LenelS2
1212 Pittsford-Victor Road
Pittsford, New York 14534 USA
Tel 866.788.5095 Fax 585.248.9185
www.LenelS2.com

FICAM Configuration Guide

HID pivCLASS for OnGuard

The instructions in this document are provided to assist you in configuring a FICAM-compliant solution using either an HID® pivCLASS® Authentication Module (PAM) or Embedded Authentication for HID with the LNL-4420 (LNL-X4420) Intelligent Dual Reader Controller.

Other FICAM-Compliant Systems Integrated in OnGuard

Instructions are also included to assist you in configuring these additonal Embedded Authentication solutions:

- TI EntryPoint with the LNL-4420 (LNL-X4420) Intelligent Dual Reader Controller
- Validation Agent with the LNL-X4420 Intelligent Dual Reader Controller

Note: This document is intended as a help guide only, and is not official documentation from LenelS2. For any questions, follow your standard method of technical support.

pivCLASS PACS SERVICE

- Configure the pivCLASS PACS Service on page 4
- Configure a PAM in the PACS Service on page 13
- Use pivCLASS Registration Workstation to Enroll Credentials on page 16

PAM DEVICE

- Set PAM to Default IP Address on page 17
- Set PAM to New IP Address on page 18
- Verify New IP Address on PAM Web Page on page 19

OnGuard

- Configure OnGuard to Work with a PAM Device on page 20
- LNL-3300-M5 Setup Information on page 26
- Configure HID Embedded Authentication on page 27
- Configure EntryPoint Embedded Authentication on page 35
  - EntryPoint Card Registration on page 40
- Configure Validation Agent Embedded Authentication on page 43

FIPS 201 Hardware Requirements

- For PAM devices with firmware 5.9.xx or later: LNL-2220/LNL-X2220, LNL-3300/LNL-3300 with downstream reader modules

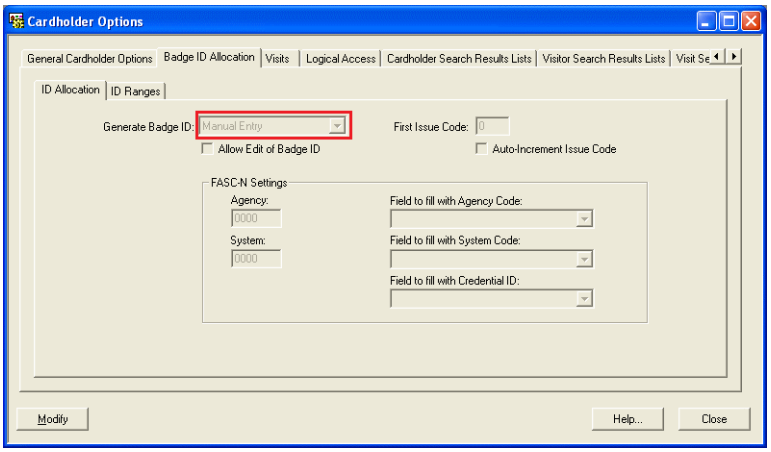
- For Embedded Authentication functionality:

Controller enabled for HID embedded authentication	Firmware	Supported readers
LNL-4420	1.275 or later	Onboard readers LNL-1320 Series 3, LNL-1300 Series 3, and LNL-1300e readers
LNL-X4420	1.275 or later	Onboard readers LNL-1320 Series 3, LNL-1300 Series 3, and LNL-1300e readers LNL-1324e (Requires OnGuard 7.6 or later)

Prerequisites

- The following applications need to be installed:
  - **OnGuard** (See Compatibility Charts to determine which versions of OnGuard are recommended for compliance.)
  - **pivCLASSPACServiceOnGuard.msi** Available at http://www.pivcheck.com/lenel Authentication is required to connect to the pivcheck website. HID Global issues the login credentials to you when your order is submitted. **Note:** Refer to the Approved Product List (APL) published by the Government Services Administration (GSA) to determine which version of the pivCLASS software is approved with each version of OnGuard.
- **HID FIPS_201_SDK** The HID FIPS 201 SDK license is required for OnGuard enrollment. Runs pivCLASS in the background.
- LenelS2 licenses: With DataConduIT being phased out, a new license (SWG-1550-1) has been created. This combines the legacy SWG-1550 and SWG-1140 licenses into one license and becomes the new requirement moving forward.
  - **SWG-1550-1** FIPS 201 Credential Management - Enables support for integrated enrollment and authenticated reader management within OnGuard. FICAM Certified in conjunction with HID pivCLASS and Technology Industries EntryPoint software and supported devices (sold separately). This includes a special DataConduIT license specific to pivCLASS and EntryPoint.
  - **SWG-AUTH-002 Max Number of FIPS-201 Authenticated Readers** - Controls the number of authenticated readers that can be configured in the OnGuard. Two (2) authenticated readers per license.
- For Embedded Authentication: **Add-On Auxiliary Module Firmware** (These modules are posted at the Partner Center on the LenelS2 Hardware Firmware Downloads page: https://partner.lenel.com/downloads/hardware/0/firmware.)
  - **LNLAUXMOD_AAM.bin** (The HID auxiliary module firmware file is required for the Embedded Authentication solution.) Copy this file to the **C:\Program Files (x86)\OnGuard** folder on the computer running Communication Server. To remove the HID auxiliary module firmware from the panel, copy **LNLAUXMOD_REMOEV_AAM.bin** to the **C:\Program Files (x86)\OnGuard** folder.
- Ports 1972, 4242, 8989, 10100, 10200, and 11000 should be opened in the Windows Firewall. Windows Firewall may be disabled but Network Discovery should be enabled (for non-production environments). **Note:** This should be done for any ports used by your system.

- OnGuard® Communication Server and Linkage Server are running.
- LSDataConduIT service is running. LSDataConduIT can be run by the Local System account. (This is the default setting.)
- After the pivCLASS PACS Service is installed:
  - Verify the pivCLASS PACS Service is running, and then configure it. (Open Windows services from **Control Panel** > **Administrative Tools** > **Services**. Locate "pivCLASS PACS Service" in the list. Right-click on the service, and then select **Properties**. On the **Log On** tab, select "This account" and configure it the same as the LSDataConduIT service.)
  - Modify the pivCLASS PACS Service to link to the Single Sign-On account.Single Sign-On must be configured in OnGuard. (From System Administration, open the **Directories** folder from the ***Administration*** menu, and then add a directory. In this example, name the directory "Microsoft Active Directory". Open the **Users** folder and link the OnGuard User to the directory account that has permission to run OnGuard applications and the LSDataConduIT service.)
  - By default, the cardholder option for badge assignment is set to "Automatic". However, for pivCLASS to be able to import the card via DataConduIT, this option must be set to "Manual Entry". This can be done in System Administration at the system level or for each badge type. (From the ***Administration*** menu, select ***Cardholder Options*** > ***Badge ID Allocation*** > ID Allocation or ***Badge Types*** > ***Badge ID Allocation*** > ID Allocation.)



- HID license with the following:
  - pivCLASS license key
  - FIPS SDK license key
  - PAM in Panel license key
  - (Optional) IDPublisher license key
- **EA-LICENSE2**: Two (2) reader Embedded Authentication licenses. HID pivCLASS licenses sold in blocks of 2.
- Base HID pivCLASS Software:
  - **PVC-CM: pivCLASS Certificate Manager** - Manages the certificates harvested for the cardholder database. It checks and validates enrolled credentials across the Federal bridge. One (1) per database. A second license is required for redundant PACS.

- **PVC-FXRDR: pivCLASS Fixed Reader Service** - Allows the pivCLASS certificate data to be pushed down to the access panels. One (1) per system.

- Enrollment Client: Use the **HID pivCLASS SDK** directly in OnGuard that runs pivCLASS in the background or the pivCLASS Registration Workstation:
  - **PVC-API-RTL** - Provides for integrated FIPS 201 enrollment into OnGuard using the HID pivCLASS enrollment module. Used with the FIPS 201 Credential Management Integration. One per enrollment workstation. The OnGuard/HID pivCLASS SDK allows enrollment to be done in OnGuard as you would a normal cardholder. Uses pivCLASS registration validation engine via the SDK - for integrated FIPS 201 enrollment into OnGuard using the HID pivCLASS enrollment module. Used with the FIPS 201 Credential Management integration. Typically, one license per workstation.
  - **PVCP-D/S-1400** - The pivCLASS Validation/Registration Workstation works through pivCLASS. Does not include PACS interoperability. One (1) license per workstation.

Compatibility Charts

Compatibility charts of currently supported OnGuard versions and components are available on the LenelS2 website: https://partner.lenel.com.

To access the OnGuard Compatibility Charts:

1. Sign in to the Partner Center, and then select **Downloads.**
2. **Choose product or service**: OnGuard.
3. **Choose version:** Select the version of OnGuard.
4. **Choose type of download:** Compatibility Charts.
5. Open the **Third Party Application Compatibility Chart** for HID pivCLASS Embedded FIPS-201 Authentication support.

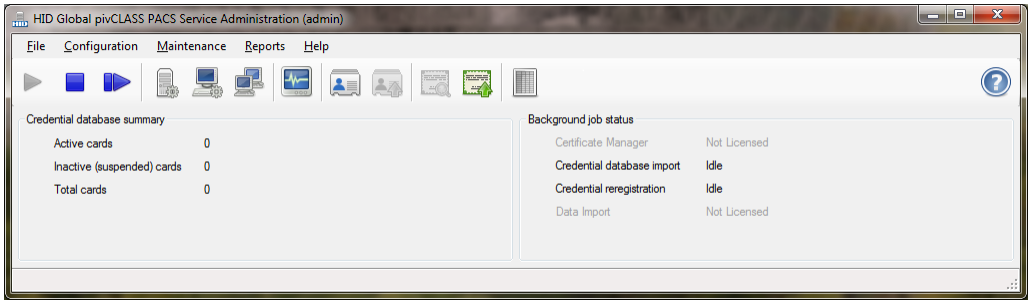
pivCLASS PACS SERVICE

Configure the pivCLASS PACS Service

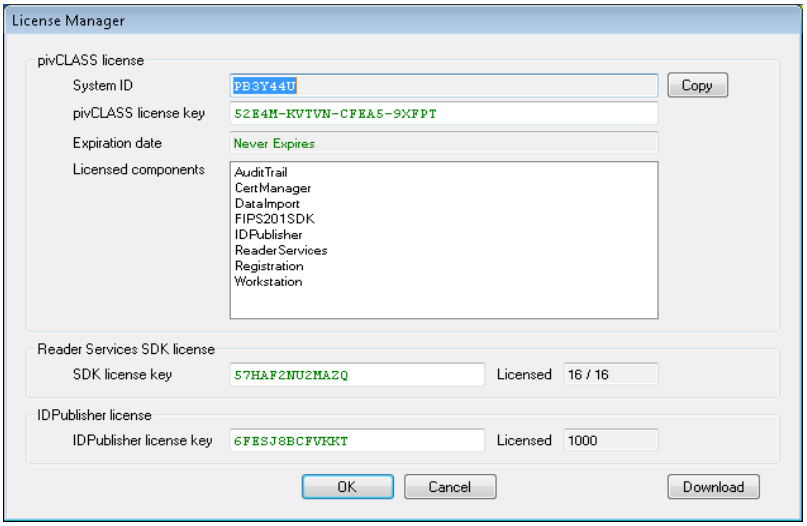
Prerequisite: In order to install and activate a permanent software license, the System ID from the pivCLASS PACS Service application needs to be registered with HID Global. Once this has been done, the license key can be downloaded or manually entered for access to purchased options.

1. Run **pivClassPACSServiceOnGuard.msi** and install the application.
2. Start the pivCLASS PACS Service application.
3. Log in. The default login credentials are **User ID**: `admin` and **Password:** `password`. Click [Login].

Figure 1. pivCLASS PACS Service Administration



4. From the **File** menu, select **License Information** to open the License Manager. Copy the **System ID** and provide it to HID Global technical support so it can be registered and associated with the license. When you have the keys, copy and paste them into their corresponding fields or download them if online.

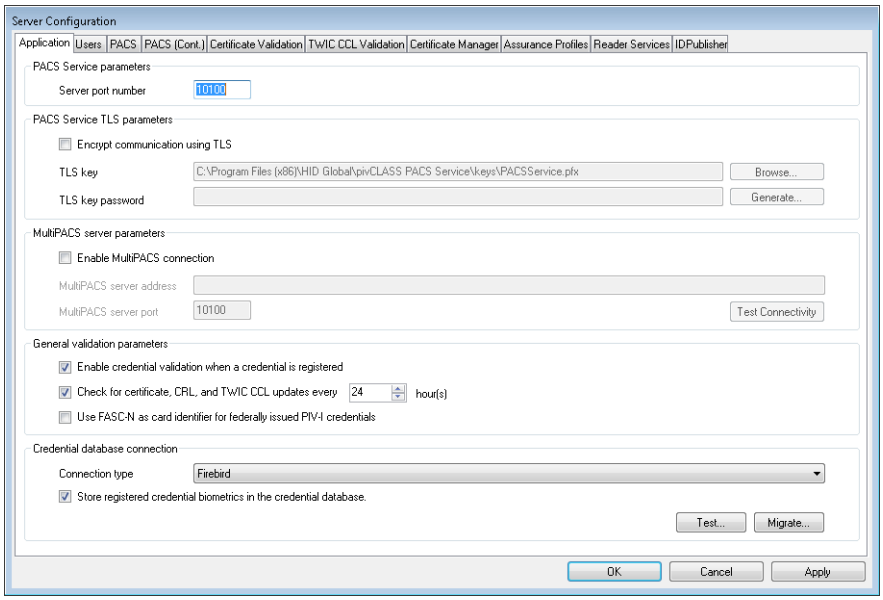


Your purchased licenses should now display in Licensed components along with the number of Licensed readers. When the license installation is complete, click [OK].

Note: With new multiple client systems, copy the **System ID** from each client.

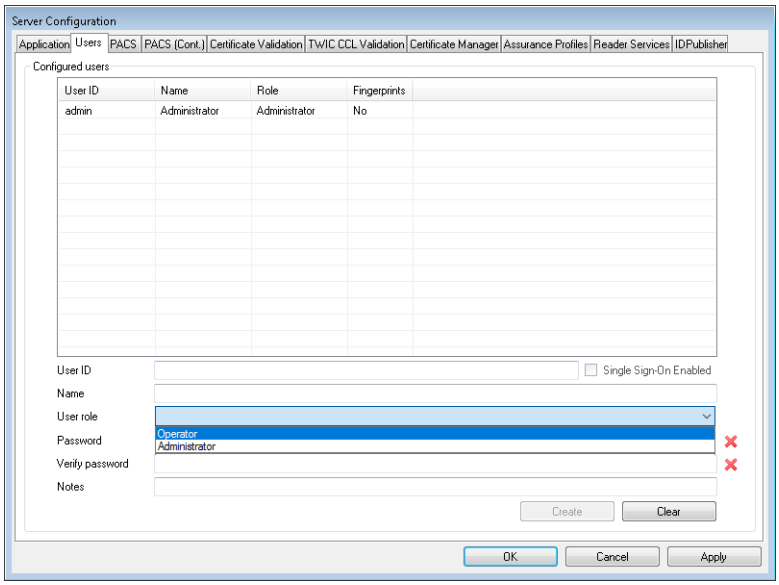
5. Click [Yes] to confirm restarting the pivCLASS PACS Service.
6. Add the OnGuard license and ensure the licenses are properly applied:
   a. Connect to the OnGuard server via a browser.
   b. Sign into License Administration with your **Username** and **Password**.
   c. Choose **View** for an existing system, or **Install** for a new system, and then browse to the license and apply it.
   d. Click [Next], and then [Finish].

e. Examine the license. The relevant licenses are listed in the Access Control section. From the **Configuration** menu, select **Edit Service Settings** to open the Server Configuration window.



