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 via the LNL-4420 (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.

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)

Prerequisites

- The following applications need to be installed:
  - OnGuard (See Compatibility Charts to determine which version of OnGuard is 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.
  - **FIPS_201_SDK** The FIPS 201 SDK license is required for OnGuard enrollment.
- Only 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. 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.)
- 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.)
- HID license with the following:
  - pivCLASS license key
  - SDK license key
  - PAM in Panel license key
  - (Optional) IDPublisher license key

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:

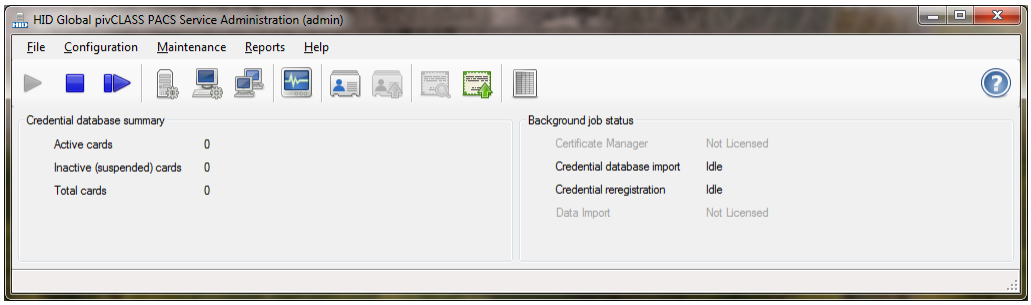
1. Sign in to the Partner Center, and then select **Downloads.**
2. **Choose product or service**: OnGuard.
3. **Choose version:** Select the version of OnGuard.
4. **Choose type of download:** Compatibility Charts.
5. Open the **Third Party Application Compatibility Chart** for HID pivCLASS Embedded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

pivCLASS PACS SERVICE

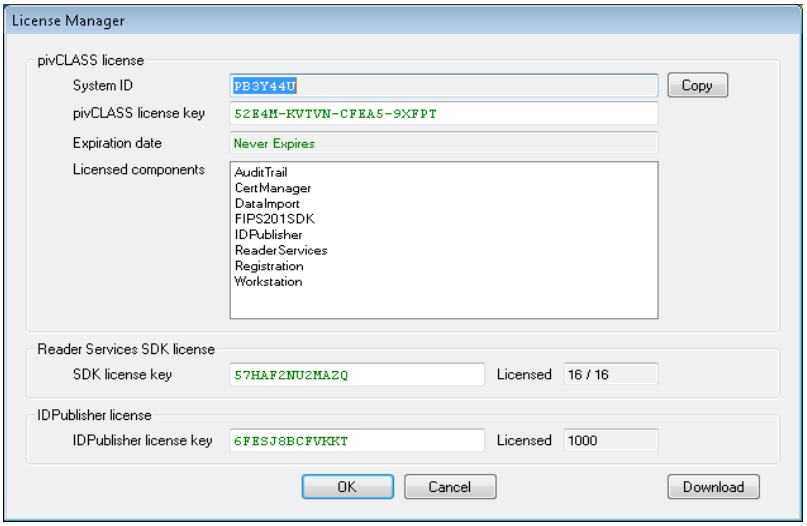
Configure the pivCLASS PACS Service

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].

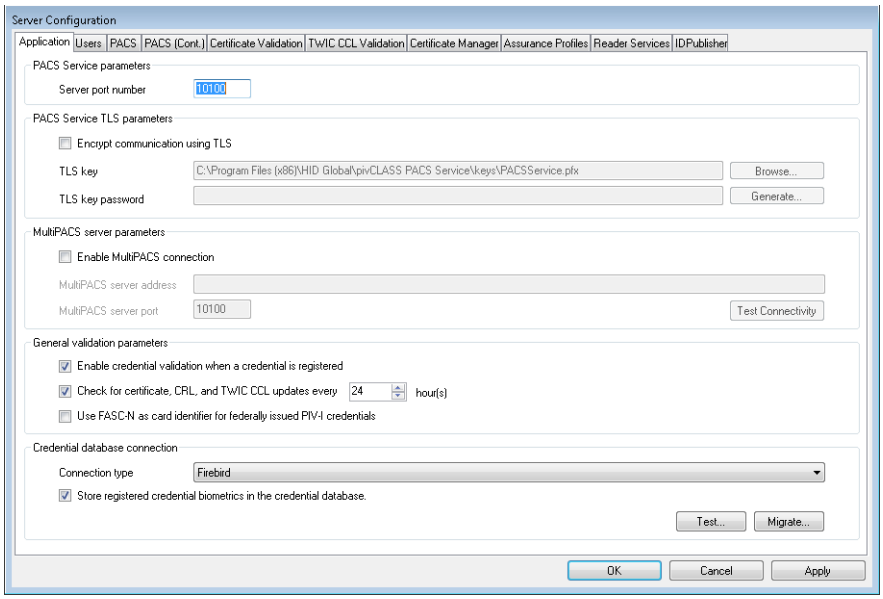
Figure 1. pivCLASS PACS Service Administration



