Troubleshooting Cisco Virtual Office

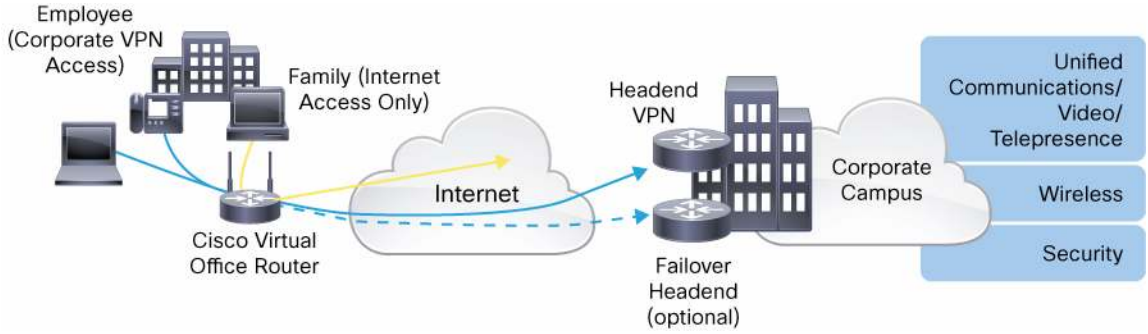
Contents

Scope of Document

This document describes some of the problems that you might face while deploying Cisco® Virtual Office and what you should do to solve them. For details about how to set up Cisco Virtual Office, please refer to the Cisco Virtual Office Deployment Guide at http://www.cisco.com/go/cvo.

Introduction to Cisco Virtual Office

Figure 1. Cisco Virtual Office



Virtual office solutions from Cisco boost flexibility and productivity by delivering secure, comprehensive, and manageable network services to teleworkers and remote offices. By providing full IP phone, wireless, data, and video services over an encrypted VPN, Cisco Virtual Office helps ensure a transparent, office-caliber experience. Video playback is smooth, voice does not stutter, and wireless connectivity is effortless (Figure 1).

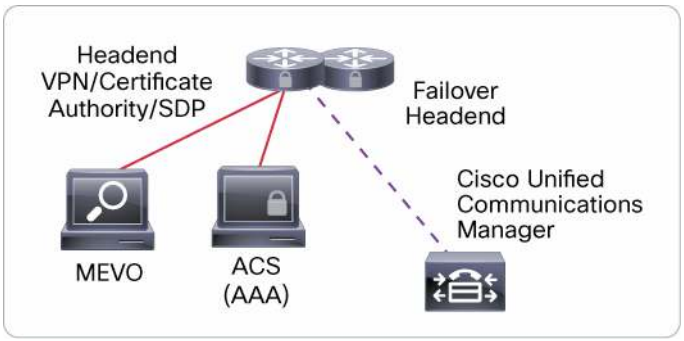
Deployment Models

You can manage the Cisco Virtual Office solution using multiple methods. This document discusses two options: The first uses Arcana Network's ManageExpress Virtual Office (MEVO) solution, and the second one uses the Cisco Security Manager and Cisco Configuration Engine.

Option 1: Cisco Virtual Office with MEVO

Figure 2 shows a single headend for management as well as tunnel aggregation. You can place the MEVO server anywhere on the network as long as it is reachable (based on IP) by the headend and the spokes.

Figure 2. Cisco Virtual Office with MEVO

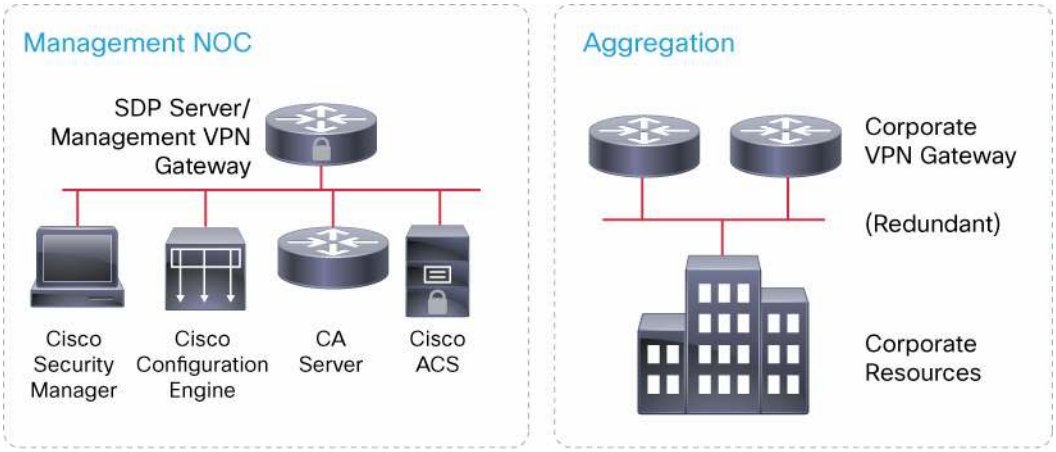


The MEVO server hosts the full configuration of the router, and this configuration is downloaded on the router in a single operation during the provisioning process. This configuration includes the Dynamic Multipoint VPN (DMVPN) tunnel as well as the certificate enrollment. The MEVO server can automatically generate this configuration based on templates for every new branch or home office to be deployed. Further, it also automates the device account creation on the Cisco ACS Versions 4.x and 5.x.

Option 2: Cisco Virtual Office with Cisco Security Manager and Cisco Configuration Engine

Figure 3 shows two separate headends: one for the management tunnel and the other for the data tunnel aggregation. In this case, the Cisco Security Manager hosts the full configuration of the router and it is pushed from the Cisco Security Manager to the Cisco Configuration Engine. The provisioning process is divided into two steps, where the first step is executed using Secure Device Provisioning (SDP) and the second step is executed by the Cisco Configuration Engine.

Figure 3. Management and Aggregation Headends



The SDP server pushes only a bootstrap configuration hosted on the Cisco Security Manager that allows the router to get a certificate and establish the management tunnel. The Cisco CNS agent on the router then establishes a connection with the Cisco Configuration Engine to get the rest of the configuration that was staged earlier.