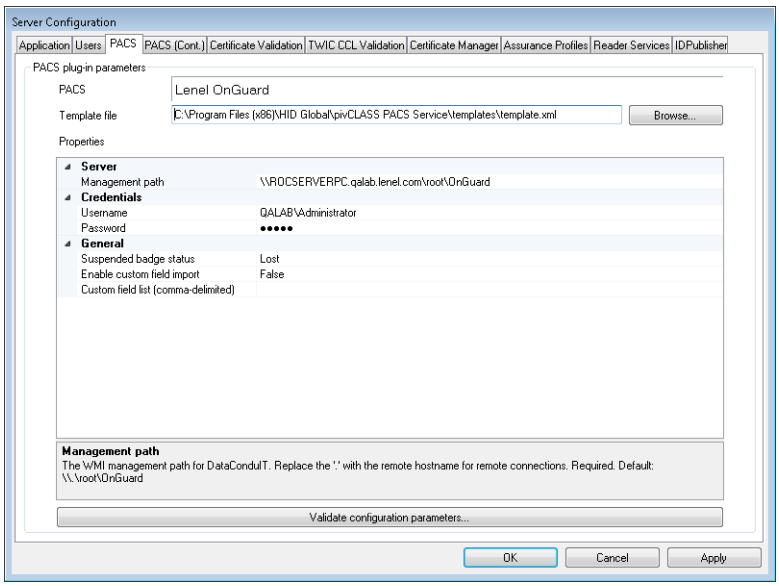
7. On the **Application** tab:
   a. Make sure the **Server port number** is `10100`. Should be the same in OnGuard.
   b. Select **Encrypt communication using TLS**.
   c. Enter the **TLS key** (path) and **TLS key password**.
   d. Select all General validation parameters, and **Check for certificate, CRL, and TWIC CCL updates every** `18` **hours**.
   e. This requires a prerequisite to install a pivCLASS database instance
   f. **Prerequisite:** Prior to performing this step, an instance of a pivCLASS database needs to be installed.
   Change **Connection type** from “Firebird” to “Microsoft SQL Server”. Then the other options are shown. Select them and Single Sign-on. If any work was done in the Firebird database, you need to [Migrate] it. Then [Test] it.
   g. De-select **Store registered credential biometrics in the credential database** the first time. Then, after installation, select it.
   h. The following settings are optional depending on your system:
      - **Enable Credential Validation When a Credential is Registered:** Select this option to validate credential registrations during registration.
      - **Store Registered Credential Biometrics in the Credential Database:** Select to store the fingerprint data in the credential database's Fingerprints table during credential registration if the credential is registered using a contact interface, and the credential is unlocked via successful PIN entry. **Note:** If biometric storage is disabled on a system that stored biometrics previously, the existing biometric templates are automatically deleted.
   a. Click [Test] to verify the connection to the database is okay.

8. On the Users tab: Create a new user. Retain the default values. ("admin" will be added to the list automatically.) Two (2) default User roles are available: Administrator and Operator. Familiarize yourself with their roles.



9. On the **PACS** tab where the connection to OnGuard is defined:

   a. Browse to the folder where the pivCLASS PACS Service is installed by default:
   C:\Program Files (x86)\HID Global\pivCLASS PACS Service\templates
   From here, select the **template.xml** file.



Note: The default **template.xml** file is the generic connection to OnGuard. Typically, this one is used but it can be modified.

   b. Under **Server**:
   Set the **Management path** as \\.\root\OnGuard. (Enter a dot "." if OnGuard and PACS

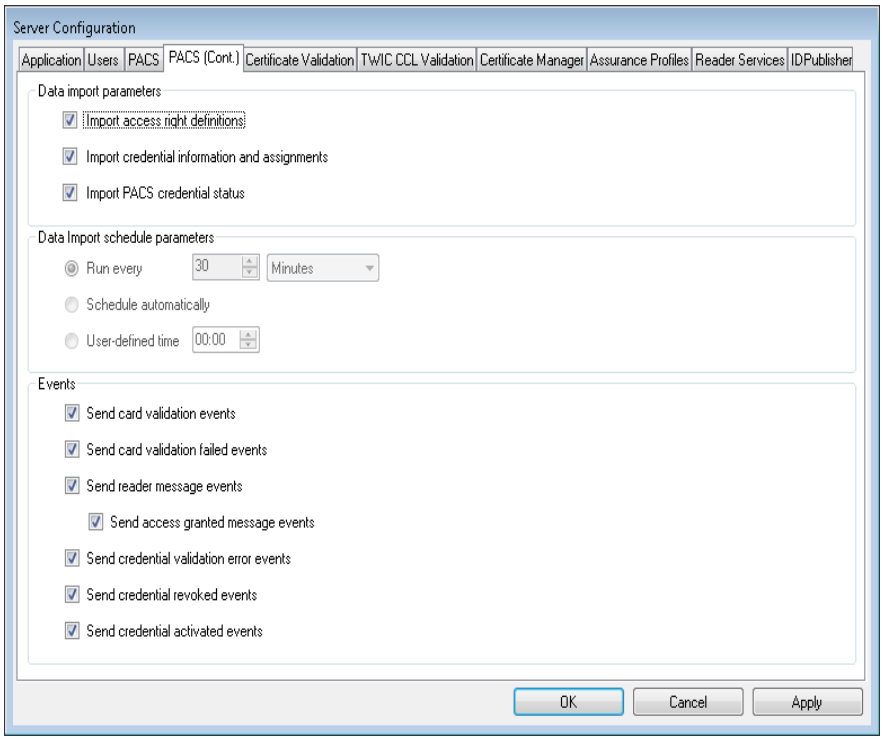
service are installed on a same computer. Otherwise - instead of a dot, enter the full name of the OnGuard server. Otherwise, change to the remote hostname of the DataConduIT service. If remote, you need to sign in with your **Username** and **Password**. To [Validate configuration parameters], DataConduIT needs to be running.)

c. Under **Credentials**:
If the PACS Service and OnGuard are installed on the same computer, leave **Username** and **Password** blank.
If OnGuard is installed on a computer different than the PACS Service, enter the **Username** and **Password** of the account used to log into that computer.

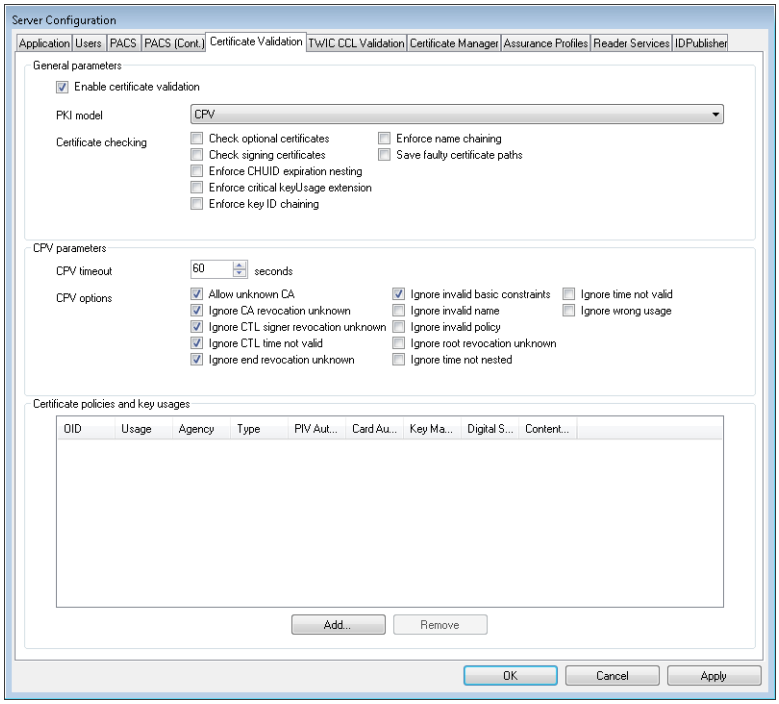
d. Under **General**:
Select "Lost" from the **Suspended Badge Status** drop-down.
Select "False" from the **Enable custom field import** drop-down, and then click [OK] to save the settings.

e. Click [Validate Configuration Properties]. You should receive confirmation that "the plug-in settings have been validated".

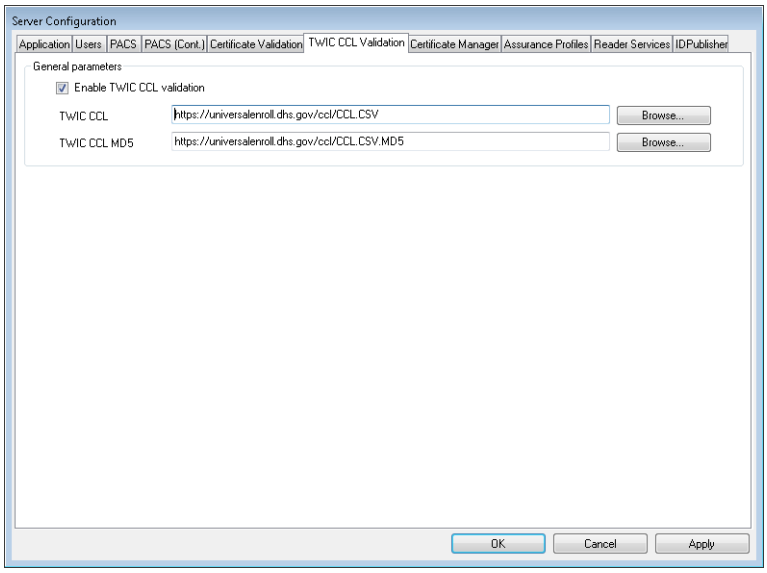
10. On the **PACS (Cont.)** tab: Select all of the **Data import parameters**. Under **Events**: Select all of the options to ensure all events are getting into OnGuard from pivCLASS.



11. Configure **Certificate Validation**. (These settings vary depending on your requirements.)



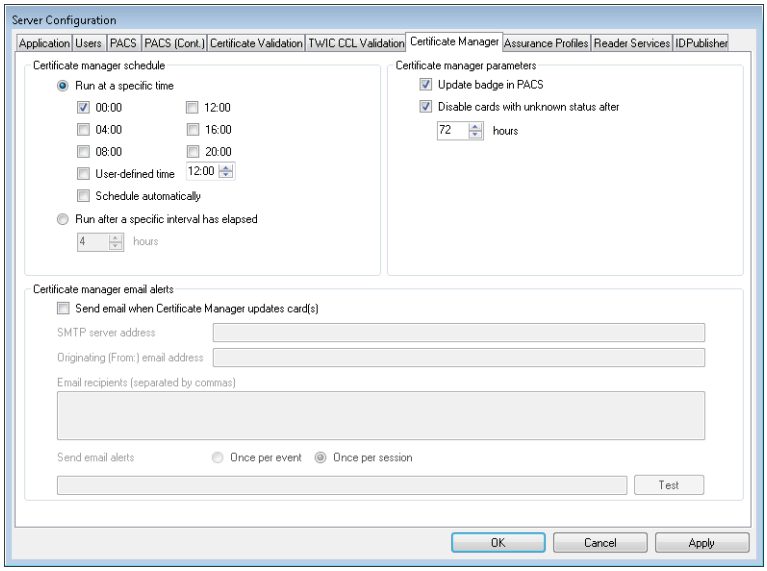
12. On the **TWIC CCL Validation** tab: Select the **Enable TWIC CCL validation** check box. (Optional) Used for TWIC-specific installations.



a. Browse to the server address for checking TWIC cards against the Certificate Revocation List (CRL): http://twic-crl.orc.com/CRLs.

b. (Optional) Browse to the server address and MD5 hash address for checking TWIC cards against the TWIC Canceled Card List (CCL) to verify if the cardholder's FASC-N has been canceled.

c. On the **Certificate Manager** tab: Goes to the Federal bridge for validating certificates.

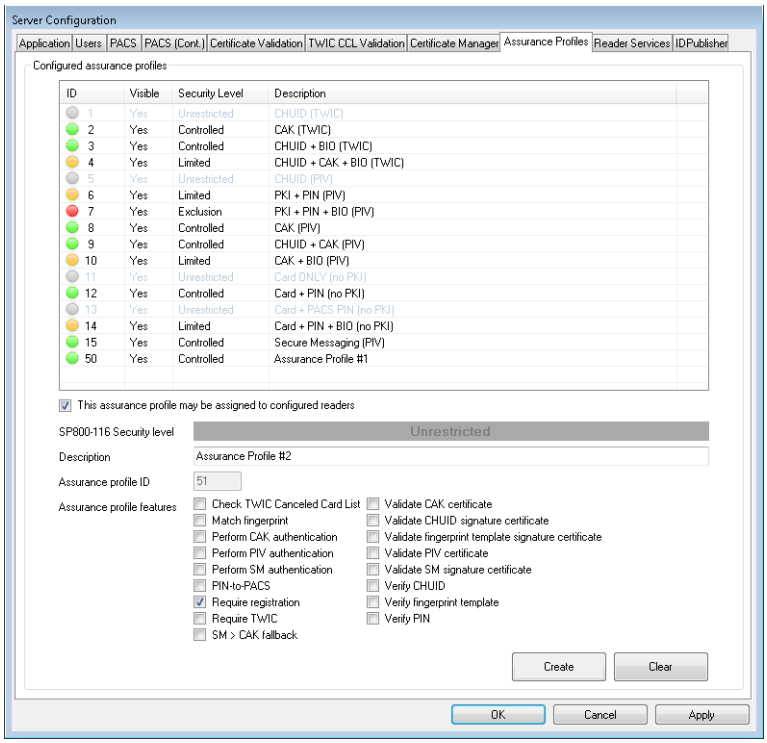


d. Select **Run at a specific time** to enable running the Certificate Manager at specific times to re-evaluate all credentials.

e. Select or enter the run schedule for specific times, or schedule re-validation at fixed intervals.

f. Select **Update badge in PACS** and **Disable card with unknown status after** 72 **hours**. 72 is the default number of hours. After the specified number of hours, cards will be disabled for those who are deactivated. To send email alerts when someone gets deactivated, enter the SMTP email address.

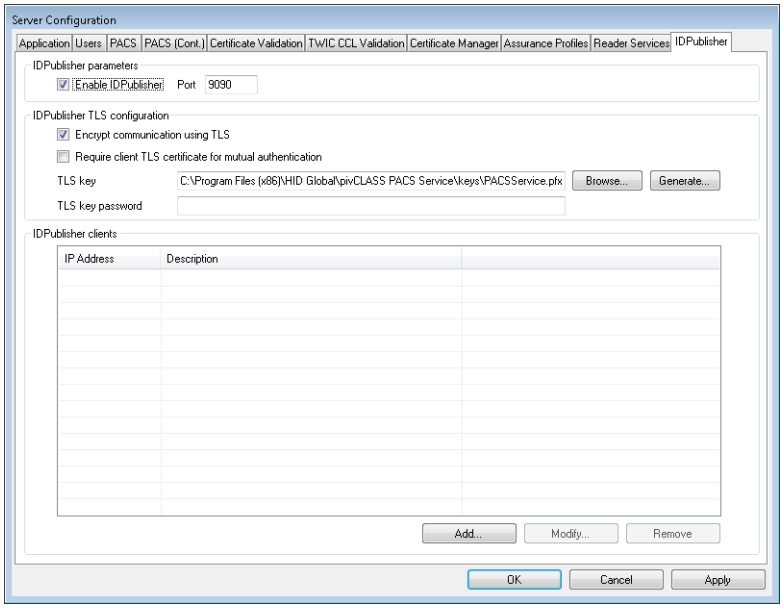
13. The **Assurance Profiles** form is set by default to SP800-116 security levels. Can add additional levels or customize as needed.



a. Select the **This assurance profile may be assigned to configured readers** check box to include the assurance profile in the drop-down list of assignable assurance profiles of applicable readers.

b. Select the **Require Registration** check box to indicate the credentials must be registered with pivCLASS for access to be granted at the door. If unchecked, the PAM will attempt a basic Certificate Path Validation (CPV) operation to validate the card's certificates. For this to succeed, the administrator must load the required trusted root CA and intermediate issuer CA certificates into the **C:\Program Files (x86)\HID Global\pivCLASS PACS Service\pam\certs** folder.

