Server Health and Configuration

View the Cisco EPN Manager Server Configuration

Use this procedure to view Cisco EPN Manager server configuration information such as the current server time, kernel version, operating system, hardware information, and so forth.

Step 1 Choose **Administration** > **Dashboards** > **System Monitoring Dashboard**.

Step 2 Click the **Overview** tab.

Step 3 Click **System Information** at the top left of the dashboard to expand the System Information field.

Change the Cisco EPN Manager Hostname

Cisco EPN Manager prompts you to enter a hostname when you install the server. For a variety of reasons, you may find a mismatch between the hostname configured on the Cisco EPN Manager server and the hostname configured elsewhere. You can resolve this issue without reinstalling Cisco EPN Manager by changing its hostname on the server. To do so:

Step 1 Open a CLI session with the Cisco EPN Manager server, making sure you enter **configure terminal** mode. See Connect via CLI.

Step 2 Enter the following command:

```
Cisco_EPN_Manager_Server/admin(config)#hostname newHostName
```

where *newHostName* is the hostname you want to assign to the Cisco EPN Manager server.

Step 3 Restart the Cisco EPN Manager server using the **ncs stop** and **ncs start** commands.

Step 4 Check the hostname configured for your SSL server certificate:

- If the hostname is the same as the one you specified in Step 2, you can stop here.
- If the hostname is different, you will need to create a new SSL server certificate configured with the hostname you specified in Step 2 and then install it. See Set Up HTTPS to Secure the Connectivity of the Web Server.

Connect via CLI

Administrators can connect to the Cisco EPN Manager server via its command-line interface (CLI). CLI access is required when you need to run commands and processes accessible only via the Cisco EPN Manager CLI. These include commands to start the server, stop it, check on its status, and so on.

Before You Begin

Before you begin, make sure you:

- Know the user ID and password of an administrative user with CLI access to that server or appliance. Unless specifically barred from doing so, all administrative users have CLI access.
- Know the IP address or host name of the Cisco EPN Manager server.

Step 1 Start up your SSH client, start an SSH session via your local machine's command line, or connect to the dedicated console on the Cisco EPN Manager physical or virtual appliance.

Step 2 Log in as appropriate: If you are using a GUI client: Enter the ID of an active administrator with CLI access and the IP address or host name of the Cisco EPN Manager server. Then initiate the connection. If you are using a command-line client or session: Log in with a command like the following:[localhost]# ssh username@IPHost -Whereusername is the user ID of a Cisco EPN Manager administrator with CLI access to the server. IPHost is the IP address or host name of the Cisco EPN Manager server or appliance. If you are using the console: A prompt is shown for the administrator user name. Enter the user name.
Cisco EPN Manager will then prompt you for the password for the administrator ID you entered.

Step 3 Enter the administrative ID password. Cisco EPN Manager will present a command prompt like the following:

```
Cisco_EPN_Manager_Server/admin#
```

Step 4 If the command you need to enter requires that you enter **configure terminal** mode, enter the following command at the prompt:

`Cisco_EPN_Manager_Server/admin#`**configure terminal**

The prompt will change from `Cisco_EPN_Manager_Server/admin#` to `Cisco_EPN_Manager_Server/admin/conf#`.

Secure the Connectivity of the Cisco EPN Manager Server

For data security, Cisco EPN Manager encrypts data in transit using standard public key cryptography methods and public key infrastructure (PKI). You can obtain more information about these technologies from the internet. Cisco EPN Manager encrypts the data that is exchanged between the following connections:

- Between the web server and the web client
- Between a CLI client and the Cisco EPN Manager CLI shell interface (handled by SSH)
- Between the Cisco EPN Manager and systems such as AAA and external storage

To secure communication between the web server and web client, use the public key cryptography services that are built in as part of the HTTPS mechanism. For that you need to generate a public key for the Cisco EPN Manager web server, store it on the server, and then share it with the web client. This can be done using the standard PKI certificate mechanism which not only shares the web server public key with the web client, but also guarantees that the public key belongs to the web server (URL) you are accessing. This prevents any third party from posing as the web server and collecting sensitive information that the web client is sending to the web server. Follow the procedure in Set Up HTTPS to Secure the Connectivity of the Web Server, on page 4

These topics provide additional steps you can take to secure the web server:

- Cisco recommends that the Cisco EPN Manager web server authenticate web clients using certificate-based authentication. This security hardening procedure is described in Set Up Certificated-Based Authentication for Web Clients
- To secure connectivity between a CLI client and the Cisco EPN Manager CLI interface, refer to the security hardening procedures in Harden the Cisco EPN Manager Server.
- To secure connectivity between the Cisco EPN Manager and systems such as AAA and external storage, refer to the recommendations in Harden Your Cisco EPN Manager Storage.

Set Up HTTPS to Secure the Connectivity of the Web Server

HTTPS operations use a server key that is generated using public key cryptography algorithms, and trust chain certificates that are generated using the server key. These certificates are applied to the Cisco EPN Manager web server. Depending upon how you generated the certificates, you may have to request the client browsers to trust these certificates the first time the browser connect s to the web server. The HTTPS mechanism ensures the security of the server machine (which in turn improves security of all other associated systems).

