AN-323

Setting Up Integrated DDNS on Controllers

Application Note

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Last Published: 24-Mar-22 3:49 PM

Contents

Setting Up Integrated DDNS on Controllers 4

Port Forwarding 4

DDNS Setup 5

Linking a Remote Protege GX Controller 6

Setting Up Integrated DDNS on Controllers

DDNS (Dynamic Domain Name Server) is a method which allows you to create a static hostname even when the external IP address of the controller is not fixed. The controller contains an integrated DDNS client which automatically updates the DDNS provider whenever the IP address changes.

In order to set up DDNS, the controller must be port forwarded so that it is externally accessible.

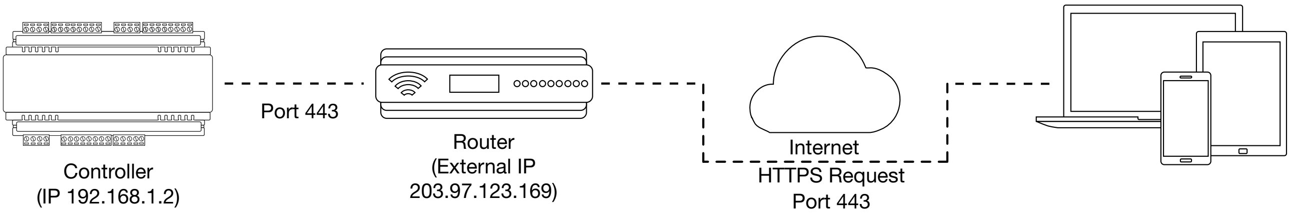
Port Forwarding

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.

HTTPS Connection

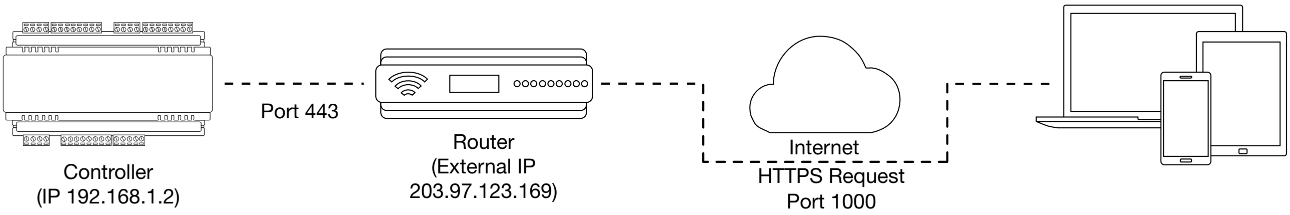
To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**. However, this can be changed if necessary in the **System Settings**.

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.



In this case, all traffic directed to the external HTTPS 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. This is especially useful if external port 443 is not available on your network.

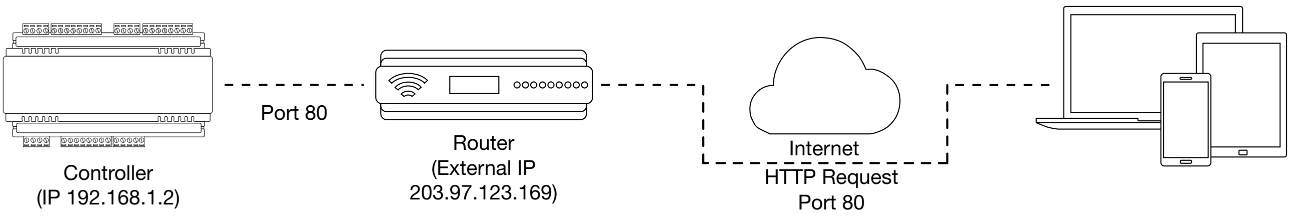


In this case, any traffic directed to **external port 1000** will be forwarded to the controller's HTTPS port. The controller's web interface can be accessed simply by appending the external port number onto the end of the URL: e.g. https://203.97.123.169:1000.

HTTP Connection

HTTP connection requires the controller to be accessible via an external port. The default port for HTTP requests is **external port 80**, but any available port can be used.

The external port must be set up to forward traffic to an internal port on the controller that accepts HTTP requests. By default this is **internal port 80**; but if required this can be changed in the **System Settings**.



Once this port has been forwarded, the controller will be accessible via the external IP address of the network. In this example, typing 203.97.123.169 into an external web browser will open the controller's web interface.

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 appropriate documentation for your router.

DDNS Setup

Controllers currently support two DDNS providers: Duck DNS (free provider) and No-IP (free accounts available, paid plans for further services).

Setting Up Duck DNS

For two-door controllers, Duck DNS can be used for HTTPS certification via third-party certificates.

1. Browse to Duck DNS and create a free account by signing in with Google or another existing account. Take note of the **Token** that is generated when you create your account.
2. Create a new **subdomain**. The full hostname will have the form [subdomain].duckdns.org.
3. The **Current IP** field should automatically populate with the external IP address of your network. Ensure that this is the controller's externally accessible IP address.
4. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
5. Navigate to the **System Settings**.
6. In the **Adaptor - Onboard Ethernet** tab, select the **Enable DDNS** checkbox.
7. Enter the **Hostname** [subdomain].duckdns.org and **DDNS Server** duckdns.org.
8. Leave the **DDNS Username** blank. For the **DDNS Password**, enter the **Token** generated by your Duck DNS account.
9. **Save** your settings.
10. Confirm that the controller is externally accessible by browsing to the hostname on another PC.

    If the controller's external port is not the default port, you will need to append the port number to the URL (e.g. controller.duckdns.org:1000).

Setting Up No-IP

The free No-IP Dynamic DNS service does not support third-party certification. This is only supported with the additional Plus Managed DNS service.

1. Browse to No-IP and create a **Dynamic DNS** account (free or paid as required).

    Free Dynamic DNS hostnames provided by No-IP require confirmation every 30 days, whereas paid accounts do not.

2. Create a new **Hostname** and select a **Domain**.
3. Ensure that the **IP Address** matches the controller's externally accessible IP address.

4. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
5. Navigate to the **System Settings**.
6. In the **Adaptor - Onboard Ethernet** tab, select the **Enable DDNS** checkbox.
7. Enter the **Hostname** and **DDNS Server**.
8. Enter the **Username** and **Password** that you used to sign up to No-IP.
9. **Save** your settings.
10. Confirm that the controller is externally accessible by browsing to the hostname on another PC.

    If the controller's external port is not the default port, you will need to append the port number to the URL (e.g. controller.ddns.org:1000).

Linking a Remote Protege GX Controller

Protege GX can be configured to link to remote controllers that have been programmed for DDNS hostname connection. Once a Protege GX controller has been configured with integrated DDNS, the DDNS URL can be entered into Protege GX to provide connection to the controller.

1. Navigate to **Sites | Controllers** and select or add the controller to link in Protege GX.
2. Enter the controller's DDNS URL into the **IP Address** field.

    This is the same URL that is entered into the **Controller Hostname** field in the controller's web interface.
3. Click **Save**.

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.