Troubleshooting Cisco Virtual Office

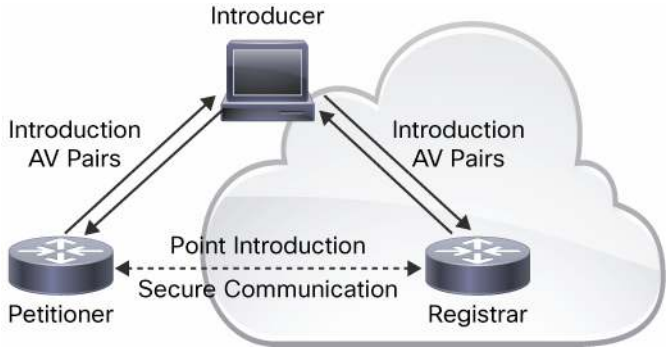
Secure Device Provisioning

SDP (also referred to as Trusted Transitive Introduction [TTI]) is a communication protocol that provides a bidirectional introduction between two end entities, such as a new network device and a VPN headend. SDP involves the following three entities (refer to Figure 4):

- **Introducer:** The introducer is a mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator. You can configure an introducer as an administrative introducer to allow an administrator to perform the introduction for multiple devices by supplying the name for the device being introduced. The supplied device name is used as if it were the name of an introducer in the normal SDP mechanism, preserving the existing functions of the SDP configuration.

- **Petitioner:** The petitioner is a client, or new device, to be introduced to the secure network.
- **Registrar:** The registrar is a server that authorizes the petitioner. The registrar can be a certificate server.

Figure 4. Secure Device Provisioning



In Cisco Virtual Office, SDP enables zero-touch deployments of the remote routers. It allows the spoke router to get a digital certificate and receive a template-based configuration. The Cisco Virtual Office spoke in this case would be the petitioner, whereas the integrated services router (ISR) headend would be the registrar. The end-user's laptop or PC is treated as the introducer.

Requirements for SDP

For SDP to function correctly, the following conditions must be satisfied:

- The SDP server must be accessible over the Internet.
- Port 443 must be open for Secure Sockets Layer (SSL) communication between the SDP server router (registrar) and the end-user computer (introducer).
- HTTP must be allowed for certificate enrollment (TCP port 80 or any other port).
- The end-user computer must have a web browser that supports JavaScript.
- The end user must have enable privileges on the client device.
- The spoke router should provide Internet access (Cisco Virtual Office default configuration).

Common Problems

Problem: The end-user SDP process does not start or does not complete.

On the registrar:

1. Make sure the customer is using the correct Cisco IOS® Software license on the spoke (advipservices or security, depending on the platform, when using DMVPN) and the correct Cisco IOS Software version on both the spoke and the SDP server. You can find recommended versions at http://www.cisco.com/go/cvo in the Cisco Virtual Office Data Sheet under "Deployment Models".
2. Ensure the required Secure HTTP (HTTPS) and HTTP ports are open on the firewall.
3. Ensure that the HTTPS and HTTP servers are enabled on the SDP registrar.
4. Make sure the SDP server can access the MEVO server over HTTP.

- Pings can be used to check reachability to the MEVO server in case there is no firewall between MEVO and the hub.
- For an HTTPS and HTTP check, run **more http://OpsXML/mevo/sdp/3-sdp_introduction.html** in enable mode on the registrar. You should see HTML code on execution of this command.

5. **Note:** If this command fails and HTTPS is used between the SDP server and MEVO, ensure that the MEVO server SSL certificate is trusted on Cisco IOS Software.
   - To check, enable **debug ip http ssl error** and run the following more command: **more https://OpsXML/mevo/sdp/3-sdp_introduction.html**.
   - If the server certificate is not trusted on the router, then you will see the following message logged after running the more command:
     Oct 27 18:13:56.222: %HTTPS: SSL handshake fail (-6992).
   - Install the MEVO certificate on the SDP server by configuring a trustpoint and enrolling with it over the terminal (cut and paste the exported MEVO certificate)

     • Export the MEVO server certificate in base 64 format

     • Configure a trustpoint (e.g. called mevo) on the sdp server with terminal enrollment ("**enrollment terminal**" under the trustpoint)

     • Authenticate with the new trustpoint: "**crypto pki authenticate mevo**" then cut and paste the exported MEVO cert.
6. Check the configuration under **crypto provisioning registrar**.
   - Ensure there are associated public key infrastructure (PKI) server, authentication list, and authorization list.
   - The template username and password are used to retrieve from MEVO the configuration for the user represented by $n. From a web browser, test by going to http://OpsXML/mevo/Configs/<user-id>_Bootstrap.cfg, where OpsXML represents the MEVO server address, and <user-id> is the username being used for provisioning. Use the template username/password configured under the registrar to access the file.
   - These credentials must be Microsoft Windows MEVO Server credentials that have access to the folder that hosts the configurations.
7. Ensure the PKI server configured is enabled: **`show crypto pki server`**.
8. If the configuration is pushed to the spoke successfully but the completion (deployment successful) page is not loading on the browser, ensure that MEVO can access the spoke router through the headend.
9. If all of the previous steps are correct, ask the customer to contact Arcana to ensure Microsoft Internet Information Server (IIS) on the MEVO Windows server is configured correctly.

Basic DMVPN Troubleshooting

DMVPN is the preferred and most commonly deployed VPN technology in Cisco Virtual Office. It provides multiple advantages such as dual active-active tunnels, instantaneous routing failover, spoke-to-spoke dynamic tunnels, and split tunneling that make it very well-suited for the Cisco Virtual Office solution.

Common Problems

Problem: The DMVPN tunnel does not come up.

1. Verify that the router got the certificate: **show crypto pki cert**. If the certificate is not present:

a. Verify that the correct port for Simple Certificate Enrollment Process (SCEP) enrollment is allowed through the firewall.

b. Verify that the certificate server on the SDP router is enabled.

c. Make sure the root certificate authority certificate is present on the spoke router.

d. Verify that the clocks match on the hub and the spoke.

