Mobile Access Portal Gateway Installation Instructions

Part No. 24-10737-8, Rev. B
Software Release 2.0
Issued September 1, 2014

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

Applications

The Mobile Access Portal (MAP) Gateway is a local display replacement solution that enables users to leverage the power of mobility using smart phones, tablets, or laptop computers to interact with building automation equipment controls. The MAP Gateway serves up web pages through a built-in Wi-Fi access point, which allows users to view and in some cases edit equipment controller configuration parameters, setpoints, schedules, and alarms through a browser. A mobile application is not required to use the MAP Gateway with your mobile device.

The wireless connection on the MAP Gateway allows users of a supported mobile device to be up to 30 m (100 ft, line of sight) away indoors and up to 91 m (300 ft, line of sight) away outdoors. Power may be supplied via the SAB (sensor/actuator bus), the FCB (field controller bus), or a micro USB port.

When used as a portable device, the MAP Gateway can be strung using a lanyard. In this configuration, the MAP Gateway can be carried from site to site, depending on the needs and workflow of field personnel.

North American Emissions Compliance

United States

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference, in which case the users will be required to correct the interference at their own expense.

RF Transmitters: Compliance Statement (Part 15.19)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning (Part 15.21)

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure (OET Bulletin 65)

To comply with FCC RF exposure requirements for mobile transmitting devices, this transmitter should only be used or installed at locations where there is at least 20 cm separation distance between the antenna and all persons.

Industry Canada Statement

The term **IC** before the certification/registration number only signifies that the Industry Canada technical specifications were met.

Le terme « IC » précédant le numéro d'accréditation/inscription signifie simplement que le produit est conforme aux spécifications techniques d'Industry Canada.

Installation

Observe the following guidelines:

- Verify that all parts shipped with the MAP Gateway.
- Keep the unit encased in the protective shell. If not protected by the enclosure in which it ships, the MAP Gateway may be subject to physical damage.

Parts Included (Portable Configuration)

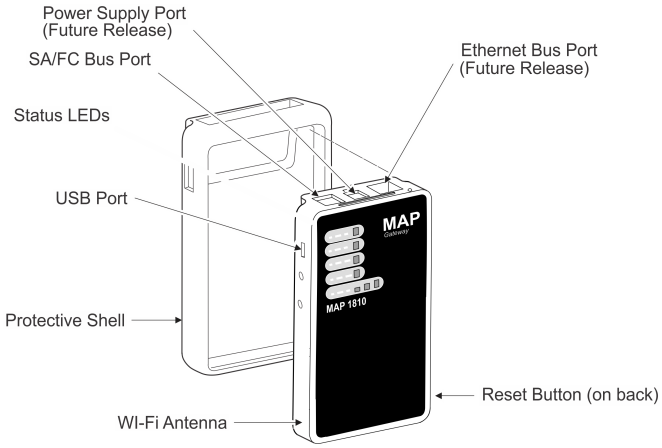
- MAP Gateway
- Protective shell
- 6-pin RJ-12 connector cable
- Lanyard
- Installation Instructions
- Quick Start Guide

Special Tools Needed

To use the MAP Gateway, you need a mobile device (tablet or smart phone) or computer (laptop or desktop) that supports Wi-Fi.

Features

Figure 1: MAP Gateway Features (Portable Unit)



Portable Use

When used as a portable unit, the MAP Gateway should be housed in the supplied shell. During use, the unit can be temporarily hung on nearby equipment using the supplied lanyard.

CAUTION

Risk of Personal Injury. Do not wear or hold the MAP Gateway during use, and only use or install the MAP Gateway at locations where there is at least 20 cm between the built-in antenna and all persons. Failure to do so may result in minor or moderate personal injury.

MISE EN GARDE:

Risque de blessure. Ne pas porter ou soutenir l'MAP Gateway durant son utilisation et utiliser ou installer l'MAP Gateway uniquement à un emplacement offrant une distance minimum de 20 cm entre l'antenne intégrée et toute personne. Le non-respect de cette précaution risque de provoquer des blessures légères ou de gravité modérée.

Observe the following guidelines when using a portable MAP Gateway:

- Do not use the RJ-12 cable to support the weight of the MAP Gateway. Use the lanyard to support it.
- Keep the MAP Gateway in the protective shell with which it ships. To insert the MAP Gateway into the shell, stretch the shell edges and slide the MAP Gateway unit into place (*Figure 2*). This shell protects the unit from drops up to 1.22 m (4 ft).
- The MAP Gateway has not been designed for prolonged outdoor use. Leaving it in outdoor environments (such as inside roof top units) may result in damage.
- Objects (including ductwork, cabinets, doors, and glass) can impede the wireless signal. Minimize the number of objects between the connected computer or mobile device and the MAP Gateway. Use line of sight, if possible.
- Metal objects (such as cabinet doors, enclosures and pipes) and concrete objects (such as pillars, walls and ceilings) may limit Wi-Fi service limits. To accommodate potential structural obstacles on site, the MAP Gateway can be mounted flat or on the side.

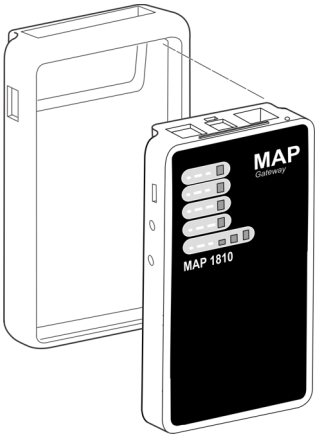
CAUTION

Risk of Property Damage. Do not use the RJ-12 cable or any other field bus cable or electrical cable to support the weight of the MAP Gateway. Hanging the MAP Gateway from anything other than the supplied lanyard may result in damage to the product or peripheral equipment.

