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<sup>®</sup> pivCLASS<sup>®</sup> 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 <a href="http://www.pivcheck.com/lenel">http://www.pivcheck.com/lenel</a> 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 <a href="https://www.pivcheck.com/lenel">Approved Product List</a> (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: <a href="https://partner.lenel.com/downloads/hardware/0/firmware">https://partner.lenel.com/downloads/hardware/0/firmware</a>.)
  - 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<sup>®</sup> 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 LSDataCondulT 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.)

🖏 Cardholder Options	
General Cardholder Options Badge ID Allocation Visits   Logical Access ID Allocation   ID Ranges	Cardholder Search Results Lists   Visitor Search Results Lists   Visit S∈ ◀   ▶
Generate Badge ID: Manual Entry	First Issue Code: 0 Auto-Increment Issue Code
FASC-N Settings Agency. Jono System Jono	Field to fill with Agency Code: Field to fill with System Code: Field to fill with Credential ID: Field to fill with Credential ID:
Modify	Help Close

- 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: <u>https://partner.lenel.com</u>.

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

HID Global pivCLASS PACS Service Administration (admin)		
<u>File Configuration Maintenance Reports</u> Help		
Credential database summary	Background job status	
Active cards 0	Certificate Manager Not Licensed	
Inactive (suspended) cards 0	Credential database import Idle	
Total cards 0	Credential reregistration Idle	
	Data Import Not Licensed	

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.

pivCLASS license				
System ID	PB3Y44U			Сору
pivCLASS license key	52E4M-KVTVN-CFEA5-9XFP	r		
Expiration date	Never Expires			
Licensed components	AuditTrail CertManager DataImport FIPS201SDK IDPublisher ReaderServices Registration Workstation			
Reader Services SDK license				
SDK license key	57HAF2NU2MAZQ	Licensed	16 / 16	
IDPublisher license				
IDPublisher license key	6FESJ8BCFVKKT	Licensed	1000	
IDPublisher license IDPublisher license key	6FESJ8BCFVKKT	Licensed	1000	

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.

Server Configuration		
Application Users PACS PACS (C	Cont.) Certificate Validation TWIC CCL Validation Certificate Manager Assurance Profiles Reader Services IDPublisher	
PACS Service parameters		
Server port number	10100	
PACS Service TLS parameters		
Encrypt communication	n using TLS	
TLS key	C:\Program Files (x86)\HID Global\pivCLASS PACS Service\keys\PACSService.pfx Browse	
TLS key password	Generate	
MultiPACS server parameters		
Enable MultiPACS conn	nection	
MultiPACS server address		
MultiPACS server port	10100 Test Connectin	vity
General validation parameters		
👿 Enable credential valida	ation when a credential is registered	
👿 Check for certificate, CF	RL, and TWIC CCL updates every 24 🚔 hour(s)	
Use FASC-N as card ide	lentifier for federally issued PIV-I credentials	
Credential database connection		
Connection type	Firebird	-
Store registered credent	ntial biometrics in the credential database.	
	Test Migrate	
	OK Cancel	Apply

- 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.

UserID	Name	Role	Fingerprints			
admin	Administrator	Administrator	No			
User ID				Sing	le Sign-On Enabled	
Name Userrole Password Verifypassword Notes	Operator Administrator				~	×

- 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.

ıg-in parameters		
CS	Lenel OnGuard	
nplate file	C:\Program Files (x86)\HID Global\pivCLASS PACS Service\templates\template.xml	Browse
perties		
Server		
Management path	\\ROCSERVERPC.galab.lenel.com\root\OnGuard	
Credentials		
Username	QALAB\Administrator	
Password	*****	
General		
Suspended badge :	status Lost	
Enable custom field	import False	
Custom field list (cor	mma-delimited)	
anagement path e WMI management	path for DataCondul T. Replace the '' with the remote hostname for remote connections. Required. E	Default:
	Cardenitas Server Management path Credenitas Usemane Password Enable custom field Custom field list (cor	An parameters Server  Server  Management path  UR0CSERVERPC.galab.lenel.com/voot/OnGuard  Credential  Usensme  QALABVAdministrator  Password  General  Evable custom field import  Custom field list (comma-delimited)   anagement path  word/OnGuard  Evable.custom field list (comma-delimited)   anagement path  word/OnGuard  Anagement path for DataCondulT. Replace the ',' with the remote hostname for remote connections. Required D  voot/OnGuard

- *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.