2. If you use PKI authentication, authorization, and accounting (AAA), verify that the spoke has a corresponding account on the AAA server; this account should be the fully qualified domain name (FQDN) of the spoke with a password “cisco”, and the account should have the following Cisco av-pair: pki:cert-application=all.
3. Verify that the Internet Security Association and Key Management Protocol (ISAKMP) policy and IP Security (IPsec) profiles match on the spoke and hub routers.
4. Make sure that the following ports are not being blocked: User Datagram Protocol (UDP) 500 (ISAKMP), UDP 4500 (Network Address Translation Traversal [NAT-T]), and IP 50 Encapsulating Security Payload (ESP)).

Problem: The connection is flapping.

This problem is usually noticed from the routing protocol (for example, Enhanced IGRP [EIGRP] log messages). There are three common reasons:

1. Overlapping DMVPN tunnel address: You can detect this problem by using the **show dmvpn** or **show ip nhrp** command on the hub router. The nonbroadcast multiaccess (NBMA) address in the output would be changing.
2. Overlapping corporate VLAN subnet: You can detect this problem by using the **show ip route <spoke-corp-VLAN-address>** command on the hub router. The neighbor address in the output would be changing.
3. Problem on the ISP network that is causing packets to get dropped

Troubleshooting Management with Arcana Network’s MEVO

Common Problems

Problem: Configuration was pushed but the spoke router doesn’t show as “online” on MEVO

Problem: MEVO fails to configure the autonomous access point on a spoke (status on MEVO shows as “online”).

Do the following to resolve these problems:

1. Verify that the DMVPN tunnel and routing are up on the spoke.

   a. The **show crypto isakmp sa** command should show a session to the DMVPN hub in QM_IDLE. Alternatively, using **sh crypto isakmp sa** on the hub should show a session in QM_IDLE to the spoke.

   b. The **show ip eigrp neighbors** command should show the DMVPN hubs as neighbors to the spoke. Alternatively, **show ip eigrp neighbors** on the hub should show the spoke as a neighbor.

   c. The **show ip route eigrp** command should show the set of routes advertised by the hubs to the spoke.

2. If all of these steps are successful, verify that MEVO is able to reach the spoke.

   a. Make sure MEVO is reachable from the hub (ping from MEVO to hub or conversely).

b. From the MEVO windows server, ping the routable VLAN (typically, VLAN 10) IP address of the spoke. Alternatively, ping MEVO from the spoke with source interface VLAN 10.

c. When reachable, go to the Request tab on the MEVO user interface, select the appropriate request (corresponding to the router that failed), click the Options button, and select Retry.

Troubleshooting Management with Cisco Security Manager and Cisco Configuration Engine

Common Problems During Provisioning

Problem: The spoke router does not get the full configuration.

1. Check if the bootstrap configuration got pushed (**show run** on the spoke router). If the configuration was pushed, there should be crypto map and a CNS configuration). If there is not, check the bootstrap template on Cisco Security Manager (flexconfig) for any wrong or unsupported commands. Also verify that the SDP server trusts the CSM certificate (a trustpoint should be configured on the SDP server and enrolled with the exported CSM certificate over the terminal, as described for the MEVO certificate in step 5 of the "The end-user SDP process does not start or does not complete" problem). Make sure that the template username and password under the registrar are valid CSM admin credentials: paste the following URL in a browser, replacing $n with an actual username/device configured on CSM, and "cvo_sdp" with your bootstrap template's name: https://cvo-csm/athena/SDPReg%3Fdevice=$n&template=cvo_sdp. Use the username/password configured under the registrar to verify that the authentication succeeds.
2. If the spoke router got the bootstrap configuration, the problem could be that it cannot establish the management IPsec tunnel:
   a. Verify that the router got the certificate using **show crypto pki cert**.
   b. Verify that the clocks match on the management hub and the spoke.
   c. If you use PKI-AAA, verify that the spoke has a corresponding account on the AAA server; this account should be the FQDN of the spoke with a password "cisco", and the account should have the following Cisco av-pair: pki:cert-application=all.
   d. Verify that the ISAKMP policy and IPsec profiles match on the spoke and hub routers.
   e. Make sure that the following ports are not being blocked: UDP 500 (ISAKMP), UDP 4500 (NAT-T), and IP 50 (ESP).
3. If the management tunnel is up, verify that the routing is properly configured.
4. Make sure that the Cisco Configuration Engine can reach the spoke through the management hub (SDP server).

Problems with Cisco Configuration Engine

Problem: Cisco Configuration Engine installation fails and complains about missing domain information

The following error message is seen when trying to run the installation script **ce_install.sh**:

```
[root@cvoce RPMS]# ./ce_install.sh
Can't find domain information.  CE 3.0 installation aborted!!!
```

Solution: This error occurs when the resolv.conf file is not configured properly. Open the resolv.conf file and make sure the command **search** <*domain*> and **nameserver** <*dns-address*> are configured, as shown in the following example:

```
[root@cvoce RPMS]# vi /etc/resolv.conf
```

```
search cisco.com
nameserver 208.67.222.222
```

Problem: Cisco Configuration Engine installation fails and complains about mismatch in hostname.

The following error message is seen when trying to run the installation script **ce_install.sh**:

```
[root@cvoce RPMS]# ./ce_install.sh
Hostname value retrieval by system calls ‘gethostbyaddr()’ and command
‘hostname’ have different values returned. Please correct it before
installing Config Engine 3.0
```

Solution: This error happens when there is a mismatch between the contents of the /etc/hosts and /etc/sysconfig/network files. Make sure the correct hostname and IP address are configured in these files, as shown in the following example:

```
[root@cvoce]# vi /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost localhost.cisco.com
192.168.0.3       cvoce cvoce.cisco.com

[root@cvove]# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=cvoce
GATEWAY=192.168.0.1
```

Make all the necessary changes to the files then reboot the server for those changes to take effect.

Problem: Cisco Configuration Engine installation fails and complains about lack of memory on the machine.

An error message similar to the following is seen when trying to run the installation script **ce_install.sh**:

```
=================================================
=======  System Requirement Check :          =======
=================================================
check OS.......... ok
check CPU.......... ok
check Ram.......... The machine has only 1034496 Kbytes memory. Minimum
requirement: 2000000 Kbytes.
Installation aborted.
```

Solution: The Linux server that hosts Cisco Configuration Engine should meet the minimum memory requirement (2 GB of RAM). The RAM on the machine needs to be upgraded.

