AN-311

# Protege GX ASSA ABLOY DSR Integration

Application Note

Last Published: 11-May-22 1:55 PM

# Contents

# Introduction

Protege GX integration with ASSA ABLOY DSR (Door Service Router) software systems and IP-enabled locks combines wireless or PoE locking system technology with integrated electronic access control, intruder detection and building automation.

In this integration a single Protege GX controller communicates with the ASSA ABLOY DSR server, which in turn communicates with the IP-enabled locks.

All users, access levels, schedules and credentials are configured and maintained in Protege GX and sent via the controller to the DSR server, which then sends this configuration to the locks.

All access decisions are made by the locks. Lock events, alarms and status are communicated from the locks back to Protege GX, via the DSR server.

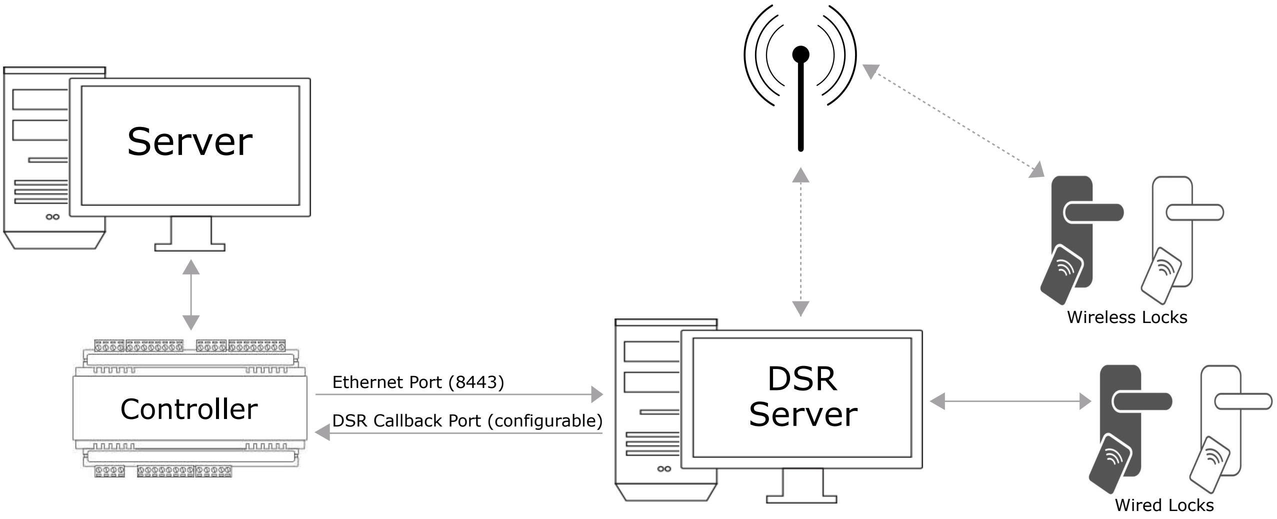
PoE locks operate as an online lock, and return and receive live data through the DSR server callback response process. WiFi locks operate as an offline lock and periodically connect to the DSR server to obtain any configuration changes and upload alarms/events/status.

## Network Architecture

The DSR server, Protege GX controller and Protege GX server must all be able to communicate with each other over TCP/IP.

The Protege GX controller sends user credential and access configuration to the DSR server via the defined **Ethernet Port** (8443 is the default).

The DSR server returns status and event updates via the configurable **DSR Callback Port**.



The Protege GX server and DSR server must be installed on separate machines.

# Prerequisites

## Software Requirements

| Software | Version | Notes |
|---|---|---|
| Protege GX software | 4.3.308 or higher | |
| ASSA ABLOY DSR software | 8.0.13 | Other versions have not been validated and may not be supported, or may include new options that are not supported. |

## Hardware Requirements

| Controllers | Firmware Version | Notes |
|---|---|---|
| Protege GX Controller | 2.08.1154 or higher | 1 x Protege GX controller per DSR server.<br>A controller can support up to 1024 ASSA ABLOY IP-enabled locks in this integration. To support more locks an additional Protege GX controller and DSR server must be installed per additional 1024 locks. |
| **ASSA ABLOY Locks** | **Firmware Version** | **Notes** |
| IN120 WiFi Lock | v3_0p09_cx_v3535 **only** | Locks have been tested and functionality confirmed with this firmware version only. |
| IN220 PoE Lock | | |
| Passport 1000 P1 PoE Lock | | |
| Passport 1000 P2 WiFi Lock | | |

This integration has been tested and validated with the locks listed above. Other locks supported by the DSR system may be suitable for this integration but have not been validated and may require testing.

DSR lock configuration has been tested with the **multiCLASS** reader configuration only. Other read head types should operate but will require on-site validation.

## Protege GX Licensing Requirements

| License | Order Code | Notes |
|---|---|---|
| Protege GX ASSA ABLOY DSR Door License | PRT-GX-DSR-DOR | 1 x license required per door with an ASSA ABLOY lock connected. |

It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

This document includes the Protege GX requirements and configuration instructions for this integration. It does not include the installation or configuration of ASSA ABLOY IP-enabled locks or the DSR software. For specific ASSA ABLOY requirements and compatibility, refer to the relevant ASSA ABLOY documentation: https://secure.intelligentopenings.com/en/resources/partner-area/

# System Capacity

It is important to be aware of the DSR system capacity and the factors that affect these limits.

- The DSR system currently allows up to 9,999 credential records.
- All locks store the full DSR server credential database.
- Only credentials for users with access to DSR system locks are sent to the DSR server.
- Protege GX will send the first 9,999 credentials and PINs in the Protege GX database that are assigned to a user with an access level containing one or more doors assigned to integrated locks.

  Credentials and PINs for users who do not require access to ASSA ABLOY locks are not sent to the DSR server. The Protege GX database for the site can contain more than 9,999 users when using the integration.

- Each credential is stored in the DSR server as a unique record, so if a Protege GX user has five credentials they will be sent and stored as five credential records in the DSR server and the locks.
- Dual credential configurations utilize two credentials (card and PIN) for each user. For sites not requiring dual credential authorization, user PINs can be excluded from being sent.

  To exclude sending user PINs to the DSR server add the following command to the controller programming:

  ```
  DSRSendPINCredential = false
  ```

- All IP-enabled locks cache events locally while offline (current maximum capacity of 9,999).

  If the cache reaches the maximum capacity, older events will be overwritten with new events.

# Programming Example

The following programming example demonstrates a basic configuration scenario.

The example site will have two doors. The front door will have a PoE lock, while the back door, being used less and too far for cabling, will have a WiFi lock installed.

Managers will have access to both doors at all times, while staff and visitors can only access the front door during office hours. Visitors will also be restricted to one time access.

## Prepare the DSR System

The ASSA ABLOY DSR server and locks require the following programming for the integration:

1. TLS/SSL security must be enabled on the DSR server.
2. The ASSA ABLOY locks need to be programmed with the correct credential configuration.
3. WiFi locks will need alarms configured to wake on specific events.

### Enable TLS/SSL Security on the DSR Server

1. Open the **DSR Support Tool** and navigate to **Configuration Settings | Server Settings | WS Encryption & Port Configuration**.
2. Set the **TLS/SSL Security** setting to True, then click **Update Configuration**.
3. Open the Windows Services snap-in and start the **ASSA ABLOY Door Service Router** service.

For more information, see Security Configuration (page 14).

### Program Credential Configuration on the DSR Locks

Our site has MIFARE DESFire EV1 cards for staff and uses HID 34 Bit cards for visitors. The DSR locks need to be configured to read both credential formats.

1. Open the **Lock Configuration Tool** and navigate to **Lock Profile | Reader Setup**.
2. Set the **Reader** to multiCLASS Reader.
3. Set the first **Card Type** to HID Prox for the visitor cards.
4. Set the second **Card Type** to MIFARE DESFire EV1 and the **Card Data Type** to CSN for the staff cards.
5. **Save** the setup and **Configure** each of the locks to synchronize the profile.

For more information, see Credential Configuration (page 15).

### Set the WiFi Lock Alarms

We want the WiFi lock to wake and update when specific events occur.

1. Open the **Lock Configuration Tool** and navigate to **Lock Profile | Alarms**.
2. Turn on the **Denied** alarm so the lock will wake and receive updates when a user is denied entry.
3. Turn on the **Low Battery** alarm so the lock will wake and generate a trouble input alert when its batteries start running low.
4. Turn on the **Tamper Alarm** so the lock will wake and generate a tamper alert when a tamper is detected.
5. **Save** the alarms configuration then **Configure** the WiFi lock to synchronize the changes.

Additional alarms can be set, however increasing the number of alarms increases battery consumption.

For more information, see WiFi Lock Alarms (page 15).

# Protege GX Programming

Enabling and configuring the ASSA ABLOY DSR integration in Protege GX requires the following steps:

1. The integration must be enabled on the Protege GX controller.
2. Ethernet communication must be programmed on the controller's onboard reader expander.
3. A door record needs to be configured for each physical door that has an IP-enabled lock connected.
4. Trouble input records need to be configured for each door.
5. A smart reader record needs to be created for each lock.
6. Access levels need to be configured to provide users access to DSR doors.
7. Credential types need to be configured with the compatible DSR credential formats.
8. Access levels and credentials need to be assigned to users.

