AN-189

Protege WX Connectivity Guide

Application Note

Last Published: 22-Oct-21 11:16 AM

Contents

Introduction

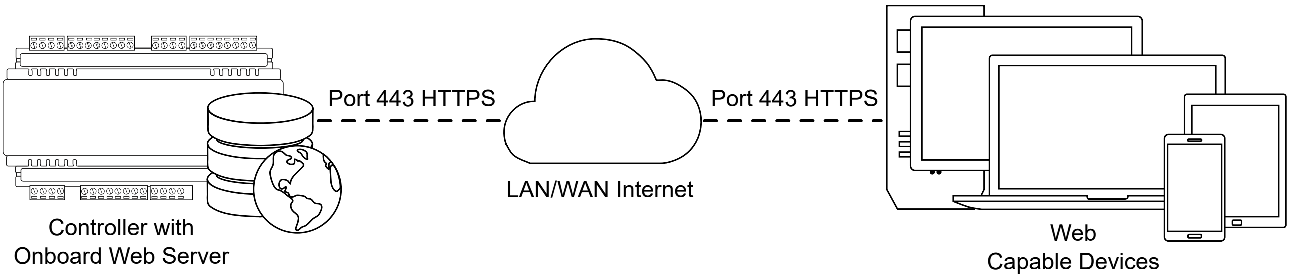
At face value, using Protege WX is as simple as opening up a web browser and navigating to a site. However, depending on your network configuration, there are different methods for connecting to the controller and accessing the web interface.

This application note covers:

- Protege WX web connectivity
- Connecting to Protege WX within the LAN (Local Area Network)
- Connecting to Protege WX externally

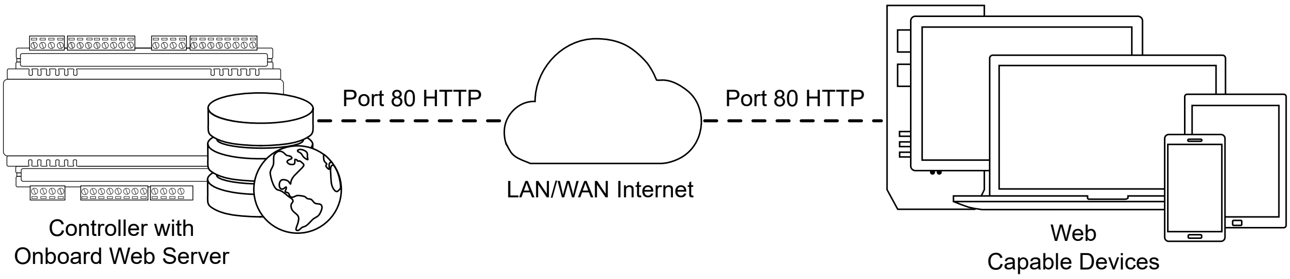
Protege WX Web Connectivity

The Protege WX interface is accessed using a standard web browser. The controller contains an onboard web server that sends the web pages to the browser through an **HTTPS** connection using the standard HTTPS web port (the default port is **443**) as shown below.



For information on HTTPS configuration, refer to AN-280: Configuring HTTPS Connection to the Protege WX Controller, available from the ICT website.

Protege WX controllers that are not configured for HTTPS send the web pages to the browser through an **HTTP** connection using the standard HTTP web port (the default port is **80**) as shown below.

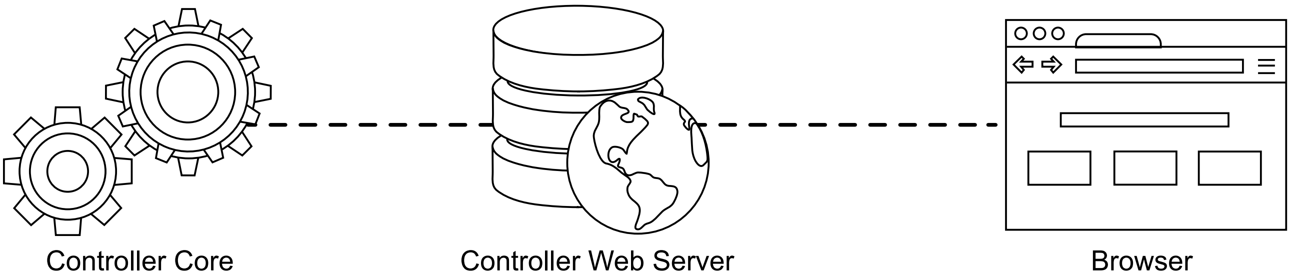


The HTTPS/HTTP port can be changed through the controller's **System Settings** if necessary, but you should retain the default port unless you are required to use another port by your system administrator.