4. From the **File** menu, select **License Information**, and then enter the license keys. (See Prerequisites.)

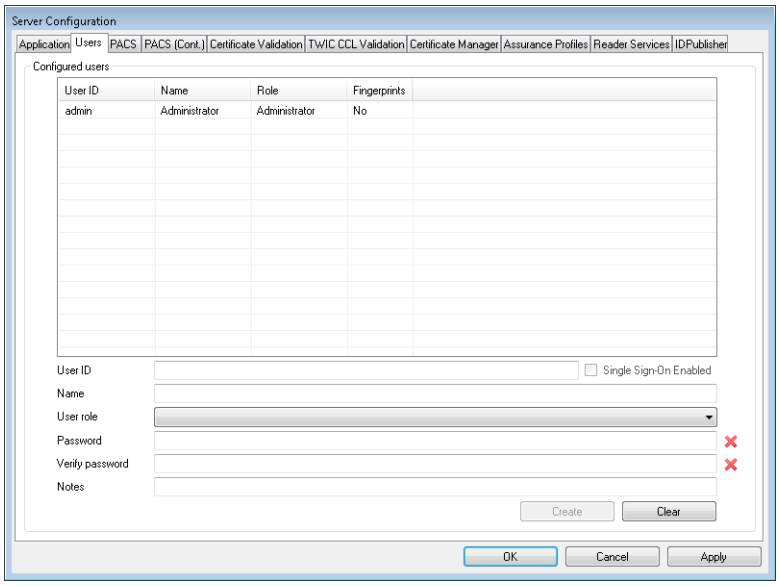


5. From the **Configuration** menu, select **Edit Service Settings** to open the Server Configuration window.

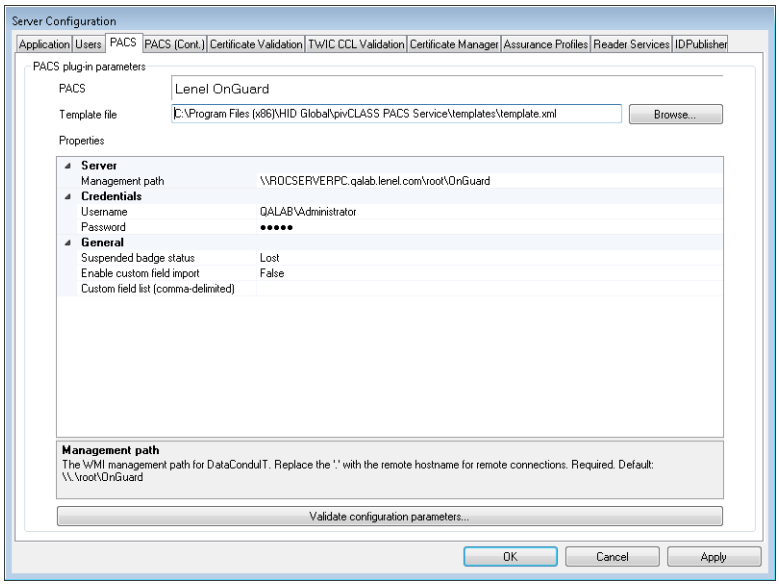


6. On the **Application** tab:
   a. Make sure the **Server port number** is `10100`.
   b. The following settings are optional depending on your system:
      - **Enable Credential Validation When a Credential is Registered:** Select this option to validate credential registrations during registration.
      - **Check For Certificate, CRL, and TWIC CCL Updates Every** `24` **hour(s):** Select this option to specify the pivCLASS software will update its certificates, CRLs, and TWIC CCL and MD5 files periodically. Select how often the update is to occur in hours.
      - **Connection Type:** Select the connection type “Firebird”. Choosing this connection type pre-configures the default Firebird settings. The Firebird database file is located in the **C:\Program Files (x86)\HID Global\pivCLASS PACS Service\db** folder.
      - **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.

7. On the **Users** tab: Create a new user. Retain the default values. ("admin" will be added to the list automatically.)



8. On the **PACs** tab: 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.



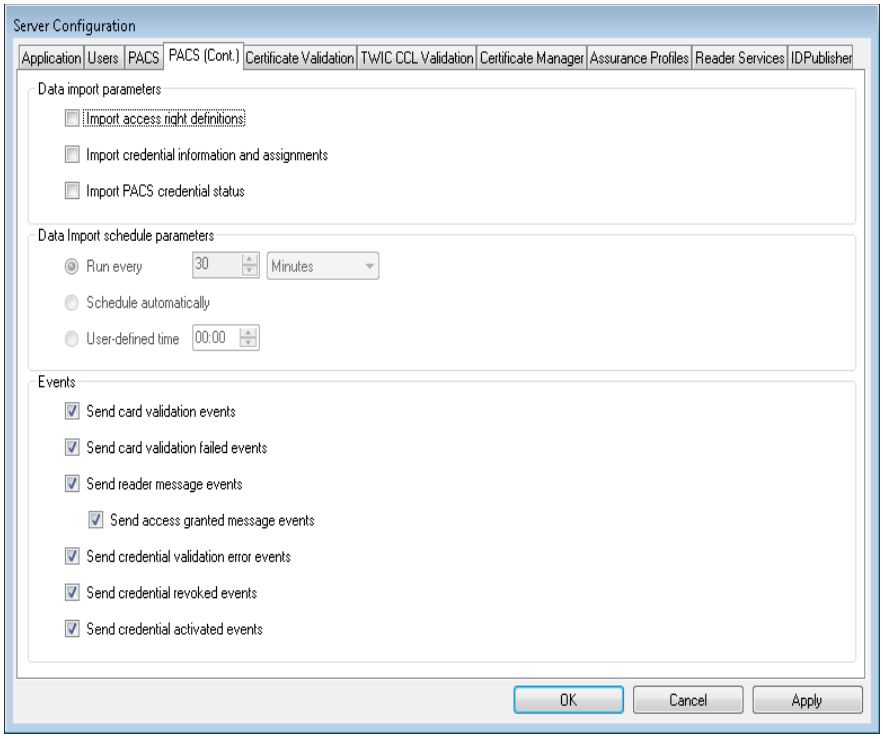
a. Under **Server**:
Set the **Management path** as \\.\root\OnGuard. (Enter a dot "." if OnGuard and PACS service are installed on a same computer. Otherwise - instead of a dot, enter the full name of the OnGuard server.)

b. 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.

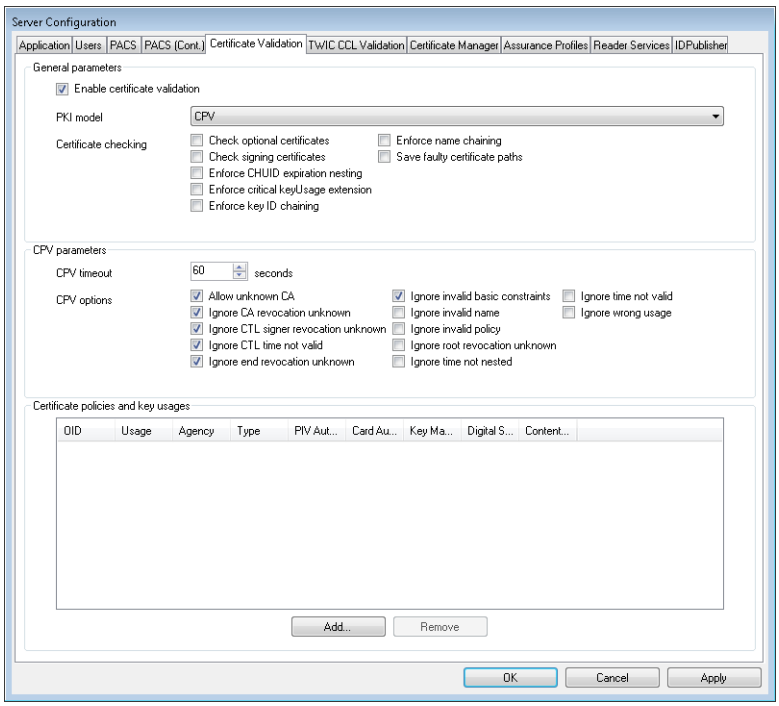
c. Under **General**:
Select "Lost" from the **Suspended Badge Status** drop-down.
Select "False" from the **Enable custom field import** drop-down, and then click [OK] to save the settings.