## Enable DSR Integration on the Protege GX Controller

1. Navigate to **Sites | Controllers** and select the controller that will communicate with the DSR server.
2. In the **Commands** section enter the command: `DSRIP = true`
3. **Save** the controller configuration.

For more information, see Enabling the Integration (page 16).

## Program the Onboard Reader Expander

1. Navigate to **Expanders | Reader Expanders** and select the controller's onboard reader expander.
2. Set the **Ethernet Network Type** to Third Party Generic.
3. Set the **Ethernet Port** to 8443.
4. In the **Commands** section add:

   `PortThree = 14`

   `DSRIPAddress = 192.168.1.123` (the IP address of the DSR server in our scenario)

   `DSRCallbackPort = 9090` (the default DSR server callback port)
5. Click **Save**. Wait for the programming to be downloaded to the controller, then right click on the reader expander record and click **Update Module**.

For more information, see Programming the Onboard Reader Expander (page 16).

## Create the Door Records

In our programming scenario the site has two doors that will accept Card or PIN authentication.

1. Navigate to **Programming | Doors**.
2. Add the Front Door record and set the **Door Type** to Card or PIN.
3. Add the Back Door record and set the **Door Type** to Card or PIN.
4. **Save** the door configurations.

For more information, see Creating Doors (page 17).

## Create the Trouble Inputs

Trouble inputs are used to report the Door Forced Open, Door Left Open, Low Battery and Offline lock statuses. Each trouble input needs to be created for each door.

1. Navigate to **Programming | Trouble Inputs**.
2. Add a trouble input called Front Door Forced Open.
   - **Module Type**: Door (DR)
   - **Module Address**: Front Door
   - **Module Input**: 1
   - **Trouble Group**: 3 - Access
   - **Trouble Group Options**: AC Failure/Module Tamper/Forced Door
3. Add a trouble input called Front Door Left Open.
   - **Module Type**: Door (DR)
   - **Module Address**: Front Door
   - **Module Input**: 2
   - **Trouble Group**: 3 - Access
   - **Trouble Group Options**: Battery/Module Lost/Door Left Open
4. Add a trouble input called Front Door Low Battery.
   - **Module Type**: Door (DR)
   - **Module Address**: Front Door
   - **Module Input**: 4
   - **Trouble Group**: 3 - Access
   - **Trouble Group Options**: Battery/Module Lost/Door Left Open
5. Add a trouble input called Front Door Lock Offline.
   - **Module Type**: Door (DR)
   - **Module Address**: Front Door
   - **Module Input**: 6
   - **Trouble Group**: 2 - System
   - **Trouble Group Options**: Battery/Module Lost/Door Left Open
6. Add a trouble input called Back Door Forced Open.
   - **Module Type**: Door (DR)
   - **Module Address**: Back Door
   - **Module Input**: 1
   - **Trouble Group**: 3 - Access
   - **Trouble Group Options**: AC Failure/Module Tamper/Forced Door
7. Add a trouble input called Back Door Left Open.
   - **Module Type**: Door (DR)
   - **Module Address**: Back Door
   - **Module Input**: 2
   - **Trouble Group**: 3 - Access
   - **Trouble Group Options**: Battery/Module Lost/Door Left Open

8. Add a trouble input called Back Door Low Battery.
   - **Module Type**: Door (DR)
   - **Module Address**: Back Door
   - **Module Input**: 4
   - **Trouble Group**: 3 - Access
   - **Trouble Group Options**: Battery/Module Lost/Door Left Open
9. Add a trouble input called Back Door Lock Offline.
   - **Module Type**: Door (DR)
   - **Module Address**: Back Door
   - **Module Input**: 6
   - **Trouble Group**: 2 - System
   - **Trouble Group Options**: Battery/Module Lost/Door Left Open

For more information, see Trouble Input Settings (page 18).

## Create the Smart Reader Records

Smart reader records provide the configuration to identify each of the locks.

1. Navigate to **Expanders | Smart Readers**.
2. In the toolbar, select the **Controller** that has the DSR integration enabled.
3. Create a new smart reader record called Front Door Lock.
   - Set the **Expander Address** to 1
   - Set the **Expander Port** to Ethernet
   - Set the **Configured Address** to <not set>
   - Add the command: `SerialNumber = CP1234567890` (the serial number of our front lock)
   - Add the command: `ConfiguredAddress = 1`
   - Go to the **Reader** tab and set the **Reader One Door** to Front Door
4. Create a new smart reader record called Back Door Lock.
   - Set the **Expander Address** to 1
   - Set the **Expander Port** to Ethernet
   - Set the **Configured Address** to <not set>
   - Add the command: `SerialNumber = CP0987654321` (the serial number of our back lock)
   - Add the command: `ConfiguredAddress = 2`
   - Go to the **Reader** tab and set the **Reader One Door** to Back Door
5. Click **Save**.

For more information, see Creating Smart Reader Records (page 19).

## Create Schedules

For our scenario we need a 24-7 schedule to provide manager access at all times, and a Mon-Fri 8-6 schedule to provide staff and visitor access during office hours. Navigate to **Sites | Schedules** and create the two schedules.

For information on creating schedules, see the Protege GX Operator Reference Manual.

## Create the Access Levels

At this site managers will have access to both doors. Staff and visitors will have access via the front door only.

1. Navigate to **Users | Access Levels**.
2. Create a new access level called Manager.
   - Select the 24-7 **Operating Schedule**
   - In the **Commands** section enter the command: `DoubleSwipeAccess = true`

     This will allow managers to latch unlock a door by badging twice at the lock (see page 25).
   - In the **Doors** tab add the Front Door and Back Door
3. Create a new access level called Staff.
   - Select the Mon-Fri 8-6 **Operating Schedule**
   - In the **Doors** tab add the Front Door
4. Create a new access level called Visitor.
   - Select the Mon-Fri 8-6 **Operating Schedule**
   - In the **Commands** section enter the command: `OneTimeAccess = true`

     This restricts visitors to only one access occasion at each of the included locks (see page 26).
   - In the **Doors** tab add the Front Door
5. Click **Save**.

For more information, see Creating Access Levels (page 19).

## Configure the Credential Types

1. Navigate to **Sites | Credential Types**.
2. Add a credential type called DSR HID 34 Bit.

   In the **Commands** section enter: `DSRCredFormat = HID_34_BIT_PROPRIETARY`
3. Add a credential type called DSR MIFARE DESFire EV1 PROX_RAW.

   In the **Commands** section enter: `DSRCredFormat = PROX_RAW`
4. **Save** the credential type configurations.

For more information, see Configuring Credential Types (page 20).

## Configure the User Settings

1. Navigate to **Users | Users**.
2. Add Betty Manager.
   - Assign a **6-digit PIN**.
   - In the **Credentials** section, add the hexadecimal value of Betty's DESFire card in the **Credential** field of the DSR MIFARE DESFire EV1 PROX_RAW credential type.

     Credentials with PROX_RAW formats must be entered in hexadecimal format (see page 21).

     - Go to a lock and badge the MIFARE DESFire card that will be assigned to Betty.
     - Navigate to **Monitoring | Status Page View** and find the related Read raw credential data event.

       For example:

       ```
       Read raw credential data At Smart Reader 'Main Entrance Door 1' (SR0),
       Door 'Main Entrance Door 1' (DR8) : 56 bit 0x04698d326e5180
       ```

       The number at the end of the event description, **after** the **0x** hexadecimal format indicator, is the card number in hexadecimal format (e.g. 04698d326e5180).

       Take note of that number and enter it into the **Credential** field.

       You can also click the ellipsis **[...]** button at the top right of the list to **Copy** the event and paste it into a text file. Then copy and paste the required hex number into the Credential field.

   - Go to the **Access Levels** tab and assign the Manager access level.
3. Add Dirk Staff.
   - In the **Credentials** section, add the hexadecimal value of Dirk's DESFire card in the **Credential** field of the DSR MIFARE DESFire EV1 PROX_RAW credential type.
   - Go to the **Access Levels** tab and assign the Staff access level.
4. Add Victor Visitor.
   - In the **Credentials** section, add the site:card number of the DSR HID 34 Bit credential assigned to Victor (e.g. 1234:2468).
   - Go to the **Access Levels** tab and assign the Visitor access level.
5. **Save** the user configurations.

Betty Manager will now be able to access both doors at any time, using either her PIN or the DESFire card assigned above. Betty will also be able to latch unlock a door by badging her card twice at the lock.

Dirk Staff will be able to access the front door during office hours, using the DESFire card assigned above.

Victor Visitor will be able to enter the front door on one occasion only, during business hours, using HID 34 Bit card 1234:2468.

# Essential Programming

## DSR Server Configuration

DSR server security configuration is performed in ASSA ABLOY'S **DSR Support Tool**, while reader credential programming and WiFi lock alarms are configured in the ASSA ABLOY **Lock Configuration Tool (LCT)**.

### Security Configuration

The Protege GX ASSA ABLOY DSR integration supports TLS/SSL cryptographic security protocols.

TLS/SSL security is a prerequisite of this integration, and **must be enabled** on the DSR server, via the DSR Support Tool.

WS Encryption is **not** supported.

1. In the **DSR Support Tool**, navigate to **Configuration Settings | Server Settings | WS Encryption & Port Configuration**.
2. Ensure that **WS Encryption** is set to False.
3. Set **TLS/SSL Security** to True.
4. The **Sentinel-Bit** setting is not relevant to the integration.
5. The **Access Data Port** will automatically be updated to the default port of 8443 after TLS/SSL is enabled.

