

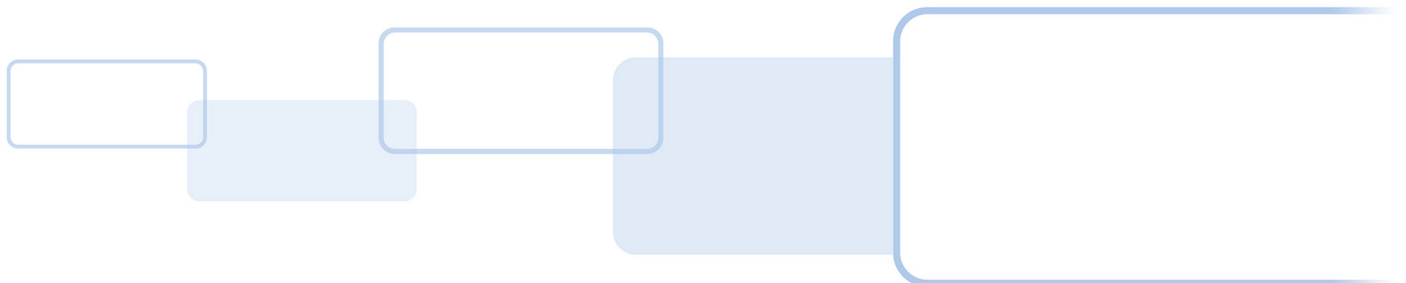
PIVCLASS[®] AUTHENTICATION MODULE

MODEL M2000

INSTALLATION AND CONFIGURATION GUIDE

PLT-01628, Rev. D.5

March 2020



Copyright

© 2014 - 2020 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID Brick logo, the Chain Design, pivCLASS, Seos, and iCLASS are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

MIFARE and DESFire are registered trademarks of NXP Semiconductors N.V. and are used under license.

Revision history

Date	Description	Revision
March 2020	Updates implemented: ■ <i>Section 6.3.3 Troubleshoot communication issues</i>. Note added regarding recommendations for enabling debug messaging.	D.5

Contacts

For additional offices around the world, see www.hidglobal.com/contact/corporate-offices

Americas and Corporate

611 Center Ridge Drive
Austin, TX 78753
USA
Phone: 866 607 7339
Fax: 949 732 2120

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong
Phone: 852 3160 9833
Fax: 852 3160 4809

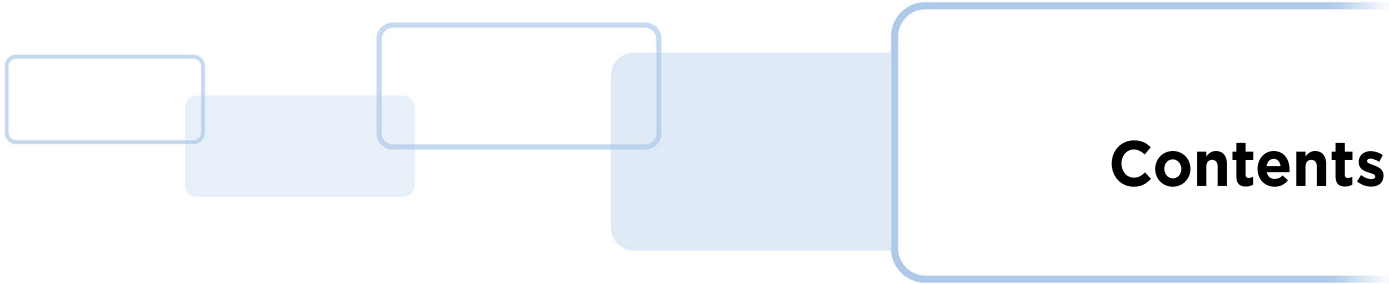
Europe, Middle East and Africa (EMEA)

Haverhill Business Park Phoenix Road
Haverhill, Suffolk CB9 7AE
United Kingdom
Phone: 44 (0) 1440 711 822
Fax: 44 (0) 1440 714 840

Brazil

Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP
Brazil
Phone: +55 11 5514-7100

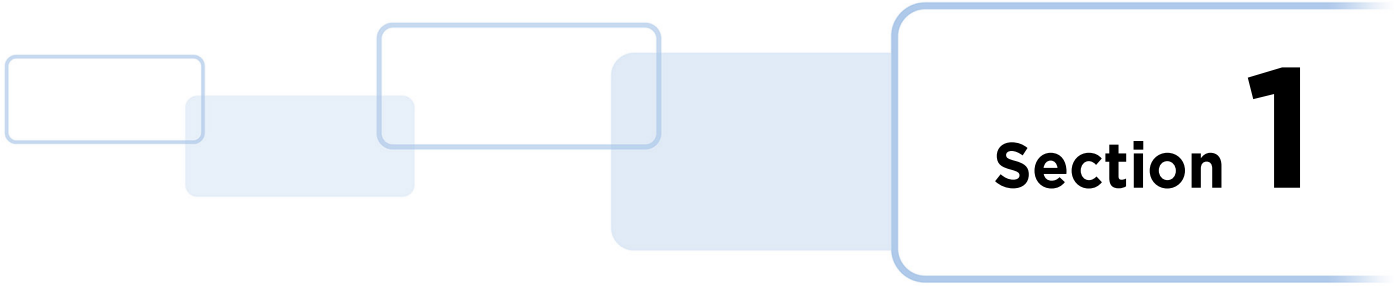
HID Global Technical Support: www.hidglobal.com/support



Contents

Section 1: Introduction	5
1.1 Product overview	5
1.2 Scope of document	5
1.3 Assumed knowledge	5
1.4 Prerequisites	6
1.5 Glossary	6
Section 2: Specifications	7
2.1 Technical specifications	7
2.2 Cable specifications	7
Section 3: Module description	9
3.1 Physical features	9
3.2 Security features	11
3.3 Card Passthrough	11
3.3.1 PAM operation without Card Passthrough	11
3.3.2 PAM operation with Card Passthrough	12
Section 4: Installing the module	13
4.1 Checking the package contents	13
4.2 Installation preparation	13
4.2.1 Creating a SD card image	14
4.3 Enclosure installation	15
4.3.1 PAM mounting dimensions	15
4.4 Making jumper connections	16
4.5 Wiring connections	17
4.5.1 Connecting PAM to supported reader port	17
4.5.2 Connecting PAM to PACS panel reader port	17
4.6 Connecting to the network	18
4.7 Connecting to the power supply	18
4.8 Applying power	19
4.9 Disabling power	19
Section 5: PAM configuration	21
5.1 Overview	21

- 5.2 PAM DIP switches 21
- 5.3 PAM Configuration application overview 22
- 5.4 Manual PAM configuration 23
 - 5.4.1 Panel API communication options 23
 - 5.4.2 Configure the PAM to communicate with the PACS Service 24
 - 5.4.3 Configure PAM in Reader Services 27
- 5.5 Automatic PAM configuration 32
 - 5.5.1 Panel API communication options 32
 - 5.5.2 Add automatically discovered PAM 33
- Section 6: Troubleshooting 35**
 - 6.1 LED activity 35
 - 6.2 Resetting to factory defaults 36
 - 6.3 Troubleshooting configuration problems 37
 - 6.3.1 Troubleshoot pivCLASS Reader Services communication 37
 - 6.3.2 Wiegand output problems 37
 - 6.3.3 Troubleshoot communication issues 37
 - 6.4 Swapping a PAM. 38
- Section 7: Regulatory 39**



Section 1

1 Introduction

1.1 Product overview

The HID Global pivCLASS® Authentication Module (PAM) allows organizations to upgrade existing Physical Access Control Systems (PACS) to full HSPD-12 compliance with all of the functionality defined in FIPS 201-2, FICAM FRTC 1.3.3, and associated publications.

HSPD-12 compliance supports verification of the following card types:

- Personal Identity Verification (PIV) card.
- Personal Identity Verification-Interoperable (PIV-I) card.
- Commercial Identity Verification (CIV) card (also known as PIV-C).
- Common Access Card (CAC). Standard identification card for United States Defense personnel.
- First Responder Authentication Credential (FRAC) card.
- Transportation Worker Identification Credential (TWIC) card.

PAM validates the credentials at the time of access. This validation confirms the card is not counterfeited, cloned, copied, lost or stolen. FIPS 201-2 and NIST SP 800-116-1 define specific authentication mechanisms and their application to authenticate PKI based credentials for access to uncontrolled, controlled, limited, and exclusion areas.

The PAM is installed between a PACS panel and a supported smart card reader. The PAM validates smart cards at the assurance level set in the pivCLASS Reader Services or by the API. If the card is valid, the PAM sends the card's derived badge ID to the PACS.

1.2 Scope of document

This document provides information on the installation and configuration of the HID Global pivCLASS Authentication Module (PAM).

1.3 Assumed knowledge

This document is aimed at experienced installers with knowledge of Physical Access Control Systems (PACS).