Problem: Cisco Configuration Engine cannot ping other machines, and conversely.

Solution: This error might be caused by a misconfiguration on the WAN interface of the Cisco Configuration Engine server. Check the configuration under the WAN interface (and possibly in the “network” file if the default gateway is configured there) to make sure the correct parameters (IP address, netmask, network, and default gateway) are configured, as shown in the following example:

```
[root@cvoce RPMS]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.0.255
HWADDR=00:0C:29:33:C0:92
IPADDR=192.168.0.3
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
TYPE=Ethernet

[root@cvoce RPMS]# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=cvoce
GATEWAY=192.168.0.1
```

After making any necessary changes, restart the network services using the following command:

```
service network restart
```

Problem: Neither https://<CE-address> nor http://<CE-address> pages are opening.

Solution: This problem occurs when the HTTPD service on Cisco Configuration Engine is not running. Run the following command to start the HTTPD service:

```
/etc/init.d/httpd start
```

Problem: HTTPD service is running but https://<CE-address> does not lead to the Cisco Configuration Engine GUI.

Solution: Do the following to identify the root cause of the problem and resolve it:

1. Check whether Apache is listening on port 443 for SSL connections by issuing the command: **lsof -i -n -P | grep httpd | grep 443**, as shown in the example that follows:

```
[root@cvoce RPMS]# lsof -i -n -P | grep httpd | grep 443
httpd    6565    root    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6591  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6592  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6593  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6594  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6595  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6596  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6597  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
httpd    6598  apache    4u  IPv6  11906       TCP *:443 (LISTEN)
```

No output with that command means that cryptographic communication was not enabled on Cisco Configuration Engine. To enable it, run setup again (go to /opt/ConfigEngine/CSCOcnsie/bin and issue the **setup** command) and answer **Yes** to the question about cryptographic operation:

```
Enable cryptographic (crypto) operation between Event Gateway(s)/Config server
and device(s) (y/n)? [n] y
```

Please refer to the “Installing Cisco Configuration Engine” section of the deployment guide for more information about setting up Cisco Configuration Engine.

2. If Apache was listening on port 443, then the problem might be that the firewall on the Linux server that hosts the Cisco Configuration Engine is blocking SSL traffic. To check the firewall configuration, issue the command:

   /sbin/iptables -L –n

   If the Linux firewall was enabled, the output of the above command will be similar to the following:

```
Chain INPUT (policy ACCEPT)
target                      prot opt source      destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target                      prot opt source      destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source        destination
ACCEPT     all  --  0.0.0.0/0     0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0     0.0.0.0/0      icmp type 255
ACCEPT     esp  --  0.0.0.0/0     0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0     0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0     224.0.0.251    udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0     0.0.0.0/0      udp dpt:631
ACCEPT     all  --  0.0.0.0/0     0.0.0.0/0      state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0     0.0.0.0/0      state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0     0.0.0.0/0      state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0     0.0.0.0/0      state NEW tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0     0.0.0.0/0      state NEW tcp dpt:25
REJECT     all  --  0.0.0.0/0     0.0.0.0/0      reject-with icmp-host-prohibited
```

Make sure there’s an “ACCEPT” request entry for TCP 443 under the INPUT section. To add such an entry, use the following command:

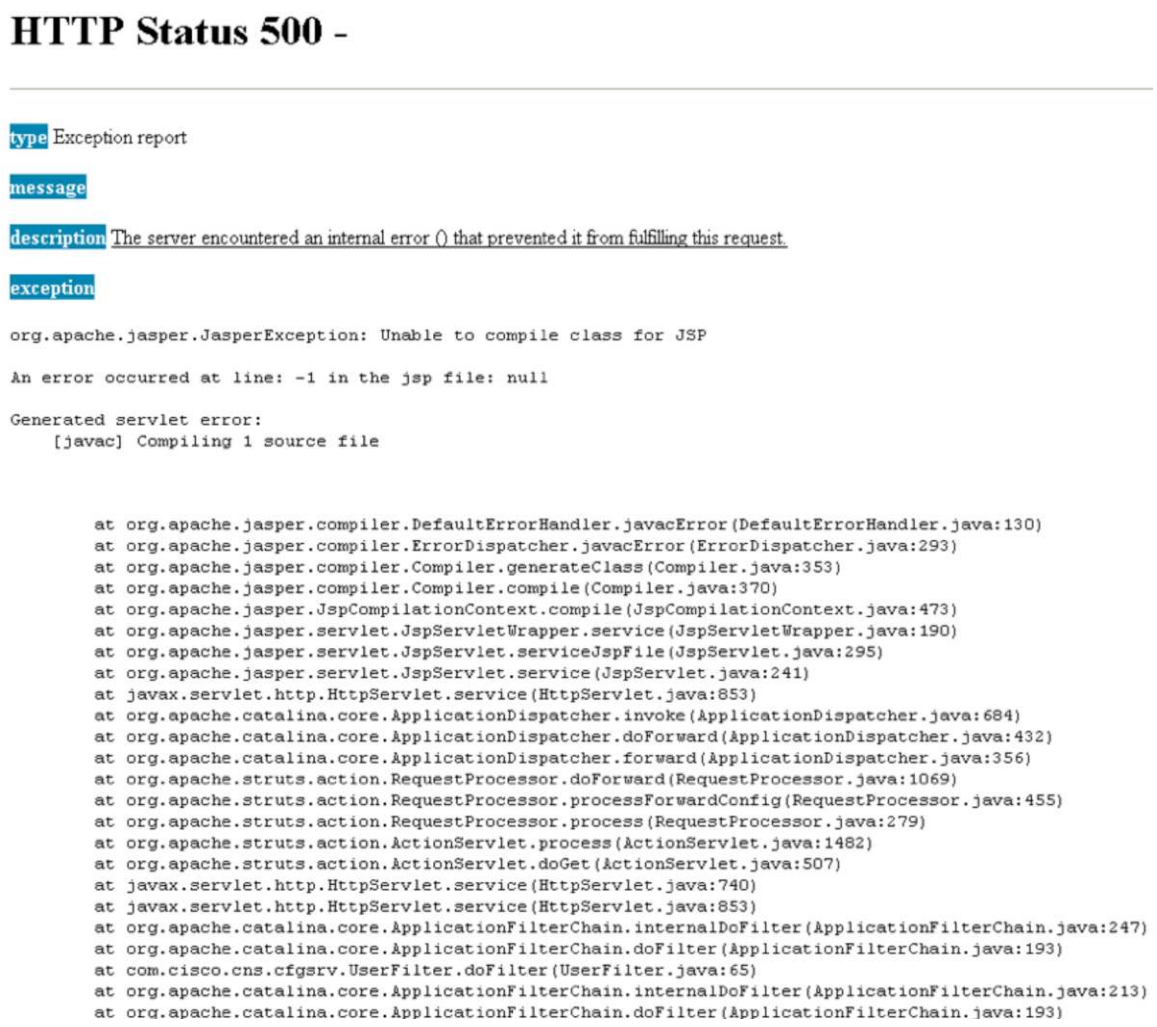
```
iptables -I INPUT -p tcp --destination-port 443 -j ACCEPT
```