   This is the port that DSR opens for the Protege GX controller to communicate through, so the setting must match the **Ethernet Port** setting for the onboard reader expander (see page 16). The reader expander's Ethernet Port setting should be updated to mirror the updated DSR Access Data Port.
6. The **Lock Port** is the port DSR uses to communicate with the locks, and must match the lock configuration.
7. The **Security Valve** default setting is 127.0.0.1 and **must not be modified**.
8. Click **Update Configuration**.
9. You will need to manually **start the DSR service**, as this is automatically stopped when the configuration is updated.
   - Open the Windows **Services** snap-in by pressing the **Windows + R** keys, then typing **services.msc** into the search bar and pressing **Enter**.
   - Locate the **ASSA ABLOY Door Service Router** service and wait for it to stop.
   - Once the service has stopped, right click and **Start** the service.
10. To access the DSR Support Tool, you will need to enter the new URL: https://127.0.0.1:8443/dsrsupport/app/viewOnlineAPTab
11. There will be a warning: **Your connection isn't private**. Click the **Advanced** button below the warning.

    This warning may vary slightly in different browsers.
12. Click the **Continue to 127.0.0.1 (unsafe)** hyperlink to continue.
13. Confirm the updated security settings.

## Credential Configuration

The ASSA ABLOY locks in the integration need to be programmed with the correct credential configuration to recognize the Protege GX credentials.

The reader setup is configured as part of the lock profile in the ASSA ABLOY LCT (Lock Configuration Tool).

1. In the **Lock Configuration Tool**, navigate to **Lock Profile | Reader Setup**.
2. Set the **Reader** to multiCLASS Reader.

   This is the only tested read head type. Other read head types should operate but will require on-site validation.

3. Select the **Card Type** technologies as required for your credential type(s).
   - Select **HID Prox** to enable the following credential formats:
     - HID 26 Bit
     - HID 34 Bit
     - HID 34 Bit Proprietary
     - HID 37 Bit

     No additional configuration is required.

   - Select **MIFARE DESFire EV1** to enable MIFARE DESFire EV1.
     - Set the **Card Data Type** to CSN.
   - Select **MIFARE Classic 1K** to enable MIFARE Classic 1K.
     - Set the **Card Data Type** to Application.
     - Configure the KEY, Sector, Bit and other credential settings as required.
4. **Save** the reader setup. You must then **Configure** the locks to sync the updated profile.

If you have multiple lock profiles you will need to repeat the above credential configuration for each profile.

## WiFi Lock Alarms

ASSA ABLOY WiFi locks are configured to wake and send/receive updates periodically - typically daily in most scenarios. This means that events and status updates are cached, and only passed to Protege GX when these updates occur.

For some events or status updates it may not be acceptable to wait for this periodic update, so it is possible to configure alarms that will cause WiFi locks to wake when specific events occur and send/check for updates.

For example, when a user is denied access it may be preferable for the lock to wake and check for updates, in case the user is new and their credential details have not yet been downloaded. This will ensure that the lock is updated so the next time the user attempts to gain access their credential will be recognized.

Alarms for WiFi locks can be configured in the **Lock Profile** in the ASSA ABLOY **Lock Configuration Tool**. Refer to the appropriate ASSA ABLOY documentation for further information.

**Note**: Increasing the number of events that trigger immediate communication increases the battery consumption on WiFi locks.

# Configuration in Protege GX

## Enabling the Integration

The ASSA ABLOY DSR Integration needs to first be enabled on the Protege GX controller.

**IMPORTANT**: There must be only one controller enabled to communicate with each DSR server. Unexpected communication errors may result if multiple controllers communicate with a DSR server.

1. Navigate to **Sites | Controllers** and select the controller that will be used to communicate with the DSR server in this integration.
2. Expand the **Commands** section and enter the command: `DSRIP = true`
3. Click **Save**.

A controller can support up to 1024 ASSA ABLOY IP-enabled locks in this DSR integration. To support more locks an additional Protege GX controller and DSR server must be installed per additional 1024 locks.

## Enabling the Onboard Reader Expander

In this integration the controller's onboard reader expander must be addressed and its ethernet port must be enabled. If the onboard reader expander is not already enabled, complete the following steps:

1. Navigate to **Sites | Controllers** and select the controller that has the ASSA ABLOY DSR integration enabled.
2. In the **Configuration** tab, set the **Register as Reader Expander** field to any address that is not currently being used by a reader expander.
3. Click **Save**.
4. Navigate to **Expanders | Reader Expanders**. Select the relevant **Controller** in the toolbar.
5. **Add** a new reader expander and set the **Physical Address** to the address selected above.
6. Click **Save**.
7. In the **Module Configuration** window, review settings to create the inputs, outputs, trouble inputs and doors associated with the onboard reader expander. This may not be necessary if the onboard reader expander is only being used to receive data from the DSR server.
8. Click **Add Now**.

## Programming the Onboard Reader Expander

Communication with the DSR server is via the ethernet interface. The DSR server will send data to the Protege GX controller over a specified TCP/IP port, so the controller's onboard reader expander must be configured to receive incoming data over the ethernet network.

1. Navigate to **Expanders | Reader Expanders** and select the onboard reader expander of the controller that has the ASSA ABLOY DSR integration enabled.
2. Set the **Ethernet Network Type** to Third Party Generic. This enables the ethernet communication protocol required for the DSR integration.
3. Set the **Ethernet Port** to 8443. This is the port the controller will use to communicate with the DSR server and must match the DSR server's **Access Data Port** setting (see page 14).
4. To specify the DSR communication protocol, expand the **Commands** section and enter the command:
   `PortThree = 14`
5. To define the DSR server connection address, enter the command: `DSRIPAddress = x`
   where **x** is the IP address of the DSR server.

6. To define the DSR callback port, enter the command: `DSRCallbackPort = y`

   where **y** is the port number that the DSR server will use to send callback events to Protege GX.

   This can be any available port number. The default is 9090.

7. Click **Save**. Wait for the programming to be downloaded to the controller, then right click on the reader expander record and click **Update Module**.

Ensure that the firewall on the PC where the DSR server is installed is not blocking traffic on the ports assigned for communication and callback.

## Creating Doors

Each physical door that has an IP-enabled lock connected needs a door record configured in Protege GX. Each door record must then be assigned to a corresponding smart reader record that is mapped to the lock.

If the door records do not already exist, they will need to be added.

Unlike most locking integrations, where a specific **door type** must be configured to define the credential types that will be recognized by the doors, in this integration all access decisions are managed by the locks so a custom door type is not required.

1. Navigate to **Programming | Doors**.
2. **Add** a new door record with a **Name** that identifies its location.
3. Set the **Door Type** to the required authentication method.

   DSR supports only Card or PIN and Card and PIN. All other settings will be treated as Card or PIN.

4. Click **Save**.

Repeat the above steps to create the record for each door with an IP-enabled lock connected.

## Trouble Input Settings

The Door Forced Open, Door Left Open, Low Battery and Offline statuses are reported in Protege GX using trouble inputs. These trouble input records must exist for each door that is integrated with an IP-enabled lock.

Navigate to **Programming | Trouble Inputs** and create four trouble inputs for each door, with the following configurations.

### Door Forced Open

- **Module Type**: Door (DR)
- **Module Address**: Select the DSR door record.
- **Module Input**: 1
- **Trouble Group**: 3 - Access
- **Trouble Group Options**: AC Failure/Module Tamper/Forced Door

### Door Left Open

- **Module Type**: Door (DR)
- **Module Address**: Select the DSR door record.
- **Module Input**: 2
- **Trouble Group**: 3 - Access
- **Trouble Group Options**: Battery/Module Lost/Door Left Open

### Low Battery

- **Module Type**: Door (DR)
- **Module Address**: Select the DSR door record.
- **Module Input**: 4
- **Trouble Group**: 3 - Access
- **Trouble Group Options**: Battery/Module Lost/Door Left Open

### Lock Offline

- **Module Type**: Door (DR)
- **Module Address**: Select the DSR door record.
- **Module Input**: 6
- **Trouble Group**: 2 - System
- **Trouble Group Options**: Battery/Module Lost/Door Left Open

## Creating Smart Reader Records

In this integration each ASSA ABLOY IP-enabled lock is mapped to a Protege GX smart reader. This provides the configuration required for the controller to recognize each lock in the data sent from the DSR server.

1. Navigate to **Expanders | Smart Readers**.
2. In the toolbar, select the **Controller** that has the DSR integration enabled.
3. Click **Add** to create a new smart reader record that will represent a specific ASSA ABLOY lock.
4. Set the **Expander Address** to the Physical Address of the controller's onboard reader expander.
5. Set the **Expander Port** to Ethernet.
6. Set the **Configured Address** to <not set>.

   > The address will be configured by a command (see below).

7. To map the ASSA ABLOY lock to the smart reader record, expand the **Commands** section and enter the command: `SerialNumber = x`

   where **x** is the serial number of the lock this smart reader will represent.

   > The serial number can be found in the ASSA ABLOY Lock Configuration Tool.

8. Enter the command: `ConfiguredAddress = y`

   where **y** is the configured address of the smart reader.

   > Each smart reader must be assigned a unique configured address from 1 to 1024.

9. Go to the **Reader** tab and select the **Reader One Door** for this smart reader.

   This is the door connected to the ASSA ABLOY lock that is mapped to the smart reader.