14. On the IDPublisher tab:



Note: The IDPublisher tab is displayed if the IDPublisher option is licensed,

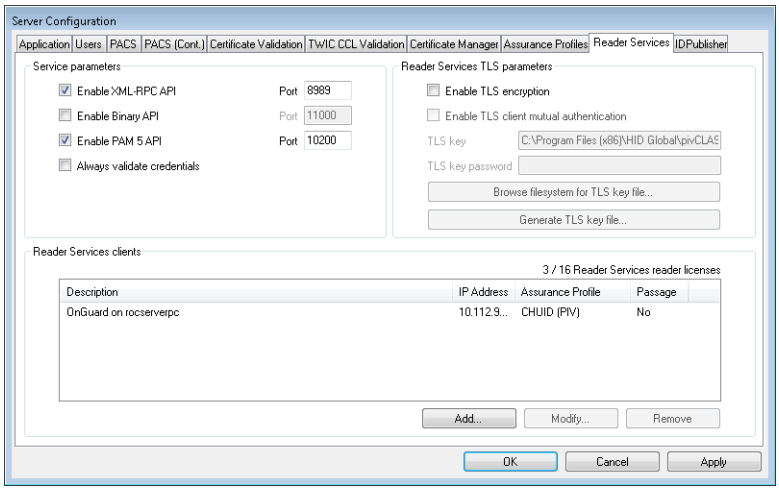
a. Select the **Enable IDPublisher** check box.

b. **Port:** `9090`

c. Select the **Encrypt communication using TLS** check box.

d. **TLS key:** Click [Browse] to select the private key used for securing the TLS connection, or click [Generate] to generate a key.

15. On the **Reader Services** tab:



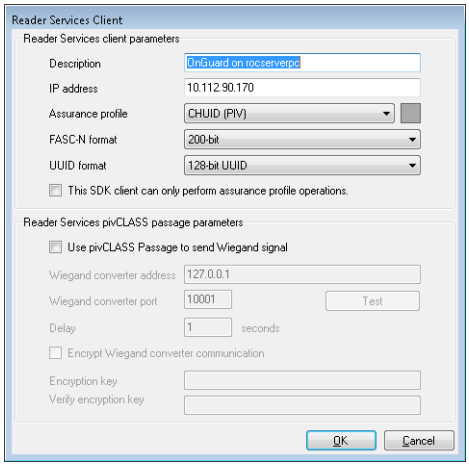
a. Select the **Enable XML-RPC API** check box. **Port** is set to `8989`.

Note: In OnGuard System Administration **FIPS 201 Credentials** folder, make sure the **XML-RPC Port** is set to the same for the caching status proxy service.

b. Select the Enable **PAM 5 API** check box with **Port** set to `10200`.

c. De-select **Enable TLS encryption** to avoid issues the first time you connect. After that, select it.

d. Define one (1) reader service client. Click [Add] to add a Reader Services client. (This is the computer on which pivCLASS is installed.)



e. In **Description**, enter a meaningful name for the client.

f. Enter the **IP Address**. This is the IP address of the OnGuard computer. Typically, the IPv4 address. This is used to push the information down from the Certificate Manager to the panels.

g. Click [OK] to save the client settings and close the dialog. Click [Apply], and then [OK].

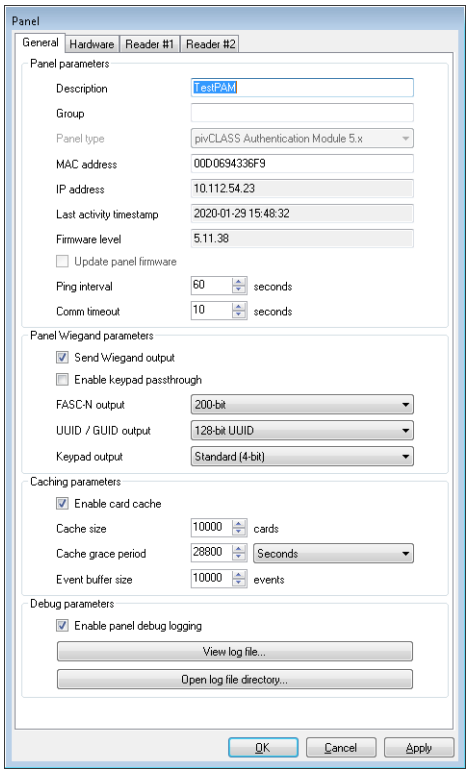
h. Click [Yes] to confirm restarting the pivCLASS PACS Service.

Note: If the Communication Server is running on a computer other than the OnGuard server computer, you may need to add another Reader Services client with the IP address of the computer where the Communication Server is running.

Configure a PAM in the PACS Service

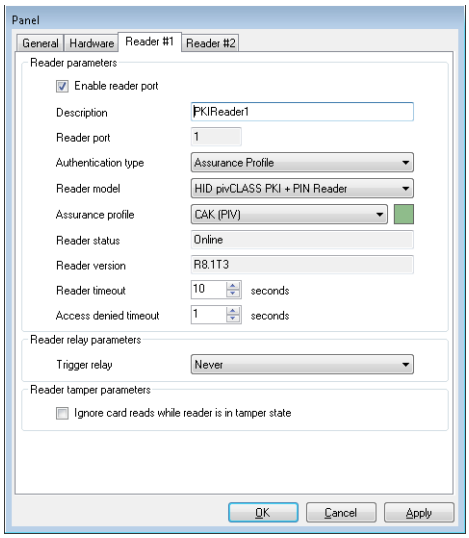
Note: If the PAM device does not have a valid IP address yet, this can be done later. (For instructions, refer to PAM DEVICE on page 17.)

1. At the PACS Service main window, right-click in the **Reader Services** window to bring up the context menu. From the **New** menu, select **pivCLASS Authentication Module 5.x**. The Panel dialog is opened.



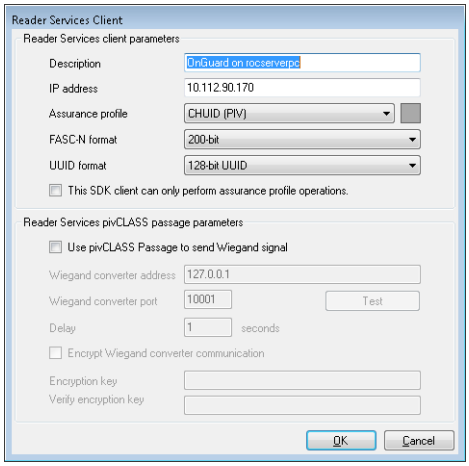
   a. On the **General** tab: Enter a name for the PAM in **Description**. (This name will be also used in OnGuard). In this example, “TESTPAM” was used.
   b. Enter the **MAC address** of the PAM device. (Later, this PAM device will be configured on its web page to communicate with the pivCLASS PACS service.)
   c. Select the **Send Wiegand output, Enable card cache**, and **Enable panel debug logging** check boxes.
   d. Select “200-bit” for **FASC-N output** and “128-bit UUID” for **UUID / GUID output**.

2. On the **Reader #1** tab: Enter a name for your reader in **Description**. In this example, “PKIReader1”.



   a. Choose “1” as the **Reader port**.
   b. Choose “HID pivClass PKI + PIN Reader” or another entry as the **Reader model**.
   c. Choose an **Assurance profile.** In this example, “CAK (PIV)”.
   d. Use the same steps to add Reader #2.

3. On the **Server Configuration** > **Reader Services** tab: Add a new client. (This is the computer on which OnGuard is installed.)



   a. In **Description**, enter a meaningful name for the client, for example, the name of the computer where OnGuard is installed.
   b. Enter the **IP Address** of the OnGuard computer.

Note: You may need to configure this as an IPv6 address instead of an IPv4 address. You may discover what needs to be configured later when adding and saving an authenticated reader in OnGuard. An error would then display reporting the Client “with IPv6 ipaddress”

is not responding. In this case, copy this “IPv6 ipaddress” and paste it into the **IP Address** field for the Reader Services client in the pivCLASS PACS Service.

c. Select the **Assurance profile** you want to use.

d. Select “200-bit” for the **FASC-N format** and “128-bit UUID” for the **UUID format**.

e. Click [OK] to save Reader Service client.

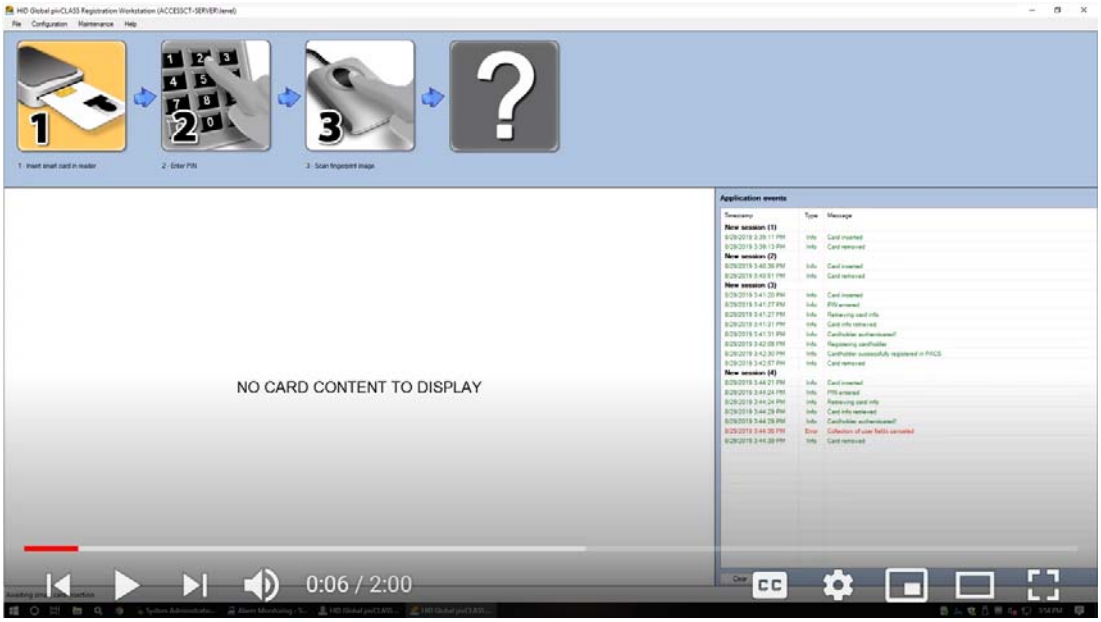
f. If the Communication Server is running on a computer different than the OnGuard server, add this computer as another Reader Services client.

4. On the **Server Configuration** > **Applications** tab and **Users** tab: Retain the default settings.
5. On the **Server Configuration** > On the **TWIC CCL Validation** tab: Select the **Enable TWIC CCL validation** check box.
6. On the **Server Configuration** > **Certificate Validation** tab: Select the **Enable certificate validation** and specify the **PKI model** as “CPV”.
7. On the **Server Configuration** > **Certificate Manager** tab: Select **Update badge in PACS** and **Disable card with unknown status**.
8. From the **Configuration** menu, select **Manage Clients**: Click [Add], and then enter the **System ID** of the computer where OnGuard is installed.
9. From the **Maintenance** menu, select **Enable Debug Logging**.
10. Open the Windows services from **Control Panel** > **Administrative Tools** > **Services**. Locate the pivCLASS PACS service in the list. Right-click on the service, and then select **Properties**. On the **Log On** tab, select “This account” and configure it for the account with permissions to run OnGuard and LSDataConduIT.

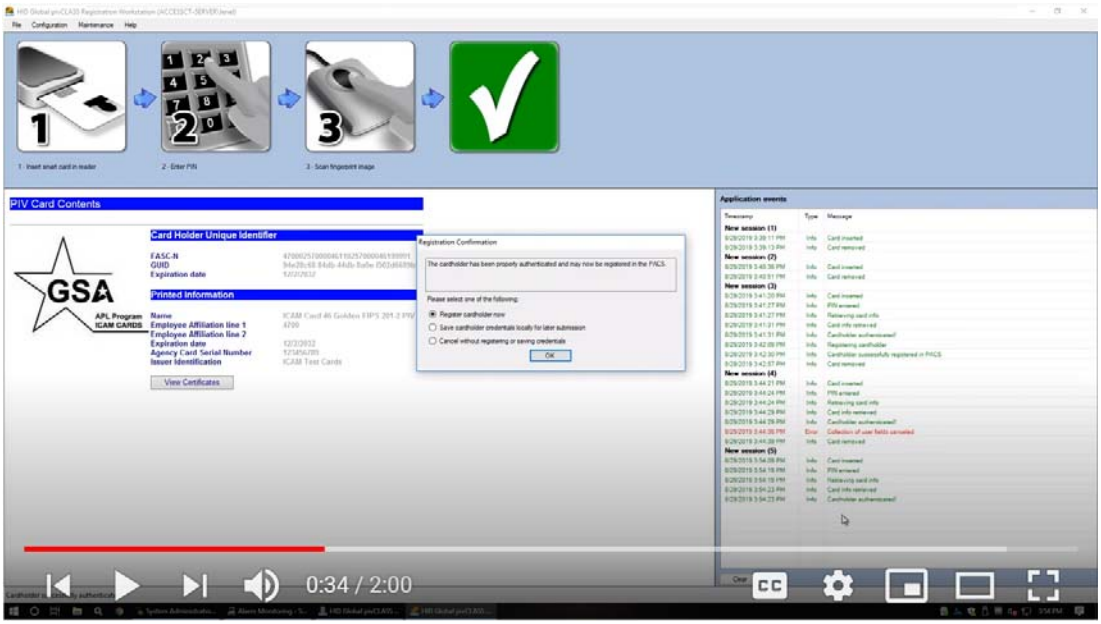
    Important: This step is mandatory in order to work with the LSDataConduIT service on the OnGuard server.

Use pivCLASS Registration Workstation to Enroll Credentials

1. Ensure the PC/SC-compatible smart card reader is connected to the workstation, and the pivCLASS enrollment application is running.
2. Insert the card in the reader.



3. Enter the card PIN on the screen or using a connected keyboard. Once the card is read, The information from the card is shown and the Registration Confirmation dialog is opened.



4. Select **Register cardholder now**. Optionally, select S**ave cardholder credentials locally for later admission** for a later registration. If you are only validating the credentials, select **Cancel without registering or saving credentials**. Click [OK].
5. If you have the data import connected to this application, the associated access levels will be available in the User Fields dialog. Up to three (3) access levels can be assigned here rather than doing this in OnGuard. Click [OK] to register the card.

6. After the card is registered, remove the card, and then use it in the system to validate the card.
   a. From System Administration, navigate to Cardholders.
   b. Search for the credential. The card and phone information populates the cardholder, the badging information comes through, and the access levels are assigned.

PAM DEVICE

Set PAM to Default IP Address

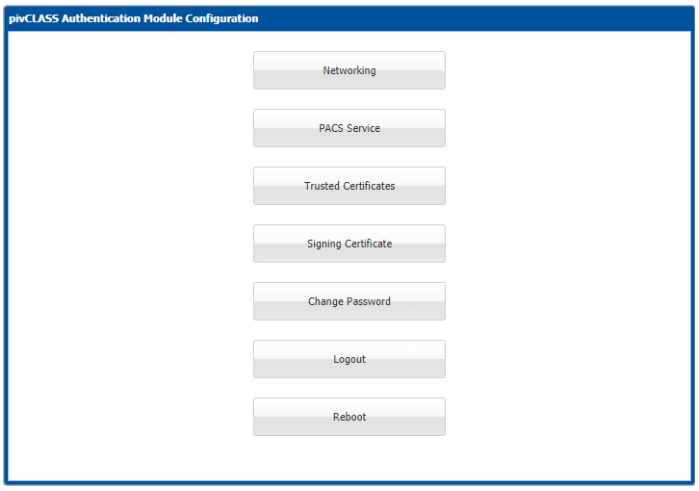
Reset the PAM to the factory defaults. This needs to be done to set the PAM to the default IP address: 192.168.0.222.

