AN-201

Protege GX Push Notification Setup

Application Note

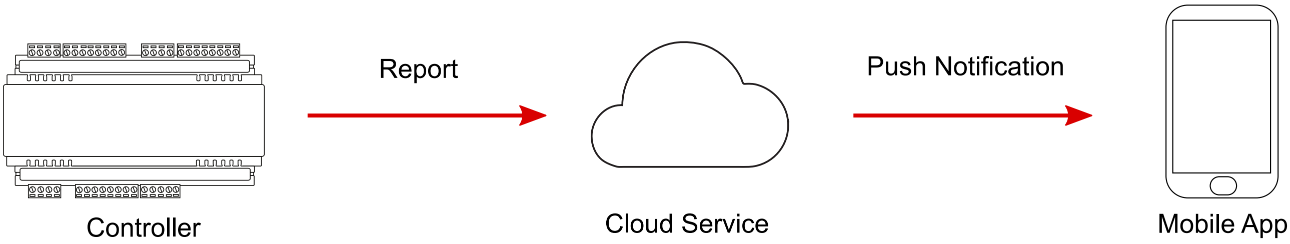
Last Published: 18-Dec-24 3:45 PM

Contents

Configuring Push Notifications

Push notifications for the Protege Mobile App give you instant awareness of important events happening on site, such as area arming and disarming, alarms and tampers.

This feature uses a special Report IP service that is hosted on the controller. The reporting service monitors one or more areas. When a reportable event such as an alarm occurs, the controller sends the report to the ICT cloud service, which then sends out notifications to the mobile app accounts connected to that Protege GX place.



As Protege GX supports cross controller communications, you can assign areas from multiple controllers to a single push notification service. The controller that hosts the service will report changes from all of the areas monitored by the service. Alternatively, you can create an additional push notification service for each controller.

Push notifications are also supported on Protege WX and Protege X. They are configured automatically when you enable push notifications in the mobile app.

Prerequisites

This functionality is available in Protege GX version 4.2.194 or higher.

Before you begin, ensure that the controller is able to report out over port **10105**. Depending on the network you may need to create a firewall rule to allow this.

Permissions

To enable push notifications on their mobile app, the Protege GX operator needs permission to view the push notification service and the controller it is programmed on.

You can enable the required permissions in the operator's role by setting the **Controller programming windows** table to Grant read only access or Grant full access. Alternatively, use a security level and record group for more granular control of permissions.

For more information about creating roles and security levels, see Application Note 191: Programming Operator Roles in Protege GX.

Creating the Report IP Service

Push notifications use a specially configured Report IP service:

1. Navigate to **Programming | Services** .
2. Select the **Controller** that will host this service in the toolbar.
3. Click **Add**.
4. For the service **Name** enter **PUSH - DO NOT TOUCH**.

   The service name must be entered **exactly** as above.

5. Set the **Service type** to Report IP.

6. Set the **Service mode** to 1 - Start with controller OS.
7. Select the **General** tab.
8. Set the **Client code** to the last six characters of the controller that the service is hosted by. For example, if the controller's serial number is C29E2FDA, the client code is 9E2FDA.
9. Set the **Reporting protocol** to Armor IP (TCP) encrypted.
10. Set the **Encryption level** to AES 256 bit.
11. Generate the 32 character encryption key at https://www.ict.co/Key-Generator. On the Key Generator page, click **Generate key** then copy the resulting code and paste it into the **Encryption key** field.
12. Set the **IP address / Host name** to **40.86.94.33**.
13. Set the **IP port number** to **10105**.
14. Select the **Options** tab and enable the types of events you want to report:
    - Report open
    - Report close
    - Report alarms
    - Report tampers
    - Report restore
    - Report bypass
15. Click **Save**.
16. Right click on the service and select **Start service**.

Configuring the Areas

The reporting service must be assigned to all the areas that you wish to receive push notifications for, similar to a normal IP reporting service.

1. Navigate to **Programming | Areas** and select the area to enable push notifications for.
2. Select the **Configuration** tab and scroll down to the **Reporting services** section.
3. Click **Add** and select the **PUSH - DO NOT TOUCH** service, then click **OK**.
4. Click **Save**.

Enabling Push Notifications

To activate the push notification service, you must connect your Protege Mobile App to the Protege GX place. The operator account must have access to view **controllers** and **services**.

1. Log in to the Protege Mobile App.
2. From the main menu, select **My Places** and tap the plus (**+**) icon to add a place.
3. Set the **Type** to Protege GX.
4. Enter the **Name**.
5. Enter the **External Address** of the Protege GX Web Client. This is the URL that you use to access your system from outside the site's WiFi coverage.

    > You must use the HTTPS URL.

6. Enter the **Internal Address** of the Protege GX Web Client.
7. Enter the **Username** and **Password** that you use to access Protege GX.
8. Enable **Push Notifications**.
9. Tap **Save**.

10. Read the disclaimer and tap **Accept**.
11. Select the **Site Name** for the Protege GX site.
12. Select the **Push Notification Services** that you will receive notifications from.
13. If your web client uses a self-signed certificate, tap **Accept** to accept the certificate.

Once this is complete the push notification service will connect to the Protege cloud service and begin sending push notifications.

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.