Also make sure that Tibgate ports (11011, 11013, 11015, 11017, and 11019) are allowed for connections to the devices. Use the same command shown previously, replacing 443 with the corresponding port number.

Problem: Opening some of the pages in the Cisco Configuration Engine web GUI results in an HTTP 500 error, sometimes dumping Java compilation errors.

An example of what could be seen on the GUI in this case is shown in Figure 5.

Figure 5. HTTP 500 Error



S7: This error occurs when the Cisco Configuration Engine server doesn't have enough RAM to perform all the possible tasks on the GUI.

To check on memory usage, open a terminal window and login as "root" to Cisco Configuration Engine. Issue the **free** command, as follows:

```
[root@stealth-ce ~]# free
             total       used       free     shared    buffers     cached
Mem:       8298812    2994572    5304240          0      47352     384768
-/+ buffers/cache:    2562452    5736360
Swap:      4620280          0    4620280
```

where “Mem” represents RAM. If the RAM is already consumed, additional RAM should be added to the server It is recommended to have a minimum of 4 GB of RAM on the server for Cisco Configuration Engine to operate properly with up to 20,000 devices.

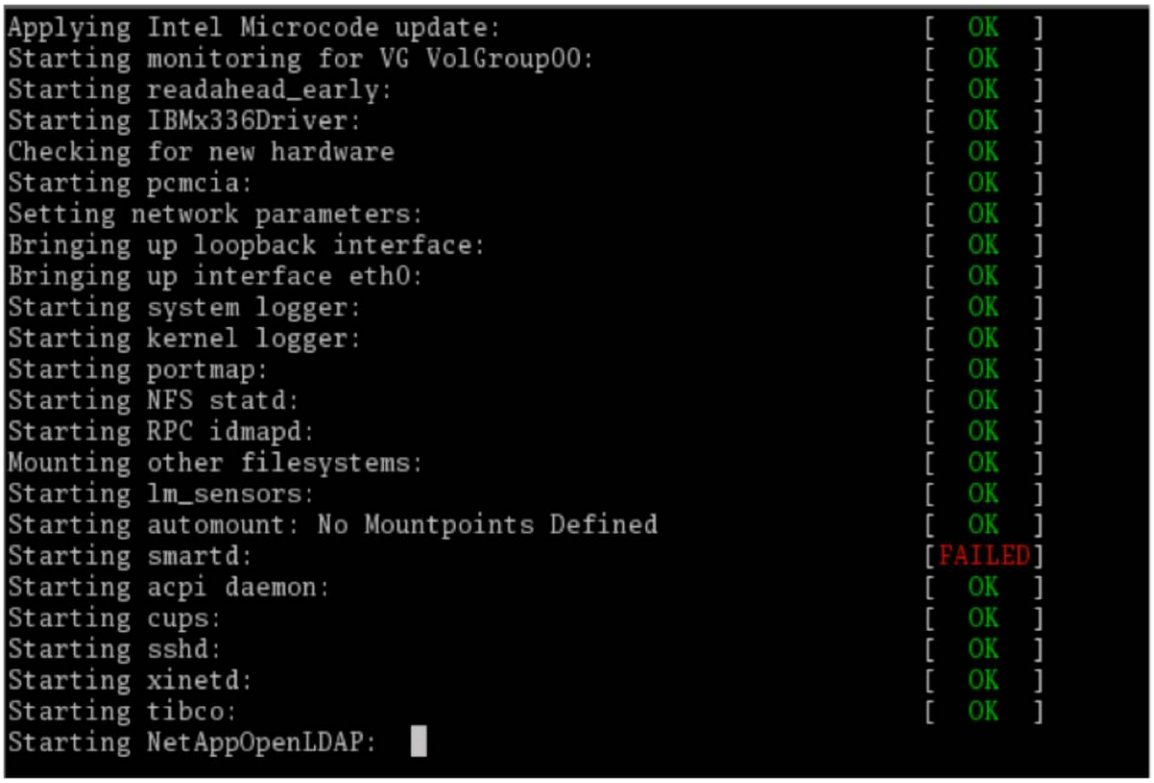
Note that SWAP memory should always be more than the RAM (a minimum of twice the size of RAM is recommended for SWAP). Thus, if upgrading the RAM, make sure that enough SWAP space is still available.

You can increase SWAP space by resizing the partitions on the server, or by using a SWAP file as described in http://www.linux.com/feature/113956.

Problem: When booting up, Cisco Configuration Engine gets stuck in “Starting NetAppOpenLDAP”.

Figure 6 shows this scenario.

Figure 6. Cisco Configuration Engine Stuck in Starting NetAppOpenLDAP.