10. Click **Save**.

Repeat the above process for each ASSA ABLOY IP-enabled lock. Every lock in the DSR system will need to be mapped to a smart reader record in Protege GX.

## Creating Access Levels

Access levels are required to provide users with access to DSR doors. A single access level may be used for access to all DSR doors, or multiple access levels may be used to provide more specific access control.

> Importantly, access levels play a pivotal role in determining which user credentials are sent to the DSR server and locks. Only credentials for users with an access level that provides access to a DSR door are sent, so access levels should exclude users who do not require access, in order to optimize System Capacity (see page 7).

1. Navigate to **Users | Access Levels**.
2. **Add** a new access level with a **Name** that identifies its access function.
3. Select the **Operating Schedule** that defines when this access level will allow user access.
4. Add the DSR **Doors** or **Doors Groups** this access level will allow users to access.
5. Click **Save**.
6. Navigate to **Users | Users | Access Levels**, select the user(s) who will need access to these doors, and **Add** the access level to the user(s).

> **Note**: All other access level settings are ignored by DSR.

## Configuring Credential Types

Protege GX sends user access privilege configurations to the DSR server, which in turn sends this information to the locks for making access decisions. For the locks to recognize Protege GX credentials, each Protege GX credential type must be configured with a compatible DSR credential format.

The locks must also be programmed to read these formats in the Lock Profile Reader Setup (see page 15).

1. Navigate to **Sites | Credential Types** and click **Add**.
2. Enter the **Name** for the credential type.
3. Expand the **Commands** section and enter the command: `DSRCredFormat = x`

   where **x** is the configured lock credential format for the credential type.

   DSR credential formats must be entered exactly as provided below.
4. Click **Save**.

**Note**: All other credential type settings are ignored in DSR.

### Supported DSR Credential Formats

The following credential formats are currently supported by DSR systems and IP-enabled locks:

- PROX_H_10301
- PROX_H_10302
- PROX_H_10304
- HID_33_BIT_PROPRIETARY
- HID_34_BIT_PROPRIETARY
- CORPORATE_1000
- PROX_RAW
- MAGNETIC_TRACK_2
- CORPORATE_1000_48
- PIV_40_BCD_MSB
- PIV_64_BCD_MSB
- PIV_75
- PIV_128_BCD_MSB
- PIV_200_BCD_MSB
- U_1000_56

If changing the **DSR credential format** for an existing credential type, the credential must first be **removed from all users** with that credential type assigned. Otherwise, the format mismatch will cause the locks to go out of sync (see page 37).

IP-enabled locks can be configured to read a vast array of highly configurable formats. While the integration supports the known DSR credential formats, only the following examples have currently been verified.

| Credential Format | `DSRCredFormat =` |
|---|---|
| HID 26 bit | PROX_H_10301 |
| HID 34 bit | HID_34_BIT_PROPRIETARY |
| HID 37 bit | PROX_RAW |
| MIFARE Classic 1K | PROX_RAW |
| MIFARE DESFire EV1 | PROX_RAW |

While the above credential formats have been tested and are supported by the integration, individual site and lock configurations vary significantly and a sample may be required to test and verify specific formats.

Your lock provider will need to supply details of the lock configuration and DSR credential format. A sample credential or raw data sample will help to test and verify the credential configuration.

## Assigning Credentials to Users

Each credential must be entered under the appropriate credential type created earlier, not as a card number.

1. Navigate to **Users | Users** and select or add the required user.
2. Scroll down to the **Credentials** section and add or update the necessary DSR credential type(s).
3. Enter the user's unique credential in the **Credential** field.
4. Click **Save**.

### Entering Credentials

- For all credential types using the **PROX_RAW** credential format the user's **Credential** must be entered in hexadecimal format (e.g. 04698d326e5180).
- For all other supported credential formats the user's **Credential** must be entered in the format of **xxxx:yyyy** where **xxxx** represents the site code, and **yyyy** represents the card number (e.g. 1234:2468).
- Where there is no site code the user's **Credential** must be entered in the format of **:yyyy** (including the preceding colon) where **yyyy** represents the card number (e.g. :2468).

### Identifying Hexadecimal Card Numbers

The raw hexadecimal data of PROX_RAW format cards can be identified by generating a read event.

1. Badge the card at one of the configured DSR locks. The lock will generate a general Denied Access event because it does not recognize the credential.
2. Navigate to **Monitoring | Status Page View**. The event will appear as a Read raw credential data event.

   For example:

   ```
   Read raw credential data At Smart Reader 'Main Entrance Door 1' (SR0), Door
   'Main Entrance Door 1' (DR8) : 56 bit 0x04698d326e5180
   ```

   The number at the end of the event string is the raw card data.

   - The 'bit' (e.g. 56 bit) identifies the credential format.
   - The 0x identifies that the number following is in hexadecimal format.
   - The number after the 0x is the card number that must be entered into the Credential field.

     (e.g. 04698d326e5180)
3. You can click the ellipsis **[...]** button at the top right of the events list to **Copy** a highlighted event and paste it into a text file. You can then copy and paste the required hexadecimal number into the Credential field.

## Add Credential to User

The raw card credential can also be assigned to a new or existing user directly from the event.

This adds the full raw card data string, so the user's credential will need to be edited afterwards. Care should be taken when assigning to users who already have access to DSR locks as the locks will become out of sync.

1. Right click the Read raw credential data event.
2. Select **Add New User** to create a new user to assign the raw credential to.
   - Select the **Credential Type** to assign the credential to, then click **OK**.

     A new user is created with the name 'User From Credential: ...', according to the type selected.
   - Remove the 'bit' format and 0x prefix from the **Credential** field, so that only the card number remains.

     For example, 56 bit 0x04698d326e5180 would be updated to 04698d326e5180.
   - Update the user's other details as required, then **Save**.
3. Select **Add Credential to Existing User** to assign the raw credential to a current user.
   - Use the dropdown list or enter a search in the **Record** field to select the user, then click **OK**.
   - Select the **Credential Type** to assign the credential to, then click **OK**.
   - Remove the 'bit' format and 0x prefix from the **Credential** field, so that only the card number remains.

     For example, 56 bit 0x04698d326e5180 would be updated to 04698d326e5180.
   - Click **Save**.

   **IMPORTANT**: If the existing user is already assigned an access level that gives them access to DSR doors, the raw credential will immediately be sent to the locks. This will cause the locks to go out of sync.

   After the credential is updated you will need to **Reload** the locks, as explained in the Troubleshooting section (see page 37). Alternatively, remove any access levels that give the user access to DSR locks before adding the raw credential. The credential will not be sent to the locks until you edit the credential and reassign the access level(s), so the locks will not go out of sync.

# Additional Programming

The following additional programming and functionality is supported in this integration.

## Schedules

Protege GX schedules are sent to the DSR server, including holiday groups and holiday mode settings. However, there are some limitations to the DSR implementation of holiday functionality.

The following table identifies the Protege GX schedule programming supported by the DSR integration.

<table>
<tr><th colspan="2">Sites | Schedules | Configuration</th></tr>
<tr><td>Periods</td><td>✓</td></tr>
<tr><td>Holiday Mode | Disabled on Holiday</td><td>✓</td></tr>
<tr><td>Holiday Mode | Enabled on Holiday</td><td>✗</td></tr>
<tr><td>Holiday Mode | Ignore Holiday</td><td>✓</td></tr>
<tr><th colspan="2">Sites | Holiday Groups | Holidays</th></tr>
<tr><td>Repeat</td><td>✗</td></tr>
<tr><td>Start Date / End Date (same date)</td><td>✓</td></tr>
<tr><td>Start Date / End Date (date range)</td><td>✗</td></tr>
</table>

- The DSR system is unable to support a date range for schedule exceptions, so each day/date of a holiday period needs to be created as an individual fixed date holiday record within the holiday group.
- Holidays will need to be individually created for each recurring year if required to repeat annually.

## User Functionality

### Protege GX User Settings

The following table identifies the Protege GX user programming supported by the DSR integration.

| **Users \| General** | |
|---|---|
| PIN | ✓ |
| PIN Expiry Time | ✓ |
| Card Numbers | ✗ |
| User Expiry Date/Time | ✓ |
| User Disable/Deletion | ✗ |
| User Area | ✗ |
| Credentials (including Disabled, Start, End) | ✓ |
| **Users \| Access Levels** | |
| Access Level Expires | ✗ |
| Schedule | ✓ |
| **Users \| Options \| General Options** | |
| Disable User | ✓ |
| Show a greeting message to user | ✗ |
| Go directly to the Menu on login | ✗ |
| User can Acknowledge Alarm Memory | ✗ |
| Show Alarm Memory on Login | ✗ |
| Turn Off the Primary Area if User has Access on Login | ✗ |
| Turn Off the User Area on Login if User has access | ✗ |
| Acknowledge System Troubles | ✗ |
| Treat User PIN Plus 1 as Duress | ✗ |
| **Users \| Options \| Advanced Options** | |
| User has super rights and can override antipassback | ✓ |
| User Operates Extended Door Access Function | ✓ |
| User Loiter Expiry Count Enabled | ✗ |
| User can Edit User Settings from Keypad | ✗ |
| User is a Duress User | ✗ |
| Rearm Area in Stay Mode | ✗ |
| **Users \| Options \| Dual Custody Options** | |
| Dual Custody Master | ✗ |
| Dual Custody Provider | ✗ |

# User PIN Codes

Locks with keypads support user PIN entry, with Card and PIN and Card or PIN access operation.

