

Importing SSL Certificates to NAC Profiler

Document ID: 107726

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Main Task: Install the Certificate

- Two Options
- Option 1: Use OpenSSL Toolkit on Beacon/NPS to Generate Sign
- Option 2: Generate/Submit CSR to Internal/External CA

Verify

Troubleshoot

Related Information

Introduction

The Profiler system web-based UI can use digital certificates so that the authenticity of the embedded web server on the Cisco NAC Profiler Server can be verified by the browser as it connects for access to the Profiler user interface served by HTTPS. The system leverages one of the most common applications of PKI and digital certificates where the web browser validates that an SSL web server is authentic so that the user feels secure that their interaction with the web server is, in fact, trusted and their communications with it secure. This is the same mechanism that is used today to secure e-commerce and other secure communications with web sites of many types that use SSL.

The Profiler system ships with a "self-signed" digital certificate that allows access to the UI but without verification of the onboard SSL web server as trusted. Until the default certificate is replaced with one created with environment-specific attributes, such as the server name, and is signed by a Certificate Authority (CA), web browsers that access the Profiler UI display a warning similar to this example, which indicate that the browser does not recognize the CA that issued the certificate and is unable verify it as a trusted site.



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- NAC Server

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Main Task: Install the Certificate

Most browsers require the user to provide additional input to continue the connection, which can be bothersome.

In order to fully utilize the increased security afforded by the use of digital certificates for SSL security of the Profiler interface, changes to the SSL subsystem configuration of the NPS must be made. Those changes require the replacement of the private key and digital certificate that are used by the system by default with those issued by a trusted Certificate Authority and that are specific to the installation. After this procedure, the browser initiates a HTTPS session with the Server and takes the user immediately to the UI login process to bypass the certificate warnings.

Two Options

There are two alternatives for this on the NPS systems:

1. Utilize the OpenSSL toolkit resident on the appliance to generate a signed certificate that can be installed on the NPS Server system and the PCs used to manage the system through the Web UI.

This option can be used in environments that do not currently have an internal CA and choose not to rely on the commercial CA providers that charge a fee to provide a signed digital certificate that is recognized by most commercial browsers automatically.

2. Use the OpenSSL toolkit to generate a Certificate Signing Request for the NPS system that is submitted to either an internal or external commercial CA service, which returns a ready-to-use, signed digital certificate for use on the system.

It is typically a matter of the internal security policy of the organization in which the Profiler system is installed to make the determination of which option to use in a specific environment. Detailed instructions for both options are provided in the remainder of this document.

Option 1: Use OpenSSL Toolkit on Beacon/NPS to Generate Sign

Prior to beginning the procedure outlined, it is important to verify that the Profiler system is properly configured to utilize the enterprise name service, and that a DNS entry is made such that the system has a fully qualified domain name (FQDN). In order to verify that this is the case, ensure that you are able to open a UI session with the Profiler system with the FQDN of the system (that is, <https://beacon.bspruce.com/beacon>) instead of the IP address (or VIP in the case of HA systems) in the URL when you browse to the UI.

This procedure is used in cases when it is not desired to submit the CSR to an off-appliance CA for signing. This procedure allows for the creation of a signed certificate with the OpenSSL toolkit on the appliance exclusively – nothing needs to be submitted to another system or commercial CA to generate a signed certificate for the Profiler system.

The success of this procedure is dependent upon following it as specified. The command syntax is long and prone to errors. Ensure that you are in the correct directory as specified in the instructions before you execute the commands. Information for the DNs generated for the CA Certificate and Certificate Signing Request, such as country, state, city, server name, etc., must be entered identically (case sensitive), so be sure to make notes as you complete the steps to ensure that the process goes smoothly.

1. Initiate an SSH or console session to the NPS appliance and elevate to root access. For HA systems, ensure that you are on the Primary system by initiating an SSH to the VIP.

