Mobile Access Portal Gateway Network and IT Guidance
Technical Guide
S1-YK-MAP1810-0P S1-YK-MAP1810-0S Software Release 3.0

Purchasing an SSL Certificate from a Public Certificate Authority 44Document

Introduction

This document contains important information about connecting a Mobile Access Portal Gateway (MAP Gateway) to your network. From an IT perspective, a system device such as a MAP Gateway is simply a node on the network. However, MAP Gateway 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 securely.

Network security is an important issue. 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 be offline for a period of time.

Concepts

This section describes IT concepts as they are used when working with MAP Gateway.

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 MAP Gateway 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 only running programs that are themselves signed, or only allowing signed code to have access to certain features of the machine. This process may continue for several layers.

Self-Signed and Root Certificates

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.

MAP Gateway is shipped with a default Johnson Controls® self signed certificate. Only one certificate can be installed on MAP Gateway at a time. You must delete or overwrite the existing certificate when you install a new certificate. MAP Gateway can be run on your network with a self-signed certificate.

However, if you want to expose the MAP Gateway UI on a public network, 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 using a certificate signing request (CSR). A certificate signed by a Public Certificate Authority is considered a root certificate because there is not a higher authority for it to be certified by.

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 MAP Gateway 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 Local Area Network (LAN) or public for use on the internet or a Wide Area Network (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 MAP Gateway 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 MAP Gateway 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 MAP Gateway the First Time

IMPORTANT - If you are going to use the MAP Gateway on Ethernet, you must plug it into external power before you attach the field bus adapter.

The following instructions are based on the information in the Quick Start Guide (Part No. 24-10737-16), which comes with each individual MAP Gateway. The default login credentials for each MAP Gateway are included in the Quick Start Guide that ships with each device.

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

2. In the Wi-Fi settings of your device or laptop, connect to the MAP Gateway Wi-Fi network using your default credentials. These credentials are included on a sticker in the Quick Start Guide that came with your device.

3. Direct your browser to www.mapgwy.com to open the MAP Gateway browser interface.

4. Use your default Admin login credentials that are also included on a sticker in the Quick Start Guide that came with your device.

5. Read and accept the MAP Gateway license agreement.

6. The first time you log in to the MAP Gateway you must change the default Admin password and Wi-Fi passphrase.

    a. a.Enter a new Admin password to replace the default password from Step 4. You must confirm the Admin password change by entering the new password twice.

b. Enter a new Wi-Fi pass-phrase to replace the dafault pass-phrase from Step 2.

You may now use your MAP Gateway through Wi-Fi. If you are connecting your MAP Gateway to an Ethernet network, continue to *Connecting the MAP Gateway to Ethernet*.

Connecting the MAP Gateway to Ethernet

These instructions are for additional settings required when connecting the MAP Gateway to an Ethernet network. These settings occur after the steps in *Connecting to MAP Gateway the First Time*.

IMPORTANT - When using the MAP Gateway on Ethernet, you must plug it into external power before you attach the field bus adapter.

1. In the MAP Gateway UI, navigate to Settings > Ethernet.
2. In the Ethernet drop-down list, select **On** to enable the MAP Ethernet port.
3. Click **Save** on the bottom of the screen.
4. By default, the MAP Gateway 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.
5. Enter only this IP address directly into your browser address bar to access the MAP Gateway over your Ethernet network.

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

To use your MAP Gateway 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 MAP Gateway with a DNS:

If you have a Dynamic Name Server on your network, the MAP Gateway 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 Work-flow

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

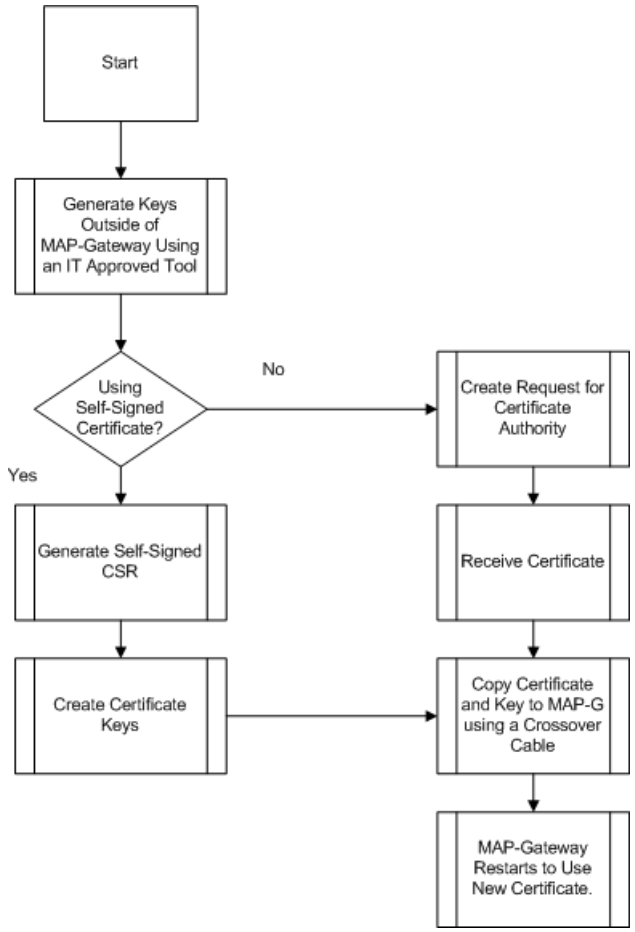


Figure 1: Certificate Work-flow

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 2014 by Christian Hohnstädt. However, you must be sure to use a key generation tool that your IT department recommends or approves.

Table 1: Generating a Private Key

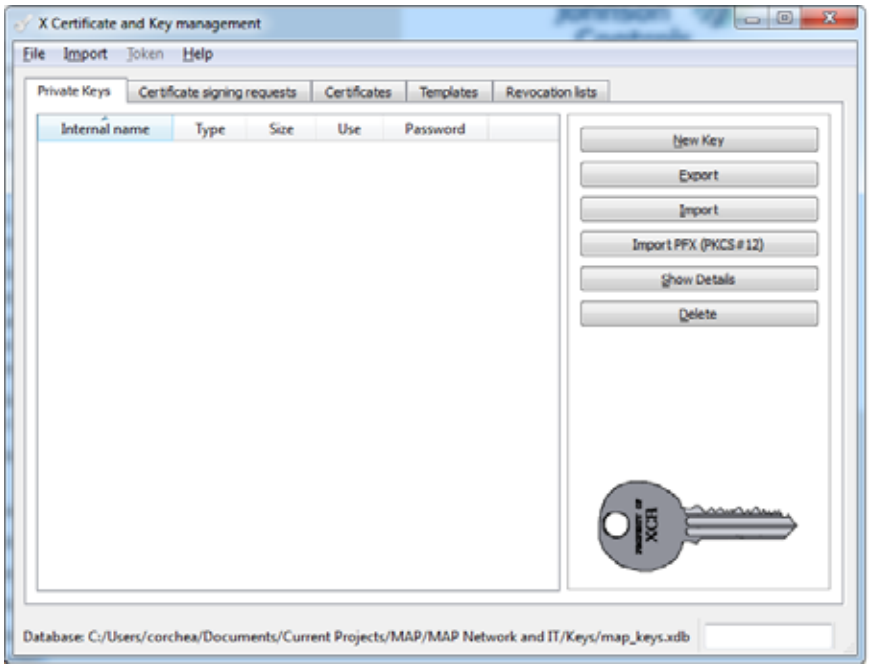
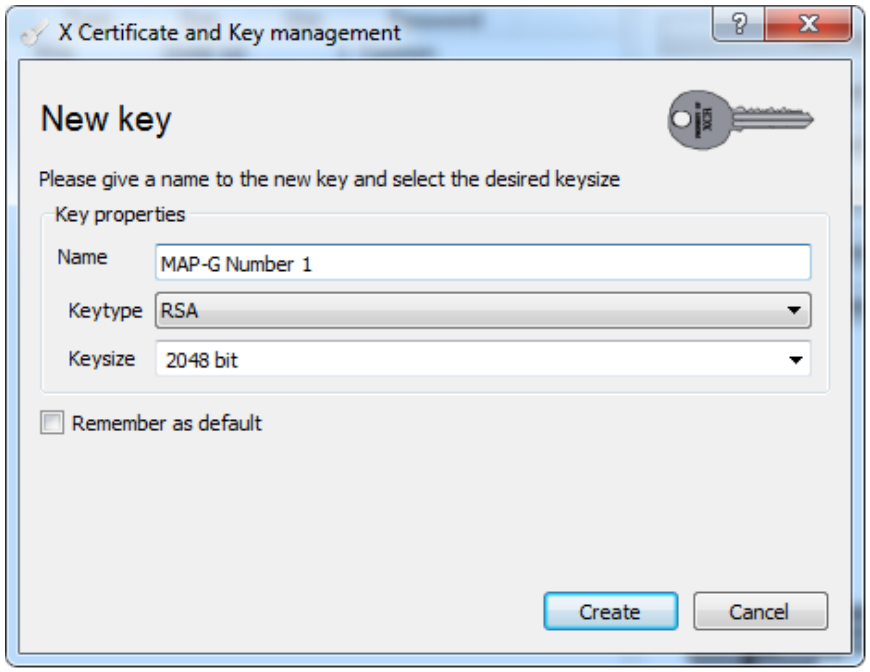
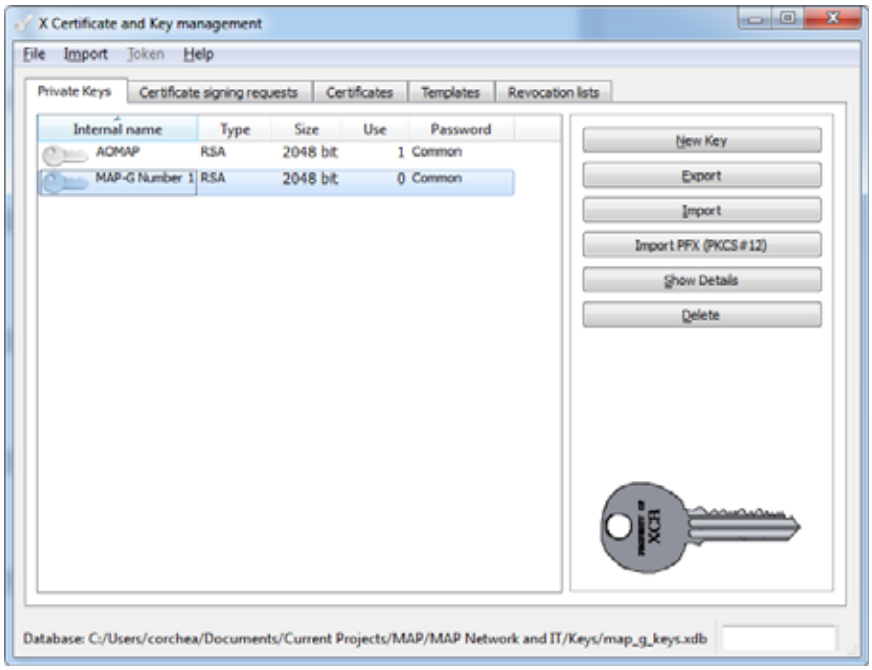
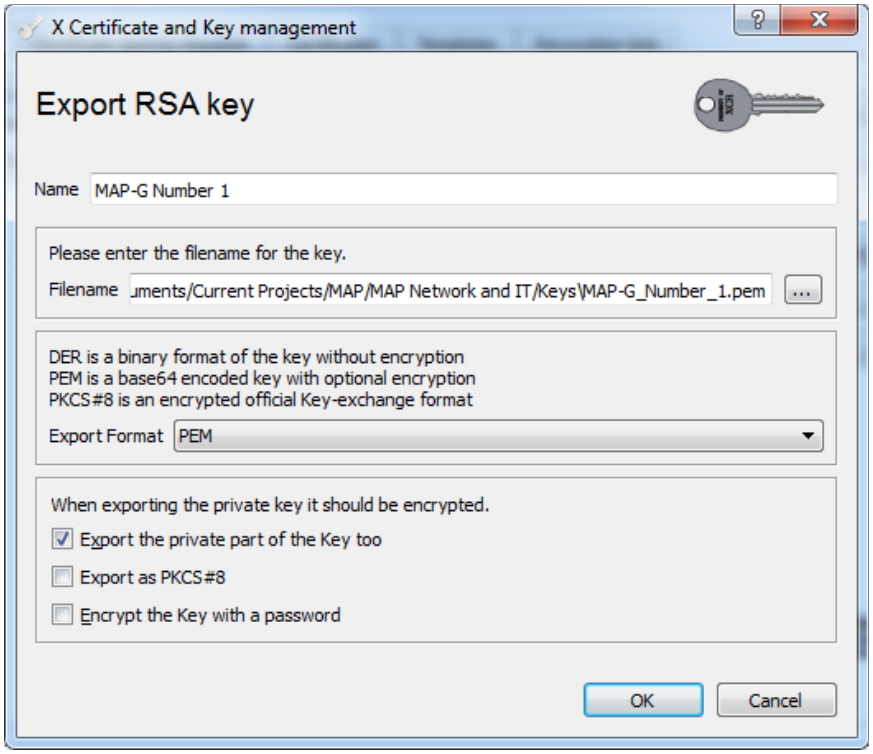
1.	**Figure 2: Key Generating Software** 	Open your key generating software and click **New Key**.
2.	**Figure 3: New Key Screen** 	Name the new key. Select a Keytype of RSA and a Key-size of 2048 bit from the respective drop-down lists. Click Create.

Table 1: Generating a Private Key (Continued)

3.	**Figure 4: New Key Created** 	The new key appears in your list of Private Keys. Select the private key you created and select Export.
4.	**Figure 5: Export Private Key** 	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 MAP Gateway. This is the file you use when *Adding a Private Key and Certificate to MAP Gateway.*

Implementing SSL for MAP Gateway

To implement third-party or self-signed SSL certificates for MAP Gateway, 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 MAP Gateway. Follow the instructions included in the *Installing the Root Certificate on a Client That is Connecting to MAP Gateway* section. If you need to create a request for a root certificate from a third party, see the *Creating a Certificate Request (CSR)* section.
- 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 MAP Gateway.

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 2014 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.