1. Remove power from the PAM. (Disconnect the power cord/black input attached to power).
2. Set DIP switches 1 & 8 to **ON** with the other switches to OFF.

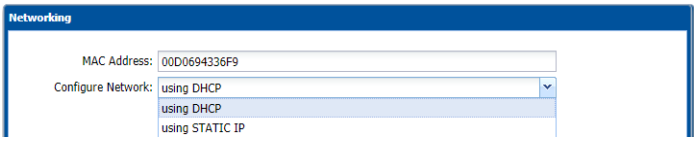
3. Apply power to the PAM.
4. Wait until the FAULT, READER 1, READER 2 and RS-485 LEDs flash Red/Green/Red/Green continuously. This indicates the PAM device is successfully reset to the factory defaults.
5. Connect the network cable from the PAM to the test computer.
6. Change the test computer subnet to 192.168.0.0 to configure the PAM:
   a. From the Start Menu, select **Control Panel**, and then **Network and Sharing Center**.
   b. Click on **Local Area Network**. Select **IPV4** > **Properties.**
   c. Select **Use the following IP Address** and enter the following:
      IP address: 192.168.0.10
      Subnet mask: 255.255.255.0
      Default gateway: 192.168.0.1
   d. Click [OK]. Now the test computer will be in 192.168.0.0 subnet.
7. Remove power from the PAM.
8. Set DIP switch 8 to OFF (**Leave DIP switch 1 ON**).
9. Apply power to the PAM.

Set PAM to New IP Address

1. Enter the default IP address 192.168.0.222 in a web browser to access the HID PAM Configuration Tool.
2. Log onto the page: `admin` \ `password`



3. Click [Networking] to assign a new IP address for the PAM device.



   a. **MAC address** is displayed and not editable.

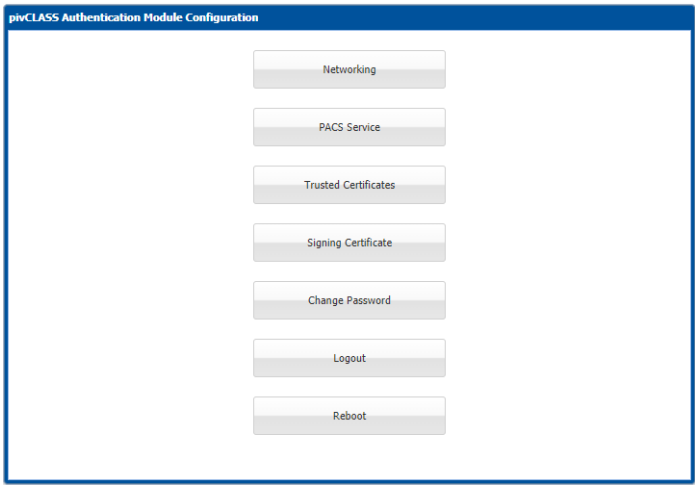
b. **Configure Network** - Choose **using DHCP** or **STATIC IP**.
   Select **using DHCP** to configure the PAM to obtain a network address dynamically.
   Select **using STATIC IP** to manually configure - Enter a new **IP address** for the PAM device. Also enter the correct **Subnet Mask** and **Default Gateway** addresses.

c. Click [Save].

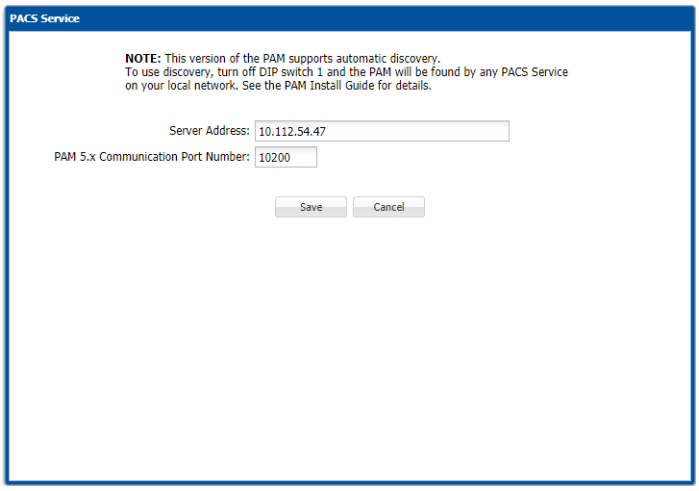
4. Click [Reboot]. The PAM will reboot. After that, connect the network cable from the network of the newly assigned IP address.

Verify New IP Address on PAM Web Page

5. In the Command Prompt, ping the newly assigned PAM IP Address to verify the PAM is in the network.
6. Enter the new PAM IP address in a web browser to access the HID PAM Configuration Tool.
7. Log onto the page: `admin` \ `password`.



8. Click [PACS Service].

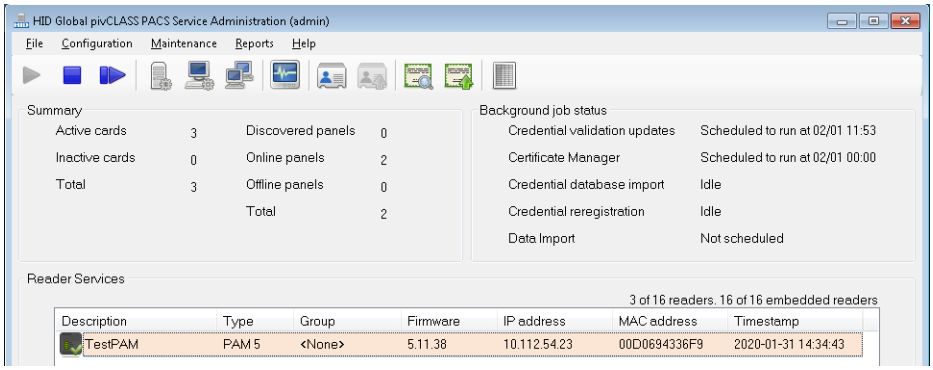


a. Enter the **IP address** of the computer where the PACS Service is installed.

b. **Port number:** `10200`

c. Click [Save]. A message should display confirming the connection to the PACS Service was successful.

9. Verify the new IP address is now displayed properly for the PAM device in pivCLASS PACS Service > **Reader Services**.



OnGuard

Configure OnGuard to Work with a PAM Device

This section includes examples of how to configure a PAM in the OnGuard software. (For more information on configuring FIPS 201 functionality, refer to “NIST SP 800-116 Support” in the System Administration User Guide.)

Note: The IP addresses of devices described in this section are provided as examples. You will need to replace these addresses with actual, working IP addresses.

From System Administration, complete the following steps:

1. Set up Single Sign-On:
   a. From the **Administration** menu, select **Directories**. Add a directory, for example “Microsoft Active Directory.”.
   b. From the **Administration** menu, select **Users**. Link the OnGuard User to the account in this directory. This account should have permissions to run OnGuard applications and the LSDataConduIT service.

Note: The pivCLASS PACS service should also be running under this user account, not the local account.

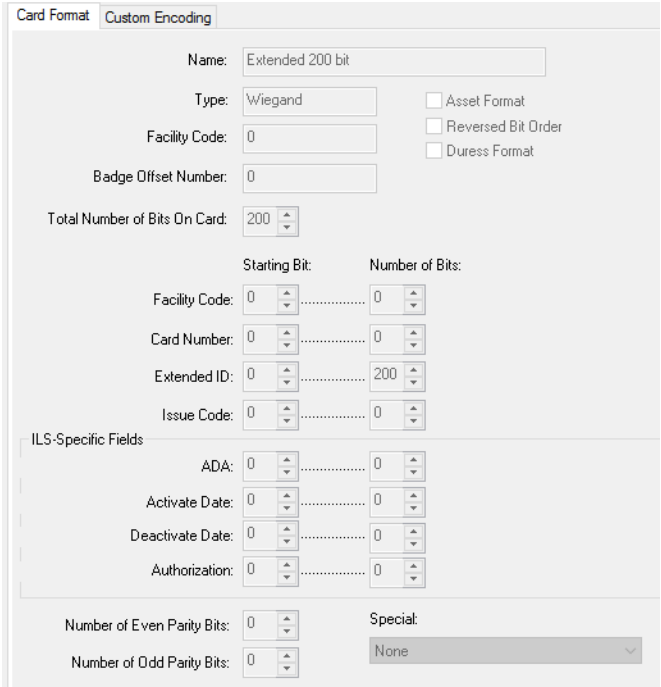
2. Make sure the Windows service **Smart Card** is running. This service is required for OnGuard to communicate properly with the pivCLASS PACS service.
3. From the **Administration** menu, select **FIPS 201 Credentials**.
4. On the **General** tab:
   a. **Cardholder photograph import method:** Choose either “Always import” or Prompt to import”.
   b. **System ID** is populated. It is unique to the machine, and is not the ID of the server location. License keys are unique by machine.

c. If the FIPS 201 SDK license is preregistered, click [Download License] to push the preloaded license down to OnGuard. This populates the **License key** field. To download, you need to be online. If you have the license, enter the key by copying and pasting it. Click [OK] to save.

5. On the **Credential Validation** tab: Define how authentication is done with SDK. Keep the default settings, but set the Credential Validation settings to **Validate on Caching Status Proxy**. This pulls in the configuration from the pivCLASS PACS Service. Click [OK] to save.
6. On the **Catching Status Proxy** tab: Define the link with the PACS Server.
   a. Select the **Caching status proxy service**. This should match the name of the pivCLASS PACS Service. From Control Panel, select **Administrative Tools** > **Component Services** > **Services**, and then locate the pivCLASS service. (The service name is context sensitive.)
   b. In the **Server hostname** field, enter the IP address (or the full name) of the computer where PACS Service is installed.
   c. The server **Port** number is `10100` from the pivCLASS PACS Service > Application tab.
   d. Select all three (3) check boxes in the Enrollment settings section.
   e. Select "Returned" status for the badge status.
   f. Enter `8989` in the **XML-RPC Port** field (or whatever port number is set for the XML-RPC API port in the PACS service).
   g. Leave the **Enable communication using SSL** unchecked during initial configuration to avoid issues with encryption until the system is set up.
   h. Click [Test Connection]. A message should display confirming you are "Successfully connected to Caching Status Proxy server".
   i. Click [OK] to save the settings.
7. On the **Authentication Modes** tab:
   a. Click [Modify].
   b. Click [Download] to download all of the authentication modes from the PACS Service. You will see the list populated with the modes such as CHUID, CAK, CHUID + BIO, etc. No errors should occur.
8. From the **Administration** menu, select **System Options**.
   a. On the **General System Options** tab, click [Modify].
   b. Under the OpenAccess host section, select the **Generate software events** check box, and then click [OK].
9. Configure Linkage server host:
   a. Browse to the computer where OnGuard is running.
   b. Add an access panel, for instance one that supports on-board readers, with the correct IP Address: 10.112.10.215.
10. From the **Additional Hardware** menu, select **Logical Sources**.
    a. Add a logical source: In **Name**, enter "pivCLASS PACS Service" (exactly as it is spelled), select a **World time zone,** and then click [OK]. The logical source name is the same as the Caching status proxy service. See step 6.a.
    b. On the **Logical Devices** tab, click [Add], enter "Certificate Manager" in **Name**, select "pivCLASS PACS Service" from **Logical Source** drop-down, and then click [OK].
    c. Add the other devices: The PAM ("TestPAM") and the reader(s). The reader name is "TestPAM.PKIReader1" which uses the names configured in the PACS Service for the PAM ("TestPAM") and the reader ("PKIReader1").

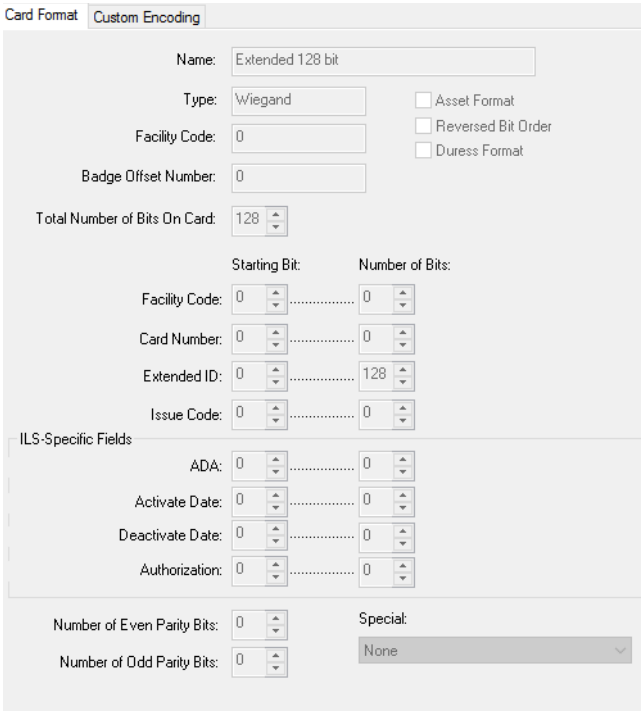
11. Create card formats for reading PIV cards:
    a. From the **Administration** menu, select **Card Formats**.
    b. Add a Wiegand card format with **Total Number of Bits On Card** = 200 and **Extended ID** = 0 - 200. Name this card format. For example, “Extended 200 bit”.

Figure 1. Extended ID 200 bit card format



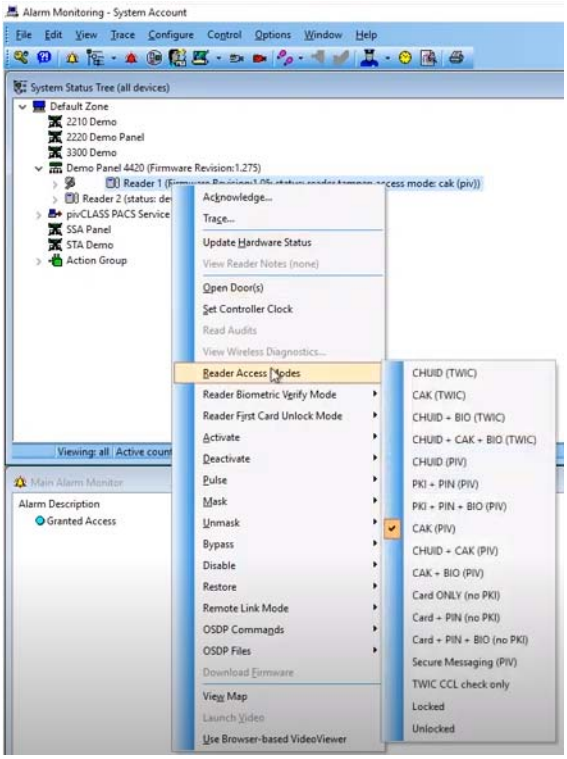
    c. Add a Wiegand card format with **Total Number of Bits On Card** = 128 and **Extended ID** = 0 - 128. Name this card format. For example “Extended 128 bit”. This card format supports PIV-I cards.

Figure 2. Extended ID 128 bit card format

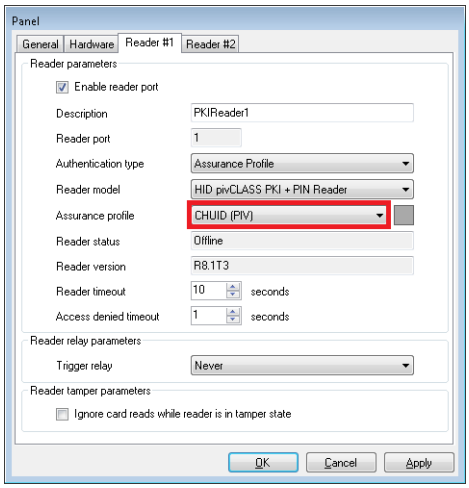


12. Make sure the LSDataConduIT Service is running. If not, start it.
13. Add the PAM device as a reader:
    a. From the **Access Control** menu, select **Readers and Doors**. On the **General** tab:
    b. Add a reader with the name “TestPAM.PKIReader1” (where “TestPAM” is a name of the PAM device configured in the PACS service application and “PKIReader1” is a name of the reader).
    c. Assign these card formats to the reader: Extended 200-bit and Extended 128-bit.
    d. Select the **Authenticated reader** check box, and then assign the reader online and offline modes. For example, “CAK (PIV)” and “Locked”, respectively. The reader **online** modes are the assurance profiles from pivCLASS Reader Services. The reader **offline** modes include Locked, Unlocked, and Card Only.