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

9. On the **PACS (Cont.)** tab: Under **Events**: Select the **Send card validation events** and **Send card validation failed events** check boxes.

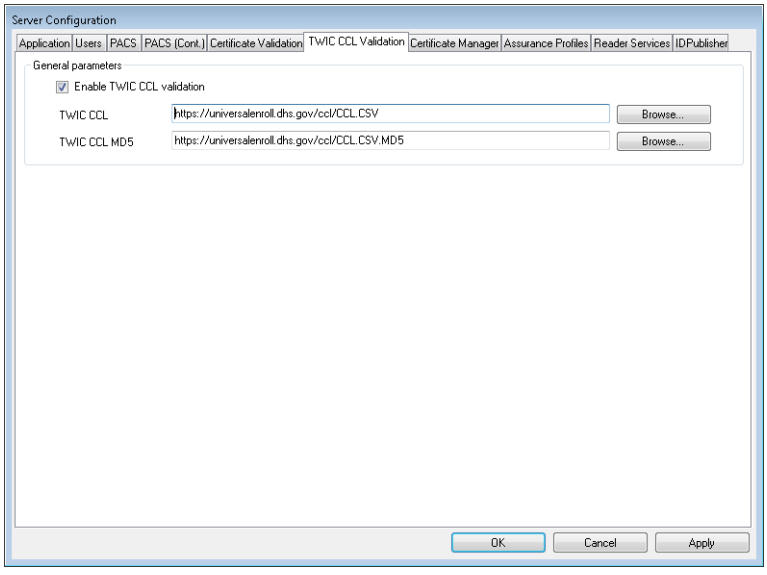


10. On the **Certificate Validation** tab:



a. Select the **Enable certificate validation** check box.
b. Specify the **PKI model** as "CPV" for revocation status checking.
c. Set the **CPV timeout** to 60 seconds and choose the CPV options to be used for certificate validation.

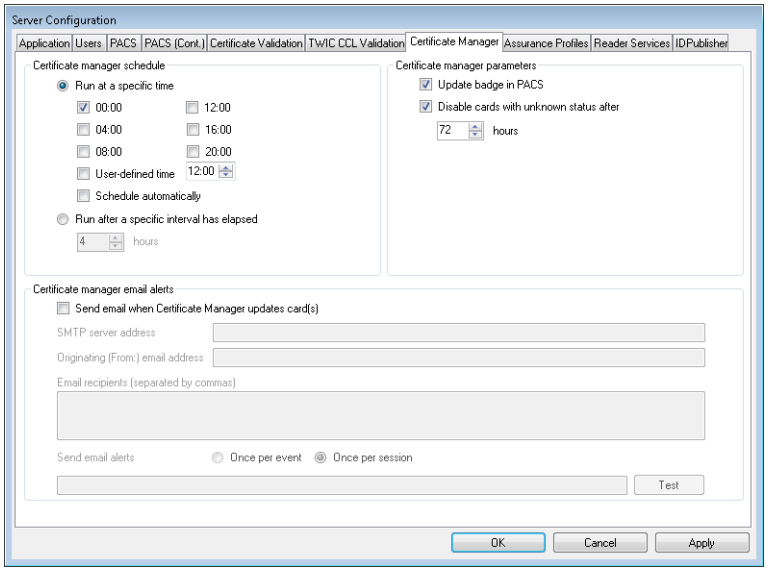
11. On the **TWIC CCL Validation** tab: Select the **Enable TWIC CCL validation** check box.



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.

12. On the **Certificate Manager** tab:

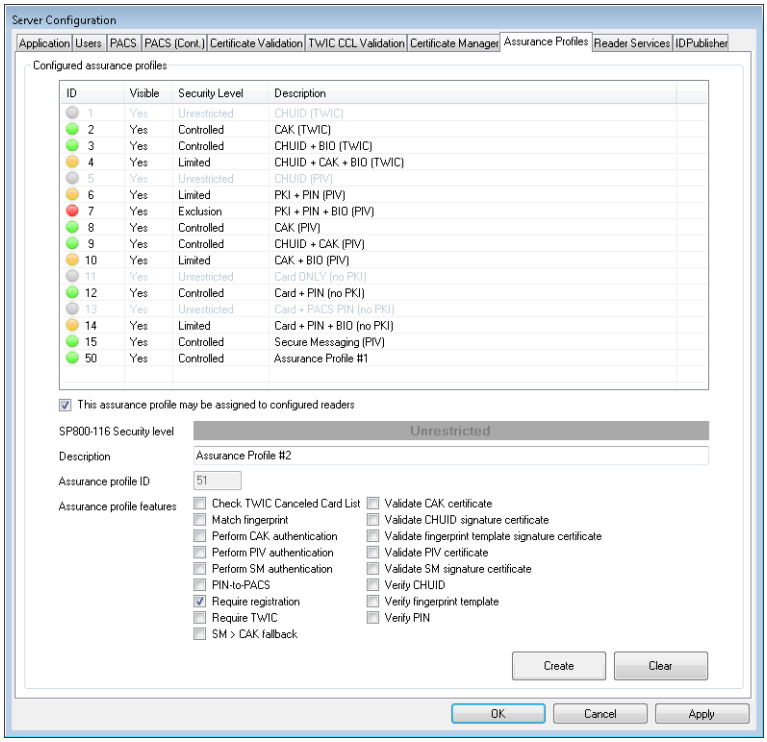


a. Select **Run at a specific time** to enable running the Certificate Manager at specific times to re-evaluate all credentials.

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

c. Select **Update badge in PACS** and **Disable card with unknown status after** *nnn* **hours**.