Use one of the following two methods to generate and install the web server certificate (do not use the methods together).

Signing Entity	Description	See:
Self-signed certificates	You generate the self-signed certificates and then apply them to the web server. This method can be used on: • Deployments that do not use HA • HA deployments that *do not* use virtual IP addresses.	Generate and Apply Self-Signed Web Server Certificate, on page 5

Signing Entity	Description	See:
Certificate Authority (CA) signed certificates	A Certificate Authority (CA) generates and issues these certificates. The certificates bind a public key to the name of the entity (for example, a server or device) that is identified in the certificate. You must generate a Certificate Signing Request (CSR) file from the Cisco EPN Manager server, and submit the CSR file (which contains the server key) to the CA. When you receive the certificates, you apply them to the web server. These certificates can be generated by an external CA or an internal CA. • External CA—An external CA organization validates identities and issues the certificates, usually for a fee. (Popular browsers are usually pre-installed with Root and Intermediate certificates issued by the external CA organization). • Internal CA—Uses a certificate-generating server within your organization (this avoids a fee). The internal CA functions exactly the same way as an external fee-based CA. This method can be used on: • Deployments that do not use HA • HA deployments that *do* use virtual IP addresses (including SSL connections between browser-based clients) **Note** Depending on your deployment, you may need to instruct your users to install the CA-signed Root and Intermediate certificates to their browser or OS certificate store. Ask your organization's IT administrator if this is required. Instructions are provided in Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 13.	Generate and Apply a CA-Signed Web Server Certificate, on page 6

Generate and Apply Self-Signed Web Server Certificate

The following procedure generates an RSA key and then applies a self-signed certificate with domain information.

Before You Begin

Make sure you have the fully qualified domain name (FQDN) of the server. You will need it for this procedure.

Step 1 Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

Step 2 Enter the following command:

```
ncs key genkey -newdn
```

Step 3 To activate the certificate, restart Cisco EPN Manager . See Stop and Restart Cisco EPN Manager , on page 18.

Generate and Apply a CA-Signed Web Server Certificate

The following topics explain how to generate and apply CA-signed certificates to the Cisco EPN Manager web server. The procedures are slightly different depending on whether or not your deployment is using HA, and if it is using HA, whether or not you are using HA with virtual IP addresses.

You may need to instruct your users to install the Root and Intermediate CA certificates to their browser or OS certificate store. Ask your organization's IT administrator if this is required. Instructions are provided in Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 13.

Deployment Type	Summary of Steps
Deployment without HA	For deployments without HA, you must request the certificate, import it into your web server, and restart the web server to apply it, as described in these topics: 1 Request a CA-Signed Web Server Certificate, on page 6 2 Import and Apply a CA-Signed Web Server Certificate—No HA, on page 7
High availability deployment *not using* virtual IP addresses	For HA deployments that do not use virtual IPs, you must request separate certificates for the primary and secondary servers and then import the appropriate certificate onto each server. When you restart the servers to apply the certificates, you must restart them in a specific order. The entire procedure is described in these topics: 1 Request a CA-Signed Web Server Certificate, on page 6 2 Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses, on page 8
High availability deployment *using* virtual IP addresses	For HA deployments that use virtual IPs, you only need to request a single certificate for both servers. You must remove HA on the servers, import the certificate on both servers, and then restart the servers to apply the certificate (you must restart the servers in a specific order). Finally, you reconfigure HA by registering the secondary server on the primary server. The entire procedure is described in these topics: 1 Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 10 2 Register the Secondary Server on the Primary Server

Request a CA-Signed Web Server Certificate

Use this procedure to request a CA-signed web server certificate for your deployment. You should use this procedure if:

- Your deployment does not use HA
- Your deployment uses HA but does not use virtual IP addressing (you will need to perform the following procedure on both servers)

Note If your deployment uses HA with virtual IP addresses, use the procedure in Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 10.

Before You Begin

Make sure SCP is enabled on your machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 Generate a Certificate Signing Request (CSR) file for the Cisco EPN Manager server:

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Enter the following command to generate the CSR file in the default backup repository (defaultRepo):

```
ncs key genkey -newdn -csr CertName.csr repository defaultRepo
```

where *CertName* is an arbitrary name of your choice.

Step 2 Copy the CSR file from the Cisco EPN Manager server to your local machine.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Log in as the Linux CLI root user. See Log In and Out as the Linux CLI root User.

c) Copy the file from the Cisco EPN Manager server to your local machine. For example:

```
scp /localdisk/defaultRepo/CertName.csr clientUserName@clientIP:/destinationFolder
```

d) Log out as the Linux CLI root user.

Step 3 Submit the CSR file to a Certificate Authority of your choice.

Note Once you have generated and sent the CSR file for certification, do *not* use the **genkey** command to generate a new key on the same Cisco EPN Manager server. If you do, when you try to import the signed certificate file, you will receive an error due to a mismatch between keys in the file and on the Cisco EPN Manager server.