MISE EN GARDE:

Risque de dégâts matériels. Ne pas utiliser le câble RJ-12 ou tout autre câble de bus de terrain ou câble électrique pour soutenir le poids de l'MAP Gateway. La suspension de l'MAP Gateway à tout autre élément que la longe fournie risque d'endommager le produit ou les équipements périphériques.

Figure 2: Portable MAP Gateway and Protective Shell



Wiring

Wiring Consideration and Guidelines

Observe the following guidelines when wiring the MAP Gateway:

- Do not allow the MAP Gateway to hang from the cable connection.
- Provide some slack in the cable between the MAP Gateway and the controller.

SA/FC Port

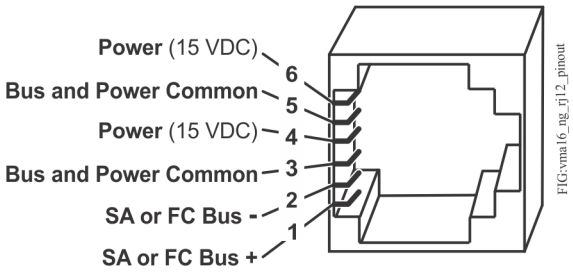
The MAP Gateway has one RS-485 FC/SA bus port that connects through a supplied 6-pin modular jack and cable assembly. For data transmission and voltage specifications, see the *Technical Specifications* section.

Do not plug the SA/FC connector into a standard phone jack.

See the *Features* section for the location of the communications terminal on the MAP Gateway.

Figure 3: SA/FC Port Pin

(RJ-12 Modular Jack)



Field Bus Communications Connections

To connect the MAP Gateway to the SA/FC field bus for communication, connect one end of the RJ-12 cable to the MAP Gateway and the other end of the cable to a controller or network sensor.

Note: The MAP Gateway has a dedicated MS/TP bus address of 03. The number of MAP Gateway units that can be connected simultaneously to one MS/TP bus depends on the number of FC and SA ports available and connected to the bus. The MS/TP bus can accommodate one MAP Gateway on the FC bus and one MAP Gateway for each SA bus connected to the trunk.

Performance of the MAP Gateway varies based on the number of SA bus connections and amount of traffic.

Operation

Accessing Controllers Using the MAP Gateway

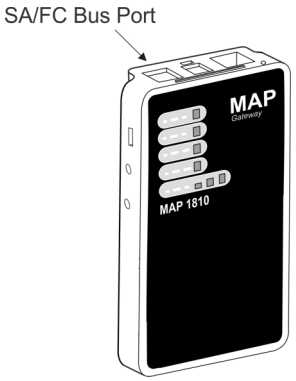
Once the MAP Gateway is physically connected to the MS/TP network, users have access to all devices on the network.

To interact with a device or product on the network (to view devices, setpoints, or view alarms), users select the device using a web-enabled device that is connected to the MAP Gateway Wi-Fi network. To use the network, users must have a web-enabled device that uses a supported Internet browser. For information on connecting to the network, see *Connecting to the MAP Gateway Wi-Fi Network*.

Connecting to the MAP Gateway Wi-Fi Network

1. To physically connect the MAP Gateway to your equipment, plug one end of the supplied RJ-12 cable to the SA/FC bus port of your equipment, and plug the other end of the RJ-12 cable to the SA/FC port on the MAP Gateway (*Figure 4*).

Figure 4: Connecting the Portable MAP Gateway to Your Equipment



2. Wait for the Wi-Fi LEDs on the MAP Gateway to begin flashing in succession (scanning). The unit is now ready for a device to connect to its Wi-Fi network.
3. In the Wi-Fi settings of your mobile device or laptop, connect to the MAP Gateway Wi-Fi network. If this is your first time using the device, use the default SSID and passphrase provided in the Quick Start Guide that shipped with your device.
4. Open a web browser to access the MAP Gateway interface. If it is your first time connecting to the MAP Gateway Wi-Fi network, you are prompted to install a secure certificate. Follow on-screen instructions or see *Installing the Root Certificate* in the *Appendix: Root Certificates* for more information.

   Note: A secure certificate is a file installed on a user's mobile device or computer that identifies the MAP Gateway as a trusted website. This digital certificate establishes the identity and authenticity of Johnson Controls as secure and reliable.

   Note: The MAP Gateway should direct you to the device's internal website, www.mapgwy.com. If it does not, direct your browser to www.mapgwy.com.

   Note: If you do not import the security certificate as a trusted root certificate, the website www.mapgwy.com appears as an untrusted URL in your browser. For information on importing the security certificate as a trusted root certificate, see *Importing the Root Certificate* in the *Appendix: Root Certificates*.
5. Log in to the MAP Gateway network. If this is your first time using the device, use the default login information provided in the Quick Start Guide that shipped with your device.

Once the MAP Gateway is physically connected to the MS/TP network, all devices on the network that have an equipment number are available.

To interact with a device or product on the network (to view devices, set points, or view alarms), select a device using the mobile device that is connected to the MAP Gateway.

Reset Button Operation and Descriptions

If you lose your password or if you want to restore the unit to factory defaults, the MAP Gateway offers two reset functions: a Reset SSID and Passphrase function that resets Wi-Fi settings, and a Reset to Factory Defaults function that resets all unit settings (including user profiles).

The Reset SSID and Passphrase function is intended for individuals who forget their Wi-Fi connection information, and the Reset to Factory Defaults function is for use by administrators who may want to clear all user profiles from a device. For information on resetting the unit, see *Table 1*.

Important:	To use a unit that is reset to factory defaults, you must have the default login information supplied in the Quick Start Guide that shipped with the unit.

The reset button is on the back of the device, and it is embedded into the MAP Gateway housing so that it cannot be activated by accident. To reach the reset button, use a small screwdriver or similar tool.

