Creating and Installing SSL Certificates
(for Stealthwatch System v6.10)
Copyrights and Trademarks

© 2017 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>1</td>
</tr>
<tr>
<td>Creating Certificates</td>
<td>2</td>
</tr>
<tr>
<td>Creating a Private Key</td>
<td>2</td>
</tr>
<tr>
<td>Creating a Certificate Signing Request</td>
<td>2</td>
</tr>
<tr>
<td>Creating a Certificate Chain</td>
<td>4</td>
</tr>
<tr>
<td>Installing Certificates</td>
<td>5</td>
</tr>
<tr>
<td>Verification</td>
<td>7</td>
</tr>
</tbody>
</table>
Introduction

This document provides the procedures for creating and installing third party or internal verified certificates to your Stealthwatch System.

Note: The Stealthwatch system only supports certificates in PEM format and encrypted with RSA.

Audience

The primary audience for this guide includes administrators responsible for configuring the Stealthwatch System.

Before You Begin

Before creating and installing the certificates, you should do the following:

- Check that your Stealthwatch system is communicating by following these steps:
- Go to the SMC client interface. Check the Alarm Table to make sure there are no active Management Channel Down or Failover Channel Down alarms.
- Go to the SMC client interface. Open the Flow Collector Dashboard. Check that all three sections of the dashboard have data.
- Check that you have the proper Stealthwatch licenses.

Note: For additional information, see the Stealthwatch Certificates Troubleshooting Guide.
Creating Certificates

Creating a Private Key

To create a private key for each appliance (Stealthwatch Management Console, Flow Sensor, Flow Collector, UDP Director), complete the following steps:

1. Access the terminal emulator window for the appliance and enter the appliance IP address.
2. Log in as the root user.
3. To navigate to a temp folder, type the following command:
   ```
   cd /lancope/var/admin/tmp
   ```
4. To generate a private key, type the following command:
   ```
   openssl genrsa -des3 -out server.key 4096
   ```
5. Type a password and press Enter.
   Note: Type in a phrase that is long with multiple classes of characters, but that you can remember (you’ll have to type it at least twice). For password guidelines, see the National Institute of Standards and Technology Digital Identity Guidelines.
6. To decrypt the private key, type the following commands:
   ```
   cp server.key server.key.org
   openssl rsa -in server.key.org -out server_smcl.key
   ```
   Note: The key can be downloaded from this link: https://SMC_IP/smc/files/admin/tmp. You can also decrypt the key after you get the certificate back from the Certificate Authority, after step 6 in the next section.

Creating a Certificate Signing Request

To make a Certificate Signing Request (CSR) with OpenSSL for each appliance, complete the following steps:

Note: You will have several server certificates once you have completed this section. The following image shows an example of the created certificates:
1. Access the terminal emulator window for the appliance and enter the appliance IP address.
2. Log in as the root user.
3. To navigate to a temp folder, type the following command:
   \texttt{cd /lancope/var/admin/tmp}
4. To generate a CSR, type the following command:
   \texttt{openssl req -new -key server_smcl.key -out server_smcl.csr}
5. Enter the required information (sample answers in bold). For additional information, see the \textit{Stealthwatch Certificates Troubleshooting Guide}.
   \begin{itemize}
   \item \textbf{Country Name (2 letter code)} [GB]: \textbf{US}
   \item \textbf{State or Province Name (full name)} [Berkshire]: \textbf{Georgia}
   \item \textbf{Locality Name (eg, city)} [Newbury]: \textbf{Atlanta}
   \item \textbf{Organization Name (eg, company)} [My Company Ltd]: \textbf{Your Company Inc}
   \item \textbf{Organizational Unit Name (eg, section)} []: \textbf{Information Technology}
   \item \textbf{Common Name (eg, your name or your server's hostname)} []: \textbf{server_mysmc1.company.com}
   \item \textbf{Email Address} []: \textbf{john.doe@email.com}
   \end{itemize}
   Please enter the following 'extra' attributes to be sent with your certificate request:
   \begin{itemize}
   \item A challenge password []:
   \item An optional company name []:
   \end{itemize}

\textbf{CAUTION!} Do not have any certificates with duplicate names. The common name must be unique. We recommend you use the Fully Qualified Domain Name.
6. Send the CSR, \texttt{server_smcl.csr}, to a Certificate Authority, such as VeriSign or GoDaddy, or an internal CA to create the endpoint certificate.
   \begin{enumerate}
   \item a. Request the Certificate Authority provide you with TLS Enhanced Values and PEM format when creating the endpoint certificate.
      \begin{enumerate}
      \item \textbf{TLS Web Server Authentication} (1.3.6.1.5.5.7.3.1)
      \item \textbf{TLS Web Client Authentication} (1.3.6.1.5.5.7.3.2)
      \end{enumerate}
   \item b. Follow the instructions the CA provides.
   \end{enumerate}
Creating a Certificate Chain