The CA will send you digitally-signed certificates either in a single file with the name *CertFilename***.cer**, or as a set of multiple files.

Step 4 (HA deployments not using virtual IP addresses) Repeat these steps for the secondary server.

What to Do Next

When you receive the certificates from the CA, import and apply the certificates. Use one of the following procedures, depending on your deployment:

- Import and Apply a CA-Signed Web Server Certificate—No HA, on page 7
- Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses, on page 8

Import and Apply a CA-Signed Web Server Certificate—No HA

This topic explains how to import and apply CA-signed web server certificates to a deployment that does not use HA.

Before You Begin

- You must have the CA-signed certificates you requested using Request a CA-Signed Web Server Certificate, on page 6. You cannot perform the following procedure until you have received the certificates.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 If you receive only one CER file from the CA, proceed to Step 2. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

a) Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) Save this new file with a new name in the format *CertFilename*.**cer**.

Step 2 Copy the CER file from your local machine to the backup repository on the Cisco EPN Manager server.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
b) Log in as the Linux CLI root user. See Log In and Out as the Linux CLI root User.
c) Retrieve the file from your local machine and copy it to the Cisco EPN Manager server default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

d) Log out as the Linux CLI root user.

Step 3 As the Cisco EPN Manager CLI admin user, import the CER file.

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Step 4 Restart Cisco EPN Manager to activate this certificate. See Stop and Restart Cisco EPN Manager , on page 18.

What to Do Next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 13 for more information.

Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses

This topic explains how to import and apply CA-signed web server certificates to an HA deployment that is *not* using virtual IP addresses. (If you have an HA deployment that *does* use virtual IPs, see Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 10.) This procedure is similar to the procedure for a deployment that does have HA, except that you have to perform the procedure on both the primary server and the secondary server.

Note When you restart the servers, follow these steps carefully because the servers must be restarted in a specific sequence.

Before You Begin

- You must have the CA-signed certificates you requested using Request a CA-Signed Web Server Certificate, on page 6. You cannot perform the following procedure until you have received the certificates for each server.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 Import the primary certificates onto the primary server.

a) If you received only one CER file from the CA, proceed to Step 1(b). If you received multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

   1 Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

   2 Save this new file with a new name in the format *CertFilename***.cer**.

b) Log in to the primary Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

c) Log in as the Linux CLI root user. See Log In and Out as the Linux CLI root User.

d) Retrieve the CER file from your local machine and copy it to the Cisco EPN Manager server's default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/fullPathToCERfile /localdisk/defaultRepo
```

e) Log out as the Linux CLI root user.

Step 2 Perform the previous step on the secondary server.

Step 3 On the *secondary* server, import the CER file.

a) Log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

b) Verify that the secondary server is stopped.

c) Import the CER file:

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Note Do not restart the secondary server until you reach Step 5.

Step 4 On the *primary* server, import the CER file.

a) Log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

b) Verify that the primary server is stopped.

c) Import the CER file:

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Note Do not restart the primary server until you reach Step 6.

Step 5 On the *secondary* server, run the following commands:

a) Run the **ncs start** command to restart the server.

b) Verify that the secondary server has restarted.

c) Run the **ncs status** command and verify that the HA status of the secondary server is **Secondary Lost Primary**.

Step 6 On the *primary* server, run the following commands:

a) Run the **ncs start** command to restart the server.

b) Verify that the primary server has restarted.

c) Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted.

Once all the processes on the primary server are up and running, HA registration is automatically triggered between the secondary and primary servers (and an email is sent to the registered email addresses). This normally completes after a few minutes.

Step 7 Verify the HA status on the primary and secondary servers by running the **ncs ha status** command on both servers. You should see the following:

- The primary server state is **Primary Active**.
- The secondary server state is **Secondary Syncing**.

What to Do Next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 13 for more information.

Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses

If you have a high availability deployment that uses virtual IP addresses, you need to make only one certificate request. When you receive the certificate from the CA, you install the same certificate on both the primary and secondary servers. This is different from HA deployments that do not use IP addressing, where you make two certificate requests and install one certificate on the primary server and the other (different) certificate on the secondary server.

For more information on virtual IPs and HA, see Using Virtual IP Addressing With HA

Before You Begin

Make sure SCP is enabled on your machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 Generate a CSR file and private key for the primary and secondary servers. You will install the private key on both servers, and submit the CSR file to a Certificate Authority of your choice. The following example shows how to create these files using openssl in Linux.

a) Generate the CSR file in the default backup repository.

openssl req -newkey rsa:2048 -nodes -keyout *ServerKeyFileName* **-out** *CSRFileName* **-config** *opensslCSRconfigFileName*

where:

- *ServerKeyFileName* is the name you want to use for the private key file.
- *CSRFileName* is the name that you want to use for the CSR request file, which will be submitted to the CA.
- *opensslCSRconfigFileName* is the name of the file that contains the openssl configurations used to generate the CSR file.

b) Using a text editor, edit the file with openssl configurations (*opensslCSRconfigFileName* in (a)) to have contents similar to the following.

