AN-254

Configuring OSDP Readers in Protege

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: 02-Jun-23 01:35 PM

Contents

Introduction

OSDP (Open Supervised Device Protocol) is an industry standard communications protocol, developed to improve interoperability among access control and security products. Unlike older standards such as Wiegand, OSDP utilizes a two-way channel and encrypted communications between the reader and the expander module, known as secure channel communication.

ICT controllers and reader expanders support OSDP reader connections on their RS-485 reader ports, allowing you to extend your system with readers from a number of manufacturers.

OSDP readers function in a similar way to ICT readers using RS-485, but the Protege modules require additional configuration. This document outlines the prerequisites and supported functionality for OSDP readers in the Protege system, and the programming steps required. It does not include configuration of third-party devices.

ICT card readers also support OSDP and secure channel communication, and can be configured for OSDP operation with a Protege system. All Protege system prerequisites and programming are as documented here, the same as required for third-party readers. For ICT card reader information and programming, see Application Note 321: Configuring ICT Readers for OSDP Communication.

Supported Readers

The number of access control devices which have been tested and verified as compliant for OSDP 2.2 is constantly growing. The SIA website provides a comprehensive list of OSDP Verified Products.

Supported Baud Rates

Protege modules support OSDP readers with baud rates set at 9600, 19200 and 38400. The OSDP reader should be configured with one of these supported baud rates before being connected to a Protege module.

Supported Functionality

The ICT implementation of OSDP conforms to a subset of the OSDP 2.2 standard specification.

Protege hardware supports a maximum of two OSDP readers connected to each reader port.

Feature	Supported	Note
Communications		
Secure Channel communications	✓	Supports 128 bit AES encryption. For more information, see Secure Channel Communication (page 8).
Offline operation	✗	
Input Functions		
Wiegand card read (OSDP_RAW)	✓	Card reads must send the raw Wiegand bit stream to be decoded by the ICT controller. Card and site codes decoded by the OSDP reader itself are **not** supported.
Keypad entry (OSDP_KPD)	✓	Numeric key presses are processed after the hash (**#**) key is pressed (i.e. the hash key is treated as an Enter key). Pressing the star (*****) key cancels the numeric entry (i.e. the star key is treated as a Cancel key).
Tamper (OSDP_LSTATR)	✓	The osdp_LSTATR command is used to monitor both reader tamper and power loss states. Whenever the command is received by the connected Protege module the associated trouble input state will be updated. See Programming the Reader Tamper Switch (see page 21)
Biometric read	✗	
Digital input	✗	
Output Functions		
Buzzer control (OSDP_BUZZ)	✓	
LED control (OSDP_LED)	✓	
Output control	✗	
Text display	✗	
Date/Time display	✗	

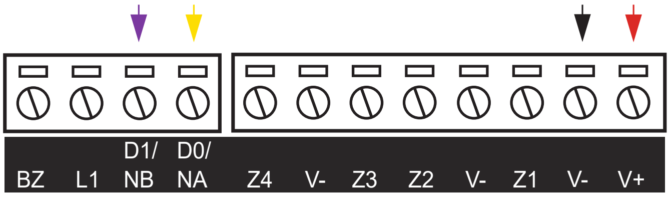
Connecting OSDP Readers

When using the OSDP protocol the reader should be connected to the reader port of the Protege controller or reader expander using a standard RS-485 wiring configuration.

- The reader's RS-485 **A** wire should be wired to the reader port's **D0/NA** connection.
- The reader's RS-485 **B** wire should be wired to the readers port's **D1/NB** connection.

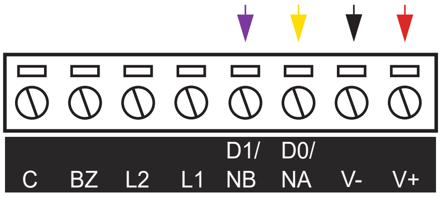
Reader Port Connections

The diagram below illustrates the wiring connection for an OSDP reader connected to a Protege controller.



This connection example shows wiring for ICT readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

The diagram below illustrates the wiring connection for an OSDP reader connected to a Protege reader expander.



This connection example shows wiring for ICT readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Reader Wiring Connections

The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	**V+** 12VDC positive
12VDC- negative	**V-** 12VDC negative
RS-485 **A**	**D0/NA** RS-485 A
RS-485 **B**	**D1/NB** RS-485 B
Shield (drain)	Frame grounded at one point only

OSDP Reader Location

As two OSDP readers can be connected to the same Protege module reader port, each OSDP reader is configured as either an Entry or Exit reader in the **Reader location** setting of the associated **smart reader** record.