Server Conf	iguration	n		2							
Application	Users F	PACS	PACS (Cont.)	Certificate Validation	TWIC CCL Valid	ation Certifica	ate Manager	Assurance Prol	iles Reader S	ervices	DPublisher
-Data imp	ort paran	neters									
<b>V</b>	Import a	ccess	right definitions								
V	Import ci	redenti	al information a	and assignments							
<b>V</b>	Import P.	'ACS ci	redential status	3							
-Data Imp	oort sche	dule pa	arameters								
۲	Run eve	ery	30	Minutes	-						
0	Schedul	le autoi	matically								
0	User-def	fined tir	me 00:00	A V							
Events											
<b>v</b>	Send ca	ard valio	dation events								
<b>v</b>	Send ca	ard valio	dation failed ev	/ents							
<b>V</b>	Send rea	ader m	essage events								
	🔽 Sen	nd acce	ess granted me	essage events							
<b>V</b>	Send cre	edentia	al validation err	or events							
<b>v</b>	Send cre	edentia	al revoked eve	nts							
<b>V</b>	Send cre	edentia	al activated ev	ents							
						ſ	OK		Cancel		Apply

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

	oninguration											
Applica	ation Users PA	CS PACS (	Cont.) Cert	ificate Valida	ation TWIC C	CL Validation	Certificate	Manager As:	urance Profi	les Reader Se	rvices IDPub	lisher
Ger	neral parameters											
	📝 Enable cer	rtificate valid	ation									
	PKI model		CPV									•
	Certificate che	cking	Cher Cher Enfo Enfo	ck optional o ck signing c rce CHUID rce critical k rce key ID o	certificates ertificates expiration nes xeyUsage exte chaining	Ei S. Ing Insion	nforce name ave faulty ci	chaining ertificate path	\$			
- CPV	/ parameters											
	CPV timeout		60	🚖 secon	ds							
Cert	CPV options	and key usag	<ul> <li>✓ Allov</li> <li>✓ Igno</li> <li>✓ Igno</li> <li>✓ Igno</li> <li>✓ Igno</li> </ul>	v unknown I re CA revoc re CTL sign re CTL time re end revo	CA ation unknown er revocation u not valid cation unknow	n 📄 Inknown 📄	Ignore inva Ignore inva Ignore inva Ignore roo Ignore time	alid basic con alid name alid policy revocation u not nested	straints 📄	Ignore time no Ignore wrong	ot valid usage	
				<b>T</b>		o						
	OID	Usage	Agency	Type	PIV Aut	Lard Au	Key Ma	Digital S	Content			
	OID	Usage	Agency	1 ype	Add.		Key Ma Remove	Digital S	Content			
	OID	Usage	Agency	Type	PIV Aut		Remove	Digital S	Content	Cancel		λροίν

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

Server Configuration		
Application Users PACS PAC	CS (Cont.) Certificate Validation TWIC CCL Validation Certificate Manager Assu	rance Profiles Reader Services IDPublisher
General parameters		
Enable TWIC CCL	validation	
TWIC CCL	https://universalenroll.dhs.gov/ccl/CCL.CSV	Browse
TWIC CCL MD5	https://universalenroll.dhs.gov/ccl/CCL.CSV.MD5	Browse
	OK	Cancel Apply

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

Server Configuration	
Application Users PACS PACS (Cont.) Certificate Validation TWIC CCL Valid	ation Certificate Manager Assurance Profiles Reader Services IDPublisher
Certificate manager schedule	Certificate manager parameters
Run at a specific time	Update badge in PACS
00:00 12:00	Disable cards with unknown status after
04:00 16:00	72 🚔 hours
08:00 20:00	
User-defined time 12:00 🔿	
Schedule automatically	
Run after a specific interval has elapsed	
4 hours	
Certificate manager email alerts	
Send email when Certificate Manager updates card(s)	
SMTP server address	
Originating (From:) email address	
Email recipients (separated by commas)	
Candenail data	
Send email alerts Ounce per event Ounce per s	ession
	Test

- 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.

gureo	d assura	ance profiles					
ID		Visible	Security Level	Description			
0	2	Yes	Controlled	CAK (TWIC)			
0	3	Yes	Controlled	CHUID + BIO (TWIC)			
0	4	Yes	Limited	CHUID + CAK + BIO (TWIC)			
	5	Yes					
0	6	Yes	Limited	PKI + PIN (PIV)			
۲	7	Yes	Exclusion	PKI + PIN + BIO (PIV)			
	8	Yes	Controlled	CAK (PIV)			
	9	Yes	Controlled	CHUID + CAK (PIV)			
0	10	Yes	Limited	CAK + BIO (PIV)			
		Yes		Card ONLY (no PKI)			
0	12	Yes	Controlled	Card + PIN (no PKI)			
		Yes		Card + PACS PIN (no PKI)			
0	14	Yes	Limited	Card + PIN + BIO (no PKI)			
9	15	Yes	Controlled	Secure Messaging (PIV)			
	50	Yes	Controlled	Assurance Profile #1			
SP8	00-116	Security leve	el	Unrestricted			
Des	cription		Assurance Pr	ofile #2			
Assu	urance p	orofile ID	51				
Assı	irance p	orofile feature	ES Check TV Match fing Perform C Perform S PIN-to-PA V Require r SM > CAK	//C Canceled Card List     V Validate CAX certificate       kX authentication     V Validate CHUID signature certificate       vX authentication     V Validate PIV certificate       vauthentication     Validate PIV certificate       vauthentication     Validate PIV certificate       vauthentication     Validate SM signature certificate       S     Verify FIUID       gistration     Verify fingerprint template       v/C     Verify PIN			