```
[req]
 distinguished_name = req_distinguished_name
 req_extensions = v3_req

 [req_distinguished_name]
 countryName = Country
 countryName_default = US
 stateOrProvinceName = State
 stateOrProvinceName_default = CA
 localityName = City
 localityName_default = San Jose
 organizationName = Organization
 organizationName_default = Cisco Systems
 organizationalUnitName = Organizational Unit
 organizationalUnitName_default = CSG
 commonName = Common Name
 commonName_default = example.cisco.com
 commonName_max = 64

 [ v3_req ]
 # Extensions to add to a certificate request
 basicConstraints = CA:FALSE
 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 subjectAltName = @alt_names

 [alt_names]
 DNS.1 = example.cisco.com
 DNS.2 = example-pri.cisco.com
 DNS.3 = example-sec.cisco.com
```

```
IP.1 = 209.165.200.224
IP.2 = 209.165.200.225
IP.3 = 209.165.200.226
```

In this example:

- The virtual IP address is 209.165.200.224. The FQDN for is **example.cisco.com**. The FQDN is also used for the DNS server name.
- The primary server IP address is 209.165.200.225. Its hostname is **example-pri**. This hostname should be included in /etc/hosts and other hostname setting files.
- The secondary server IP address is 209.165.200.226. Its hostname is **example-sec**.

Step 2 Submit the CSR file to a Certificate Authority of your choice. The CA will send you digitally-signed certificates either in a single file with the name *CertFilename***.cer**, or as a set of multiple files.

Step 3 If you receive only one CER file from the CA, proceed to Step 4. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

a) Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) Save this new file with a new name in the format *CertFilename***.cer**.

Step 4 On the primary server, copy the CER file to the backup repository on each server.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Log in as the Linux CLI root user. See Log In and Out as the Linux CLI root User.

c) Retrieve the file from your local machine and copy it to the server's default backup repository (defaultRepo).

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

d) Log out as the Linux CLI root user.

Step 5 Repeat the previous step on the secondary server.

Step 6 On the *primary* server, as the Cisco EPN Manager CLI admin user, remove the HA settings:

```
ncs ha remove
```

Run the **ncs ha status** to verify if the HA settings is removed before proceeding with the next step.

Step 7 On both the primary and secondary server, import the CER file.

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Step 8 Restart the primary and secondary servers. Because they are not yet paired for HA, the order does not matter. See Stop and Restart Cisco EPN Manager , on page 18.

Note If the server does not restart, it may indicate that you mistakenly imported an individual certificate file instead of a concatenated certificate file (even though the import operation appeared to be successful). To fix this, repeat the import operation using the (correct) concatenated certificate file.

Step 9 Verify the status of the primary and secondary servers by running the **ncs status** command on both servers.

Step 10 Register the secondary server on the primary server for HA. See Register the Secondary Server on the Primary Server.

What to Do Next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 13 for more information.

Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store

Ask your organization's IT administrator if your users should install the CA Root and Intermediate CA certificates to their browser or OS certificate store. If not done in situations where it is required, users will see indications on their browsers that the browsers are not trusted.

Depending on your browser type and version, the exact steps for this procedure may be slightly different.

Before You Begin

If you are adding the certificates to an Internet Explorer browser, you must have Administrator privileges on your client machine.

Step 1 For Firefox browsers, follow these steps to import the certificates.

a) Choose **Tools** > **Options**, then click **Advanced** from the options on the left.
b) Click **Certificates** from the list at the top of the window, then click **View Certificates**. This opens the browser's Certificate Manager dialog box.
c) In the Certificate Manager dialog box, click the **Authorities** tab, then click **Import** at the bottom of the dialog box.
d) In the **Select File...** dialog box, browse to the CA-signed Root certificate file, then click **Open**.
e) Import the file.
f) Repeat the import steps for the CA-signed Intermediate certificate file.

Step 2 For Internet Explorer browsers, use the Microsoft Certificate Manager tool to import the certificates. To use this tool, users must have Administrator privileges on their client machine.

a) In Windows 7, click **Start**.
b) Enter **certmgr.msc** in the Search text box, the hit Return.
c) Launch the Microsoft Certificate Manager by clicking the program's icon in the Search results.
d) In the left column of the Certificate Manager GUI, choose **Trusted Root Certification Authorities**.
e) Left-click **Certificates**, then choose **All Tasks** > **Import**.
f) Click **Next**, then browse to the CA-signed Root certificate file, and import it.
g) Repeat the import steps for the CA-signed Intermediate certificate file, but choose **Intermediate Certification Authorities** as the first step for importing the certificate.

Change the HTTPS Server Port

Because many devices use HTTPS to relay device configuration information, HTTPS is enabled by default in Cisco EPN Manager . (HTTP is not used by Cisco EPN Manager and is disabled by default.) If needed, you can change the port for the HTTPS server by following these steps.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 In the HTTPS area, enter the new port number, then click **Save**.

Step 3 Restart Cisco EPN Manager to apply your changes. See Stop and Restart Cisco EPN Manager , on page 18.

View Existing CA Certificates

To view existing certificate for the Cisco EPN Manager server:

Step 1 Log in to the Cisco EPN Manager Admin CLI as the admin user.

Step 2 To view the list of CA Certificates that exist in the Cisco EPN Manager trust store, enter the following command:

