# Verasys Smart Building Hub Network and IT Guidance

Technical Bulletin

LC-SBH100-0

Issued January 2017

Refer to the [QuickLIT website](#) for the most up-to-date version of this document.

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Concepts</td>
<td>3</td>
</tr>
<tr>
<td>Chain of Trust</td>
<td>3</td>
</tr>
<tr>
<td>Self-Signed Certificates and Certificates Signed by a Public Certificate Authority</td>
<td>3</td>
</tr>
<tr>
<td>Public and Private Keys</td>
<td>3</td>
</tr>
<tr>
<td>Man-in-the-Middle Attack</td>
<td>4</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>4</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>4</td>
</tr>
<tr>
<td>Domain Name System (DNS)</td>
<td>4</td>
</tr>
<tr>
<td>Steps</td>
<td>4</td>
</tr>
<tr>
<td>Connecting to Smart Building Hub the First Time</td>
<td>4</td>
</tr>
<tr>
<td>Connecting the Smart Building Hub to Ethernet</td>
<td>5</td>
</tr>
<tr>
<td>Certificate Workflow</td>
<td>6</td>
</tr>
<tr>
<td>Generating a Private Key</td>
<td>7</td>
</tr>
<tr>
<td>Implementing SSL for Smart Building Hub</td>
<td>9</td>
</tr>
<tr>
<td>Creating a Self-Signed Certificate</td>
<td>10</td>
</tr>
<tr>
<td>Uninstalling a Certificate on a Client that Has Connected to the Smart Building Hub</td>
<td>15</td>
</tr>
<tr>
<td>Uninstalling the Security Certificate on iOS® Platforms</td>
<td>15</td>
</tr>
<tr>
<td>Uninstalling the Security Certificate in the Windows® Internet Explorer® Web Browser</td>
<td>15</td>
</tr>
<tr>
<td>Uninstalling a Certificate in Google Chrome</td>
<td>19</td>
</tr>
<tr>
<td>Adding a Private Key and Certificate to Smart Building Hub</td>
<td>22</td>
</tr>
<tr>
<td>Installing a Security Certificate on a Client That is Connected to Smart Building Hub</td>
<td>24</td>
</tr>
<tr>
<td>Installing the Security Certificate in Internet Explorer</td>
<td>24</td>
</tr>
<tr>
<td>Installing the Security Certificate in Google Chrome</td>
<td>31</td>
</tr>
<tr>
<td>Importing a Certificate Signed by a Public CA</td>
<td>36</td>
</tr>
</tbody>
</table>
Creating a Certificate Request ................................................................. 40
Creating a Certificate Request (CSR) ....................................................... 40
Purchasing an SSL Certificate from a Public Authority ......................... 43
Verasys Smart Building Hub Network and IT Guidance Technical Bulletin

Introduction
This document contains important information about connecting a Verasys™ Smart Building Hub to your network. From an IT perspective, a system device such as a Smart Building Hub is simply a node on the network. However, Smart Building Hub uses communication protocols, security methods, and other technologies that you should consider carefully.

**IMPORTANT:** Engage appropriate network security professionals to ensure that the certificates are handled. Typically, the IT organization must approve configurations that expose networks to the Internet. Be sure to fully read and understand IT compliance documentation for your site. Use care when performing steps on system components because restarts may be required that conflict with compliance requirements. For example, upgrading firmware or installing new SSL certificates may require the computer to be offline for a period of time.

Concepts
This section describes IT concepts as they are used when working with Smart Building Hub.

Chain of Trust
A chain of trust is designed to allow multiple users to create and use software on the system, which would be more difficult if all the keys were stored directly in hardware. It starts with warnings from the Smart Building Hub UI when you attempt to use it without the software being digitally signed. The signing authority only signs boot programs that enforce security, such as running only programs that are themselves signed, or allowing only signed code to have access to certain features of the machine. This process may continue for several layers.

Self-Signed Certificates and Certificates Signed by a Public Certificate Authority
A self-signed certificate is a certificate that is signed by the same entity that it certifies. This term does not refer to the identity of the person or organization that actually performed the signing procedure. A self-signed certificate is a certificate signed with its own private key, that is, the entity signing the certificate is also the entity that created the certificate.