## Card or PIN

When the PIN is used as the primary credential (Card or PIN) the lock keypad requires entry of a **6-digit PIN**.

## Card and PIN

For Card and Pin authentication the integration will only recognize a **4-digit PIN**. If the user has a longer PIN in Protege GX the integration will recognize the first 4 digits as the user's valid PIN.

When the user PIN is used as the secondary credential (Card and PIN) the keypad interaction for dual credential authentication depends on whether the lock is configured in Standard (Sx) or Persona (Px) mode.

- In **Standard** mode: After entering the 4-digit PIN the user must press * on the keypad.
- In **Persona** mode: The user simply enters their 4-digit PIN.

**Note**: If using a combination of Card or PIN and Card and PIN across a site, it will be necessary for all users to have 6-digit PINs to access all necessary configurations.

# DSR Supervisor

The integration supports the DSR supervisor feature, through the use of the Protege GX super user setting.

**IMPORTANT**: A DSR supervisor can access a lock outside the unlock schedule, but unlike a Protege GX super user cannot access a DSR door that is locked down.

To enable DSR supervisor access for a user:

1. In Protege GX, navigate to **Users | Users** and select the user to assign DSR supervisor access to.
2. In the **Options** tab, enable the **User has super rights and can override antipassback** option.
3. Click **Save**.

Be aware that this will also enable super user privileges for the user in related Protege GX functionality.

# DSR Double Swipe

The integration supports the DSR double swipe functionality, which allows an authorized user to latch unlock a door by badging twice at the lock. The door will remain in the latch unlocked state until the user double swipes again, or it is overridden by another valid operation.

Double swipe functionality is only supported by locks in **Persona** (Px) mode. It is not supported by locks in Standard (Sx) mode. If double swipe access is applied to a lock in Standard mode, the lock will be latch unlocked by a single swipe from an authorized user.

DSR double swipe functionality is applied through Protege GX access levels, by adding the required command.

To enable DSR double swipe functionality:

1. Navigate to **Users | Access Levels** and select the access level to enable double swipe functionality for, or add a new access level specifically for this purpose.
2. Expand the **Commands** section and enter the command: `DoubleSwipeAccess = true`
3. Select a valid **Operating Schedule**. This cannot be set to Always.
4. Click **Save**.

**IMPORTANT**: To enable double swipe functionality, access levels with double swipe enabled must have a valid operating schedule assigned. If the schedule is set to **Always** the double swipe functionality is ignored in DSR.

## DSR One Time Access

The integration supports the DSR one time access functionality, which restricts a user to only one access occasion at each of the included locks.

DSR one time access is applied through Protege GX access levels, by adding the required command.

To enable DSR one time access functionality:

1. Navigate to **Users | Access Levels** and select the access level to enable one time access functionality for, or add a new access level specifically for this purpose.
2. Expand the **Commands** section and enter the command: `OneTimeAccess = true`
3. Click **Save**.

Each access level should have only one of double swipe or one time access enabled. Separate access levels are required for each feature. If a user has both assigned, one time access will take priority and double swipe functionality will be ignored by DSR.

Users with one time access assigned occupy one authorization each. The integration is restricted to 4,096 authorizations, so it is important to delete one time users after their access is complete, otherwise the integration can quickly reach the maximum number of authorizations.

## Authorization and User Option Behavior

In addition to the DSR supervisor, double swipe and one time access functionality, the Protege GX **User Operates Extended Door Access Function** and **Disable User** options also impact user access in this integration.

The table below illustrates the operational behavior when the various DSR authorization and Protege GX user options are applied in combination.

The integration applies a conservative approach and enforces the more secure result.

Important points to note:

- The integration prioritizes the Protege GX **Disable User** setting above all other options, including DSR supervisor, double swipe and one time access functionality.
- The integration prioritizes one time access over double swipe functionality, whereas DSR normally prioritizes double swipe over one time access.

| DSR Authorization Type | | | Protege GX User Option | | Behavior | |
|---|---|---|---|---|---|---|
| Supervisor | Double Swipe | One Time | Extended Access | Disable User | DSR | Integration |
| ✗ | ✗ | ✗ | ✓ | ✗ | Extended | Extended |
| ✗ | ✗ | ✗ | ✗ | ✓ | Disable | Disable |
| ✗ | ✗ | ✗ | ✓ | ✓ | Extended | **Disable** * |
| ✗ | ✓ | ✗ | ✗ | ✗ | Double Swipe | Double Swipe |
| ✗ | ✓ | ✗ | ✓ | ✗ | Double Swipe + Extended | **Double Swipe** * |
| ✗ | ✓ | ✗ | ✗ | ✓ | Disable | Disable |
| ✗ | ✓ | ✗ | ✓ | ✓ | Double Swipe + Extended | **Disable** * |
| ✓ | ✗ | ✗ | ✗ | ✗ | Supervisor | Supervisor |
| ✓ | ✗ | ✗ | ✓ | ✗ | Supervisor | Supervisor |
| ✓ | ✗ | ✗ | ✗ | ✓ | Disable | Disable |
| ✓ | ✗ | ✗ | ✓ | ✓ | Supervisor | **Disable** * |
| ✗ | ✗ | ✓ | ✗ | ✗ | One Time | One Time |
| ✗ | ✗ | ✓ | ✓ | ✗ | One Time | One Time |
| ✗ | ✗ | ✓ | ✗ | ✓ | Disable | Disable |
| ✗ | ✗ | ✓ | ✓ | ✓ | One Time | **Disable** * |
| ✓ | ✓ | ✗ | ✗ | ✗ | Supervisor + Double Swipe | Supervisor + Double Swipe |
| ✓ | ✓ | ✗ | ✓ | ✗ | Supervisor + Double Swipe | Supervisor + Double Swipe |
| ✓ | ✓ | ✗ | ✗ | ✓ | Disable | Disable |
| ✓ | ✓ | ✗ | ✓ | ✓ | Supervisor + Double Swipe | Disable |
| ✓ | ✗ | ✓ | ✗ | ✗ | Supervisor | Supervisor |
| ✓ | ✗ | ✓ | ✓ | ✗ | Supervisor | Supervisor |
| ✓ | ✗ | ✓ | ✗ | ✓ | Disable | Disable |
| ✓ | ✗ | ✓ | ✓ | ✓ | Supervisor | **Disable** * |
| ✗ | ✓ | ✓ | ✗ | ✗ | Double Swipe | **One Time** * |
| ✗ | ✓ | ✓ | ✓ | ✗ | Double Swipe + Extended | **One Time** * |
| ✗ | ✓ | ✓ | ✗ | ✓ | Disable | Disable |
| ✗ | ✓ | ✓ | ✓ | ✓ | Double Swipe + Extended | **Disable** * |

# Door Functionality

## Protege GX Door Settings

The following table identifies the Protege GX door programming supported by the DSR integration.

* **Door Type**: DSR supports only Card or PIN and Card and PIN. All other settings will be treated as Card or PIN.

<table>
<tr><th colspan="2">Doors | General | Setup</th></tr>
<tr><td>Door Type *</td><td>✓</td></tr>
<tr><td>Slave Door</td><td>✗</td></tr>
<tr><td>Area Inside Door</td><td>✗</td></tr>
<tr><td>Area Outside Door</td><td>✗</td></tr>
<tr><td>Unlock Schedule</td><td>✗</td></tr>
<tr><td>Door Pre-Alarm Delay Time</td><td>✗</td></tr>
<tr><td>Door Left Open Alarm Time</td><td>✓</td></tr>
<tr><td>Interlock Door Group</td><td>✗</td></tr>
<tr><th colspan="2">Doors | Options | Door Options</th></tr>
<tr><td>Always Check Unlock Schedule</td><td>✗</td></tr>
<tr><td>Enable Open/Close Events on Schedule</td><td>✗</td></tr>
<tr><td>Relock on Door Close</td><td>✓</td></tr>
<tr><td>Relock on Door Open</td><td>✓</td></tr>
<tr><td>Unlock Door On REX</td><td>✗</td></tr>
<tr><td>Unlock Door On REN</td><td>✗</td></tr>
<tr><td>Schedule Operates Late to Open</td><td>✗</td></tr>
<tr><th colspan="2">Doors | Options | Door Options 2</th></tr>
<tr><td>Door Lock Follows Inside Area</td><td>✗</td></tr>
<tr><td>Door Lock Follows Outside Area</td><td>✗</td></tr>
<tr><td>Prevent Slave Unlock on Inside Area</td><td>✗</td></tr>
<tr><td>Prevent Unlock on Schedule if Inside Area Armed</td><td>✗</td></tr>
<tr><td>Prevent Unlock on Schedule if Outside Area Armed</td><td>✗</td></tr>
<tr><td>Area Disarmed AND Schedule Valid Unlock Door</td><td>✗</td></tr>
<tr><td>Area Disarmed OR Schedule Valid Unlock Door</td><td>✗</td></tr>
<tr><td>Enable Access Taken on REX/REN Events</td><td>✗</td></tr>
<tr><td>Schedule Overrides Latch</td><td>✗</td></tr>
<tr><th colspan="2">Doors | Advanced Options | Advanced Options</th></tr>
</table>

| | |
|---|---|
| Update User Area when Passback Disabled | ✗ |
| Lock out REX when Inside Area Armed | ✗ |
| Deny Entry if Inside Area is Armed | ✗ |
| Deny Exit if Outside Area is Armed | ✗ |
| Prompt User For Access Reason Code | ✗ |
| Enable Access Taken on Door Unlock Events | ✗ |
| **Doors \| Advanced Options \| Extended Access Time Options** | |
| Door Extended Access Time | ✓ |
| Antipassback Entry User Reset Time | ✗ |
| Antipassback Exit User Reset Time | ✗ |
| Reset Antipassback Status on Schedule | ✗ |
| Enable Timed User Antipassback Reset | ✗ |
| Antipassback Reset Schedule | ✗ |

## DSR Wait for 2nd PIN Duration

The integration supports DSR Wait for 2nd PIN Duration, which defines the maximum time that a keypad will wait for a user to enter their PIN after presenting their card when logging in to a keypad that requires dual credential authentication.

