FortiNAC

SSL Certificates How To

Version: 8.x
Date: 10/30/2018
Rev: F

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINETTRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE

http://training.fortinet.com

FORTIGUARD CENTER

http://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Tuesday, August 28, 2018

Contents

Process Overview

In order to secure communications with FortiNAC, trusted SSL certificates need to be installed. The basic steps to do this are as follows:

1. **Obtain a Valid SSL Certificate from a Certificate Authority (CA).**

   A Certificate Signing Request (CSR) is issued and submitted to the Certificate Authority (examples are GoDaddy, DigiCert and GlobalSign). Depending upon the type of certificate, the CSR may be generated in FortiNAC, or from another source. The CA then issues the certificates based on the CSR.

2. **Upload the Certificate Received from the CA.**

   Once the certificates are received from the CA, these files must be installed on FortiNAC for the appropriate target (Administrative UI, Captive Portal, Persistent Agent).

3. **Activate Certificates.**

   Depending upon the target, additional steps are necessary in order for the certificate usage to take effect.

4. **Create Certificate Expiration Warning Alarms.**

   To avoid potential agent communication and web access issues with FortiNAC, create alarms to notify when FortiNAC's SSL Certificate is approaching its expiration date.

Implementation Considerations

- In High Availability (HA) environments using a shared IP address (L2 HA), only the certificate files for the Portal target are replicated from the Primary Server to the Secondary Server. If securing the Admin UI and Persistent Agent communication, see **Applying Certificates for L2 and L3 HA**.
- In L3 HA environments where Primary and Secondary Servers are on separate subnets, none of the certificate files are copied to the Secondary. See **Applying Certificates for L2 and L3 HA**.

Certificate Options

SSL Certificates can be issued from the following Certificate Authorities (CA):

- **Third party public** - certificates issued from Certificate Authorities like GoDaddy, DigiCert, GlobalSign, etc.
- **Corporate Owned Internal CA** - certificates issued from within the organization. You may act as your own Certificate Authority (CA) and use your own internal certificate, as long as all systems in your domain use the same certificate.
- **Self-Signed** - FortiNAC issues its own certificate. This option is not as secure, but is an option in situations where a new certificate is not yet available and one is needed (e.g. Administrative UI). **Important:** This type of certificate cannot be used for the Persistent Agent certificate target (for Persistent Agent communication) or the Portal target when using Dissolvable Agents.

Wildcard Certificates

Wildcard certificates can be issued by generating a Certificate Signing Request (CSR) in FortiNAC or a third party. To generate a wildcard CSR using FortiNAC, see **UI Method: Obtaining a Valid SSL Certificate from a Certificate Authority (CA).**

To use a wildcard certificate already generated, skip the section entitled **UI Method: Obtaining a Valid SSL Certificate from a Certificate Authority** and proceed to **UI Method: Upload the Certificate Received from the CA**.

Ensure the following when importing a wildcard certificate:

- The Wildcard Private Key cannot be password protected.
- The actual Fully-Qualified Host Name must be entered in the **Fully-Qualified Host Name** field under **System > Settings > Portal SSL**. Entering the wildcard name in this field will cause the application of the certificate to fail.

Subject Alternative Name (SAN) Certificates

A SAN certificate can be used to secure multiple host names and/or ip addresses. For example, in a Layer 2 HA environment the virtual, Primary, and Secondary appliance host names and their corresponding ip addresses can all be secured with one certificate.

To generate a SAN Certificate using FortiNAC, see **UI Method: Obtaining a Valid SSL Certificate from a Certificate Authority (CA).**

Applying Certificates for L2 and L3 HA

The following procedures apply to all appliances configured for High Availability (including FortiNAC Control Manager).

Administrative UI Method (Requires HA Failover)

1. Secure the Primary Appliances.
2. Force Failover.
3. Secure Secondary Appliances.
4. Restore Control to Primary Appliances.

CLI Method (Does Not Require HA Failover)

1. Secure Primary Appliances via Administrative UI.
2. Secure Secondary Appliances via CLI.

Create Certificate for Use with Multiple PODs

If a wildcard or SAN certificate needs to be created to use with multiple PODs, create the certificate on one POD and install the certificate and Private Key files on all the PODs.

1. Login to the Administrative UI of one of the PODs and generate the CSR (if requesting a SAN, ensure the names of all appliances that will be using the certificate are included).
2. Once the certificates are received from the CA, login to the POD which the CSR was generated and install the certificates. Refer to the following sections:
    a. UI Method: Upload the Certificate Received from the CA
    b. Copying a Certificate to Another Target
    c. UI Method: Activating Certificates
3. Copy the key to a text file.
    a. In Certificate Management, highlight one of the Certificate targets that now has the certificate installed and click Details.
    b. Click on the Private Key tab.
    c. Copy the content to a text file and save. Ensure the complete content is captured.

