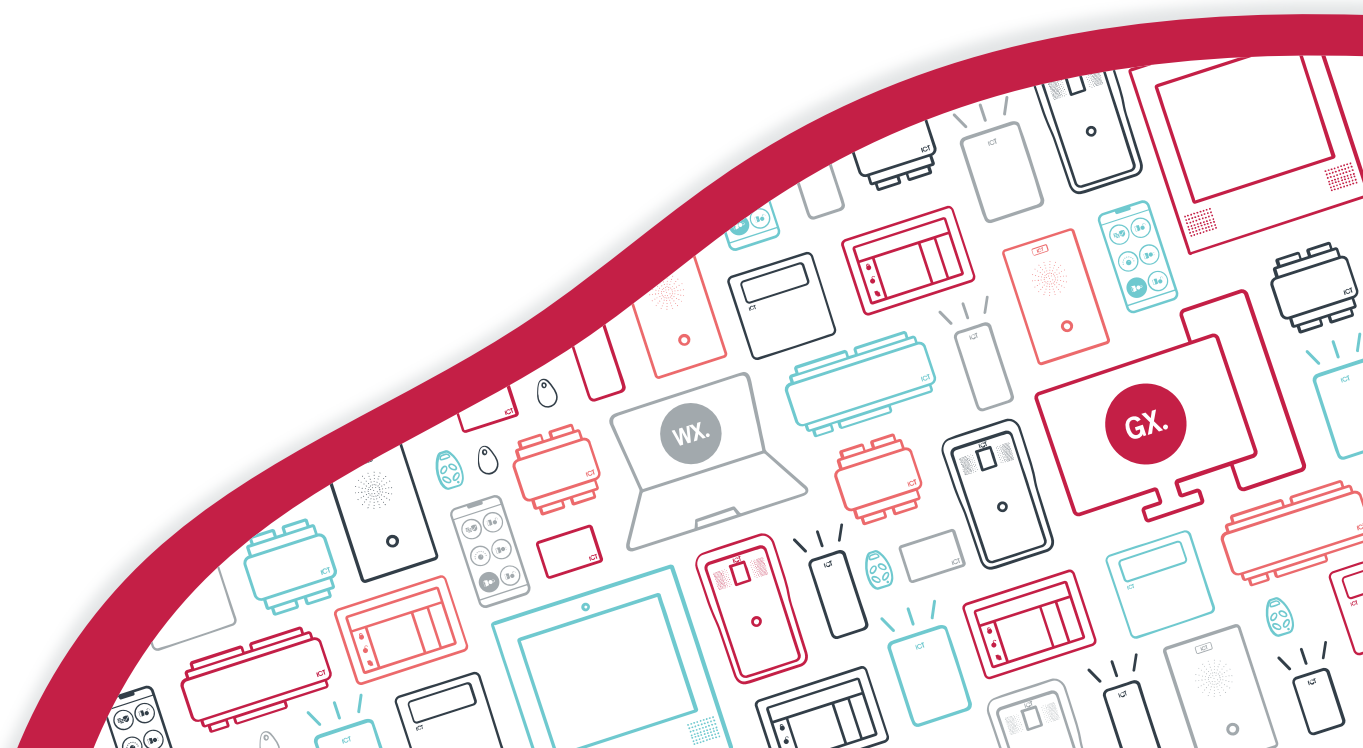
AN-297

Princeton Identity Biometric Integration with Protege GX

Application Note



Last Published: 13-Oct-22 3:07 PM

Contents

Introduction

Princeton Identity is a biometric identification system that allows facilities to identify registered users through iris and facial recognition software. The system allows a site to provide access to users solely via their biometric data (single factor identification), or for added security a biometric reader can be combined with an access control reader to require card and biometric credentials (dual factor identification).

Protege GX integrates with Princeton Identity enrollment and identity devices, turning every user's face into the world's most unique access credential.