Controller Core

The controller's web server talks to the controller core to query for events and system status, and to send programming update requests.

The web server and the controller core run independently so that the processing of physical devices is not impacted by programming changes via the web browser.

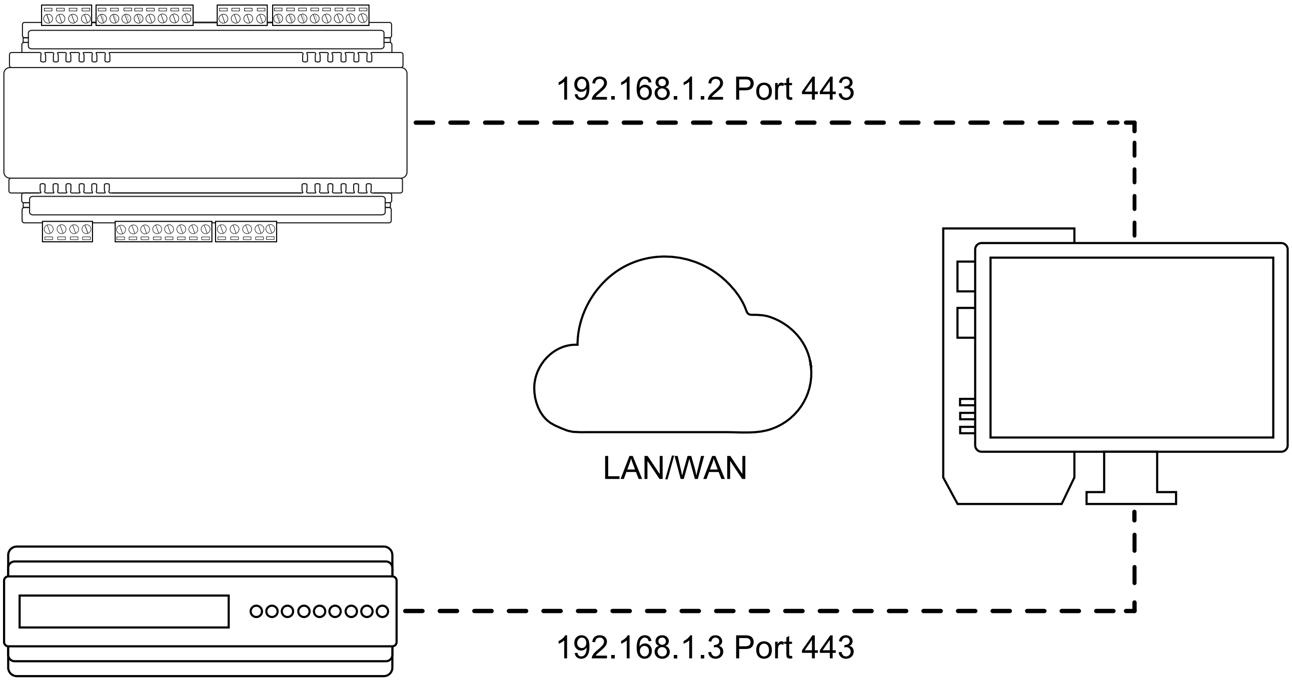


Device IP Addresses

Web browsers will always attempt to communicate on port 443 for HTTPS requests (port 80 for HTTP), but communications between the controller and the web browser are independent from connections to other devices on the same network that use these ports, as each device is identified by its IP address.

The controller can be accessed on port 443 while a DVR system or IP camera on the same network is also being accessed using port 443. There are no port conflicts between devices with different IP addresses.

Think of the IP address like a street address. The message is sent to the building (device) based on its address, and is then directed to the specific apartment (port) within the building. In this way the same web port can be used to communicate with countless devices with unique IP addresses.



Connecting to Protege WX within the LAN

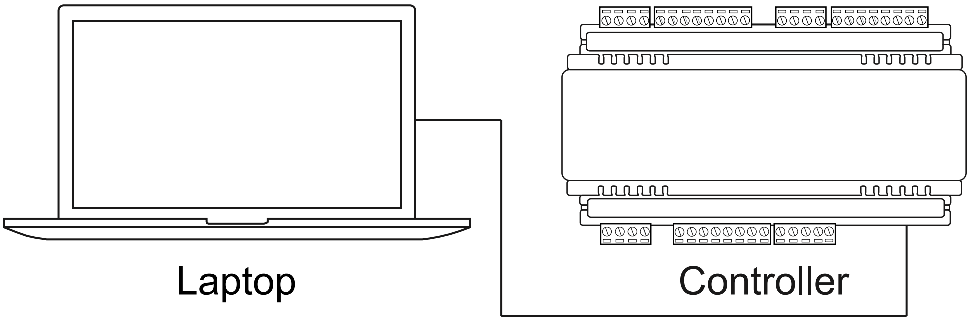
There are three main methods of connecting to the Protege WX controller within the LAN (Local Area Network).