Example:

```
-----BEGIN RSA PRIVATE KEY-----
...Private Key Data...
-----END RSA PRIVATE KEY-----
```

4. Login to the Administrative UI of the next POD.
5. Upload Private Key file created in the previous step.
    a. Choose Private Key option **Upload Private Key**.
    b. Choose the Private Key file.
6. Upload certificate files using the same process as in the previous POD.
7. Repeat process for each POD.

Administrative UI Instructions

The following describes how to obtain a certificate from the Certificate Authority, upload the certificate, copy the certificate to another target, and activate the certificate from the Admin UI.

UI Method: Obtaining a Valid SSL Certificate from CA

If a Certificate Signing Request (CSR) has not yet been issued, create one in FortiNAC.

To generate a CSR:

1. Select **System > Settings**
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Generate CSR**.

Figure 1: Generate CSR

5. Select the certificate target.

   Admin UI: Generates CSR for the Administrative User Interface.

   Persistent Agent: Generates CSR for Communications between FortiNAC and the Persistent Agent.

   Portal: Generates a CSR to secure the Captive Portal and Dissolvable Agent communications.

   RADIUS Server: Generates CSR for communications with the integrated FortiNAC RADIUS server set to use 802.1x and PEAP.

   Note: The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the **Details** button and select the **Private Key** tab.

6. Enter the Common Name (Fully-Qualified Host Name). This is the Host Name to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (e.g. *.Fortinetnetworks.com).
7. Enter the remaining information for the certificate in the dialog box.
8. Click **OK** to generate the CSR.

Figure 2: Generated CSR

9. Copy the section with the certificate request to include the following:

   -----BEGIN CERTIFICATE REQUEST-----

   ...Certificate Request Data...

   -----END CERTIFICATE REQUEST-----

10. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC.

    Important: Make sure there are no spaces, characters or carriage returns added to the Certificate Request.

11. Click **OK** to exit the "Certificate Generated" screen.
12. Send the Certificate Request file to the CA to request a Valid SSL Certificate. Note the following before submitting:

- **Not all Certificate Authorities ask for the same information when requesting a certificate.** For example, some CA's ask for a server type (apache, etc) while others do not. If prompted, choose apache. FortiNAC requires a non-encrypted certificate in one of the following formats:

  PEM*

  DER

  PKCS#7

  P7B

  ***Note:** If the certificate will be installed on another system via CLI, choose PEM. Otherwise, the files will need to be converted later on when installing the certificates using CLI (see Appendix section SSL File Conversion Tools).

- **Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature.** However, certificates with SHA2 encryption can be requested using this CSR.
- **Agent versions prior to 3.1.5 are not compatible with SHA2.** Contact Support to verify appropriate SHA version based on current deployment.
- **Do not generate a new CSR for the same target after submitting request to CA.** When a certificate request is generated, a matching private key is stored on the appliance in a temporary location. When the resulting certificate is obtained from the authority and uploaded, the matching private key is then moved into the live certificate configuration location. As such, generating more than one certificate request for a single target will overwrite the previous private key stored in the temporary location with a new private key. Certificates obtained using the initial certificate request would then be invalid as the private key stored in the temporary location would no longer match.

UI Method: Issuing a Self-Signed Certificate

Self-Signed Certificates can be used in the event there are no certificates issued by a third party or internal Certificate Authority that are available.

To generate a Self-Signed Certificate:

1. Select **System > Settings**
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Generate CSR**.
5. Select the certificate target.

   Admin UI: Generates CSR for the Administrative User Interface.

   Persistent Agent: Not recommended when using Self-Signed Certificates.

   Portal: Not recommended when using Self-Signed Certificates.

6. Select Use Result as Self-Signed Certificate
7. Enter the Common Name (Fully-Qualified Host Name). This is the Host Name to be secured by the certificate.
8. Click **OK**.
9. Export the certificate. There are various methods to do this.

Note: Exporting the certificate may not be possible with Internet Explorer.

FireFox:

To export certificate to use for other browsers:

a. Browse to https://<appliance name>:8443

The message "Your connection is not secure" displays.

b. Click the padlock or "i" next to the URL

c. Click the > next to the host name

d. Click **More Information**

e Under the Details tab click the Export button.

f. Save as PEM.

