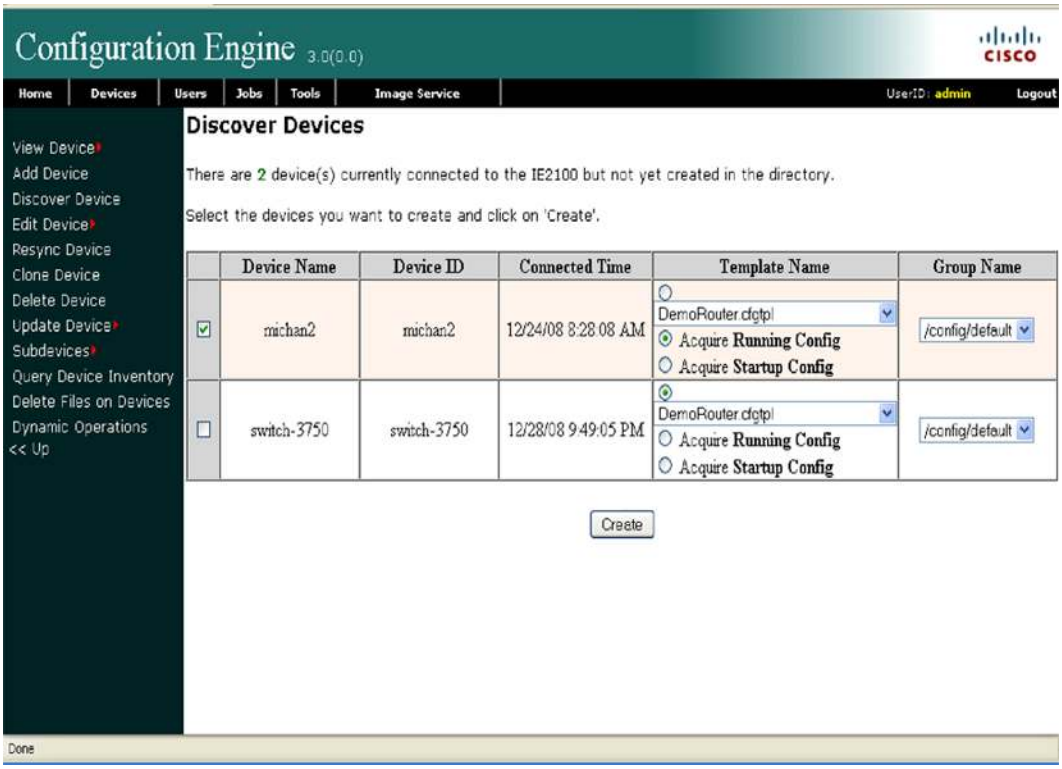
The Cisco Configuration Engine automates configuration updates by generating device-specific configuration changes, sending them to the device, making the configuration change, and logging the results. The following steps describe the process in brief. The first step is to discover the devices as they connect to the Cisco Configuration Engine. You can update the devices only after they have been added in the configuration engine.

Before making updates from the Cisco Configuration Engine, make sure that the following Cisco Networking Services commands are configured on the remote device, pointing to the Cisco Configuration Engine to be used:

```
ip host cvoexpress-ce 10.1.1.1
cns trusted-server all-agents cvoexpress-ce
cns event cvoexpress-ce source bv1
cns config partial cvoexpress-ce source bv1
cns exec source bv1
cns image server http://cvoexpress-ce/cns/HttpMsgDispatcher status
    http://cvoexpress-ce/cns/HttpMsgDispatcher
```

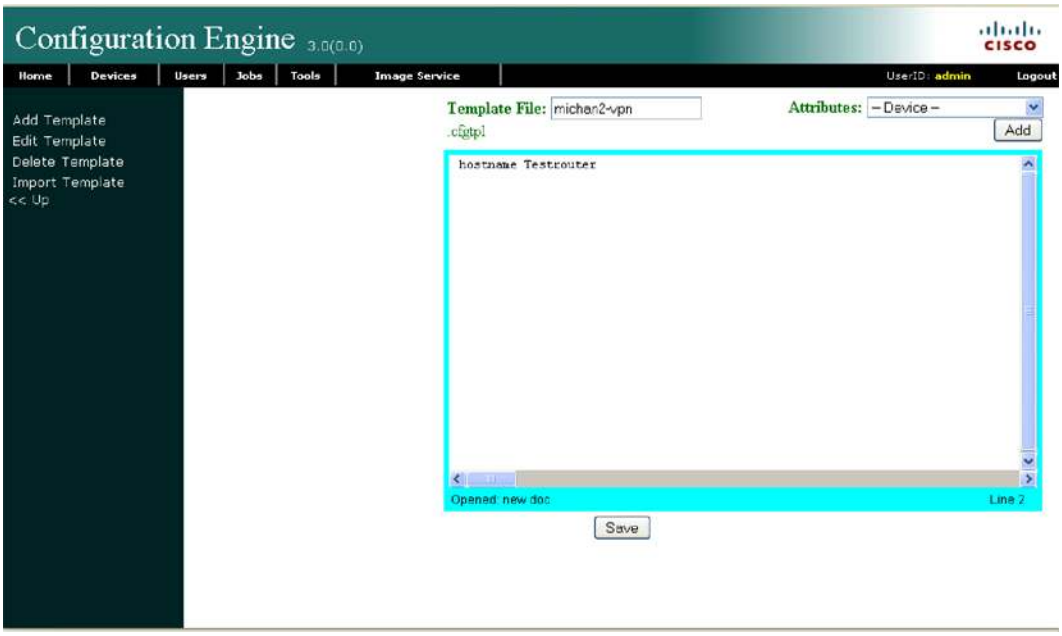
1. Log into the GUI and then discover devices:
   a. Choose Devices > Discover Device.
   b. Select the device that you want to add (Figure 8).