Solution: The Lightweight Directory Access Protocol (LDAP) database might get corrupted whenever Cisco Configuration Engine is ungracefully restarted, for example, in case of a power failure. To resolve this problem, implement the following steps:

1. Open a terminal window and log in as “root” to Cisco Configuration Engine. If Cisco Configuration Engine is not accessible, manually reload the server and try again.
2. Shut down the OpenLDAP server by issuing the following command:
   `/etc/init.d/NetAppOpenLDAP stop`

3. Run the following command to recover the data, where $(DIR) is the directory where Cisco Configuration Engine was installed (default is /opt/ConfigEngine):

   ```
   $(DIR}/bdb/bin/db_recover -h ${DIR}/openldap/var/openldap-data
   ```

4. If an error similar to the following occurs:

   ```
   $(DIR)/bdb/bin/db_recover: error while loading shared libraries: libdb-4.3.so:
   cannot open shared object file: No such file or directory
   ```

   then run the following command:

   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$(DIR)/bdb/lib:$(DIR)/unixodbc/lib
   ```

   and run the data recovery command mentioned previously again.

5. Gracefully restart the Cisco Configuration Engine using: **setup –r**.

Problems with Cisco Security Manager

Problem: Cisco Security Manager fails to discover the router (DMVPN hub or the master spoke).

When trying to discover the router, Cisco Security Manager fails and complains about wrong parameters. Figure 7 shows the error message that Cisco Security Manager gives.

Figure 7. Failure to Discover Device

Solution: This error can happen for several reasons:

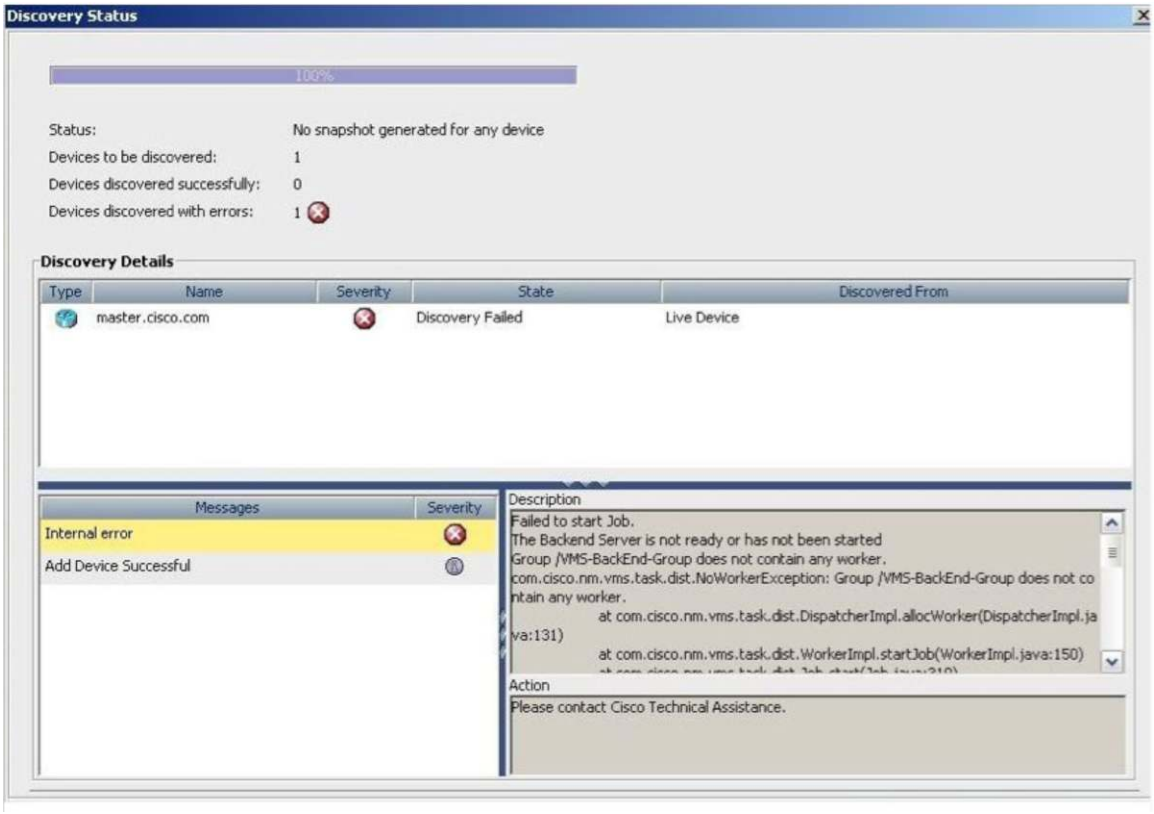
1. One or more of the parameters configured for the device on Cisco Security Manager is wrong. Make sure that all the parameters (Hostname, IP Address, Login Username, Login Password, and Enable Password) are configured properly on Cisco Security Manager when discovering the device.
2. Make sure that the router is running an image no later than Cisco IOS Software Release 12.4(20)T. Cisco Security Manager does not recognize software versions that are newer than Release 12.4(20)T, for example, 12.4(22)T.

3. If HTTPS is the method of choice to access devices on Cisco Security Manager, make sure that it is enabled on the router that is being discovered. You should configure the command ip http secure-server on the router to enable HTTPS.

Problem: Cisco Security Manager fails to discover a device, complaining about a backend server problem.

When trying to discover the router, Cisco Security Manager fails and complains about the backend server not being ready or started. Figure 8 shows the corresponding error message.

Figure 8. Backend Server Failure



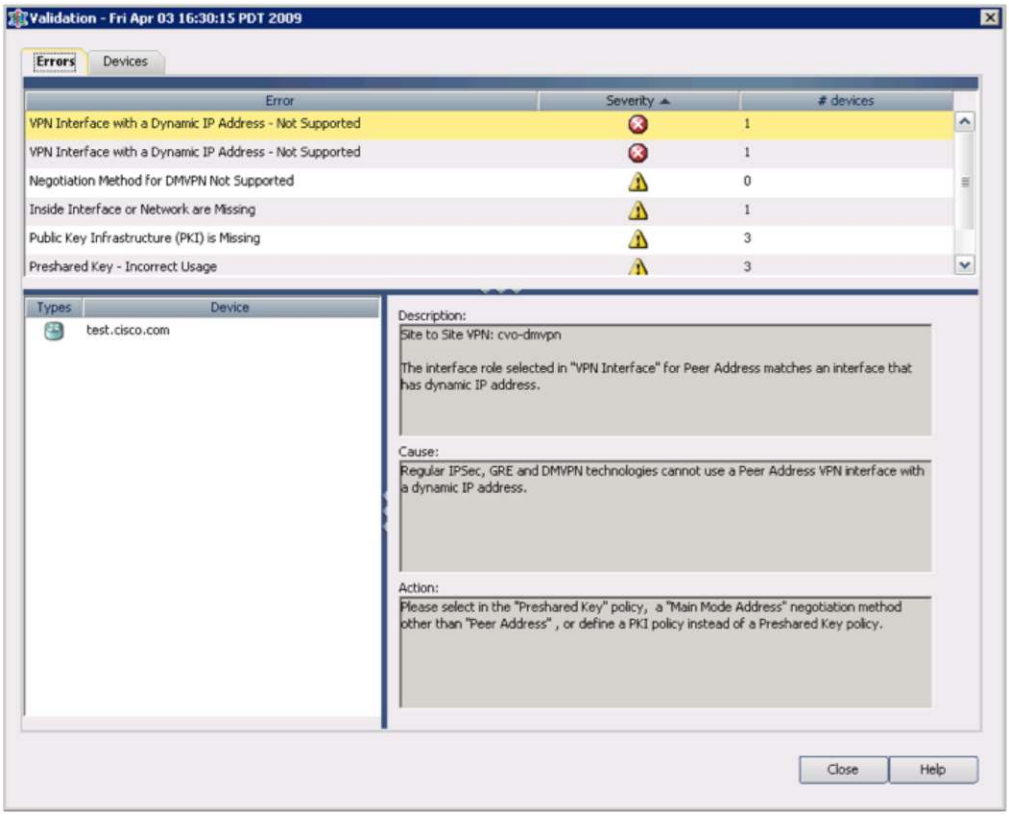