FortiNAC CLI:

a. SSH to the FortiNAC Server or Control Server and type

```
echo -n | openssl s_client -connect <appliance name>:8443 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert
```

Example:

echo -n | openssl s_client -connect qa6-74.Fortinetnetworks.com:8443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert

depth=0 CN = qa6-74.Fortinetnetworks.com

verify error:num=18:self signed certificate

verify return:1

depth=0 CN = qa6-74.Fortinetnetworks.com

verify return:1

DONE

b. ftp or scp file to desired location.

```
ftp <destination ip or name>
scp server.cert root@<location>:/<path>
```

10. Import the certificate to the browser.

FireFox:

a. Browse to https://<appliance name>:8443

The message "Your connection is not secure" displays.

b. Click **Advanced**

c. Click **Add Exception**

d. Click **Confirm Security Exception**

e. Close the browser completely and reopen.

Internet Explorer (IE):

a. Browse to https://<appliance name>:8443

b. Under start menu, in search bar type **certmgr.msc**.

c. Navigate to folder **Trusted Root Certification Authorities\Certificates**.

d. Click **Action > All Tasks > Import**

e. Browse and select the filename of the certificate.

f. Click **Open**

g. Click **Next**

h. Ensure Place all certificates in Certificate store Trusted Root Certification Authorities is selected

i. Click **Next**

j. Click **Finish**

k. When prompted to install certificate, click **Yes**

"The import was successful" should display.

l. Close the browser completely and reopen.

The URL should now display as secure.

UI Method: Upload the Certificate Received from the CA

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.

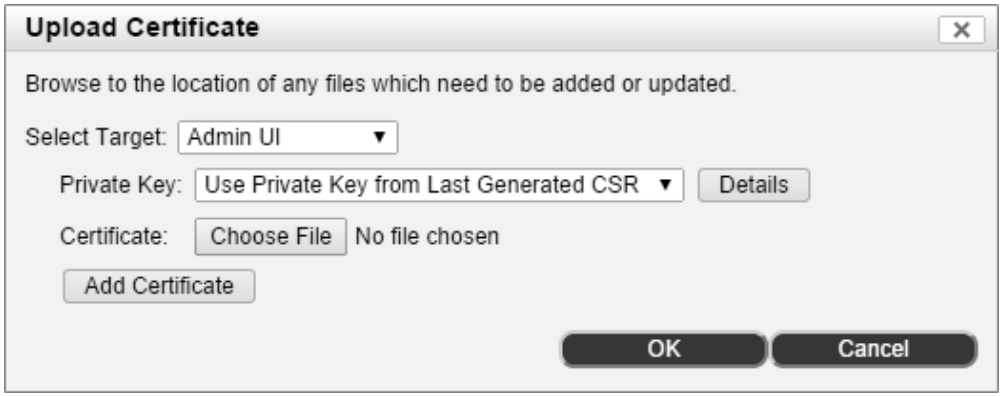

Figure 3: Upload Certificate

1. Save the file(s) received from the CA to your PC.
2. Select **System > Settings**.
3. Expand the **Security folder**.
4. Select **Certificate Management** from the tree.
5. Click **Upload Certificate**.
6. Select the target where the certificate will be uploaded.

   Admin UI: Secures the Administrative User Interface.

   Persistent Agent: Secures the communications between FortiNAC and the Persistent Agent.

   Portal: Secures the captive portal and communications between FortiNAC and the Dissolvable Agent.

   RADIUS Server: Secures communication for integrated FortiNAC RADIUS server set to use 802.1x and PEAP.
7. Do one of the following:
   - Select **Use Private Key from Last Generated CSR** to use the key from the most recent CSR for the selected target.
   - Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
   - Select **Upload Private Key** to upload a key stored outside FortiNAC. Click **Choose** to find and upload the private key.
8. Click the **Choose File** button to find and select the certificate to be uploaded. Users can also upload CA certificates and CA bundles.

Important: Upload any relevant intermediate certificate files needed for the creation of a complete certificate chain of authority. The Certificate Authority should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.

9. Click the **Add Certificate** button if multiple certificates were returned. Use this to enter each additional certificate file.
10. Click **OK**.

Copying a Certificate to Another Target

If the certificate is intended to be used for multiple targets, copy the certificate to the new target:

1. Highlight the target with the desired certificate installed.
2. Click **Copy Certificate**.
3. Select the new target from the drop-down menu.
4. Click **OK**.

UI Method: Activating Certificates

Certificates for the Administrative User Interface and Persistent Agent activate automatically upon installation. No further action is required.

To begin using the certificate when connecting to the Portal, do the following:

1. Navigate to **System** > **Settings**.
2. Expand the **Security** folder, and then click **Portal SSL**.
3. In the **SSL Mode** field, select **Valid SSL Certificate**.
4. Click **Save Settings** (this may take several minutes).

Proceed to Validate.

CLI Instructions

The following describes how to obtain a certificate from the Certificate Authority, upload the certificate, and activate the certificate from the CLI.