Smart Building Hub is shipped with a default Verasys™ self-signed certificate that provides secure communication. Only one certificate can be installed on Smart Building Hub at a time. You will overwrite the existing certificate when you install a new certificate. Smart Building Hub can be run on your network with a self-signed certificate.

However, if you need to expose the Smart Building Hub UI on a public network and have browsers that indicate a trusted site, you must get a signed certificate matching your domain name. You can acquire a valid signed certificate from your IT department or purchase it from a Public Certificate Authority (CA) using a certificate signing request (CSR). A certificate signed by a CA is used to establish a secure connection between your browser and the Smart Building Hub.

Public and Private Keys
Public and private keys are used to verify that the entity requesting access to a system is who or what it claims to be.
**Man-in-the-Middle Attack**

This is a type of security breach where a person injects themselves between the user and the entity the user is trying to communicate with on the network. The person then has the ability to intercept and read traffic or send false information on to the destination. To guard against this type of attack, we strongly recommend that you use an Ethernet crossover cable to directly connect Smart Building Hub to your computer when transferring keys to the device. This setup creates a network of two and makes a man-in-the-middle attack improbable.

**IP Addresses**

An IP address uniquely identifies devices on a TCP/IP network. An IP address can be private for use on a LAN or public for use on the internet or a WAN.

**Dynamic Host Configuration Protocol (DHCP)**

DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a device is plugged into a different location on the network. DHCP can also assign dial-up users an IP address automatically when they connect to the network. Some DHCP servers can support fixed addresses for devices that need a static IP address.

The Smart Building Hub can obtain its IP address and other network information using DHCP. Each device that can connect to the Ethernet network needs a unique IP address. Without DHCP, the IP address must be entered manually for each device; and, if the devices are moved to another subnet on the network, you must enter a new IP address. The Smart Building Hub supports both dynamic and static IP address assignments.

**Domain Name System (DNS)**

DNS is the Internet standard for naming host devices and mapping host domain names to IP addresses. A DNS server is a computer registered to join the Domain Name System. A domain name is a meaningful and easy-to-remember handle for an Internet address. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts to ensure that they are unique.

**Steps**

**Connecting to Smart Building Hub the First Time**

1. Connect the RS-485 port of the Smart Building Hub to the field bus port of the equipment controller using the supplied RJ-12 cable or field bus adapter. The Smart Building Hub's LEDs flash, indicating that the device is initializing. When the Fault LED turns off and the Wi-Fi LEDs flash in succession, the Smart Building Hub is ready to use.

2. In the Wi-Fi settings of your device or laptop, connect to the Smart Building Hub Wi-Fi network using your default credentials. These credentials are included on a sticker in the Quick Start Guide (Part No. 24-10737-121) that came with your device.

3. Direct your browser to www.smartbuildinghub.com to open the Smart Building Hub browser interface.

**IMPORTANT:** If you are going to use the Smart Building Hub on Ethernet, you must plug it into external power before you attach the field bus adapter.
Note: Smart Building Hub ships with a private Smartbuildinghub.com SSL certificate installed to ensure secure communication with the Smartbuildinghub.com. However, this certificate does not indicate that it is trusted in a browser. If you wish to install your own certificate, refer to Adding a Private Key and Certificate to Smart Building Hub. Use your default Admin login credentials that are also included on a sticker in the Quick Start Guide (Part No. 24-10737-121) that came with your device.

4. Read and accept the Smart Building Hub license agreement.

5. The first time you log in to the Smart Building Hub, the Change Password and Passphrase web page appears. You must change the Admin password and Wi-Fi passphrase.

   IMPORTANT: After you change the Wi-Fi passphrase or SSID the webserver restarts and you must rejoin the Smart Building Hub Wi-Fi network using the new passphrase. On some mobile devices you must select and “forget” the original Smart Building Hub Wi-Fi network before rejoining the network with the new passphrase.

   Note: Replace the Wi-Fi Passphrase in the New Wi-Fi Passphrase field and click Save.

You may now use your Smart Building Hub through Wi-Fi. If you are connecting your Smart Building Hub to an Ethernet network, continue to Connecting the Smart Building Hub to Ethernet.

Connecting the Smart Building Hub to Ethernet

These instructions are for additional settings that are required when connecting the Smart Building Hub to an Ethernet network. These settings occur after the steps in Connecting to Smart Building Hub the First Time.

