# Mobile Access Portal Gateway Network and IT Guidance Technical Bulletin

TL-MAP1810-0Px TL-MAP1810-0Sx

Code No. LIT-12012015 Software Release 4.2 Issued August 2017

Refer to the QuickLIT website for the most up-to-date version of this document.

Document Introduction	2
Concepts	2
Chain of Trust	2
Self-Signed Certificates and Certificates Signed by a Public Certificate Authority	2
Public and Private Keys	2
Man-in-the-Middle Attack	2
IP Addresses	2
Dynamic Host Configuration Protocol (DHCP)	3
Domain Name System (DNS)	3
Steps	3
Connecting to MAP Gateway the First Time	3
Connecting the MAP Gateway to Ethernet	4
Certificate Workflow	5
Generating a Private Key	5
Implementing SSL for MAP Gateway	8
Creating a Self-Signed Certificate	8
Uninstalling a Certificate on a Client That Has Connected to the MAP Gateway	12
Adding a Private Key and Certificate to MAP Gateway	21
Installing a Security Certificate on a Client That is Connecting to MAP Gateway	24
Importing a Certificate Signed by a Public CA	38
Creating a Certificate Request	42
Creating a Certificate Request (CSR)	42
Purchasing an SSL Certificate from a Public Certificate Authority	48



# **Document 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 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.

MAP Gateway is shipped with a default Johnson Controls® self signed certificate that provides secure communication. Only one certificate can be installed on MAP Gateway at a time. You will 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 need to expose the MAP Gateway UI on a public network and have browsers 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 MAP Gateway.

# 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 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 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.

- 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 (Part No. 24-10737-16)* that came with your device.
- 3. Direct your browser to www.mapgwy.com to open the MAP Gateway browser interface.
- 4. Note: MAP Gateway ships with a private mapgwy.com SSL certificate installed to ensure secure communication with the MAP Gateway. 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 MAP Gateway*.

Use your default Admin login credentials that are also included on a sticker in the *Quick Start Guide (Part No. 24-10737-16)* 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, the Change Password and Passphrase web page appears. You must change the Admin password and Wi-Fi passphrase.
  - a. **Important:** After you change the Wi-Fi passphrase or SSID the webserver restarts and you must rejoin the MAP Gateway Wi-Fi network using the new passphrase. On some mobile devices you must select and "forget" the original MAP Gateway Wi-Fi network before rejoining the network with the new passphrase.

Replace the default password in the **New Admin Password** field. Confirm the change by entering the new password in the **Verify New Admin Password** field.

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

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 Workflow**

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 certificate signed by a public certificate authority to install on the MAP Gateway device. The instructions for how to install and uninstall these certificates to establish trust between the MAP Gateway and the browser you are using varies by the browser type.



## 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 2014 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.

X Certificate and Key management	
<u>F</u> ile I <u>m</u> port <u>Token</u> <u>H</u> elp	
Private Keys Certificate signing requests Certificates	Templates Revocation lists
Internal name Type Size Use	Password New Key
	Export
	Import
	Import PFX (PKCS#12)
	Show Details
	Delete
Database: C:/Users/corchea/Documents/Current Projects/N	MAP/MAP Network and IT/Keys/map_keys.xdb

Figure 2: Key Generating Software

2. Name the new key. Select a Keytype of **RSA** and a Keysize of **2048 bit** from the respective drop-down lists. Click **Create**.

🕜 X Certifica	ate and Key management	? ×
New ke	у	
Please give a	name to the new key and select the desired keysize	
Key proper	ties	
Name	MAP-G Number 1	
Keytype	RSA	•
Keysize	2048 bit	•
Remembe	er as default	
	Create	Cancel

Figure 3: New Key Screen

3. The new key appears in your list of Private Keys. Select the private key you created and select Export.

ate Keys	Certificate	e signing req	uests	Cer	tificates	Templates	Revocatio	on lists	
Internal	name	Type	Size		Use	Passwor	ł		
AOM	AP	RSA	2048	bit	1	Common			<u>N</u> ew Key
MAP-	G Number 1	RSA	2048	bit	0	Common			<u>E</u> xport
									Import
									Import PFX (PKCS#12)
									Show Details
									Delete
								(	

#### 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 MAP Gateway. This is the file you use when *Adding a Private Key and Certificate to MAP Gateway*.

