# Best Practices: Harden Your Cisco EPN Manager Security

Security hardening entails making adjustments to ensure that the following components optimize 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)

This appendix will first cover a few core security concepts that administrators should know about. It will then cover the specific tasks that need to be completed in order to optimize Cisco EPN Manager security.



# Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco EPN Manager product, you should have a good understanding of the following security concepts.

## HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco EPN Manager now supports TLS only.

**Note** TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

**Note** Device database backup fails if the device uses TLS version less than 1.2 for HTTPSS communication. For example, NCS2000/ONS 10.5 version.

# SSL Certificates

SSL certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.
2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.
- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

# 1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco EPN Manager server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is

established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.

**Note** A client might need to store multiple server certificates to enable interaction with multiple servers.


To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. You can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully.

# Cisco EPN Manager Security Hardening Overview

Hardening Cisco EPN Manager security requires completion of the following tasks:

(During installation)

- Configuring HTTPS and setting up 1-way SSL authentication for standalone servers and HA environments
- Shutting down insecure and unused ports
- Configuring network firewalls
- Configuring external authentication

(Post installation)

- Updating certificates in response to changes (like setting a new hostname or IP address)
- Hardening the Cisco EPN Manager server, as needed

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 Cisco EPN Manager.

| Hardening Procedure | The procedure hardens: |
|---|---|
| Make Web Server Connectivity Secure By Using HTTPS, on page 4 | Cisco EPN Manager web server |
| Set Up Certificate-Based Authentication for Web Clients, on page 4 | |
| Configure and Manage OCSP on the Server, on page 7 | |
| Disable Insecure Ports and Services, on page 8 | Cisco EPN Manager server |
| Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices | |
| Set Up External Authentication Using the CLI | |
| Disable Accounts Not Needed for Day-to-Day Operations, on page 9 | |
| Harden NTP | |
| Harden Your Cisco EPN Manager Storage, on page 9 | 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 4
2. Set Up Certificate-Based Authentication for Web Clients, on page 4
3. Configure a Custom OCSP Responder on the Server, on page 7

## 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 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.

## Set Up Certificate-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 certificate to ensure that the client is authentic and then it validates the username 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).

Best Practices: Harden Your Cisco EPN Manager Security

**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. 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.

To configure certificate-based authentication:

**Step 1** Generate the client certificate files using a CA, which 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) If you receive 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 username 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** Import the Root CA and Intermediate CA certificate files, one at a time, into the Cisco EPN Manager web server.

a) Import the Root CA certificate file with this command:

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

Where:

- *aliasName* is the short name supplied for the CA certificate.
- *rootCACertFile* is the Root CA certificate filename.
- *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 with this command:

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

Where:

- *intermediateCACertFile* is the Intermediate CA certificate filename.

Best Practices: Harden Your Cisco EPN Manager Security

**Step 4** Restart the server(s). The procedure you should follow depends on whether 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** (Optional) You can enter the following command to check what is configured on the server:

```
show security-status
```

**Step 3** Enter the following command to enable client certificate authentication:

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

**Step 4** Enter the following command to enable the custom OCSP responder URL to override a value of the OCSP responder URL in the certificate.

```
ncs certvalidation custom-ocsp-responder enable
```

**Step 5** Enter the following command to set the custom OCSP responder URL:

```
ncs certvalidation custom-ocsp-responder set url1 responderURL
```

Where:

- *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:

```
ncs certvalidation custom-ocsp-responder clear url1
```

# 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** The show security-status command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. 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.

**Note** In High Availability setup, ensure you disable FTP and TFTP services on the secondary server before configuring High Availability. See Enable FTP/TFTP/SFTP Service on the Server for more information.

**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.

## 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 Your Cisco EPN Manager Storage

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

Contact your Cisco representative for more information about hardening your internal or external storage. In the case of external storage, also contact your storage vendor.

If you ever uninstall or remove Cisco EPN Manager, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted).

## Harden NFS-Based Storage

Since NFS does not have built-in security, you must implement as many of the following security measures as possible to secure the NFS server:

- Set up a firewall in front of the NFS server—To do this practically, tie down the ports that NFS will use in various configuration files and then specify those ports in the firewall configurations.
- Use a port mapper—On the NFS server, only allow NFS transactions that involve specific IP addresses.
- To prevent attacks via a compromised DNS, only specify IP addresses (and not domain names) when configuring NFS.
- When setting up the export of folders, use the **root_squash** option in the /etc/exports file.
- When configuring the /etc/exports file, use the **secure** option.
- When configuring the backup staging and storage folders, use the **nosuid** and **noexec** mount options.

**Note** It is not mandatory to configure a staging folder.

- For the storage folder (and optional staging folder), configure a file access permission value of **755** (which grants all users read and write privileges) and set userid **65534** (the user **nobody**, who does not have any system privileges) as the owner.

Best Practices: Harden Your Cisco EPN Manager Security

- Tunnel NFS traffic either through SSH or SSL/TLS. For SSH, use RSA key-based authentication instead of user authentication.

Do not rely on just one of these measures to secure your NFS-based storage. Your best bet is to implement the combination of measures that best suits your situation. Also keep in mind that this list is not an exhaustive one. To achieve a higher level of confidence when hardening your storage, we recommend that you discuss your situation with a Linux system admin and a security expert beforehand.