Best Practices: Harden Your Cisco EPN Manager Security

Cisco EPN Manager Security Hardening Overview

Security hardening entails making adjustments to ensure that all of the following components make optimal use of their security mechanisms:

- Cisco EPN Manager web server
- Cisco EPN Manager server
- Cisco EPN Manager storage system (local or external)
- Communication between Cisco EPN Manager and devices
- User authentication system (local or external)
- Time synchronizing system that use Network Time Protocol (NTP)

Although your primary source of information is your Cisco representative, who can provide server hardening guidance specific to your deployment, you can also follow the steps listed below to secure your Cisco EPN Manager product.

Hardening Procedure	The procedure hardens:
Make Web Server Connectivity Secure By Using HTTPS, on page 2	Cisco EPN Manager Web server
Set Up Certificated-Based Authentication for Web Clients, on page 2	
Configure and Manage OCSP on the Server, on page 5	

Hardening Procedure	The procedure hardens:
Disable Insecure Ports and Services, on page 6	Cisco EPN Manager Server
Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices, on page 7	
Set Up External Authentication Using the CLI, on page 8	
Disable Accounts Not Needed for Day-to-Day Operations, on page 8	
Harden NTP, on page 9	
Harden Your Cisco EPN Manager Storage, on page 10	Cisco EPN Manager storage system (local or external)

Harden the Cisco EPN Manager Web Server

To harden the Cisco EPN Manager web server, do the following:

1. Make Web Server Connectivity Secure By Using HTTPS, on page 2
2. Set Up Certificated-Based Authentication for Web Clients, on page 2
3. Configure a Custom OCSP Responder on the Server, on page 5

Make Web Server Connectivity Secure By Using HTTPS

The Cisco EPN Manager web server should be configured to use HTTPS instead of HTTP. This protects the systems that connect to the Cisco EPN Manager web server and also avoids the possibility of any client indirectly intruding into the Cisco EPN Manager web server and other participating systems. HTTPS requires using a Certificate Authority (CA) certificate in the web server and appropriate SSL mechanisms. For information on how to set this up, see Set Up HTTPS to Secure the Connectivity of the Web Server.

Set Up Certificated-Based Authentication for Web Clients

For higher-level security, the Cisco EPN Manager server should authenticate clients by using certificate-based authentication. With this form of authentication, Cisco EPN Manager first validates the client's associated certificatee to ensure that the client is authentic, then it validates the user's user name and password. This mechanism prevents unauthorized machines (that is, machines for which no certificate exists) to connect with the web server. Cisco EPN Manager implements this feature using the Online Certificate Status Protocol (OCSP).

Note The certificate(s) discussed in this topic uniquely identify the *clients*. This is different from the certificate for the *web server*, which was used to set up HTTPS operation (see Make Web Server Connectivity Secure By Using HTTPS, on page 2). While this procedure is similar to the procedure for generating CER files for web server certificates, it is not exactly the same. You might need to use other tools (such as OpenSSL). In addition, there are different methods for generating CA certificate files. If you need assistance, contact your Cisco representative.

Step 1 Generate the client certificate files using a CA. This normally involves the following steps:

a) Generate the public key.
b) Generate the CSR file containing the public key.
c) Submit the CSR file to a CA to get the certificate file(s).
d) When you receive the certificate files, if you have multiple files, do not concatenate the files to make a single CER/PEM file. Instead:

- Give the *Client* certificate file to the application user to keep in the client machine.
- Keep the *Root* and all *Intermediate* CA certificates. You will import them into the server in Step 4.

Note You should get these certificates from the root and intermediate CA servers. Do not use any files received from a non- trusted source.

Note Do not import the Client CA certificate into the web server. Keep that file with the client machine—for example, on an insertable card, a hardware or software token device, and so forth. When the client browser tries to connect to the Cisco EPN Manager web server, the web server instructs the client browser to ask for the Client certificate. The user must provide the Client certificate, and then enter their user name and password.

Step 2 Log in to the Cisco EPN Manager server using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server. Do not enter config mode.

Step 3 Enable client certificate authentication on the Cisco EPN Manager web server. The following command instructs the web server to enable and use certificate-based client authentication (instead of using user names and passwords alone).

```
ncs run client-auth enable
```

Step 4 Import the Root CA and Intermediate CA certificate files separately (one at a time) into the Cisco EPN Manager web server.

a) Import the Root CA certificate file.

```
ncs key importcacert aliasName rootCACertFile repository repoName
```

Where:

- *aliasName* is the short name supplied for the CA certificate.
- *rootCACertFile* is the Root CA certificate file name.
- *repoName* is the location of the Cisco EPN Manager repository where the certificate file is hosted.