Implementation of this feature in Protege GX requires a command to be added to each door.

1. Navigate to **Programming | Doors** and select the door(s) to program the wait duration for.
2. Expand the **Commands** section and enter the command: `DualCredPendingTime = x`

   where **x** is the duration in seconds.
3. Click **Save**.

## DSR Invalid Attempts Until Lockout

The integration supports DSR Invalid Attempts Until Lockout, which defines the number of invalid login attempts that can be made before lockout is activated.

Implementation of this feature in Protege GX requires a command to be added to each door.

1. Navigate to **Programming | Doors** and select the door(s) to program the number of invalid attempts for.
2. Expand the **Commands** section and enter the command: `LockOutAttempts = x`

   where **x** is the number of invalid attempts that will activate lockout.
3. Click **Save**.

The lockout feature in DSR is supported for locks operating in Standard (Sx) mode only. Lockout is not supported for locks operating in Persona (Px) mode.

## DSR Extended Unlock Duration

The integration supports DSR Extended Unlock Duration, which defines the duration that a door remains opens for users identified as requiring extended access.

In Protege GX this is programmed via the **Extended Door Access Time** setting of each door.

1. Navigate to **Programming | Doors** and select the door(s) to configure the extended access time for.
2. In the **Advanced Options** tab set the **Extended Door Access Time** (in seconds).
3. Click **Save**.

The extended duration operates for users with **User Operates Extended Door Access Function** enabled.

## DSR Door Ajar Time

The integration supports DSR Door Ajar Time, which defines the maximum amount of time after a door opening event is generated before a door left open alarm is generated.

In Protege GX this is programmed via the Door Left Open Alarm Time setting of each door.

1. Navigate to **Programming | Doors** and select the door(s) to configure the extended access time for.
2. Set the **Door Left Open Alarm Time** (in seconds).
3. Click **Save**.

# Device Specific Commands

The integration supports a range of additional customizable ASSA ABLOY lock functions which can be programmed using commands.

## Device Commands

Only the device commands specified in the table below are supported by this integration. Unsupported commands will not be sent to the DSR server.

| ID | Command | Value Type |
|---|---|---|
| 35 | Daylight Savings Time In Effect Flag | BOOL |
| 36 | Daylight Savings Time Mode Select | U8 |
| 37 | Daylight Savings Time Skip Forward Month | U8 |
| 38 | Daylight Savings Time Skip Forward Day | U8 |
| 39 | Daylight Savings Time Skip Forward Week | U8 |
| 40 | Daylight Savings Time Skip Forward DOW | U8 |
| 41 | Daylight Savings Time Skip Forward Hour | U8 |
| 42 | Daylight Savings Time Skip Forward Minute | U8 |
| 43 | Daylight Savings Time Skip Forward Adjust | U8 |
| 44 | Daylight Savings Time Fall Back Month | U8 |
| 45 | Daylight Savings Time Fall Back Day | U8 |
| 46 | Daylight Savings Time Fall Back Week | U8 |
| 47 | Daylight Savings Time Fall Back DOW | U8 |
| 48 | Daylight Savings Time Fall Back Hour | U8 |
| 49 | Daylight Savings Time Fall Back Minute | U8 |
| 50 | Daylight Savings Time Fall Back Adjust | U8 |
| | | |
| 72 | Visible Feedback Enable | BOOL |
| 73 | Audible Feedback Enable | BOOL |
| 74 | Visible Indicators Enable | BOOL |
| 75 | Audible Indicators Enable | BOOL |
| | | |
| 78 | Duration Of Lockout (seconds) | U8 |
| 80 | Invalid Credential Idle Reset Time (seconds) | U8 |
| 102 | Strike Unlock Duration (seconds) | U8 |
| | | |
| 114 | Scheduling Algorithm | U8 |
| 115 | Scheduler Awake Duration (decaseconds) | U8 |

| ID | Command | Value Type |
|---|---|---|
| 116 | Period Scheduler Awakens (minutes) | U16 |
| 117 | Scheduler Hour Of Day Map | STRING |
| 118 | Scheduler Day Of Week Map | U8 |
| 119 | Scheduler Day Of Month Map | U32 |
| 120 | Scheduler On At Hours:Minutes #1 | U16 |
| 121 | Scheduler On At Hours:Minutes #2 | U16 |
| 122 | Scheduler On At Hours:Minutes #3 | U16 |
| 123 | Scheduler On At Hours:Minutes #4 | U16 |
| | | |
| 131 | Inhibit Voltage Threshold | U8 |
| 132 | Low Voltage Warning Threshold | U8 |
| | | |
| 141 | Mag Card Separator Inclusion | BOOL |
| 142 | Mag Card Fields | U8 |
| 143 | Mag Card Data Offset | U8 |
| 144 | Mag Card Data Digits | U8 |
| | | |
| 150 | Fail Open/Secure | BOOL |
| 152 | RX Held Time (seconds) | U8 |
| 155 | Passage Mode Indicator | BOOL |
| 157 | Prox Strip Sentinel | BOOL |
| 158 | iClass Prox Strip Sentinel | BOOL |
| 160 | Use 2nd Credential | BOOL |
| 162 | Lock Description | STRING |
| 163 | Anti-Tailgating | U8 |
| 164 | Anti-Tailgating Delay | U8 |
| 166 | Prox 37 Add Sentinel | BOOL |
| 167 | RTC Recovery Mode | U8 |
| 168 | Audible Access | BOOL |

For information on the specific functionality and configuration options of the device commands, refer to the relevant ASSA ABLOY documentation.

For **Mag Card** commands, DSR will only send MAGNETIC_TRACK_2 credentials to locks that support magstripe readers. It will not send magstripe credentials to IN120 or IN220 lock types.

- **Mag Card Separator Inclusion**: Indicates whether the field separator character is part of the data to be returned. If set, rather than being deleted from the string sent to the server, the separator character will be included. This allows the server to make additional decisions based on the contents of the cards.
- **Mag Card Fields**: Defines which fields are to be returned. If a magnetic card contains 12;3456789;399 the configuration can be programmed to return only the 1st and 3rd fields, resulting in 12399 being returned.
- **Mag Card Data Offset**: Defines the offset into the concatenated string to start returning digits. Using the example above, and programming this option with a value of 2, the returned value would be 2399.
- **Mag Card Data Digits**: Defines the number of digits to return. Normally, the full number of concatenated digits would be returned, however in the 2399 example above, if this option were set to 3 the number returned would be 239.

Magstripe card credentials are sent in decimal value using card format **MAGNETIC_TRACK_2**

The **Anti-Tailgating** feature supports a maximum delay time of 25.5 seconds, entered in **deciseconds**. For example, a delay of 10 seconds would be configured by programming a value of 100.

## Programming Device Specific Commands

The behavior is specific to each lock, and must therefore be added to the programming of the corresponding smart reader record for each lock device, as required.

1. Navigate to **Expanders | Smart Readers** and select the smart reader record(s) to customize.
2. Expand the **Commands** section and add the required command(s) for the desired functionality, as described in the table below.

   Each device command must be added in a separate command line, in the format:

   `DSC = <ID>,<value>`

   Where the `<ID>` corresponds to the relevant command ID (from the Device Commands table above), and the `<value>` represents the value to be applied to the function.

For example:

```
DSC = 78,12
DSC = 72,true
DSC = 162,MAINLOCK
```

### Valid Values

The supported value types and their valid values are as follows:

| Type | Description |
|---|---|
| BOOL | Boolean. Valid values are **true** and **false** |
| STRING | All standard **alphanumeric** characters are valid |
| U8 | 8 bit unsigned char. Valid values are numeric values from **0 to 255** |
| U16 | 16 bit unsigned short. Valid values are numeric values from **0 to 65535** |
| U32 | 32 bit unsigned integer. Valid values are numeric values from **0 to 4,294,967,295** |

# DSR Integration Commands Summary

| | | |
|---|---|---|
| Controller | | |
| `DSRIP = true` | Enables DSR integration | (see page 16) |
| `DSRSendPINCredential = false` | Excludes sending user PINs to DSR | (see page 7) |
| Reader Expander | | |
| `PortThree = 14` | Enables the DSR communication protocol | (see page 16) |
| `DSRIPAddress = <IPAddress>` | Defines the DSR server connection address | |
| `DSRCallbackPort = <Port>` | Defines the DSR callback port | |
| Smart Reader | | |
| `SerialNumber = <Serial>` | Maps the ASSA ABLOY lock to the smart reader | (see page 19) |
| `ConfiguredAddress = x` | Defines the Configured Address of the smart reader | |
| `DSC = <CommandID>,<Value>` | Defines DSR Device Specific Command programming | (see page 31) |
| Credential Type | | |
| `DSRCredFormat = <Format>` | Defines DSR credential formats | (see page 20) |
| Access Level | | |
| `DoubleSwipeAccess = true` | Enables DSR Double Swipe access | (see page 25) |
| `OneTimeAccess = true` | Enables DSR One Time access | (see page 26) |
| Door | | |
| `DualCredPendingTime = x` | Defines the DSR Wait for 2nd PIN Duration | (see page 29) |
| `LockOutAttempts = x` | Defines the DSR Invalid Attempts Until Lockout | (see page 29) |

# Operation

## Access Control Limitations

The following Protege GX access control features are **not** supported by DSR locks:

- Door alarm settings
- LED control
- Antipassback
- Function codes
- Double and triple badging

  DSR Double Swipe functionality (see page 25) partially addresses this feature.