Solution: One possible reason for this problem is changing the hostname on the Cisco Security Manager server. If the hostname of the Cisco Security Manager (Windows) server was changed, the script named hostnamechange.pl must be executed, as described as follows, in order for the backend server to be started properly:

1. Open a command prompt window on the Cisco Security Manager server.
2. Go to NMSROOT\bin, where NMSROOT is the root directory of Cisco Security Manager (C:\PROGRA~1\CSCOpx is the default), by issuing the following command
   `cd C:\PROGRA~1\CSCOpx\bin`
3. Run the script using the command
   `perl hostnamechange.pl`

Problem: When submitting the Cisco Security Manager configuration, it complains about the VPN interface.

Cisco Security Manager complains about the VPN interface having a dynamic IP address, which is not supported. Figure 9 shows the corresponding error message.

Figure 9. Dynamic Address on VPN Interface



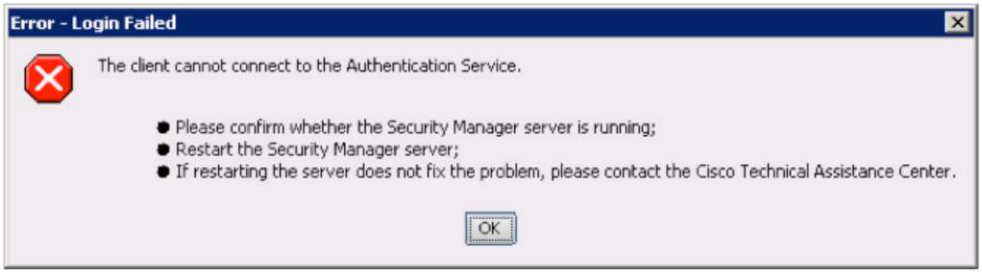
Solution: This error occurs when the preshared key (PSK) policy is not unassigned from the DMVPN topology. To resolve this problem, go to the DMVPN topology configuration wizard, right click on the PSK policy, and choose “Unassign Policy”, as shown in Figure 10.

Figure 10. Unassign PSK Policy

Problem: Cisco Security Manager client and the https://<CSM-address> page are not accessible

The error shown in Figure 11 appears when trying to login to the Cisco Security Manager client.

Figure 11. Cisco Security Manager Client Not Accessible



Solution: This error happens when one (or both) of the Apache and Tomcat services is not started. Go to Control Panel->Administrative Tools->Services and make sure that Apache and Tomcat are started.

Problem: Apache and Tomcat are up, but https://<CSM-address> gives a 403 Forbidden Error and Cisco Security Manager client is not accessible

The error shown in Figure 12 appears when trying to login to the Cisco Security Manager client.

Figure 12. CMF Session ID Problem

Solution: This error happens when the Apache service does not register properly with the daemon manager. To resolve the problem, implement the following steps:

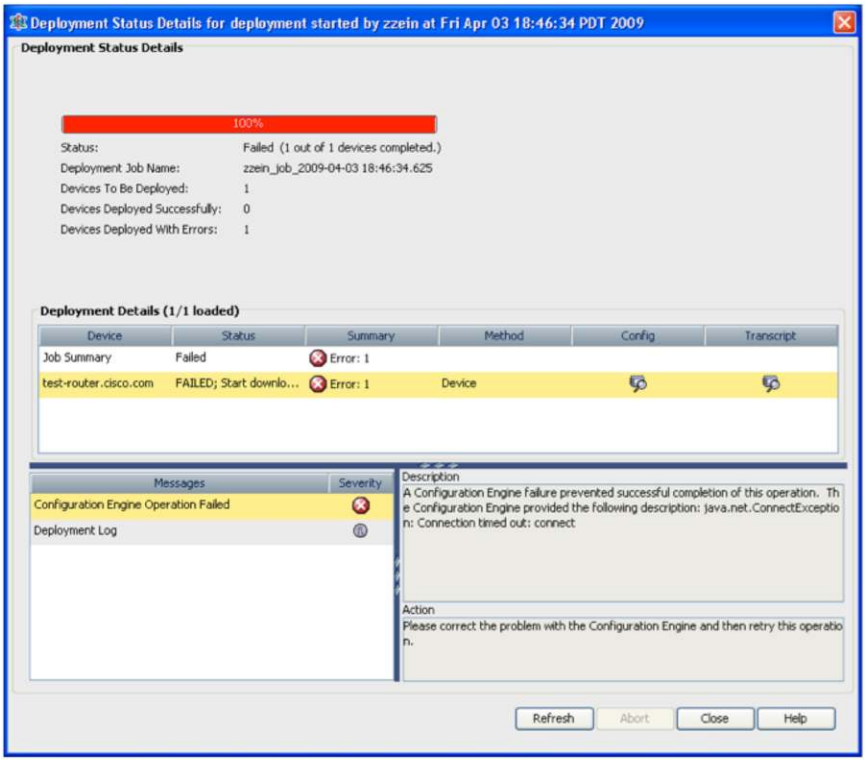
1. Go to Control Panel->Administrative Tools->Services and stop the daemon manager service.
2. Open a command prompt window and issue the following command to unregister the Apache process:
   ```
   pdreg –u Apache
   ```
3. Register the Apache again using the correct parameters, as follows. Replace “C:\PROGRA~1\” with the CSM installation directory if the default one was not used.
   ```
   pdreg -r Apache -e "C:\PROGRA~1\CSCOpx\MDC\Apache\Apache.exe" -f "-d
   C:\PROGRA~1\CSCOpx\MDC\Apache -D SSL" -d Tomcat
   ```
4. Start the daemon manager service again.

Problems with the Interaction Between Cisco Security Manager and Cisco Configuration Engine

Problem: Cisco Security Manager cannot reach the Cisco Configuration Engine.

When trying to deploy a job to Cisco Configuration Engine, Cisco Security Manager client returns the error shown in Figure 13.