V Certificate and Key management
Export RSA key
Name MAP-G Number 1
Please enter the filename for the key.
Filename _uments/Current Projects/MAP/MAP Network and IT/Keys\MAP-G_Number_1.pem
DER is a binary format of the key without encryption PEM is a base64 encoded key with optional encryption PKCS#8 is an encrypted official Key-exchange format
Export Format PEM
When exporting the private key it should be encrypted.
Export the private part of the Key too
Export as PKCS#8
Encrypt the Key with a password
OK Cancel

Figure 5: Export Private Key

# 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 a Security Certificate on a Client That is Connecting to MAP Gateway* section. If you
  need to create a request for a certificate signed by a public CA, 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.

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

🗸 X Certificate	and Key	management				
<u>F</u> ile I <u>m</u> port	<u>T</u> oken	<u>H</u> elp				
Private Keys	Certifi	cate signing requests	Certificates	Templates	Revocation lis	its
Internal r	ame	commonName	CA Se	erial Exp	iry date	New Certificate
						Export
						Import
						Show Details
						Delete
						Import <u>P</u> KCS#12
						Import PKCS#7
						Plain View
٩		111			•	Jasmineets Dinkooo Jins
Database: C:/U	sers/corc	hea/Documents/Curr	ent Projects/M/	AP/MAP Netw	ork and IT/Ke	ys/map_keys.xdb

#### Figure 6: New Certificate

2. Accept the defaults unless they conflict with your IT policies and select the Subject Tab.

X Certificate and Key management	8
Create x509 Certificate	a Stranger (
Source Subject Extensions Key usage Netscape	Advanced
Signing request	
<ul> <li>Sign this Certificate signing request</li> <li>✓ Copy extensions from the request</li> </ul>	▼ Show request
Modify subject of the request	· · · · · · · · · · · · · · · · · · ·
~ ·	
Oreate a self signed certificate with the serial     42	
Use this Certificate for signing	•
Signature algorithm	SHA 1
Template for the new certificate	
focuord er.	Apply extensions Apply subject Apply all
	OK Cancel

Figure 7: Create the Certificate

- 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 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.

ource Subject	Extensions	Key usage	Netscape	Advanced		
Distinguished name						
Internal name	MAP-G Numbe	er 1		organizationName	My Organization	
countryName	US			organizationalUnitName	Facility	
stateOrProvinceName	WI			commonName	www.mapgwy.com	I
localityName	Milwaukee			emailAddress		
Τνρ	e			Content		Add

Figure 8: Subject Tab Properties

4. Select the **Extensions** tab.

X Certificate and Key managem	ent		? <mark>×</mark>
Create x509 Certifica	te		Command Star
Source Subject Extension	Key usage Netscape A	dvanced	
X509v3 Basic Constraints			Key identifier
Type Not defined		•	Subject Key Identifier
Path length		Critical	Authority Key Identifier
Validity Not before	2015-03-09 21:23 GMT •	Time range	Years
X509v3 Subject Alternative Name			Edit
X509v3 Issuer Alternative Name			Edit
X509v3 CRL Distribution Points			Edit
Authority Information Access	OCSP 🔻		Edit
			OK Cancel

#### Figure 9: Extensions Tab Properties

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. Select the certificate and click Export.

Figure 10: New Certificate Created

Private Keys Certificate	e signing requests Ce	ertificates	Templates	Revocation	lists
Internal name	commonName	CA	Serial	Expiry c	New Certificate
MAP-G Number	1 www.mapgwy.com		42	2016-02-23	
					Export
					Import
					Show Details
					Delete
					Import PKCS#12
					Import PKCS#7
					Plain View
	"		_		a Farminacta Otsubboo Jim

6. 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*.



Figure 11: New Certificate Export

7. Click Finish.

Figure 12: Successfully Created Certificate Message



# Uninstalling a 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 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 mapgwy.com certificate, and then tap **Remove** twice.