OSDP reader location is **not** determined by the reader address.

Secure Channel Communication

Secure channel is the two-way encryption and authentication scheme used by OSDP devices to protect communication between controllers and readers, by requiring them to establish a secure session.

A secure channel session is initiated with a handshake that involves two command-reply transactions between the controller and reader, which perform mutual authentication and establish an encrypted session using a shared AES-128 key to secure the communication between the two devices.

Once the communication session between the two devices is secured the reader will not accept communication from another device without a new secure session being established.

Key Rotation

OSDP 2.2 advocates key rotation, whereby a new key is shared between the controller and the reader within the existing secure session. A new session is then established using the new key.

Whether using randomly generated keys or manual key management, key rotation can be performed from the user interface at any time. Because a secure session is already established the reader does not need to be placed in installation mode or reconfigured. It is updated with the new key from the controller within the established session.

Users who are conscious of digital security will want to rotate keys in much the same way as they would the digital certificate for a website.

Random Key Generation

The preferred method of session key management is random key generation, using **OSDP installation mode**. The reader is initially placed in installation mode so that a secure encrypted session can be established between the module and the reader, and a session key is randomly generated by the controller and shared with the reader.

Activating OSDP Installation Mode in OSDP Readers

Installation mode is required for the Protege module to establish secure communications with the OSDP reader. The reader must be placed in installation mode first, to allow the controller to initiate the secure session process.

See the OSDP reader's installation manual for instructions on activating installation mode.

The reader only needs to be placed in installation mode to establish a secure session during initial commissioning or replacement. Once readers are connected over a secure channel a new randomly generated key can be initiated from the user interface and the reader will remain online and be updated with the new key.

Activating OSDP Installation Mode from the User Interface

Once the reader has been placed in installation mode, the process of pairing the module with the reader is initiated from the user interface to establish the secure connection.

When in installation mode the Protege module will attempt to establish a session with the reader. If a session can be established the module will send a command to program the reader with a custom encryption key which is randomly generated by the controller. After the reader is configured with the key the module will terminate the session and create a new session using the custom key.

This process can be performed from the user interface at any time to initiate a new randomly generated key. The reader does not need to be placed in installation mode again once the secure channel connection is established.

Manual Key Management

For sites who prefer not to use installation mode to randomly generate session keys, these can be managed manually. The reader must be preconfigured with an encryption key which matches the key assigned in the associated system programming. The controller will not be able to initiate a secure session with a reader which is not configured with the expected encryption key.

See the OSDP reader's installation manual for instructions on configuring encryption keys.

The reader only needs to be preconfigured with the initial session key. Once readers are connected over a secure channel a new key can be programmed in the user interface and the reader will remain online and be updated with the new key. This can be performed at any time to update the shared encryption key.

Manual Key Diversification

The actual key used by the Protege module when initiating a secure session will be diversified and unique to each reader. Most ODSP readers will diversify the key they are programmed with, so the reader needs to be programmed with exactly the same key as programmed in the Protege system.

If the third-party reader does not automatically diversify its encryption key, you must use the manual diversification method outlined below to create the diversified key to be programmed on the reader.

ICT tSec readers with firmware version 1.04.277 and above will automatically diversify the key that has been configured, so your OSDP TLV config should contain the same key as entered in the system programming.

Key Diversification Method

Protege modules use a key diversification method which is optionally recommended by the OSDP 2.2 specification.

- The diversified key is generated by encrypting data derived from the client unique identifier (cUID) using the key entered in the reader expander configuration.
- The cUID is generated by the client (PD) and typically incorporates the serial number of the PD.
- The cUID must be 8 bytes long.
- The key data is encrypted using AES-128 with Cipher Block Chaining (CBC) and an initialization vector of 0.

Key Diversification Example

- Base key (from the Protege module programming): `FA6905847CC465FD827530AD3B194211`
- cUID: `0A00170202CAFEDE`
- Inverted (bitwise not) cUID: `F5FFE8FDFD350121`
- Concatenated cUID: `0A00170202CAFEDEF5FFE8FDFD350121`
- AES Initialisation vector (IV): `00000000000000000000000000000000`

  The concatenated cUID must be AES encrypted using the original base key. A number of AES encryption calculators can be found online for this purpose.