1.4 Prerequisites

The following prerequisites are required:

1. Install hardware components, including the following:
 - PACS panels (if applicable)
 - Supported Smart Card readers:
 - pivCLASS (PIN, BIO or CAK)
 - Veridt Multimode
 - 12 - 24V DC UL294 Access Control/Burglary Power Supply, capable of supporting power requirements as specified in *Section 2 Specifications*.
2. Protect the hardware components in the enclosure. See *Section 4.3 Enclosure installation*.
3. Observe the necessary regulatory information. See *Section 7 Regulatory*.
4. The pivCLASS Reader Services software has been installed and configured.
5. Ensure Administrators and Users are familiar with PACS operating concepts.

1.5 Glossary

Term	Description
BIO	Biometrics
CAC	Department of Defense Common Access Cards
CHUID	Cardholder Unique Identifier
CIV	Commercial Identity Verification credential or PIV-C
FRAC	First Responder Authentication Credential
PAM	pivCLASS Authentication Module
PKI	Public Key Infrastructure
TPK	TWIC Private Key
TWIC	Transportation Worker Identification Credential

Section 2

2 Specifications

2.1 Technical specifications

Parameter	Specification
Dimensions	6.70 x 6.05 in (17 x 15.4 cm) 7.32 x 6.61 in (18.6 x 16.8 cm), including Enclosure
Power	Input: 12 V DC @ 1.2Amp, 24 V DC @ 600mA (Note: PAM has a <10ms in-rush of ~2.2A on power on) Output Reader Power: 11.5 V DC, 300 mA (each)
Relays (if equipped)	Dry Contacts Coil: 5 V DC, 360mW Contacts: 28 V DC, 5 Amp (resistive loads only)
Environmental	32° to 120°F (0° to 49°C) 0 to 85% RHNC, Indoor Only
Communication	Host: 10/100 Ethernet TCP/IP TLS (AES Encryption) Smart Card Readers: Two (2) RS-485 FDX Serial Ports Access Control System Reader Interface Module: Two (2) Wiegand Ports

2.2 Cable specifications

Option	Length	Specification
Input Circuits ¹	500 feet (152 m)	2-conductor, shielded, using Alpha 1292C (22 AWG) or Alpha 2421C (18 AWG), or equivalent
Output Circuits ¹	500 feet (152 m)	2-conductor, using Alpha 1172C (22 AWG) or Alpha 1897C (18 AWG), or equivalent
Wiegand	500 feet (152 m)	Alpha 1295C, 22 AWG, 5-conductor, stranded, overall shield
Ethernet	300 feet (91 m)	Cat5, Cat5E, and Cat6
RS-485	500 feet (152 m)	Belden 3108A or equivalent, 22 AWG, 6-conductor, stranded overall shield

¹Minimum wire gauge depends on cable length and current requirements.

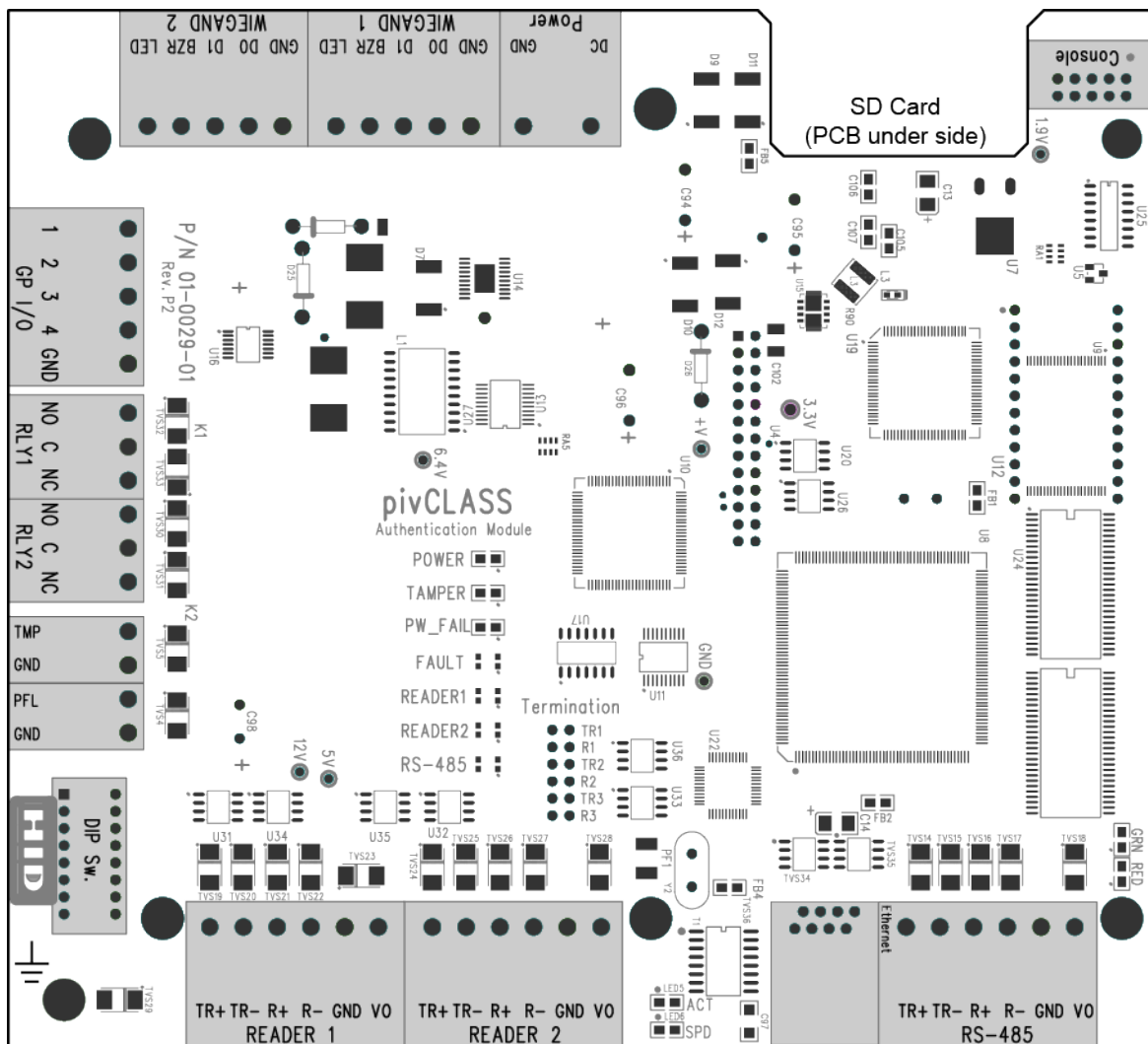
This page is intentionally left blank.

Section 3

3 Module description

This chapter describes the physical and security features of the pivCLASS Authentication Module (PAM).

3.1 Physical features



Physical features include:

- **Console:** For internal use.
- **SD Card Socket:** Insertion point for the SD Card with PAM Firmware.
- **Power Connector:** Connects the PAM to the power supply.
- **Ground Connector:** Connect the PAM to Earth ($\perp$) using the grounding lug on the PAM
- **Wiegand 1 and 2 Connector:** Connects the PAM to the PACS.
- **GP I/O:** General Purpose I/O. Reserved for future use.
- **Relay 1 and 2 (if equipped):** Customer configurable for auxiliary purposes.



CAUTION

Do not use relays for access control, this voids UL certification.

- **Tamper Monitoring:** Enables the system to monitor a normally closed or open (NC/NO) tamper line wired to the case. This sends a log message back to Reader Services if the tamper line is activated. Typically, this monitoring is done by the PACS.

PIN	Assignment
1	TMP
2	GND

- **Power Failure Monitoring:** Enables the system to monitor a normally closed or open (NC/NO) power fail line. This sends a log message back to Reader Services if the power fail line is activated. Typically, this monitoring is done by the PACS.

PIN	Assignment
1	PFL
2	GND

- **DIP Switch:** Configures the mode on which the PAM is running.
- **Reader 1 and 2 Connector:** Connects to the supported reader.
- **Termination Resistor Jumpers:** Located on the board from the Reader 2 Connector and includes RS-485 ports. Use when connecting Reader 1 and 2. If using lengths greater than 200 feet (61 m) or if there is RF or other EMI interference, refer for the information in *Section 4.4 Making jumper connections*.
- **Ethernet:** Connects the PAM to the Network.



WARNING

It is recommended to disable POE power on the port the PAM is connected to if the switch is a POE switch.

If using a Rev A PAM (91000ANNNN or 91000ABNNN), the POE power must be turned off to prevent damage to PAM or switch; or use a non-POE switch.

Note: If using a Rev A PAM (91000ANNNN or 91000ABNNN), some Gigabit Ethernet Switches may require setting the port to 100 Mbps or 10 Mbps.

- **RS-485:** A serial port reserved for future use.

3.2 Security features

Security features include:

- All TCP ports are closed except for a single port that only accepts authenticated requests from the pivCLASS Reader Services. The default port is 10200.
- Communicates with the pivCLASS Reader Services by way of 256-bit AES encrypted over Ethernet TCP/IP.
- Web interface for initial PAM configuration (or enabling SSH). Accessed with a DIP switch setting on the PAM.
- FIPS 140-2 certified.
- Cryptographic firmware.