Table 2: Creating a Self-Signed Certificate

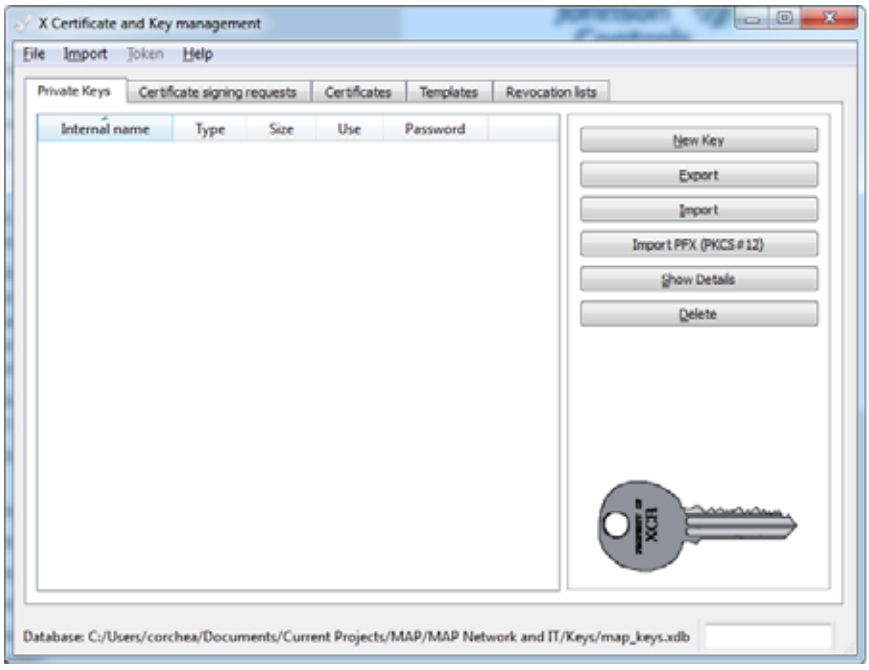
1.	**Figure 6: New Certificate** 	Open your certificate creating-application, select the Certificates tab if necessary, and click New Certificate. The Create Certificate screen appears.

Table 2: Creating a Self-Signed Certificate (Continued)

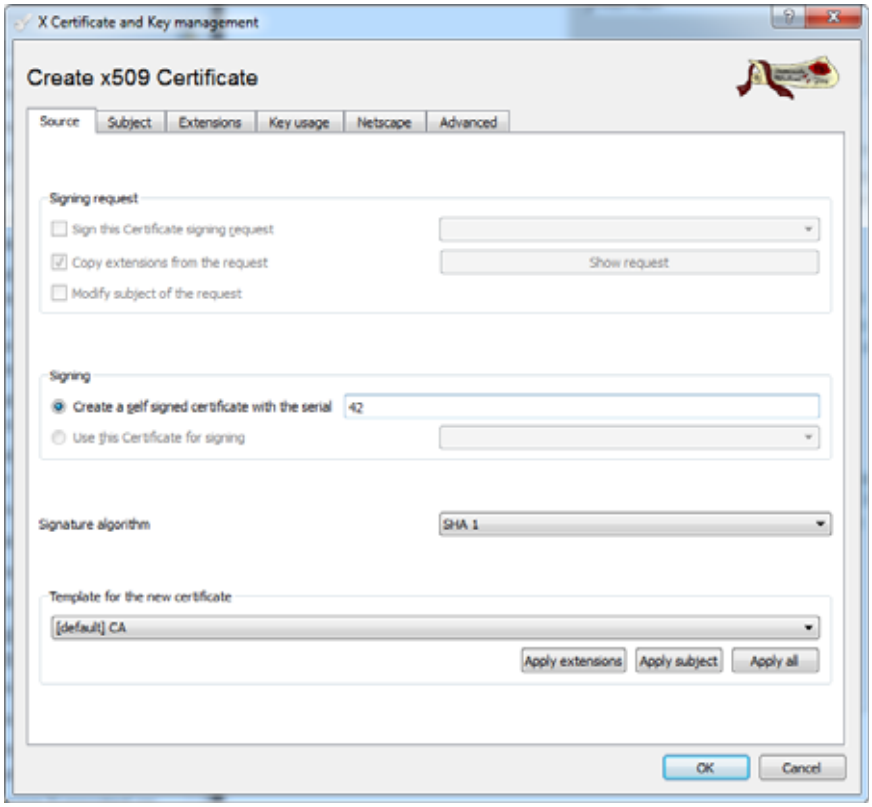
2.	**Figure 7: Create the Certificate** 	Accept the defaults unless they conflict with your IT policies and select the **Subject** Tab.

Table 2: Creating a Self-Signed Certificate (Continued)

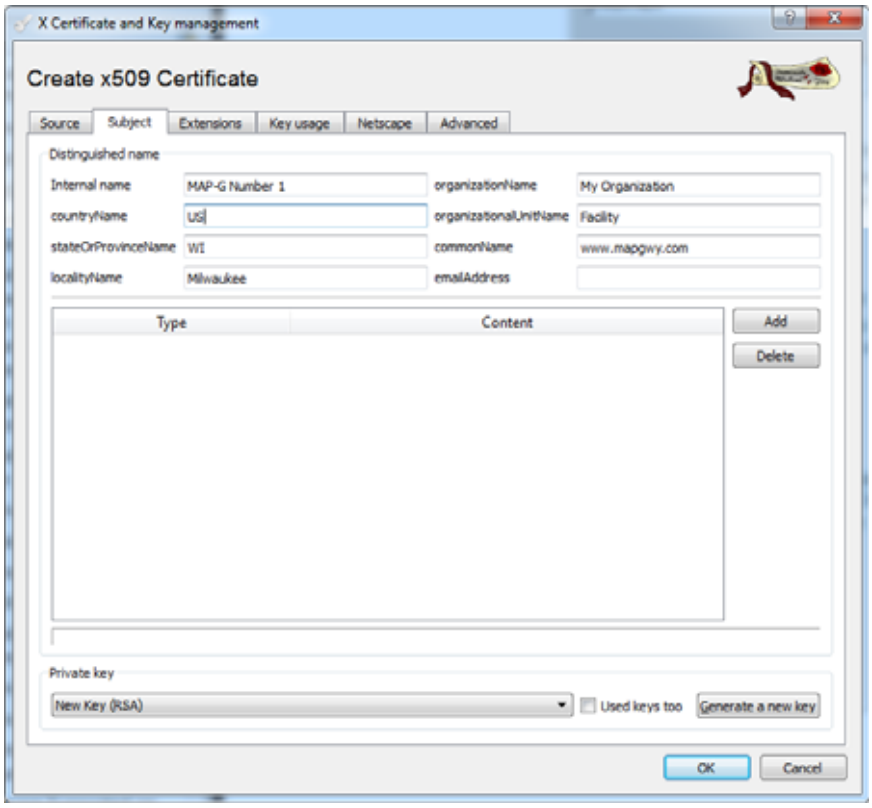
3.	**Figure 8: Subject Tab Properties** 	In the Distinguished name properties window, enter the following information: • **Internal name:** This name is only used internally and does not appear in the certificate. • **organizationName:** the name of your organization • **country/Name:** the country in which your organization is located • **organizationUnitName:** 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 MAP Gateway 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 **New Key (RSA),** 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. Select the **Extensions** tab

Table 2: Creating a Self-Signed Certificate (Continued)

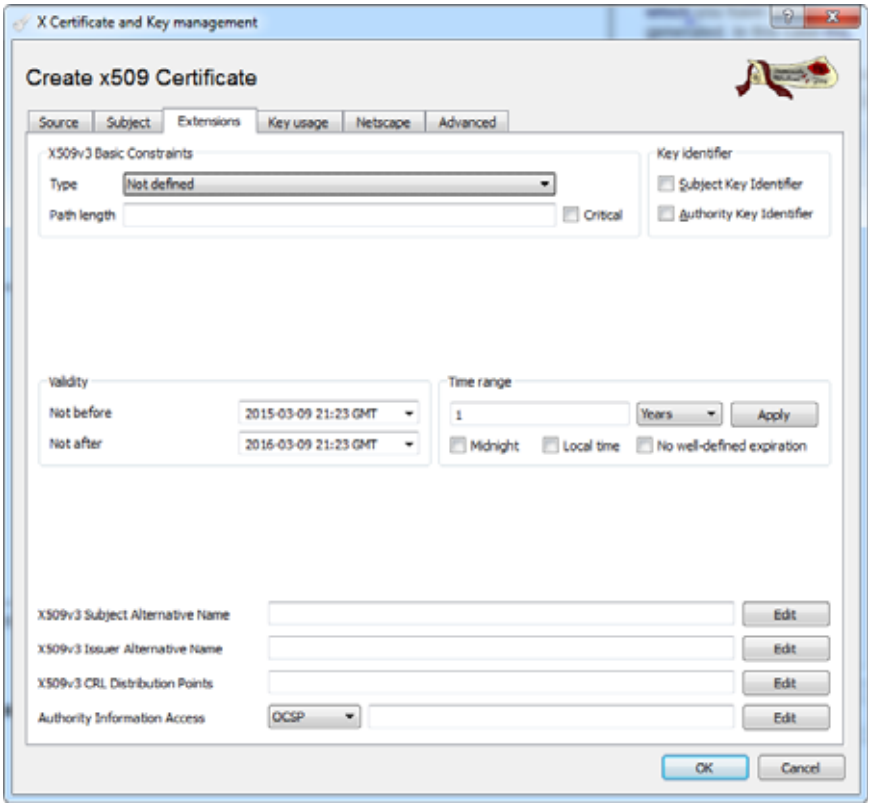
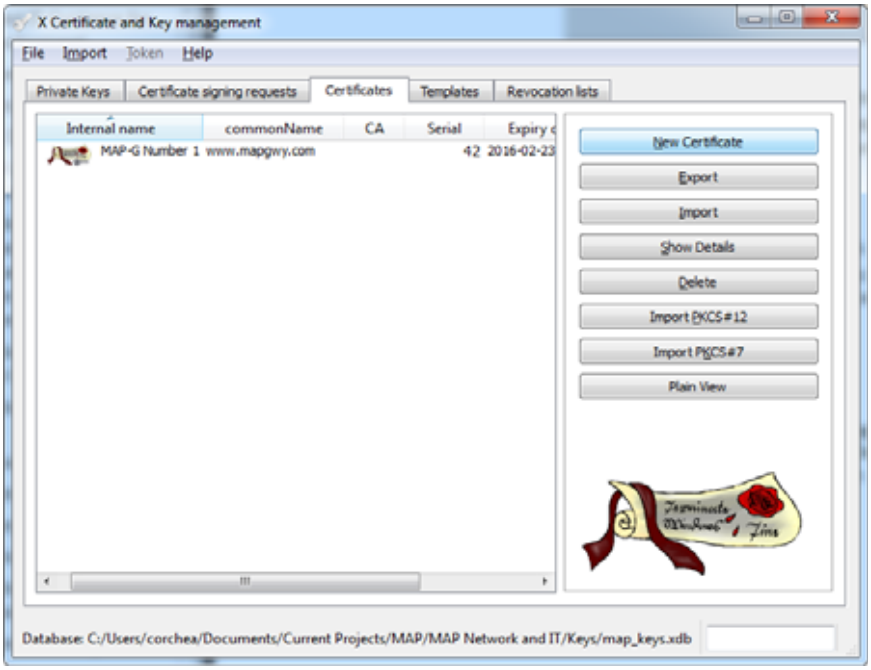
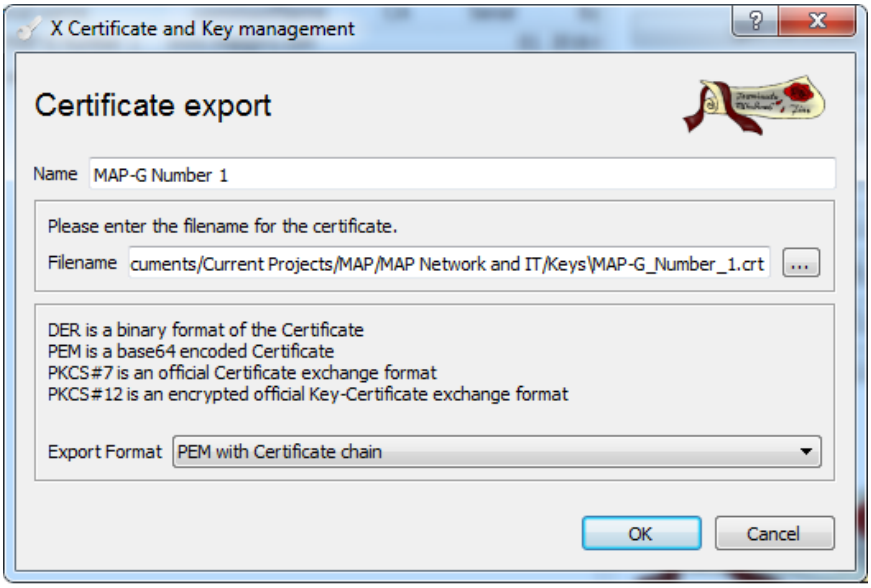
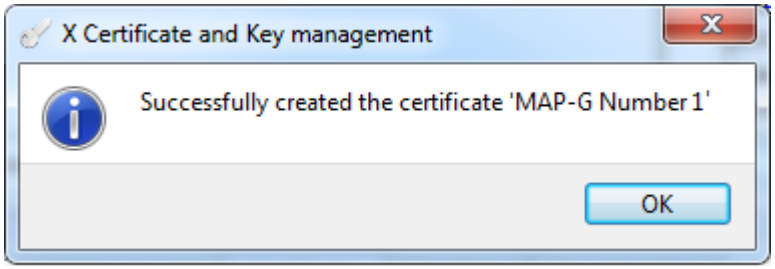
4.	**Figure 9: Extensions Tab Properties** 	Use the **Validity** and **Time range** sections to define time limits and valid ranges for your certificate. Click **OK**.
5.	**Figure 10: New Certificate Created** 	The new certificate is now in your list of certificates with the internal name you assigned. Select the certificate and click **Export.**

Table 2: Creating a Self-Signed Certificate (Continued)

6.	**Figure 11: New Certificate Export** 	Choose an export format of **PEM with Certificate chain** and click OK to save the file to a location where you can access the file to place into your MAP Gateway. This is the file you use when Adding a Private Key and Certificate to MAP Gateway.
7.	**Figure 12: Successfully Created Certificate Message** 	Click **Finish**.