   IMPORTANT: When using the Smart Building Hub on Ethernet, you must plug it into external power before you attach the field bus adapter.

1. In the Smart Building Hub UI, navigate to Settings > Ethernet.

2. In the Ethernet drop-down list, select On to enable the SBH Ethernet port.

3. Click Save on the bottom of the screen.

   By default, the Smart Building Hub is configured to dynamically receive an IP address from your network using DHCP. Take note of the address that automatically appears in the IP Address field.

4. Enter the IP address from Step 3 into your browser address bar to access the Smart Building Hub over your Ethernet network.

You can use static or manual settings rather than automatic settings with your Smart Building Hub. However, if you do so, you must contact your IT department for all necessary manual settings to ensure that your Smart Building Hub works on your company’s network.

   To use your Smart Building Hub with a static IP Address:

   Configure your own static IP address parameters by setting Auto DHCP Configure to Off under Settings > Ethernet. Obtain necessary network settings from your IT department.

   To use your Smart Building Hub with a DNS:

   If you have a Dynamic Name Server on your network, the Smart Building Hub can be accessed by a unique name instead of using an IP address. To enable DNS, set the Auto DNS Configure setting to On under Settings > Ethernet.
**Certificate Workflow**

The following flowchart gives a general overview of how to create and install certificates on Smart Building Hub. This process covers how to generate self-signed certificates and keys in addition to how to create a request for a certificate signed by a public certificate authority to install on the Smart Building Hub device. The instructions for how to install and uninstall these certificates to establish trust between the Smart Building Hub and the browser you are using varies by the browser type.

![Certificate Workflow Flowchart](image)

**Figure 1: Certificate Workflow**
Generating a Private Key

This procedure describes how to generate a new private key. **Note that you may be required to first create an encrypted database.** The password for this encrypted database is used to encrypt the private key and must be protected. The screen shots used to illustrate key generation were made with the XCA - X Certificate and key management application, copyright 2015 by Christian Hohnstädt. However, you must be sure to use a key generation tool that your IT department recommends or approves.

1. Open your key generating software and click **New Key**.

2. Name the new key. Select a Keytype of **RSA** and a Keysize of **2048 bit** from the respective drop-down lists. Click **Create**.
3. The new key appears in your list of Private Keys. Select the private key you created and select **Export**.

**Figure 4: New Key Created**

4. Export the private key for your device in PEM format. Click **OK** to save to a location where you can access the file to place into your Smart Building Hub. This is the file you use when **Adding a Private Key and Certificate to Smart Building Hub**.

**Figure 5: Export Private Key**
Implementing SSL for Smart Building Hub

To implement third-party or self-signed SSL certificates for Smart Building Hub, follow the steps included in this document.

The options for SSL certificates include the following:

- Third-Party – Coordinate with the local IT department before installing the Smart Building Hub. Follow the instructions included in the Installing a Security Certificate on a Client That is Connected to Smart Building Hub section. If you need to create a request for a certificate signed by a public CA, see the Creating a Certificate Request (CSR).
- Self-Signed – Follow the installation process that allows you to generate a self-signed certificate in the Creating a Self-Signed Certificate section.

Note: We do not recommend a self-signed SSL certificate for networks exposed directly to the Internet (no firewall or VPN).

You must have Port 80 (TCP) and Port 443 (SSL) open on the computer that is connected to the Smart Building Hub.
Creating a Self-Signed Certificate

The following steps demonstrate how to create a self-signed certificate using the XCA - X Certificate and key management application, copyright 2015 by Christian Hohnstädt, as an example of how to perform this task. You must make sure to use a certificate-generating application that is approved by your IT department. This procedure creates a file in a format for submitting the properties of your SSL certificate to the certificate authority.

1. Open your certificate creating-application, select the Certificates tab if necessary, and click **New Certificate**. The Create Certificate screen appears.

![Create x509 Certificate](image)

**Figure 6: New Certificate**
2. Accept the defaults unless they conflict with your IT policies and select the Subject Tab.