Note Note that this command is very different from the command used to apply the server certificate.

b) Import the Intermediate CA certificate file.

```
ncs key importcacert aliasName intermediateCACertFile repository repoName
```

Step 5 Restart the server(s). The procedure you should follow depends on whether or not your deployment is configured for high availability.

For deployments *without* high availability, restart the Cisco EPN Manager server to apply the changes.

```
ncs stop
ncs start
```

For deployments *with* high availability, follow these steps, being sure to restart the servers in the correct order.

a) On the *secondary* server, log in as the Cisco EPN Manager CLI admin user and stop the server:
```
ncs stop
```

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

b) Verify that the secondary server is stopped.

c) On the *primary* server, log in as the Cisco EPN Manager CLI admin user and stop the server:
```
ncs stop
```

Note Do not restart the primary server until you reach Step 5(f).

d) Verify that the primary server is stopped.

e) On the *secondary* server, run the following commands:

1. Run the **ncs start** command to restart the server.
2. Verify that the secondary server has restarted.
3. Run the **ncs status** command and verify that the Health Monitor process is running.
4. Run the **ncs ha status** command and verify that the HA status of the secondary server is **Secondary Lost Primary**.

f) On the *primary* server, run the following commands:

1. Run the **ncs start** command to restart the server.
2. Verify that the primary server has restarted.
3. 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.

g) 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**.

Configure and Manage OCSP on the Server

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, configure the OCSP responder URL on the Cisco EPN Manager server.

Configure a Custom OCSP Responder on the Server

To configure a custom OCSP responder URL on the Cisco EPN Manager server:

Step 1 Log in to the Cisco EPN Manager server using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server. Do not enter config mode.

Step 2 Enter the following command to enable client certificate authentication:

```
ocsp responder custom enable
```

Step 3 Enter the following command to set the custom OCSP responder URL:

```
ocsp responder set url  responderNumber responderURL
```

Where:

- *responderNumber* is the number of the OCSP responder you want to define (e.g., 1 or 2).
- *responderURL* is the URL of the OCSP responder, as taken from the client CA certificate.

Delete a Custom OCSP Responder from the Server

To delete an existing custom OCSP responder defined on the Cisco EPN Manager server:

Step 1 Execute the **show security-status** command to view the custom OCSP responders that are currently configured on the server, and identify the number of the responder you want to delete.

Step 2 Delete the OCSP responder from the server:

```
ocsp responder clear url responderNumber
```

Harden the Cisco EPN Manager Server

Follow these steps to harden the Cisco EPN Manager server.

Disable Insecure Ports and Services

As a general policy, any ports that are not needed and are not secure should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager for your deployment. You can do this by listing the ports that are open and comparing it with a list of ports that are safe to disable.

You can get this list of ports which are safe to disable from Cisco Evolved Programmable Network Manager Installation Guide,which lists the ports and services used by Cisco EPN Manager .

Follow the procedure below to find out which ports are enabled.

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server. Do not enter config mode.

Step 2 Display the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information using the show security-status command. You will see output similar to the following.

```
show security-status
Open TCP Ports       22 443 1522 8082
Open UDP Ports       162 514 9991
FIPS Mode            enabled
TFTP Service         disabled
FTP Service          disabled
JMS port (61617)     disabled
Root Access          disabled
Client Auth          enabled
OCSP Responder1      http://209.165.200.224/ocsp
OCSP Responder2      http://209.165.202.128/ocsp
```

Step 3 Check the Cisco Evolved Programmable Network Manager Installation Guide for the table of ports used by Cisco EPN Manager , and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product* .

Note If you are not sure whether you should disable a port or service, contact your Cisco representative.

Step 4 Disable the insecure ports using the Cisco EPN Manager GUI.

This example disables FTP and TFTP, which are not secure protocols and should be disabled (use SFTP or SCP instead). TFTP and FTP are typically used to transfer firmware or software images to and from network devices and Cisco EPN Manager .

a) Log in to Cisco EPN Manager with a user ID that has Administrator privileges.
b) Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.
c) Under **FTP** and **TFTP**, select **Disable**, then click **Save**.
d) Restart Cisco EPN Manager . See Stop and Restart Cisco EPN Manager.

Step 5 If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco EPN Manager to operate. For more information, refer to the Cisco Evolved Programmable Network Manager Installation Guide (specifically, the information about ports that are used by Cisco EPN Manager , and suggested firewall configurations). If you need further help, contact your Cisco representative.

Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices

SNMPv3 is a higher security protocol than SNMPv2. If your devices support SNMPv3, configure the devices to use SNMPv3 to communicate with the Cisco EPN Manager server. The following procedures explain how to specify SNMPv3 when adding new devices.