14. In Alarm Monitoring, verify that all hardware is online. Change the **Reader Access Mode** from “CAK (PIV)” to something else, for example, “CHUID (PIV)”. The mode should change successfully.



15. To verify that the communication between the OnGuard server and PACS Service is correct, go to the PACS Service and make sure the **Assurance profile** of Reader #1 was changed accordingly.



16. Connect and configure a smart card reader to harvest the smart card credentials into pivCLASS and OnGuard. (The HID OMNIKEY 3121 USB is used in this example.)
    a. Connect the OMNIKEY 3121 smart card reader via USB to the test computer.

b. Make sure the OMNIKEY 3121 has the latest driver. If it does not, download it from the HID Global website.

c. Add the OMNIKEY 3121 to the computer and verify it is properly displayed in **Windows** > **Devices and Printers**.

d. In System Administration, select ***Workstations*** from the ***Administration*** menu.

e. Add the workstation for the server. If there are additional workstations, add them as well.

f. On the Encoders/Scanners (General) tab: Add the OMNIKEY 3121 as a "PC/SC Encoder" **Device type** and associate the workstation previously added with the reader.

g. On the Location tab, select **This is a standalone device attached to this workstation**.

h. On the Communications tab, choose the **PC/SC device**. This is the reader driver ("HID Global OMNIKEY 3x21 Smart Card Reader 0") that should be available in the drop-down.

17. In Forms Designer, open the **Cardholder** form:

    a. Click on **Last name** and select "Last name" from the **PIV** and **PIV-I** field options. Click [OK].

    b. Click on **First name** and select "First name" from the **PIV** and **PIV-I** field options. Click [OK].

    This is done to import first and last names from the card into System Administration.

    Important: The corresponding fields must match.

18. Open the **Badge** form.

    a. Insert a new system object, **Extended ID**. A text box for Extended ID will now appear on the Badge form.

    b. Click on **Extended ID** and select **PIV-I** to map with "Full GUID (Hexadecimal)" and **FASC-N** to map "Full 200-bit FASC-N (Hexadecimal)".

    c. Click on **Badge ID** and select **FASC-N** to map with "AC + SC + CN + CS".

    d. Click on **Deactivation date** and select "Card Expiration Date" for **PIV** and **PIV-I**.

    e. Save all of these settings. Forms Designer then connects to Application Server and saves all the settings.

19. From the **Administration** menu, select **System Options**.

    a. On the **Hardware Settings** tab: Click [Modify]. Set the **Maximum badge number length** to 18 and **Maximum extended ID length** to 32 bytes. Click [OK] to save the settings.

Note: **Maximum badge number length** can also be set to 14, 15, or 16 depending on the card format. **Maximum extended ID length** should be set to 25 for PIV and CAK cards, and 32 for full values, such as 200-bit cards that need to pass through the bytes.

20. Insert the card into the OMNIKEY 3121 Card Scanner to test.

    Important: Before importing the cardholder and card information from a PIV or TWIC card, the following must be done: certificates registration, verification, and enrollment of the card into the PACS Service database - proper certificates and Certificates Revocation Lists (CRLs) should be installed on the computer where the PACS service is running.
    Verify that the certificates and updated CRLs exist on the computer.
    Use **mmc.exe**.

21. From the **Administration** menu, select **Cardholders**.

    a. Click [Add].

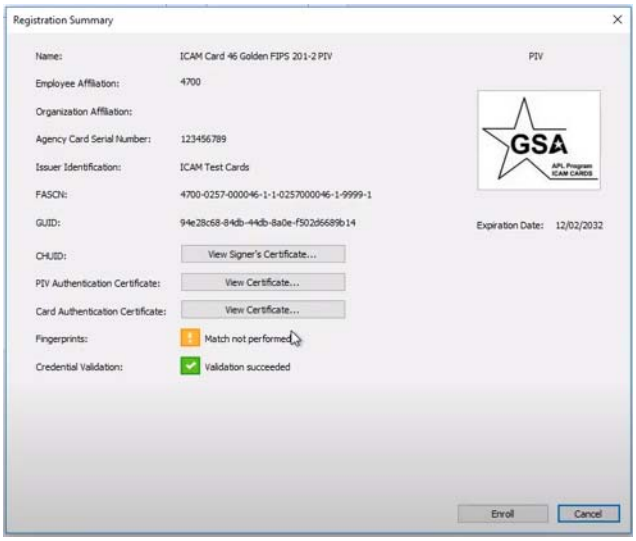
    b. Make sure to select the **Badge type**. Do this before harvesting (importing) the credentials, otherwise the entered information will be cleared.

c. Click [Import]. The Select Import Source dialog is opened.

d. Select the option with the OMNIKEY card scanner. Click [OK].

e. Insert the card in the reader. You will be prompted to enter the PIN to authenticate with the card. The PIN unlocks the secure sector of the card to get the secured data (photo, certificate, first/last name, badge info off the card).

f. Enter the card password, and then click [Import]. The card information is validated using the pivCLASS validation engine in the background. Then the Registration Summary is opened. If the card is validated successfully, there will be no errors.



g. Click [Enroll]. This imports the card information into System Administration. At the end of the process, a message is displayed: “Successfully enrolled credential”. Click [OK] to import the card directly into OnGuard.

h. When asked if you want to keep the default activation dates, click [Yes], and then [OK]. Click [OK] to save record.

22. Add a new access level and assign it to the dual reader interface connected to the PAM with **Timezone** configured to “Always”.

23. Assign this access level to the new cardholder and insert their card in the HID pivCLASS reader slot. An “Access Granted” event will be displayed in Alarm Monitoring from the reader and another event from PAM. **Note:** Access will not be granted for cards that are not registered or are not in the system.

LNL-3300-M5 Setup Information

From System Administration, complete the following steps:

1. From the **Access Control** menu, select **Access Panels**.

2. On the LNL-3300-M5 tab, add a panel of this type with the correct **IP Address**: `10.112.10.10`.

3. From the **Access Control** menu, select **Readers and Doors**. Add a reader configured as follows:

   a. **Name:** PAM M5UL.PivClass Reader 2

   b. **Type:** 8RP Board Reader 1-8

   c. **Output:** F/2F Format

d. **Port:** Port 2
e. **Address:** 1
f. Select the **Authenticated reader** check box.

4. From the **Additional Hardware** menu, select **Logical Sources**.
   a. Add a logical source: In **Name**, enter "pivCLASS PACS Service" (exactly as it is spelled), select a **World time zone,** and then click [OK].
   b. On the **Logical Devices** tab, click [Add], enter "Certificate Manager" in **Name**, select "pivCLASS PACS Service" from **Logical Source** drop-down, and then click [OK].
   c. Add the other devices (the PAM and authenticated readers) using their PivCLASS names as described in a previous step.

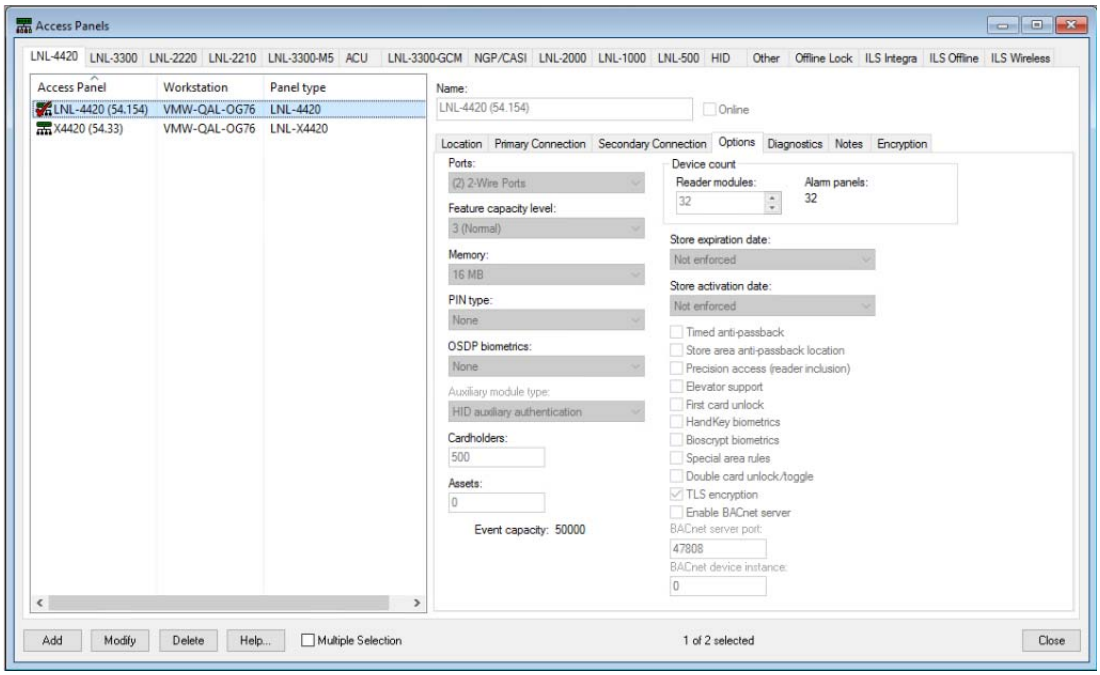
Configure HID Embedded Authentication

1. Copy the HID auxiliary module firmware (**LNLAUXMOD_AAM.bin**) to the **C:\Program Files (x86)\OnGuard** folder.

Note: To remove the HID auxiliary module firmware from the panel, copy **LNLAUXMOD_REMOVE_AAM.bin** to the **C:\Program Files (x86)\OnGuard** folder.

2. Enable panel-based authentication in System Administration:
   a. From the **Access Control** menu, select **Access Panels**, and then **LNL-4420.** Click [Add].
   b. On the **Location** sub-tab:
      - Name the controller and mark it **Online**.
      - Select or browse to the workstation or server to which the controller is or will be connected.
      - Select **Panel type** (LNL-X4420 or LNL-4420). If **Panel type** is "LNL-4420", make sure DIP switch 4 is enabled on that panel.
      - Enter the panel's **Address** which must match the DIP switch setting on the panel.
      - Select the timezone and enable **Daylight savings**.
   a. On the **Primary Connection** sub-tab: Enter the **IP address**.
   b. (Optional) If you are adding a secondary connection for an X-series panel, configure this on the **Secondary Connection** sub-tab.

c. On the **Options** sub-tab: Select “HID auxiliary authentication” as the **Auxiliary module typ**e and enable **TLS encryption**.



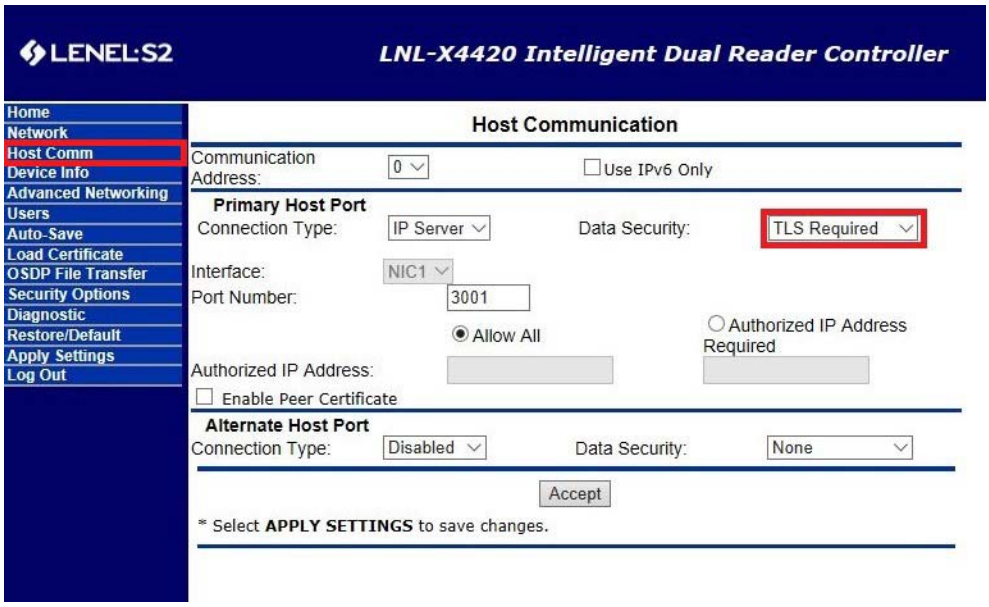
d. Click [OK], and then add the controller to a monitoring zone.

3. From Alarm Monitoring, open the System Status Tree. Locate the LNL-4420 (LNL-X4420) and check the firmware version. It should be 1.275 or later. If not, right-click on the panel, and then select **Auxiliary Module Firmware** > **Download Firmware** to download the firmware to the panel. The panel will be flashing and offline, and then it will reboot. Firmware is available for downloading at the Partner Center (See Prerequisites.)

4. Return to System Administration and open the panel’s web page in a browser. On the LNL-4420 (LNL-X4420) **Location** tab, click [Configuration Web Page] and log into the panel.

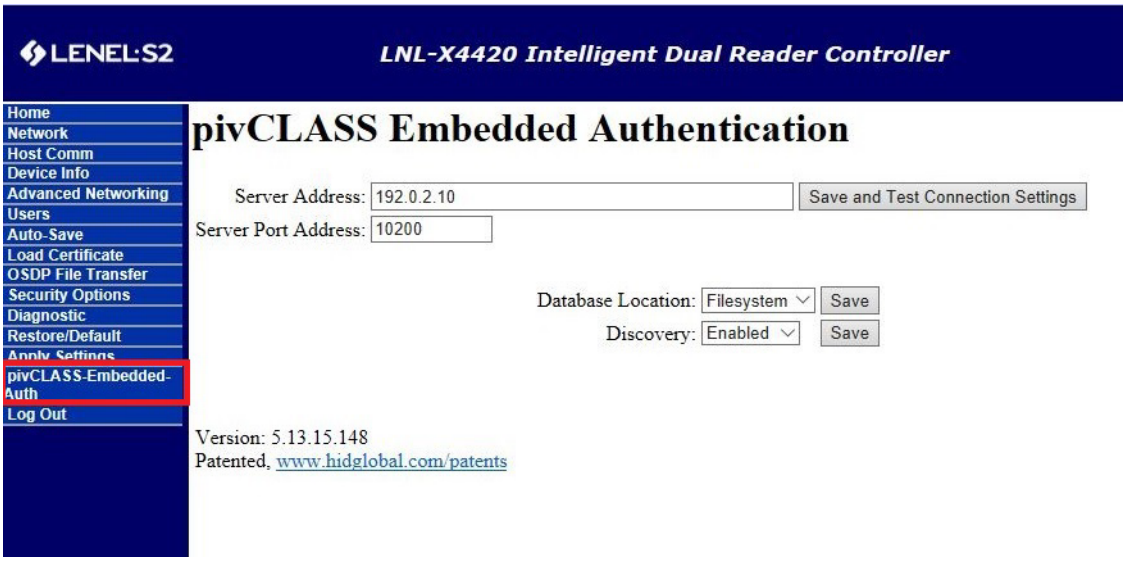
   a. Select **Host Comm** from the sidebar, and then select “TLS Required” from the **Data Security** drop-down. Click [Accept].