## Uninstalling the Security Certificate in Apple® Safari® for Mac

1. In Applications > Utilities, double-click the Keychain Access Application.

Keychains login Micrertificates Cocal Items System	Certificate	mtg.com Issued by: Johnson Cont Expires: Thursday, Marcl O This certificate is mar	rols Map Gateway h 7, 2024 at 7:17:27 A ked as trusted for "1	M Central Standard Time	
C System Roots	Name		Kind	Expires	Keychair
	🖂 (a. 1977).	the direction And	certificate	1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	login
	🖂 dagahatik		certificate	C,	login
Category	🕨 📴 💷 🗤 🖓		certificate	C , ,	login
All Items	📷 C 👘	······································	certificate		login
Passwords	🔤	ngri Assurance -	certificate		login
Casura Natas	🕨 📴 💭 💷		certificate		login
Secure Notes	Þ 📴 🖑 💷		certificate	0.000	login
My Certificates	📷 mapgwy	.com	certificate	Mar 7, 2024, 7:17:27 AM	login
🖞 Keys					
📴 Certificates					

Figure 13: Keychain Access

- 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** 1. On the Tools menu, click **Internet options**.

**Figure 14: Internet Options Selection** 



2. In the Internet Properties dialog box, click the **Content** tab, and then click **Certificates**.

**Figure 15: Internet Properties Content Tab** 

1 Internet Properties
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state Certificates Publishers
AutoComplete AutoComplete stores previous entries Settings or you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
OK Cancel Apply

3. 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.

**Figure 16: Certificates** 

Certificates				×	
Intended purpose: <a></a>	•			•	
Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ					
Issued To	Issued By	Expiratio	Friendly Name	*	
JCI Root CA	JCI Root CA	6/5/2022	<none></none>		
Johnson Controls M	Johnson Controls Map	11/24/2023	<none></none>		
Microsoft Authentic	Microsoft Authenticod	12/31/1999 12/31/2020	Microsoft Authe		
Microsoft Root Cert	Microsoft Root Certifi	5/9/2021	Microsoft Root C	=	
Microsoft Root Cert	Microsoft Root Certifi	3/22/2036	Microsoft Root C		
NO LIABILITY ACC	NO LIABILITY ACCEP	1/7/2004	VeriSign Time St		
RSA Security 2048 V3	RSA Security 2048 V3	2/22/2026	RSA Security 20		
SecureTrust CA	SecureTrust CA	12/31/2029	Trustwave	-	
Import Export	Remove		Advan	ced	
Certificate intended purpos	es				
<all></all>					
View					
Learn more about <u>certificate</u> :	2		Clos	e	

4. In the Certificates warning dialog box, click Yes. A Root Certificate Store warning appears.

Figure 17: Certificates Warning

Certificate	5	83
<b></b>	Deleting system root certificates might prevent some Windows components from working properly. The list of system critical root certificates can be reviewed at http://support.microsoft.com/?id=293781. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?	
	Yes No	

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.



Root Certif	ficate Store	×
4	Do you want to DELETE the following certificate from the Root Store? Subject : admin@jci.com, Building Efficiency, Johnson Controls Map Gateway, Milwaukee, Johnson Controls, WI, US Issuer : Self Issued Time Validity : Tuesday, November 26, 2013 through Friday, November 24, 2023 Serial Number : 00F69EB9 112CCFE6 7A Thumbprint (sha1) : D665FD37 046FC140 5E35B7E6 2CF55482 CFA83E70 Thumbprint (md5) : D30D63DE 9CACC4C6 4C53450D 86196750	
	Yes No	

6. In the Certificates dialog box, click **Close**, and then click **OK**.

Figure 19: Trusted Root Certification Authorities Tab

Certificates				×		
Intended purpose: <a></a>						
Intermediate Certification Au	Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ					
Issued To	Issued By	Expiratio	Friendly Name	*		
JCI Root CA	JCI Root CA	6/5/2022	<none></none>			
Johnson Controls M Microsoft Authentic Microsoft Root Aut Microsoft Root Cert Microsoft Root Cert NO LIABILITY ACC RSA Security 2048 V3 SecureTrust CA	Johnson Controls Map Microsoft Authenticod Microsoft Root Authority Microsoft Root Certifi Microsoft Root Certifi NO LIABILITY ACCEP RSA Security 2048 V3 SecureTrust CA	11/24/2023 12/31/1999 12/31/2020 5/9/2021 3/22/2036 1/7/2004 2/22/2026 12/31/2029	<none> Microsoft Authe Microsoft Root A Microsoft Root C VeriSign Time St RSA Security 20 Trustwave Advan</none>	T ced		
Certificate intended purpose <all></all>	25		View			
Learn more about <u>certificates</u>	i.		Clos	e		

### Uninstalling a Certificate in Google® Chrome™

1. Click the Customize and control Google Chrome button

Ξ

and select Settings.