- If you are connected to the network when you use the reset button, you are disconnected.
- If you press the reset button for more than nine seconds, the reset operation is cancelled.
- If a fault condition already exists, the reset button is disabled.

Figure 5: Using the Reset Button

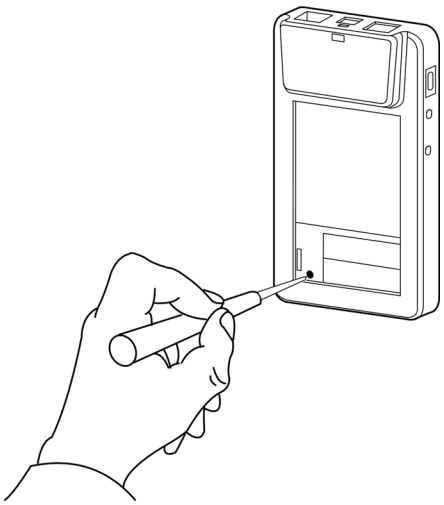


Table 1: Reset Button Operation and Descriptions

Reset Function	Reset Operation[2]
Reset SSID and Passphrase	1. Press and hold the reset button for 2 seconds. The Fault LED displays Slow Flicker behavior. 2. Release the reset button within 3 seconds. The Fault LED displays Fast Flicker behavior. 3. Within 5 seconds, press the reset button again, and then immediately release it. (If you press the reset button for longer than 5 seconds, the reset operation is cancelled.) The SSID and passphrase are reset to factory defaults, the LEDs stop flickering for 2 seconds, and then the LEDs return to normal operation, based on the current state of the device.
Reset to Factory Defaults[1]	1. Press and hold the reset button for 6 seconds. The Fault LED displays Slow Flicker behavior. 2. Release the reset button within 3 seconds. The Fault LED displays Fast Flicker behavior. 3. Within 5 seconds, press the reset button again, and then immediately release it. (If you press the reset button for longer than 5 seconds, the reset operation is cancelled.) 4. All unit settings are reset to factory defaults, the LEDs stop flashing for 2 seconds, and then the LEDs return to normal operation, based on the current state of the device.

1 Resets all unit settings, including user profiles.
2 For information on LED designations and flicker behavior, see *Table 2*.

Status Indication LEDs

The MAP Gateway communicates status via LEDs.The following functional states are indicated using LEDs:

- power
- fault
- SA/FC bus communication
- Ethernet communication
- Wi-Fi strength

See *MAP Gateway LED Designations and Descriptions* for a comprehensive list of MAP Gateway LED functional information.

MAP Gateway LED Designations and Descriptions

Table 2: LED Designations and Descriptions

LED Name	Color	Normal	Descriptions/Other Conditions
Power	**Green**	On Steady (no flashing)	Off = No power On Steady = Power supplied by primary voltage
Fault	**Red**	Off	Off = No faults/normal operation On Steady = Missing hardware, missing software, operating system has not yet initialized, or reset is in progress. Slow Flicker (1/2 second/.5 Hz) = Startup sequence Medium Flicker (2 seconds/2 Hz) = Software upgrade in progress Fast Flicker (5 seconds/5 Hz) = Fault
SA/FC Bus	**Green**	Flicker	Off = Receiving data On Steady = Transmitting data Flicker = Data transmission
Ethernet	**Green**	On Steady	Off = Communication not established On Steady = Communication established Flicker = Data transmission
Wi-Fi	**Yellow**	On Steady	Off = No Wi-Fi signal Wi-Fi strength is indicated by the number of LEDs that are lit, with one lit LED indicating weak wireless signal strength (between 1% and 49%) and three lit LEDs indicating excellent wireless signal strength (at least 75%).

LED Test Sequence at Startup

During startup, the MAP Gateway automatically initiates a self-test to verify proper operation of the unit. Immediately after connecting supply power, the following LED lighting sequence occurs:

1. The Power LED turns on, and stays lit.
2. The Fault LED indicator flashes for approximately 40 seconds, then turns off when the MAP Gateway is fully functional.
3. The Wi-Fi LEDs light up in succession (scanning), indicating that the MAP Gateway is waiting for a device to join its Wi-Fi network.

Repair Information

If the MAP Gateway fails to operate within its specifications, replace it. The MAP Gateway is not a serviceable product; however, it does support software updates to enable feature enhancements. For a replacement unit, software updates or accessories, contact the nearest Johnson Controls® representative.

Do not open the MAP Gateway housing. The MAP Gateway has no user-serviceable parts inside.

The MAP Gateway requires no periodic field maintenance.

Troubleshooting

Table 3: Launch Issues Troubleshooting Information

Problem	Resolution
You are not directed to the MAP Gateway login page when you launch a web browser.	**Reason** Device behavior can vary based on the device and Internet browser in use. For instance, some devices cache browser information and do not automatically redirect users to the MAP Gateway login page when the browser is launched. **Resolution** Direct your browser to www.mapgwy.com.
After the controller or HVAC device to which a MAP Gateway is connected is upgraded, the connected MAP Gateway no longer displays active or current data.	**Resolution** Unplug the MAP Gateway from the SA (sensor actuator) or FC (field controller) bus, then plug the MAP Gateway back in. **Resolution**
Every time I install the SSL certificate on my device, it asks me to re-install it. What should I do?	**Resolution** 1. Verify the time on your client device is correct. If the device time is not current (for example, after a hard reset), please close the browser, set the time, and then try to install the certificate. 2. Check your Web Browser Settings and verify that Cookies are enabled.