![Figure 7: Create the Certificate](image)

3. In the Distinguished name properties window, enter the following information:
   - Internal name: This name is only used internally and does not appear in the certificate.
   - organizationName: the name of your organization
   - countryName: the country in which your organization is located
   - organizationalUnitName: the name of your department within the organization
   - stateOrProvinceName: the state in which your organization is located
   - commonName: the domain name without https://. The domain name should be the site used to browse to the Smart Building Hub UI.
   - localityName: the city in which your organization is located
   - emailAddress: typically, the address of the administrator of your organization.
   - Private key: This drop-down list contains private keys that you have already generated. In this case, select Verasys Smart Building Hub (RSA: 2048 bit), which was generated in the Generating a Private Key section of this document. If you have not created a private key or wish to create a new one, click Generate a new key and follow the steps in Generating a Private Key in this document.
Figure 8: Subject Tab Properties
4. Select the Extensions tab.

![Figure 9: Extensions Tab Properties](image)

5. Use the Validity and Time range sections to define time limits and valid ranges for your certificate. Click **OK**. The new certificate is now in your list of certificates with the internal name you assigned.
6. Select the certificate and click **Export**.

![Figure 10: New Certificate Created](image)

7. Choose an export format of PEM and click **OK** to save the file to a location where you can access the file to place into your Smart Building Hub. This is the file you use when *Adding a Private Key and Certificate to Smart Building Hub*.

![Figure 11: New Certificate Export](image)

8. Click **OK**.
Uninstalling a Certificate on a Client that Has Connected to the Smart Building Hub

If you are removing or replacing a Smart Building Hub and wish to uninstall the certificate from your computer, follow the procedures in this section that are appropriate for your operating system. Note that you do not need to uninstall the certificate because a new certificate overwrites existing certificates on Smart Building Hub.

Uninstalling the Security Certificate on iOS® Platforms

To remove the Smart Building Hub security certificate on an iOS platform, navigate to Settings > General > Profiles, select the Smartbuildinghub.com certificate, and then tap Remove twice.

Uninstalling the Security Certificate in the Windows® Internet Explorer® Web Browser

1. On the Tools menu, click Internet options.

Figure 12: Internet Options Selection
2. In the Internet Properties dialog box, click the **Content** tab, and then click **Certificates**.

   ![Figure 13: Internet Properties Content Tab](image)

3. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab, select the **Smart Building Hub authority**, and then click **Remove**. A Certificates warning appears.

   ![Figure 14: Certificates](image)
4. In the Certificates warning dialog box, click Yes. A Root Certificate Store warning appears.

**Figure 15: Certificates Warning**

![Certificates Warning](image)

5. In the Root Certificate Store warning dialog box, click Yes. You return to the Trusted Root Certification Authorities tab of the Certificates dialog box.

**Figure 16: Root Certificate Store Warning Dialog**

![Root Certificate Store Warning](image)
6. In the Certificates dialog box, click **Close**, and then click **OK**.

**Figure 17: Trusted Root Certification Authorities Tab**
Uninstalling a Certificate in Google Chrome

1. Click the **Customize and control Google Chrome** button and select **Settings**.

   ![Google Chrome Customize and Control Google Chrome Menu](image)

2. Scroll down to the bottom of the pane and select **Show advanced settings**.

   ![Advanced Settings](image)

3. Scroll to the HTTPS/SSL section and click **Manage certificates**.

   ![HTTPS/SSL](image)
4. Select the **Trusted Root Certification Authorities** tab.

**Figure 21: Trusted Root Certificate Authority Tab**

5. Select the Smart Building Hub authority, and then click **Remove**. A Certificates warning appears.

**Figure 22: Certificates Warning**
6. Click **Yes**. The certificate is removed immediately.

**Figure 23: Certificate Removal Warning**
**Adding a Private Key and Certificate to Smart Building Hub**

This process describes how to add the private key and certificate to your Smart Building Hub.

**Note:** To prevent the possibility of a man-in-the-middle attack, we strongly recommend that you use an Ethernet crossover cable to directly connect the Smart Building Hub to your computer when transferring keys to the Smart Building Hub.

1. Connect to Smart Building Hub through an Ethernet crossover cable. The direct connection helps prevent man-in-the-middle type attacks when adding security keys and certificates.

2. Log in to your Smart Building Hub UI by opening your web browser and entering www.smartbuildinghub.com. You must be logged in as an administrator to perform these tasks.