Figure 20: Google Chrome Customize and control Google Chrome menu

	☆ <b>=</b>
New tab	Ctrl+T
New window	Ctrl+N
New incognito window	Ctrl+Shift+N
Bookmarks	Þ
Recent Tabs	►.
Edit Cut	Copy Paste
Zoom – 100	% + []
Save page as	Ctrl+S
Find	Ctrl+F
Print	Ctrl+P
Tools	►.
History	Ctrl+H
Downloads	Ctrl+J
Sign in to Chrome	
Settings	
About Google Chrome	
Help	
Exit	

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

Figure 21: Advanced Settings

Default browser



3. Scroll to the HTTPS/SSL section click Manage certificates and select the Trusted Root Certification Authorities tab.

# Figure 22: HTTPS/SSL

HTTPS/SSL

Manage certificates...

Check for server certificate revocation

4. Select the Johnson Controls authority, and then click **Remove**. A Certificates warning appears.

Figure 23: Trusted Root Certification Authority Tab

Certificates							×
Intended purpose:	<all></all>						•
Intermediate Certifica	ation Au	Ithorities	Trusted Root C	ertification Aut	horities	Trusted Pub	4
Issued To		Issued B	у	Expiratio	Friend	y Name	*
AddTrust Exter America Online Baltimore Cyber Class 3 Public P Class 3 Public P Copyright (c) 19 Copyright (c) 19 DigiCert Assure DigiCert High As Entrust Root Ce	nal Roo rTru rima 997 d ID ssur ertifi	AddTrus America Baltimore Class 3 P Class 3 P Copyrigh DigiCert DigiCert Entrust P	t External CA Online Root CyberTrust Public Primary Public Primary Aut (c) 1997 Mi Assured ID R High Assuran Root Certifica	5/30/2020 11/19/2037 5/12/2025 8/1/2028 1/7/2004 12/30/1999 11/9/2031 11/9/2031 11/27/2026	USERTI Americi Baltimo VeriSig VeriSig Microso DigiCer DigiCer Entrusi	rust a Online R ore Cyber n Class 3 n oft Timest t t	THE
Import Ex	port	R	emove			Advan	iced
Certificate intended p	ourpose	S					
						View	
Learn more about cert	tificates					Clos	e

5. Click Yes. The certificate is removed immediately.

# Figure 24: Certificate Removal Warning

Certificates	
<u>^</u>	Certificates that are issued by the certification authorities or any subordinate certification authorities will no longer be trusted. Do you want to delete the certificate(s)?
	<u>Y</u> es <u>N</u> o

# 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.
- 1. Connect to MAP Gateway 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 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.



Figure 25: MAP Gateway UI Device List

3. Click Settings and select SSL.

🔹 Settings: SSL - Map Gatew 🗙 🚺					x
← → C 🕼 bttps://10.9.40.45	/#settings/ssl	x 🖡	0	w	≡
🔹 MAP Gateway Login  👻 System Dashb	oard 뷇 JCI Document Mana 🧔 Device List - Map Ga				
Choose a device 🔻	settings SSL				Î
< Menu	Current Certificate				
Settings	mapgwy.com Private Kev				
Wifi		1			
Ethernet					
SSL					
Software Updates					
Administration					=
About	New Catificate				
Diagnostics	New Certificate				
BACnet Time Sync					
		1			
OS Version: 201501211430	Cancel				Ļ

#### Figure 26: MAP Gateway SSL Screen

- 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.
- 8. To apply the new certificate and private key, the MAP Gateway 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 MAP Gateway goes offline while restarting and displays the 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.

## Figure 27: Reset Warning Screen



9. When the connection is reestablished, log in to MAP Gateway and use normally.

Figure 28: Device Resetting Screen



# Installing a Security Certificate on a Client That is Connecting to MAP Gateway

Until the security certificate for the MAP Gateway is added as a trusted certificate, you receive a security alert every time you visit the **www.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.





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.
- 4. Click Continue.