- Resulting diversified key: `E6248DE5382BD5AB25F28B44C3718B4F`

The OSDP reader must then be preconfigured with the **resulting diversified key**. This is what the Protege module will use when attempting to establish a secure connection with the reader.

Unencrypted Communications

While it is not recommended, OSDP readers can be connected to Protege modules without configuring secure channel communication. This is compliant with the OSDP 2.2 'basic' profile, but not with the 'secure' profile.

Protege GX Programming

The following sections outline the steps required to configure Protege GX controllers and reader expanders to communicate with OSDP readers connected to their reader ports.

Protege GX Prerequisites

OSDP readers are supported on the reader ports of Protege controllers and reader expanders. The following prerequisites are required to connect OSDP readers to a Protege GX system.

Component	Version	Notes
Protege GX Software	4.3.329.3 or higher	
Protege GX Controller	2.08.1353 or higher	The minimum firmware version is required even if OSDP readers are not connected to the onboard reader ports.
Protege Reader Expander	1.12.599 or higher	

No licenses are required for connecting OSDP readers to Protege GX systems.

Configuring the Controller's Onboard Reader Expander

If OSDP readers are to be connected to a Protege GX controller's reader ports, first the controller's onboard reader expander needs to be configured.

1. Navigate to **Sites | Controllers** and select the controller with OSDP readers connected.
2. In the **Configuration** tab, set the following:
   - **Register as reader expander**: The address of a reader expander which will represent the controller's onboard reader expander.
   - **Onboard reader lock outputs**: Set to Controller relay 3/4 outputs.
3. Click **Save**.
4. If necessary, navigate to **Expanders | Reader expanders** and create a new reader expander record with a **Physical address** matching the **Register as reader expander** address set above.

Configuring Reader Expander Ports

Each reader port which has an OSDP reader connected needs to be configured to enable OSDP operation.

> Before configuring the reader ports you should check that there are no smart reader records already referencing the expander's address and port. The automated smart reader creation process is unable to check for records linked to the expander, so if any do exist duplicates will be created which will result in errors when saving.

1. Navigate to **Expanders | Reader expanders** and configure the reader expanders that will have OSDP readers connected (including the controller's onboard reader expander, if applicable).
2. If an OSDP reader is connected to Port 1, in the **General** tab set the **Port 1 network type** to OSDP.
3. If an OSDP reader is connected to Port 2, in the **General** tab set the **Port 2 network type** to OSDP.
4. If using function codes the door that the OSDP reader will control needs to be assigned in the **Reader 1/2** tab.

   > Function codes will not operate correctly if the reader 1/2 door is <not set>.

   - Select the **Reader 1/2** tab for the reader port that the reader is physically connected to.
   - Set the **Reader 1/2 door** to the door that the OSDP reader will control.
5. Click **Save**. The associated OSDP smart reader records will be automatically generated.

OSDP Smart Readers

One smart reader record is required for each OSDP reader connected to the system. The smart reader provides the configuration for the Protege system to communicate with the OSDP reader.

> Even if two OSDP readers are connected to the same reader port to provide entry/exit from a single door, two smart reader records are required.

When a reader expander's **Port 1/2 network type** is changed to OSDP and the reader expander record is **saved** the system automatically generates the required smart reader records associated with those reader ports.

- Two smart reader records are created for each OSDP enabled reader port, to accommodate connecting up to two OSDP readers (entry and exit) per port.
- Each automatically created smart reader is associated with the specific reader expander and configured with its expander address and expander port settings, and these cannot be altered.
- An OSDP smart reader record can be manually deleted, and a new smart reader record can be manually added and associated with the expander and port, but a maximum of two smart readers can be associated with any OSDP reader port and an error message will be displayed if more are attempted.
- If the Port 1/2 network type setting is changed from OSDP, any associated smart reader records will be deleted. A popup message will prompt for confirmation before deleting.
- OSDP smart readers are specifically associated with the OSDP reader port they are created for and cannot be assigned for other smart reader functions.
- OSDP smart readers do not require smart reader licenses and will not impact the usage of any existing smart reader records or licenses.

Configuring Smart Reader Records

The auto-generated smart reader records will need to be customized for the OSDP readers they represent.

1. Navigate to **Expanders | Smart readers**.
2. If necessary, edit the smart reader **Name** to clearly identify the OSDP reader it represents.
3. The **Expander address** is automatically configured to the **Physical address** of the reader expander this OSDP smart reader is associated with, and cannot be changed.
4. The **Expander port** is automatically configured to the reader port this OSDP smart reader is associated with, and cannot be changed.
5. Select the **Configured address** for the OSDP reader. This is the OSDP address of the reader **+ 1**.