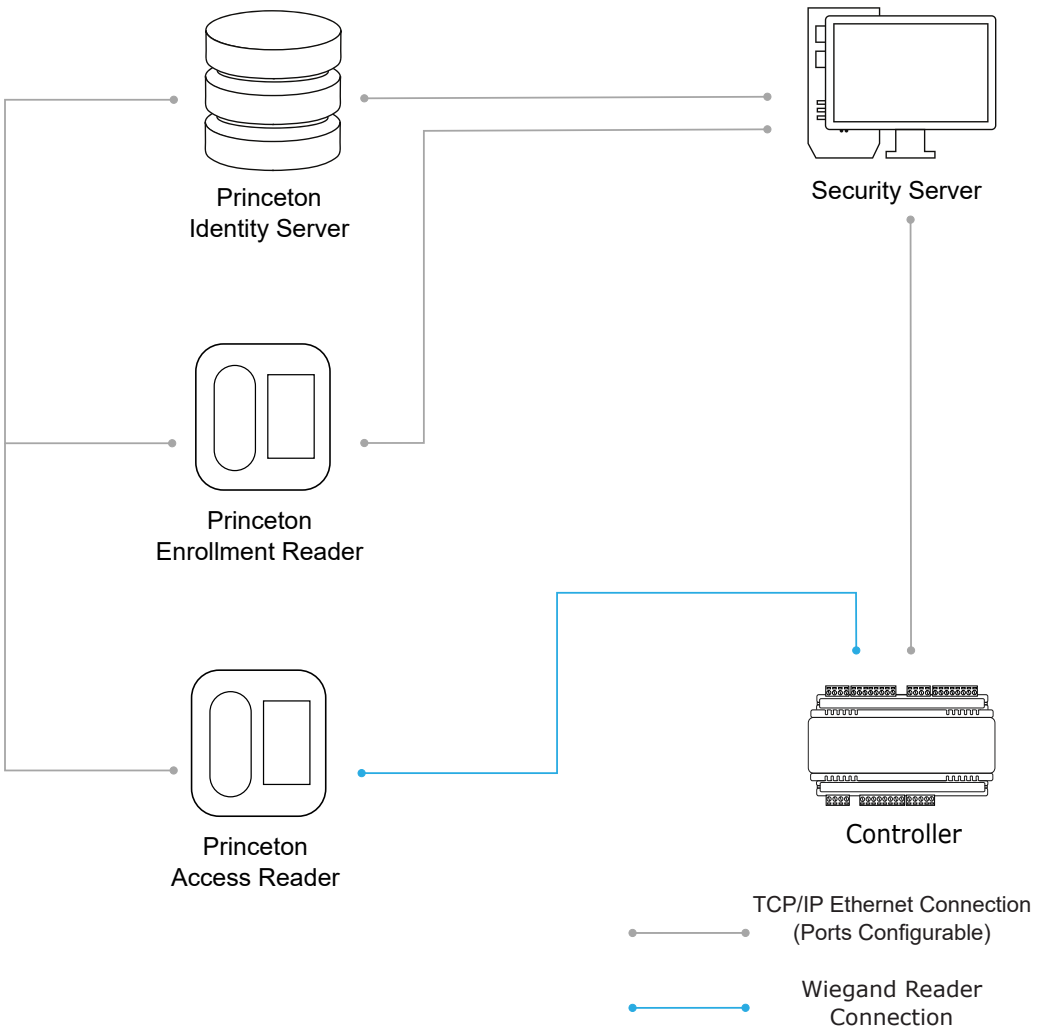
Using iris identification, face capture, and other biometrics, the system offers multifactor hands-free capabilities, giving the user a fast and frictionless enrollment and access experience.

Enrollment is both quick and easy. Users scan their face at an enrollment reader. The reader sends the scanned data to the Identity Server, which creates a unique credential identification and sends it on to the Protege GX server. Protege GX then assigns the biometric credential type and ID to the user, completing an integrated biometric access control system.

Integration Architecture

In this integration, the Protege GX server communicates with the Princeton Identity server (IDS100) and any enrollment readers over the ethernet network. The Princeton system enrolls users' biometric data, then sends a unique credential number to Protege GX.

Standard Princeton Identity readers which are not used for enrollment are then connected to Protege GX controllers or reader expanders using standard Wiegand configuration. When a user scans their face at a biometric reader, the biometric reader sends the user's credential to the reader expander just like a normal card reader. The Protege GX controller then decides whether access is granted or denied.



Prerequisites

Software Requirements

The following software must be installed and operational.

Software	Version	Notes
Protege GX	4.3.287.5 or higher	
IDS100 Identity Server	2.14.1.2627	This is the **only** tested and supported version for this integration. You will need the IP address and port of the server to configure this integration.

Compatible Readers

The following Princeton biometric readers are compatible with this integration.

Biometric Reader	Version	Notes
Access200e Enrollment Reader	2.16.0.3506	This is the **only** tested and supported version for this integration. You will need the IP address and port of any reader used for enrollment.
Access200 Identity Reader	N/A	Princeton Identity readers allow a standard Wiegand input from a proximity reader for dual factor authentication.

Licensing

License	Order Code	Notes
Protege GX Princeton Identity Biometric Integration license	PRT-GX-BIO-PR	1 per Princeton Identity reader connected to the Protege GX system

Connecting Princeton Biometric Readers

The **Princeton Identity Server** (IDS) and **enrollment readers** need to be connected to your local network.

You should be able to connect to the IDS web interface to verify and configure connections:

- Open an internet browser (Chrome is recommended) and enter: https://<IP Address>:8443.

  The IP address of the IDS is displayed on the module once it is powered and booted up.

- The default username is admin.
- The default password is password.
- Once connected to the IDS you can view and edit the connected Princeton Identity devices.

For further information on configuring Princeton hardware, refer to the Princeton Identity website.

Configuring Princeton Biometric Integration

Enable the Integration

Princeton biometric integration must be enabled and configured for each Protege GX site.

1. Navigate to **Global | Sites** and select the site to enable the Princeton biometric integration for.
2. Select the **Biometrics** tab, then check the **Enable Princeton integration** checkbox.