   **Note:** If your computer does not connect to the Smart Building Hub UI, disconnect any other network connections, LAN or wireless, and try again. If your computer is connected to another network, it might not redirect to the Smart Building Hub UI when you enter www.smartbuildinghub.com.

3. Click **Settings** and select **SSL**.

   ![Figure 24: Smart Building Hub SSL Screen](image)

4. Navigate to the location of the private key file (**.pem**) that you created for your site. Right-click the file and select **Open with**, and then select **Notepad**.

5. Select all the text and copy the entire file. Paste this file as a plain text file in the Private Key box of your Smart Building Hub SSL settings Private Key box.

---

Verasys Smart Building Hub Network and IT Guidance Technical Bulletin

22
6. Navigate to the location of the security certificate (***.crt) that you created for your site. Right-click the file and select **Open with**, then select **Notepad**.

7. Copy the entire file. Paste this file as a plain text file in the New Certificate box of your Smart Building Hub SSL settings Private Key box and click **Save**. A reset warning screen appears.

8. To apply the new certificate and private key, the Smart Building Hub web server must restart. Click **OK**. The fault light flashes (for 5 seconds), and then turns off (the rest of the lights continue to function normally). The Smart Building Hub goes offline while restarting and displays the Device Resetting Screen.

**Figure 25: Reset Warning Screen**

**Figure 26: Device Resetting Screen**

**Note:** When an SSL key or certificate is very corrupted, the SSL page detects it and alerts you to the corrupted key or certificate.

However, if the corruption is minor, for example an extra space was copied while installing the certificate or a character was missed, the UI does not detect the problem and allows the corrupted key or certificate to be saved. The server detects the error and returns the Error Saving SSL Settings message. While this properly prevents the bad key or certificate from being used, it does not inform you as to the source of the problem.

In this case, you need to recopy and reinstall the SSL Key or Certificate.

9. When the connection is reestablished, log in to Smart Building Hub and use normally.
Installing a Security Certificate on a Client That is Connected to Smart Building Hub

Until the security certificate for the Smart Building Hub is added as a trusted certificate, you receive a security alert every time you visit the www.smartbuildinghub.com website. How you install the certificate differs based on the web browser and device platform.

Installing the Security Certificate in Internet Explorer

1. Navigate to www.smartbuildinghub.com/download tlsprofile, and then download the rootCA.pem file.
2. On the Tools menu, click Internet options then select the Content tab.

Figure 27: Internet Options Selection
3. In the **Internet Properties** dialog box, click the **Content** tab, and then click **Certificates**.

Figure 28: Internet Properties Content Tab
4. Select the **Trusted Root Certification Authorities** tab.

   **Figure 29: Trusted Root Certification Authorities Tab**

   ![Figure 29: Trusted Root Certification Authorities Tab](image)

5. Click **Import**. The Certificate Import Wizard opens.

   **Figure 30: Certificate Import Wizard**

   ![Figure 30: Certificate Import Wizard](image)
6. In the **Certificate Import Wizard** dialog box, click **Next**.

   **Figure 31: Certificate Import Wizard - Select File to Import**

   ![Certificate Import Wizard - Select File to Import](image)

   *Note: More than one certificate can be stored in a single file in the following formats:
   - Personal Information Exchange- PKCS #12 (.PFX, .P12)
   - Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
   - Microsoft Serialazed Certificate Store (.SST)*

   Learn more about [certificate file formats](#)

   ![Certificate Import Wizard - Select File to Import](image)

6. Browse to the rootCA.pem security certificate file, select it, click **Open**, and then click **Next**.

   **Figure 32: Selecting the rootCA.pem Security Certificate File**

   ![Selecting the rootCA.pem Security Certificate File](image)

   *Note: More than one certificate can be stored in a single file in the following formats:
   - Personal Information Exchange- PKCS #12 (.PFX, .P12)
   - Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
   - Microsoft Serialazed Certificate Store (.SST)*

   ![Selecting the rootCA.pem Security Certificate File](image)

   *Note: More than one certificate can be stored in a single file in the following formats:
   - Personal Information Exchange- PKCS #12 (.PFX, .P12)
   - Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
   - Microsoft Serialazed Certificate Store (.SST)*

   ![Selecting the rootCA.pem Security Certificate File](image)

   Learn more about [certificate file formats](#)

   ![Selecting the rootCA.pem Security Certificate File](image)

7. **Note:** Install the **rootCA.pem** file and not the www.smartbuildinghub.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any Smart Building Hub you use. If you install the www.smartbuildinghub.com file that the browser prompts you to install instead, you need to add a new certificate for each new Smart Building Hub device that you use.
8. On the **Certificate Store** page of the Wizard, select **Place all certificates in the following store**, verify that the certificate store listed is Trusted Root Certification Authorities, and then click **Next**.