   The supported OSDP reader address range is from **0 to 127**. Because it is not possible to assign an address of 0 in the user interface, 1 is deducted from the **Configured address** to calculate the reader's OSDP address.

6. In the **Reader** tab, set the **Reader one format** to the format that will be used by the OSDP reader.
7. Set the **Reader location** to Entry or Exit.
8. Select the **Door** that this OSDP reader will control.

   If using function codes this door must also be assigned in the **Reader 1/2** tab of the reader expander that the OSDP reader is physically connected to.

9. Click **Save**.
10. A module update is required to load the smart reader settings onto the reader expander.
    - Navigate to **Expanders | Reader expanders** and select the reader expander that the OSDP reader is connected to.
    - Wait for the configuration changes to be downloaded to the controller, then right click on the reader expander record and click **Update module**.

The reader expander will identify the OSDP reader and automatically detect its baud rate to establish a connection. Supported reader baud rates are 9600, 19200 and 38400.

Configuring Secure Channel Communication

The secure channel session key may be preconfigured, or randomly generated using OSDP installation mode. Once the communication session between the two devices is secured the reader will not accept communication with another device, without a new secure session being established.

It is recommended that you validate that the readers are working with unencrypted communications before configuring secure channel.

Configuring Random Key Generation

If a key is manually programmed in the smart reader this overrides random key generation. When installation mode is activated the manual key is used to establish a secure connection. A new key will **not** be generated. If legacy port session key commands exist in reader expander programming, installation mode will not activate.

The process of pairing the Protege module with the OSDP reader is initiated from the user interface.

1. You must first place the OSDP reader in installation mode so that it is ready to accept the session initiation. See the OSDP reader's installation manual for instructions on activating installation mode.

   ICT readers can be placed into installation mode by applying a **Hex** TLV with the Hex code **080103**, or with the Protege Config App **Device Mode** TLV set to **OSDP Install Mode**.

2. To activate installation mode in Protege GX, navigate to **Expanders | Reader expanders**.
3. Right click on the reader expander record and click **Activate OSDP install mode**. This will trigger a module update and place the module in installation mode.

When in installation mode the Protege module will attempt to establish a session with the reader. If a session can be established the module will send a command to program the reader with a custom encryption key which is randomly generated by the controller. After the reader is configured with the key the module will terminate the session and create a new session using the custom key.

Once a secure session is established, key rotation can be performed by simply activating OSDP install mode from the user interface. The reader does not need to be placed in installation mode again. A new key is randomly generated by the controller and updated to the reader within the existing secure session. A new session is then established using the new key. This process can be performed from the user interface at any time.

Randomly generated session keys are stored on the controller and associated reader expanders, not in the software. If the controller is defaulted or replaced a new secure session will need to be established with any OSDP readers connected to its reader ports. This includes placing the reader in installation mode so that it will accept initiation of a new secure session from a new connection. If the controller and reader expander are replaced simultaneously, the same will apply to OSDP readers connected the to the expander's reader ports.

Configuring Manual Key Management

For sites who prefer not to use installation mode to randomly generate session keys, these can be managed manually. Before you begin, you will need to generate 128 bit encryption keys for use with your OSDP readers.

OpenSSL is a useful tool for generating encryption keys.

Configuring OSDP Readers with Session Keys

The reader must be preconfigured with an encryption key which matches the key assigned in the associated smart reader programming.

ICT readers can be configured by applying a **Hex** TLV with the Hex code **0311<SessionKey>FF**. For example, for key FC9905847CC465FD827530AD3B194213 apply TLV **0311**FC9905847CC465FD827530AD3B194213**FF**.

Configuring Session Keys in Protege GX

1. In Protege GX, navigate to **Expanders | Smart readers** and select the appropriate smart reader record.
2. In the **Commands** field, enter the following command:

   ```
   SessionKey = X
   ```

   Where **X** is the AES encryption key to be used in secure sessions with the reader.

   Once a secure session is established, the session key can be updated at any time to perform manual key rotation within the secure session, without the reader needing to be preconfigured with the new key.

3. A module update is required to update the reader expander configuration and trigger a secure session with the connected OSDP readers.
   - Navigate to **Expanders | Reader expanders** and select the reader expander that the OSDP reader is connected to.
   - Wait for the configuration changes to be downloaded to the controller, then right click on the reader expander record and click **Update module**.