- 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:

ver Configuration	PACS (Cont.) Certificate Validation   TWIC CCL Validation   Certificate Manager   Assurance Profiles   Reader Services   IDPublisher								
IDPublisher parameters	sheri Pot 9030								
IDPublisher TLS configu	ration								
Encrypt communication using TLS									
🔲 Require client	Require client TLS certificate for mutual authentication								
TLS key	TLS key C:\Program Files (x86)\HID Global\pivCLASS PACS Service\keys\PACSService.pfx Browse Generate								
TLS key password									
IDPublisher clients									
IP Address	Description								
-									
	Add Modify Remove								
	OK Cancel Apply								

- *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:

Server Configuration					
Application Users PACS	PACS (Cont.) Certificate Valida	tion TWIC CCL Validatio	on Certificate Manager A	ssurance Profiles Reade	r Services IDPublisher
Service parameters			Reader Services TLS pa	arameters	
🗵 Enable×ML	-RPC API P	ort 8989	📃 Enable TLS er	ncryption	
📃 Enable Binar	ry API P	ort 11000	📃 Enable TLS cli	ient mutual authentication	n
🗵 Enable PAM	5API P	ort 10200	TLS key	C:\Program Files (x86)	HID Global\pivCLAS
🔲 Always valid	ate credentials		TLS key password		
			Brow	wse filesystem for TLS ke	y file
				Generate TLS key file.	
- Beader Services clien	ts				
				3 / 16 Reader Se	rvices reader licenses
Description			IP Address	Assurance Profile	Passage
OnGuard on ro	cserverpc		10.112.9	Chuid (PIV)	No
			Add	Modify	Remove
			0	K Cance	el Apply

- 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.)

Description	Dec. and an another second	
Description	Unduard on tocserverpo	
IP address	10.112.90.170	
Assurance profile	CHUID (PIV)	<b></b>
FASC-N format	200-bit	•
UUID format	128-bit UUID	•
This SDK client can or	nly perform assurance profile ope	rations.
Reader Services pivCLASS pass	sage parameters ge to send Wiegand signal	
Reader Services pivCLASS pass	sage parameters ge to send Wiegand signal (127.0.0.1)	
Reader Services pivCLASS pass Use pivCLASS Passag Wiegand converter addres Wiegand converter port	sage parameters ge to send Wiegand signal [127.0.0.1 [10001]	Test
Reader Services pivCLASS pass Use pivCLASS Passag Wiegand converter addres Wiegand converter port Delay	sage parameters ge to send Wiegand signal 127.0.0.1 10001 1 seconds	Test
Reader Services pivCLASS pass Use pivCLASS Passag Wiegand converter addres Wiegand converter port Delay Encrypt Wiegand comv	sage parameters ge to send Wiegand signal 127.0.0.1 10001 1 seconds verter communication	Test
Reader Services pivCLASS pass Use pivCLASS Passeg Wiegand converter addres Wiegand converter port Delay Encrypt Wiegand conv Encrypt Wiegand conv Encryption key	sage parameters ge to send Wiegand signal 127.0.0.1 10001 1 seconds verter communication	Test

- 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.

Panel	
General Hardware Reader #1	Reader #2
Panel parameters	
Description	TestPAM
Group	
Panel type	pivCLASS Authentication Module 5.x 👻
MAC address	00D 0694336F9
IP address	10.112.54.23
Last activity timestamp	2020-01-29 15:48:32
Firmware level	5.11.38
Update panel firmware	
Ping interval	60 🔿 seconds
Comm timeout	10 🔿 seconds
Panel Wiegand parameters	
👿 Send Wiegand output	
🔲 Enable keypad passthr	ough
FASC-N output	200-bit 👻
UUID / GUID output	128-bit UUID 🔹
Keypad output	Standard (4-bit)
Caching parameters	
Enable card cache	
Cache size	10000 🔷 cards
Cache grace period	28800 ≑ Seconds 👻
Event buffer size	10000 🔷 events
Debug parameters	
🔽 Enable panel debug log	iging .
	View log file
	Open log file directory
	<u>Q</u> K <u>C</u> ancel Apply

- 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".

General Hardware Header #1 Reader parameters	Reader #2				
👿 Enable reader port					
Description	PKIReader1				
Reader port	1				
Authentication type	Assurance Profile				
Reader model	HID pivCLASS PKI + PIN Reader				
Assurance profile	CAK (PIV)				
Reader status	Online				
Reader version	R8.1T3				
Reader timeout	10 🔶 seconds				
Access denied timeout	1 🚔 seconds				
Reader relay parameters					
Trigger relay	Never				
Reader tamper parameters					
📄 Ignore card reads while	e reader is in tamper state				

- 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.)

Reader Services Client	
Reader Services client paramete	ers
Description	OnGuard on rocserverpc
IP address	10.112.90.170
Assurance profile	CHUID (PIV)
FASC-N format	200-bit 👻
UUID format	128-bit UUID 👻
This SDK client can or	nly perform assurance profile operations.
Reader Services pivCLASS pas	sage parameters
🔲 Use pivCLASS Passag	ge to send Wiegand signal
Wiegand converter addres	127.0.0.1
Wiegand converter port	10001 Test
Delay	1 seconds
Encrypt Wiegand com	verter communication
Encryption key	
Verify encryption key	
	<u>Q</u> K <u>C</u> ancel

- 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 Save 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.