Prior to using OpenSSL for the first time, some file structure utilized by OpenSSL must be initialized. Complete these steps to initialize OpenSSL:

2. Change the directory to /etc/pki/CA with this command:

```
cd /etc/pki/CA/
```

Create a new directory called **newcerts**, and issue these commands:

```
mkdir newcerts touch index.txt
```

3. Use vi to create a new file named **serial**; insert **01** in the file, and commit the changes. (:wq!)

Change this directory:

```
cd /etc/pki/tls/certs
```

4. Generate a new private key for the system with this command:

```
openssl genrsa -out profilerFQDN.key 1024
```

(where 'profilerFQDN' is replaced with the Fully Qualified Domain Name of the NPS appliance when deployed standalone. For HA systems, the FQDN of the VIP must be used).

If the Profiler system is not in DNS, the IP address of the server (VIP) can be used instead of the FQDN, but the certificate is tied to this IP address, which requires the use of the IP in the URL (that is, https://10.10.0.1/profiler) to avoid the certificate warnings.

5. Generate a CA certificate to use to generate the Server certificate with this command, which creates a 3 year CA certificate, and the key generated in step #4:

```
openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem
```

You are prompted for several attributes that are incorporated into the certificate request and the formation of a Distinguished Name (DN) for the CA certificate. For some of these items, a default value is suggested (in []). Enter the desired value for each parameter of the DN or '.' In order to skip the item, be sure to make a note of the DN parameters used in this step. They must be identical to those specified in the generation of the Certificate Signing Request for the Server certificate in step #7.

Move the CA certificate created in the last step to the required directory:

```
mv cacert.pem /etc/pki/CA
```

Generate a Certificate Signing Request for the Profiler system with the new private key:

```
openssl req -new -key profilerFQDN.key -out profilerFQDN.csr
```

6. Just as in step #5, you are prompted to complete a DN for the system for the Server CSR. Ensure that you use the same values for the Server CSR that were used for the CA Certificate in step #5. If there are any variations in the parameters, the CSR is not created successfully. In addition, you are prompted to create a passphrase for the certificate. Be sure to make a note of the passphrase.
7. Generate the Server certificate with the CSR and private key generated in the previous steps. The output of this step is the signed certificate that is installed on the Profiler Server (or servers, in the case of HA pairs).

```
openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key
```

You are prompted to sign and commit the certificate. Enter **y** to confirm signing and committing the certificate to complete the server certificate generation.

8. Move the certificate file to the location specified by the internal security policy (if applicable) or use the default locations:

The certificates must be placed in `/etc/pki/tls/certs/` if no location is specified by internal security policy.

```
mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
```

9. Move the private key file to the location specified by the internal security policy (if applicable) or use the default locations:

The private key must be placed in `/etc/pki/tls/private/` if no location is specified by internal security policy. Use the command:

```
mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
```

10. Edit the **ssl.conf** file with an editor such as `vi` to make necessary changes to force the Profiler web server to use the new private key and certificate (`ssl.conf` is found in `/etc/httpd/conf.d/`).
 - a. In **ssl.conf**, the Server Certificate portion begins on line 107. Change the `SSLCertificateFile` configuration item from the factory default (`/etc/pki/tls/certs/localhost.cert`) to point to the new certificate file that was created on the system in step #8.
 - b. In **ssl.conf**, the Server Private Key portion begins on line 114. Change the `Server Private Key` configuration item from the factory default (`etc/pki/tls/private/localhost.key`) to point to the new private key file placed on the system in step #9.

11. Restart the Apache web server on the appliance with this command:

```
apachectl -k restart
```

Note: If the system is deployed standalone, skip to step #13.

12. For HA NPS systems only, complete these steps to install the private key and CRT on the other member (current Secondary) of the HA pair. This ensures that, regardless of which appliance is Primary in the pair, the SSL security mechanisms for the UI operate identically.