Uninstalling the Root Certificate On a Client That Has Connected to the MAP Gateway

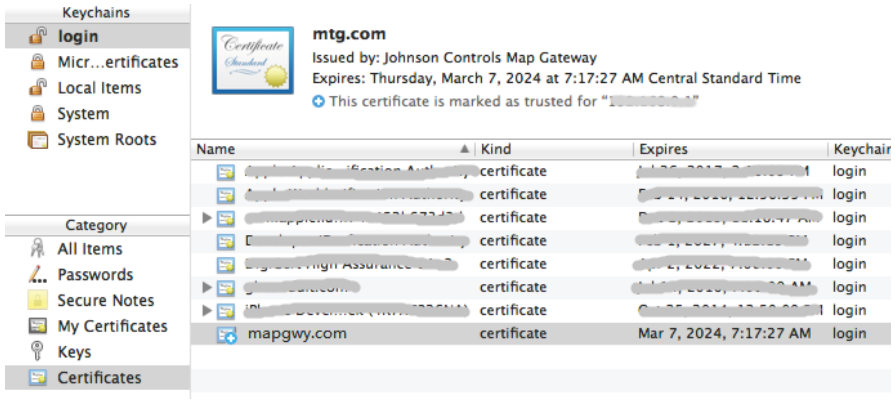
If you are removing or replacing a MAP Gateway and wish to uninstall the root certificate from your computer, follow the procedures in this section that are appropriate to your operating system. Note that you do not need to uninstall the certificate because a new certificate overwrites existing certificates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

Uninstalling the Security Certificate on iOS® Platforms

To remove the MAP Gateway security certificate on an iOS platform, navigate to Settings > General > Profiles, select the map-gwy.com certificate, and then tap **Remove** twice.

Uninstalling the Security Certificate in Apple® Safari® for Mac

Table 3: Uninstalling the Security Certificate in Apple® Safari® for Mac

1.	**Figure 13: Keychain Access** 	In Applications > Utilities, double-click the Keychain Access Application.
2.		Right-click the certificate you wish to remove (in this case, **www.mapgwy.com**), and then click **Delete**.
3.		Enter your administrator credentials, and click **Update Settings** to remove the certificate from the keychain.

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

Table 4: Uninstalling the Security Certificate in Internet Explorer

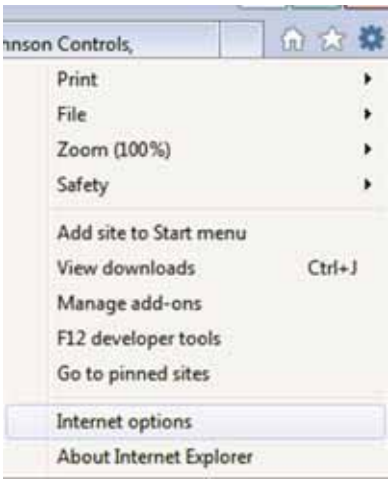
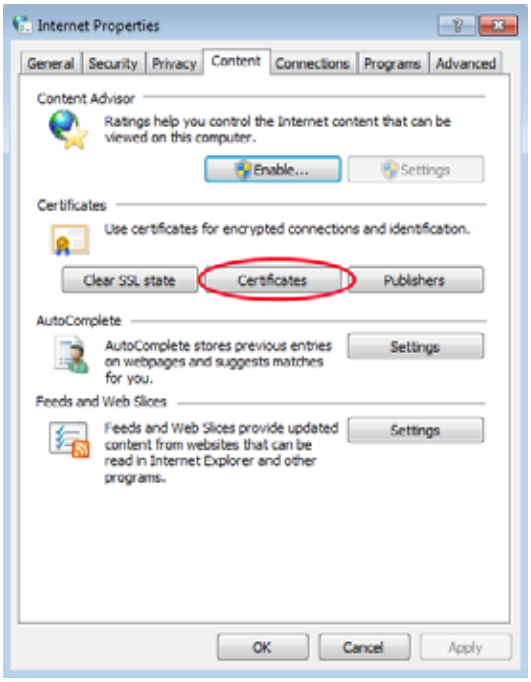
1.	**Figure 14: Internet Options Selection** 	On the Tools menu, click **Internet options.**
2.	**Figure 15: Internet Properties Content Tab** 	In the Internet Properties dialog box, click the **Content** tab, and then click **Certificates**.

Table 4: Uninstalling the Security Certificate in Internet Explorer (Continued)

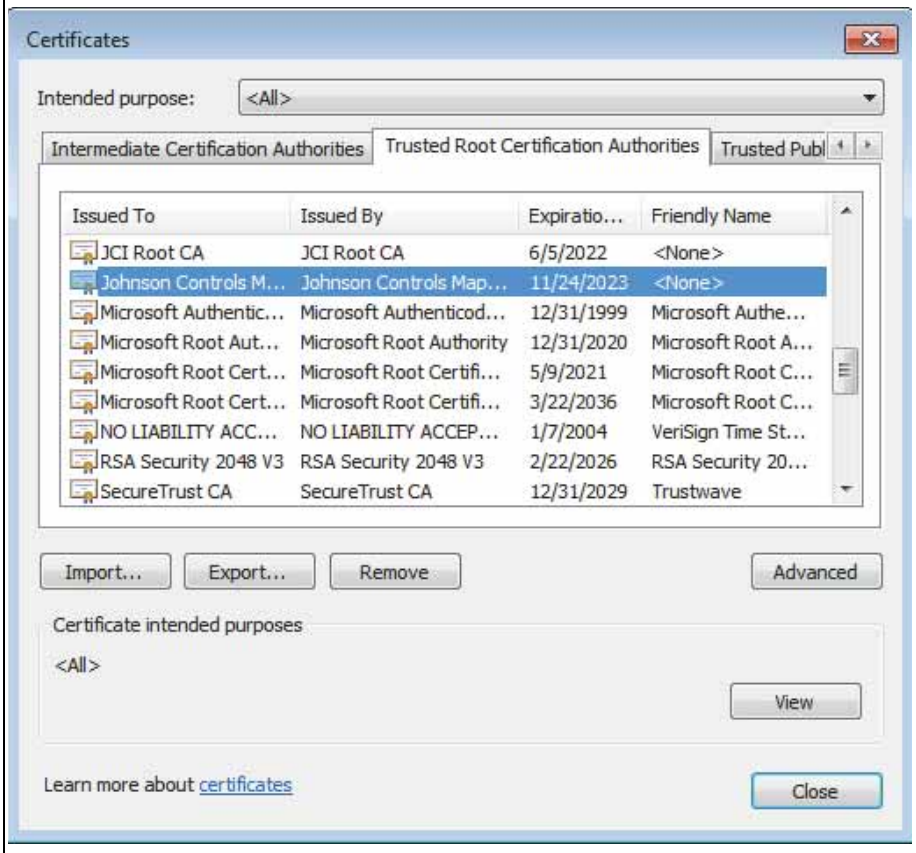
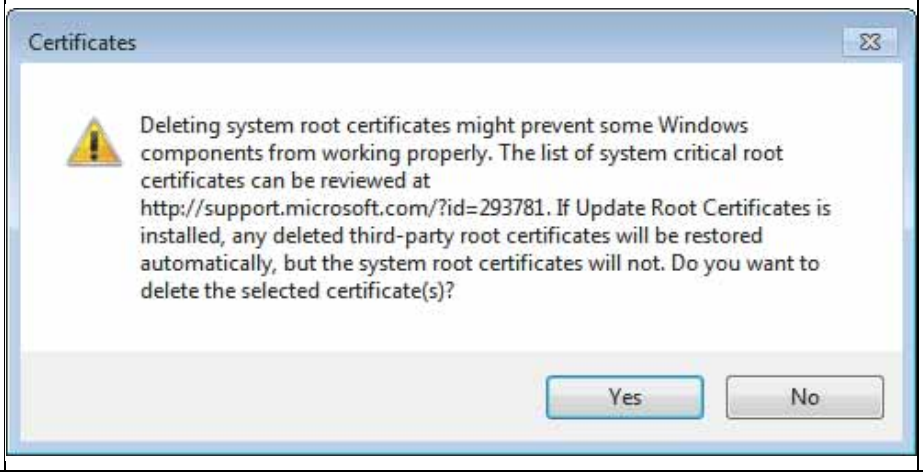
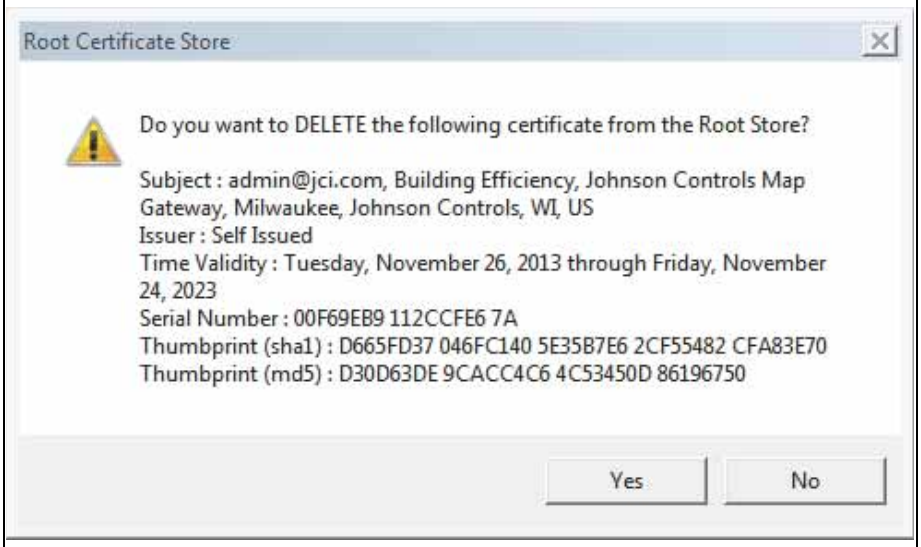
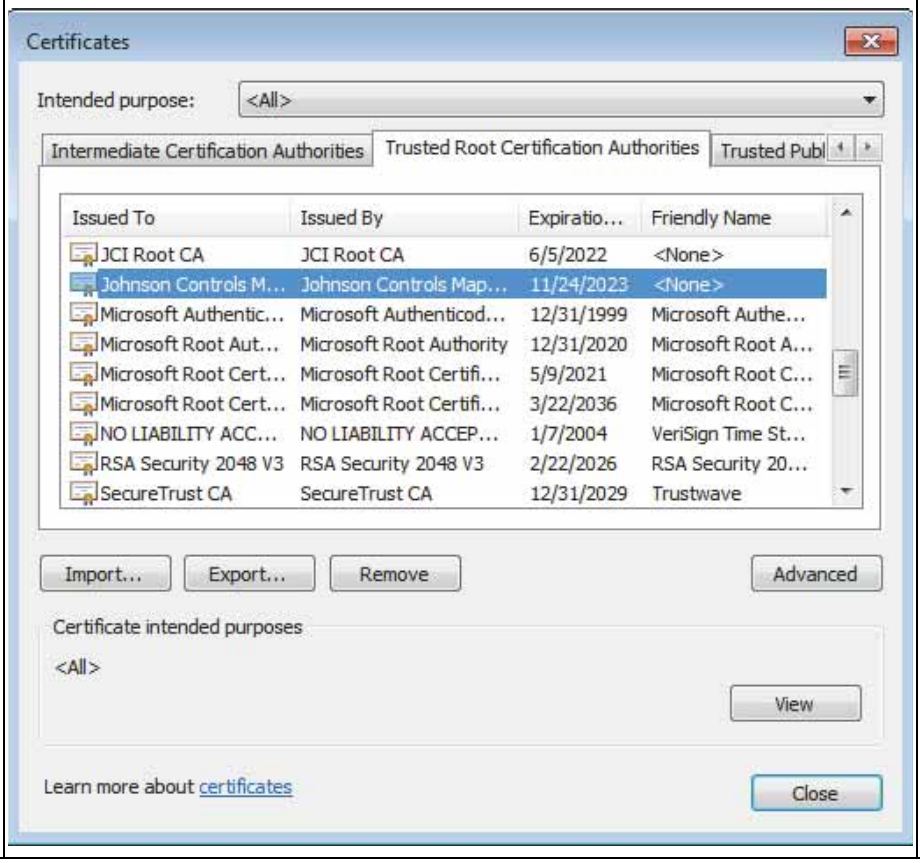
3.	**Figure 16: Certificates** 	In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab, select the Johnson Controls authority, and then click **Remove**. A Certificates warning appears.
4.	**Figure 17: Certificates Warning** 	In the Certificates warning dialog box, click **Yes**. A Root Certificate Store warning appears.

Table 4: Uninstalling the Security Certificate in Internet Explorer (Continued)

5.	**Figure 18: Root Certificate Store Warning Dialog** 	In the Root Certificate Store warning dialog box, click Yes. You return to the **Trusted Root Certification Authorities** tab of the Certificates dialog box.
6.	**Figure 19: Trusted Root Certification Authorities Tab** 	In the Certificates dialog box, click **Close**, and then click **OK**.