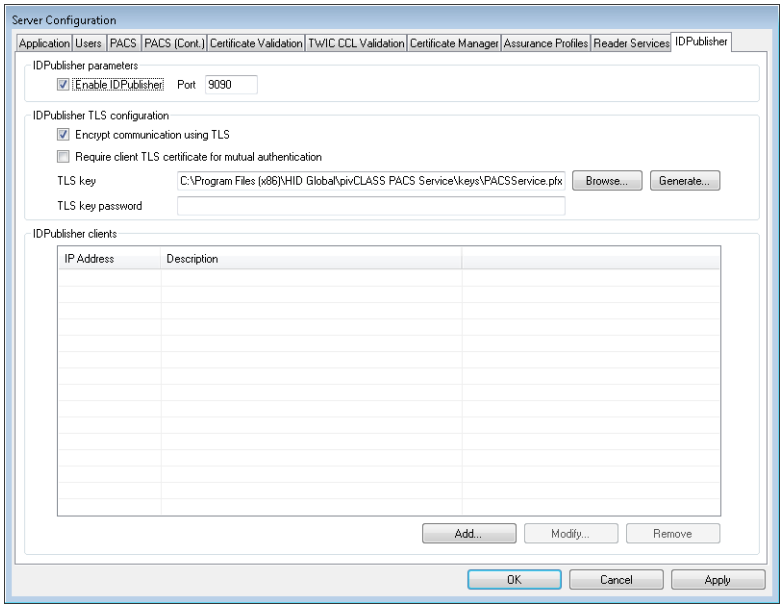
13. Use the **Assurance Profiles** form to create and update assurance profiles.



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,

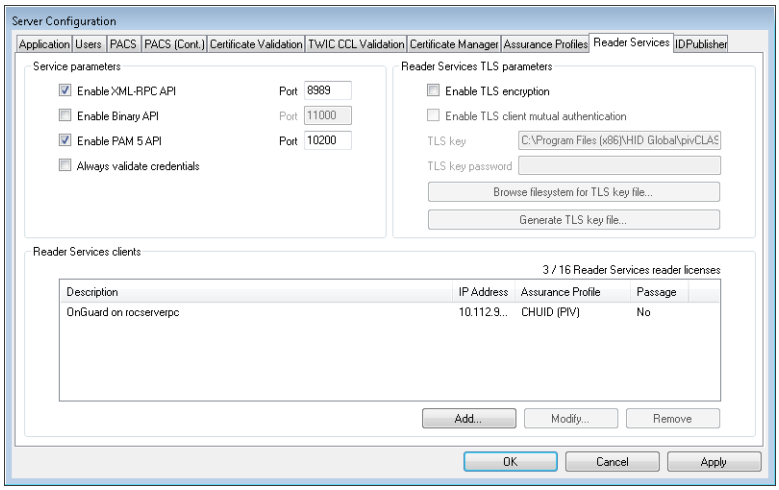
a. Select the **Enable IDPublisher** check box.

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:

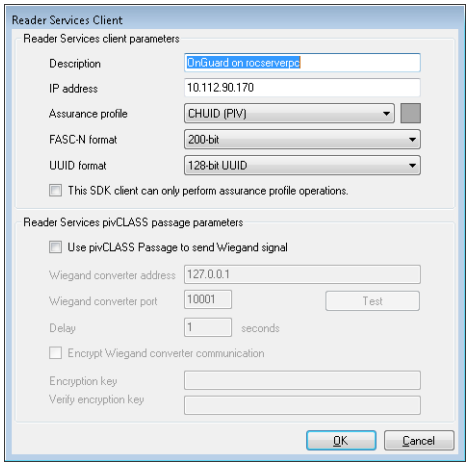


a. Select the **Enable XML-RPC API** check box. **Port** is set to 8989 by default.

Note: In the OnGuard® System Administration **FIPS 201 Credentials** folder, make sure the Cashing Status Proxy **Port** is the same as the **XML-RPC Port**.

b. Select the Enable **PAM 5 API** check box with **Port** set to `10200` (Only for PAM configuration.)

c. Click [Add] to add a Reader Services client. (This is the computer on which OnGuard is installed.)



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

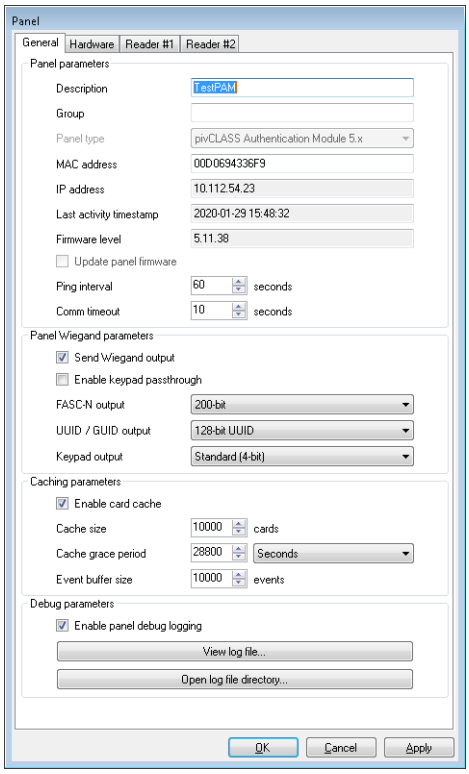
e. Enter the **IP Address**. This is the IP address of the OnGuard computer. Click [OK] to save the client settings and close the dialog. Click [OK] to save all configuration changes.

f. If the Communication Server is running on a different computer from the OnGuard server computer, add another Reader Services client with the IP address of the Communication Server computer.

Configure a PAM in the PACS Service

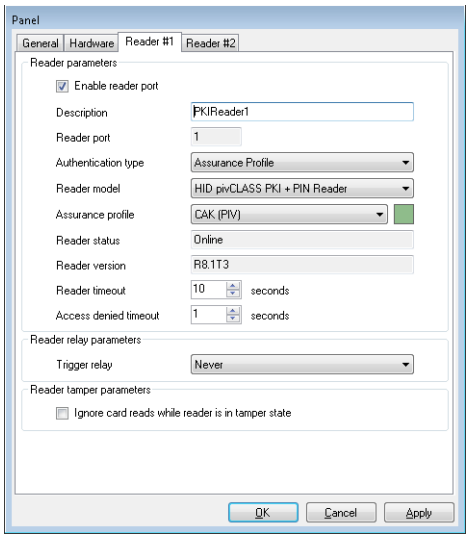
Note: If the PAM device does not have a valid IP address yet, this can be done later. (For instructions, refer to PAM DEVICE on page 14.)