- Direct wired connection
- Wired connection via network switch
- Wireless connection

Accessing Protege WX Using a Wired Connection

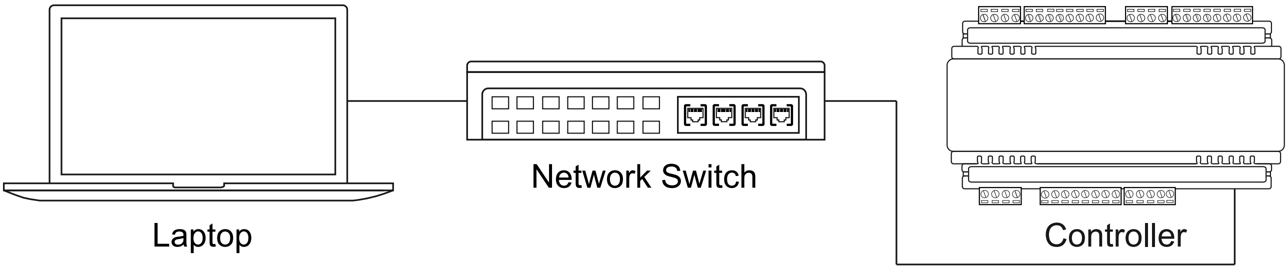
Direct Wired Connection

Connecting the Protege WX controller directly to your PC or laptop enables you to easily carry out onsite programming. Only the controller's IP address is required to access the web interface through the browser.



Wired Connection via Network

For live installations the controller should be interfaced using a standard segment (<100m in length) and should be connected to a suitable ethernet hub or switch.



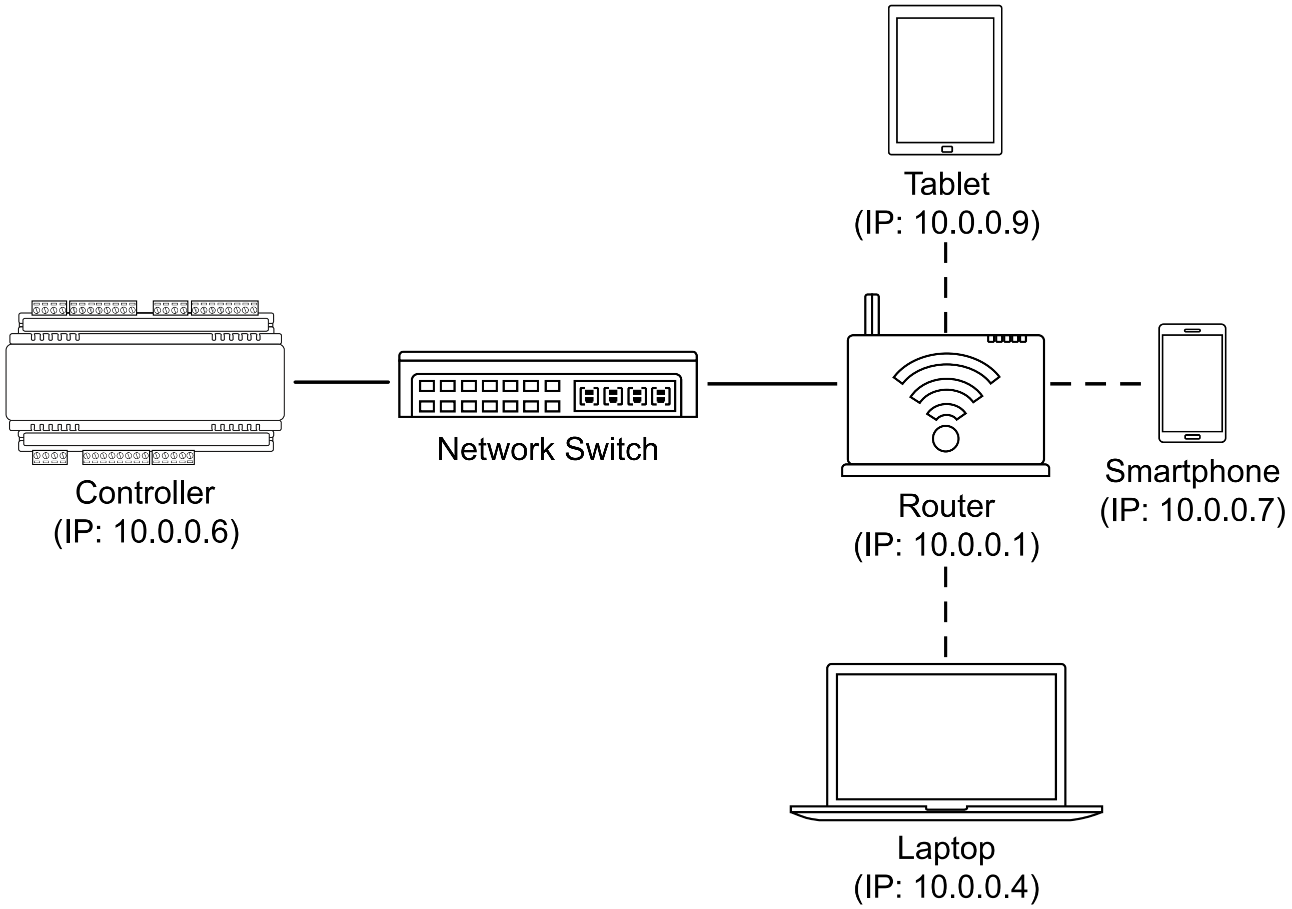
When connecting to the Protege WX interface via a network switch, you are still only required to enter the controller's IP address in order to access the web interface through the browser.