CLI Method: (FortiNAC Server)

Applicable models: NS5xxCA/6xxCA/7xxCA

Note: In order to secure the Captive Portal, the certificate files need to be placed in the **/bsc/siteConfiguration/apache_ssl** directory of the FortiNAC Server and must use the file names **server.key**, **server.crt** and **server.ca-bundle**. These files can then be used to secure the Admin UI and Persistent Agent certificate targets using the **ImportCertificateWithKey** command.

Even if the portal will not be used, the files can still be saved in the apache_ssl directory using these names for consistency purposes.

Obtaining a Valid SSL Certificate from a Certificate Authority (CA)

If a Certificate Signing Request (CSR) has not yet been issued, create one in FortiNAC.

1. Log into FortiNAC as `root`.
2. Navigate to **/bsc/siteConfiguration/apache_ssl** and generate the Certificate Request. Type

   ```
   openssl req -newkey rsa:2048 -new -keyout encrypted.key -days 1095 -out certificaterequest.csr
   ```

3. Enter the appropriate information. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (e.g. *.Fortinetnetworks.com).

   Note: A PEM pass phrase must be entered during the creation of the key. Make note of whatever pass phrase is entered, as it will be needed for decrypting the Private Key. In the below example, "Fortinet" was chosen as the PEM pass phrase.

   Example input:

   ```
   Generating a 2048 bit RSA private key
   ........+++
   .....+++
   writing new private key to 'encrypted.key' Enter PEM
   pass phrase: Fortinet
   Verifying - Enter PEM pass phrase: Fortinet
   -----
   You are about to be asked to enter information that will be incorporated into your
   certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN. Th ere are
   quite a few fields but you can leave some blank For some fields there will be a default
   value.
   If you enter '.', the field will be left blank.

   -----
   ```

```
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:New Hampshire Locality
Name (eg, city) [Newbury]:Concord
Organization Name (eg, company) [My Company Ltd]:Fortinet Organizational Unit Name
(eg, section) []:Information Technology
Common Name (eg, your name or your server's hostname) []:svm1-1200.Fortinetnet works.com
Email Address []:.
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Two files are created: the Private Key (encrypted.key) and the Certificate Signing Request (certificaterequest.csr).

4. Decrypt the Private Key using the PEM pass phrase entered in previous step. An unencrypted Private Key is created.

   `openssl rsa -in encrypted.key -out server.key`

5. Enter pass phrase for encrypted.key: `Fortinet`

   "writing RSA key" will display.

6. Type

   `cat server.key`

   The key should have the following format:

   ```
   -----BEGIN RSA PRIVATE KEY-----
   ...Private Key Data...
   -----END RSA PRIVATE KEY-----
   ```

7. Type

   `cat certificaterequest.csr`

   The certificate should have the following format:

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   ...Certificate Request Data...
   -----END CERTIFICATE REQUEST-----
   ```

   The Certificate Request can be viewed with the below command:

   `openssl req -noout -text -in certificaterequest.csr`

8. Submit the certificate request file (certificaterequest.csr) to the CA. If requesting a SAN certificate, provide the FQDN of all appliances to be secured. The amount of time it takes for the CA to respond with the certificate files after CSR submission will vary. Note the following before submitting:

- **Not all Certificate Authorities ask for the same information when requesting a certificate.** For example, some CA's ask for a server type (apache, etc) while others do not. If prompted, choose apache. FortiNAC requires a non-encrypted certificate. Use PEM format.
- **Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature.** However, certificates with SHA2 encryption can be requested using this CSR.
- **Agent versions prior to 3.1.5 are not compatible with SHA2.** Contact Support to verify appropriate SHA version based on current deployment.
- **Do not generate a new CSR for the same target after submitting request to CA.** When a certificate request is generated, a matching private key is stored on the appliance in a temporary location. When the resulting certificate is obtained from the authority and uploaded, the matching private key is then moved into the live certificate configuration location. As such, generating more than one certificate request for a single target will overwrite the previous private key stored in the temporary location with a new private key. Certificates obtained using the initial certificate request would then be invalid as the private key stored in the temporary location would no longer match.

Import and Activate Certificates

After receiving the certificate files from the CA, upload them to FortiNAC. The Certificate Authority will generally return:

- Certificate
- CA bundle containing any intermediate and root certificates to ensure authenticity of the certificate.

The certificate, the key, and bundle (containing only the intermediate and root certificates) must be in separate files.