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.



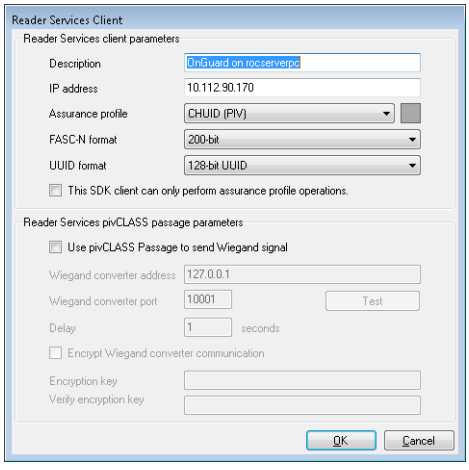
   a. On the **General** tab: Enter a name for the PAM in **Description**. (This name will be also used in OnGuard). In this example, “TESTPAM” was used.
   b. Enter the **MAC address** of the PAM device. (Later, this PAM device will be configured on its web page to communicate with the pivCLASS PACS service.)
   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.

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.**

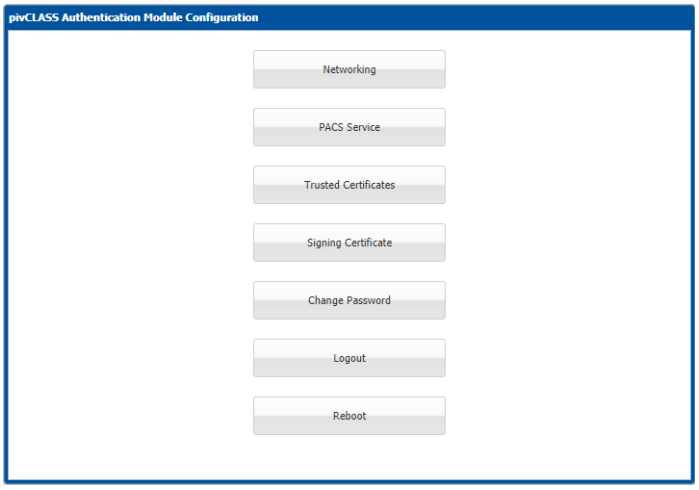
    c. Select **Use the following IP Address** and enter the following:
    IP address: 192.168.0.10
    Subnet mask: 255.255.255.0
    Default gateway: 192.168.0.1

    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`



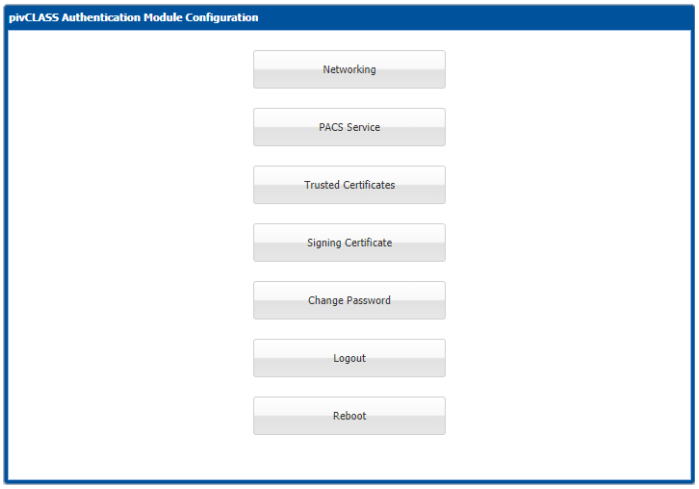
3. Click [Networking] to assign a new IP address for the PAM device.

   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.

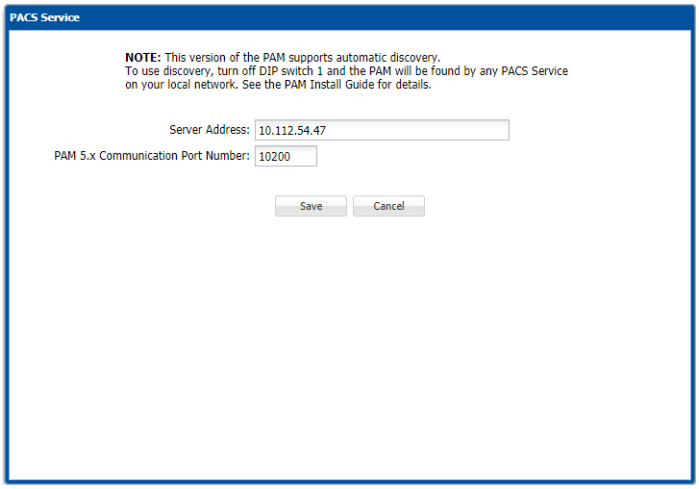
Verify New IP Address on PAM Web Page

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`

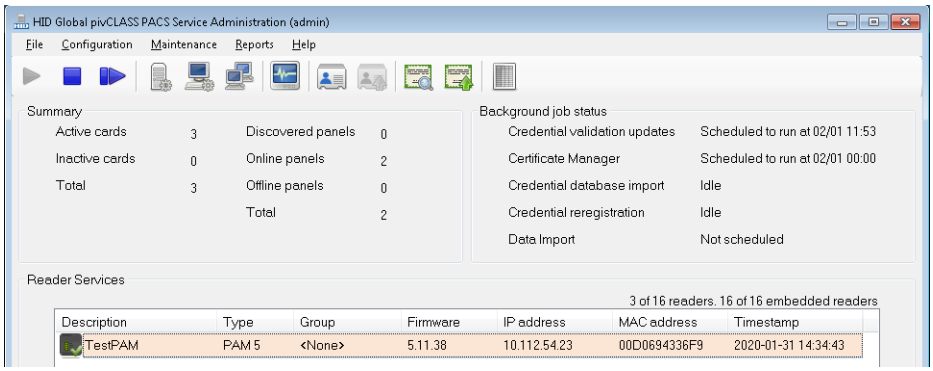


8. Click [PACS Service].



   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, enter the FIPS 201 SDK License Key in the **License Key** field. Alternately, you can simply click on [Download License].
5. On the **Credential Validation** tab: Keep the default settings, but set the Credential Validation settings to **Validate on Caching Status Proxy**.
6. On the **Catching Status Proxy** tab:
   a. Select “pivCLASS” as the **Caching status proxy service**.
   b. In the **Server hostname** field, enter the IP address (or the full name) of the computer where PACS Service is installed.
   c. `10100` in **Port** field.
   d. Select all three (3) check boxes in the Enrollment settings section.

e. Select “Returned” status for the badge status.

f. Enter 8989 (or whatever port number is set for the XML-RPC port in the PACS service) in the **XML-RPC Port** field.

g. Click [Test Connection]. A message should display confirming you are “Successfully connected to Caching Status Proxy server”.

h. 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**. On the **General System Options** tab, select the **Generate software events** check box under the **OpenAccess host** section, and then click [OK].