Upon module update, the reader expander will make **one attempt** to establish a secure session with each OSDP smart reader associated with its expander address (see page 12). If session creation fails for any reason (e.g. key mismatch) you will need to apply another module update to trigger a new session creation attempt.

Once a secure session is established, key rotation can be performed by simply updating the SessionKey command and performing a module update. The reader does not need to be preconfigured with the new key. The new key is updated to the reader within the existing secure session. A new session is then established using the new key. This process can be performed from the user interface at any time to program a new key.

Port Session Keys

It is possible to apply a session key to the reader port of the reader expander, rather than each smart reader.

This is a legacy programming option which provides backward compatibility for existing installations and is not recommended. It is not compliant with the OSDP 2.2 requirement to use one unique session key per reader, and installation mode is disabled if a key is manually programmed in the reader expander.

- If there is more than one reader connected to the reader port they will both use the same session key. This is not compliant with OSDP 2.2 which requires one key per reader.
- If session key commands exist in the smart reader programming they will take precedence over any port session key commands in the reader expander programming.
- Installation mode will not activate if session key commands exist in the reader expander programming.

Configuring Port Session Keys in Protege GX

1. To program port session keys, navigate to **Expanders | Reader expanders** and select the required reader expander.
2. In the **Commands** field, enter the following commands:

   ```
   Port1SessionKey = X
   Port2SessionKey = Y
   ```

   Where **X** and **Y** are the AES encryption keys to be used in secure sessions with the readers on ports 1 and 2 respectively.

3. A module update is required to update the reader expander configuration and trigger a secure session with the connected OSDP readers. Wait for the configuration changes to be downloaded to the controller, then right click on the reader expander record and click **Update module**.

Upon module update, the reader expander will make **one attempt** to establish a secure session with each OSDP smart reader associated with its expander address (see page 12). If session creation fails for any reason (e.g. key mismatch) you will need to apply another module update to trigger a new session creation attempt.

Configuring Unencrypted Communications

While it is not recommended for live operation, OSDP readers can be connected to Protege modules without configuring secure channel communication.

> Unencrypted communication is compliant with the OSDP 2.2 'basic' profile, but not with the 'secure' profile.

Protege modules are unencrypted by default and when configured for OSDP operation will communicate with an unencrypted reader without requiring any session key programming. However, if installation mode is ever initiated in Protege GX a session key will be generated and the module will stop communicating with the reader.

1. To force unencrypted communications, navigate to **Expanders | Reader expanders** and select the required reader expander.
2. In the **Commands** field, enter the following commands:

   ```
   Port1SessionKey = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   Port2SessionKey = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   ```

   > These commands must be entered to ensure unencrypted communications. If no PortSessionKey command is present, a session key will be randomly generated by the controller when OSDP installation mode is activated.

   > You must also ensure that no session key commands exist in the smart reader programming as they will take precedence over the commands in the reader expander programming.

3. A module update is required to update the reader expander configuration. Wait for the configuration changes to be downloaded to the controller, then right click on the reader expander record and click **Update module**.

Protege WX Programming

The following sections outline the steps required to configure Protege WX controllers and reader expanders to communicate with OSDP readers connected to their reader ports.

Protege WX Prerequisites

OSDP readers are supported on the reader ports of Protege controllers and reader expanders. The following prerequisites are required to connect OSDP readers to a Protege WX system.

Component	Version	Notes
Protege WX Controller	4.00.1465 or higher	The minimum firmware version is required even if OSDP readers are not connected to the onboard reader ports.
Protege Reader Expander	1.12.599 or higher	

No licenses are required for connecting OSDP readers to Protege WX systems. However, advanced mode must be enabled on your controller.

Configuring Reader Expander Ports

Each reader port which has an OSDP reader connected needs to be configured to enable OSDP operation.

1. Navigate to **Expanders | Reader Expanders** and configure the reader expanders that will have OSDP readers connected (including the controller's onboard reader expander, if applicable).
2. If an OSDP reader is connected to Port 1, in the **General** tab set the **Port 1 Network Type** to OSDP.
3. If an OSDP reader is connected to Port 2, in the **General** tab set the **Port 2 Network Type** to OSDP.
4. Click **Save**. The associated OSDP smart reader records will be automatically generated.

If any pre-existing smart reader record references an expander's OSDP port the automated smart reader process will link to and use this as the port's OSDP smart reader. It will not create or allow duplicate port assignments.

OSDP Smart Readers

One smart reader record is required for each OSDP reader connected to the system. The smart reader provides the configuration for the Protege system to communicate with the OSDP reader.

Even if two OSDP readers are connected to the same reader port to provide entry/exit from a single door, two smart reader records are required.

When a reader expander's **Port 1/2 network type** is changed to OSDP and the reader expander record is **saved** the system automatically generates the required smart reader records associated with those reader ports.

- Two smart reader records are created for each OSDP enabled reader port, to accommodate connecting up to two OSDP readers (entry and exit) per port.
- Each automatically created smart reader is associated with the specific reader expander and configured with its expander address and expander port settings, and these cannot be altered.
- An OSDP smart reader record can be manually deleted, and a new smart reader record can be manually added and associated with the expander and port, but a maximum of two smart readers can be associated with any OSDP reader port and an error message will be displayed if more are attempted.
- If the Port 1/2 network type setting is changed from OSDP, any associated smart reader records will be deleted. A popup message will prompt for confirmation before deleting.
- OSDP smart readers are specifically associated with the OSDP reader port they are created for and cannot be assigned for other smart reader functions.
- OSDP smart readers do not require smart reader licenses and will not impact the usage of any existing smart reader records or licenses.

Configuring Smart Reader Records

The auto-generated smart reader records will need to be customized for the OSDP readers they represent.

1. Navigate to **Expanders | Smart Readers**.
2. If necessary, edit the smart reader **Name** to clearly identify the OSDP reader it represents.
3. The **Expander Address** is automatically configured to the **Physical Address** of the reader expander this OSDP smart reader is associated with, and cannot be changed.
4. The **Expander Port** is automatically configured to the reader port this OSDP smart reader is associated with, and cannot be changed.
5. Select the **Configured Address** for the OSDP reader. This is the OSDP address of the reader **+ 1**.

   The supported OSDP reader address range is from **0 to 127**. Because it is not possible to assign an address of 0 in the user interface, 1 is deducted from the **Configured Address** to calculate the reader's OSDP address.

6. In the **Reader** tab, set the **Reader One Format** to the format that will be used by the OSDP reader.
7. Set the **Reader Location** to Entry or Exit.
8. Select the **Door** that this OSDP reader will control.
9. Click **Save**.
10. A module update is required to load the smart reader settings onto the reader expander.
    - Navigate to **Expanders | Reader Expanders** and select the reader expander that the OSDP reader is connected to.
    - In the toolbar, click **Restart** to update the module.

The reader expander will identify the OSDP reader and automatically detect its baud rate to establish a connection. Supported reader baud rates are 9600, 19200 and 38400.

Configuring Secure Channel Communication

The secure channel session key may be preconfigured, or randomly generated using OSDP installation mode. Once the communication session between the two devices is secured the reader will not accept communication with another device, without a new secure session being established.

It is recommended that you validate that the readers are working with unencrypted communications before configuring secure channel.

Configuring Random Key Generation

If a key is manually programmed in the smart reader this overrides random key generation. When installation mode is activated the manual key is used to establish a secure connection. A new key will **not** be generated. If legacy port session key commands exist in reader expander programming, installation mode will not activate.

The process of pairing the Protege module with the OSDP reader is initiated from the user interface.

1. You must first place the OSDP reader in installation mode so that it is ready to accept the session initiation. See the OSDP reader's installation manual for instructions on activating installation mode.

   ICT readers can be placed into installation mode by applying a **Hex** TLV with the Hex code **080103**, or with the Protege Config App **Device Mode** TLV set to **OSDP Install Mode**.