Technical Specifications

Table 4: MAP Gateway

Product Code[1]	**TL-MAP1810-0Px:** Metasys®/FX Portable MAP Gateway (Includes MAP Gateway, RJ-12 cable, bumper guard, and lanyard.) US-compatible countries.
Power Consumption	From SA/FC bus: 15 VDC at 2.7 VA maximum
Ambient Temperature Conditions	**Operating:** 0 to 50°C (32 to 122°F) **Operating Survival:** -30 to 60°C (-22 to 140°F) **Non-Operating:** -40 to 70°C (-40 to 158°F)
Ambient Humidity Conditions	**Storage:** -40 to 70°C (-40 to 158°F); 5 to 95% RH 30°C (86°F) maximum dew point conditions **Operating:** -40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point conditions
Transmission Power (Typical)	**Wireless Local Area Network (WLAN) Transmission Power:** +14.5 dBm, 54 Mbps +12.5 dBm, 65 Mbps

Table 4: MAP Gateway

WLAN Receiver Sensitivity (Typical)	-76 dBm, 10% packet error rate (PER), 54 Mbps -73 dBm, 10% PER, 65 Mbps
Transmission Speeds	**Wireless Communication:** 2.4 GHz ISM bands, 802.11 b/g/n, 11/22/54 Mbps **Serial Communication (SA/FC Bus):** 9600, 19.2k, 38.4k, or 115.2k bps
Transmission Range (Typical)	**Wireless Communication:** 30 m (100 ft) line-of-sight indoors 91 m (300 ft) line-of-sight outdoors **WLAN Range Performance:** 0 - 50 ft = Excellent 50 - 100 ft = Good 100 - 300 ft = Weakest, approaching out of range
Wireless Security	WPA2-PSK TKIP (Wi-Fi Protected Access Pre-Shared Key mode Temporal Key Integrity Protocol)
Network and Serial Interfaces	One SA/FC port (6-pin port; connects with 1.5 m [4.9 ft] RJ-12 field bus cable) One USB port (Micro-B port; 2.0; supports Open Host Controller Interface [Open HCI] specification)
Dimensions **(H x W x D)**	Unit alone: 120 x 70 x 24.5 mm (4-23/32 x 2-3/4 x 31/32 in. when used vertically) Unit in shell: 128 x 75 x 29.5 mm (5-1/32 x 2-61/64 x 1-5/32 in. when used vertically)
Housing	White Acrylonitrile butadiene styrene (ABS) bracket Black silicone shell
Weight	Unit alone: 0.10 kg (0.22 lb) Unit in shell: 0.15 kg (0.33 lb) **Note:** Weights do not include any peripheral components such as cables, lanyard, or an external power supply.
Web Browser Requirements for Computers and Handheld Devices	**Computer:** Windows® Internet Explorer® 10, Apple® Safari® 6.1 and later **Handheld Device**: The handheld device must be running Internet Explorer Mobile for Windows Mobile version 5 or version 6 operating system (OS); or Apple® iPhone® and iPod touch® iOS version 6.1 or greater. Other web browsers may display the UI but the functionality is not guaranteed.

Table 4: MAP Gateway

Compliance	**United States** UL Listed File E365459, ANSI/UL 60950-1, Information Technology Equipment; UL 2043 (Stationary version only), Suitable for Use in Other Environmental Air Space in Accordance with Section 300.22, (C) of the National Electric Code. Transmission Complies with FCC Part 15.247 Regulations for Low Power Unlicensed Transmitters Transmitter FCC Identification: OEJ-MAPWIFI FCC Compliant to CFR 47, Part 15, Subpart B, Class A
	Canada: Industry Canada IC: 279A-MAPWIFI ULC Listed File E365459, CAN/CSA-C22.2 No. 60950-1, Safety of Information Technology Equipment
CE	**Europe:** CE Mark – Johnson Controls, Inc. declares that this product is in compliance with the essential requirements and other relevant provisions of the R&TTE Directive 1999/05/EC and EMC Directive 2004/108/EC. IC: RSS-210 **CE Emission:** EN61000-6-3: 2007; Generic standards for residential, commercial, and light-industrial environments. ETSI EN 301 489-1:2001-09, ETSI EN301 489-3:2001-11 (Class 2), IEC 60950-1/ EN 60950-1

1 Last digit (**x**) represents non-US country requirements.

The performance specifications are nominal and conform to acceptable industry standard. For application at conditions beyond these specifications, consult the local Johnson Controls office. Johnson Controls, Inc. shall not be liable for damages resulting from misapplication or misuse of its products.

Appendix: Root Certificates

Installing the Root Certificate

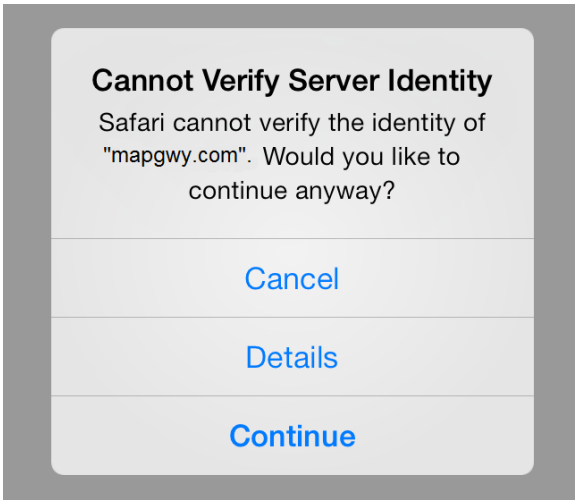
Until the security certificate for the MAP Gateway is added as a trusted root certificate, you receive a security alert every time you visit the mapgwy.com website. How you install the certificate differs based on the web browser and device platform.