Access Level 1	Norm	
Access Level 2:	None	
Access Level 2:	None	÷

- 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

vivCLASS Authentication Module Configur	ation	
	Networking	
	PACS Service	
	Trusted Certificates	
	Signing Certificate	
	Change Password	
	Logout	
	Reboot	

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

Networking		
MAC Address:	00D0694336F9	
Configure Network:	using DHCP	~
	using DHCP	
	using STATIC IP	

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.

Networking	
PACS Service	
Trusted Certificates	
Signing Certificate	
Change Password	
Logout	
Reboot	

8. Click [PACS Service].

DICC Constan	
PACS Service	
NOTE: This version of th To use discovery, turn of on your local network. Se	e PAM supports automatic discovery. f DIP switch 1 and the PAM will be found by any PACS Service e the PAM Install Guide for details.
Server Address:	10.112.54.47
PAM 5.x Communication Port Number:	10200
	Save Cancel

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**.

븶 HID	Global pivCLASS	PACS Service A	dministration (	admin)						
<u>F</u> ile	<u>C</u> onfiguration	<u>M</u> aintenance	<u>R</u> eports <u>H</u>	<u>H</u> elp						
					*					
Sum	imary						Background job statu	s		
	Active cards	3	Discove	red panels	0		Credential valida	ation updates	Scheduled to run	at 02/01 11:53
	Inactive cards	0	0 Online panels 3 Offline panels		2		Certificate Manager Credential database import		Scheduled to run at 02/01 00:00 Idle	
	Total	3			0					
			Total			Credential reregistration		Idle		
					Data Import		Not scheduled			
Rea	der Services									
								3 of 16 read	lers. 16 of 16 embe	dded readers
	Description		Туре	Group		Firmware	IP address	MAC addres:	s Timestamp	
	TestPAM		PAM 5	<none></none>		5.11.38	10.112.54.23	00D0694336F	F9 2020-01-31 1	14:34:43

## 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

0	
Card Format Custom Encoding	
Name:	Extended 200 bit
Туре:	Wiegand Asset Format
Facility Code:	0 Reversed Bit Urder Duress Format
Badge Offset Number:	0
Total Number of Bits On Card:	200 🜲
	Starting Bit: Number of Bits:
Facility Code:	
Card Number:	
Extended ID:	
Issue Code:	
ADA:	0 🔹 0 🔹
Activate Date:	0 • •
Deactivate Date:	0
Authorization:	0 -
Number of Even Parity Bits:	0 🗘 Special:
Number of Odd Parity Bits:	0 None V

 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.

Card Format Custom Encoding	
Name:	Extended 128 bit
Туре:	Wiegand Asset Format
Facility Code:	0 Reversed Bit Order Duress Format
Badge Offset Number:	0
Total Number of Bits On Card:	128 🜲
	Starting Bit: Number of Bits:
Facility Code:	
Card Number:	
Extended ID:	0 🔹 128 🔹
Issue Code: II S-Specific Fields	
ADA:	0 * 0 *
Activate Date:	0 🗼 0 🛓
Deactivate Date:	0 +
Authorization:	
Number of Even Parity Bits:	0 🐥 Special:
Number of Odd Parity Bits:	0 A

#### 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.

Panel			
General Hardware Reader #1	Reader #2		
Reader parameters			
🔽 Enable reader port			
Description	PKIReader1		
Reader port	1		
Authentication type	Assurance Profile		
Reader model	HID pivCLASS PKI + PIN Reader		
Assurance profile	CHUID (PIV)		
Reader status	Offline		
Reader version	R8.1T3		
Reader timeout	10 🔄 seconds		
Access denied timeout	1 seconds		
Reader relay parameters			
Trigger relay	Never		
Reader tamper parameters			
Ignore card reads while	e reader is in tamper state		
	<u>D</u> K <u>C</u> ancel Apply		

- 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.

ICAM Card 46 Golden FIPS 201-2 PIV 4700	PIV
4700	
	$\wedge$
123456789	GSA
ICAM Test Cards	APL Program IEAN CARES
4700-0257-000046-1-1-0257000046-1-99999-1	
94e28c58-84db-44db-8a0e-f502d5589b14	Expiration Date: 12/02/203
View Signer's Certificate	
View Certificate	
View Certificate	
Natch not performed	
Validation succeeded	
	12346789 ICA41 Test Cards 4700 0257 000046-1-0257000046-1-9999-1 94e20c58-84b-44b-8a0e-f50265689614 Vew Signer's Certificate Vew Certificate Vew Certificate Wew Certificate Wew Certificate

- 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, copyLNLAUXMOD\_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 type** and enable **TLS encryption**.