Figure 8. Discover Devices: Cisco Configuration Engine



2. Create a configuration template for the router update.
   a. Choose Tools > Template Manager > Add Template.
   b. Select the template type (.cfgtpl) and name the template.
   c. Enter the template content. The template content will be executed on the routers (Figure 9).

Figure 9. Template Content: Cisco Configuration Engine

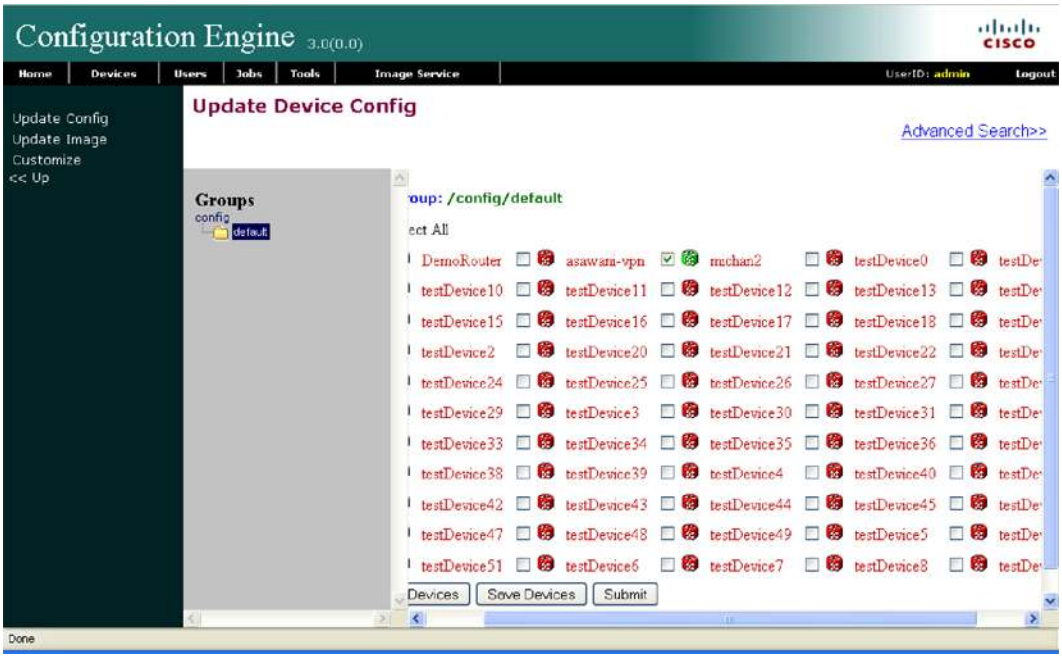


3. Update the configuration file.

   a. Choose Device > Update Device > Update Config.

   b. Select the devices for which you want to update the configuration and click Submit (Figure 10).