Installing the Security Certificate on iOS

To install the root security certificate on mobile iOS platforms such as iPhones and iPads:

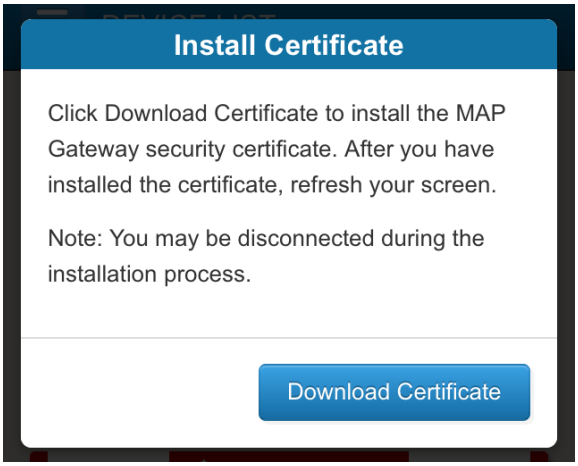
1. When you visit the mapgwy.com website, and you are prompted that your device cannot verify the identify of mapgwy.com, tap **Continue**.

Figure 6: Installing the MAP Gateway Security Certificate



2. On the Install MTG Profile screen, tap **Download Certificate**.

Figure 7: Installing the MAP Gateway Security Certificate

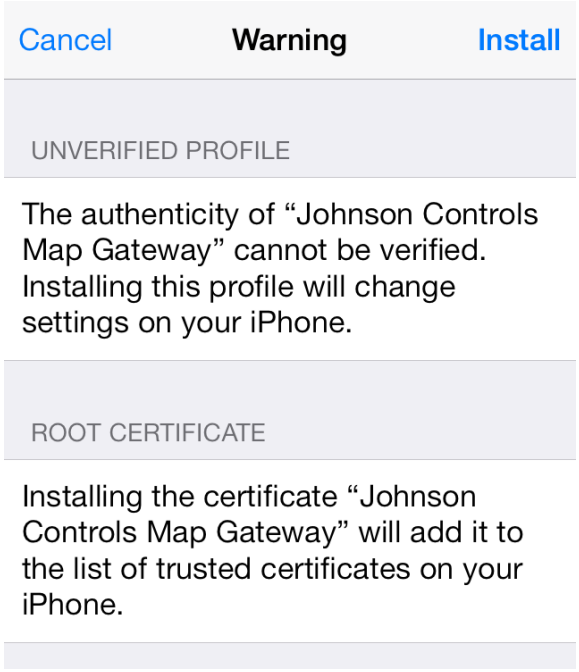


3. On the Install Profile screen, tap **Install**.

Figure 8: Installing the MAP Gateway Security Certificate

4. On the Warning screen, tap **Install**.

Figure 9: Installing the MAP Gateway Security Certificate



5. On the Profile Installed screen, tap **Done**.

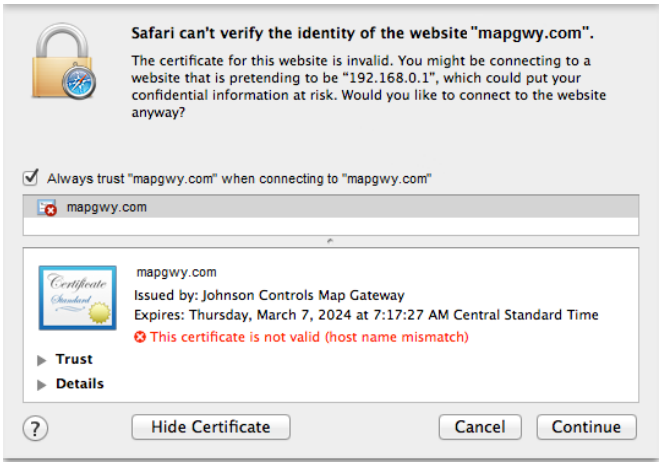
Figure 10: Installing the MAP Gateway Security Certificate

To verify that the security certificate is installed, go to the Settings menu of your mobile device. If the security certificate is installed, Johnson Controls Map Gateway appears in the Profile menu and is listed as Trusted.

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. Check the box that says **Always trust "mapgwy.com" when connecting to "mapgwy.com"**.
4. Click **Continue**.

Figure 11: Confirm mapgwy.com as a Trusted Site

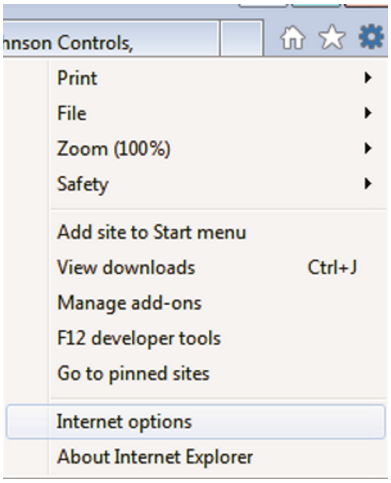


Installing the Security Certificate in Internet Explorer

To install a root security certificate in Internet Explorer 10:

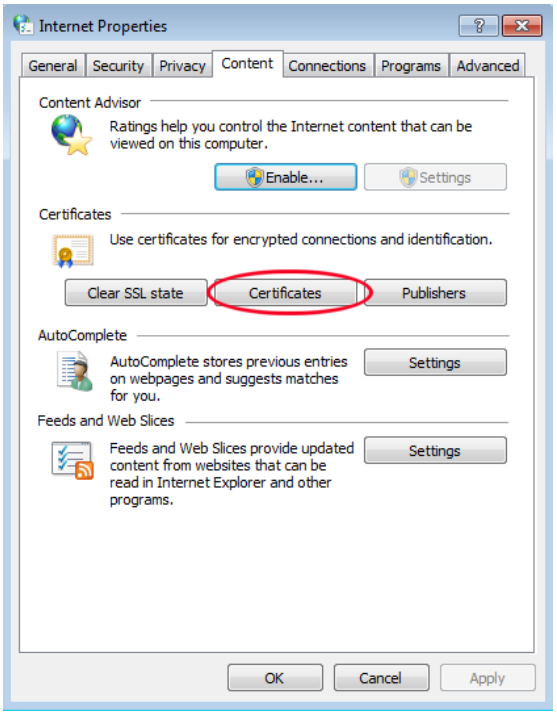
1. Navigate to **www.mapgwy.com/downloadtlsprofile**, and then download the **rootCA.pem** file.
2. On the Tools menu, click **Internet options**.