IL-4420 LNL-3300 L	NL-2220 LNL-2210	LNL-3300-M5 ACU LNL-330	D-GCM NGP/CASI LNL-2000 LNL-1000 L	NL-500 HID Other Offline Lock ILS Integra I	LS Offline ILS Wireless
Access Panel	Workstation	Panel type	Name:		
LNL-4420 (54.154)	VMW-QAL-OG76	LNL-4420	LNL-4420 (54.154)	Online	
mttru-≪420 (54.33)	VMW-QAL-OG76	LNL-X4420	Location Primary Connection Secondary Co Pots: (2) 2:Wer Ports Feature capacity level: 3 (Normal) Memory: 16 MB PIN type: None OSDP biometrica: None OSDP biometrica: None Cardholders: 500 Assets: 0 Event capacity: 50000	Unime	
		>			

- 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].

Home		Host Co	mmunication	
Host Comm Device Info	Communication Address:	0 ~	Use IPv6 O	nly
Advanced Networking Users Auto-Save	Primary Host Port Connection Type:	IP Server $\vee$	Data Security:	TLS Required 🗸
Load Certificate OSDP File Transfer Security Options Diagnostic Restore/Default Apply Settings Log Out	Interface: Port Number: Authorized IP Address:	NIC1 > 3001 © Allow All		O Authorized IP Address Required
	Alternate Host Port Connection Type:	Disabled V	Data Security:	None ~
	Connection Type: * Select APPLY SETTI	Disabled V	Data Security: Accept	None

#### 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].

LENEL:S2	LNL-X4420	Intelligent Dual Read	ler Controller
ome etwork ost Comm	pivCLASS Embed	ded Authentica	tion
dvanced Networking	Server Address: 192.0.2.10		Save and Test Connection Settings
ers to-Save ad Certificate DDP File Transfer curity Options agnostic store/Default nNV Settings rCLASS-Embedded- th	Server Port Address: 10200	Database Location: Filesystem Discovery: Enabled	Save Save
g Out	Version: 5.13.15.148 Patented, <u>www.hidglobal.com/patents</u>		

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.

Panel	
General	
Panel parameters	
Description	4420-135
Group	
Panel type	pivCLASS Embedded Authentication
MAC address	000FE5072BB8
IP address	10.112.54.135
Last activity timestamp	2020-01-29 15:47:57
Firmware level	5.9.35
Update panel firmware	3
Ping interval	60 🚔 seconds
Comm timeout	10 🚔 seconds
Reader licenses	16
Caching parameters	
🗹 Enable card cache	
Cache size	10000 🚔 cards
Cache grace period	28800 🜩 Seconds 👻
Event buffer size	10000 < events
Debug parameters	
🔲 Enable panel debug lo	ogging
	View log file
	Open log file directory
	UK Lancel Apply

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.

Canada					
Benefal					
Panel paramete	a	[accession]			
Descriptio	n	DOOFE	9070	DC3	
Group					
Panel typ		prvCLASS Embedded Authentication			
MAC add	000	000FE507DDC3			
IP addres		192.168.133.250			
Last activ	ty timestamp	2019-08-29 09:09:49			
Firmware	evel	5.9.35	5		
🗌 Upda	te panel firmwar	0			
Pinginter	val	60	¢	seconds	
Comm tim	eout	10	*	seconds	
Reader lic	enses	2	٥		
Caching param	eters				
Cache siz	e	10000		cards	
Cache tirr	e-to-live	28800	4	Seconds ~	
Cache gr	ce period	28800	•	Seconds v	
Event but	fer size	10000	•	events	
Debug paramet	ers				
🗌 Enabl	e panel debug l	ogging			
		View	logf	ie	
		Open log t	file d	irectory	
-				G. (884)	

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

ummary Active cards Inactive cards Total	3 0 3	Discove Online p Offline p Total	red panels anels anels	0 2 0 2	Background job statu Credential valide Certificate Mana Credential datab Credential rereg	s ation updates ger ase import istration	Scheduled to run at 02/0 Scheduled to run at 02/0 Idle Idle	1 11:53 1 00:00
eader Services					Data Import	3 of 16 read	Notscheduled	eaders

- 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.
- Add a Magnetic card format for the Embedded Authentication (LNL-4420/LNL-X4420) readers. 6. 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.

Card Earnat	0 · F	l.		
Card Format	Custom Enco	ding		
	Nam	e: PIV Mag Format		
	Тур	e: Magnetic	Asset Fo	ormat
	Facility Code	e: 0	Guest F	ormat
Badge	Offset Numbe	r: 0	Duress F	Format
Acces	s Control Tracl	k: 2 🔺	Total Characters on Tracl	k 2: 32 🔺 Minimum
Access Co	ntrol Fields on	Track 2		
Field:		Field Length (Pad/Truncate on Left):	Field Order (0 == N/A):	Offset from Start of Track 2
Facility Cod	le	0 🛓		0
Card Numb	er	15 💂	2 🔺	0
Issue Code		0	3 🚔	15

#### 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: <u>https://partner.lenel.com/downloads/</u> <u>hardware/0/firmware</u>.)
  - 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<sup>®</sup> 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 LSDataCondulT 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.)

騸 Cardholder Options	
Seneral Cardholder Options         General Cardholder Options         ID Allocation       ID Ranges         ID Allocation       ID Ranges         Generate Badge ID       Manual Entry         FASCN Settings         Agency:         00000         System:	Cardholder Search Results Lists   Visitor Search Results   Visitor Search Results   Visitor S
Modily	Field to fill with Credential ID:

#### **Compatibility Charts**

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

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:

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

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.