1. Log into the server as `root`. Copy the certificate files received from the CA to **/bsc/siteConfiguration/apache_ssl**
2. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. Complete the steps in Appendix section Create SSL Certificate Bundle before proceeding.
3. If CSR was not generated in FortiNAC, verify Private Key is in RSA format. Type:

   ```
   cat <filename>
   ```

   Header should look like this: -----BEGIN RSA PRIVATE KEY-----

   If Key Header looks like this: -----BEGIN PRIVATE KEY-----

   The Key is not in the correct format and needs to be converted. Covert the file by running the following command (on a Linux server):

   ```
   openssl rsa -in <old_file_name> -out <new_file>
   ```

   Complete SSL Certificate installation using the newly converted Private Key file.
4. Backup the existing .keystore file. Type

   ```
   cp /bsc/campusMgr/.keystore /bsc/campusMgr/.keystore.bak
   ```
5. Ensure the names of the files are the following:
   key = **server.key**
   certificate = **server.crt**
   bundle = **server.ca-bundle**
6. Import files to the keystore using the appropriate alias for each applicable certificate target.
   Agent alias name: agent
   Portal alias name: portal
   Admin UI alias name: tomcat

   Type

   ```
   ImportCertificateWithKey -alias <port name> -cas server.ca-bundle -key server.key -cert
   server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass ^8Bradford%23
   ```

Example
ImportCertificateWithKey -alias tomcat -cas server.ca-bundle -key server.key -cert server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass ^8Bradford%23

"Successfully imported key and certificate chain" will display.

7. Activate Certificate for each target.

   Admin UI - Restart the tomcat-admin service. In CLI type
   `service tomcat-admin restart`

   Agent - (No action is necessary)

   Captive Portal - Restart apache service via CLI. Type
   `service httpd restart`

Proceed to Validate.

CLI Method: (Control Server / Application Server Pair)

Applicable models: NS1200/2200/8200/9200/1000C/1000A/2000C/2000A

Note: In order to secure the Captive Portal, the certificate files need to be placed in the **/bsc/siteConfiguration/apache_ssl** directory of the FortiNAC Application Server and must use the file names **server.key**, **server.crt** and **server.ca-bundle**. These files can then be used to secure the Persistent Agent certificate target using the **ImportCertificateWithKey** command.

Even if the portal will not be used, the files can still be saved in the apache_ssl directory using these names for consistency purposes.

Obtaining a Valid SSL Certificate from a Certificate Authority (CA)

If a Certificate Signing Request (CSR) has not yet been issued, create one in FortiNAC.

1. Determine what will be secured in FortiNAC. There are three possible certificate targets:

   Admin UI: Secures the Administrative User Interface. To secure the Admin UI, certificates must be installed on the Control Server.

   Persistent Agent: Secures the communications between FortiNAC and the Persistent Agent. To secure this target, certificates must be installed on the Application Server.

   Portal: Secures the captive portal and communications between FortiNAC and the Dissolvable Agent. To secure this target, certificates must be installed on the Application Server.
2. Log into the Control Server as `root`.
3. Navigate to **/bsc/campusMgr** and generate the Certificate Request. Type

   ```
   openssl req -newkey rsa:2048 -new -keyout encrypted.key -days 1095 -out certificaterequest.csr
   ```
4. Enter the appropriate information. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (e.g. *.Fortinetnetworks.com).

   Note: A PEM pass phrase must be entered during the creation of the key. Make note of whatever pass phrase is entered, as it will be needed for decrypting the Private Key. In the below example, "Fortinet" was chosen as the PEM pass phrase.

   Example input:

   ```
   Generating a 2048 bit RSA private key
   ........+++
   .....+++
   writing new private key to 'encrypted.key' Enter PEM
   pass phrase: Fortinet
   Verifying - Enter PEM pass phrase: Fortinet
   -----
   ```

```
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN. Th ere are
quite a few fields but you can leave some blank For some fields there will be a default
value.
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:New Hampshire Locality
Name (eg, city) [Newbury]:Concord
Organization Name (eg, company) [My Company Ltd]:Fortinet Organizational Unit Name
(eg, section) []:Information Technology
Common Name (eg, your name or your server's hostname) []:svm1-1200.Fortinetnet works.com
Email Address []:.
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Two files will be created: the Private Key (encrypted.key) and the Certificate Signing Request (certificaterequest.csr).

5. Decrypt the Private Key using the PEM pass phrase entered in step 4. An unencrypted Private Key will be created.

   openssl rsa -in encrypted.key -out server.key

6. Enter pass phrase for encrypted.key: `Fortinet`

   "writing RSA key" will display.

7. Type

   cat server.key

   The key should have the following format:

   -----BEGIN RSA PRIVATE KEY-----
   ...Private Key Data...
   -----END RSA PRIVATE KEY-----

8. Type

   cat certificaterequest.csr

   The certificate should have the following format:

   -----BEGIN CERTIFICATE REQUEST-----
   ...Certificate Request Data...
   -----END CERTIFICATE REQUEST-----

   The Certificate Request can be viewed with the below command:

   openssl req -noout -text -in certificaterequest.csr

9. Submit the certificate request file (certificaterequest.csr) to the CA. If requesting a SAN

certificate, provide the FQDN of all appliances to be secured. The amount of time it takes for the CA to respond with the certificate files after CSR submission will vary. Note the following before submitting:

- **Not all Certificate Authorities ask for the same information when requesting a certificate.** For example, some CA's ask for a server type (apache, etc) while others do not. If prompted, choose apache. FortiNAC requires a non-encrypted certificate. Use PEM format.
- **Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature.** However, certificates with SHA2 encryption can be requested using this CSR.
- **Agent versions prior to 3.1.5 are not compatible with SHA2.** Contact Support to verify appropriate SHA version based on current deployment.
- **Do not generate a new CSR for the same target after submitting request to CA.** When a certificate request is generated, a matching private key is stored on the appliance in a temporary location. When the resulting certificate is obtained from the authority and uploaded, the matching private key is then moved into the live certificate configuration location. As such, generating more than one certificate request for a single target will overwrite the previous private key stored in the temporary location with a new private key. Certificates obtained using the initial certificate request would then be invalid as the private key stored in the temporary location would no longer match.

Import and Activate Certificates

Once the certificate files are received from the CA, upload them to FortiNAC. The Certificate Authority will generally return:

- Certificate
- CA bundle containing any intermediate and root certificates to ensure authenticity of the certificate.

The certificate, the key, and bundle (containing only the intermediate and root certificates) must be in separate files.

Securing Administrative UI

1. Log into the Control Server as `root`. Copy the certificate files received from the CA to **/bsc/campusMgr**
2. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. Complete the steps in Appendix section Create SSL Certificate Bundle before proceeding.
3. Verify Private Key is in RSA format. Review the private key file using a text editor. Alternatively, if in Linux, the file can be viewed by running the command:

   `cat <filename>`

   Header should look like this: -----BEGIN RSA PRIVATE KEY-----

   If Key Header looks like this: -----BEGIN PRIVATE KEY-----

   The Key is not in the correct format and needs to be converted. Covert the file by running the following command (on a Linux server):

   `openssl rsa -in <old_file_name> -out <new_file>`

   Complete SSL Certificate installation using the newly converted Private Key file.
4. Backup the existing .keystore file. Type
   `cp /bsc/campusMgr/.keystore /bsc/campusMgr/.keystore.bak`
5. Import files to the keystore using the alias "tomcat"

   Type
   `ImportCertificateWithKey -alias tomcat -cas <CA-Bundle> -key <Private-Key> -cert <Leaf-Certificate> -keystore /bsc/campusMgr/.keystore -v -force -import -storepass ^8Bradford%23`

   Example
   `ImportCertificateWithKey -alias tomcat -cas server.ca-bundle -key server.key -cert server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass ^8Bradford%23`

   "Successfully imported key and certificate chain" will display.
6. Activate Certificate by restarting the tomcat-admin service. Type

   `service tomcat-admin restart`

Securing Agent and Captive Portal

1. Log into the Application Server as `root`. Copy the key, leaf certificate and bundle files to **/bsc/siteConfiguration/apache_ssl**
2. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. Complete the steps in Appendix section Create SSL Certificate Bundle before proceeding.