Figure 12: Internet Explorer Internet Options



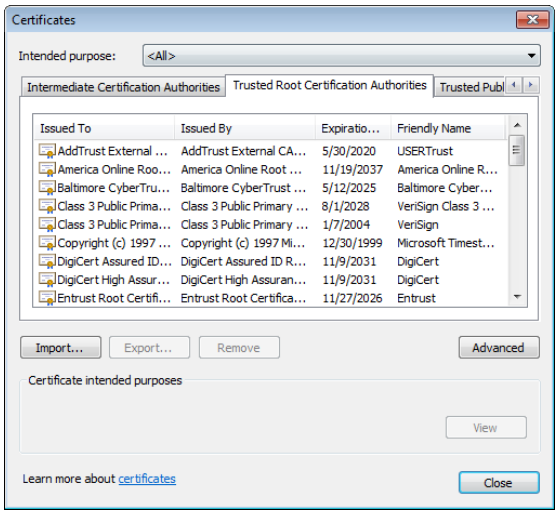
3. In the Internet Properties dialog box, click the Content tab, and then click **Certificates**.

Figure 13: Internet Explorer Properties Content Tab



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

Figure 14: The Certificates Dialog Box



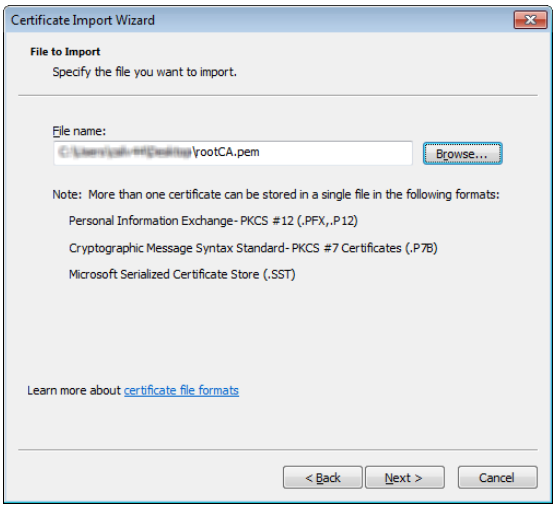
5. In the Certificate Import Wizard dialog box, click **Next**.

Figure 15: Certificate Import Wizard

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

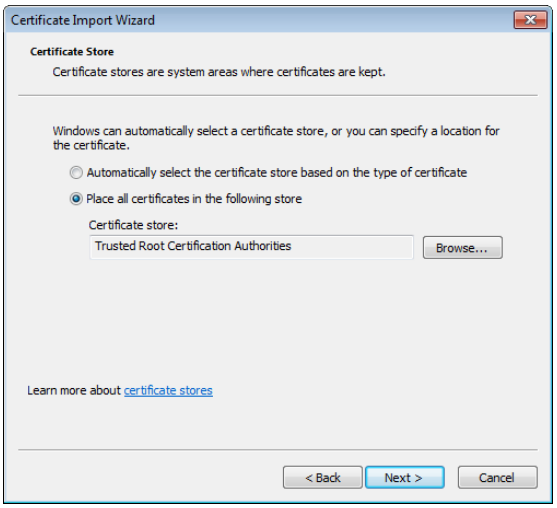
   Note: Install the **rootCA.pem** file and not the mapgwy.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any MAP Gateway you use. If you install the mapgwy.com file that the browser prompts you to install instead, you need to add a new root certificate for each new MAP Gateway device that you use.

Figure 16: Importing the Certificate



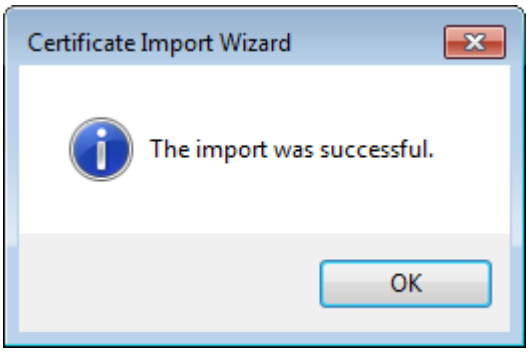
7. On the Certificate Store page of the wizard, select **Place all certificates in the following store**, verify that the certificate store listed is **Trusted Root Certification Authorities**, and then click **Next**.

Figure 17: Certificate Store Options



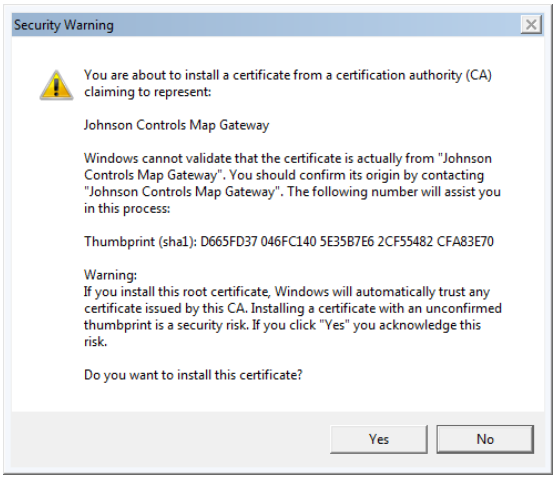
8. Click **Finish**. A success message appears.