3.3 Card Passthrough

The PAM, through version 5 of the PAM firmware, controls the functions of the reader, this includes:

- When the reader polls (looks for a card in the RF field and contact if equipped).
- How it polls (what technologies it polls for).
- All of the Audio Video (AV) feedback to the end-user.

These polling operations are usually requested from the PAM in 100ms - 200ms intervals.

When operating in an Assurance Profile only mode, the PAM will issue a command to the reader to poll the High Frequency (HF) range of the reader to detect a card. Once a card is found, the PAM will determine the card type. If the card is a PIV, CAC, TWIC, PIV-I, CIV, or FRAC card, the PAM will then process the data and perform validations per the current configuration. If the card is determined to not be a PIV, CAC, TWIC, PIV-I, CIV, or FRAC card, it will flag the card as a non-vaild card and stop processing it. In this mode all credential processing is completed on the secure side of the door in the PAM.

When Card Passthrough is enabled on the PAM, the PAM will poll for the PIV/TWIC (or like card) as described above, and will then issue an additional command for the reader to autonomously poll. When the reader preforms an autonomous poll, the reader will poll for any technology that it is configured for and then process the card internally in the reader. The processed data is then sent down to the PAM. The PAM will recognize the data as not being from a PIV/TWIC (or like card) and then pass it through to the panel (hence the "Passthrough"). This allows the reader to poll and process technologies such as iCLASS, Seos, Prox, MIFARE, DESFire, etc.

3.3.1 PAM operation without Card Passthrough

The reader polling cycle, when not in Card Passthrough mode, is controlled completely by the PAM. The PAM will issue a command to scan the HF field and then to scan the contact slot interface:

1. Scan for PIV or like card
2. Get Response
3. Scan for contact card
4. Get response
5. Disconnect (this step may not be needed)
6. Get response
7. Start over

3.3.2 PAM operation with Card Passthrough

When Card Passthrough is enabled, the PAM will direct the reader to perform an autonomous poll and process using a scan and process command. This can be sent at any point after receiving the response from the previous command to the reader. Current implementation has it after the HF poll.

Example process of PAM with Card Passthrough enabled:

1. Scan for PIV or like card
2. Get Response
3. Send Scan and process command
4. Get response
5. Scan for contact card
6. Get response
7. Disconnect (this step may not be needed)
8. Get response
9. Start over

Section 4

4 Installing the module

This chapter describes installing, connecting and powering the pivCLASS Authentication Module (PAM).



CAUTION
ELECTROSTATIC SENSITIVE DEVICES
Observe precautions for handling

4.1 Checking the package contents

Before installing the PAM, unpack the contents of the shipping container and make sure that you have the items listed.

Item	Quantity
pivCLASS Authentication Module (PAM)	1
Secure Digital (SD) Card with PAM Firmware (Note: Depending on configuration this may be pre-installed in the PAM)	1
Jumpers	6
Termination Resistors (118 ohm)	4

4.2 Installation preparation

Carry out the following:

1. Obtain an Ethernet cable or switch to connect the PAM. The choices are:
 - Crossover cable connects to the pivCLASS PACS Service Application (for configuration).
 - Straight-through cable connects to a hub or switch.
2. Prepare the UL294 Listed Enclosure.
3. Remove the PAM from its packaging.

Note: Ensure the SD Card is correctly seated.

4.2.1 Creating a SD card image

If your PC has a SD card reader/writer, you can create a SD card consisting of the latest release PAM firmware by downloading the SD card image from the software distribution web site.

Note:

- Make sure to utilize the SD cards shipped from HID Global. Do not use SD cards acquired through other means.
- If creating a SD Card to upgrade from previous to 5.x firmware, make sure to verify the power supply is minimally compliant to the specifications listed in *Section 2 Specifications*. Early versions of PAM had lower power requirements resulting in possible power supply issues for existing installations.

1. Install the following tools:

- 7-zip from: <https://7-zip.org/download.html>
- HDD Raw Copy Tool from: <https://hddguru.com/software/HDD-Raw-Copy-Tool>

2. Open a web browser and enter the address of the pivCLASS software distribution site.

Note: This was provided in the entitlement email from HID Global and usually takes the form of:

https://www.pivcheck.com/<pcs_name>

3. From the **firmware** directory download the desired SD card image file, for example:

firmware_A.B.C.D.dd.bz2 (where **A.B.C.D** is the release number).

4. Unzip the **.bz2** file using 7-zip. The file size will be approximately two GB.

5. To create the SD Card Image, launch the HDD Guru HDD Raw Copy Tool.

6. Double-click on **File** to browse to the location containing the **.dd** file.

7. Select the file and click **Continue**.

8. Select the SD card as the destination and click **START** to begin the sector copy.

9. When complete, the SD card can be removed and is available for use in a PAM.

Note: After booting, the PAM will be returned to factory defaults.

4.3 Enclosure installation

Install the PAM in a UL 294 Listed enclosure. Furthermore, install the PACS and appropriate power supply (not supplied by HID Global) according to the manufacturer's instructions.

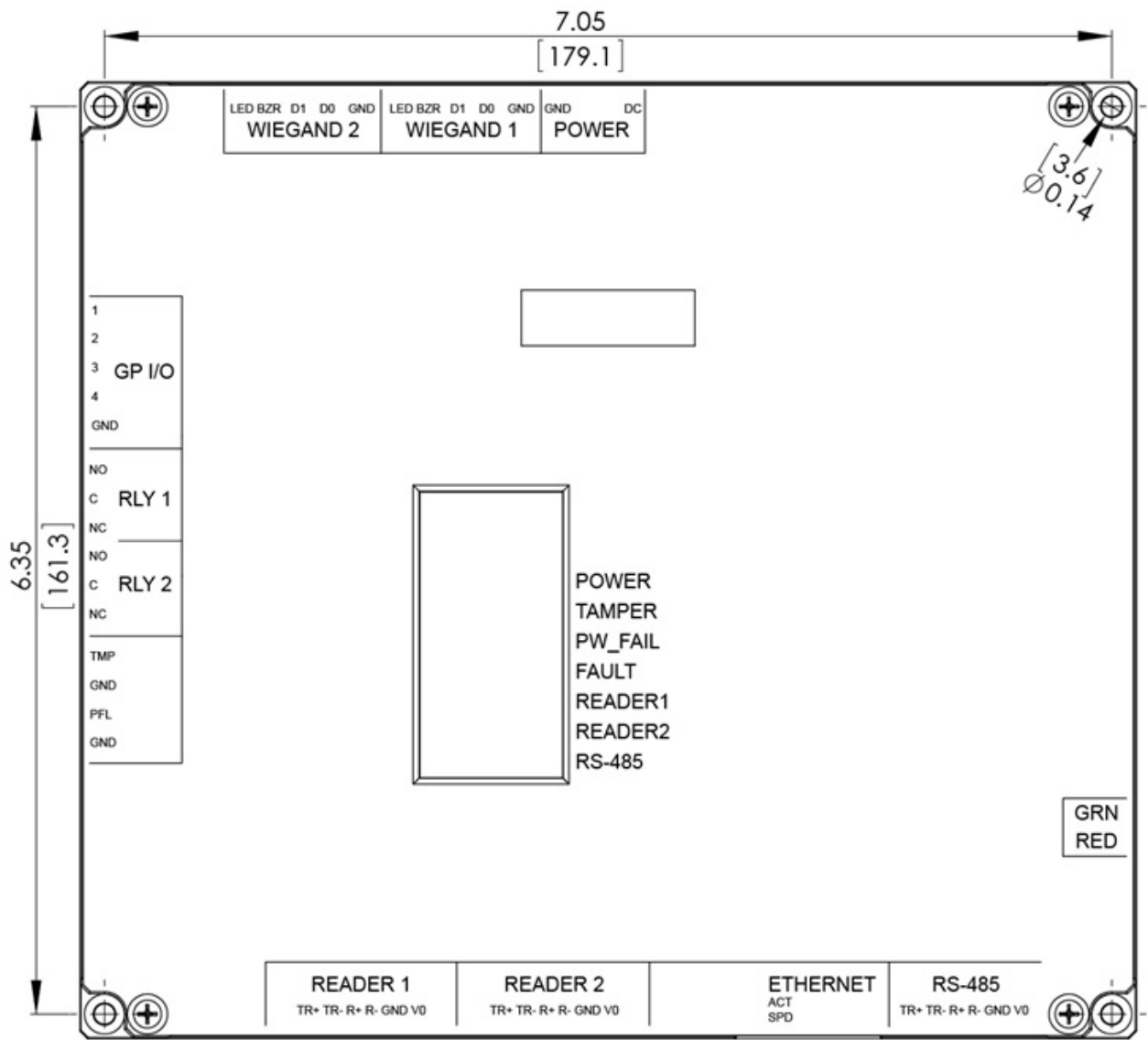
4.3.1 PAM mounting dimensions

Use the dimensions below to mark the drilling holes on the enclosure (the illustration is not to scale).



WARNING

Connecting pivCLASS Authentication Modules while power is applied may result in damage.