9. Also 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].

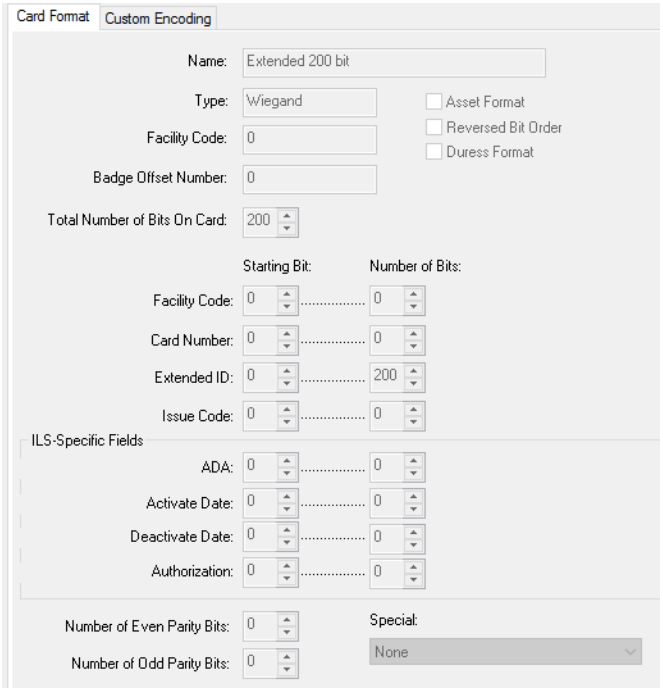
    b. On the **Logical Devices** tab, click [Add], enter “Certificate Manager” in **Name**, select “pivCLASS PACS Service” from **Logical Source** drop-down, and then click [OK].

    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. From the **Administration** menu, select **Card Formats**.

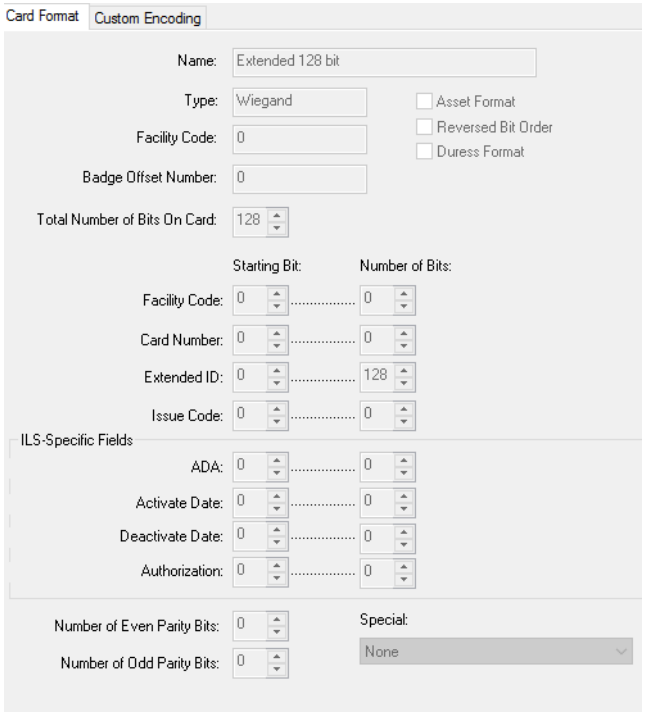
    a. Add a Wiegand card format with **Extended ID** = 0 - 200. Name this card format. For example, “Extended 200-bit”.

Figure 1. Extended ID 200-bit card format



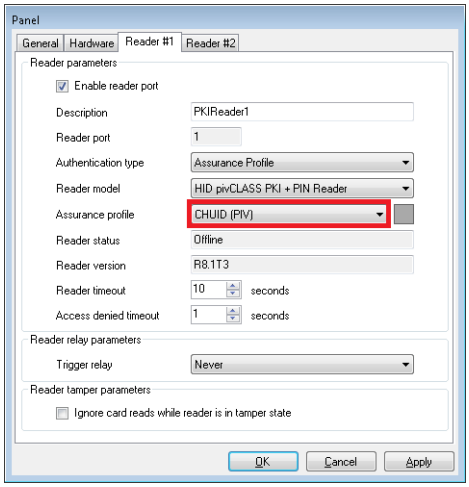
b. Add a Wiegand card format with **Extended ID** = 0 - 128. Name this card format. For example “Extended 128-bit”. Supports PIV-I cards.

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.
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. 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.



15. Connect and configure the Omnikey Card Scanner:
    a. Make sure the OMNIKEY 3121 Card Scanner is connected via USB to the test computer.
    b. Make sure the OMNIKEY 3121 Card Scanner has the latest driver. You can get the latest driver from the HID Global website. (The OMNIKEY CardMan 3121Scanner was used in this example.)
    c. Add the OMNIKEY 3121 Card Scanner to the computer and verify it is properly displayed in **Windows** > **Devices and Printers**.
    d. Configure the scanner in System Administration. From the **Administration** menu, select **Workstations**. Add the OMNIKEY 3121 Card Scanner as a "PC/SC Encoder".
16. 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.
17. 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.

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

a. On the **Hardware Settings** tab: Set the **Maximum badge number length** to 18 and **Maximum extended id length** to 32 bytes. Save the settings.

19. 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**.

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

a. Click [Add], then click [Import].

b. Select the OMNIKEY card scanner.

c. Enter `112233` for the password, and then click [Import].

d. In the dialog box, click [Enroll]. This will import the card information into System Administration. At the end of the process, a message is displayed confirming "Import is successful". Click [OK].

e. When asked if you want to keep the default activation dates, click [Yes], and then [OK]. The new cardholder will be added with their first and last name, extended ID, and deactivation date from the card.