Home	Host Communication			
Network		Host Co	minumcation	
Host Comm Device Info	Communication	0 ~	Use IPv6 Or	nly
Advanced Networking	Address.	Terrane and the second s		11.2 · · · ·
Users	Primary Host Port			
Auto-Save	Connection Type:	IP Server ∨	Data Security:	TLS Required V
Load Certificate				
OSDP File Transfer	Interface:	NIC1 V		
Security Options	Port Number:	3001		
Diagnostic				Authorized ID Address
Restore/Default		Allow All		Dequired
Apply Settings	And In stand ID Address			Required
Log Out	Authorized IP Address:			11 A A A A A A A A A A A A A A A A A A
	Enable Peer Certific	ate		
	Alternate Host Port			
	Connection Type:	Disabled V	Data Security	None V
	e ettile etter type:		e and e e e e anny :	
		L	Accent	
	And a second sec		Accept	
	* Select APPLY SETTI	NGS to save changes.		

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<br/>LNLAUXMOD\_ENTRYPOINT\_REMOVE\_AAM.bin to the<br/>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].

🚟 Access Panels	
NGP/CASI LNL-4420 LNL-3300 LNL-3300-M5 ACU LNL-3300-GC	M LNL-2220 LNL-2210 LNL-2000 LNL-1000 LNL-500 HID Other Offline Lock ILS Integra ILS Offline ILS 🔹
Access Panel Workstation	Name:         LNL 4420 with EntryPoint         Location       Options         Ports:       Device court         Parts:       Device court         32       32         3 (Nomai)       Store expiration date:         Nemory:       Not enforced         16 M8       Store expiration date:         None       Not enforced         None       Precision access (reader inclusion)         Auxiliary module type:       First card unlock:         EntryPfoint       Precision access (reader inclusion)         Auxiliary authentication       Bioexcrypt biometrics         Double card unlock:       Precision access (reader inclusion)         Auxiliary authentication       Bioexcrypt biometrics         EntryPfoint       TLS encryption         Assets:       Double card unlock-/toggle         Wend respectly: 1000       BACnet server         BACnet server       BACnet server         BACnet device instance:       0
OK Cancel Clear Help	Add Mode Close

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.

orking Server Configuration Server URL:
orking Server Configuration Server URL:
Server URL: http://MuSopuer/barcupped
(https://resourceorhostname)
Username: hars
ofer O Change password   O Change password
Password:
Configs Deserved
edded
Number of Listening Threads: 5 V
Diagnostic Logging
Enable diagnostic logging to system log
Advanced diagnostics enabled
Save Configuration
Cave comgatation
Test Configuration
Test Server Configuration
Test License
HARS Configuration
Please specify a bars ini file (*.ini)
Browse
Diowse
Load hars.ini
Optional Revert back to the previous hars.ini file.
Revert hars.ini
Download Current HARS ini file.
Download Hars.ini
License Information
License monitation
Please specify a license file (ti.lic.signed)
Browse
Load License
License is not installed.
Certificate Information
Please specify a certificate file (*.pem)
Browse
The Particle
Load Certificate
Contificate is not installed

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".

i igui e ii liata	indea ib accorticata format
Card Format Custom Encoding	
Name:	Extended 200 bit
Туре:	Wiegand Asset Format
Facility Code:	0 Reversed Bit Order Duress Format
Badge Offset Number:	0
Total Number of Bits On Card:	200 🔦
	Starting Bit: Number of Bits:
Facility Code:	0 -
Card Number:	0
Extended ID:	0 🔹
Issue Code:	
ADA:	0 -
Activate Date:	0 -
Deactivate Date:	0
Authorization:	0 🔹 0 🔹
Number of Even Parity Bits:	0 - Special:
Number of Odd Parity Bits:	0 🗘 None 🗸

#### 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. Exte	ended ID 1	28-bit card format	
Card Format	Custom Encoding			
	Name:	Extended 128 bit		
	Туре:	Wiegand	Asset Format	
	Facility Code:	0	Reversed Bit Order Duress Format	
В	adge Offset Number:	0		
Total Nu	mber of Bits On Card:	128 🔹		
		Starting Bit:	Number of Bits:	
	Facility Code:	0	0 🔹	
	Card Number:	0	0 🛓	
	Extended ID:	0 +	128 🔹	
- ILS-Specific	Issue Code: Fields	0 -	0 🐥	
	ADA:	0	0 *	
	Activate Date:	0 🔹	0 🚔	
	Deactivate Date:	0 🔹	0	
	Authorization:	0	0	
Numb	er of Even Parity Bits:	0	Special:	
Num	ber of Odd Parity Bits:	0	None	

- 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".

ard Format	Custom Encodir	ng		
	Name:	PIV Mag Format		
	Туре:	Magnetic	As	set Format
	Facility Code:	0	🗌 Gu	uest Format
Badge	Offset Number:	0	Du	iress Format
Acces	s Control Track:	2	Total Characters on	Track 2: 32 🚔 🗌 Minimur
Access Co	ntrol Fields on Tr	ack 2		
Field:	Fie (P	eld Length ad/Truncate on Left):	Field Order (0 == N/A):	Offset from Start of Track 2
Facility Cod	le 0	* *	1 🛓	0
Card Numb	er 1!	5 🚔	2 🌩	0
Issue Code	0	* *	3 🔺	15
Field Order	& Offset: 💿	Contiguous Starting at	Beginning of Track 2	2 (Custom Fields Appended)
		Determined by Custom	Fields	

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.