Note:

- The mounting hole diameter is 0.14 inch (0.36 cm).
- The recommended mounting screw size is #6 (Imperial) or M4 (Metric).
- The recommended clearance around the sides of the PAM is least 1 inch to allow for wiring and access to the SD card.
- The recommended clearance between the PAM and the chassis is at least 1 inch (2.54 cm) for adequate ventilation.
- Unless already provided by the PACS system, connect a tamper switch (default is Normally Closed) to monitor the enclosure.

4.4 Making jumper connections

The PAM includes jumper locations (TR1, R1, TR2, R2, TR3, and R3) identified as **Termination**. They apply to the RS-485 port terminations (the two reader connections and the RS-485 port - intended for future use). By default, the jumpers are set to **OFF**.

If your installation uses long wires between the PAM and the readers, for example 200 feet (61 m) or greater, or if there is significant EMF interference, you must install the jumpers. Jumpers need to be installed on the **Termination** pins found on the PAM, located above the Reader 2 port (refer to the diagram in *Section 3.1 Physical features*).

Jumpers are configured in the following pairs:

- TR1 and R1 for Reader 1
- TR2 and R2 for Reader 2

You must install a resistor (typically 120 ohm, +/- 2 ohm) across the RS-485 terminals of the connected reader (labeled RXA & RXB for the TR+ & TR- pair and TXA and TXB for the R+ & R- pair on a pivCLASS reader).

4.5 Wiring connections

This section explains wiring the PAM to the PACS panel and supported reader(s).

4.5.1 Connecting PAM to supported reader port

Using a small flat-head screwdriver (1/8 inch or smaller), connect the **Reader 1** or **Reader 2** connector on the PAM to the supported reader(s) according to the following table.



WARNING

Do not apply VDC to any connector from the reader other than +VDC.
Applying 12 V DC or greater to the GPIO lines may result in damage to the reader.

PAM Connections (READER 1 or 2)	Reader (Pigtail)	Reader (Terminal)
TR+	Red/Green	GPIO1 (P2-7)
TR-	Tan	GPIO2 (P2-6)
R+	Gray	GPIO4 (P2-1)
R-	Pink	GPIO3 (P2-2)
GND (Ground)	Black	GND (P1-3)
VO (Voltage Out)	Red	+VDC (P1-4)

4.5.2 Connecting PAM to PACS panel reader port

Using a small flat-head screwdriver (1/8 inch or smaller), connect the PAM **Wiegand 1** or **Wiegand 2** connector (or both) to the PACS Panel Reader port. Reader 1 corresponds to Wiegand 1 and Reader 2 corresponds to Wiegand 2. See table below.

Note: Ensure connecting the correct connectors, since Wiegand 2 and 1 are flipped compared to Reader 1 and 2. See *Section 4.3.1: PAM mounting dimensions*.

PAM Connections (WIEGAND 1 or 2)	PACS Panel Connections (READER 1 or 2)
GND	GROUND
D0	DATA0/DATA
D1	DATA1/CLOCK
BZR	BEEPER
LED	GREEN LED

Note: Some PACS may have multiple LED wires, for example, red/green.

The PAM checks for a constant signal on the LED input (Green LED) indicating access granted by the PACS after Wiegand is sent. If this signal is not received within one second of sending the Wiegand card number and PIN then it will be considered access denied (this is the default setting for time-out and is configurable for each PAM in the pivCLASS PACS Service). Any type of blinking or flashing signals from the panel are not supported.

Some PACS panels may signal on the LED input (Green LED) when access is not granted. In these cases BZR should be wired to another output from the PACS panel (most likely the red LED). The PAM will ensure that the BZR input is not signaled and the LED is signaled in order to interpret the PACS as having provided access. No configuration change is necessary for this so it is important that the wiring is done with consideration for the behavior of the PACS panel.

4.6 Connecting to the network

Connect the Ethernet cable between the Ethernet port and the PC, hub or switch. There are two LEDs for the Ethernet connection; one indicates speed (SPD) and the other indicating Activity (ACT). The ACT LED (LED5) blinks when there is network activity.

Note:

- For Rev A of the PAM (91000ABNNN or 91000ANNNN): Some Gigabit Ethernet Switches may require setting the port to 100 Mbps or 10 Mbps and/or disabling Energy Efficient Ethernet/"Green" capability of the port. If the switch is a PoE switch and the PoE port must be used, PoE capability must be disabled.
- For Rev B of the PAM (91000BNNNN or 91000BBNNN): It is still suggested to disable POE capability on the port used, however is not required. No other restrictions from Rev A apply.

4.7 Connecting to the power supply

Using a small flathead screwdriver (1/8 inch or smaller):

1. Connect the PAM to Earth Ground ($\perp$) using the grounding lug on the PAM, see *Section 3.1 Physical features*.
2. Connect the PAM Power connector to the power supply. Connect only to a Listed Access Control / Burglary Power - limited power supply.

Important: Connect the PAM to a power supply that has a battery backup or which is plugged into an Uninterruptable Power Supply (UPS). Power loss during normal operation might result in the loss of data or, in extreme cases, might render the SD card unbootable.

Install in accordance with NFPA70 (NEC) Local Codes, and authorities having jurisdiction. Follow all National and Local Codes.

The following table provides the power supply connections for each power connector.



CAUTION

Do not connect to AC. PAM does not support POE Power.

PIN	Power Connector	DC Power Connections
1	DC	+
2		Not Used
3	GND	-

4.8 Applying power

After attaching all PAM connections apply power and configure the PAM (see *Section 5 PAM configuration*).

4.9 Disabling power

For powering off the PAM, ensure all processes are complete and remove power.



CAUTION

Do not remove power to reboot, unless it is absolutely necessary, as data corruption on the SD card may occur.

For PAM Configuration and setup, see *Section 5 PAM configuration*.

This page is intentionally left blank.

Section 5

5 PAM configuration

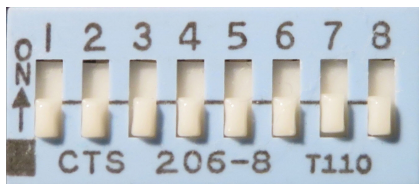
5.1 Overview

This section describes the pivCLASS Authentication Module (PAM) Configuration application and provides procedures for PAM setup. When the PAM is placed into setup mode the PAM Configuration application, accessed through a web browser using a supplied IP address, provides an interface to configure the PAM.

Note: From firmware version 5.4 and onwards the Panel Auto Discovery feature can be used to configure the PAM. The feature can be used if the PACS Service is on the same subnet and/or the network is setup to allow UDP broadcast messages from Panel to the PACS Service computer. If Auto Discovery Mode is enabled then the use of the PAM Configuration tool is not required.

5.2 PAM DIP switches

The following are the DIP Switch settings for the PAM Hardware.



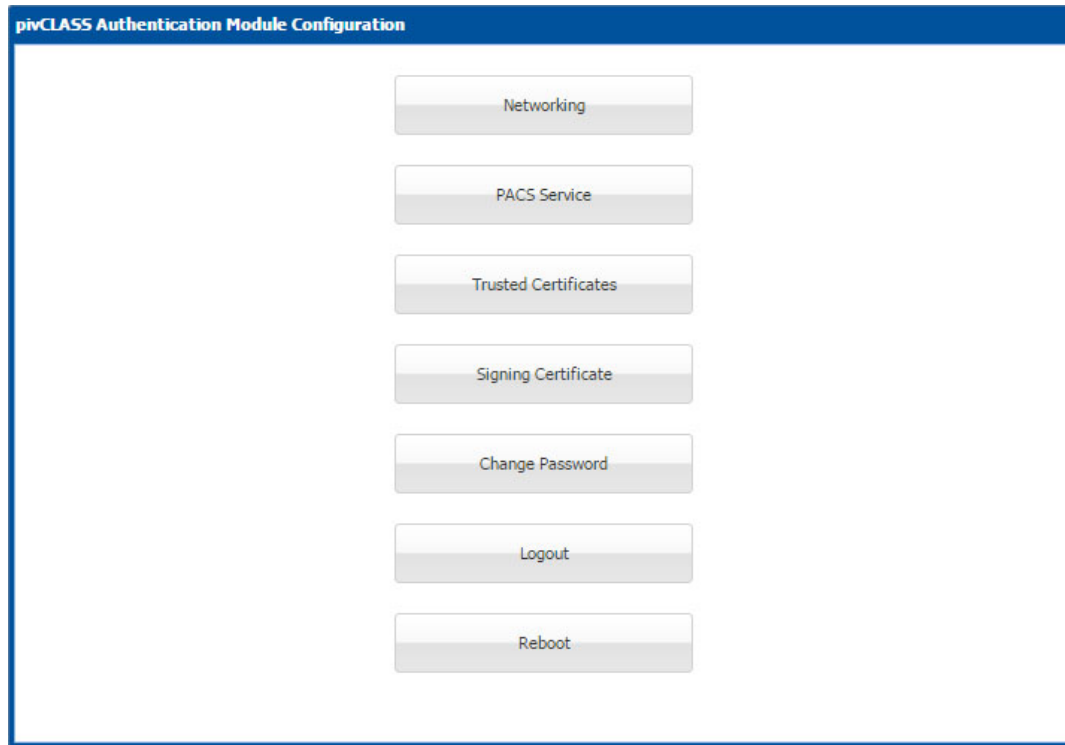
General Dip Switch Functions

DIP Switch	Function
1	When set to OFF , enables Auto Discovery Mode and disables Internet browser capability. When set to ON , enables Internet browser capability and disables Auto Discovery Mode. Note: Out of the box dip switch 1 is set to OFF (Auto Discovery Mode enabled).
2	When set to ON , enables SSH.
3 to 7	Not used.
8	When set to ON at boot up, causes a factory reset.