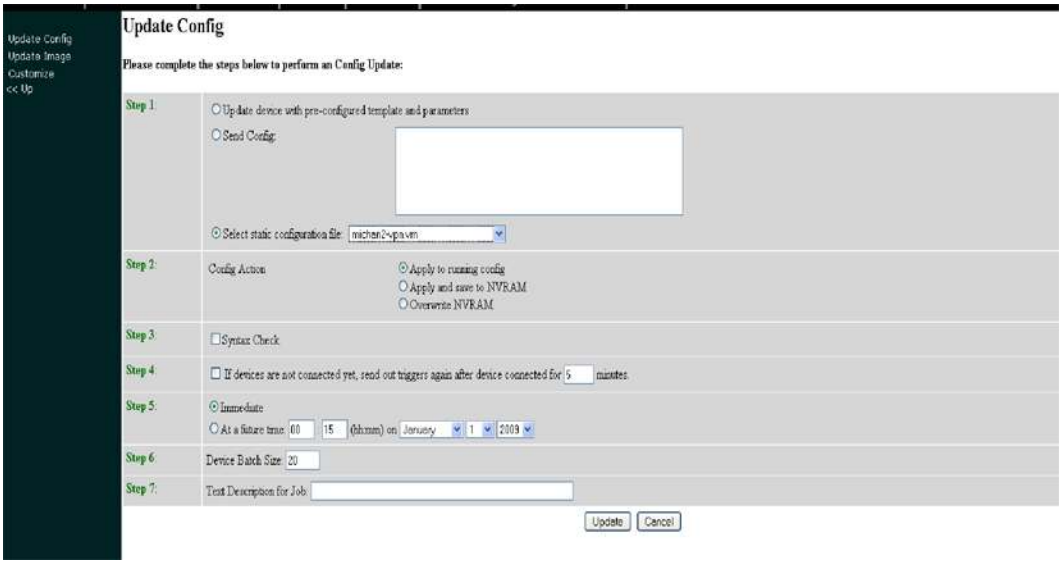
Figure 10. Update Device Config: Cisco Configuration Engine



   c. Select the Send Notification checkbox if you want a notification to be sent. Click Next.

d. Select a static configuration file and choose the template that you want to push to the router. It is also possible to type the command-line interface (CLI) commands in the textbox and select Send Config (Figure 11).

Figure 11. Completing Update Device Config: Cisco Configuration Engine



e. Make sure that “If devices are not connected yet, send out triggers again after device connected for 1 minutes” is enabled. This selection helps ensure that if the routers are offline they will get the configuration updates as soon as they connect.

f. Complete the form and click Update.

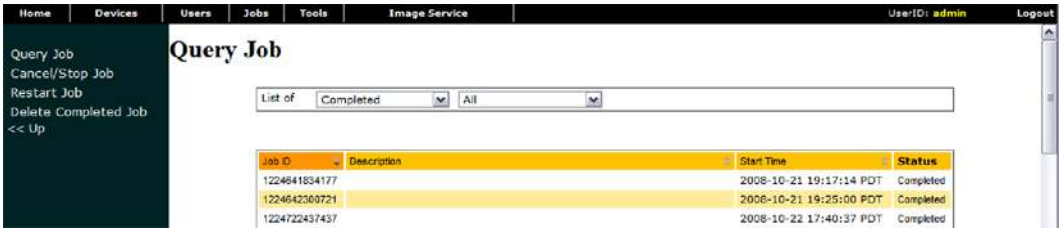
4. Check the status of the upgrade.

   a. Choose Jobs > Query Jobs.

   b. Select the job that is associated with the configuration update that was just created.

   The Cisco Configuration Engine shows that status of the job and error messages for any errors that occurred (Figure 12).

Figure 12. Query Job Window: Cisco Configuration Engine



Updating Images Using the Cisco Configuration Engine

The Cisco Configuration Engine also updates remote routers with the latest Cisco IOS Software. More information on Cisco IOS Software image upgrade using the configuration engine can be found in the Cisco Configuration Engine Administration Guide.

Pre-installation Questionnaire

Table 1 summarizes the information that you should obtain prior to installation of Cisco Virtual Office Express. These values and questions can help in preparing the configurations using the preceding examples, expediting the process of setting up the VPN.

Table 1. Preinstallation Questionnaire

Company-Specific Information	
Domain name	
DNS server IP address	
NTP server IP address	
Time zone	
Call manager TFTP server IP address	
VPN Headend Information	
Platform	
WAN IP address, mask, and default gateway	
Location where the template configuration will be stored	
Management server routable subnet (starting and ending subnets)	
Cisco Configuration Engine (Y/N)	
Cisco Configuration Engine IP address	
Cisco Configuration Engine hostname	
Spoke Router	
Platform	
Split Tunneling (Y/N)	
Corporate data subnets	
Management subnets	
Wireless (Y/N)	
SSID	
AAA Authentication (Y/N)	
AAA server IP address	
AAA shared key	
Authentication and accounting ports	
IEEE 802.1x (Y/N)	
Backup call manager TFTP server IP address	
Directory Services IP	
Phone Services IP	
Authentication Proxy (Y/N)	

References

For more information, please visit the resources listed here or contact your local Cisco account team.

- Cisco Virtual Office: http://www.cisco.com/go/cvo
- Cisco Configuration Engine Guide: http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/3.5/installation/guide/CE_3_ig_install.html

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.**

Printed in USA C11-684946-00 08/11