Connecting to Protege WX Using Wireless Devices

As Protege WX is accessible through a web browser, you are able to access the web interface from your smartphone, tablet or other wireless device without the need for a hardwired connection to a network switch or the controller.

As long as your controller is on the same **subnet** as the router, you can enter the IP address of the controller into a web browser on your device to access the web interface.

For example, if the router has the IP address of 10.0.0.1 you could set the controller 's IP address to 10.0.0.6 and, by connecting the controller to a network switch that is linked to the router, use the router's wireless network to access the web interface from a wireless device on the same network. As these devices are assigned an IP address on the same subnet when they connect to the router, you are not required to enter a port number.


Tablet
(IP: 10.0.0.9)
Controller
(IP: 10.0.0.6)
Network Switch
Router
(IP: 10.0.0.1)
Smartphone
(IP: 10.0.0.7)
Laptop
(IP: 10.0.0.4)

Connecting to Protege WX Externally

Specific configuration is required in order to access the controller over the internet.

1. Network Address Translation (NAT) must be set up on the router. NAT is most commonly used to enable each device within a network to have its own IP address.

   While each device has its own IP address within the network, from outside your network every request appears to be coming from the single publicly visible IP address assigned by your Internet Service Provider.

2. You also need to configure port forwarding in order to ensure that packets received on a particular external port are sent to the intended device on the internal network.

   Port forwarding is a method of making devices within your network accessible to/from the internet even when they are behind a router.

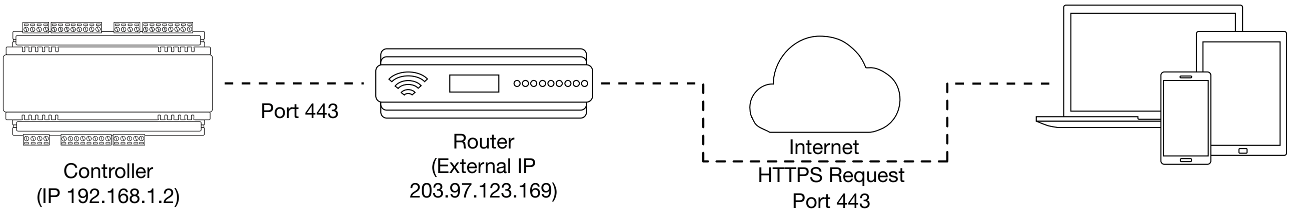
3. The controller's default gateway must be set to the IP address of the router. This tells the controller where to send/receive external communications.

Port Forwarding

In order for the controller to be accessible externally, port forwarding must be configured at the router. Port forwarding is a method of mapping an IP address and port on a local subnet to an external port, so that the networked device is accessible over the internet.