	Safari can't verify the identity of the website "mapgwy.com". The certificate for this website is invalid. You might be connecting to a website that is pretending to be "192.168.0.1", which could put your confidential information at risk. Would you like to connect to the website anyway?
🗹 Always trus	t "mapgwy.com" when connecting to "mapgwy.com"
📷 mapgwy.	com
Certificate	mapgwy.com Issued by: Johnson Controls Map Gateway Expires: Thursday, March 7, 2024 at 7:17:27 AM Central Standard Time This certificate is not valid (host name mismatch)
▶ Details	
?	Hide Certificate         Cancel         Continue

# Figure 30: Trust MAP Gateway Identity Screen

# Installing the Security Certificate in Internet Explorer

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

## Figure 31: Internet Options Selection

inson Controls,	🔓 🏷 🏶
Print	•
File	+
Zoom (100%)	+
Safety	+
Add site to Start menu	
View downloads	Ctrl+J
Manage add-ons	
F12 developer tools	
Go to pinned sites	
Internet options	
About Internet Explorer	

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

#### Figure 32: Internet Properties Content Tab

😢 Internet Properties	? ×
General Security Privacy Content Connections Programs Adv	vanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.	
Enable 🛞 Settings	
Certificates	
Use certificates for encrypted connections and identification	on.
Clear SSL state Certificates D Publishers	
AutoComplete	
on webpages and suggests matches	
Feeds and Web Slices	
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.	
OK Cancel A	pply

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

Certificates				×
Intended purpose: <a>All&gt;</a> Intermediate Certification Au	uthorities Trusted Root Co	ertification Aut	horities Trusted Publ	•
Issued To	Issued By	Expiratio	Friendly Name	*
AddTrust External America Online Roo Baltimore CyberTru Class 3 Public Prima Class 3 Public Prima Copyright (c) 1997 DigiCert Assured ID DigiCert High Assur Entrust Root Certifi	AddTrust External CA America Online Root Baltimore CyberTrust Class 3 Public Primary Class 3 Public Primary Copyright (c) 1997 Mi DigiCert Assured ID R DigiCert High Assuran Entrust Root Certifica	5/30/2020 11/19/2037 5/12/2025 8/1/2028 1/7/2004 12/30/1999 11/9/2031 11/9/2031 11/27/2026	USERTrust America Online R Baltimore Cyber VeriSign Class 3 VeriSign Microsoft Timest DigiCert DigiCert Entrust	4
Import Export Certificate intended purpose	Remove		Advan	iced
Learn more about <u>certificates</u>	1		Clos	e

Figure 33: Trusted Root Certification Authorities Tab

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



#### Figure 34: Certificate Install Wizard

- 6. 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 certificate for each new MAP Gateway device that you use.

Certificate Import Wizard	×			
File to Import				
Specify the file you want to import.				
<u>Fi</u> le name:				
C Laser California (rootCA.pem Browse				
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 Serialized Certificate Store (.SST)				
Learn more about <u>certificate file formats</u>				
< <u>B</u> ack <u>N</u> ext > Cance	2			

Figure 35: Certificate Import Wizard - Select File to Import

7. 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**.

Certificate Import Wizard					
-	Certificate Store Certificate stores are system areas where certificates are kept.				
	Windows can automatically select a certificate store, or you can specify a location for the certificate.				
	$\bigcirc$ Automatically select the certificate store based on the type of certificate				
	Place all certificates in the following store				
	Certificate store:				
	Trusted Root Certification Authorities Browse				
	Learn more about <u>certificate stores</u>				
_					
	< Back Next > Canc	el			

Figure 36: Certificate Import Wizard Certificate Store

8. In the Security Warning dialog box, click **Yes**.

Figure	37.	Certificate	Import	Wizard	Security	Warning
Iguie	57.	Certificate	mport	<b>VVIZAI</b> U	occurry	wanning

Security W	arning	×
	You are about to install a certificate from a certification authority (CA) claiming to represent: Johnson Controls Map Gateway Windows cannot validate that the certificate is actually from "Johnson Controls Map Gateway". You should confirm its origin by contacting "Johnson Controls Map Gateway". The following number will assist you in this process: Thumbprint (sha1): D665FD37 046FC140 5E35B7E6 2CF55482 CFA83E70	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?	
	Yes No	

9. Click **Finish**. A success message appears.

## Figure 38: Wizard Complete



10. Click **OK**.

### Installing the Security Certificate in Google® Chrome™

- 1. Navigate to www.mapgwy.com/ downloadtlsprofile, and then download the rootCA.pem file.
- 2. On the Chrome menu (  $\equiv$  ), click **Settings**.