   Once this is enabled, a default Princeton Iris credential type will be created and assigned to the site configuration below. This can be viewed in **Sites | Credential types**.

   Do not to rename or otherwise edit the Princeton Iris credential type, as this will make it difficult to identify users who are enrolled with a Princeton biometric credential.
3. Enter the **Default facility number** that will be used for enrolled credentials.
4. The **Default enrollment reader** will be selected after the readers have been added.
5. Enter the **IP address** of the Princeton Identity Server (IDS).
6. Enter the **IP port** of the Princeton Identity Server (IDS). The default port is 8443.
7. Enter the **Username** that will be used to connect with the Princeton Identity Server (IDS).
8. Enter the **Password** that will be used to connect with the Princeton Identity Server (IDS).
9. Click **Save**.

Adding the Enrollment Readers

Each Princeton Identity reader used for enrolling biometric credentials needs to be configured in Protege GX. A PRT-GX-BIO-PR license is required for each reader added.

Biometric readers used for reading credentials do not need to be added here, as they are managed by the Princeton IDS.

1. Navigate to **Sites | Biometric readers** and click **Add**.
2. Enter a **Name** for the Princeton Identity reader. This would typically identify its location.
3. Enter the reader's **IP address**.
4. Set the reader's **IP port**. The default is 443.
5. Set the **Type** to Princeton.
6. Click **Save**.

For the reader's status to be Online, both the reader and IDS must be online and able to communicate.

When all Princeton Identity readers have been added, navigate to **Global | Sites | Biometrics** and set the **Default enrollment reader**.

Creating a Custom Door Type

1. Navigate to **Programming | Door types** and create a new Princeton Biometric door type.
2. Assign a **Name**.
3. In the **General** tab, set the **Entry reading mode** to Custom.

4. In the **Entry credential types** section click **Add** to assign the PrincetonIris credential type that is created when the integration is enabled. Add any other credential types that are required.
5. Repeat as above for **Exit reading mode** and **Exit credential types** if required.
6. Click **Save**.
7. Navigate to **Programming | Doors**. For every door to be controlled using a Princeton Identity reader, set the **Door type** to the custom door type created above. These doors can then be assigned to access levels to give users access to them.

Configuring Reader Expanders

Reader expanders can use customized credential types to recognize alternative forms of user identification from connected Wiegand devices. To enable biometric identification, the reader expander will need to be configured to recognize data from the connected Princeton Identity reader as a custom credential.

This configuration is only required when the Princeton Identity readers are attached to reader expanders.

1. Navigate to **Expanders | Reader expanders**.
2. Select the Reader Expander and set the following **Configuration** options:
   - **Port 1/2 network type**: Set to Wiegand under either **Port 1 network type** or **Port 2 network type**, as appropriate to the port the device is connected to.
   - **Ethernet network type**: Disabled
3. Click **Save**.
4. Select the appropriate **Reader** tab for the port in use (**Reader 1** or **Reader 2**) and set the **Reader format** to Custom credential.
5. Click **Save**.
6. Repeat the above steps for every reader expander that has a Princeton Identity reader connected.
7. The reader expanders that have been configured will require a module update. Right click on each reader expander record and click **Update module**.

Capturing Biometric User Credentials

1. Ensure that the Princeton Identity reader is set to Enrollment Mode.
2. Navigate to **Users | Users** and select a user to capture a biometric credential for.
3. Go to the **Biometrics** tab, and from the **Enrollment device** dropdown select the appropriate Princeton Identity enrollment reader.
4. Position the user in front of the reader, and in Protege GX click **Capture**. Then follow the instructions on the Princeton Identity reader.
5. If the scan is successful a pop-up message will advise that the user's face data has been stored.

   If the capture has not been performed in accordance with the reader requirements, Protege GX will display an error message indicating why the scan has failed (see next page). You will need to start the scan again to capture the biometric credential.

When the capture has been completed successfully, the user's biometric credential is stored and the PrincetonIris credential type is added to the user's **Credentials** list in the **General** tab.

Appendix: Error Messages & Troubleshooting

Capture Messages

The following messages may be displayed in Protege GX during the capture process:

- **Scan finished successfully**: The capture has been successful and the user's credential data has been stored.
- **Cannot capture biometrics from Princeton Capture Reader**: Indicates an incorrect or incomplete capture from the reader, such as the user not looking at the reader, or moving.
- **Cannot capture biometrics from Princeton Capture Reader, please check Reader Mode**: Indicates that the Princeton Identity reader is set to Identify Mode instead of Enrollment Mode.
- **Cannot connect to Princeton Capture Reader**: Typically indicates that the Princeton Identity reader is offline.
- **Cannot connect to Princeton Identity Server**: Indicates invalid IDS connection details in the Protege GX site configuration, such as incorrect IP address.
- **Cannot authenticate with Princeton Identity Server**: Indicates invalid IDS authentication details in the Protege GX site configuration, such as incorrect username or password.

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