3. Verify Private Key is in RSA format. Review the private key file using a text editor. Alternatively, if in Linux, the file can be viewed by running the command:

   ```
   cat <filename>
   ```

   Header should look like this: -----BEGIN RSA PRIVATE KEY-----

   If Key Header looks like this: -----BEGIN PRIVATE KEY-----

   The Key is not in the correct format and needs to be converted. Covert the file by running the following command (on a Linux server):

   ```
   openssl rsa -in <old_file_name> -out <new_file>
   ```

   Complete SSL Certificate installation using the newly converted Private Key file.

4. Ensure the names of the files are the following:
   key = server.key
   certificate = server.crt
   bundle = server.ca-bundle

5. Backup the existing .keystore file. Type
   ```
   cp /bsc/campusMgr/.keystore /bsc/campusMgr/.keystore.bak
   ```

6. Import files to the keystore using the appropriate alias for each applicable certificate target.
   Agent alias name: agent
   Portal alias name: portal

   Type
   ```
   ImportCertificateWithKey -alias <alias name> -cas server.ca-bundle -key server.key -cert
   server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass ^8Bradford%23
   ```

   Example
   ```
   ImportCertificateWithKey -alias portal -cas server.ca-bundle -key server.key -cert
   server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass ^8Bradford%23
   ```

   "Successfully imported key and certificate chain" will display.

7. Activate Certificate for each target.
   Agent - (No action is necessary)
   Captive Portal - Restart apache service via CLI. Type
   ```
   service httpd restart
   ```

Proceed to Validate.

Validate

- **Administrative UI and Captive Portal**: Verify new certificate is being used by examining the certificate details in the browser (such as the security lock icon or whichever method is offered by that browser). **Important**: ensure the name used in the URL is the one specified in the certificate.

- **Certificate Details**: Login and navigate to **System > Settings > Security > Certificate Management**. Verify certificate details display for each target.

Create Certificate Expiration Warning Alarms

Three events are enabled by default in Network Sentry:

- **Certificate Expiration Warning**: Generated when a certificate is due to expire within 30 days.
- **Certificate Expiration Warning (CRITICAL)**: Generated when a certificate is due to expire within 7 days.
- **Certificate Expired**: Generated when a certificate has expired.

You must create alarms to send emails when these events are generated. To create alarms, do the following:

1. Navigate to **Logs > Event to Alarm Mappings**.
2. Create one alarm for each event with the following settings:

   Select the **Notify Users** setting.

   Select the type of messaging (Email or SMS) and Admin group desired to be notified.

   Set the Trigger Rule to **One Event to One Alarm**.

   For detailed instructions on creating alarms, refer to the Online Help topic **Add or Modify Alarm Mapping.**

Renew a Certificate

SSL Certificates must be renewed periodically or they expire. However, the existing certificate must be used until the new one arrives. Some Certificate Authorities allow managing certificates such that it can be renewed without generating a new request file. In these cases, the private key will remain the same and the new certificate can be imported when it arrives.

Administrative UI Method

1. Save the file(s) received from the CA to your PC.
2. Select the target where the certificate will be uploaded. See Step 6 under **UI Method: Upload the Certificate Received from the CA**.
3. Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. See Step 7 under **UI Method: Upload the Certificate Received from the CA**.
4. Continue with steps 8-10 under to complete the process.
5. Copy certificate to other targets as necessary. See **Copying Certificate to Another Target**.

CLI Method

Follow the applicable instructions using the new files. Use the same Private Key file.
CLI Method: Import and Activate Certificates (FortiNAC Server)
CLI Method: Import and Activate Certificates (Control Server/Application Server Pair)

Troubleshooting Tips

If something is wrong with the uploaded certificate files, FortiNAC will display an error and will not apply the certificate.

Common Causes for Certificate Upload Errors

- The wildcard name (e.g., *.Fortinetnetworks.com) was placed in the **Fully- Qualified Host Name Field** in the Portal SSL view under **System > Settings > Security**. To correct, change the entry to the true Fully-Qualified Host Name and click **Save Settings**.
- There are extra spaces, characters, and/or carriage returns above, below, or within the text body of any of the files.
- The certificate was not generated with the current key and there is mismatch.

  This can happen if the OK button in the Generate CSR screen had been clicked after saving the Certificate Request. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key.

  To confirm the certificate and key match, use the following tool:

  https://www.sslshopper.com/certificate-key-matcher.html

  If the key and certificate do not match, generate a new CSR and submit for a new certificate.

- An error displays indicating the private key is invalid. This can occur if the Private Key is not a RSA Private Key. To confirm, (if the certificate is in PEM format), open the certificate in a text editor. If the content looks something like the following:

  ```
  ----BEGIN PRIVATE KEY----
  ...Private key Data…
  ----END PRIVATE KEY----
  ```

  then the key will need to be converted to a RSA key. Run the following command:

  ```
  openssl rsa -in <old_file_name> -out  <new_file>
  ```

- The following error displays in UI: "Unable to update apache configuration." This can occur if SSH communication is failing (as the appliance establishes a SSH session to restart apache service). If appliance is a pair, verify Control Server can SSH to Application Server. If appliance is a single device, verify appliance can SSH to itself (without being prompted to enter a password).

Note: For additional troubleshooting assistance, contact Support.

Appendix

Create SSL Certificate Bundle

If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle.

1. Confirm the files are in PEM format. When opened in a text editor, the content should look similar to the format:
   -----BEGIN CERTIFICATE1-----
   sajaisjkajfsdvjJV;kjvd;Kjv;Js;FDJVKjv
   -----END CERTIFICTATE1-----

   If the content does not have these types of headers, convert to PEM format first. See Appendix section SSL File Conversion Tools.

2. Append all intermediate files into a single text file (server.ca-bundle).

   a. Determine the order in which the certificates will be listed in the bundle (order is important). This is done by using keytool to review each certificate.

      Use the following command to decode and view the content of each certificate:
      `keytool -v -printcert -file <certificate filename>`

   b. Start with the leaf certificate. Look at the Issuer to determine the certificate to be listed first in the bundle.

      keytool -v -printcert -file server.crt
      Owner: CN=bcm.mydomain.edu, OU=ITS Servers & Apps, O=My Organization,L=Somewhere, ST=NY, C=US
      Issuer: CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US

   c. The first Intermediate Certificate's Owner should match the leaf certificate's Issuer.

      keytool -v -printcert -file InCommonServerCA.pem
      Owner: CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US
      Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE

   d. The next Intermediate Certificate's Owner should match the first Intermediate certificate's Issuer. In this case it is the Root certificate (which will always be listed last).

      keytool -v -printcert -file AddTrustUTNSGCCA.pem
      Owner: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
      Issuer: CN=UTN - DATACorp SGC, OU=http://www.usertrust.com, O=The

USERTRUST Network, L=Salt Lake City, ST=UT, C=US

e. Create a new text file (bundle.crt) and append the certificate files in order.

   Example of importing the text content of each intermediate and root certificate (in the appropriate order) into a new bundle called server.ca-bundle:
   cat InCommonServerCA.pem >> server.ca-bundle
   cat AddTrustUTNSGCCA.pem >> server.ca-bundle

f. View the bundle and ensure there are no spaces between the start and end of each file.

   ```
   cat server.ca-bundle
   ```

   Example Bundle content:
   -----BEGIN CERTIFICATE1-----
   sajaisjkajfsdvjJV;kjvd;Kjv;Js;FDJVKjv
   -----END CERTIFICTATE1-----
   -----BEGIN CERTIFICATE2----
   sajdjsaskdjfkjdskvjsadvkjBDSVKBkdjv
   -----END CERTIFCATE2-----

3. Proceed to Import Certificates.

Create Keystore for SSL/TLS Communications for LDAP

If you choose to use SSL or TLS security protocols for communications with your LDAP directory, you must have a security certificate. You must obtain a valid certificate from a Certificate Authority. That certificate must be saved to a specific directory on your FortiNACappliance.

SSL or TLS protocols are selected on the Directory Configuration window when you set up the connection to your LDAP directory. See Add/Modify Directory - Connection Tab for information on configuring the connection to your LDAP directory. Follow the steps below to import your certificate.

Note: You should be logged in as root to follow this procedure.

1. When you have received your certificate from the Certificate Authority, copy the file to the `/bsc/campusMgr/` directory on your Network Sentry server.
2. Use the keytool command to import the certificate into a keystore file.

   For example, if your certificate file is named MainCertificate.der, you would type the following:

   ```
   keytool -import -trustcacerts -alias <MyLDAP> -file
   MainCertificate.der -keystore .keystore
   ```

   Note: Depending on the file extension of your certificate file, you may need to modify the command shown above. For additional information on using the keytool key and certificate management tool go to the Sun web site java.sun.com.
3. When the script responds with the **Trust this certificate?** prompt, type **Yes** and press **Enter**.
4. At the prompt for the keystore password, type in the following password and press **Enter**:

   `^8Bradford%23`
5. To view the certificate, navigate to the `/bsc/campusMgr/` directory and type the following:

   `keytool -list -v -keystore .keystore`
6. Type the password used to import the certificate and press **Enter**.

Note: The keystore is cached on startup. Therefore, it is recommended that you restart FortiNAC after making any changes to the keystore.

Modify Web.xml To Prevent Use of Port 8080

To ensure that users connect to the Admin UI using a secure port you must modify the web.xml file.

Note: This procedure is no longer necessary as of FortiNAC version 8.2.

Important: This change must be made after each upgrade because the web.xml is overwritten during the upgrade. A README should be put in place as a reminder to follow this procedure upon upgrade.

1. Use vi or another editor to open the following file in a text editor:
   `/bsc/campusMgr/ui/ROOT/WEB-INF/web.xml`
2. Locate the security-constraint for ALL.
3. Change the transport-guarantee to CONFIDENTIAL. This value matches the API security-constraint.
4. Save the changes to the file.

SSL File Conversion Tools

Convert **DER/Binary** to **PEM** Format:
```
openssl x509 -inform der -in <filename> -out <newfilename>
```

Example converting certificate.cer:
```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Convert **P7B/PKCS#7** to **PEM** Format:
```
openssl pkcs7 -print_certs -in <filename> -out <newfilename>
```

Example converting certificate.p7b:
```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer
```

Convert **PFX/PKCS#12** to **PEM** Format:
```
openssl pkcs12 -in <filename> -out <newfilename> –nodes
```

Example converting certificate.pfx:
```
openssl pkcs12 -in certificate.pfx -out certificate.cer –nodes
```