2. To activate installation mode in Protege WX, navigate to **Expanders | Reader Expanders**.
3. Select the reader expander record then click the **OSDP Install Mode** icon in the toolbar. This will trigger a module update and place the module in installation mode.

   This option is accessible when at least one of the **Port Network Type** settings is set to OSDP. If the selected reader expander does not have any ports configured for OSDP the icon is disabled and cannot be selected.

When in installation mode the Protege module will attempt to establish a session with the reader. If a session can be established the module will send a command to program the reader with a custom encryption key which is randomly generated by the controller. After the reader is configured with the key the module will terminate the session and create a new session using the custom key.

Once a secure session is established, key rotation can be performed by simply activating OSDP install mode from the user interface. The reader does not need to be placed in installation mode again. A new key is randomly generated by the controller and updated to the reader within the existing secure session. A new session is then established using the new key. This process can be performed from the user interface at any time.

Randomly generated session keys are stored on the controller and associated reader expanders. If the controller is defaulted or replaced a new secure session will need to be established with any OSDP readers connected to its reader ports. This includes placing the reader in installation mode so that it will accept initiation of a new secure session from a new connection. If the controller and reader expander are replaced simultaneously, the same will apply to OSDP readers connected the to the expander's reader ports.

Configuring Manual Key Management

For sites who prefer not to use installation mode to randomly generate session keys, these can be managed manually. Before you begin, you will need to generate 128 bit encryption keys for use with your OSDP readers.

OpenSSL is a useful tool for generating encryption keys.

Configuring OSDP Readers with Session Keys

The reader must be preconfigured with an encryption key which matches the key assigned in the associated smart reader programming.

ICT readers can be configured by applying a **Hex** TLV with the Hex code **0311<SessionKey>FF**. For example, for key FC9905847CC465FD827530AD3B194213 apply TLV **0311**FC9905847CC465FD827530AD3B194213**FF**.

Configuring Session Keys in Protege WX

1. In Protege WX, navigate to **Expanders | Smart Readers** and select the appropriate smart reader record.
2. In the **Commands** field, enter the following command:

   ```
   SessionKey = X
   ```

   Where **X** is the AES encryption key to be used in secure sessions with the reader.

   Once a secure session is established, the session key can be updated at any time to perform manual key rotation within the secure session, without the reader needing to be preconfigured with the new key.

3. A module update is required to update the reader expander configuration and trigger a secure session with the connected OSDP readers.
   - Navigate to **Expanders | Reader Expanders** and select the reader expander that the OSDP reader is connected to.
   - In the toolbar, click **Restart** to update the module.

Upon module update, the reader expander will make **one attempt** to establish a secure session with each OSDP smart reader associated with its expander address (see page 17). If session creation fails for any reason (e.g. key mismatch) you will need to apply another module update to trigger a new session creation attempt.

Once a secure session is established, key rotation can be performed by simply updating the SessionKey command and performing a module update. The reader does not need to be preconfigured with the new key. The new key is updated to the reader within the existing secure session. A new session is then established using the new key. This process can be performed from the user interface at any time to program a new key.

Port Session Keys

It is possible to apply a session key to the reader port of the reader expander, rather than each smart reader.

This is a legacy programming option which provides backward compatibility for existing installations and is not recommended. It is not compliant with the OSDP 2.2 requirement to use one unique session key per reader, and installation mode is disabled if a key is manually programmed in the reader expander.

- If there is more than one reader connected to the reader port they will both use the same session key. This is not compliant with OSDP 2.2 which requires one key per reader.
- If session key commands exist in the smart reader programming they will take precedence over any port session key commands in the reader expander programming.
- Installation mode will not activate if session key commands exist in the reader expander programming.

Configuring Port Session Keys in Protege WX

1. To program port session keys, navigate to **Expanders | Reader Expanders** and select the required reader expander.
2. In the **Commands** field, enter the following commands:

   ```
   Port1SessionKey = X
   Port2SessionKey = Y
   ```

   Where **X** and **Y** are the AES encryption keys to be used in secure sessions with the readers on ports 1 and 2 respectively.

3. A module update is required to update the reader expander configuration and trigger a secure session with the connected OSDP readers. In the toolbar, click **Restart** to update the module.

Upon module update, the reader expander will make **one attempt** to establish a secure session with each OSDP smart reader associated with its expander address (see page 17). If session creation fails for any reason (e.g. key mismatch) you will need to apply another module update to trigger a new session creation attempt.

Configuring Unencrypted Communications

While it is not recommended for live operation, OSDP readers can be connected to Protege modules without configuring secure channel communication.

Unencrypted communication is compliant with the OSDP 2.2 'basic' profile, but not with the 'secure' profile.

Protege modules are unencrypted by default and when configured for OSDP operation will communicate with an unencrypted reader without requiring any session key programming. However, if installation mode is ever initiated in Protege WX a session key will be generated and the module will stop communicating with the reader.

1. To force unencrypted communications, navigate to **Expanders | Reader Expanders** and select the required reader expander.
2. In the **Commands** field, enter the following commands:

   ```
   Port1SessionKey = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   Port2SessionKey = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   ```