Uninstalling the Root Certificate in Google Chrome

Table 5: Uninstalling the Root Certificate in Google Chrome

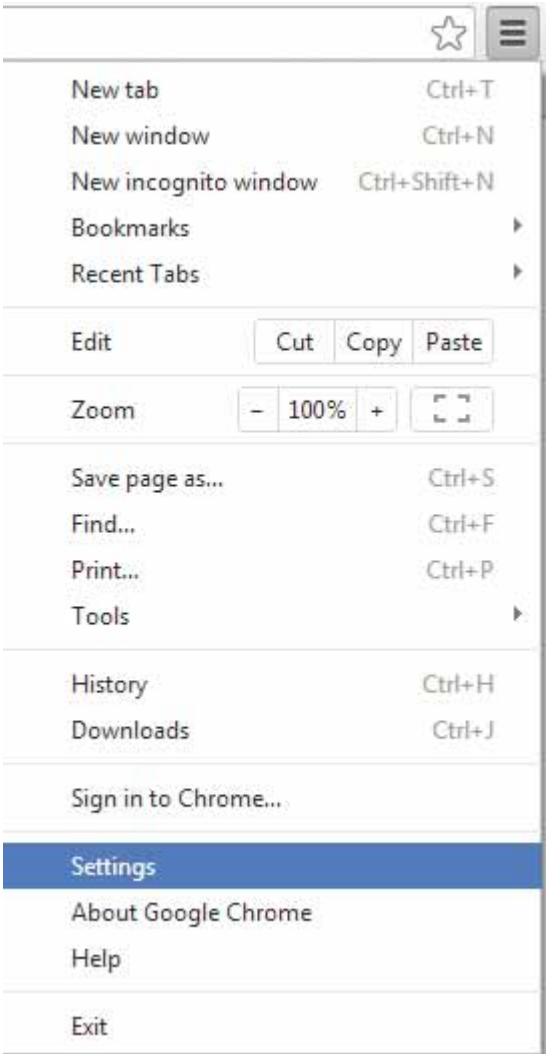
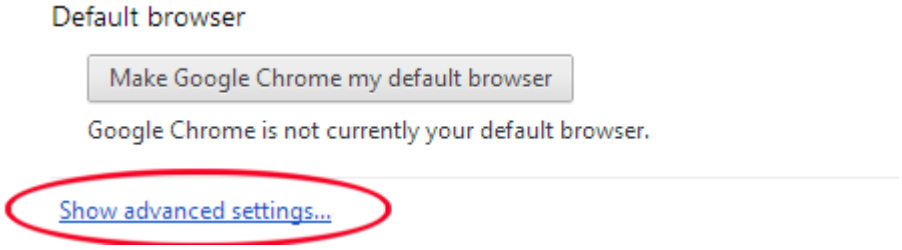
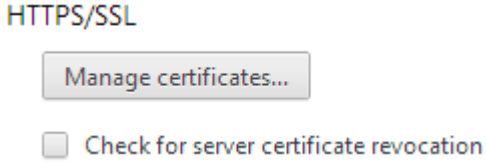
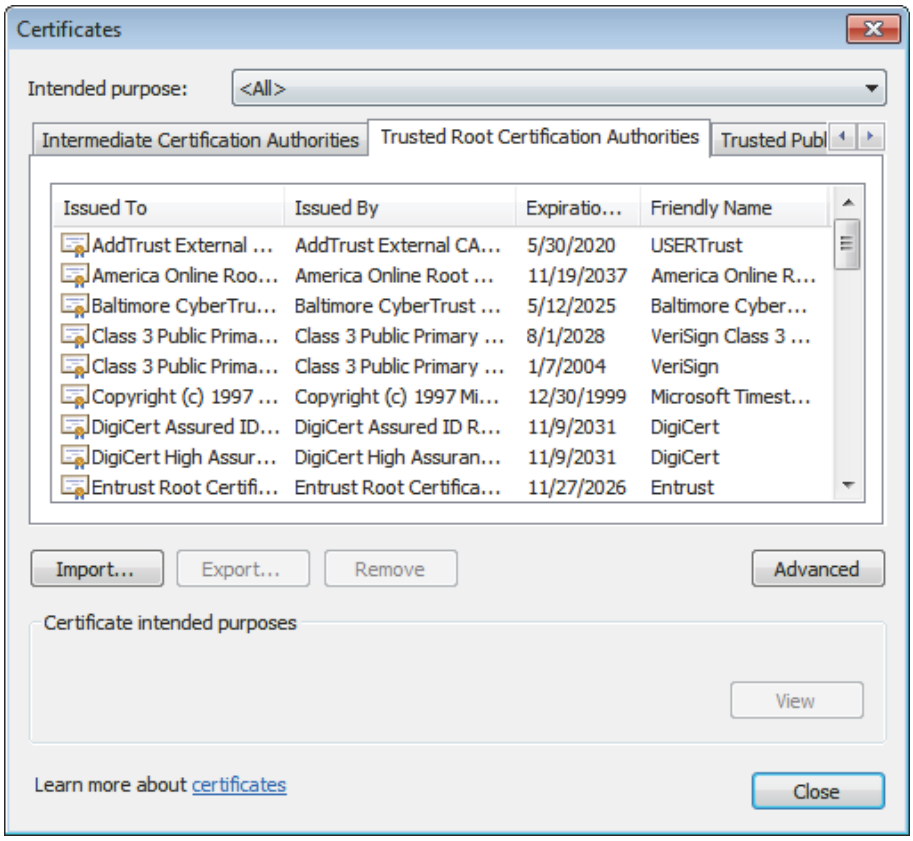
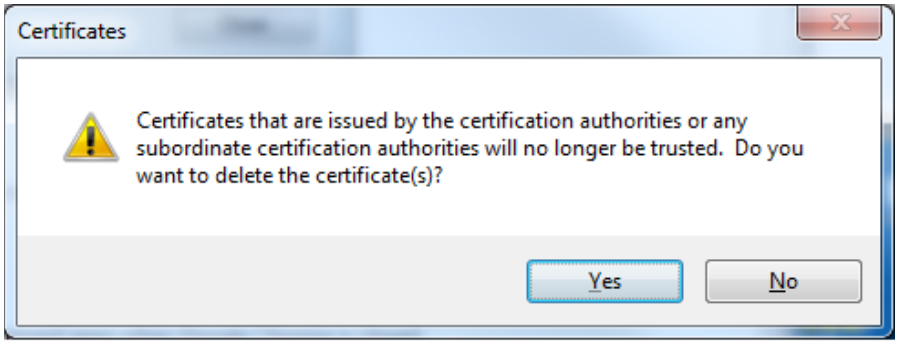
1.	**Figure 20: Google Chrome Customize and control Google Chrome menu** 	Click the **Customize and control Google Chrome** button  and select **Settings**.
2.	**Figure 21: Advanced Settings** 	Scroll down to the bottom of the pane and select S**how advanced settings.**
3.	**Figure 22: HTTPS/SSL** 	Scroll to the **HTTPS/SSL** section click **Manage certificates** and select the **Trusted Root Certification Authorities** tab.

Table 5: Uninstalling the Root Certificate in Google Chrome (Continued)

4.	**Figure 23: Trusted Root Certification Authority Tab** 	Select the Johnson Controls authority, and then click **Remove**. A Certificates warning appears.
5.	**Figure 24: Certificate Removal Warning** 	Click **Yes**. The **certificate is removed immediately**.

Adding a Private Key and Certificate to MAP Gateway

This process describes how to add the private key and certificate to your MAP Gateway.

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 MAP Gateway to your computer when transferring keys to the MAP Gateway.

Table 6: Adding a Private Key and Certificate to MAP Gateway

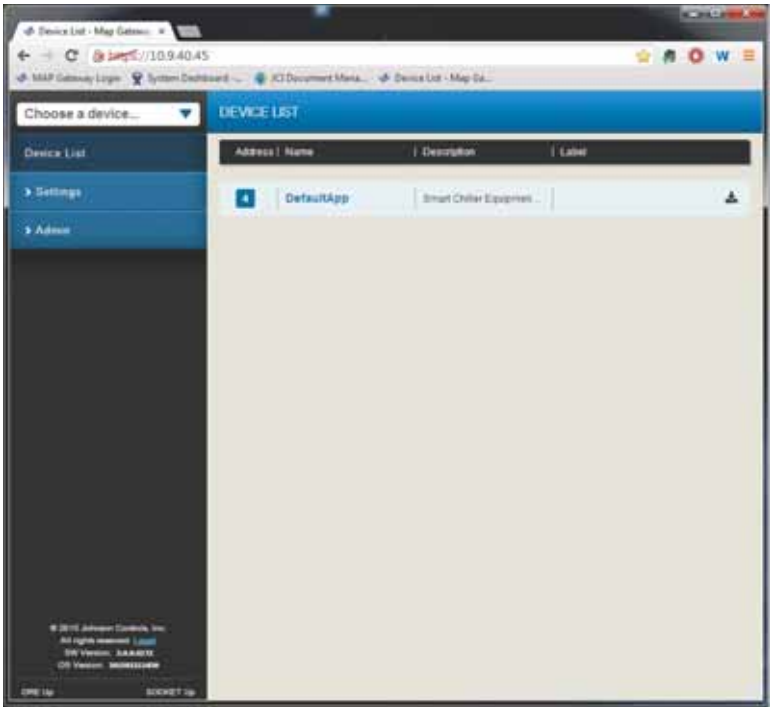
1.		Connect to MAP Gateway through an Ethernet cross-over cable. The direct connection helps prevent man-in-the-middle type attacks when adding security keys and certificates.
2.	**Figure 25: Advanced Settings** 	Log in to your MAP Gateway UI by opening your web browser and entering www.mapgwy.com. You must be logged in as an administrator to perform these tasks. **NOTE:** If your computer does not connect to the MAP Gateway 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 MAP Gateway UI when you enter www.mapgwy.com.

Table 6: Adding a Private Key and Certificate to MAP Gateway (Continued)

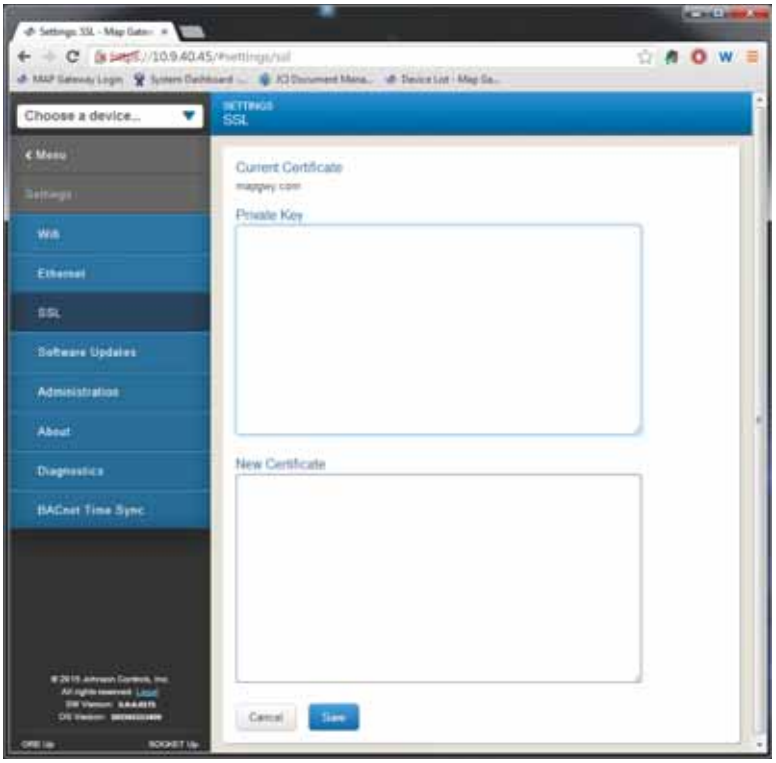
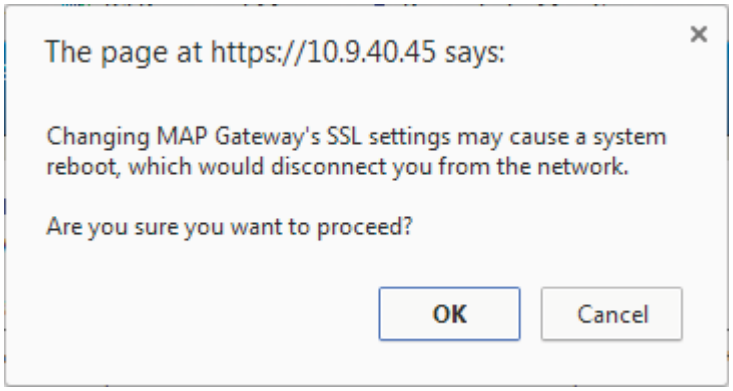
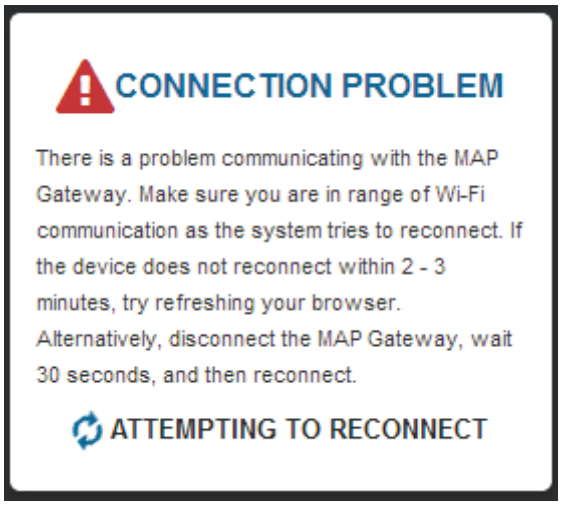
3.	**Figure 26: MAP Gateway SSL Screen** 	Click **Settings** and select **SSL**.
4.		Navigate to the location of the private key file (***.pem) that you created for your site. Right-click the file and select **Open with**, and then select **Notepad**.
5.		Select all the text and copy the entire file. Paste this file as a plain text file in the Private Key box of your MAP Gateway SSL settings Private Key box.
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 MAP Gateway SSL settings Private Key box and click Save. A reset warning screen appears.

Table 6: Adding a Private Key and Certificate to MAP Gateway (Continued)

8.	**Figure 27: Reset Warning Screen** 	To apply the new certificate and private key, the MAP Gateway must reset. Click **OK**. MAP Gateway goes offline while resetting.
9.	**Figure 28: Device Resetting Screen** 	When the connection is reestablished, log in to MAP Gateway and use normally.

Installing the Root Certificate on a Client That is Connecting to MAP Gateway

Until the security certificate for the MAP Gateway is added as a trusted root certificate, you receive a security alert every time you visit the mapgwy.com website. How you install the certificate differs based on the web browser and device platform.

Installing the Security Certificate on iOS

Mobile iOS platforms such as iPhones and iPads do not require a separate installation of SSL for MAP Gateway. When you connect to the MAP Gateway Wi-Fi access point and open Safari, you are automatically taken to **www.mapgwy.com.** Click **Continue** when presented with the **Cannot Verify Server Identity** screen. The MAP Gateway login screen appears.

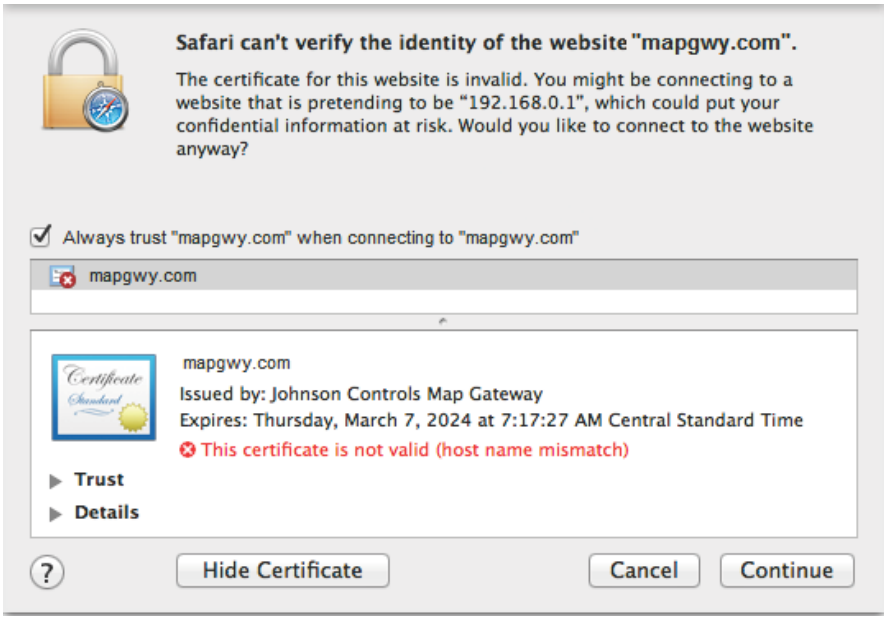
Figure 29: Verify Identity in iOS

Installing the Security Certificate in Apple® Safari® for Mac OS

Table 7: Installing the Security Certificate in Apple® Safari® for Mac OS

1.		Navigate to **www.mapgwy.com/downloadtlsprofile**. A screen appears saying **Safari can't verify the identity of the website mapgwy.com.**
2.		Click **Show Certificate**. The screen expands to show the certificate.
3.		Select the **Always trust "mapgwy.com" when connecting to "mapgwy.com"** checkbox.