Figure 13. Cisco Configuration Engine Unreachable Error



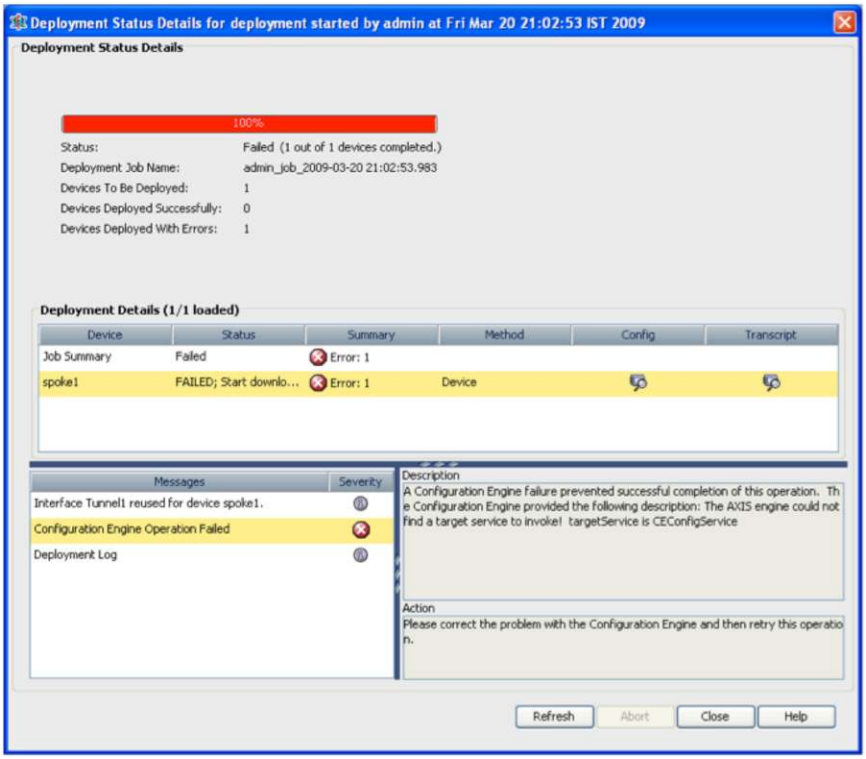
Solution: There are several reasons for this error. Following are the reasons and their solutions:

1. Cisco Security Manager cannot reach Cisco Configuration Engine: Try to ping the Cisco Configuration Engine IP address from the Cisco Security Manager server. Ping failure means Cisco Security Manager cannot reach Cisco Configuration Engine. Make sure that Cisco Configuration Engine is up and reachable, and that the Cisco Security Manager server has access to the Internet.
2. HTTPS access is not enabled or is blocked on Cisco Configuration Engine: Cisco Security Manager uses HTTPS to connect to the Cisco Configuration Engine. Please refer to P5 and P6 in the “Problems with Cisco Configuration Engine” section of this guide for more information about solving this problem.
3. Access credentials configured for Cisco Configuration Engine on Cisco Security Manager are wrong: Make sure that the correct username and password to access Cisco Configuration Engine with HTTPS are configured on Cisco Security Manager.

Problem: Cisco Security Manager gives an "AXIS engine" error when deploying a job to Cisco Configuration Engine.

When deploying a job to Cisco Configuration Engine, Cisco Security Manager client gives the error message shown in Figure 14.

Figure 14. AXIS Engine Error



Solution: This error means that the services on Cisco Configuration Engine have not been properly started. Open a terminal to Cisco Configuration Engine and run the command **setup –r** to restart the services. When this process is finished, open a web browser and go to https://<*CE-address*>/cns/services/CEConfigService, a page similar to the one in Figure 15 should open, indicating the AXIS engine is running properly.

Figure 15. AXIS Engine Running

Problem: A job is staged on Cisco Configuration Engine from Cisco Security Manager, The CNS event from the device to Cisco Configuration Engine is up, but the job does not get pushed to the device.

Solution:

1. This error might be caused by a mismatch in the date and time set on Cisco Security Manager and Cisco Configuration Engine. If the Cisco Configuration Engine date is behind, the job staged from Cisco Security Manager will appear to be scheduled for a future time and will not be pushed to the device until the correct time comes, even if the event to the device is established earlier. Check the date and time set on both Cisco Security Manager and Cisco Configuration Engine and make sure they match and are current.
2. Another reason why this error might occur is if an authentication error from Cisco Configuration Engine happens. Make sure that the spoke is configured with the correct **cns trusted-server** command pointing to the Cisco Configuration Engine, as follows:
   ```
   cns trusted-server all-agents cvoce
   ```

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 C07-704290-00 04/12