Figure 18: The Certificate Import Success Message



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

Figure 19: Non-Validated Certificate Security Warning

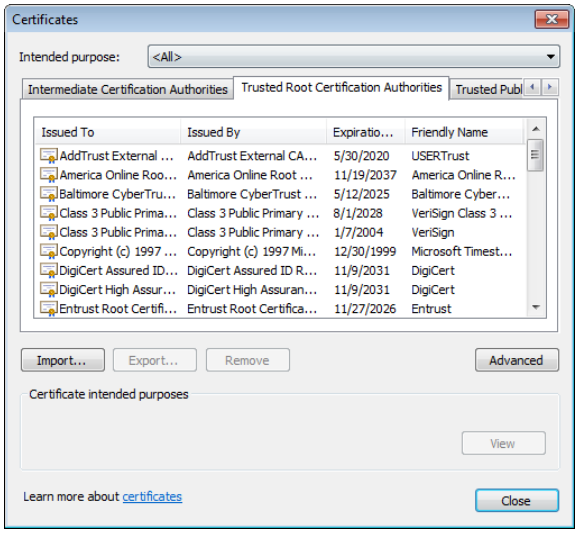


10. Click **OK**.

Importing the Root Certificate

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

Figure 20: The Certificates Dialog Box



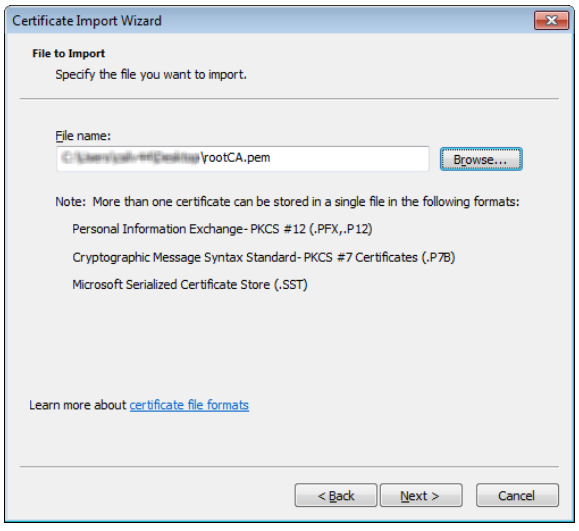
2. In the Certificate Import Wizard dialog box, click **Next**.

Figure 21: Certificate Import Wizard

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

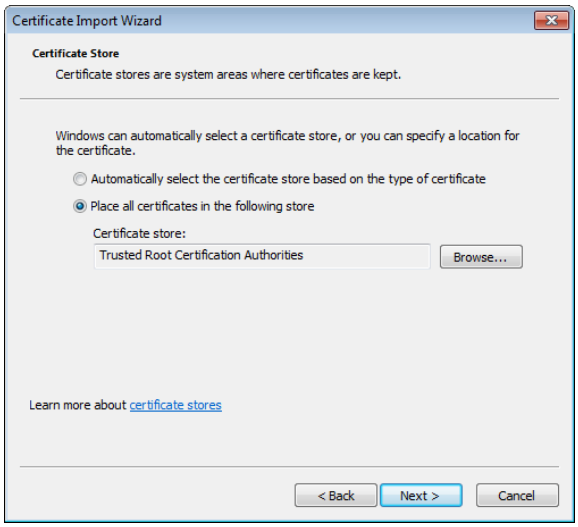
   Note: Install the **rootCA.pem** file and not the mapgwy.com file that the browser prompts you to install. The rootCA.pem file certifies your device for any MAP Gateway you use. If you install the mapgwy.com file that the browser prompts you to install instead, you need to add a new root certificate for each new MAP Gateway device that you use.

Figure 22: Importing the Certificate



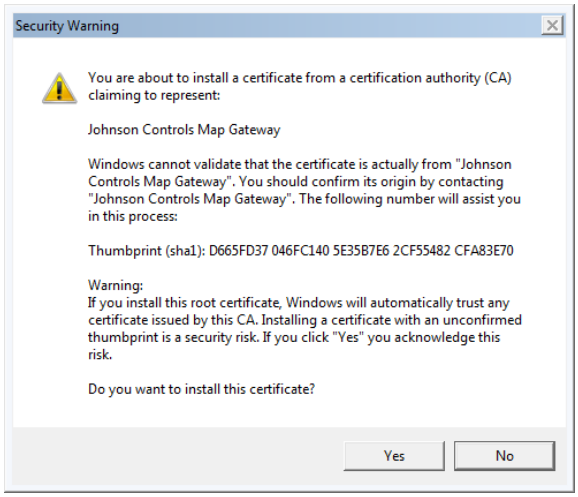
4. On the Certificate Store page of the wizard, select **Place all certificates in the following store**, verify that the certificate store listed is **Trusted Root Certification Authorities**, and then click **Next**.

Figure 23: Certificate Store Options



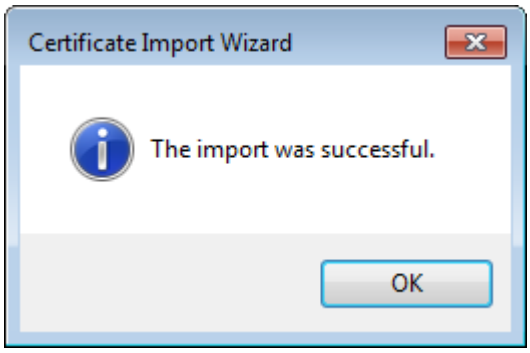
5. In the Security Warning dialog box, click **Yes**.

Figure 24: Non-Validated Certificate Security Warning



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

Figure 25: The Certificate Import Success Message



7. Click **OK**.

Uninstalling the Root Certificate

If you are removing or replacing a MAP Gateway and wish to uninstall the root certificate, follow the procedures in this section that are appropriate to your operating system. Note that it is not necessary to uninstall the certificate.