To create a certificate chain from a third party certificate, complete the following steps:

**Note:** You will need the whole chain when uploading the SSL endpoint certificate. It will look like the inverse of the certification path, with the Root CA last. The following is an example of the chain:

```
Intermediate certificate
--Begin----
<chain>
--End-----
```

```
Secondary CA Certificate
--Begin----
<chain>
--End-----
```

```
Root CA
--Begin----
<chain>
--End-----
```

1. Extract the certificate zip file received from the third party.
2. Follow the next steps to export the certificates on Windows:

**Note:** We recommend using a Windows VM to export the certificates instead of Mac OS/X.

   a. Open the certificate in your operating system’s certificate viewer.
   b. Click **Certification Path**. Choose your Issuing/Secondary/Intermediate CA, and then click **View Certificate**.
   c. The certificate will pop-up as a new window. Click **Details**, and then click **Copy To File**.
   d. Run through the export wizard, using X.509 as the export type.

**Note:** You will have to do this for every step in the certificate path, including the Root CA. When you are on the last step of the path, **View Certificate** will be greyed out.

3. Use a text editor to make the chain certificate look like the example above.
Installing Certificates

To install the certificates, complete the following steps:

**CAUTION!** We recommend you do this at a maintenance window because this will break communications between your Stealthwatch appliances. Communications will not be restored until you complete all of the steps.

1. Install the root Certificate Authority (CA) certificate that was exported previously and the endpoint certificate, with the chain, on each appliance by following these steps:
   a. Log in as an admin user to the Appliance Admin interface for the appliance where you are applying the certificate.
   b. From the main menu, select **Configuration > Certificate Authority Certificates**.
   c. Click **Choose File** or **Browse**, and select the certificate.
   d. In the Name field, type a name to identify the certificate. **Note:** The suggested name is the host name of the appliance on which the certificate will be installed. Valid characters are alphanumeric, dash (-), underscore (_), and dot (.). Do not use spaces or any other special characters.
   e. Click **Add Certificate**.
   f. Click **Submit**.

2. Install the individual Secure Socket Layer (SSL) Server certificates and keys on each appliance by following these steps:
   a. Log in as admin user to the Appliance Admin interface for the appliance where you are applying the SSL certificate.
   b. From the main menu, select **Configuration > SSL Certificate**.
   c. In the “SSL Server Identity” section, in the Target Certificate File (PEM-encoded) field, click **Choose File** or **Browse** to access the file that contains the endpoint certificate for the appliance.
   d. In the “Certificate Chain (PEM-encoded) (Optional)” field, add the chain created in the last section of the previous chapter. **Note:** The certificate chain is only optional if you are using a self-signed certificate.
   e. In the “Private Key (Not Encrypted) (PEM-encoded)” field, click **Choose File** or **Browse** to access the location of the private key file, `server_smcl.key`, for the appliance.
   f. Click **Upload Certificate** to upload and apply the certificates from the provided fields to the appliance.
3. Reboot the appliance.

4. Import the endpoint certificate to the Java Runtime Environment’s (JRE) cacerts file on every computer that is using the SMC client interface by following these steps:
   a. Open a command prompt as an administrator.
   b. Change the directory to your Java Home Bin folder.

   **Note:** Install the endpoint certificate to the version of Java that you are using. Your path may be different from the following examples.

   i. Example path on Windows:
      ```
      cd C:\Program Files (x86)\Java\jre1.8.0_101\bin
      ```
   ii. Example path on Mac OS/X:
      ```
      cd /System/Library/Internet Plug Ins/JavaAppletPlugin.plugin/Home/bin
      ```

   c. Type the following command to import the endpoint certificate into the trust store:
      i. Command on Windows:
         ```
         .\keytool -import -alias <alias> -keystore ..\lib\security\cacerts -file <path to cert>
         ```
      ii. Command on Mac OS/X:
         ```
         sudo keytool -import -alias <alias> -keystore ..\lib\security\cacerts -file <path to cert>
         ```

   d. Type the keystore password.

   **Note:** The default keystore password is changeit.

   e. Type `yes` to trust the certificate.

5. Install the endpoint certificate to every computer’s operating system certificate store/keychain that connects to Stealthwatch. Refer to your Operating System’s Help.
Verification

To verify your certificates are working properly, complete the following steps:

**Note:** This section is optional, but highly recommended.

1. Log in to the SMC Web App. Click the padlock on your browser and view the certificate. Verify that it is using the endpoint certificate and not the default Lancope certificate.
2. Go to the SMC client interface. Check the Alarm Table to make sure there are no active Management Channel Down or Failover Channel Down alarms.
3. Go to the SMC client interface. Open the Flow Collector Dashboard. Check that all three sections of the dashboard have data. If not, there is likely an issue with the certificates setup. The following image is an example of the dashboard:

![Dashboard Example](image-url)