<b>Entry</b> Point	
Enter Details	
First Name:	Card
Middle Name:	
Last Name:	ICAM
PACS PIN:	
Add Photo	
	Cancel OK

#### **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: <u>https://partner.lenel.com/downloads/</u> <u>hardware/0/firmware</u>.)
  - 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.)

General Cardholder Uptions Badge ID Allocation   Visits   Logical Access	Eardholder Search Hesults Lists   Visitor Search Hesults Lists   Visit Se
Generate Badge ID: Manual Entry	First Issue Code:
- FASC-N Settings Agency: 0000 System: 0000	Field to fill with Agency Code:

#### **Compatibility Charts**

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

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.

łome Network	Host Communication			
lost Comm Device Info	Communication Address:	0 ~	Use IPv6 Or	nly
Advanced Networking Jsers Auto-Save	Primary Host Port Connection Type:	IP Server $\vee$	Data Security:	TLS Required V
oad Certificate SDP File Transfer	Interface:	NIC1 V		
Diagnostic Restore/Default	Port Number.	Allow All		O Authorized IP Address
Apply Settings .og Out	Authorized IP Address:			required
	Alternate Host Port Connection Type:	Disabled V	Data Security:	None ~
			Accept	
	* Select APPLY SETTI	NGS to save changes.		

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<br/>LNLAUXMOD\_VALIDATIONAGENT\_REMOVE\_AAM.bin to the<br/>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].

KA_panel       1-094F8A2151A4       ALPHA_REGIO         R_panel       I-094F8A2151A4       BETHA_REGIO         I-094F8A2151A4       BETHA_REGIO         C_panel       I-094F8A2151A4         I-094F8A2151A4       THETA_REGIO         Decision       Decision         C_panel       I-094F8A2151A4         THETA_REGIO       Decision         Decision       Decision         Decision       Decision         Decision       Decision         Decision       Decision         BitMomory:       Date only         T6 MB       Store area artipastback location         None       Distore area artipastback location         OSDP biometrics:       Decision course (seder inclusion)         Autiany module type:       Decision course (seder inclusion)         Autiany module type:       Decision course (seder inclusion)	ccess Panel	Workstation	Segment	Name:		
B panel       I-094F8A2161A4       BETHA.REGIOI       Location       Primary Connection       Secondary Connection       Options       Dagnostics       Web Page Users       Notes         Ports:	A_panel	I-094F8A2161A4	ALPHA_REGIO	A_panel	☑ Qnline	
Bender modules:       Aum panels:         22 Wire Ports       32         Beader modules:       32         3 (Nomal)       Store egpiration date:         Memory:       Date only         16 MB       V         PIN type:       Date only         Nome       Imed antipasaback (coation)         Nore       Imed antipasaback (coation)         Auxiliary module type:       Imed and unlock         Nore       Imed antipasaback (coation)         Imed antipasaback       Imed antipasaback (coa	B_panel	I-094F8A2161A4 I-094F8A2161A4	BETHA_REGION	Location Primary Connection Secondary C	connection Options Diagnostics Web Page Users Notes	
3 (Normal)       Store expiration date:         Memory:       Date only         16 MB       Store expiration date:         P]N type:       Store actigation date:         None       Imed anti-passback         OSDP biometrics:       Imed anti-passback         None       Imed anti-passback         Store are anti-passback       Imed anti-passback         Imed anti-passback       Imed anti-passback         None       Imed anti-passback         Imed anti-passback       Imed anti-passback         Imed				Ports: (2) 2-Wire Ports Feature capacity level:	Device count           Reader modules:         Alam panels:           32         32	
Memory:     Date only       16 MB     Store activation date:       P[N type:     Not enforce       None     Imed anti-pasaback       OSDP biometrics:     Imed anti-pasaback       None     Presign access (reader inclusion)       Audiary module type:     Bervator support.       None     Imat cand unlock				3 (Normal)	Store expiration date:	
16 MB     Store actlyzion date:       P[N type:     Not enforced       None     Imed anti-passback       QSDP biometrics:     Store actlyzion access (reader inclusion)       None     Precision access (reader inclusion)       Auxilary module type:     First card unlock				Memory:	Date only ~	
PIN type:     Note enforced       None     Imed anti-passback       QSDP biometrics:     Store area anti-passback (ocation Rone       None     Precision access (reader inclusion)       Auxiliary module type:     Elevator support       None     First card unlock				16 MB ~	Store activation date:	
None				PIN type:	Not enforced ~	
QSDP biometrics:     Intere arrepassuak       None     Precision access (reader inclusion)       Auxiliary module type:     Precision support       None     Precision access (reader inclusion)				None ~		
None     Precision access (reader inclusion)       Auxiliary module type:     Bevator support       None     First card unlock				QSDP biometrics:	Store area anti-passback location	
Auxiliary module type: None First card unlock				None ~	Precision access (reader inclusion)	
None First card unlock				Auxiliary module type:	Eevator support	
				None ~	First card unlock	
				Auxiliary module type:	Evator support     First card unlock	

- 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.