## Manual Commands

Protege GX manual door commands are supported by PoE locks.

Manual commands are not supported by WiFi locks and will be ignored.

To send a manual command to a PoE lock:

1. Navigate to **Programing | Doors** and select the door(s) to send the command to.
2. Right click the door record and select the required command:

   DSR supports only one lockdown state, so all lockdown commands will initiate **Full Lockdown**. However the Protege GX event generated will show the specific lockdown state triggered by the operator.

### DSR Panic Mode

The integration supports DSR Panic Mode on PoE locks, which is initiated by Protege GX Lockdown.

Any of the Protege GX lockdown commands (Allow Entry, Allow Exit, Allow Entry+Exit, Deny Entry+Exit) will trigger panic mode on the selected lock(s). The Protege GX lockdown Clear command will clear panic mode.

WiFi locks do not support Protege GX lockdown commands so panic mode cannot be initiated.

## Lock Status

The following lock status/events are sent from the DSR server to the Protege GX controller:

- Door Open
- Door Forced Open
- Door Left Open
- Door Closed
- Door Locked
- Request to Exit
- Granted Access
- Denied Access
- Low Battery

**Note**: Fixed handle locks send a Request to Exit event after every Access Granted event. This is because the inside handle turns whenever the outside handle is turned, which triggers the REX in DSR.

## Status Updates and Events

When viewing events in Protege GX, the **Field Time** represents the time the event is recorded at the lock, while the **Logged Time** is the time the record is received from the DSR server and logged in Protege GX.

Status and event messaging examples are provided in Event Messaging (see page 38).

- Online locks automatically send events and status updates to the DSR server as they occur. DSR then returns them to the Protege GX controller via the callback response.
- Offline locks will send on next update, unless configured in DSR to wake on specific events (see page 15).

  Due to the offline nature of WiFi locks the status displayed in Protege GX status lists may not accurately reflect the current state of the lock.

## Lock Status

The table below identifies the status displayed for online and offline locks for each event or lock state.

| Action | PoE Door Status | WiFi Door Status |
|---|---|---|
| Idle | Closed, Locked | Closed |
| Access Granted | Closed, Locked | Closed |
| Access Denied | Closed, Locked | Closed |
| Door Open | Open, Locked | Open |
| Door Closed | Closed, Locked | Closed |
| Door Forced | Forced Open, Locked | Forced Open |
| Door Left Open | Left Open, Locked | Left Open |
| Manual Command:<br>Unlock Latched - Door Closed | Closed, Unlocked By User Latched | Closed |
| Manual Command:<br>Unlock Latched - Door Open | Open, Unlocked By User Latched | Open |
| Manual Command:<br>Lockdown (any) - Door Closed | Closed, Locked Down (Full Lockdown) | Closed |
| Manual Command:<br>Lockdown (any) - Door Open | Open, Locked Down (Full Lockdown) | Open |
| Manual Command:<br>Lockdown (any) - Door Forced | Forced Open, Locked Down (Full Lockdown) | Forced Open |

Manual commands are not supported by WiFi locks and will be ignored, therefore the status does not change when a manual command is triggered.

The Door Forced Open, Door Left Open, Low Battery and Offline statuses are reported in Protege GX using trouble inputs (see page 18).

When a lock goes offline its status cannot be determined until it comes back online and updates.

**Known Issue**: There is a limitation when a lock goes offline while its status is Unlocked Latched - Door Open where the lock is unable to recognize a door closed event after it comes back online. To recover the lock, close the door and send a manual command to lock the door.

# Troubleshooting

## Locks Out of Sync

Integrated locks can become 'Out of Sync' with the DSR server. This occurs when a credential has been sent in an unexpected range or format that the lock does not recognize.

In the DSR Support Tool this is identified on the homepage by the **Sync Status** being displayed in red.

This can be easily rectified in the DSR Support Tool by selecting the lock, which displays the **Lock Detail** page. Clicking the **Reload Lock** button will reload the lock and resolve the Sync Status issue.

**IMPORTANT**: The credential record that caused the sync issue must be corrected before reloading the lock, otherwise the same issue will occur and the lock will remain out of sync.

# Event Messaging

The following Protege GX event messages are supported by the DSR integration.

| Connecting to DSR |
|---|
| <READER_EXPANDER_NAME> Connecting to DSR |
| • Example: Onboard Reader Expander Connecting to DSR |
| **Online with DSR** |
| <READER_EXPANDER_NAME> Online with DSR |
| • Example: Onboard Reader Expander Online with DSR |
| **Offline with DSR** |
| <READER_EXPANDER_NAME> Offline with DSR |
| • Example: Onboard Reader Expander Offline with DSR |
| **Synchronization Completed** |
| <READER_EXPANDER_NAME> Sync with DSR Completed |
| • Example: Onboard Reader Expander Sync with DSR Completed |
| **Door Forced Open** |
| Door <DOOR_NAME> (<DOOR_ID>) Forced Open<br>Trouble Input <TROUBLE_INPUT_NAME> (<TROUBLE_INPUT_ID>) Opened |
| • Example:<br>Door Main Entrance Door 1 (DR8) Forced Open<br>Trouble Input Main Entrance Door 1 Forced Open (97) Opened |
| **Door Left Open** |
| Door <DOOR_NAME> (<DOOR_ID>) Left Open<br>Trouble Input <TROUBLE_INPUT_NAME> (<TROUBLE_INPUT_ID>) Opened |
| • Example:<br>Door Main Entrance Door 1 (DR8) Left Open<br>Trouble Input Main Entrance Door 1 Left Open (98) Opened |
| **Door Locked** |
| Door <DOOR_NAME> (<DOOR_ID>) Closed |
| • Example: Door Main Entrance Door 1 (DR8) Closed |
| **Request to Exit** |
| Door <DOOR_NAME> (<DOOR_ID>) Request To Exit (Free Egress) |
| • Example: Door Main Entrance Door 1 (DR8) Request To Exit (Free Egress) |
| **Granted Access** |
| User <USER_NAME> (<USER_ID>) Granted Entry To <DOOR_NAME> (<DOOR_ID>) Access Level <ACCESS_LEVEL_NAME> (<ACCESS_LEVEL_ID>) Using Credentials : <SITE_CODE>:<CARD_NUMBER> |

| |
|---|
| • Example: User Test Manager (UN1) Granted Entry To Main Entrance Door 1 (DR8) Access Level Manager (AL1) Using Credentials : 3456:2345<br>For security purposes, in any event where a PIN code is entered the messaging will simply display PIN. |
| **Denied Access (Credential Not Recognized)** |
| Read raw credential data At Smart Reader '<SMART_READER_NAME>' (<SMART_READER_ID>), Door '<DOOR_NAME>' (<DOOR_ID>) : <CREDENTIAL_BIT> bit <CREDENTIAL_RAW_VALUE> |
| • Example: Read raw credential data At Smart Reader 'Main Entrance Door 1' (SR0), Door 'Main Entrance Door 1' (DR8) : 56 bit 0x048030c28a5b80 |
| **Denied Access (Schedule Not Valid)** |
| User <USER_NAME> (<USER_ID>) Schedule Not Valid At <DOOR_NAME> (<DOOR_ID>) Access Level <ACCESS_LEVEL_NAME> (<ACCESS_LEVEL_ID>) Using Credentials : <SITE_CODE>:<CARD_NUMBER> |
| • Example: User Test Manager (UN2) Schedule Not Valid At Main Entrance Door 1 (DR8) Access Level Manager (AL1) Using Credentials : 170:43690 |
| **Denied Access (Disabled)** |
| User <USER_NAME> (<USER_ID>) Denied Access At <DOOR_NAME> (<DOOR_ID>) Access Level <ACCESS_LEVEL_NAME> (<ACCESS_LEVEL_ID>) Using Credentials : <SITE_CODE>:<CARD_NUMBER> |
| • Example: User Test Manager (UN2) Denied Access At Main Entrance Door 1 (DR8) Access Level Manager (AL1) Using Credentials : 170:43690 |
| **User or Credential Disabled** |
| User <USER_NAME> (<USER_ID>) Record Disabled At <MODULE_TYPE_NAME><MODULE_ADDRESS> Port <READER_PORT> Using Credentials : <SITE_CODE>:<CARD_NUMBER> |
| • Example: User Test Manager (UN2) Record Disabled At RD1 Port Error Using Credentials : 170:43690<br>Note: The integration is currently not able to identify the <READER_PORT> and will display 'Error'. |
| **User or Credential Expired** |
| User <USER_NAME> (<USER_ID>) Record Expired At <MODULE_TYPE_NAME><MODULE_ADDRESS> Port <READER_PORT> Using Credentials : <SITE_CODE>:<CARD_NUMBER> |
| • Example: User Test Manager (UN2) Record Expired At RD1 Port Error Using Credentials : 170:43690<br>Note: The integration is currently not able to identify the <READER_PORT> and will display 'Error'. |
| **Denied Access by Lockdown** |
| User <USER_NAME> (<USER_ID>) Access Denied By Door Lockdown At <DOOR_NAME> (<DOOR_ID>) Using Credentials : <SITE_CODE>:<CARD_NUMBER> |
| • Example: User Test Manager (UN2) Access Denied By Door Lockdown At Main Entrance Door 1 (DR8) Using Credentials : 170:43690 |
| **Low Battery** |
| Trouble Input <TROUBLE_INPUT_NAME> (<TROUBLE_INPUT_ID>) Opened |
| • Example: Trouble Input Main Entrance Door 1 Low Battery (101) Opened |
| **Lock Offline** |
| Trouble Input <TROUBLE_INPUT_NAME> (<TROUBLE_INPUT_ID>) Opened |
| • Example: Trouble Input Main Entrance Door 1 Lock Offline (102) Opened |