Table 7: Installing the Security Certificate in Apple® Safari® for Mac OS (Continued)

4.	**Figure 30: Trust MAP Gateway Identity Screen** 	Click **Continue**.

Installing the Security Certificate in Internet Explorer

Table 8: Installing the Security Certificate in Internet Explorer

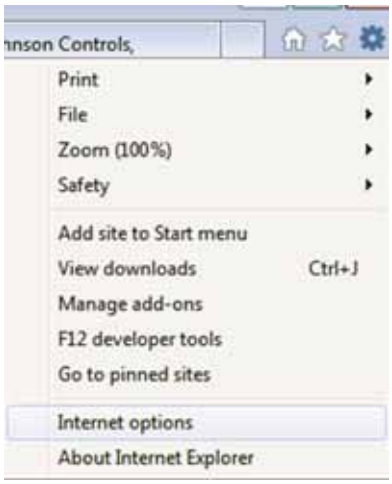
1.		Navigate to **www.mapgwy.com/downloadtlsprofile**, and then download the **rootCA.pem** file.
2.	**Figure 31: Internet Options Selection** 	On the Tools menu, click **Internet options** then select the **Content** tab.

Table 8: Installing the Security Certificate in Internet Explorer (Continued)

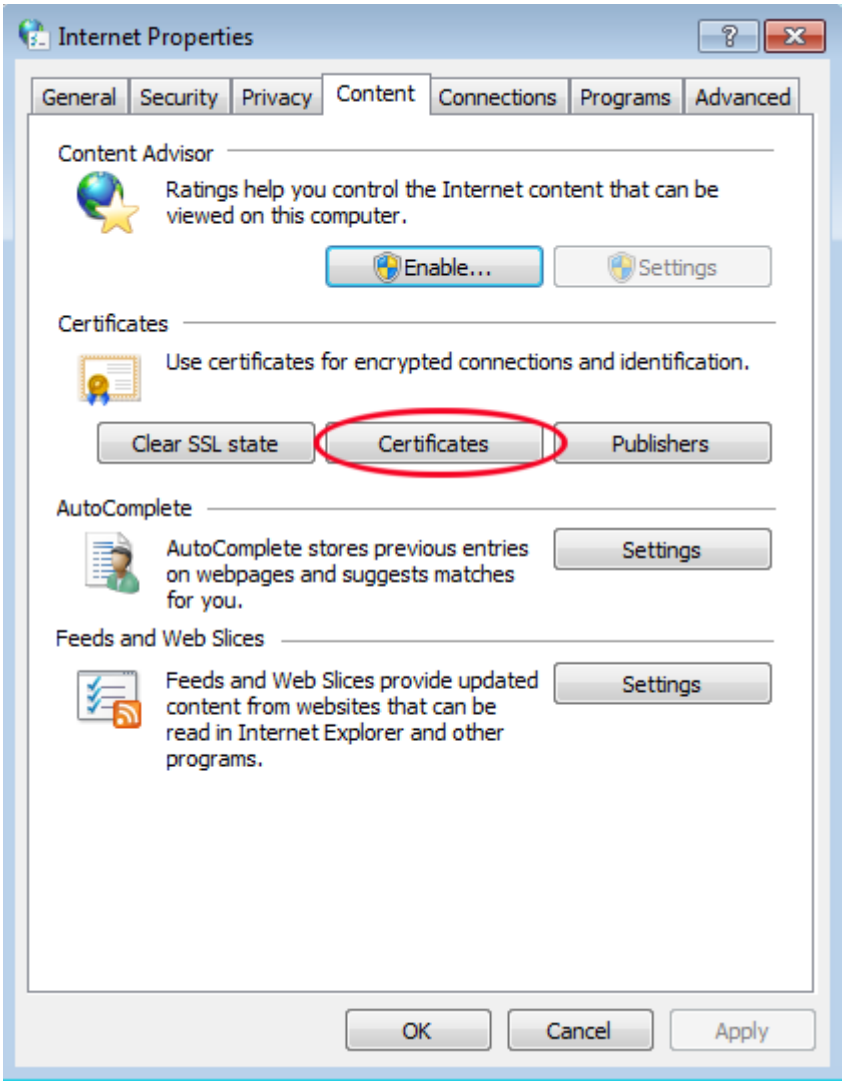
3.	**Figure 32: Internet Properties Content Tab**  	In the Internet Properties dialog box, click the **Content** tab, and then click **Certificates** and select the **Trusted Root Certification Authorities** tab.

Table 8: Installing the Security Certificate in Internet Explorer (Continued)

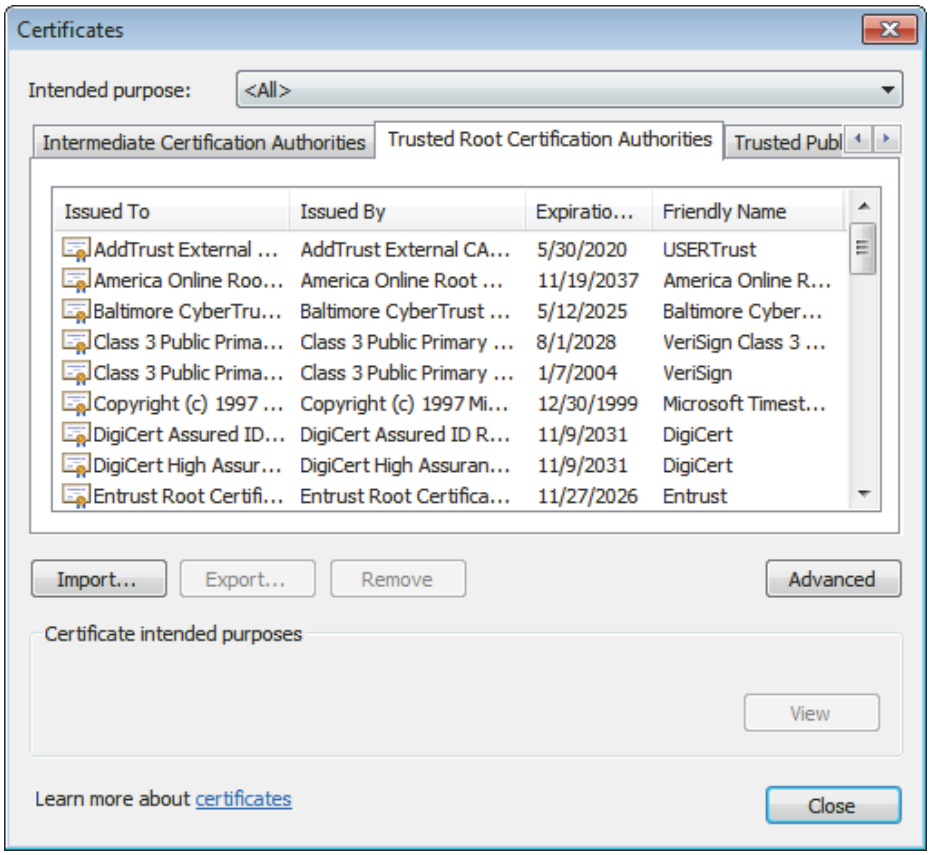
4.	**Figure 33: Trusted Root Certification Authorities Tab** 	Click **Import.** The Certificate Import Wizard opens.

Table 8: Installing the Security Certificate in Internet Explorer (Continued)

5.	**Figure 34: Certificate Install Wizard** 	In the Certificate Import Wizard dialog box, click **Next**.

Table 8: Installing the Security Certificate in Internet Explorer (Continued)

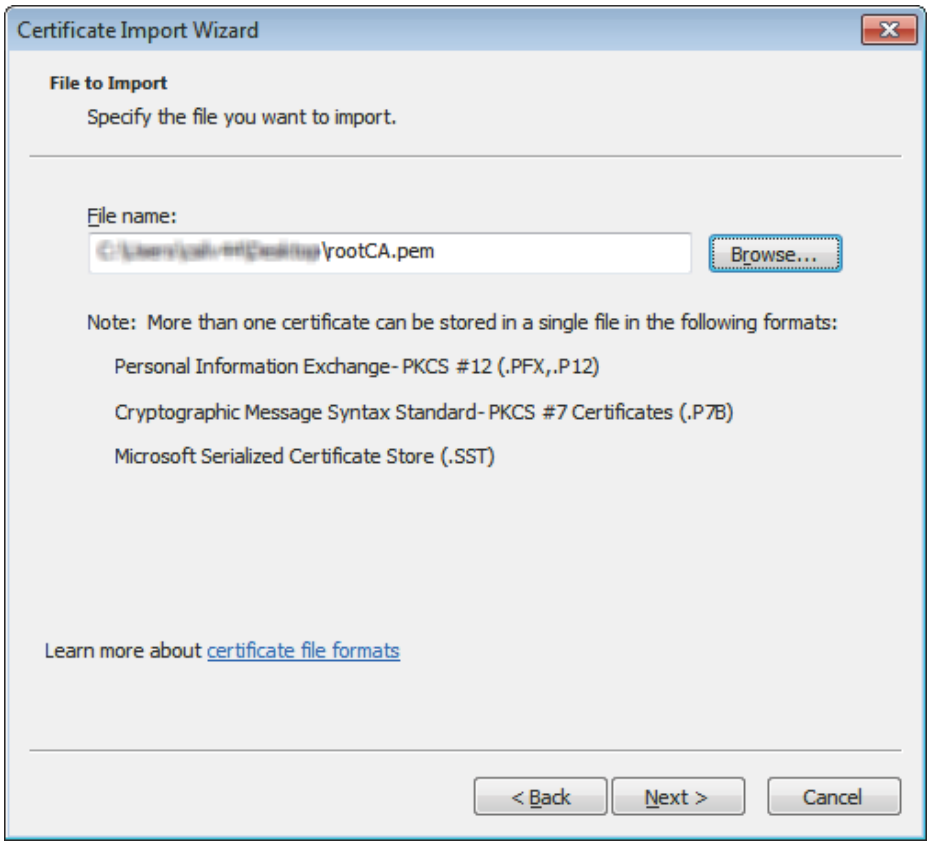
6.	**Figure 35: Certificate Import Wizard - Select File to Import** 	Browse to the **rootCA.pem** security certificate file, select it, click **Open**, and then click Next. **NOTE:** Install the **rootCA.pem** file and not the mapgwy.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any MAP Gateway you use. If you install the mapgwy.com file that the browser prompts you to install instead, you need to add a new root certificate for each new MAP Gateway device that you use.

Table 8: Installing the Security Certificate in Internet Explorer (Continued)

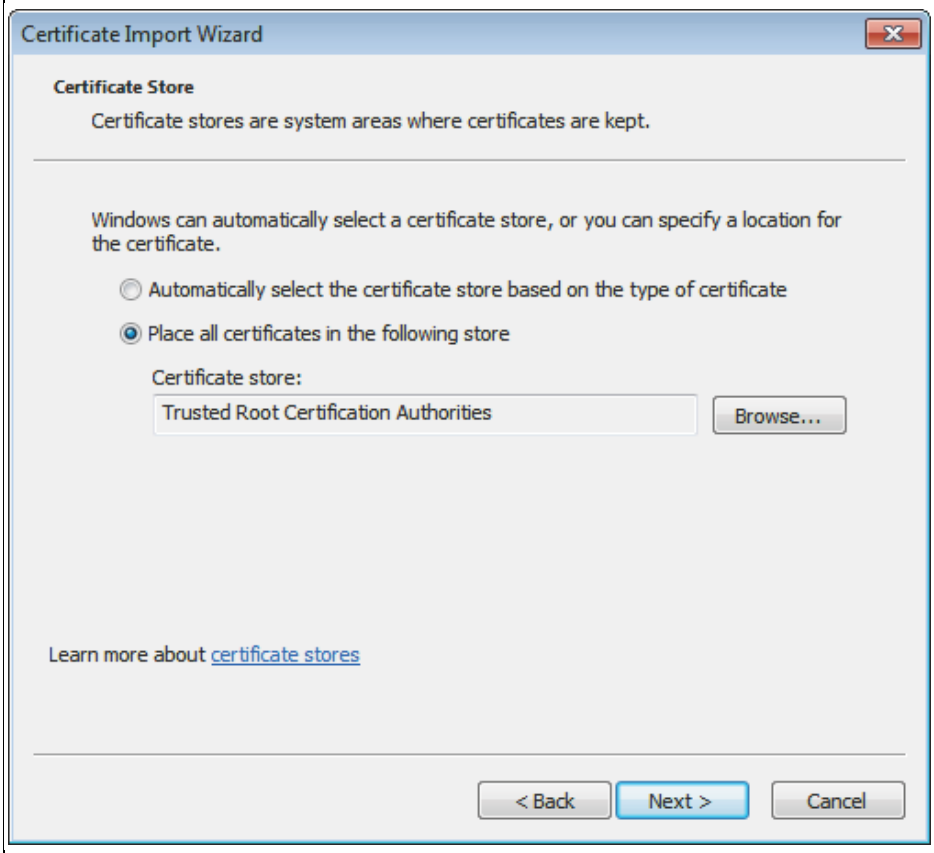
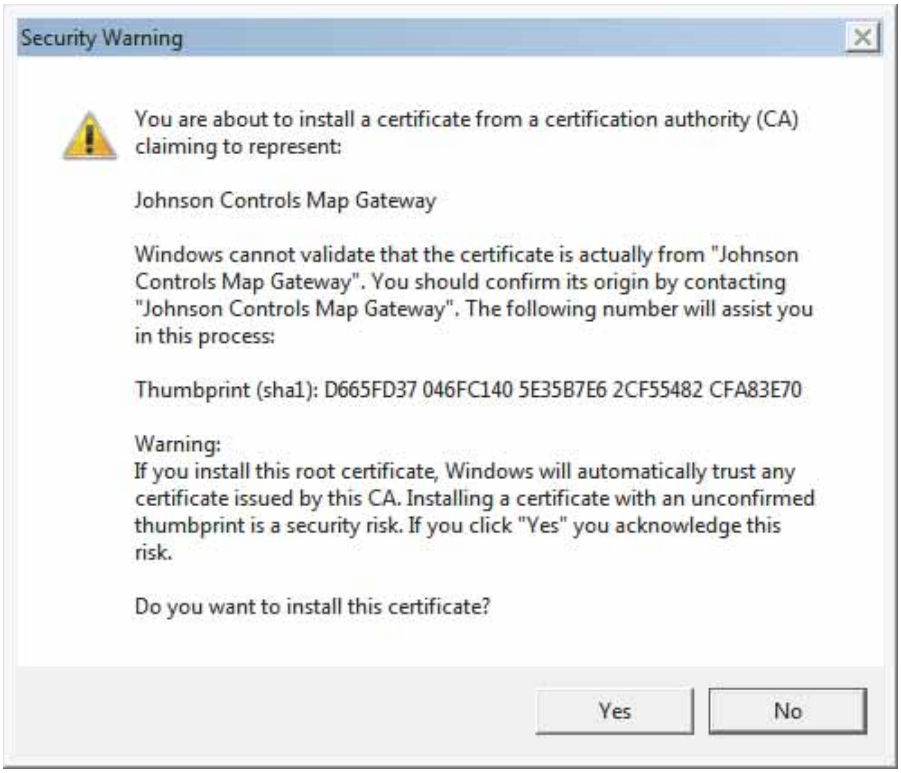
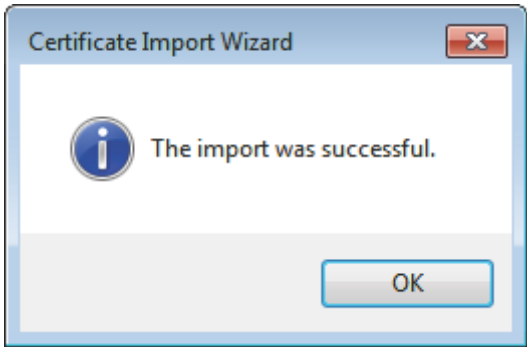
7.	**Figure 36: Certificate Import Wizard Certificate Store** 	On the Certificate Store page of the wizard, select **Place all certificates in the following store**, verify that the certificate store listed is **Trusted Root Certification Authorities**, and then click **Next**.