Figure 3. Set Host Communication to TLS



b. Select **pivCLASS Embedded Authentication** from the sidebar, and then enter the IP address of the computer where the PACS Service is running. The port should match the pivCLASS Service setting. Click [Save].

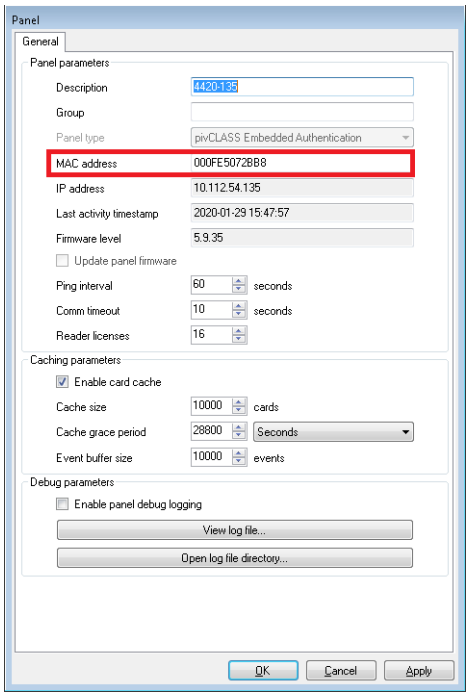
Figure 4. pivCLASS Embedded Authentication Settings



c. Click [Test Connection]. If a panel with a MAC address of this LNL-4420 is not added yet in the pivCLASS PACS Service > **Reader Services**, you will receive a message reporting the connection is successful, but the panel with that MAC address does not exist.

d. If this is the case, add the panel in the pivCLASS PACS Service: Right-click in the **Reader Services** window to bring up the context menu. From the **New** menu, select **pivCLASS**

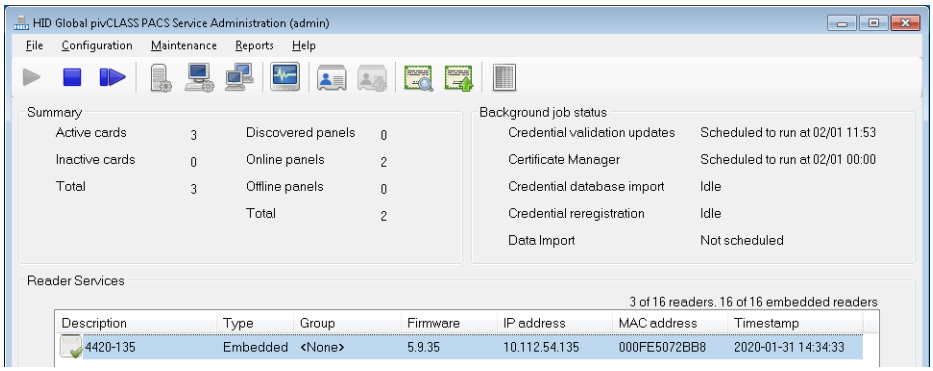
Embedded Authentication panel. When the Panel dialog is displayed, enter the **MAC address** of the panel.



Note: As of version 5.9: The pivCLASS PACS Service discovers the panel so it does not need to be added to Reader Services. The discovered panel information can be edited: Name (**Description**) the panel, and update the **IP address** and **MAC address**. **Reader licenses** should be set to the number of reader licenses allocated for this panel.

e. In pivCLASS PACS Service > **Reader Services**, the correct IP address will be displayed for the LNL-4420 (LNL-X4420).

Figure 5. Correct IP Address Shown for LNL-4420 (LNL-X4420)



f. If the panel is online in the pivCLASS PACS Service, return to the panel's web page and click [Test Connection] again. If it was offline, click [Save and Test Connection Settings]. You should see this message: "Settings updated successfully". Click [Accept]. When asked to validate the certificate, click [Yes] to confirm.

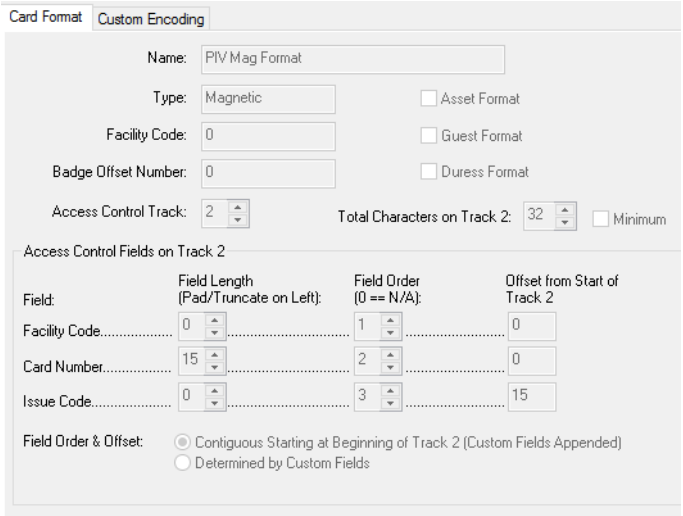
g. Select the **Apply Settings** page, and then **Apply Settings, Reboot** to save the change. Last of all, save it to the actual panel.

5. Add a reader to support FICAM authentication: Return to System Administration. From the **Access Control** menu, select **Readers and Doors**, and then add an Onboard reader to the LNL-4420 (LNL-X4420) **Panel**. Configure the Onboard reader as an **Authenticated reader** with the online and offline reader modes you require. Add the other readers, and any access levels that will be assigned to the readers.

Note: Reader online modes are from the assurance profiles in pivCLASS Reader Services. Reader offline modes include Locked, Unlocked, or Card Only.

6. Add a Magnetic card format for the Embedded Authentication (LNL-4420/LNL-X4420) readers. **Access Control Track 2** = 2, **Total Characters in Track 2 =** 32, **Card Number** = 15. Name it. For example, "PIV Mag Format". This card format was used for legacy FICAM, and is what pivCLASS uses for FICAM authentication.

Figure 6. PIV Mag Format for LNL-4420 (LNL-X4420) Embedded Authentication



Note: **Card Number** can also be set to “16” to obtain the full digits off the card. **Issue Code** length, order, and offset can be “0”.

7. Assign the “PIV Mag Format” card format to the reader.
8. Connect the HID pivCLASS reader to the reader port of the panel. The LCD screen should display “Present Card”.

Technology Industries EntryPoint for OnGuard

In an effort to achieve FIPS 201 compliance, Technology Industry’s EntryPoint solution was integrated with OnGuard.

For more information, refer to the Technology Industries documentation for configuring the EntryPoint software, the guide on setting up the DataConduIT connection, and all of the prerequisites required for this integration.

FIPS 201 Hardware Requirements

Controllers enabled for EntryPoint embedded authentication	Firmware	Supported readers
LNL-4420	1.275 or later	Onboard readers LNL-1320 Series 3, LNL-1300 Series 3, and LNL-1300e readers Schlage PIM-485 AD-402 (AD-302) wireless locks
LNL-X4420	1.275 or later	Onboard reader LNL-1320 Series 3, LNL-1300 Series 3, LNL-1324e, and LNL-1300e readers Schlage PIM-485 AD-402 (AD-302) wireless locks

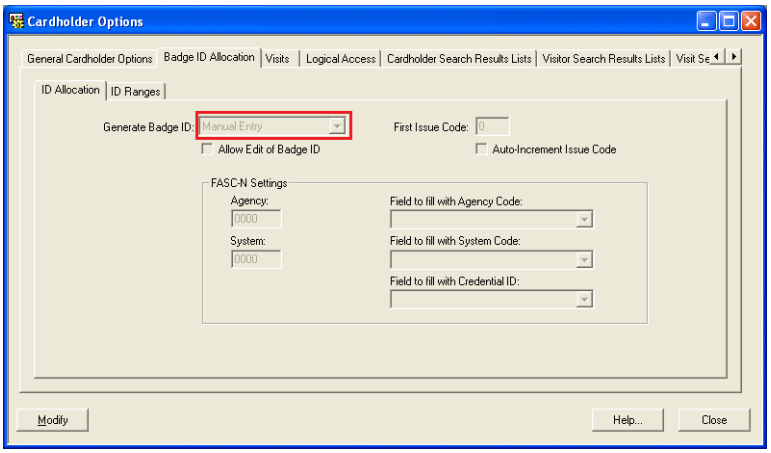
Prerequisites

- The following needs to be installed:
  - OnGuard (See Compatibility Charts to determine which versions of OnGuard are recommended for compliance.)
  - **Add-On Auxiliary Module Firmware** (These modules are posted at the Partner Center on the LenelS2 Hardware Firmware Downloads page: https://partner.lenel.com/downloads/hardware/0/firmware.)
  - **LNLAUXMOD_ENTRYPOINT_AAM.bin** (The EntryPoint auxiliary module firmware is required for the Embedded Authentication solution.) Copy this file to the **C:\Program Files (x86)\OnGuard** folder. To remove the EntryPoint auxiliary module firmware from the panel, copy **LNLAUXMOD_ENTRYPOINT_REMOVE_AAM.bin** to the **C:\Program Files (x86)\OnGuard** folder.

Note: Authentication is required to connect to the TI EntryPoint website. TI issues the login credentials to you when the order is submitted.

- LSDataConduIT Service is running. LSDataConduIT can be run by the Local System account. (This is the default setting.)
- Ports 10100, 1972 and 4242 should be opened in the Windows Firewall. Windows Firewall may be disabled but Network Discovery should be enabled (for non-production environments).
- OnGuard® Communication Server and Linkage Server are running.
- Single Sign-On must be configured in OnGuard. (From System Administration, open the **Directories** folder from the **Administration** menu, and then add a directory. In this example, name the directory “Microsoft Active Directory”. Open the **Users** folder and link the OnGuard User to the directory account that has permission to run OnGuard applications and the LSDataConduIT Service.)
- By default, the cardholder option for badge assignment is set to “Automatic”. However, for EntryPoint to be able to import the card via DataConduIT, this option must be set to “Manual Entry”. This can be done in System Administration at the system level or for each badge type.

(From the ***Administration*** menu, select ***Cardholder Options*** > ***Badge ID Allocation*** > ID Allocation or ***Badge Types*** > ***Badge ID Allocation*** > ID Allocation.)



Compatibility Charts

Compatibility charts of currently supported OnGuard versions and components are available on the LenelS2 website: https://partner.lenel.com.

To access the OnGuard Compatibility Charts:

1. Sign in to the Partner Center, and then select **Downloads.**
2. **Choose product or service**: OnGuard.
3. **Choose version:** Select the version of OnGuard.
4. **Choose type of download:** Compatibility Charts.

Open the **Third Party Applications Compatibility Chart** for Technology Industries EntryPoint Embedded FIPS-201 Authentication support.

Licensing Requirements

TI Licensing

- You need to obtain a license from Technology Industries. Licenses will be provided when your Purchase Order is submitted.
- EP-EWS Base FICAM Enrollment Package. Includes:
  - (1) Registration Workstation License for FIPS/FICAM Enrollment
  - (1) PACS or LACS Connector
  - (1) Certificate Management Engine for Periodic Revocation Checks and connection to Federal Bridge1
  - (1) Database Connector
  - 1st Year Maintenance and Support

For more information, contact Technology Industries:

http://www.entrypoint.io/support/

support@technologyindustries.com

OnGuard Licensing

With DataConduIT being phased out, a new license (SWG-1550-1) has been created. This combines the legacy SWG-1550 and SWG-1140 licenses into one license and becomes the new requirement moving forward.

- **SWG-1550-1** FIPS 201 Credential Management - Enables support for integrated enrollment and authenticated reader management within OnGuard. FICAM Certified in conjunction with HID pivCLASS and Technology Industries EntryPoint software and supported devices (sold separately). This includes a special DataConduIT license specific to pivCLASS and EntryPoint.
- The appropriate number of FIPS-201 Authenticated Readers (SWG-AUTH-XXX) licenses added to your system.

Supported Readers

EntryPoint embedded authentication uses the OSDP Extended Packet Mode to communicate to the readers. This OSDP standard is supported by multiple reader manufacturers including Veridt and Allegion. Contact these manufacturers for currently approved devices:

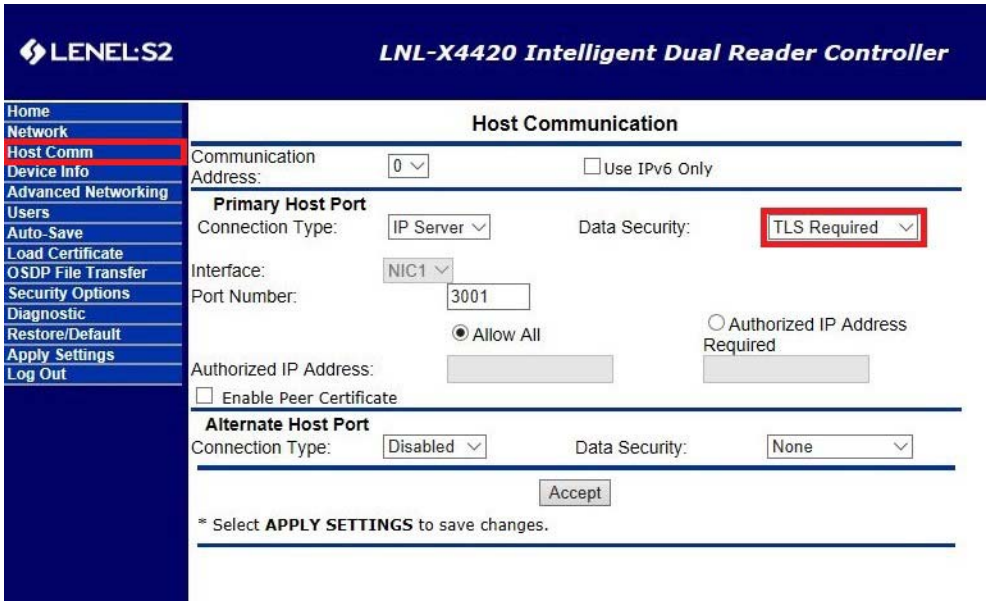
- http://veridt.com/home-pages/
- http://us.allegion.com/en/home/products/brands/aptiQ.html

EntryPoint authenticated readers support the CAK, PKI (PIV Auth), and BIO authenticated modes.

Configure EntryPoint Embedded Authentication

1. From System Administration, configure an LNL-4420 (LNL-X4420) access panel and bring it online.
2. (Optional) On the panel's web page, select **Host Comm** from the sidebar, and then select “TLS if Available” from the **Data Security** drop-down.

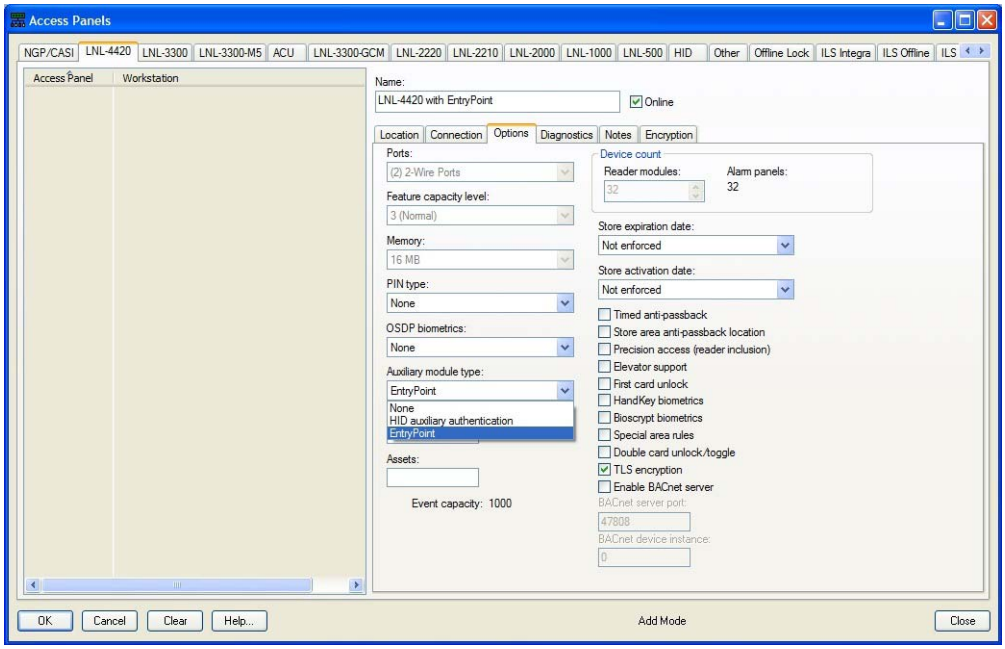
Figure 7. Set Host Communication to TLS



3. Copy the EntryPoint auxiliary module firmware file (**LNLAUXMOD_ENTRYPOINT_AAM.bin**) to **C:\Program Files (x86)\OnGuard**.