# System Debug Error Events

To assist in the initial commissioning of the integration and troubleshooting, system debug events allow viewing of integration errors between the DSR server and the controller. These events will automatically be generated whenever the error condition occurs.

These events can be viewed by navigating to **Monitoring | Status Page View**.

**System Debug Event 377 Sub 5 Data 0009:0000:0000:0000**

Indicates a failure to send a command to the DSR server.

- The debug event is generated after five failed send attempts
- The first data section (0009) is the code representing the command type in the failed packet

Refer to the Command Types table below for command types and codes.

**System Debug Event 377 Sub 100 Data 2EE2:0000:0000:0000**

Indicates that the number of user records for the lock exceeds the maximum capacity.*

- The first data section (2EE2) is the hexadecimal database ID of the last user record sent

**System Debug Event 377 Sub 101 Data 2EE6: 0004:0000:0000**

Indicates that the credential format for the user is not supported by DSR.

- The first data section (2EE6) is the hexadecimal database ID of the last user record sent
- The second data section (0004) is the database ID of the credential type record

**System Debug Event 377 Sub 102 Data 0000:0000:0000:0000**

Indicates that the system has reached the maximum number of authorizations.

This error typically occurs when there are too many one time users in the system.

## Command Types

The following table shows the command types that may be sent to the DSR server.

The **Command Code** will appear in System Debug Event 377 Sub 5 (see above) to indicate which type of command packet has failed.

| Command Code | Command Type |
|---|---|
| 0000 | DSR_COMMAND_LOCK |
| 0001 | DSR_COMMAND_UNLOCK |
| 0002 | DSR_COMMAND_LOCK_DOWN_ENABLE |
| 0003 | DSR_COMMAND_LOCK_DOWN_DISABLE |
| 0004 | DSR_COMMAND_GET_DOOR_LIST |
| 0005 | DSR_COMMAND_CONFIRM_DOOR |
| 0006 | DSR_COMMAND_REGISTER_CALLBACK |
| 0007 | DSR_COMMAND_UNREGISTER_CALLBACK |
| 0008 | DSR_COMMAND_NOTIFY_UPDATE_RESPONSE |
| 0009 | DSR_COMMAND_ADD_USER |

| Command Code | Command Type |
|---|---|
| 000A | DSR_COMMAND_MODIFY_USER |
| 000B | DSR_COMMAND_REMOVE_USER |
| 000C | DSR_COMMAND_GET_USER_ID |
| 000D | DSR_COMMAND_ADD_AUTHORIZATION |
| 000E | DSR_COMMAND_MODIFY_AUTHORIZATION |
| 000F | DSR_COMMAND_REMOVE_AUTHORIZATION |
| 0010 | DSR_COMMAND_GET_AUTHORIZATION_ID |
| 0011 | DSR_COMMAND_ADD_DAY_PERIOD |
| 0012 | DSR_COMMAND_MODIFY_DAY_PERIOD |
| 0013 | DSR_COMMAND_REMOVE_DAY_PERIOD |
| 0014 | DSR_COMMAND_GET_DAY_PERIOD_ID |
| 0015 | DSR_COMMAND_ADD_DAY_EXCEPTION |
| 0016 | DSR_COMMAND_MODIFY_DAY_EXCEPTION |
| 0017 | DSR_COMMAND_REMOVE_DAY_EXCEPTION |
| 0018 | DSR_COMMAND_GET_DAY_EXCEPTION_ID |
| 0019 | DSR_COMMAND_ADD_DAY_EXCEPTION_GROUP |
| 001A | DSR_COMMAND_MODIFY_DAY_EXCEPTION_GROUP |
| 001B | DSR_COMMAND_REMOVE_DAY_EXCEPTION_GROUP |
| 001C | DSR_COMMAND_GET_DAY_EXCEPTION_GROUP_ID |
| 001D | DSR_COMMAND_ADD_SCHEDULE |
| 001E | DSR_COMMAND_MODIFY_SCHEDULE |
| 001F | DSR_COMMAND_REMOVE_SCHEDULE |
| 0020 | DSR_COMMAND_GET_SCHEDULE_ID |
| 0021 | DSR_COMMAND_GET_NEW_LOGS |
| 0022 | DSR_COMMAND_GET_DSR_STATUS |
| 0023 | DSR_COMMAND_SET_ACCESS_POINT_MODE |
| 0024 | DSR_COMMAND_SET_DATE_TIME |
| 0025 | DSR_COMMAND_REMOVE_USER_CASCADING |
| 0026 | DSR_COMMAND_CLEAR_ALL |
| 0027 | DSR_COMMAND_GET_SUPPORTED_CREDENTIAL_FORMATS |
| 0028 | DSR_COMMAND_SEND_DEVICE_SPECIFIC_COMMAND |

# Appendix A: User Synchronization Timing

The table below illustrates the synchronization process and timing under optimum network latency conditions.

| Sync Scenario | Total Timing |
|---|---|
| Initial sync of 1 user for 1 lock | ~650ms |
| Add a new user to the system or delete existing user for 1 lock | ~650ms |
| Alter access for 1 user for 1 lock | ~650ms |
| | |
| Initial sync of 9,999 users for 1 lock | ~40 mins |
| Add a new user or delete existing user for 1 lock with 9,999 users previously synced | ~5 secs |
| Alter access for 1 user for 1 lock with 9,999 users previously synced | ~9 secs |
| | |
| Initial sync of 9,999 users for 1024 locks | ~149 mins |
| Add a new user or delete existing user for 1024 locks with 9,999 users previously synced | ~63 mins |
| Alter access for 1 user for 1024 locks with 9,999 users previously synced | ~109 mins |

* Timing based on initializing connection at the beginning of each packet, and includes overhead to allow the system controller to maintain standard operations during synchronization with the DSR server.

# Appendix B: Event Timing

The table below illustrates the timing for the DSR server to return lock events to the Protege GX controller via the callback response process, under optimum network latency conditions.

| | Minimum Callback Response | Maximum Callback Response |
|---|---|---|
| PoE Lock | 1 second | 7 seconds |
| WiFi Lock * | 10 seconds **after the lock wakes** | 20 seconds **after the lock wakes** |

* Callback response for WiFi locks begins after the lock wakes and connects to the DSR server.

# Appendix C: Frequently Asked Questions

**Q: How do I obtain the ASSA ABLOY firmware, documentation, tools and related material and/or information?**

A: Certified Integrator (CI) needs to create an account on https://secure.intelligentopenings.com/en/resources/partner-area/apply-for-account/ or go to https://www.intelligentopenings.com/en/ using the Partner Area option to gain access to available resources.

**Q: Where can I download the DSR application?**

A: ASSA ABLOY Access Control Partners who have integrated their access control system software using DSR have the application available.

**Q: How do I configure the IP-enabled locks to communicate with DSR?**

A: ASSA ABLOY lock configuration is performed using the Lock Configuration Tool (LCT).

**Q: Where can I download the LCT application?**

A: The latest LCT version is available to download from https://assaabloy.box.com/lockconfigurationtool

**Q: Can the Door Service Router (DSR) be installed on the same server as the Protege GX Database/Application server?**

A: No. DSR must be located on its own physical/virtual machine (see page 5).

**Q: How many locks can a DSR support?**

A: The number of locks supported by a DSR is currently 1024. If more than 1024 locks are to be used a second DSR would be required.

**Q: How many Protege GX controllers can connect to a DSR?**

A: One controller (PRT-CTRL-DIN or PRT-CTRL-DIN-1D) can be connected to each DSR. Unexpected communication errors may result if multiple controllers are connected to a DSR.

**Q: Does Protege GX allow for multiple DSR integrations?**

A: Yes. The DSR requires connection to a controller on a one-to-one relationship.

**Q: How many user credentials can be concurrent in the ASSA ABLOY locks?**

A: ASSA ABLOY locks store up to 9,999 user credentials (see page 7).

**Q: What is the default communication port between the DSR and the IP-enabled locks?**

A: The default port used is 2571 and must match the lock configuration.

**Q: Can the Security Valve setting be changed to a local network IP address?**

A: **No**. In the DSR security configuration (see page 14) the Security Valve value of the localhost IP is 127.0.0.1 and **must not be modified**.

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.