Table 8: Installing the Security Certificate in Internet Explorer (Continued)

8.	**Figure 37: Certificate Import Wizard Security Warning** 	In the Security Warning dialog box, click **Yes**.
9.	**Figure 38: Wizard Complete** 	Click **Finish**. A success message appears.
10.		Click **OK**.

Installing the Security Certificate in Google® Chrome™

Table 9: Installing the Security Certificate in Google® Chrome

1.		Navigate to **www.mapgwy.com/downloadtlsprofile**, and then download the **rootCA.pem** file.

Table 9: Installing the Security Certificate in Google® Chrome (Continued)

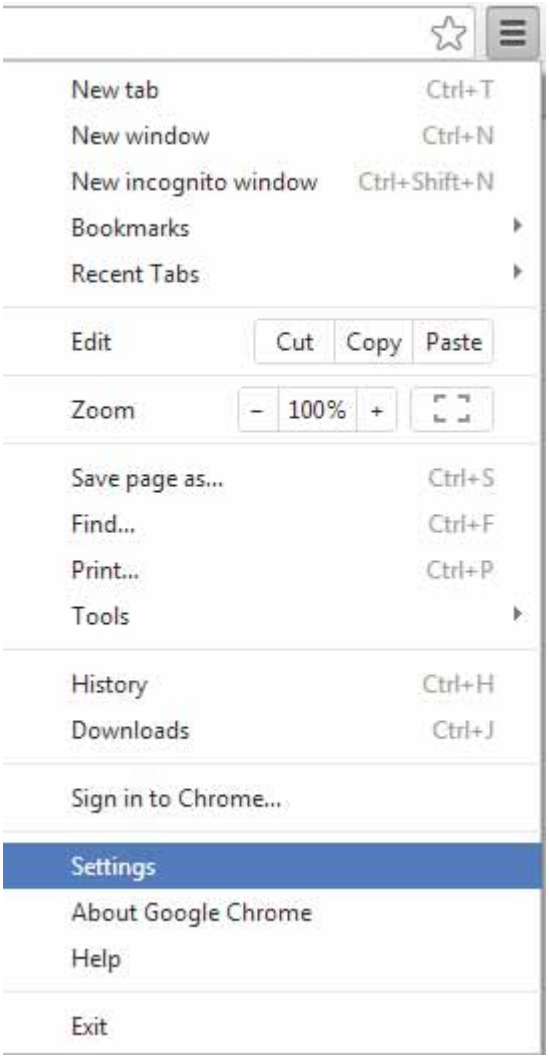
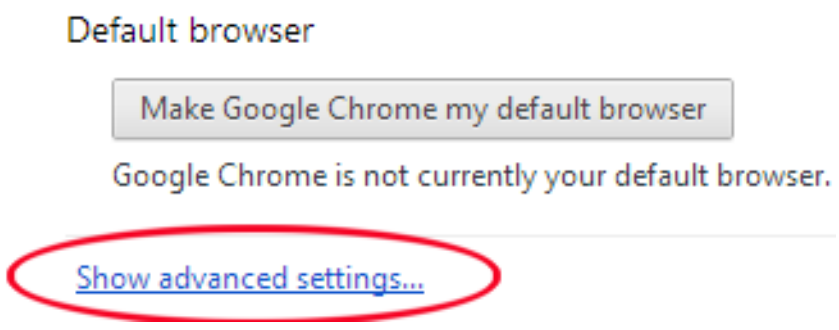
2.	**Figure 39: Chrome Settings Menu** 	On the Chrome menu  click **Settings**.
3.	**Figure 40: Advanced Settings Selection** 	At the bottom of the Settings page, click **Show advanced settings.**

Table 9: Installing the Security Certificate in Google® Chrome (Continued)

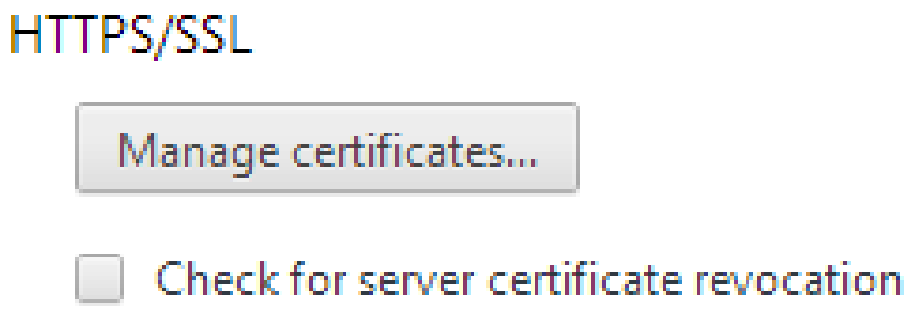
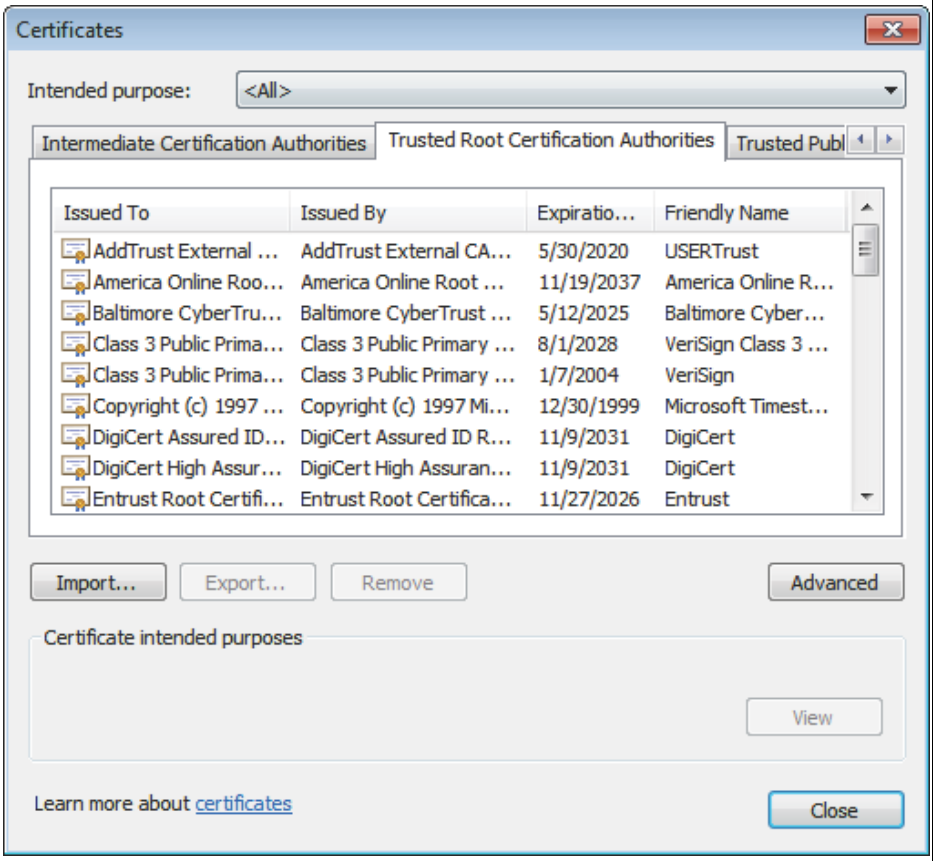
4.	**Figure 41: Manage Certificates** 	Under HTTPS/SSL, click **Manage certificates**.
5.	**Figure 42: Chrome SSL Certificates** 	In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab, and then click **Import**. The Certificate Import Wizard opens.

Table 9: Installing the Security Certificate in Google® Chrome (Continued)

6.	**Figure 43: Certificate Install wizard** 	In the Certificate Import Wizard dialog box, click **Next**.

Table 9: Installing the Security Certificate in Google® Chrome (Continued)

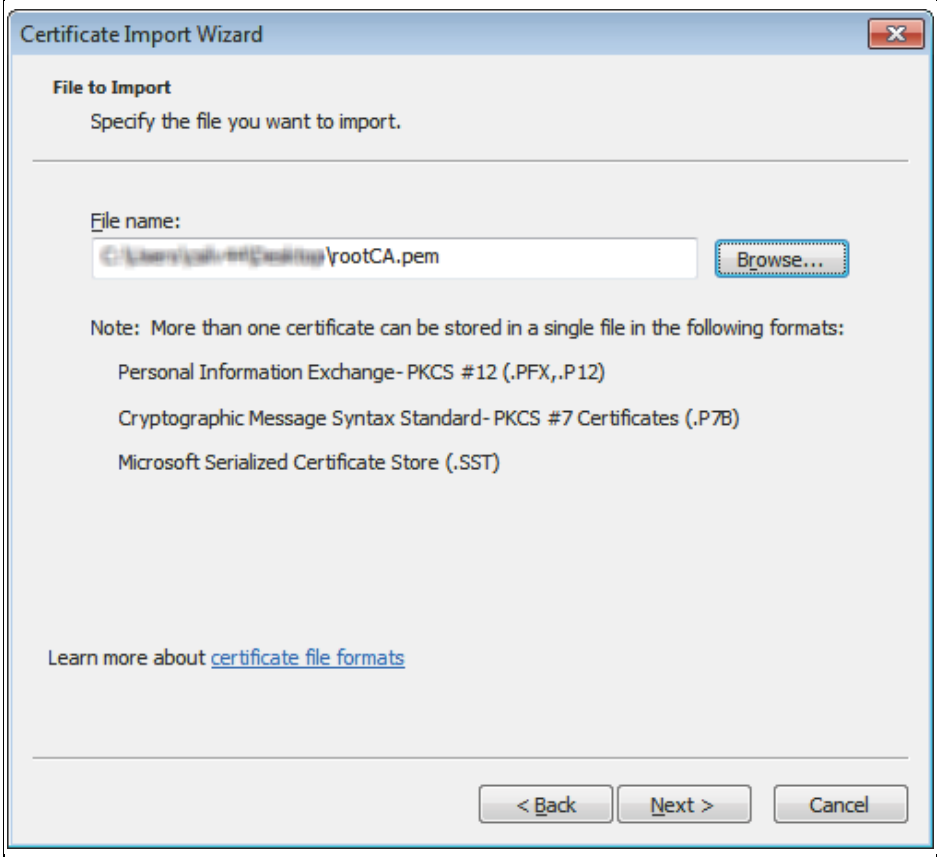
7.	**Figure 44: Certificate Import Wizard Browse** 	Browse to the rootCA.pem security certificate file, select it, click Open, and then click Next. **NOTE:** Install the rootCA.pem file and not the mapgwy.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any MAP Gateway you use. If you install the mapgwy.com file that the browser prompts you to install instead, you need to add a new root certificate for each new MAP Gateway device that you use.