**Figure 33: Certificate Import Wizard Certification Store**

![Certificate Import Wizard Certification Store](image)

Figure 34: Certificate Import Wizard Security Warning
10. In the Security Warning dialog box, click **Yes**.

   **Figure 35: Certificate Import Wizard Security Warning**

   ![Certificate Import Wizard Security Warning](image)

11. A success message appears.

   **Figure 36: Wizard Complete**

   ![Wizard Complete](image)

12. Click **OK**. The Wizard closes.
Installing the Security Certificate in Google Chrome

1. Navigate to www.smartbuildinghub.com/downloadtlsprofile, and then download the rootCA.pem file.
2. On the Chrome menu, click **Settings**.

   ![Figure 37: Chrome Settings Menu](image)

3. At the bottom of the Settings page, click **Show advanced settings**.

   ![Figure 38: Advanced Settings Selection](image)

4. Under HTTPS/SSL, click **Manage certificates**.

   ![Figure 39: Manage Certificates](image)
5. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab, and then click **Import**. The Certificate Import Wizard opens.

**Figure 40: Chrome SSL Certificates**

6. In the **Certificate Import Wizard** dialog box, click **Next**.

**Figure 41: Certificate Import Wizard**
7. Browse to the rootCA.pem security certificate file, select it, click **Open**, and then click **Next**.

**Note:** Install the rootCA.pem file and not the www.smartbuildinghub.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any Smart Building Hub you use. If you install the www.smartbuildinghub.com file that the browser prompts you to install instead, you need to add a new certificate for each new Smart Building Hub device that you use.

**Figure 42: Certificate Import Wizard Browse**
8. On the Certificate Store page of the Wizard, select **Place all certificates in the following store**, verify that the certificate store listed is Trusted Root Certification Authorities, and then click **Next**.

   **Figure 43: Certificate Import Wizard Certification Store**

9. The Completing the Certificate page of the Import Wizard appears. Click **Finish**.

   **Figure 44: Certificate Import Wizard Security Warning**
10. In the Security Warning dialog box, click Yes.

   Figure 45: Certificate Import Wizard Security Warning

11. A success message appears.

   Figure 46: Wizard Complete

12. Click OK. The Wizard closes.
**Importing a Certificate Signed by a Public CA**

If you have a certificate from a public CA, you may import it using this procedure.

1. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab, and then click **Import**. The Certificate Import Wizard opens.

2. In the Certificate Import Wizard dialog box, click **Next**.

---

**Figure 47: Chrome SSL Certificates**

**Figure 48: Certificate Import Wizard**
3. Browse to the rootCA.pem security certificate file, select it, click **Open**, and then click **Next**.

**Note:** Install the rootCA.pem file and not the www.smartbuildinghub.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any Smart Building Hub you use. If you install the www.smartbuildinghub.com file that the browser prompts you to install instead, you need to add a new certificate for each new Smart Building Hub device that you use.

**Figure 49: Certificate Import Wizard Browse**

4. On the Certificate Store page of the Wizard, select **Place all certificates in the following store**, verify that the certificate store listed is Trusted Root Certification Authorities, and then click **Next**.

**Figure 50: Certificate Import Wizard Certification Store**

**Figure 51: Certificate Import Wizard Security Warning**

6. In the Security Warning dialog box, click Yes.

**Figure 52: Certificate Import Wizard Security Warning**
7. A success message appears.

8. Click **OK**. The Wizard closes.

![Figure 53: Wizard Complete](image-url)
Creating a Certificate Request

This section describes how to create a certificate signing request as well as how to purchase an SSL certificate from a Public Certificate Authority. You must coordinate with your IT department and only use an approved Public Certificate Authority for your location.