- a. a. Copy the private key generated on the Primary appliance in step #3 to the Secondary appliance. The private key must be placed in `/etc/pki/tls/private/` if no location is specified by the internal security policy. Use this command (from the `/etc/pki/tls/private` directory on Primary):

```
scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
```

- b. Copy the signed CRT that was returned from the CA from the Primary to the Secondary appliance. The certificates must be placed in `/etc/pki/tls/certs/` if no location is specified by the internal security policy.

```
scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
```

- c. SSH to the Secondary appliance and edit its **ssl.conf** file with an editor such as vi to make necessary changes to force the web server on the Secondary to use the new private key and certificate (ssl.conf is found in /etc/httpd/conf.d/)

- a. In **ssl.conf**, the Server Certificate portion begins on line 107. Change the SSLCertificateFile configuration item from the factory default (/etc/pki/tls/certs/localhost.crt) to point to the new certificate file placed on the system in step #11b.
- b. In **ssl.conf**, the Server Private Key portion begins on line 114. Change the Server Private Key configuration item from the factory default (etc/pki/tls/private/localhost.key) to point to the new private key file placed on the system in step #11a.
- d. Restart the Apache web server on the Secondary appliance with this command:

```
apachectl -k restart
```

Because the Server certificate that was created with these steps utilized a private CA, the browsers that access the Profiler UI have to be configured to install the certificate in the Trusted Root Certificate Authority repository on Windows PCs with IE 7.0. Follow these steps:

- a. Copy the created Server Certificate to the /home/beacon directory of the appliance:

```
cp profilerFQDN.crt /home/beacon
```

- b. Use WinSCP or a comparable software to SCP the .crt file from the appliance to the PC.
 - c. Double-click the **.crt file** to start the Windows certificate manager, and click **Install Certificate**, which starts the Certificate Import Wizard.
 - d. Choose the **Radio** button. Place all the certificates in this store to activate the **Browse** button.
 - e. Choose **Browse**, and click the **Trusted Root Certification Authorities** certificate store.
 - f. Click **OK** to accept this certificate.
 - g. Repeat this process on the other PCs that are used to manage the Profiler system.
13. Access the Profiler UI and note that the HTTPS session starts with no the certificate warnings generated by the browser.

Option 2: Generate/Submit CSR to Internal/External CA

Before you begin the procedure outlined next, it is important to verify that the Profiler system is properly configured to utilize the enterprise name service, and that a DNS entry is made such that the system has a fully qualified domain name (FQDN). In order to verify that this is the case, ensure that you are able to open a UI session with the Profiler system with the FQDN of the system (that is, <https://beacon.bspruce.com/beacon>) instead of the IP address or VIP in the case of HA systems.

Complete these steps to generate a new private key for the system, generate a CSR for submission to an internal or external CA, and then place the valid signed certificate on a NPS:

1. Initiate an SSH or console session to the NPS appliance, and elevate it to root access. For HA systems, initiate SSH to the VIP to ensure that you are on the Primary system.
2. Go to the default PKI directory for NPS:

```
cd /etc/pki/tls
```

3. Use this command to generate a new private key file for the system:

```
openssl genrsa ?des3 ?out profilerFQDN.key 1024
```

Where 'profilerFQDN' is replaced with the fully qualified domain name of the NPS appliance when deployed standalone. For HA systems, the FQDN of the VIP must be used). You are prompted to enter and confirm a passphrase to complete the generation of the private key. This passphrase is required for future operations using the private key. Be sure to make note of the passphrase used for private key generation.

4. With the private key generated in the last step, generate a Certificate Signing Request (CSR) that is sent to the Certificate Authority (CA) for generation of the Certificate (CRT) for this system.

Use this command to generate the CSR

```
openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr
```

(Substitute the fully qualified domain name of the system for 'profilerFQDN'.)