DIP switch settings for a panel can be viewed in the PACS Service application via the **Hardware** tab on the **Panel** form for a configured panel. DIP switch status changes are recorded in the PACS Service log file and a DIP switch status event is sent to the PACS.

5.3 PAM Configuration application overview

The following provides an overview of the pivCLASS Authentication Module (PAM) Configuration application.



Function	Description
Networking	Used to configure the network settings that enable the PAM to connect to and communicate with the network. The network can be configured using a Static IP or using DHCP.
PACS Service	Used to enter the PACS connection information.
Trusted Certificates	Used to upload trusted certificates on the PAM and view certificate details.
Signing Certificate	This function provides options to: • View details of the PAM's Signing Certificate. • Download the PAM's Self-Signed Signing Certificate to your computer in order to save the certificate to the remote system's Trusted Store. • Download the PAM's Certificate Signing Request file in order to send it to an external Certificate Authority for signing. • Upload the external Certificate Authority signed PAM Signing Certificate. • Generate a new Private Key and Self-Signed Signing Certificate.
Change Password	Allows the user to change the access password.
Logout	Logs the user out of the PAM.
Reboot	Reboots the PAM and applies any configuration changes. You will have to log back in after the system restarts.

5.4 Manual PAM configuration

This section describes how to setup the PACS Service to PAM communication path and manually add a PAM within Reader Services.

5.4.1 Panel API communication options

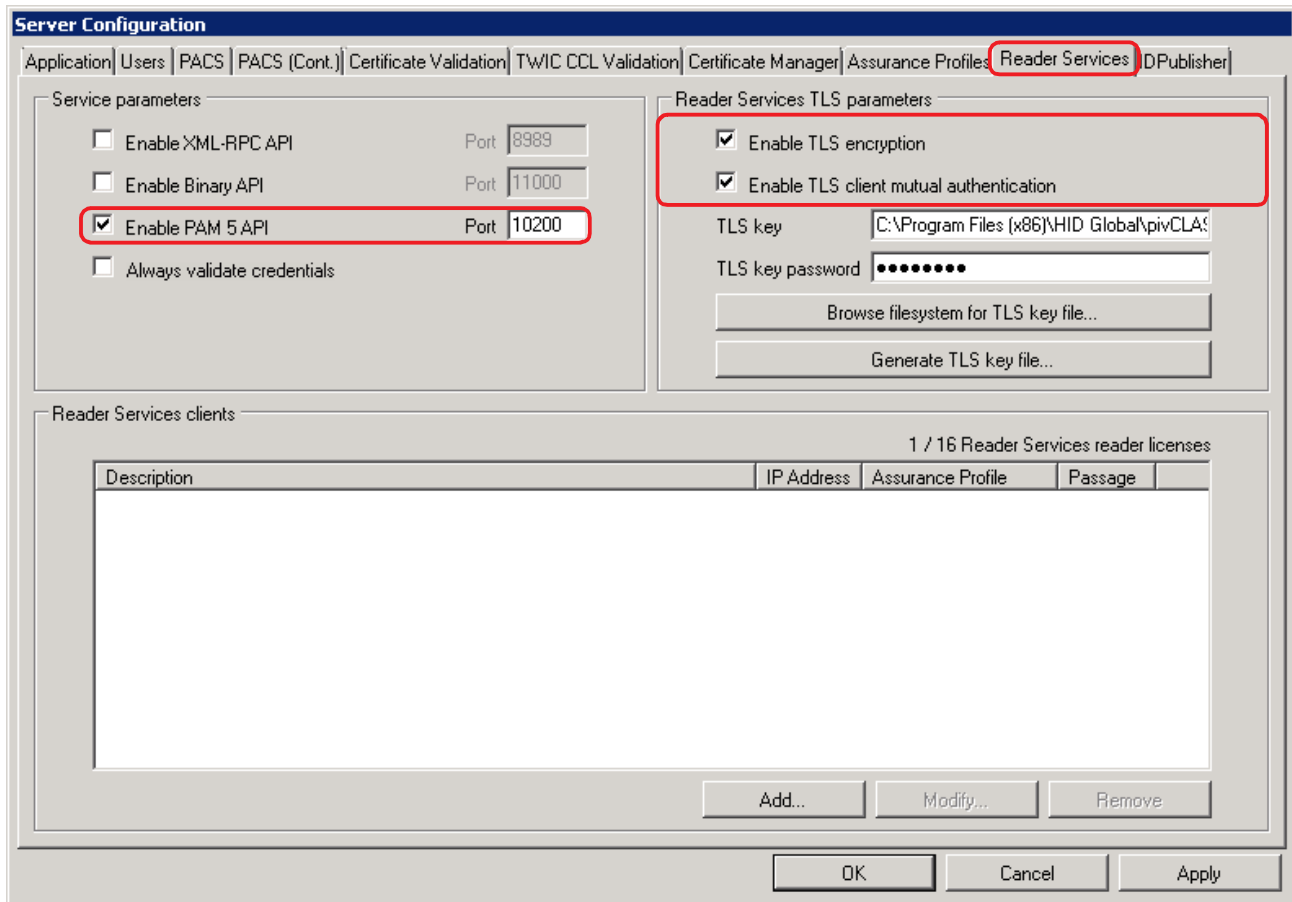
Before you begin manual PAM configuration check the panel API communication options in the PACS Service application:

1. Start the PACS Service application and select **Configuration > Edit Service Settings**.
2. Select **Reader Services** tab and ensure the **Enable PAM 5 API** option is selected.

Note: If the default port number 10200, is not accepted, enter a new port number in the **Port number** field. Record the port number and retain it for later use to configure the PAM.

3. It is recommended that the **Enable TLS encryption** and **Enable TLS client mutual authentication** options are selected to encrypt communication between the PACS Service and API client.

For additional information on PACS Service encrypted communication and TLS parameter options, select F1 while on the **Reader Services** tab to access the relevant *PACS Service Online Help* topic.



Server Configuration

Application | Users | PACS | PACS (Cont.) | Certificate Validation | TWIC CCL Validation | Certificate Manager | Assurance Profiles | **Reader Services** | DPublisher

Service parameters

- ☐ Enable XML-RPC API Port: 8989
- ☐ Enable Binary API Port: 11000
- ☒ **Enable PAM 5 API** Port: 10200
- ☐ Always validate credentials

Reader Services TLS parameters

- ☒ Enable TLS encryption
- ☒ Enable TLS client mutual authentication
- TLS key: C:\Program Files (x86)\HID Global\pivCLAS
- TLS key password:
- Browse filesystem for TLS key file...
- Generate TLS key file...

Reader Services clients

1 / 16 Reader Services reader licenses

Description	IP Address	Assurance Profile	Passage

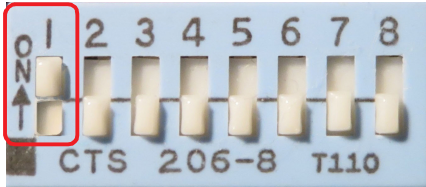
Add... Modify... Remove

OK Cancel Apply

5.4.2 Configure the PAM to communicate with the PACS Service

Follow the steps below to configure communication between the PAM and PACS Service.

1. Install the PAM and power it on.
2. Place the PAM into configuration mode:
 1. Disconnect power from the PAM.
 2. Set dip switch 1 on the PAM board to **ON**. PAM configuration mode is now enabled.



3. Reconnect power to the PAM.
3. Connect an Ethernet cable from a computer to the PAM (located on the bottom of the device).
4. Open a web browser and enter the following default url: **https://192.168.0.222** (factory default; ensure your computer is configured to the **192.168.0.x** IP range). A subnet mask example is: **255.255.255.0**.

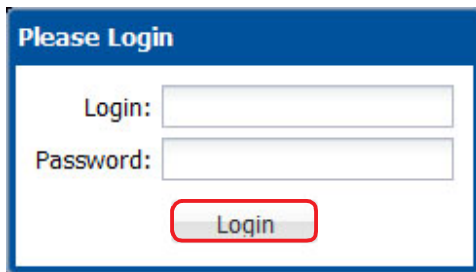
At this point your browser will present you with a security warning. The PAM is a device, not an Internet web site, and uses a self-signed certificate. Your browser cannot verify the owner of the self-signed certificate.

Depending on your browser you may be instructed to click on an **Advanced** button to find an option to proceed to the web site or add a security exception.