Note: To remove the EntryPoint auxiliary module firmware from the panel, copy **LNLAUXMOD_ENTRYPOINT_REMOVE_AAM.bin** to the **C:\ProgramFiles(x86)\OnGuard** folder.

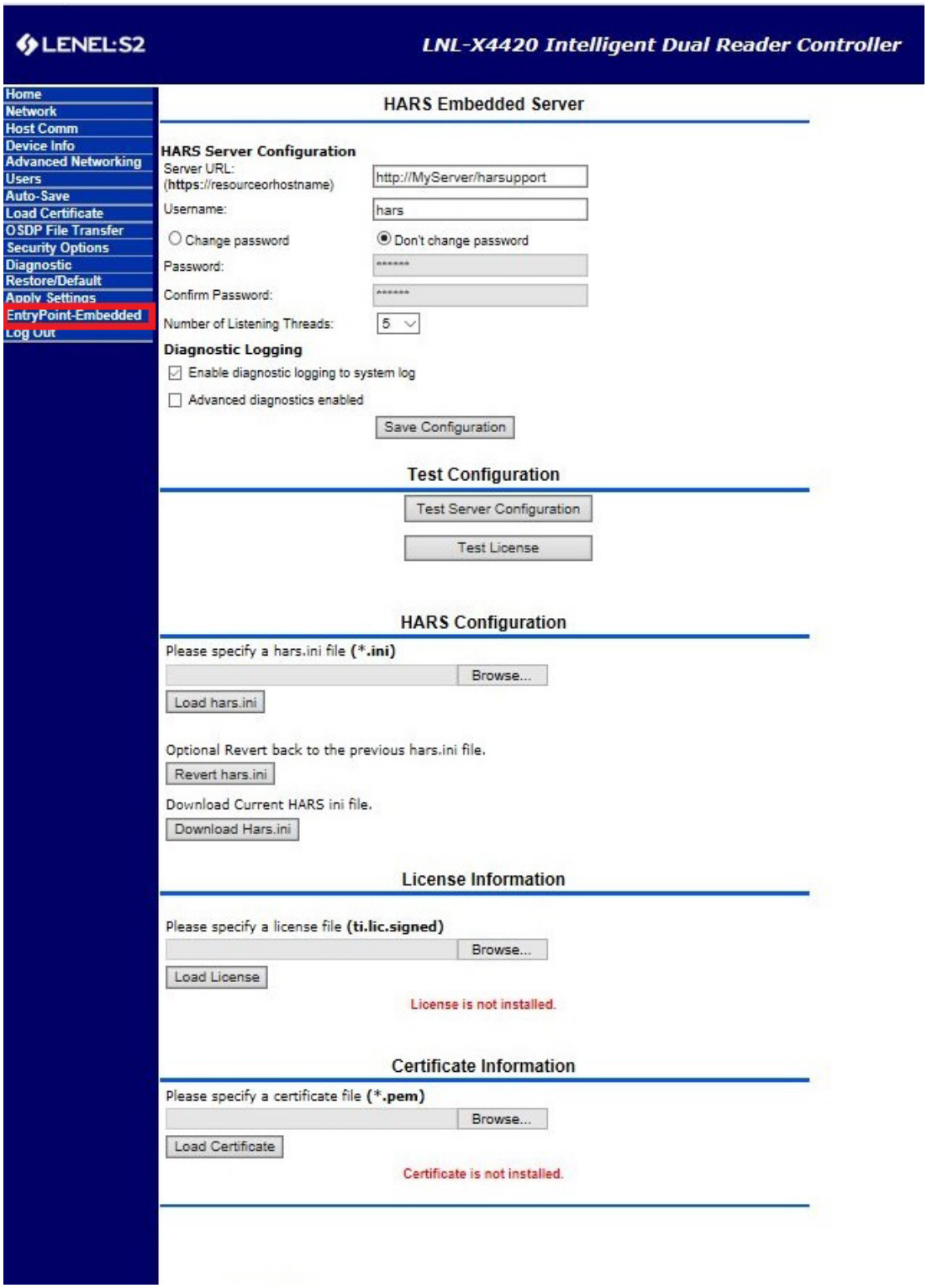
4. Enable panel-based authentication in System Administration:
   a. From the **Access Control** menu, select **Access Panels**, and then the **LNL-4420** tab.
   b. Choose LNL-4420 (LNL-X4420) as the **Panel type**.
   c. On the **LNL-4420 Options** sub-tab, select "EntryPoint" as the **Auxiliary module type**, and then click [OK].



5. In Alarm Monitoring, open the System Status Tree. Right-click on the LNL-4420 (LNL-X4420), and then select **Auxiliary Module Firmware** > **Download Firmware** to download the firmware to the panel.

6. Open the panel's web page again, and then select **EntryPoint-Embedded** from the sidebar to configure the settings.

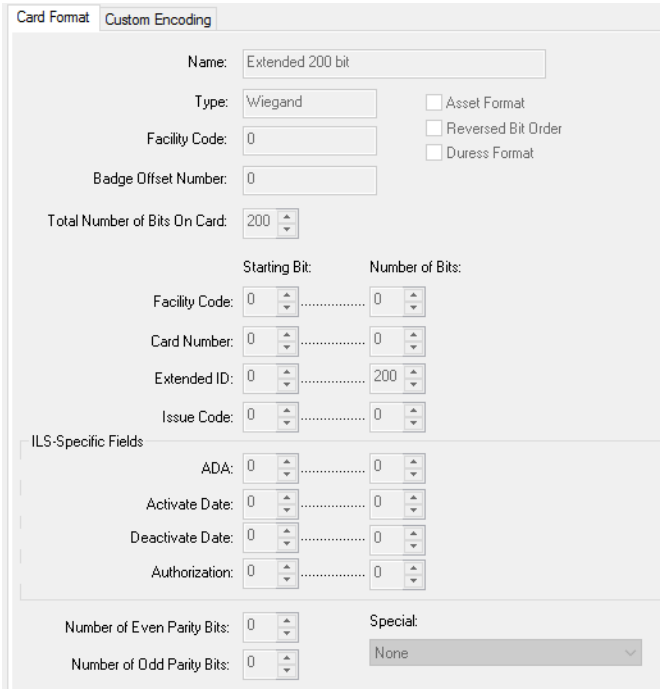
Figure 8. EntryPoint Embedded Authentication Settings



a. Add in your IP Address of the host EntryPoint server
a. Keep the **Username** “hars”
b. If you want to change the password, select **Change password**.
c. (Optional) Under Diagnostic Logging: Select **Enable diagnostic logging to system log** and **Advanced diagnostics enabled**, Click [Save Configuration].
d. Under License Information: Click [Browse] to the license file. Click [Open] in the file browser, and then click [Load License]. When the license is loaded, the license ID, and start and end date are displayed.
e. (Optional) Under Certification Information: Click [Browse] to the certificate file. Click [Open] in the file browser, and then click [Load Certificate].

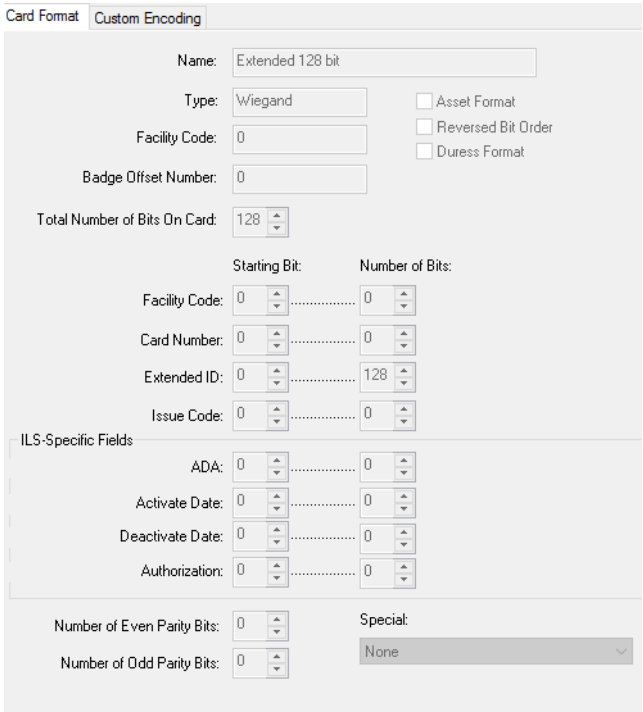
7. On the panel’s web page, open the **Apply Settings** menu option, then click [Apply Settings, Reboot]. This saves the configuration and reboots the panel.
8. When you are done configuring the connection, log off the panel’s web page.
9. Return to System Administration. From the **Access Control** menu, select **Readers and Doors**.
10. On the General tab, add an “OnBoard” reader to the LNL-4420 (LNL-X4420) panel.
11. For hard-wired readers: Add as “OSDP Protocol” reader **Type**.
12. (Optional) Add a “Schlage PIM-485” lock to the LNL-4420 (LNL-X4420) panel. Choose “Mag with Wiegand Output” as the **Output**.
13. Configure the reader or lock as an **Authenticated reader** with the online and offline reader modes you require.
14. From the **Administration** menu, select **Card Formats**.
    a. Add a Wiegand card format with **Extended ID** = 0 - 200. Enter a name for this card format. For example, “Extended 200-bit”.

Figure 1. Extended ID 200-bit card format



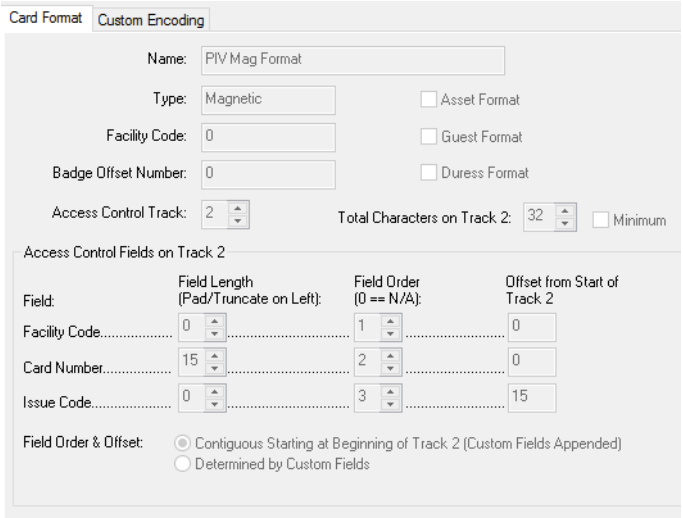
b. Add a Wiegand card format with **Extended ID** = 0 - 128. Enter a name for this card format. For example “Extended 128-bit”.

Figure 2. Extended ID 128-bit card format



15. Assign the “Extended 200-bit” and/or “Extended 128-bit” card format to the reader.
16. Add a Magnetic card format. Configure **Total characters=**32 and **Card Number**=15. Name the card format. In this example, “PIV Mag Format”.

Figure 3. Magnetic card format for LNL-4420 Embedded Authentication



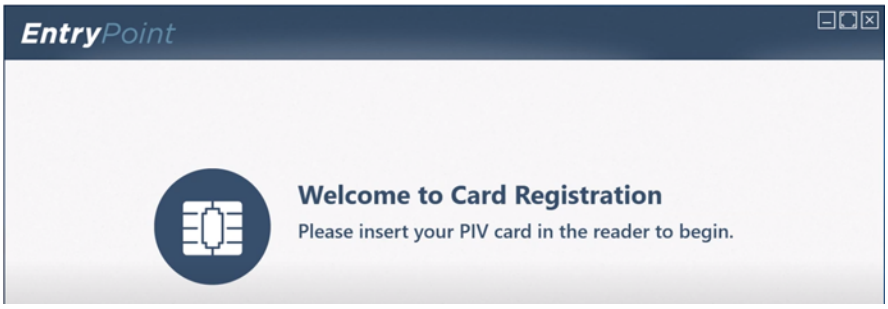
17. Assign the “PIV Mag Format” card format to the reader or lock.

Note: Schlage locks require a magnetic card format.

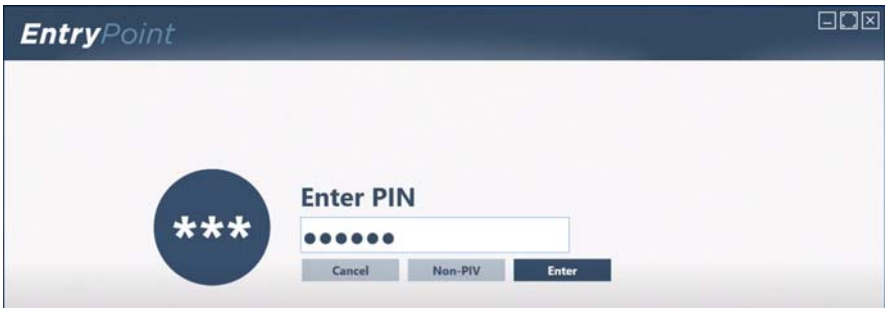
18. Connect the authenticated reader to the reader port of the panel per the reader manufacturer installation instructions.

EntryPoint Card Registration

1. Insert the PIV card in the reader.

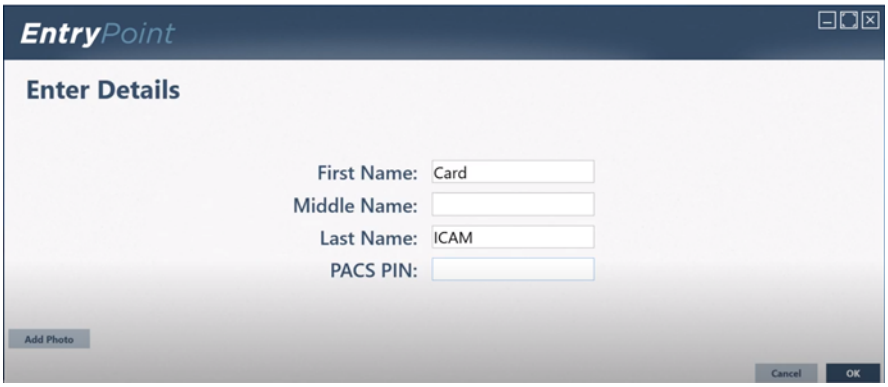


2. Enter PIN, and then click [Enter].



The card's security objects, photo, chip, and fingerprints are read.

3. Enter Details, and then click [OK]. A message then reports the card is enrolled.



Embedded Auxiliary Authentication Module: Validation Agent

Validation Agent is an Auxiliary Authentication Module (AAM) that runs inside an LNL-X4420 access panel. Validation Agent also communicates with ValTrust to receive certificate status information.

The following information will cover configuration of the Validation Agent AAM in OnGuard. See ValTrust documentation for setting up the connection of the Validation Agent AAM to ValTrust.