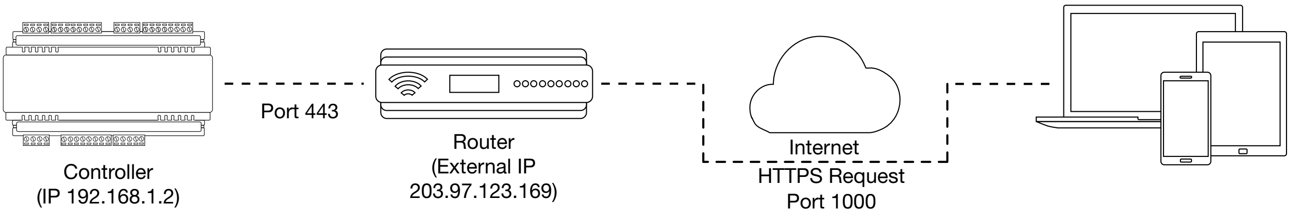
To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**, but this can be changed if necessary in the **System Settings**.

The easiest method is to configure the router to forward all traffic from **external port 443** (the default HTTPS port) to the controller's internal HTTPS port, as in the image below.



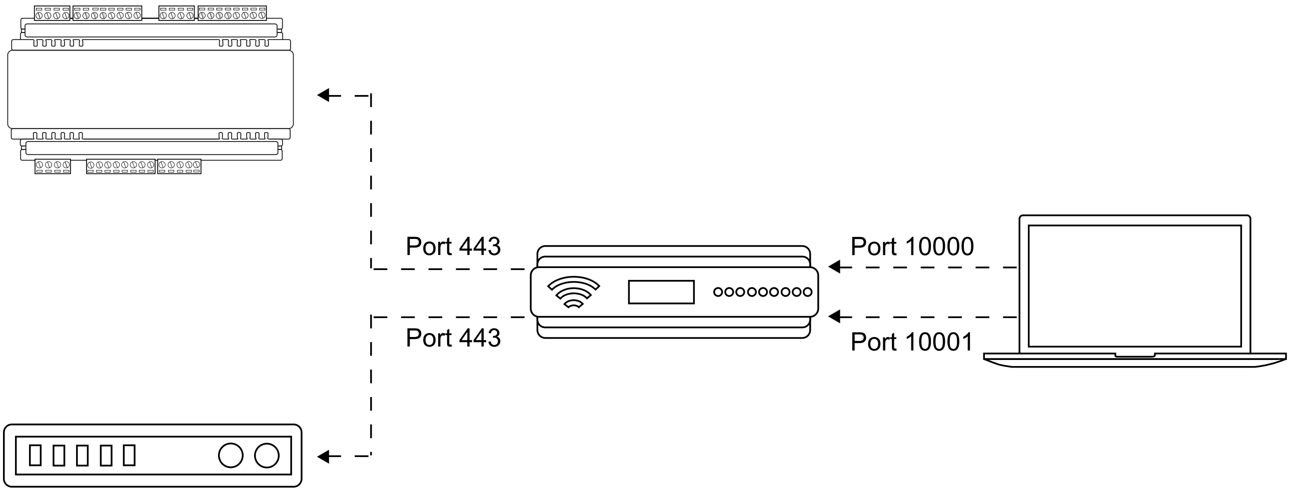
Once this port has been forwarded, the controller will be accessible via the external IP address of the network. In this case, all traffic directed to the external IP address will be forwarded to the controller. The controller's web interface could be accessed by typing https://203.97.123.169 into an external web browser.

However, it is possible to grant external access by forwarding any external port to the controller's HTTPS port, as shown below. This is especially useful if external port 443 is not available on your network.



In this case, any traffic directed to **external port 1000** will be forwarded to the controller's HTTPS port. The controller's web interface can be accessed by simply appending the external port number onto the end of the URL: e.g. https://203.97.123.169:1000.

Port forwarding also allows multiple internal devices to be accessed from the internet, even though they all use port 443 on the internal network, by forwarding a different port to each device.



Router Requirements

Port forwarding is configured from the router's utility interface, which can be accessed by browsing to the router's IP address. Different routers have different interfaces, so it is recommended that you consult the documentation for your router.

Most routers will require the following information in order to configure port forwarding:

- **Service/Application**: The name of the device/service.
- **External Port**: The port used to access the controller over the internet.
- **Internal Port**: The port used to access the controller from the internal network.
  The default is **port 443** for HTTPS, or **port 80** for HTTP.
- **Protocol**: The communication protocol used. This should be set to **TCP**.
- **Device IP**: This is the internal IP address of the controller. By default, this is set to **192.168.1.2**.

Controller Default Gateway

In order for the controller to send and receive external communications via the router, its default gateway needs to be set to the router's **internal** IP address.

1. Log in to the controller's web interface and navigate to **System Settings**.
2. In the **Default Gateway** field, enter the IP address of the router.
3. **Save** the configuration and **Restart** the controller.

Note: The default gateway must be set to the router's internal IP address that identifies it on the local internal network, not the external IP address used to connect over the internet.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.