	5
New tab	Ctrl+T
New window	Ctrl+N
New incognito window	Ctrl+Shift+N
Bookmarks	
Recent Tabs	
Edit Cut	Copy Paste
Zoom - 1009	% + []]
Save page as	Ctrl+S
Find	Ctrl+F
Print	Ctrl+P
Tools	
History	Ctrl+H
Downloads	Ctrl+J
Sign in to Chrome	
Settings	
About Google Chrome	
Help	
Exit	

#### Figure 39: Chrome Settings Menu

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

Figure 40: Advanced Settings Selection

Default browser

Make Google Chrome my default browser

Google Chrome is not currently your default browser.



4. Under HTTPS/SSL, click Manage certificates.

Figure 41: Manage Certificates

# HTTPS/SSL

Manage certificates...

Check for server certificate revocation

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

Certificates						
Intended purpose: <a></a>				•		
Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ						
Issued To	Issued By	Expiratio	Friendly Name	<b>^</b>		
AddTrust External America Online Roo Baltimore CyberTru Class 3 Public Prima Class 3 Public Prima Class 3 Public Prima Copyright (c) 1997 DigiCert Assured ID DigiCert High Assur Entrust Root Certifi	AddTrust External CA America Online Root Baltimore CyberTrust Class 3 Public Primary Class 3 Public Primary Copyright (c) 1997 Mi DigiCert Assured ID R DigiCert High Assuran Entrust Root Certifica	5/30/2020 11/19/2037 5/12/2025 8/1/2028 1/7/2004 12/30/1999 11/9/2031 11/9/2031 11/27/2026	USERTrust America Online R Baltimore Cyber VeriSign Class 3 VeriSign Microsoft Timest DigiCert DigiCert Entrust	Ŧ		
Import Export Certificate intended purpose	Remove		Advar	nced		
Learn more about <u>certificates</u>			Clos	æ		

Figure 42: Chrome SSL Certificates

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



#### Figure 43: Certificate Install 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 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 certificate for each new MAP Gateway device that you use.

Certificate Import Wizard	x			
File to Import				
Specify the file you want to import.				
<u>F</u> ile name:				
C Laser California VrootCA.pem Browse				
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 Serialized Certificate Store (.SST)				
Learn more about <u>certificate file formats</u>				
< <u>B</u> ack <u>N</u> ext > Cancel				

Figure 44: 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**.

rigule 40. Certificate impo		eolore
rtificate Import Wizard		
Certificate Store		
Certificate stores are system areas where	certificates are kept.	
Windows can automatically select a certificate the certificate.	ate store, or you can spec	ify a location for
Automatically select the certificate select	tore based on the type of	certificate
Place all certificates in the following s	store	
Certificate store:		
Trusted Root Certification Authorit	ies	Browse
Learn more about <u>certificate stores</u>		
	< Back Next	> Cancel

Figure 45: Certificate Import Wizard - Certificate Store

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





10. Click Finish. A success message appears.

#### Figure 47: Certificate Install Wizard Success



11. Click OK.

# Importing a Certificate Signed by a Public CA

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

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

Issued To	Issued By	Expiratio	Friendly Name
AddTrust External America Online Ro Baltimore CyberTru Class 3 Public Prima Class 3 Public Prima Copyright (c) 1997 DigiCert Assured ID DigiCert High Assur Entrust Root Certifi	AddTrust External CA America Online Root Baltimore CyberTrust Class 3 Public Primary Class 3 Public Primary Copyright (c) 1997 Mi DigiCert Assured ID R DigiCert High Assuran Entrust Root Certifica	5/30/2020 11/19/2037 5/12/2025 8/1/2028 1/7/2004 12/30/1999 11/9/2031 11/9/2031 11/27/2026	USERTrust America Online R Baltimore Cyber VeriSign Class 3 VeriSign Microsoft Timest DigiCert DigiCert Entrust
Import Export	Remove		Advar

Figure 48: The Certificates Dialog Box

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

Figure 49: 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 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 security certificate for each new MAP Gateway device that you use.

Certificate Import Wizard
File to Import
Specify the file you want to import.
<u>F</u> ile name:
Chamiltain mCamiltan (rootCA.pem Browse
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 Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< <u>B</u> ack <u>N</u> ext > Cancel

### Figure 50: Importing the Certificate

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**.