Table 9: Installing the Security Certificate in Google® Chrome (Continued)

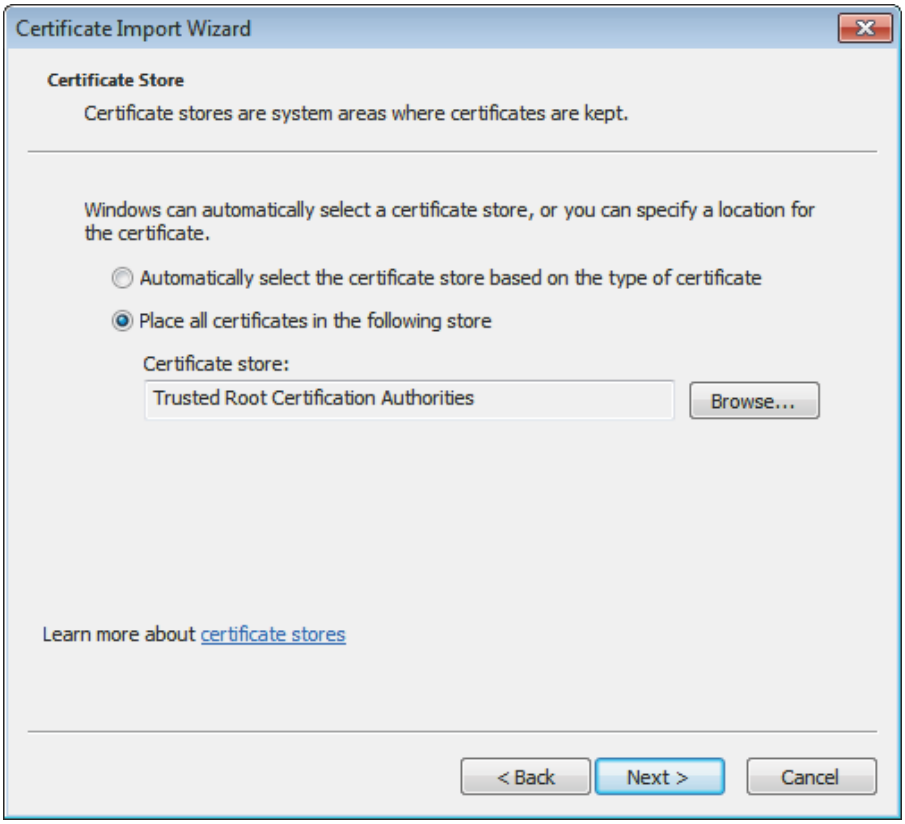
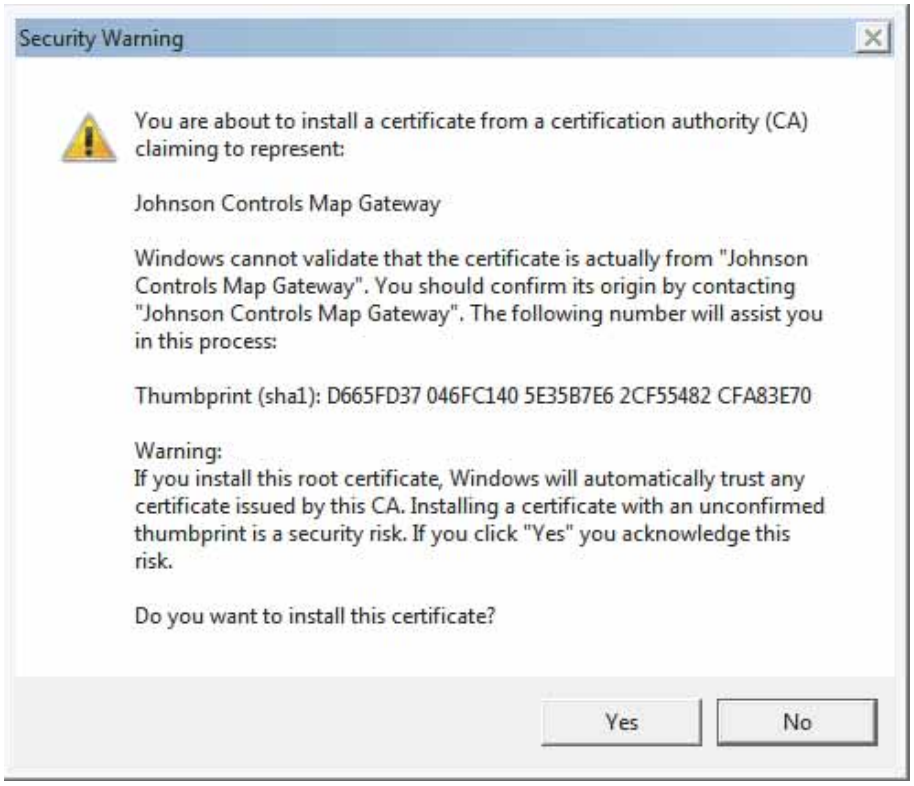
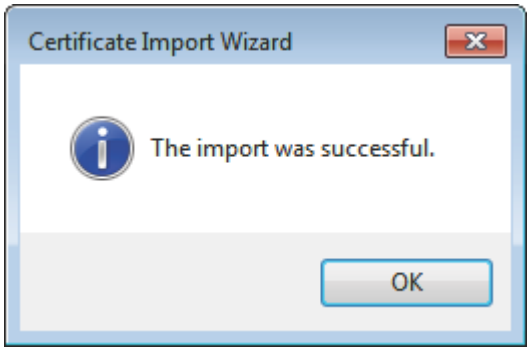
8.	**Figure 45: Certificate Import Wizard - Certificate Store** 	On the Certificate Store page of the wizard, select **Place all certificates in the following store**, verify that the certificate store listed is **Trusted Root Certification Authorities**, and then click **Next**.

Table 9: Installing the Security Certificate in Google® Chrome (Continued)

9.	**Figure 46: Security Warning** 	In the Security Warning dialog box, click **Yes**.
10.	**Figure 47: Certificate Install Wizard Success** 	Click **Finish**. A success message appears.
11.		Click **OK**.

Importing the Root Certificate

If you have a root certificate from a public certificate authority you may import it using this procedure.

Table 10: Importing The Root Certificate

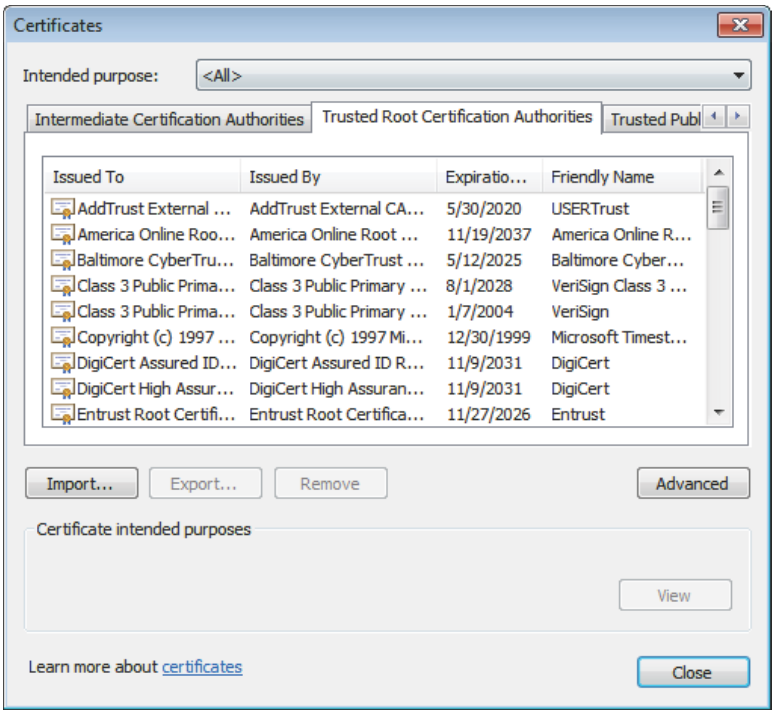
1.	**Figure 48: The Certificates Dialog Box** 	In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab, and then click **Import**. The Certificate Import Wizard opens.
2.	**Figure 49: Certificate Import Wizard** 	In the Certificate Import Wizard dialog box, click **Next.**

Table 10: Importing The Root Certificate (Continued)

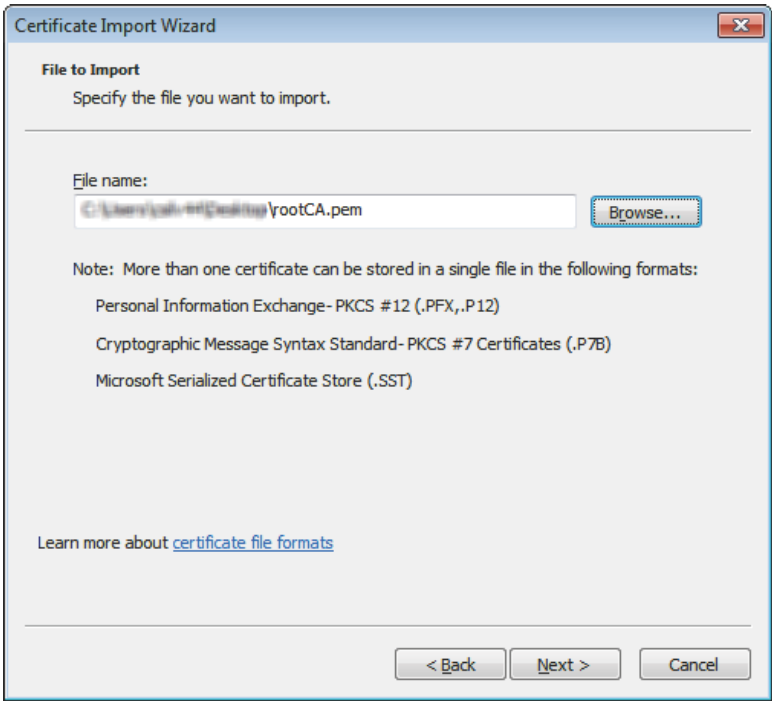
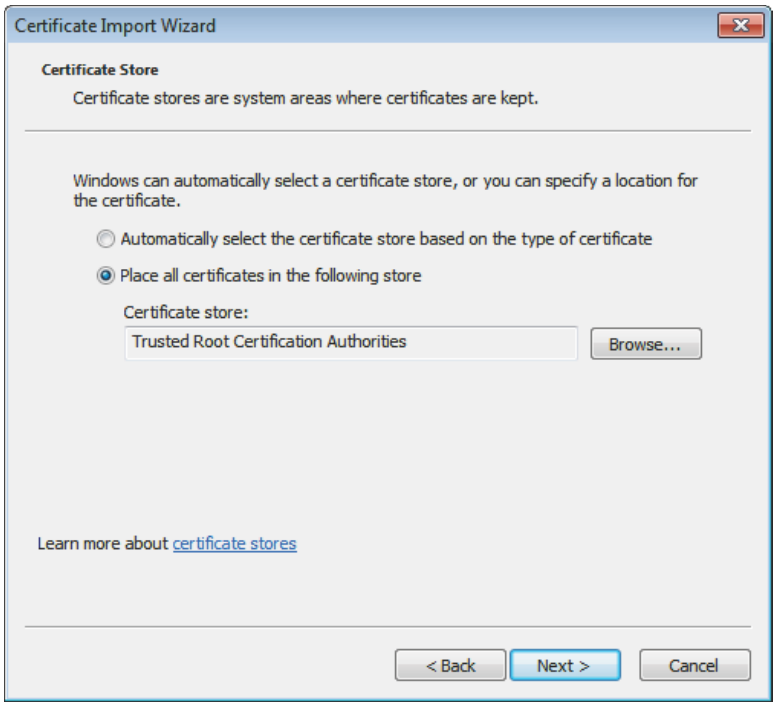
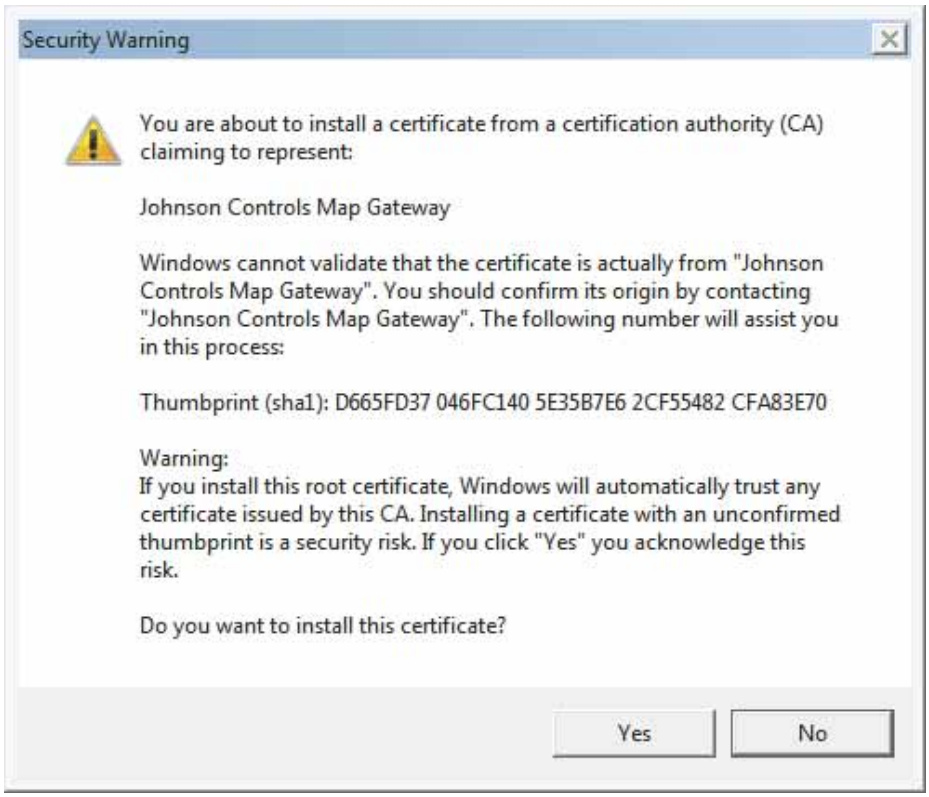
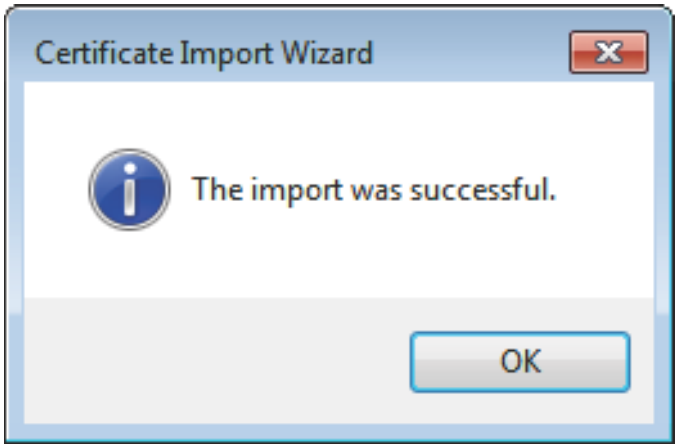
3.	**Figure 50: Importing the Certificate** 	Browse to the **rootCA.pem** security certificate file, select it, click **Open**, and then click **Next**. **NOTE:** Install the **rootCA.pem** file and not the mapgwy.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any MAP Gateway you use. If you install the mapgwy.com file that the browser prompts you to install instead, you need to add a new root certificate for each new MAP Gateway device that you use.
4.	**Figure 51: Certificate Store Options** 	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**.