   These commands must be entered to ensure unencrypted communications. If no PortSessionKey command is present, a session key will be randomly generated by the controller when OSDP installation mode is activated.

   You must also ensure that no session key commands exist in the smart reader programming as they will take precedence over the commands in the reader expander programming.

3. A module update is required to update the reader expander configuration. In the toolbar, click **Restart** to update the module.

Additional Programming

This section includes some additional configuration which may be required for your site.

Programming the Tamper Switch / Power Loss Trouble Input

If your OSDP readers have physical tamper switches or power loss reporting, you can monitor these states using a trouble input. This trouble input will open when the card reader reports either tamper switch opening or power loss using the osdp_LSTATR packet.

Readers which do not support osdp_LSTATR (including ICT card readers) are monitored using the pre-programmed Reader Tamper trouble inputs (see page 23).

To program the trouble inputs:

1. Navigate to **Programming | Trouble inputs** and select the controller to be configured.
2. Click **Add** to create a new trouble input and give it a relevant name, such as RD2 DR1 OSDP Tamper Switch / Power Loss.
3. Set the **Module type** to Door (DR).
4. For the **Module address**, select the door that the card reader controls.
5. Set the **Module input** to 3.
6. To allow reporting of this trouble input, open the **Areas and input types** tab and program the trouble input into a system area with the required input type (such as Trouble Silent).
7. Click **Save**.
8. Repeat for each OSDP reader.

Configuring LED Colors

The default LED colors for readers are blue (off) and green (on). L1 and L2 LED color settings can be configured for OSDP readers if different colors are required. To set the LED color, the configuration command needs to be added to the programming of the LED output.

1. Navigate to **Programming | Outputs** and select the LED output record. The following outputs can be configured:
   - Output 3 (Green LED Port 1)
   - Output 4 (Red LED Port 1)
   - Output 6 (Green LED Port 2)
   - Output 7 (Red LED Port 2)
2. Add the command `LEDColour = X` to the output's **Commands** field, where **X** corresponds to the appropriate color code from the table below:

Number (X)	Color
1	Red
2	Amber
6	Green
12	Blue
14	Purple

3. Click **Save**.

Custom LED colors may not function correctly when enhanced reader outputs are enabled and activated on the reader port. This is a known issue. This operation has not yet been validated with area status display functionality, function codes and 'LED follows lock' functionality (i.e. when the door's lock output is not the default reader port lock output) handled by the controller.

Notes and Limitations

Reader Outputs

The reader's buzzer is controlled automatically by the access granted or denied functions, or can be controlled manually by activating Output 5 (reader port 1) or Output 8 (reader port 2) of the associated reader expander.

The reader's LEDs are controlled automatically by the LED follows lock function. The green LED can be controlled manually by activating Output 3 (reader port 1) or Output 6 (reader port 2) of the associated reader expander. The default color is blue and the LED will change to green when activated. These colors can be configured using output commands (see page 21).

Reader Tamper Behavior

The Reader Tamper trouble inputs for OSDP readers operate based on the number of smart readers programmed for that port. If the number of readers detected by the reader expander is less than the number or smart readers programmed, the trouble input will be opened.

This is trouble input 12 for reader port 1 and trouble input 13 for reader port 2.

In addition, if the OSDP reader has a tamper switch it can be monitored by a separate customized trouble input (see page 21). The power status of the reader is also mapped to the same trouble input.

OSDP reader sabotage is monitored via the module network's intelligent reader tamper detection functionality.

Function Codes

Function codes allow you to define a function - such as arming an area or activating an output - that can be activated by users from a card reader with a PIN pad.

To use function codes on readers connected using the OSDP protocol, in addition to the **Reader** tab of the smart reader record the door must also be assigned in the **Reader 1/2** tab of the reader port that the OSDP reader is physically connected to. Function codes will not operate correctly from a reader where the **Reader 1/2 door** in the connected port's reader expander record is <not set>.

LED Color Limitations

OSDP reader LEDs are limited to displaying red, amber, green, blue or purple colors only. Any other colors configured for display on ICT readers will be converted as per the table below. This affects features such as function codes, dual credential pending LEDs and area status LEDs.

ICT Configured LED Color	OSDP Reader LED Display
Red	Red
Crimson	
Amber	Amber
Orange	
Yellow	
Green	Green
Mint	
Turquoise	
Lime	
Blue	Blue
Skyblue	
Cobalt	
Cyan	
Purple	Purple
Violet	
Magenta	

Known Issues

As of the most recent firmware version, the Protege implementation of OSDP has the following known issue:

- The **Disable green LED processing** option does not function for OSDP or RS-485 readers.

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.