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

22. 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.

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.

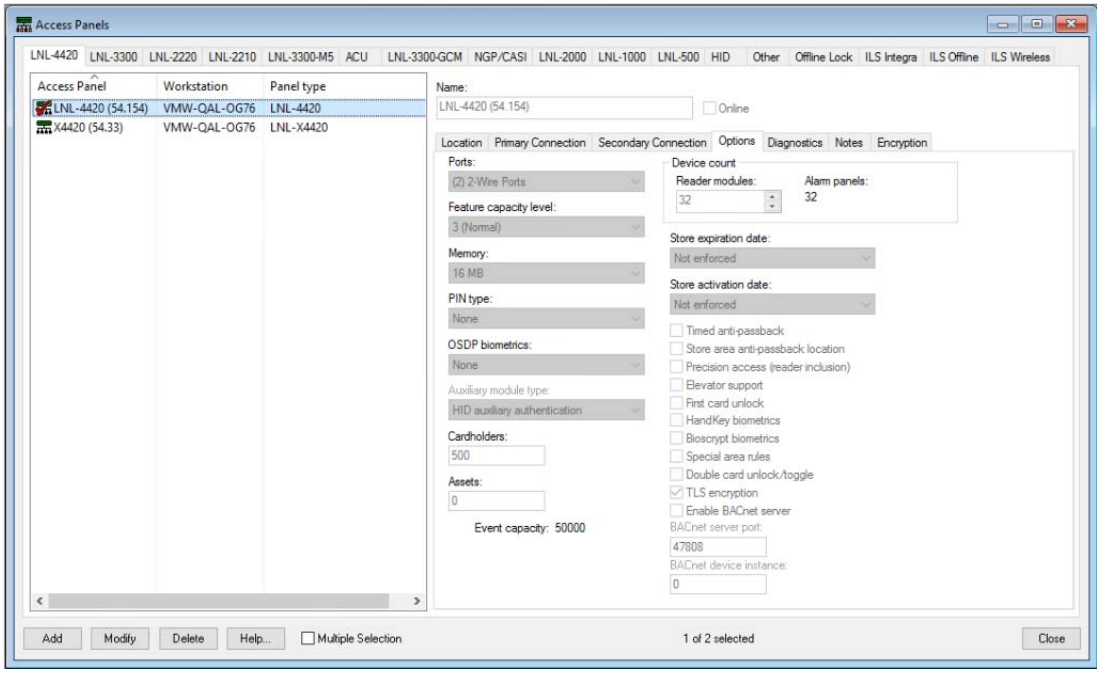
4. From the **Additional Hardware** menu, select **Logical Sources**.
   a. Add a logical source: In **Name**, enter "pivCLASS PACS Service" (exactly as it is spelled), select a **World time zone,** and then click [OK].
   b. On the **Logical Devices** tab, click [Add], enter "Certificate Manager" in **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 (LNL-4420/LNL-X4420)

1. From System Administration, configure an LNL-4420 (LNL-X4420) access panel and bring it online.
2. 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.

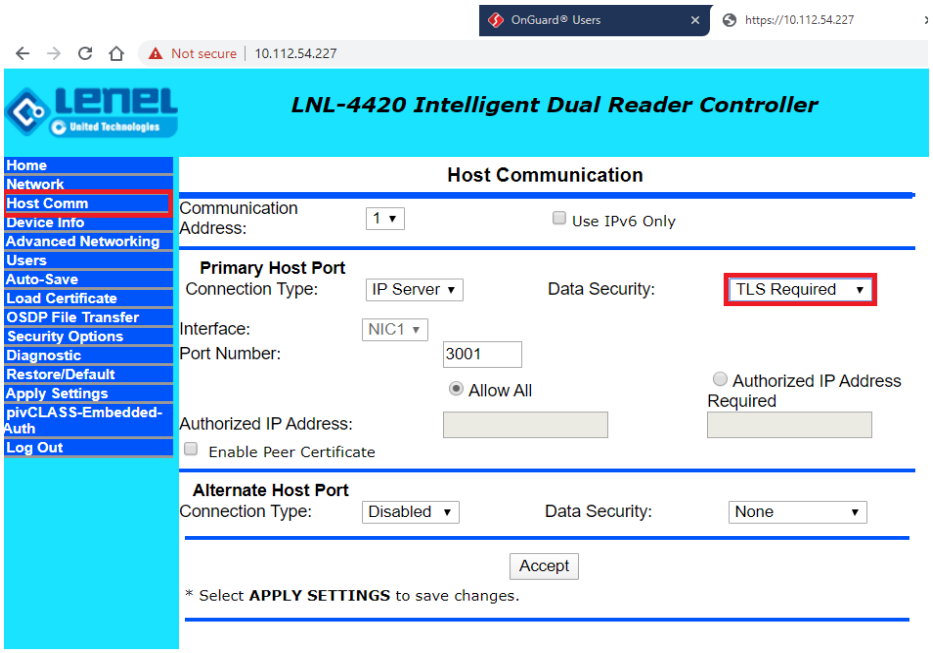
3. Enable panel-based authentication in System Administration:
   a. From the **Access Control** menu, select **Access Panels**, and then the **LNL-4420** tab.
   b. On the Location Tab, select the type of controller (LNL-4420 or LNL-X4420).
   c. On the **LNL-4420 Options** sub-tab, select "HID auxiliary authentication" as the **Auxiliary module type**, enable **TLS encryption**, and then click [OK].