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

To uninstall the Security Certificate in Apple Safari for Mac:

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

Figure 26: Keychain Access Application with MAP Gateway Certificate Selected

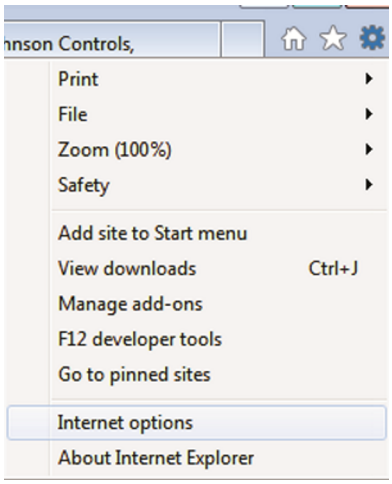
2. Right-click the certificate you wish to remove (in this case, mapgwy.com), and then click **Delete**.
3. Enter your administrator credentials, and click **Update Settings** to remove the certificate from the keychain.

Uninstalling the Security Certificate in Internet Explorer®

To uninstall a root security certificate in Windows® Internet Explorer 10:

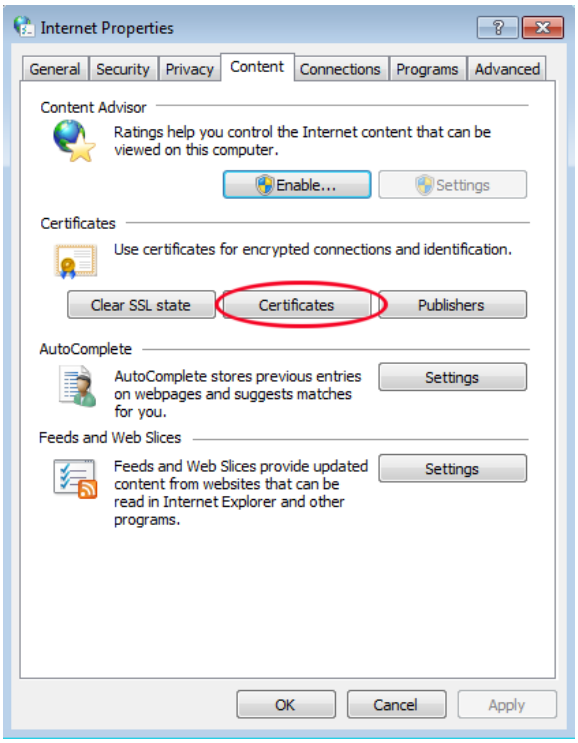
1. On the Tools menu, click **Internet options**.

Figure 27: Internet Explorer Internet Options



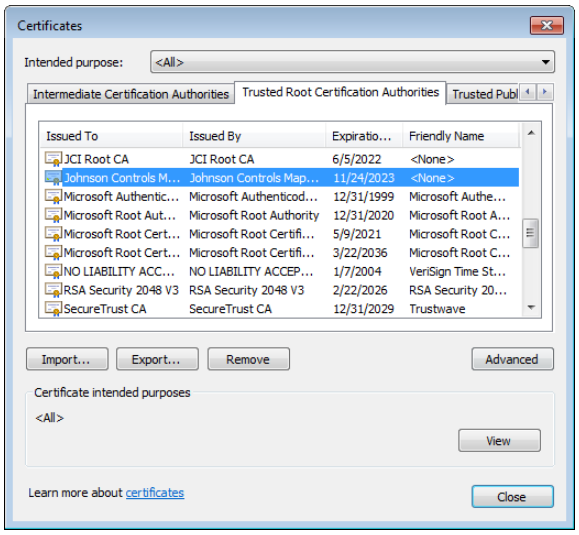
2. In the Internet Properties dialog box, click the Content tab, and then click **Certificates**.

Figure 28: Internet Explorer Properties Content Tab



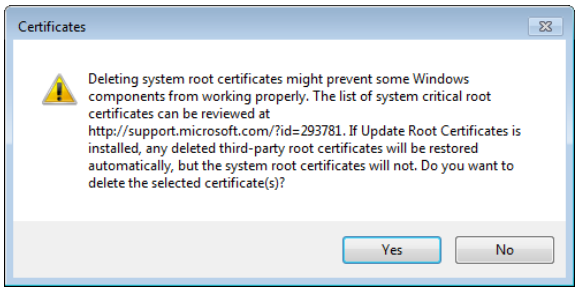
3. In the Certificates dialog box, click the Trusted Root Certification Authorities tab, select the Johnson Controls authority, and then click **Remove**. A Certificates warning appears (*Figure 30*).

Figure 29: Certificates Dialog Box



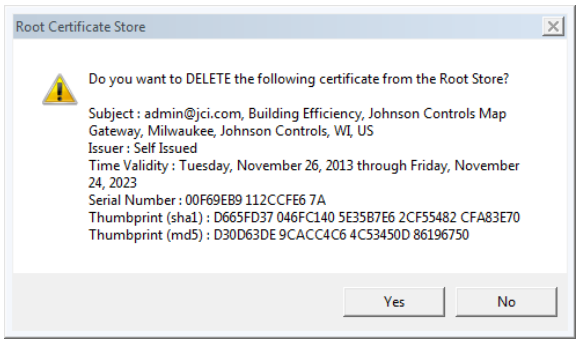
4. In the Certificates warning dialog box, click **Yes** (*Figure 30*). A Root Certificate Store warning appears (*Figure 31*).

Figure 30: Certificates Warning Dialog Box



5. In the Root Certificate Store warning dialog box, click **Yes** (*Figure 31*). You return to the Trusted Root Certification Authorities tab of the Certificates dialog box (*Figure 32*).

Figure 31: Root Certificate Store Dialog Box



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

Figure 32: The Certificates Dialog Box