Note: A self-signed certificate still encrypts your connection making your data safe from eavesdroppers.

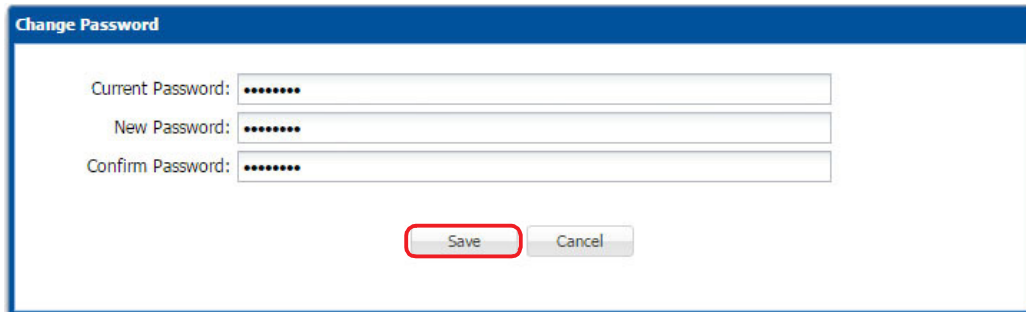
5. Enter the following login credentials and click **Login**.

- **Login:** admin
- **Password:** password



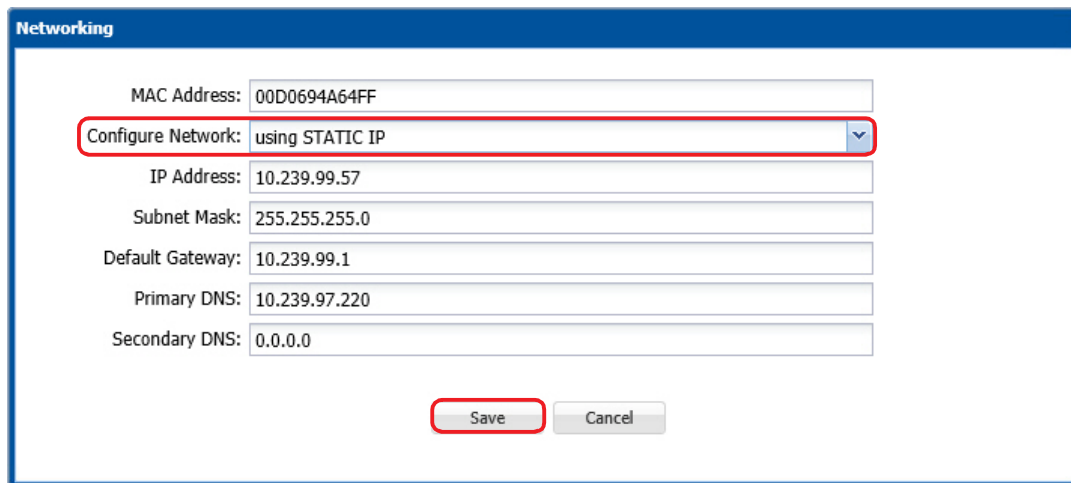
Important: For security reasons the default admin password should be changed as soon as possible. Select **Change Password** from the PAM Configuration application main menu (see *Section 5.3 PAM Configuration application overview*), Enter the **Current Password**, the **New Password** (twice to confirm) and click **Save**.

Note: Make sure to securely save password information as it is not recoverable without setting the entire panel back to factory defaults.



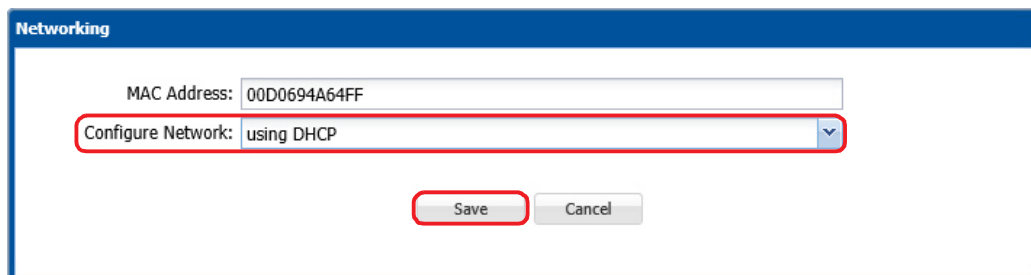
The 'Change Password' dialog box has a blue header bar with the title 'Change Password'. It contains three text input fields: 'Current Password:', 'New Password:', and 'Confirm Password:'. Each field is filled with seven dots. At the bottom, there are two buttons: 'Save' (highlighted with a red border) and 'Cancel'.

6. From the PAM Configuration application main menu, select **Networking**.
7. In the **Networking** window record the **MAC Address** for later use to create the PAM configuration in the PACS Service.
8. From the **Configure Network** drop-down menu, select one of the following options:
 - **STATIC IP:** Enter the PAM **IP Address**, **Subnet Mask**, **Default Gateway** and click **Save**.



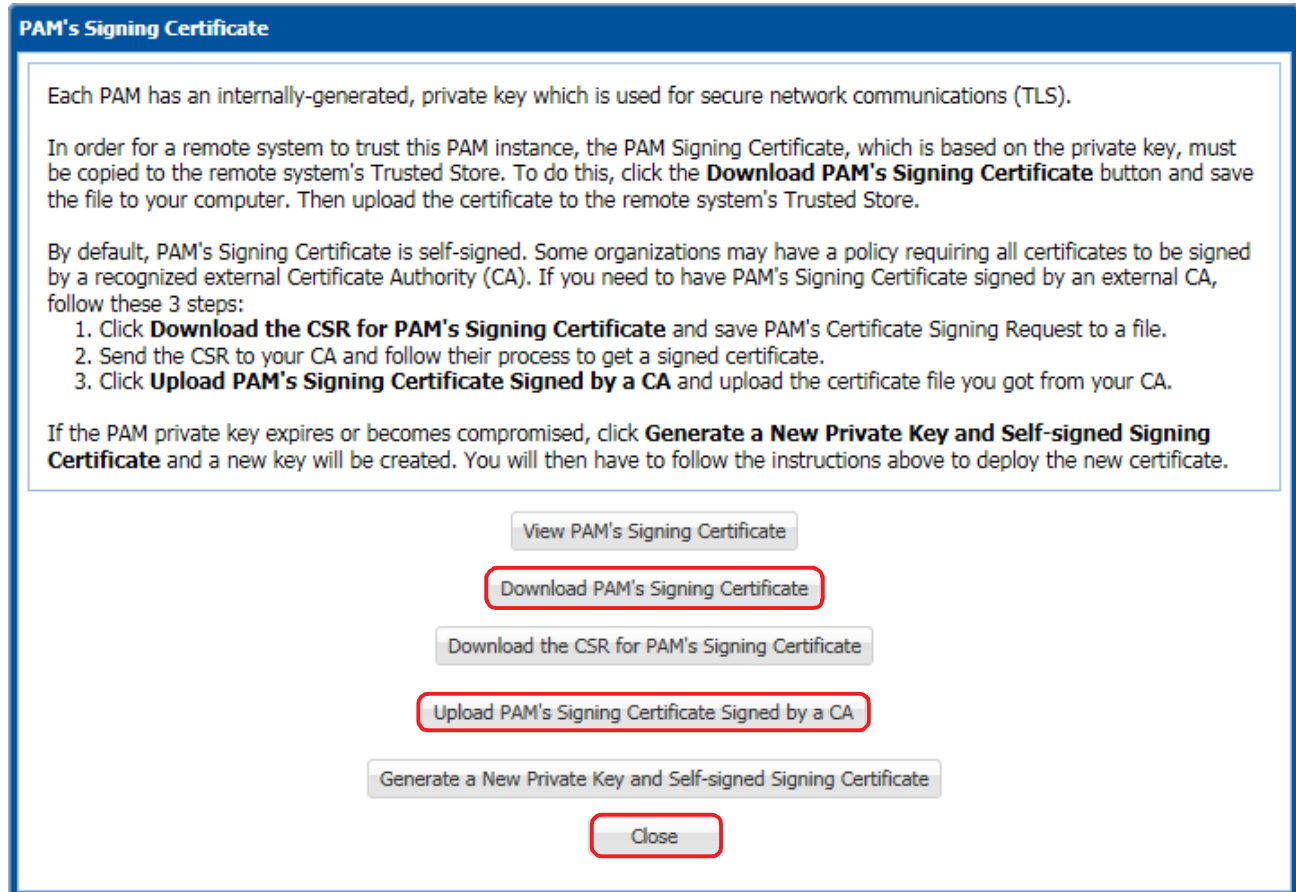
The 'Networking' dialog box has a blue header bar with the title 'Networking'. It contains several fields: 'MAC Address:' with the value '00D0694A64FF', 'Configure Network:' with a dropdown menu set to 'using STATIC IP' (highlighted with a red border), 'IP Address:' with '10.239.99.57', 'Subnet Mask:' with '255.255.255.0', 'Default Gateway:' with '10.239.99.1', 'Primary DNS:' with '10.239.97.220', and 'Secondary DNS:' with '0.0.0.0'. At the bottom, there are two buttons: 'Save' (highlighted with a red border) and 'Cancel'.