Table 10: Importing The Root Certificate (Continued)

5.	**Figure 52: Non-Validated Certificate Security Warning** 	In the Security Warning dialog box, click **Yes**.
6.	**Figure 53: The Certificate Import Success Message** 	Click **Finish**. A success message appears.
7.		Click OK.

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 MAP Gateway.
- 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 2014 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.

Table 11: Creating the Certificate Request (CSR)

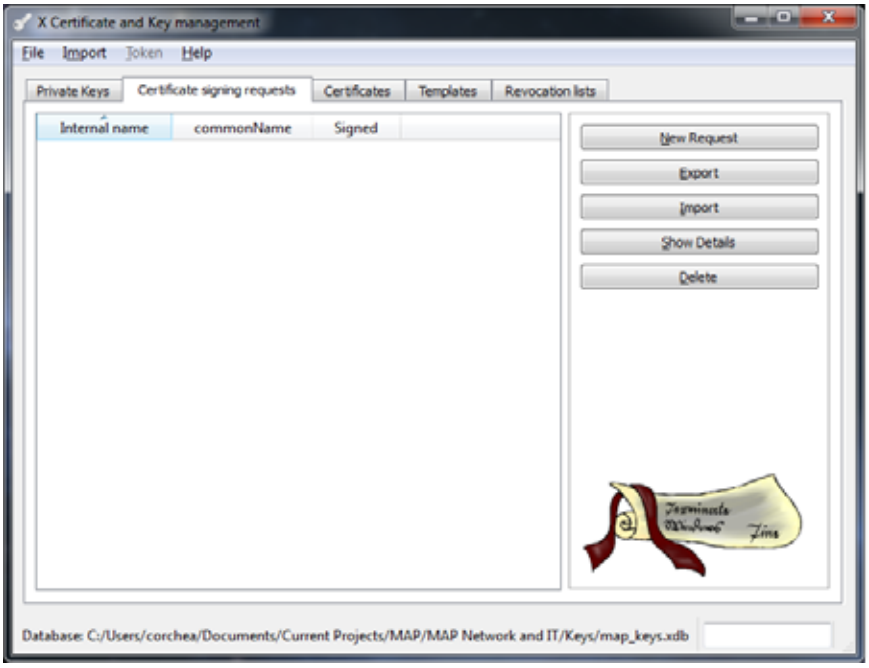
1.	**Figure 54: Figure 54: New Certificate Signing Request Tab** 	Open your certificate request creating application, select the **Certificates signing requests** tab if necessary, and click **New Certificate**. The Create Certificate signing request screen appears.

Table 11: Creating the Certificate Request (CSR) (Continued)

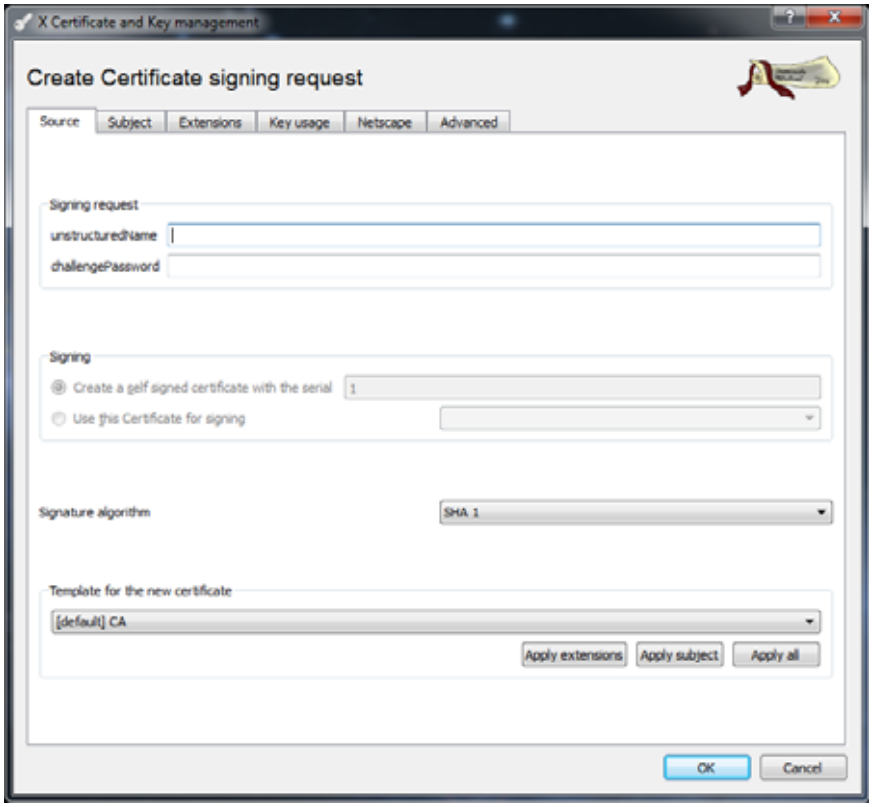
2.	**Figure 55: Create CSR Source Screen** 	In Signing request enter **unstructuredName** and **challengePassword**. The unstructured name is used by the certificate signing authority and may be set to your organization name. Accept the defaults (SHA1 and [default]CA) unless they conflict with your IT policies and click the **Subject** tab.

Table 11: Creating the Certificate Request (CSR) (Continued)

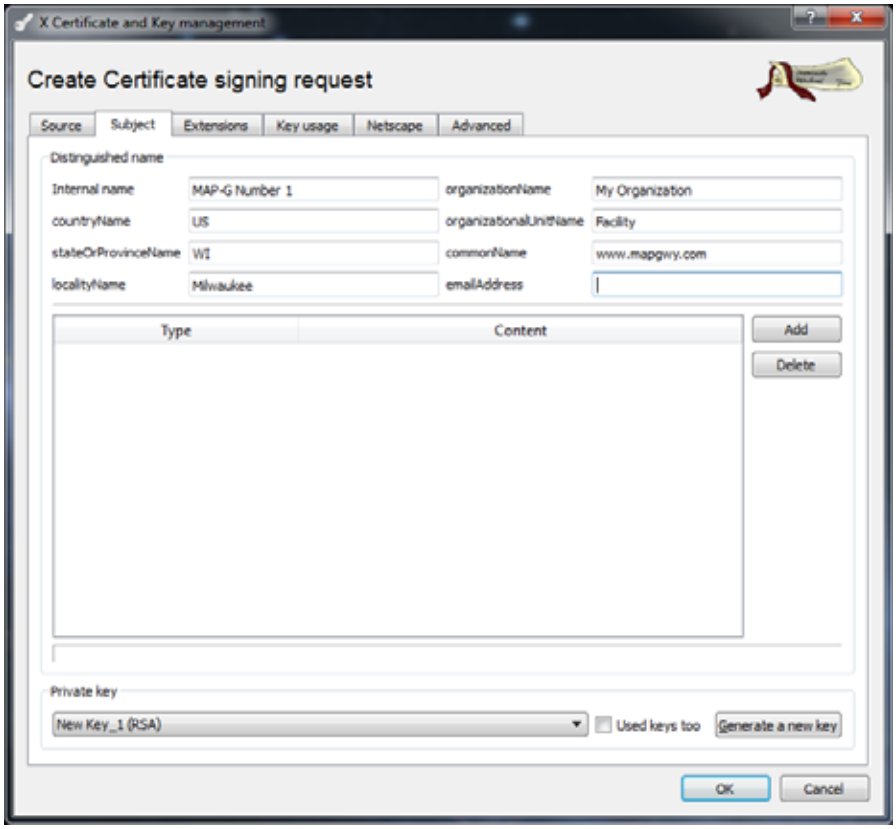
3.	**Figure 56: New CSR Subject Tab** 	In the Distinguished Name Properties window, enter the following information: • **Internal name:** This name is only used internally and does not appear in the certificate. • **organizationName:** the name of your organization • **countryName:** the country in which 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 MAP Gateway 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 New Key (RSA) 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. Select the **Extensions** tab.

Table 11: Creating the Certificate Request (CSR) (Continued)

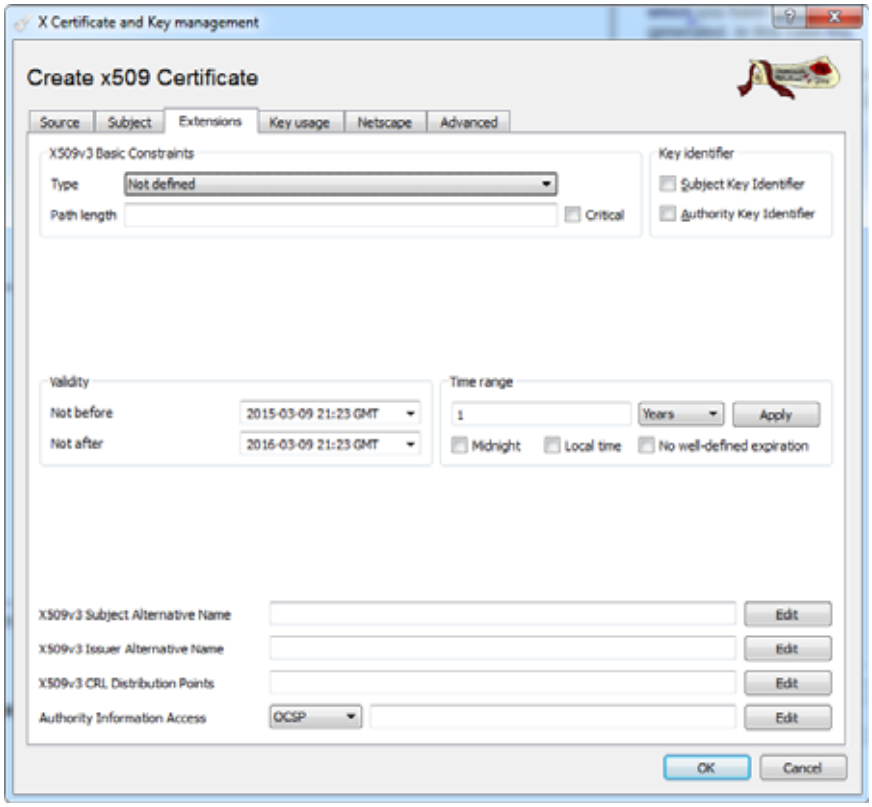
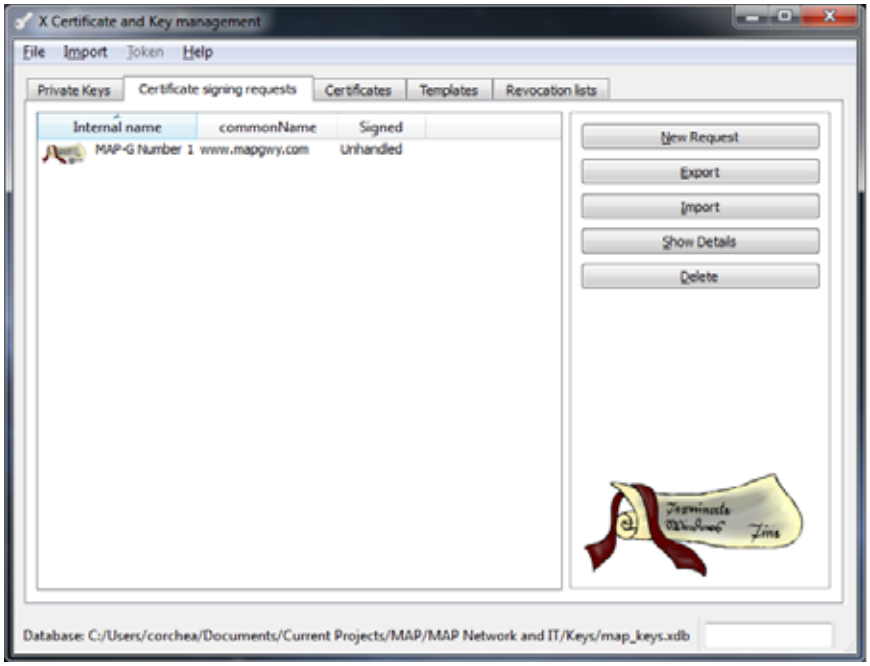
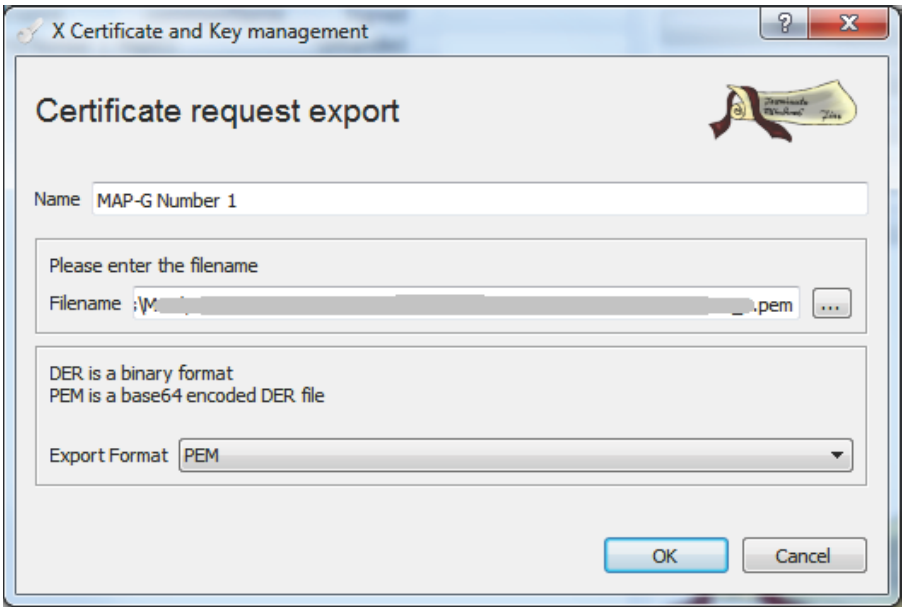
4.	**Figure 57: New CSR Extensions Tab** 	Use the **Validity** and **Time range** sections to define time limits and valid ranges for your certificate. Click **OK**.
5.	**Figure 58: New CSR Created** 	The new certificate signing request is now in your list of certificates with the internal name you assigned. Select the certificate and click **Export**.

Table 11: Creating the Certificate Request (CSR) (Continued)

6.	**Figure 59: Certificate Request Export** 	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.

Purchasing an SSL Certificate from a Public Certificate Authority

You can obtain an SSL certificate from any public certificate authority. MAP Gateway 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 the Root Certificate* to complete the process.

5136485-UTG-A-0615
Ref: LIT-12012015

York International Corporation
5005 York Drive
Norman, OK 73069