- a. You are prompted for the passphrase for the private key when you create the CSR for the system; enter it to proceed.
 - b. You are then prompted for several attributes that are incorporated into the certificate request and the formation of a Distinguished Name (DN). For some of these items, a default value is suggested (in []). Enter the desired value for each parameter of the DN or '.' to skip the item.
5. Verify the contents of the CSR with this command:

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

(Substitute the fully qualified domain name of the system for 'profilerFQDN'.) This returns information about the CSR and the DN that were entered in the last step. If any information in the CSR needs to be changed, repeat step #4 in its entirety

6. Submit the CSR to the chosen Certificate Authority (CA) in accordance with the internal policies. If the request is successful, the CA sends back an identity certificate that has been digitally signed with the CA's private key. When this new CRT signed by your chosen CA is used to replace the factory default CRT on the Profiler system, any browser that accesses the Profiler UI is able to verify the identity of the site, and the warning messages in the browser seen upon connection to the web server on the NPS server are no longer displayed prior to user authentication for as long as the CRT remains valid. (This assumes that the browser has had the CA added to its Trusted Root Certificate Authorities.)
7. Dependent upon the CA that is used, additional information possibly needs to be submitted along with the CSR, such as other credentials or proofs of identity required by the certificate authority, and the certificate authority can contact the applicant for further information.

Once the digitally signed CRT comes back from the CA, proceed with next step to replace the factory private key and certificate with those created in the steps above. For HA systems, the same procedure is used to install the private key and certificate on the Secondary appliance in the pair, as well.

8. Move the certificate and private key file to the location specified by the internal security policy, if applicable, or use the default locations:
 - a. The private key must be placed in /etc/pki/tls/private/ if no location is specified by internal security policy. Use this command:

```
mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
```

- b. The certificates must be placed in `/etc/pki/tls/certs/` if no location is specified by internal security policy.

```
mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
```

9. Edit the **ssl.conf** file with an editor such as **vi** to make necessary changes to force the web server to use the new private key and certificate (`ssl.conf` is found in `/etc/httpd/conf.d/`).

- a. In **ssl.conf**, the Server Certificate portion begins on line 107. Change the `SSLCertificateFile` configuration item from the factory default (`/etc/pki/tls/certs/localhost.crt`) to point to the new certificate file placed on the system in step #8.b.
- b. In **ssl.conf**, the Server Private Key portion begins on line 114. Change the Server Private Key configuration item from the factory default (`etc/pki/tls/private/localhost.key`) to point to the new private key file placed on the system in step #8.a.

10. Restart the Apache web server on the appliance with this command:

```
apachectl -k restart
```

Note: If the system is deployed standalone, skip to step #12.

11. For HA NPS systems only, complete these steps to install the private key and CRT on the other member (current Secondary) of the HA pair. This ensures that, regardless of which appliance is Primary in the pair, the SSL security mechanisms for the UI operate identically.

- a. Copy the private key generated on the Primary appliance in step #3 to the Secondary appliance. The private key must be placed in `/etc/pki/tls/private/` if no location is specified by internal security policy. Use this command (from the `/etc/pki/tls/private` directory on Primary):

```
scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
```

- b. . Copy the signed CRT returned from the CA from the Primary to the Secondary appliance. The certificates must be placed in `/etc/pki/tls/certs/` if no location is specified by internal security policy.

```
scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
```

- c. SSH to the Secondary appliance and edit its `ssl.conf` file with an editor such as **vi** to make necessary changes to force the web server on the Secondary to use the new private key and certificate (`ssl.conf` is found in `/etc/httpd/conf.d/`).

- a. In **ssl.conf**, the Server Certificate portion begins on line 107. Change the `SSLCertificateFile` configuration item from the factory default (`/etc/pki/tls/certs/localhost.crt`) to point to the new certificate file placed on the system in step #11.b.
- b. In **ssl.conf**, the Server Private Key portion begins on line 114. Change the Server Private Key configuration item from the factory default (`etc/pki/tls/private/localhost.key`) to point to the new private key file placed on the system in step #11.a.

- d. Restart the Apache web server on the Secondary appliance with this command:

```
apachectl -k restart
```

12. Access the Profiler UI and note that the HTTPS session starts without the certificate warnings generated by the browser. If the warning persists, verify that the browser used has the issuing CA added to its Trusted Root Certificate Authorities.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco NAC Appliance \(Clean Access\) Product Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 02, 2008

Document ID: 107726