- **DHCP** (to configure the PAM to obtain a network address dynamically) and click **Save**.



The 'Networking' dialog box has a blue header bar with the title 'Networking'. It contains several fields: 'MAC Address:' with the value '00D0694A64FF', 'Configure Network:' with a dropdown menu set to 'using DHCP' (highlighted with a red border), and two buttons at the bottom: 'Save' (highlighted with a red border) and 'Cancel'.

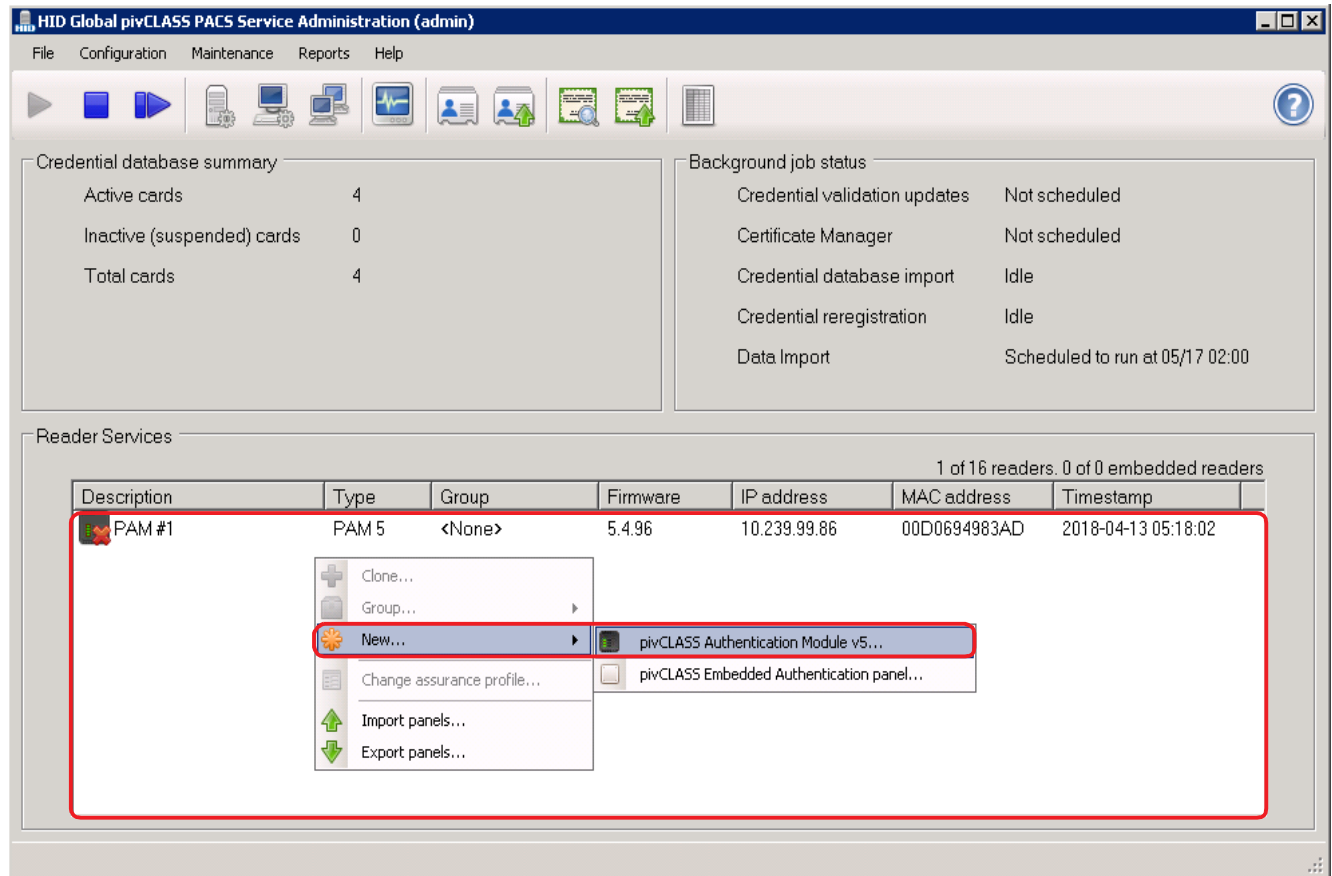
9. From the PAM Configuration application main menu, select **Signing Certificate**.
10. In the **PAM's Signing Certificate** window either:
 - Download PAM's self-signed Signing Certificate **.cer** file to your computer. Select **Download PAM's Signing Certificate**.
 - Follow the on-screen instructions to get the PAMs Signing Certificate signed by an external Certificate Authority (CA).
11. Click **Close** to exit the screen.



12. For the PACS Service to trust the PAMs Signing Certificate move/copy the certificate **.cer** file to:
C:\Program Files (x86)\HID Global\pivCLASS PACS Service\pam\clientcerts
 where: **C:\Program Files (x86)\HID Global\pivCLASS PACS Service** is the PACS Service installation directory.

5.4.3 Configure PAM in Reader Services

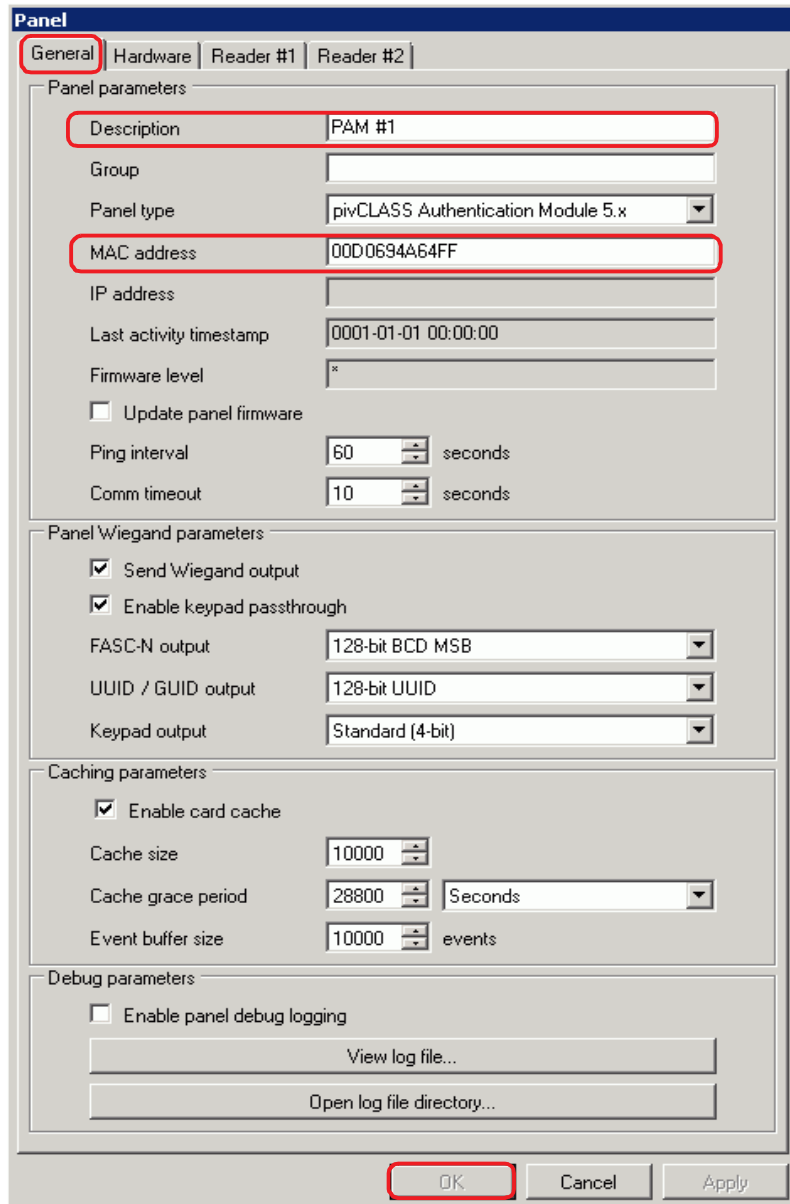
1. Start the PACS Service application.
2. On the PACS Service application main window, right-click within the **Reader Services** status window.
3. Select **New > pivCLASS Authentication Module 5** from the menu.



4. In the **Panel** dialog box, select the **General** tab and enter a description for the PAM in the **Description** field.
5. Enter the MAC address of the PAM in the **MAC address** field (do not include dashes or colons). The MAC address is the address previously recorded from the PAM Configuration window, see *Section 5.4.2 Configure the PAM to communicate with the PACS Service*, Step 6.

Note: The MAC address assigned to the PAM by the manufacturer is located on a label attached to the PAM enclosure.