```
ncs key listcacerts
```

Step 3 To see the complete trust chain for SSL/HTTPS operations, log into the Cisco EPN Manager web GUI using Google Chrome, and use Chrome to view the CA-signed certificate that the server sent to the browser. Chrome will display all the linked certificates in the trust chain.

Delete CA Certificates

Step 1 Log in to the Cisco EPN Manager server as the admin user.

Step 2 Because you will need the certificate short names for the delete command, list the short names of all the CA certificates on the Cisco EPN Manager server:

```
ncs key listcacert
```

Step 3 Locate the CA certificate you want to delete and enter the following command:

```
ncs key deletecacert aliasname
```

where *aliasname* is the short name of the CA certificate you want to delete.

Establish an SSH Session With the Cisco EPN Manager Server

When you connect to the server, use SSH and log in as the admin user. (See User Interfaces, User Types, and How To Transition Between Them for more information.)

Step 1 Start your SSH session and log in as the Cisco EPN Manager admin user.

- From the command line, enter the following, where *server-ip* is the Cisco EPN Manager :

```
ssh admin server-ip
```

- Open an SSH client and log in as **admin**.

Step 2 Enter the admin password. The prompt will change to the following:

```
(admin)
```

To view a list of the operations the admin user can perform, enter **?** at the prompt.

To enter admin config mode, enter the following command (note the change in the prompt):

```
(admin) configure terminal
(config)
```

Set Up NTP on the Server

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the Cisco EPN Manager server. Failure to manage NTP synchronizations across your network can result in anomalous results in Cisco EPN Manager . This includes all Cisco EPN Manager -related servers: Any remote FTP servers that you use for Cisco EPN Manager backups, secondary Cisco EPN Manager high-availability servers, and so on.

You specify the default and secondary NTP servers during Cisco EPN Manager server installation. You can also use Cisco EPN Manager 's **ntp server** command to add to or change the list of NTP servers after installation.

Note Cisco EPN Manager cannot be configured as an NTP server; it acts as an NTP client only. Up to three NTP servers are allowed.

Step 1 Log in to the Cisco EPN Manager server as the admin user and enter config mode. See Establish an SSH Session With the Cisco EPN Manager Server, on page 15.

Step 2 Set up the NTP server using one of the following commands.

```
ntp server ntp-server-IP ntp-key-id ntp-key
```

Where:

- *ntp-server-IP* is the IP address or hostname of the server providing the clock synchronization to the Cisco EPN Manager server
- *ntp-key-id ntp-key* is the md5 key ID md5 key of the authenticated NTP server

Set Up the Cisco EPN Manager Proxy Server

Use this procedure to configure proxies for the server and, if configured, its local authentication server. If you use a proxy server as a security barrier between your network and the Internet, you need to configure the proxy settings as shown in the following steps:

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Click the **Proxy** tab.

Step 3 Select the **Enable Proxy** check box and enter the required information about the server that has connectivity to Cisco.com and will act as the proxy.

Step 4 Select the **Authentication Proxy** check box and enter the proxy server's user name and password.

Step 5 Click **Test Connectivity** to check the connection to the proxy server.

Step 6 Click **Save**.

Set Up the SMTP E-Mail Server

To enable Cisco EPN Manager to send email notifications (for alarms, jobs, reports, and so forth), the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Mail Server Configuration**.

Step 2 Under Primary SMTP Server, complete the Hostname/IP, User Name, Password, and Confirm Password fields as appropriate for the email server you want Cisco EPN Manager to use. Enter the IP address of the physical server. and the Enter the hostname of the primary SMTP server.

Note You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.

Step 3 (Optional) Complete the same fields under Secondary SMTP Server. SMTP server username and password.

Step 4 Under Sender and Receivers, enter a legitimate email address for Cisco EPN Manager .

Step 5 When you are finished, click **Save**.

Enable FTP/TFTP/SFTP Service on the Server

FTP/TFTP/SFTP is used to transfer files between the server and devices for device configuration and software image file management. These protocols are also used in high availability deployments to transfer files to a secondary server. These services are normally enabled by default. If you installed Cisco EPN Manager in FIPS mode, they are disabled by default. If you use this page to enable these services, Cisco EPN Manager will become non-compliant with FIPS.

SFTP is the secure version of the file transfer service and is used by default. FTP is the unsecured version of the file transer service; TFTP is the simple, unsecured version of the service. If you want to use either FTP or TFTP, you must enable the service after adding the server.

To change the FTP/TFTP/SFTP password, see Change the FTP User Password, on page 20.

Step 1 Configure Cisco EPN Manager to use the FTP, TFTP, or SFTP server.

a) Choose **Administration** > **Servers** > **TFTP/FTP/SFTP Servers**.

b) From the **Select a command** drop-down list, choose **Add TFTP/FTP/SFTP Server**, then click **Go**.

- From the **Server Type** drop-down list, choose **FTP**, **TFTP**, **SFTP**, or **All**.
- Enter a user-defined name for the server.
- Enter the IP address of the server.

c) Click **Save**.

Step 2 If you want to use FTP or TFTP, enable it on the Cisco EPN Manager server.

a) Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

b) Go to the FTP or TFTP area.

c) Click **Enable**.

d) Click **Save**.

Step 3 Restart Cisco EPN Manager to apply your changes. See Stop and Restart Cisco EPN Manager , on page 18.

Configure Stored Cisco.com Credentials

Cisco EPN Manager can use stored Cisco.com credentials (user name and password) to log in to Cisco.com when it performs the following tasks:

- Checks for product software updates
- Checks for device software image updates
- Opens or reviews Cisco support cases

If these settings are not configured, Cisco EPN Manager will prompt users for their credentials when they perform these tasks. To configure a global Cisco.com user name and password:

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Credentials**.

Step 2 Under the **Cisco.com Credentials** tab, enter a user name and password, and click **Save**.

Create a Login Banner (Login Disclaimer)

When you have a message that you want to display to all users before they log in, create a login disclaimer. The text will be displayed on the GUI client login page below below the login and password fields.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Login Disclaimer**.

Step 2 Enter (or edit) the login disclaimer text.

Note Carriage returns are ignored.

Your changes will take effect immediately.

Stop and Restart Cisco EPN Manager

An Cisco EPN Manager restart is needed in rare cases, such as after a product software upgrade. When you stop the Cisco EPN Manager server, all user sessions and terminated.

To stop the server, open a CLI session with the server and enter:

```
ncs stop
```

To restart the server, open a CLI session with the server and enter:

```
ncs start
```

Configure Global SNMP Settings for Communication with Network Elements

The SNMP Settings page controls the how the server uses SNMP to reach and monitor devices. These settings will determine when a device is considered unreachable. Any changes you make on this page are applied globally and are saved across restarts, as well as across backups and restores.

Note The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network, so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. You should update the prepopulated SNMP credential with your own SNMP information.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Network and Device** > **SNMP**.

Step 2 (Optional) Select the **Trace Display Values** check box to display mediation trace-level logging data values that are fetched using SNMP.

Step 3 Choose an algorithm from the **Backoff Algorithm** drop-down list.

- **Exponential—**Each SNMP try will wait twice as long as the previous try, starting with the specified timeout for the first try.
- **Constant—**Each SNMP try will wait the same length of time (timeout). This is useful on unreliable networks where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.

Step 4 If you do not want to use the timeout and retries specified by the device, configure the following parameters.

Note If switch port tracing is taking a long time to complete, reduce the Reachability Retries value.

- **Reachability Retries—**Enter the number of global retries.
- **Reachability Timeout—**Enter a global timeout.

Step 5 In the **MaximumVarBinds per PDU** field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. This Maximum VarBinds per PDU field enables you to make necessary changes when you have any failures associated to SNMP. For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.

Step 6 Optionally adjust the **Maximum Rows per Table**.

Step 7 Click **Save**.

Manage Administrative Passwords

Change the FTP User Password

Cisco EPN Manager uses the **ftpuser** ID to access other servers using FTP. Users with Admin privileges can change the FTP password.

Step 1 Log in to the Cisco EPN Manager server as the admin user. Establish an SSH Session With the Cisco EPN Manager Server, on page 15.

Step 2 To change the Cisco EPN Manager server's FTP password, enter:

```
ncs password ftpuser username password password
```

Example

```
(admin) ncs password ftpuser FTPuser password FTPUserPassword
Initializing...
Updating FTP password.
This may take a few minutes.
Successfully updated location ftpuser
```

Change the Web GUI Root User Password

Cisco EPN Manager uses the **root** ID to perform special tasks that require root access to the web GUI.

Before You Begin

You must know the current web GUI root user password to change it.

Step 1 Log in to the Cisco EPN Manager Admin CLI as the **root** user. (For information on the Admin CLI, see User Interfaces and User Types.)

Step 2 Enter the following command, where *newpassword* is the new web GUI root password:

```
ncs password root password  newpassword
```

Example

```
ncs password root password NewWebGUIRootPassword
Password updated for web root password
```

Recovering Administrator Passwords on Virtual Appliances

This topic explains how to recover and reset the admin password on Cisco EPN Manager virtual machines (also known as OVAs).

Before You Begin

Ensure that you have:

- Physical access to the Cisco EPN Manager server.
- A copy of the installation ISO image appropriate for your version of the software.
- Access to the VMware vSphere client, and to the vSphere inventory, Datastores and Objects functions. If you do not have such access, consult your VMware administrator. Avoid accessing ESX directly from the vSphere client.

Step 1 At the Cisco EPN Manager OVA server, launch the VMware vSphere client.

Step 2 Upload the installation ISO image to the data store on the OVA virtual machine, as follows:

a) In the vSphere inventory, click **Datastores**.
b) On the **Objects** tab, select the datastore to which you will upload the file.
c) Click the **Navigate to the datastore file browser** icon.
d) If needed, click the **Create a new folder** icon and create a new folder.
e) Select the folder that you created or select an existing folder, and click the **Upload a File** icon.
If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.
f) On the local computer, find the ISO file and upload it.
g) Refresh the datastore file browser to see the uploaded file in the list.

Step 3 With the ISO image uploaded to a datastore, make it the default boot image, as follows:

a) Using the VMware vSphere client, right-click the deployed OVA and choose **Power > Shut down guest**.
b) Select **Edit Settings > Hardware**, then select **CD/DVD drive 1**.
c) Under **Device Type**, select **Datastore ISO File**, then use the **Browse** button to select the ISO image file you uploaded to the datastore.
d) Under **Device Status,** select **Connect at power on**.
e) Click the **Options** tab and select **Boot Options**. Under **Force BIOS Setup**, select **Next time VM boots, force entry into BIOS setup Screen**. This will force a boot from the virtual machine BIOS when you restart the virtual machine.
f) Click **OK**.
g) In the VMware vSphere client, right-click the deployed OVA and choose **Power > Power On**.
h) In the BIOS setup menu, find the option that controls the boot order of devices and move **DVD/CDROM** to the top.

Step 4 Follow the steps below to reset a server administrator password:

a) Save your BIOS settings and exit the BIOS setup menu. The virtual machine will boot from the ISO image and display a list of boot options.
b) Enter **3** if you are using the keyboard and monitor to access the OVA, or **4** if you are accessing via command line or console. The vSphere client displays a list of administrator user names.
c) Enter the number shown next to the administrator username for which you want to reset the password.

d) Enter the new password and verify it with a second entry.

e) Enter **Y** to save your changes and reboot.

f) Once the virtual machine has rebooted: Using the vSphere client, click on the CD icon and select **Disconnect ISO image**.

Step 5 Log in with the new admin password.

Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard

The System Monitoring Dashboard provides information about the configuration and performance of the Cisco EPN Manager server. To access the dashboard, choose **Administration** > **Dashboards** > **System Monitoring Dashboard** (your User ID must have administrator privileges to access this dashboard). If you want to customize the dashlets that are displayed in the Overview or Performance tabs, follow the instructions in Add a Predefined Dashlet To a Dashboard.

Dashboard Tab	Description
Overview	Backup and data purging jobs, Cisco EPN Manager system alarms, and utilization statistics for server CPU, disk, and memory. You can specify different time frames to check this information. To view the server time, kernel version, operating system, hardware information, and so forth, click **System Information** at the top left of the dashboard to open a field with that information. You can add and delete dashlets from the Overview dashboard.
Performance	Server syslogs and traps, and input/output. You can specify different time frames for this data, and add and remove dashlets from the Performance dashboard.
Admin	• Health—System alarms, number of jobs running, number of users logged in, and database usage distribution. You can specify different time frames for historical information. • API Health—Lists all API services with their response time statistics. • Service Details—Statistics for a specific service (response count and time trend, calls per client (clients are identified by their IP address). You can pick the service you want to check.

Improve the Cisco EPN Manager Server Performance

- Check the OVA Size, on page 23

- Compact the Database, on page 23
- Manage Server Disk Space Issues, on page 23

Check the OVA Size

If Cisco EPN Manager is using 80 percent or more of your system resources or the device/interface/flow counts recommended for the size of OVA you have installed, this can negatively impact performance. Make sure the OVA is not exceeding the device, interface, and flow record recommendations given in the installation documentation. They are the maximums for each given OVA size. You can check these from the Admin Dashboard (see Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 22). To respond to space issues, see Manage Server Disk Space Issues, on page 23.

Compact the Database

Step 1 Log in to the server as the admin user. Establish an SSH Session With the Cisco EPN Manager Server, on page 15.

Step 2 Enter the following command to compact the application database:

```
(admin)# ncs cleanup
```

Step 3 When prompted, answer **Yes** to the deep cleanup option.

Manage Server Disk Space Issues

Cisco EPN Manager will trigger alarms indicating that the server is low on disk space at the following thresholds:

- 60% usage triggers a Major alarm
- 65% usage triggers a Critical alarm

If you receive an alert, consider performing the following actions:

- Free up existing database space as explained in Compact the Database, on page 23.
- If you are saving backups to a local repository, consider using a remote backup repository. See Configure the NFS Backup Server.
- Reduce the retention period for network inventory, performance, reports, and other classes of data as explained in Data Collection and Purging.
- Add more disk space. VMware OVA technology enables you to easily add disk space to an existing server. You will need to shut down the Cisco EPN Manager server and then follow the instructions provided by VMware to expand the physical disk space. Once you restart the virtual appliance, Cisco EPN Manager automatically makes use of the additional disk space (see Data Collection and Purging).

- Set up a new server that meets at least the minimum RAM, disk space, and processor requirements of the next higher level of OVA. Back up your existing system, then restore it to a virtual machine on the higher-rated server.

Work With Server Internal SNMP Traps That Indicate System Problems

Cisco EPN Manager generates internal SNMP traps that indicate potential problems with system components. This includes hardware component failures, high availability state changes, backup status, and so forth. The failure trap is generated as soon as the failure or state change is detected, and a clearing trap is generated if the failure corrects itself. For TCAs (high CPU, memory and disk utilization traps, and so forth), the trap is generated when the threshold is exceeded.

A complete list of server internal SNMP traps is provided in Cisco Evolved Programmable Network Manager Supported Alarms. Cisco EPN Manager sends traps to notification receivers on port 162. This port cannot be customized at present.

You can customize and manage these traps as described in the following topics:

- Customize Server Internal SNMP Traps and Forward the Traps, on page 24
- Troubleshoot Server Internal SNMP Traps, on page 25

Customize Server Internal SNMP Traps and Forward the Traps

You can customize server internal SNMP traps by adjusting their severity or (for TCAs) thresholds. You can also disable and enable the traps. Server internal SNMP traps are listed in Cisco Evolved Programmable Network Manager Supported Alarms.

Note Cisco EPN Manager does not send SNMPv2 Inform or SNMPv3 notifications.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **System Event Configuration**.

Step 2 For each SNMP event you want to configure:

a) Click on the row for that event.

b) Set the **Event Severity** to Critical, Major, or Minor, as needed.

c) For the CPU, disk, memory utilization, and other hardware traps, Enter the **Threshold** percentage (from 1–99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. (You cannot set thresholds for events for which the threshold setting is shown as NE.) These events send traps whenever the associated failure is detected.

d) For backup threshold and certificate expiry (critical), enter the **Threshold** in days (from *x*–*y*, where *x* is the minimum number of days and *y* is the maximum number of days).

e) To control whether a trap is or is not generated, set the **Event Status**.

Step 3 To save all of your trap changes, click **Save** (below the table).

Step 4 If you want to configure receivers for the server internal SNMP traps, refer to the procedures in the following topics, depending on whether you want to send the information as an email or trap notification.

- Forward Alarms and Events as Email Notifications (Administrator Procedure)
- Forward Alarms and Events as SNMP Trap Notifications

Troubleshoot Server Internal SNMP Traps

Cisco Evolved Programmable Network Manager Supported Alarms provides a complete list of server internal SNMP traps, their probable cause, and recommended actions to remedy the problem. If that document does not provide the information you need, follow this procedure to troubleshoot and get more information about Cisco EPN Manager server issues.

Step 1 Ping the notification receiver from the Cisco EPN Manager server to ensure that there is connectivity between Cisco EPN Manager and your management application.

Step 2 Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

Step 3 Log in to Cisco EPN Manager with a user ID that has Administrator privileges. Select **Administration > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:

- ncs_nbi.log: This is the log of all the northbound SNMP trap messages Cisco EPN Manager has sent. Check for messages you have not received.
- ncs-# -# .log: This is the log of most other recent Cisco EPN Manager activity. Check for hardware trap messages you have not received.
- hm-# -# .log: This is the log of all Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspect log files with your case. See Open a Cisco Support Case.

Set Up Defaults for Cisco Support Requests

By default, users can create Cisco support requests from different parts of the Cisco EPN Manager GUI. If desired, you can configure the sender e-mail address and other e-mail characteristics. If you do not configure them, users can supply the information when they open a case.

If you do not want to allow users to create requests from the GUI client, you can disable that feature.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Click the **Support Request** tab.

Step 3 Select the type of interaction you prefer:

- Enable interactions directly from the server—Specify this option to create the support case directly from the Cisco EPN Manager server. E-Mails to the support provider are sent from the e-mail address associated with the Cisco EPN Manager server or the e-mail address you specify.
- Interactions via client system only—Specify this option to download the information required for your support case to a client machine. You must then e-mail the downloaded support case details and information to the support provider.

Step 4 Select your technical support provider:

- Click **Cisco** to open a support case with Cisco Technical Support, enter your Cisco.com credentials, then click **Test Connectivity** to check the connectivity to the following servers:
    - Cisco EPN Manager mail server
    - Cisco support server
    - Forum server
- Click **Third-party Support Provider** to create a service request with a third-party support provider. Enter the provider's e-mail address, the subject line, and the website URL.

Configure Cisco Product Feedback Settings

To help Cisco improve its products, Cisco EPN Manager collects the following data and sends it to Cisco:

- Product information—Product type, software version, and installed licenses.
- System information—Server operating system and available memory.
- Network information—Number and type of devices on your network.

This feature is enabled by default. Data is collected on a daily, weekly, and monthly basis and is posted to a REST URL in the Cisco cloud using HTTPS. Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Help Us Improve**, and:

- To view the types of data Cisco collects, click **What data is Cisco collecting?**
- To disable this feature, select **Not at this time, thank you**, then click **Save**.