Readers and Doors							-	
Reader Reader Reader_1_based_on_ACCESS_PANEL_2 Reader_A Control of the section of the sect	Access Panel A ACCESS_PANEL_2 A ACCESS_PANEL_1 A A_panel G G_panel G	Reader Type LNL-1320 (Dual Interface) LNL-1300 (Single Interface) Onboard Reader Onboard Reader Onboard Peader	Reader Output Magnetic Miegand / Prox Wiegand / Prox Wiegand / Prox	Port 2 Port 2 Port 1 Onboard Onboard	Address 0 0 0 0 0 0	Reader Number 0 0 0 0 0	OSDP Address	Segment ^ Default 5 Default 5 ALPHA_1 BETHA_f THETA_F
General Grouping Settings Controls Aux & Name: reader_A Panel: A_panel Type: Onboard Reader Output: OSDP Protocol Port: Onboard Gateway Address:	Aux Outputs And Aux Outputs And Address: 0 IP Pont: 0 Reader number: 0	ti-Passback Command Progra Held Open Time: Extended Open: Strike Time: Extended Strike: OSDP Baud rate: A	Mobile         N           75         Card           75         Set           3         Set           5         Set           0         -	Format agnetic Forn fiegand (64) fiegand (72) fiegand Forn	Type mat Mag Wieg Wieg nat Wieg	netic Jand Jand Jand		
Alternate Reader      Primary Reader: Reader Modes      Online: PKI + PIN + RingerPrint E ♥      CAK      Offline: PKI + PIN     PKI + PIN     CAK      Offline: Offline: PKI + PIN     Offline: PKI + P	Lock ID: 00000 Biometric Verify (Cpher First Card Unlock  Authenticated reader	Cut off on Close     Cut off on Close     Do Not Activate Strike of     Keypad:     Allow User Commands     Allow Intrusion Comman	Encryp on REX Ele Paired ds	ted Communi vator Reader: lodify Mode	cations Mod	e: ack Floors	<u>S</u> earch	Close

- 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. Exte	ended ID 20	0-bit card format
Card Format Custom Encoding		
Name:	Extended 200 bit	
Туре:	Wiegand	Asset Format
Facility Code:	0	Reversed Bit Order
Badge Offset Number:	0	Durossi omut
Total Number of Bits On Card:	200 💂	
	Starting Bit:	Number of Bits:
Facility Code:	0	0
Card Number:	0	0
Extended ID:	0	200 🔹
Issue Code:	0	0
LS-Specific Fields ADA:	0	0
Activate Date:	0 ‡	0
Deactivate Date:	0 📫	0
Authorization:	0 -	0
Number of Even Parity Bits:	0	Special:
Number of Odd Parity Bits:	0	None 🗸

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

Card Format Custom Encoding	
Name:	Extended 128 bit
Туре:	Wiegand Asset Format
Facility Code:	0 Reversed Bit Order
Badge Offset Number:	0
Total Number of Bits On Card:	128 🔹
	Starting Bit: Number of Bits:
Facility Code:	
Card Number:	0 0 .
Extended ID:	0 + 128 +
Issue Code:	0
ILS-Specific Fields	
ADA:	
Activate Date:	0 🔹 0 🔹
Deactivate Date:	0 * 0 *
Authorization:	
Number of Even Parity Bits:	0 🗘 Special:
Number of Odd Parity Bits:	0 🔹 None 🗸

#### 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".

	Name:	PIV Mag Format		
	Туре:	Magnetic	Ass	set Format
Fa	acility Code:	0	🗌 Gu	est Format
Badge Offs	et Number:	0	🗌 Du	ress Format
Access Co	ntrol Track:	2	Total Characters on	Track 2: 32 🌲 Minimur
Access Control	Fields on Tra	ack 2		
- Access Control Field:	Fields on Tra Fie (Pa	ack 2 Id Length ad/Truncate on Left):	Field Order (0 == N/A):	Offset from Start of Track 2
- Access Control Field: Facility Code	Fields on Tra Fie (Pa	ack 2 Id Length ad/Truncate on Left):	Field Order (0 == N/A): 1	Offset from Start of Track 2
Access Control Field: Facility Code Card Number	Fields on Tra Fie (Pa 0 15	ack 2 Id Length ad/Truncate on Left):	Field Order (0 == N/A): 1 + 2 +	Offset from Start of Track 2
Access Control Field: Facility Code Card Number Issue Code	Fields on Tra Fie (Pa 0 15 0	ack 2 Id Length d/Truncate on Left): 	Field Order (0 == N/A): 	0 Iffset from Start of Track 2 

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.