Method for Adding Devices	How to Specify SNMPv3	For more information, see:
Add a single device	In the **Add Device** dialog box, go to the **SNMP Properties** page and choose **v3** from the **Versions** drop-down list.	Add Devices Manually (New Device Type or Series)
Add multiple devices (bulk import)	When you edit your CSV file, enter the following: • Enter **3** in the **SNMP Version** column. • Enter the appropriate values for these columns: **snmpv3_user_name**, **snmpv3_auth_type**, **snmpv3_auth_password**, **snmpv3_privacy_type**, and **snmpv3_privacy_password**	Import Devices Using a CSV File
Add multiple devices using discovery	In the **Discovery Settings** dialog box, go to the **Credential Settings** area and click **SNMPv3 Credentials**. Click the + sign to add the device credentials.	Run Discovery With Customized Discovery Settings

Before You Begin

Make sure SNMPv3 is enabled (with the appropriate security algorithm, such as HMAC-SHA-96) on the network devices that support it.

Set Up External Authentication Using the CLI

We recommend you manage user accounts and passwords using dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+. In addition to setting up authentication using the following procedure, contact your external authentication vendor for additional security hardening suggestions.

Note If you decide to use local user authentication, check the default password policies to determine whether you want to make them stronger. See Configure Global Password Policies for Local Authentication.

Configure Cisco EPN Manager to authenticate users using external an external AAA server. You can configure the server using the web GUI or by using the command line interface (CLI). To set up remote user authentication via the GUI, see Configure External Authentication.

To configure external authentication using the CLI, follow these steps. In this example, external authentication will be done by an external TACACS+ server.

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter config mode.

Step 3 Enter the following command to setup an external authetn TACACS+ server:

```
aaa authentication tacacs+ server tacacsIP key plain shared-secret
```

Where:

- *tacacsIP* is the IP address of an active TACACS+ server.
- *shared-secret* is the plain-text shared secret for the active TACACS+ server.

Step 4 Enter the following command to create a user with administrator authority, who will be authenticated by the server specified in the previous step:

```
username username password remote role admin [email emailID]
```

Where:

- *username* is the name of the user ID.
- *password* is the plain-text password for the user.
- *emailID* is the email address of the user (optional).

Disable Accounts Not Needed for Day-to-Day Operations

The Cisco EPN Manager web GUI root user should be disabled after creating at least one other web GUI user that has root privileges. See Disable and Enable the Web GUI root User.

Harden NTP

Network Time Protocol (NTP) authenticates server date and time updates. We recommend the Cisco EPN Manager server be configured to have time synchronization over NTP. Failure to manage NTP synchronization across your network can result in anomalous results in Cisco EPN Manager . Management of network time accuracy is an extensive subject that involves the organization's network architecture, and is outside the scope of this guide. For more information on this topic, see (for example) the Cisco White Paper Network Time Protocol: Best Practices .

Because using NTP creates the possibility of security breach-related disruptions, you should also harden the NTP aspect of the Cisco EPN Manager server by using NTP version 4 (NTPv4). Cisco EPN Manager also supports NTPv3 because NTPv4 is backward compatible with NTPv3. You can configure a maximum of three NTP servers with Cisco EPN Manager .

Set Up NTP on the Cisco EPN Manager Server

To use the Network Time Protocol (NTP) to synchronize clocks on the server and network devices using an NTP server, NTP must first be set up on the Cisco EPN Manager server. For information on how to do this, see Set Up NTP on the Server.

Enable NTP Update Authentications

To set up authenticated NTP updates:

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter config mode.

Step 3 Enter the following command to setup an external NTPv4 server:

```
ntp server serverIP userID plain password
```

Where:

- *serverIP* is the IP address of the authenticating NTPv4 server you want to use.
- *userID* is the md5 key id of the NTPv4 server.
- *password* is the corresponding plain-text md5 password for the NTPv4 server.

For example:

```
ntp server 209.165.202.128 20 plain myPass123
```

Step 4 Perform these tests to make sure NTP authentication is working correctly:

a) Check the NTP update details:

```
show run
```

b) Check NTP sync details

```
show ntp
```

Harden Your Cisco EPN Manager Storage

We encourage you to secure all storage elements that will participate in your Cisco EPN Manager installation, such as the database, backup servers, and so forth.

- If you are using external storage, contact your storage vendor and your Cisco representative.
- If you are using internal storage, contact your Cisco representative.
- If you ever uninstall or remove Cisco EPN Manager , make sure that all VM-related files that may contain sensitive data are digitally shredded (as opposed to simply deleted). Contact your Cisco representative for more information