Hardware Requirements

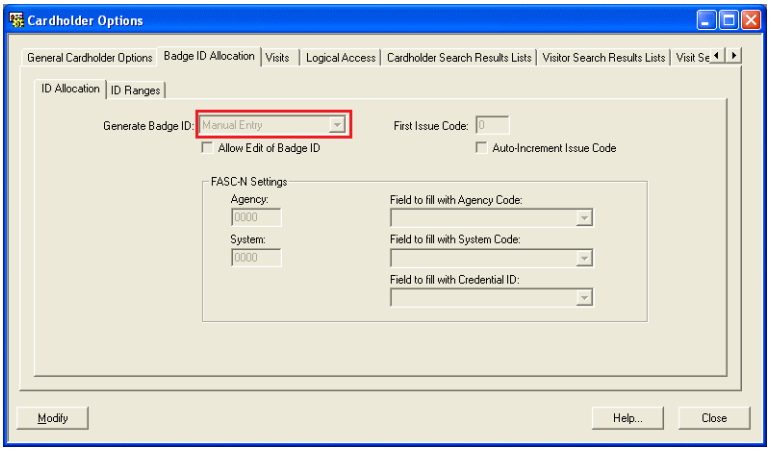
For Embedded Authentication functionality:

Controller enabled for Validation Agent embedded authentication	Firmware	Supported readers
LNL-X4420	1.305 or later	Onboard readers LNL-1320 Series 3, LNL-1300 Series 3, and LNL-1300e readers LNL-1324e

Prerequisites

- The following needs to be installed:
  - OnGuard (See Compatibility Charts to determine which versions of OnGuard are recommended for compliance.)
  - **Add-On Auxiliary Module Firmware** (These modules are posted at the Partner Center on the LenelS2 Hardware Firmware Downloads page: https://partner.lenel.com/downloads/hardware/0/firmware.)
  - **LNLAUXMOD_VALIDATIONAGENT_AAM.bin** (The Validation Agent auxiliary module firmware is required for the Embedded Authentication solution.) Copy this file to the **C:\Program Files (x86)\OnGuard** folder. To remove the Validation Agent auxiliary module firmware from the panel, copy **LNLAUXMOD_VALIDATIONAGENT_REMOVE_AAM.bin** to the **C:\Program Files (x86)\OnGuard** folder.

- By default, the cardholder option for badge assignment is set to “Automatic”. However, for Validation Agent to be able to import the card via OpenAccess, this option must be set to “Manual Entry”. This can be done in System Administration at the system level or for each badge type. (From the ***Administration*** menu, select ***Cardholder Options*** > ***Badge ID Allocation*** > ID Allocation or ***Badge Types*** > ***Badge ID Allocation*** > ID Allocation.)



Compatibility Charts

Compatibility charts of currently supported OnGuard versions and components are available on the LenelS2 website: https://partner.lenel.com.

To access the OnGuard Compatibility Charts:

1. Sign in to the Partner Center, and then select **Downloads.**
2. **Choose product or service**: OnGuard.
3. **Choose version:** Select the version of OnGuard.
4. **Choose type of download:** Compatibility Charts.

Open the **Third Party Applications Compatibility Chart** for Validation Agent Embedded FIPS-201 Authentication support.

Licensing Requirements

OnGuard Licensing

- **FIPS 201 Credential Management (SWG-1550)** - This license is required in order to select **Auxiliary Module Type** on the Panel Options form and the **Authenticated Reader** option on the Readers and Doors form.
- Additional OpenAccess licensing is required to integrate ValTrust with OnGuard (for cardholder demographic data transfer and badge data transfer).
- **MAX_NUM_FIPS201_AUTHENTICATED_READERS (SWG-AUTH-XXX)** - Allocates the appropriate number of FIPS-201 Authenticated Readers licenses added to your system.

Supported Readers

Validation Agent embedded authentication uses the OSDP Transparent Mode to communicate with the readers. This OSDP standard is supported by multiple reader manufacturers including Veridt and HID Global. Contact these manufacturers for currently approved devices:

http://veridt.com/home-pages/

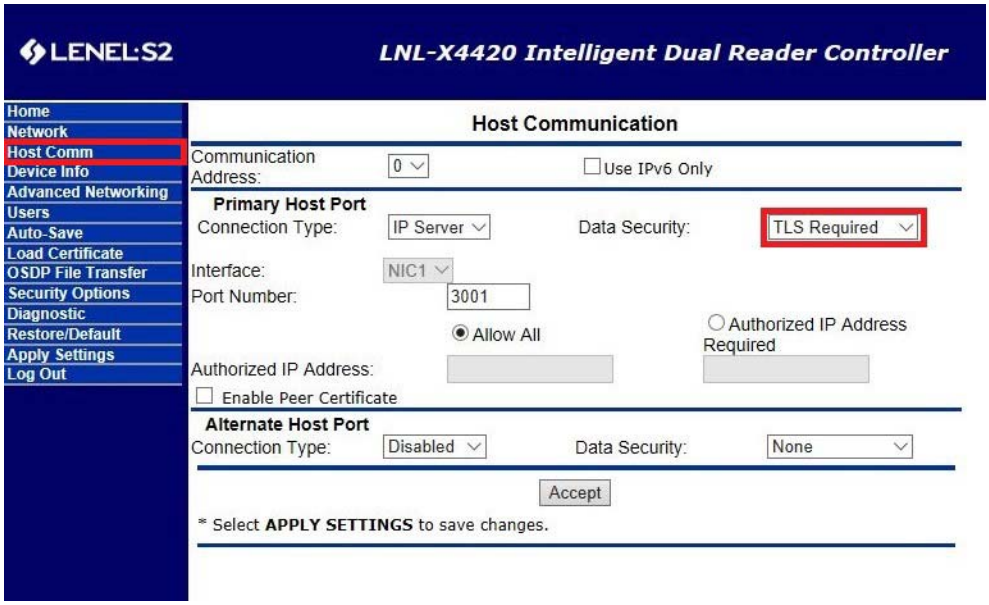
https://www.hidglobal.com/

Validation Agent authenticated readers support the CAK, PKI (PIV Auth), and BIO authenticated modes.

Configure Validation Agent Embedded Authentication

1. From System Administration, configure an LNL-X4420 access panel and bring it online.
2. (Optional) On the panel's web page, select **Host Comm** from the sidebar, and then select "TLS if Available" from the **Data Security** drop-down.

Figure 4. Set Host Communication to TLS

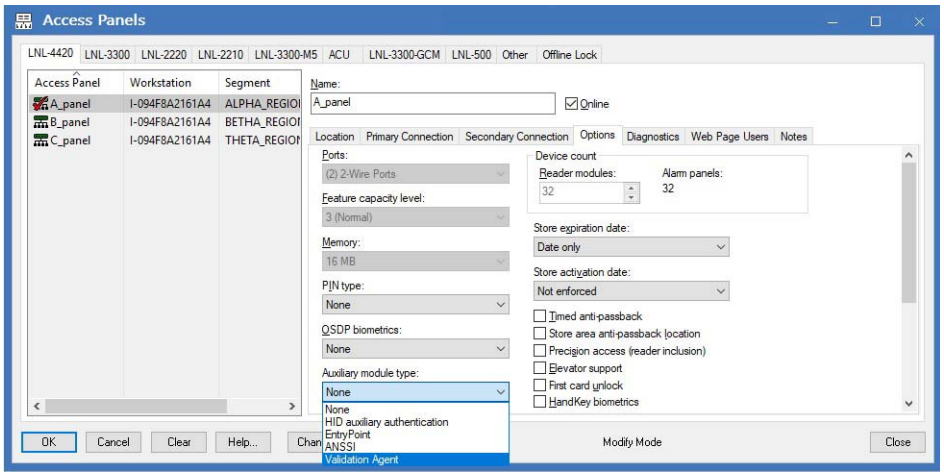


3. Copy the Validation Agent auxiliary module firmware file (**LNLAUXMOD_VALIDATIONAGENT_AAM.bin**) to **C:\Program Files (x86)\OnGuard**.

Note: To remove the EntryPoint auxiliary module firmware from the panel, copy **LNLAUXMOD_VALIDATIONAGENT_REMOVE_AAM.bin** to the **C:\ProgramFiles(x86)\OnGuard** folder.

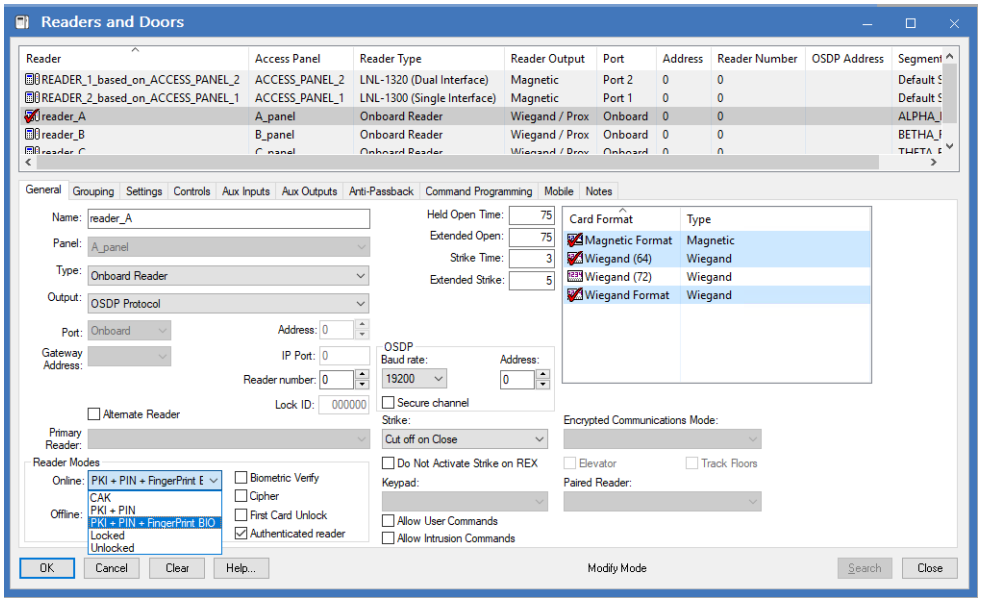
4. Enable panel-based authentication in System Administration:
   a. From the **Access Control** menu, select **Access Panels**, and then the **LNL-4420** tab.
   b. Choose LNL-X4420 as the **Panel type**.

c. On the **LNL-4420 Options** sub-tab, select “Validation Agent” as the **Auxiliary module type**, and then click [OK].



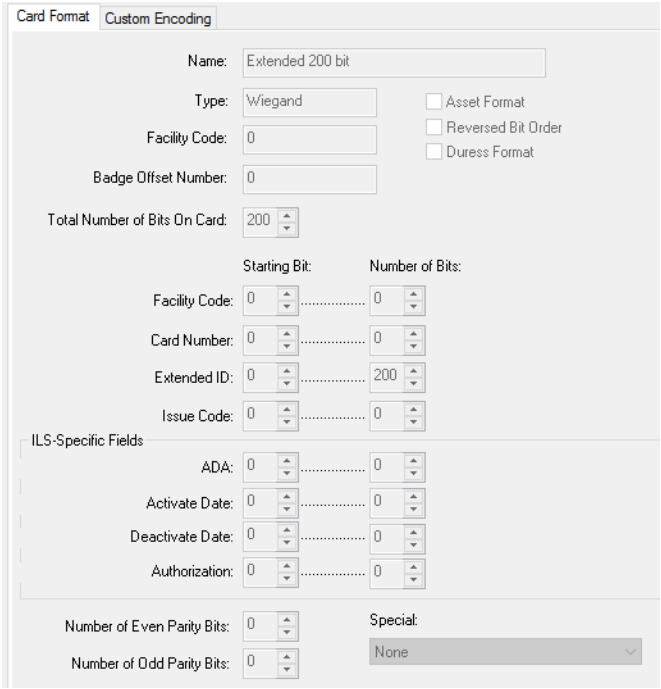
5. In Alarm Monitoring, open the System Status Tree. Right-click on the LNL-X4420, and then select **Auxiliary Module Firmware** > **Download Firmware** to download the firmware to the panel.
6. From System Administration: From the **Access Control** menu, select **Readers and Doors**.
7. On the General tab, add an “OnBoard” reader to the LNL-X4420 panel.
8. For hard-wired readers: Add as “OSDP Protocol” reader **Type**.
9. Configure the reader or lock as an **Authenticated reader** with the online and offline reader modes you require.

Note: The Reader **online** modes are the assurance profiles from pivCLASS Reader Services including the default Validation Agent reader authentication modes (CAK, PKI + PIN, and PKI + PIN + FingerPrint BIO) and any custom reader authentication modes that may have been added. Reader **offline** modes include Locked and Unlocked.



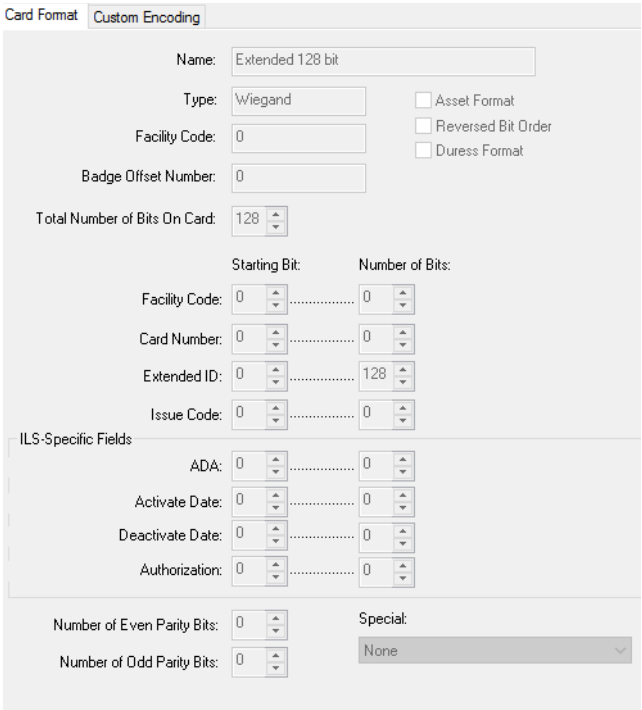
10. It is recommended to run the reader at a faster OSDP **Baud rate** than the default OSDP **Baud rate** of 9600.
11. From the **Administration** menu, select **Card Formats**.
    a. Add a Wiegand card format with **Extended ID** = 0 - 200. Enter a name for this card format. For example, “Extended 200-bit”.

Figure 1. Extended ID 200-bit card format



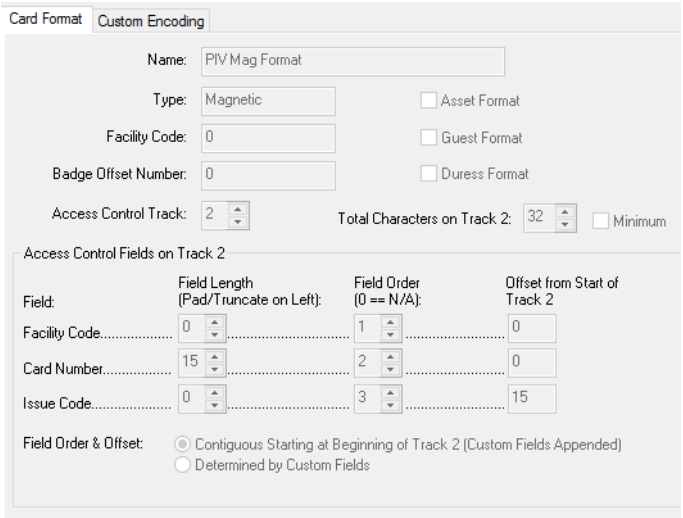
    b. Add a Wiegand card format with **Extended ID** = 0 - 128. Enter a name for this card format. For example “Extended 128-bit”.

Figure 2. Extended ID 128-bit card format



12. Assign the “Extended 200-bit” and/or “Extended 128-bit” card format to the reader.
13. Add a Magnetic card format. Configure **Total characters=**32 and **Card Number**=15. Name the card format. In this example, “PIV Mag Format”.

Figure 3. Magnetic card format for LNL-4420 Embedded Authentication



14. Assign the “PIV Mag Format” card format to the reader or lock.
15. Connect the authenticated reader to the reader port of the panel per the reader manufacturer’s installation instructions.