Certificate Import Wizard	×				
Certificate Store					
Certificate stores are system areas where certificates are kept.					
Windows can automatically select a certificate store, or you can specify a location for the certificate.					
$\bigcirc$ Automatically select the certificate store based on the type of certificate					
Place all certificates in the following store					
Certificate store:					
Trusted Root Certification Authorities Browse					
Leare more about contificate stores					
Learn more about <u>certificate stores</u>					
< Back Next > Cance	el				

#### Figure 51: Certificate Store Options

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

Figure 52: Non-Validated Certificate Security Warning



6. Click Finish. A success message appears.

#### Figure 53: The Certificate Import Success Message



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.

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.

X Certificate and Key management					
<u>File Import Token H</u> elp					
Private Keys Certificate signing requests	Certificates	Templates	Revocation li	ists	
Internal name commonName	Signed			New Request	
				Export	
				Import	
				Show Details	
				Delete	
				Assumaces Dingroof Zins	
Database: C:/Users/corchea/Documents/Current Projects/MAP/MAP Network and IT/Keys/map_keys.xdb					

Figure 54: New Certificate Signing Request Tab

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. Accept the defaults (SHA1 and [default]CA) unless they conflict with your IT policies and click the **Subject** tab.

X Certificate and Key management	? ×
Create Certificate signing request	Constant Product Tax
Source Subject Extensions Key usage Netscape	Advanced
Signing request	
unstructuredName	
challengePassword	
Signing <ul> <li>Greate a self signed certificate with the serial</li> <li>Use this Certificate for signing</li> </ul>	
Signature algorithm	SHA 1
Template for the new certificate	
[default] CA	•
	Apply extensions Apply subject Apply all
	OK Cancel

Figure 55: Create CSR Source Screen

- 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 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.
- 4. Select the **Extensions** tab.

of X Certificate and Key n	nanagement		? ×		
Create Certifica	ate signing request		(a) pressure 7744		
Source Subject I	Extensions Key usage Netscape	Advanced			
Distinguished name					
Internal name	MAP-G Number 1	organizationName	My Organization		
countryName	US	organizationalUnitName	Facility		
stateOrProvinceName	WI	commonName	www.mapgwy.com		
localityName	Milwaukee	emailAddress			
Тур	e	Content	Add		
			Delete		
Private key					
New Key_1 (RSA)		•	Used keys too Generate a new key		
OK Cancel					

Figure 56: New CSR Subject Tab

5. Use the Validity and Time range sections to define time limits and valid ranges for your certificate. Click OK.

🔗 X Certificate and Key managem	ent	<u>१</u> ×
Create x509 Certifica	te	() annual gran
Source Subject Extension	Key usage Netscape Advan	iced
X509v3 Basic Constraints		Key identifier
Type Not defined		Subject Key Identifier
Path length		Critical
Validity Not before Not after	2015-03-09 21:23 GMT ▼ 2016-03-09 21:23 GMT ▼	Years  Apply Midnight Local time No well-defined expiration
X509v3 Subject Alternative Name X509v3 Issuer Alternative Name X509v3 CRL Distribution Points Authority Information Access	OCSP T	Edit Edit Edit Edit
		OK Cancel

Figure 57: New CSR Extensions Tab

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

X Certificate and Key management		
<u>F</u> ile I <u>m</u> port <u>T</u> oken <u>H</u> elp		
Private Keys Certificate signing requests Certificates Templates Revocation	on lists	
Internal name commonName Signed	New Request	
MAP-G Number 1 www.mapgwy.com Unnancied	Export	
	Import	
	Show Details	
	Delete	
	Forminate Dunbowe Zins	
Database: C:/Users/corchea/Documents/Current Projects/MAP/MAP Network and IT/Keys/map_keys.xdb		

Figure 58: New CSR Created

7. 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.

X Certificate and Key management	? ×
Certificate request export	A Terminate The Read To A
Name MAP-G Number 1	
Please enter the filename Filename	pem
DER is a binary format PEM is a base64 encoded DER file	
Export Format PEM	
	OK Cancel

Figure 59: Certificate Request Export

# 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 <a href="https://www.namecheap.com/">https://www.namecheap.com/</a>. 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.



Building Technologies & Solutions 507 E. Michigan Street, Milwaukee, WI 53202

Metasys® and Johnson Controls® are registered trademarks of Johnson Controls. All other marks herein are the marks of their respective owners.© 2017 Johnson Controls

Published in U.S.A.