- The steps to purchase a domain name and a security certificate vary according to the registrar. Use the instructions in this document as an example. You may choose a different registrar to purchase a domain name and security certificate.
- The domain name and security certificate costs are not included as part of the purchase cost of the Smart Building Hub.
- Domain names and third-party security certificates expire. We recommend registering domain names and third-party certificates for the longest duration available (typically 3 years). Plan to renew domain names and security certificates before they expire.

Creating a Certificate Request (CSR)

The following steps demonstrate how to create a request for an SSL certificate (CSR) using the XCA - X Certificate and key management application, copyright 2015 by Christian Hohnstädt, as an example of how to perform this task. You must make sure to use a certificate request generating application that is approved by your IT department. This procedure creates a file in a format for submitting the properties of your SSL certificate to the certificate authority. Your IT department must also approve the Public Certificate Authority to which you submit your request.

1. Open your certificate request creating application, select the Certificate signing requests tab if necessary, and click New Request. The Create Certificate signing request screen appears.

![Figure 54: New Certificate Signing Request Tab](image-url)
2. In Signing request, enter unstructuredName and challengePassword. The unstructured name is used by the certificate signing authority and may be set to your organization name. Click the Subject tab.

3. In the Distinguished Name Properties window, enter the following information:
   - Internal name: This name is only used internally and does not appear in the certificate.
   - organizationName: the name of your organization
   - countryName: the country in which your organization is located
   - organizationalUnitName: the name of your department within the organization
   - stateOrProvinceName: the state in which your organization is located
   - commonName: the domain name without https://. The domain name should be the site used to browse to the Smart Building Hub UI.
   - localityName: the city in which your organization is located
   - emailAddress: Typically the address of the administrator of your organization.
   - Private key: This drop-down list contains private keys that you have already generated. In this case, select Verasys Smart Building Hub 1 (RSA:2048 bit) which was generated in the Generating a Private Key section of this document. If you have not created a private key or wish to create a new one, click Generate a new key and follow the steps in Generating a Private Key in this document.

4. Select the Extensions tab.
5. The new certificate signing request is now in your list of certificates with the internal name you assigned. Select the certificate and click **Export**.

   **Figure 56: New CSR Created**

6. Click the browse button, choose a location for the new CSR file, and click **OK**. This file will be used to purchase a certificate request from a Public Certificate Authority.

   **Figure 57: Certificate Request Export**
Purchasing an SSL Certificate from a Public Authority

You can obtain an SSL certificate from any public certificate authority. Smart Building Hub requires a basic Class 1 SSL certificate, also called a domain verified certificate. This section includes instructions using the vendor https://www.namecheap.com/. This vendor is a popular reseller of SSL certificates from several of the largest certificate authorities, including GeoTrust, Inc. The RapidSSL product from GeoTrust, Inc. is used as an example in this document. You can use any public certificate authority to purchase an SSL certificate.

1. In a web browser, browse to https://www.namecheap.com/
   **Note:** The steps to purchase a security certificate vary according to the registrar. Use these instructions as an example.
2. Navigate to the SSL certificate products.
3. Choose the RapidSSL option used in these instructions and select the longest duration available for the certificate. Click **Add to Cart**.
4. The Order Confirmation page appears. Click **Confirm Order**.
5. You are prompted to create an account with https://www.namecheap.com/. If you already have an account, log in. If you do not have an account, enter your account information and click Create Account and Continue.
6. The Order Review page appears. Review your order and select your payment option. Complete your purchase.
7. The SSL certificate purchase is complete. Click Manage My Account to view your purchased certificate.
8. On your Manage My Account page, a message appears alerting you to activate your SSL certificate. Click SSL Certificates page.
9. In the Status column, click **Activate Now**.
10. The Digital Certificate Order Form page appears. From the Select web server drop-down list, select Apache + ApacheSSL.
11. On your computer, navigate to the location where you stored the Certificate request in **Creating a Certificate Request (CSR)**. Select all of the text from the .txt file and paste the text into the Enter csr field on the Digital Certificate Order Form page.
12. Click **Next**.
13. Select the approver email address to verify ownership of the domain name. You must be able to access the mailbox of the email address selected. An email containing a validation code is sent to this email address. Click **Next**.
14. A confirmation page appears. Confirm the administrator contact information is correct. Click **Submit Order**.
15. The Digital Certificate Order Process Summary appears. Wait for the email to approve the certificate. Go to **Importing a Certificate Signed by a Public CA** to complete the process.