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

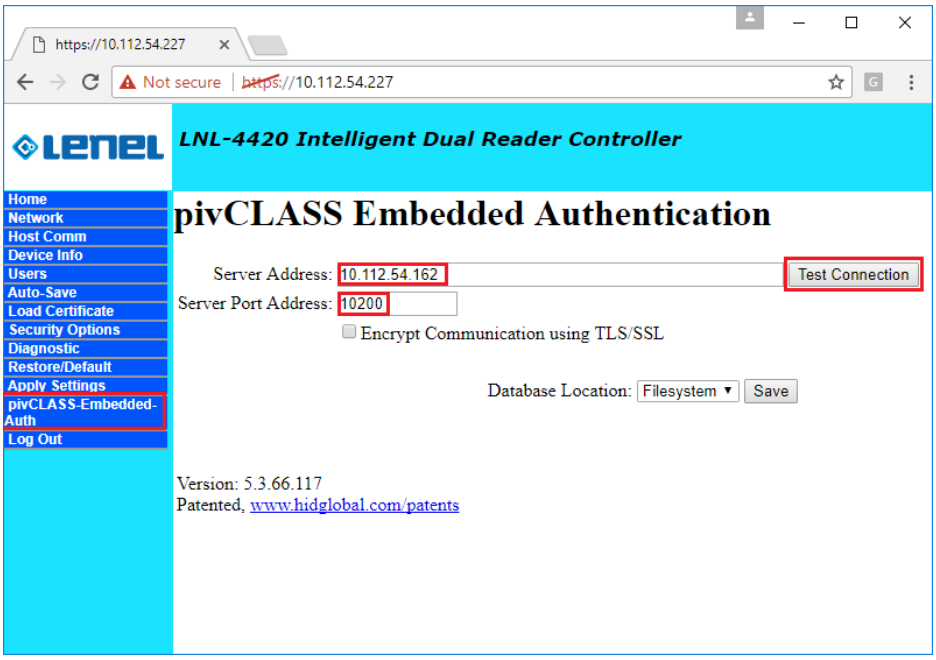
5. On the panel's web page, select the **Host Comm** page, and then select “TLS Required” from the **Data Security** drop-down.

Figure 3. Set Host Communication to TLS



6. Select the **pivCLASS Embedded Authentication** page.

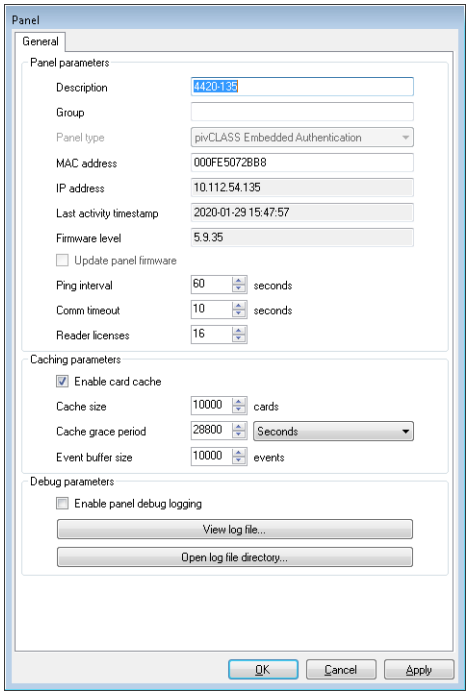
Figure 4. pivCLASS Embedded Authentication Settings



a. Configure **Server Address**: Enter the IP address of the computer where the PACS Service is running.

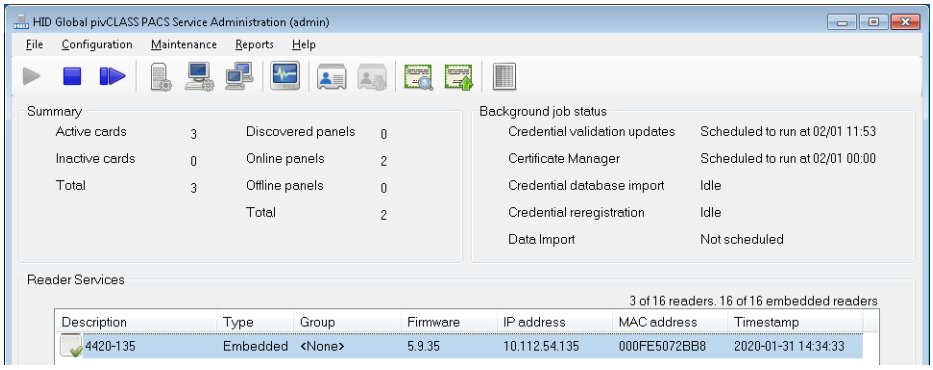
b. Click [Test Connection]. If a panel with a MAC address of this LNL-4420 is not added yet in the pivCLASS PACS Service > **Reader Services**, you will receive a message reporting the connection is successful, but the panel with that MAC address does not exist.

c. 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.



d. Now, in pivCLASS PACS Service > **Reader Services**, the correct IP address will be displayed for the LNL-4420/LNL-X4420.

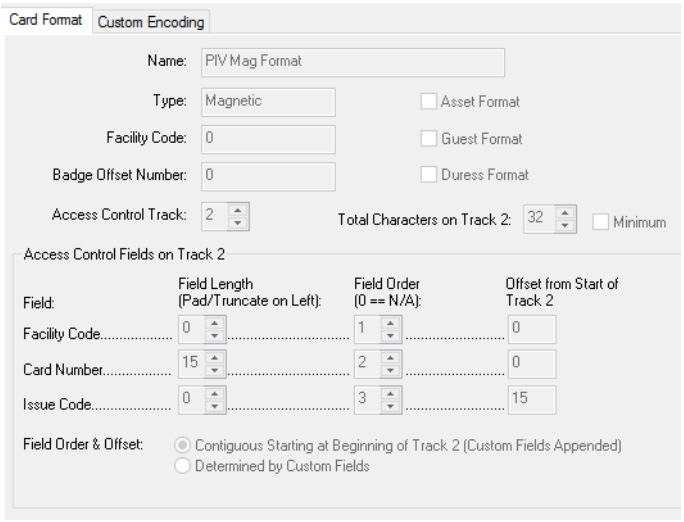
Figure 5. Correct IP Address Shown for LNL-4420



e. Back on the panel's web page, click [Test Connection] again. You should see this message: "Settings updated successfully".

7. Return to System Administration. From the **Access Control** menu, select **Readers and Doors**, and then add an Onboard reader to this LNL-4420/LNL-X4420 panel. Configure the Onboard reader as an **Authenticated reader** with the online and offline reader modes you require.
8. Add a Magnetic Card format for Embedded Authentication (LNL-4420/LNL-X4420) readers. **Total characters =** 32, **Card Number** = 15. Name it. For example, "PIV Mag Format".

Figure 6. PIV Mag Format for LNL-4420/LNL-4420 Embedded Authentication



9. Assign the "PIV Mag Format" card format to the reader.
10. Connect the HID pivCLASS reader to the reader port of the panel. The LCD screen should display "Present Card".