6. Click **OK**.



Panel

General | Hardware | Reader #1 | Reader #2

Panel parameters

Description: PAM #1

Group:

Panel type: pivCLASS Authentication Module 5.x

MAC address: 00D0694A64FF

IP address:

Last activity timestamp: 0001-01-01 00:00:00

Firmware level: *

☐ Update panel firmware

Ping interval: 60 seconds

Comm timeout: 10 seconds

Panel Wiegand parameters

☒ Send Wiegand output

☒ Enable keypad passthrough

FASC-N output: 128-bit BCD MSB

UUID / GUID output: 128-bit UUID

Keypad output: Standard (4-bit)

Caching parameters

☒ Enable card cache

Cache size: 10000

Cache grace period: 28800 Seconds

Event buffer size: 10000 events

Debug parameters

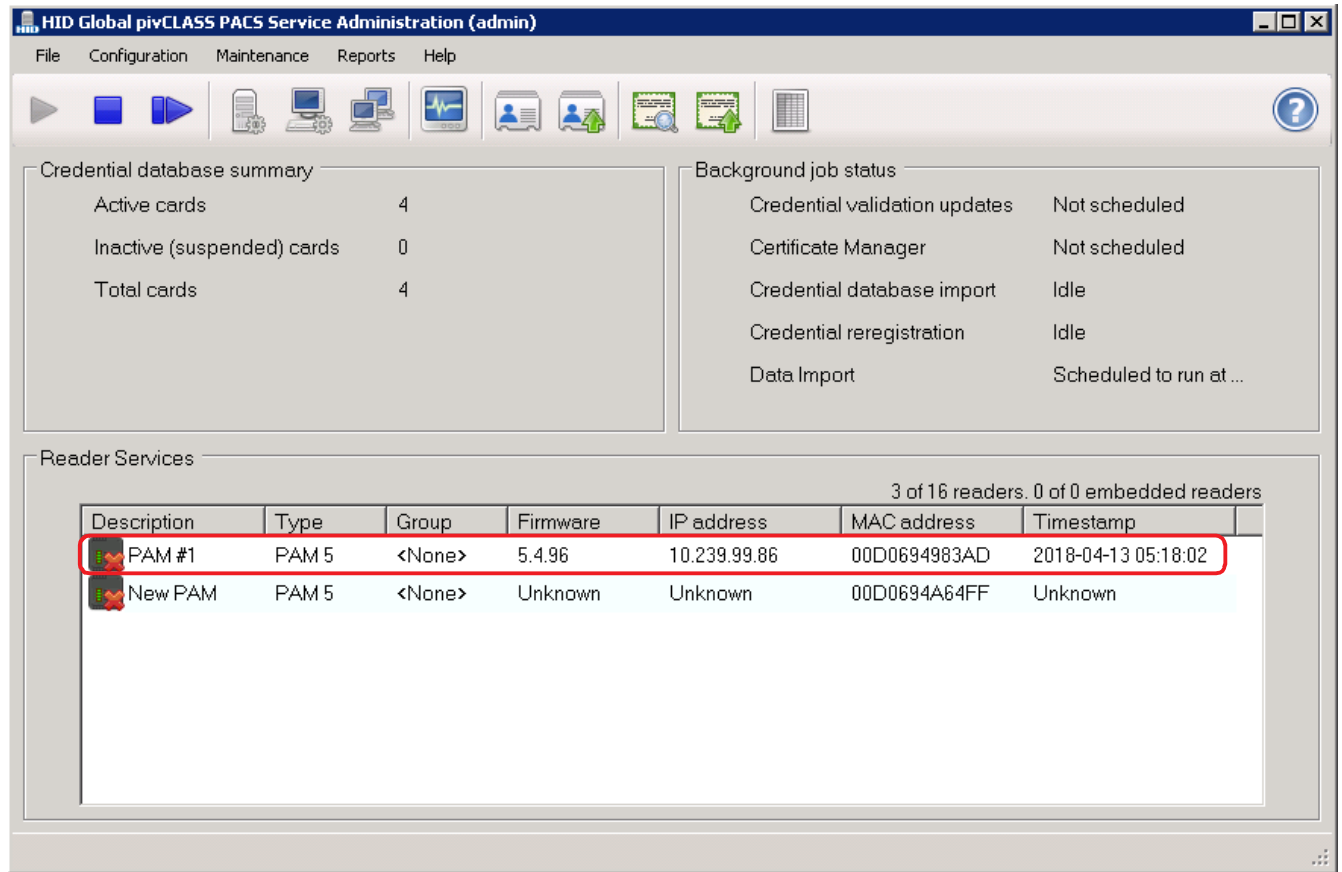
☐ Enable panel debug logging

View log file...

Open log file directory...

OK Cancel Apply

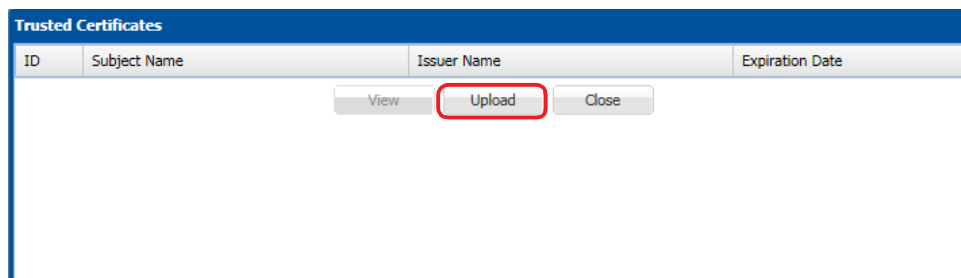
The newly created PAM is displayed in the **Reader Services** status window.



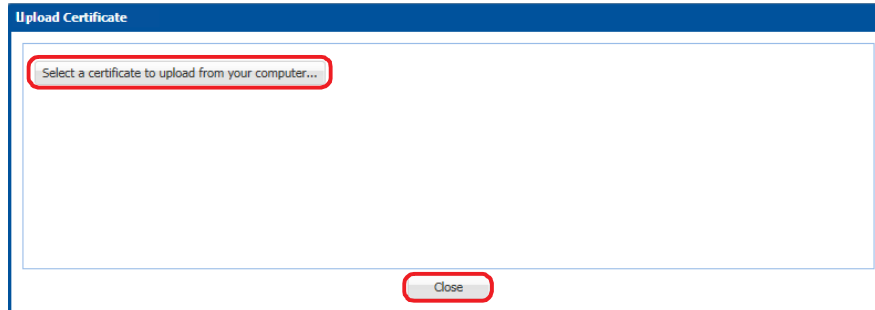
- Return to the pivCLASS Authentication Module Configuration application main menu in the web browser.

Note: Inactivity of a more than a few minutes may cause the web browser to time out. You will need to log back into the PAM Configuration application.

- From the PAM Configuration application main menu (see *Section 5.3 PAM Configuration application overview*), select **Trusted Certificates**.
- Click **Upload**.



10. Click **Select a certificate to upload from your computer** to locate and select the PACS Service TLS certificate .cer file.
11. When certificate file is displayed click **Close**.



12. Click **Close** to return to the pivCLASS Authentication Module Configuration application main menu.

ID	Subject Name	Issuer Name	Expiration Date
19	PIVDigitalSignatory V02	Entrust	Sat Aug 18 00:58:36 2018
20	TWIC ROOT	TWIC ROOT	Tue Aug 17 18:46:18 2032
21	TWIC CA 2	TWIC ROOT	Wed Jun 20 18:37:48 2018
22	TWIC CA 1	TWIC ROOT	Sun Aug 20 18:44:39 2017

View Upload Close

13. From the PAM Configuration application main menu, select **PACS Service**.
14. In the **PACS Service** window enter the following:
 - **Server Address:** Enter the network address.
 - **Server Port Number:** Enter the port number obtained from *Section 5.4.1 Panel API communication options*.
15. Click **Save**.

PACS Service

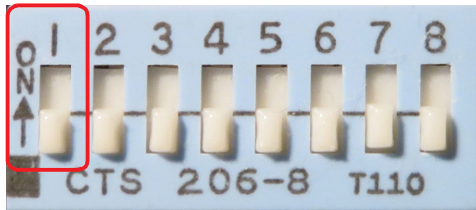
NOTE: This version of the PAM supports automatic discovery. To use discovery, turn off DIP switch 1 and the PAM will be found by any PACS Service on your local network. See the PAM Install Guide for details.

Server Address:

PAM 5.x Communication Port Number:

Save Cancel

16. From the PAM Configuration application main menu, select **Reboot**.
17. Disconnect the Ethernet cable from the computer and connect it to the switch or hub the PAM uses to communicate by the configured networking settings.
18. After the PAM has rebooted, it automatically connects to the network using the configured network settings.
19. Disable the PAM configuration application:
 1. Disconnect power from the PAM.
 2. Set dip switch 1 on the PAM board to OFF. The PAM configuration mode is now disabled.



20. Reconnect power to the PAM.

5.5 Automatic PAM configuration

This section describes how to setup the PACS Service to PAM communication path and configure a PAM in Reader Services using the automatic discovery feature.

The automatic discovery feature can be used if the PACS Service is on the same subnet and/or the network is setup to allow UDP broadcast messages from Panel to the PACS Service computer.

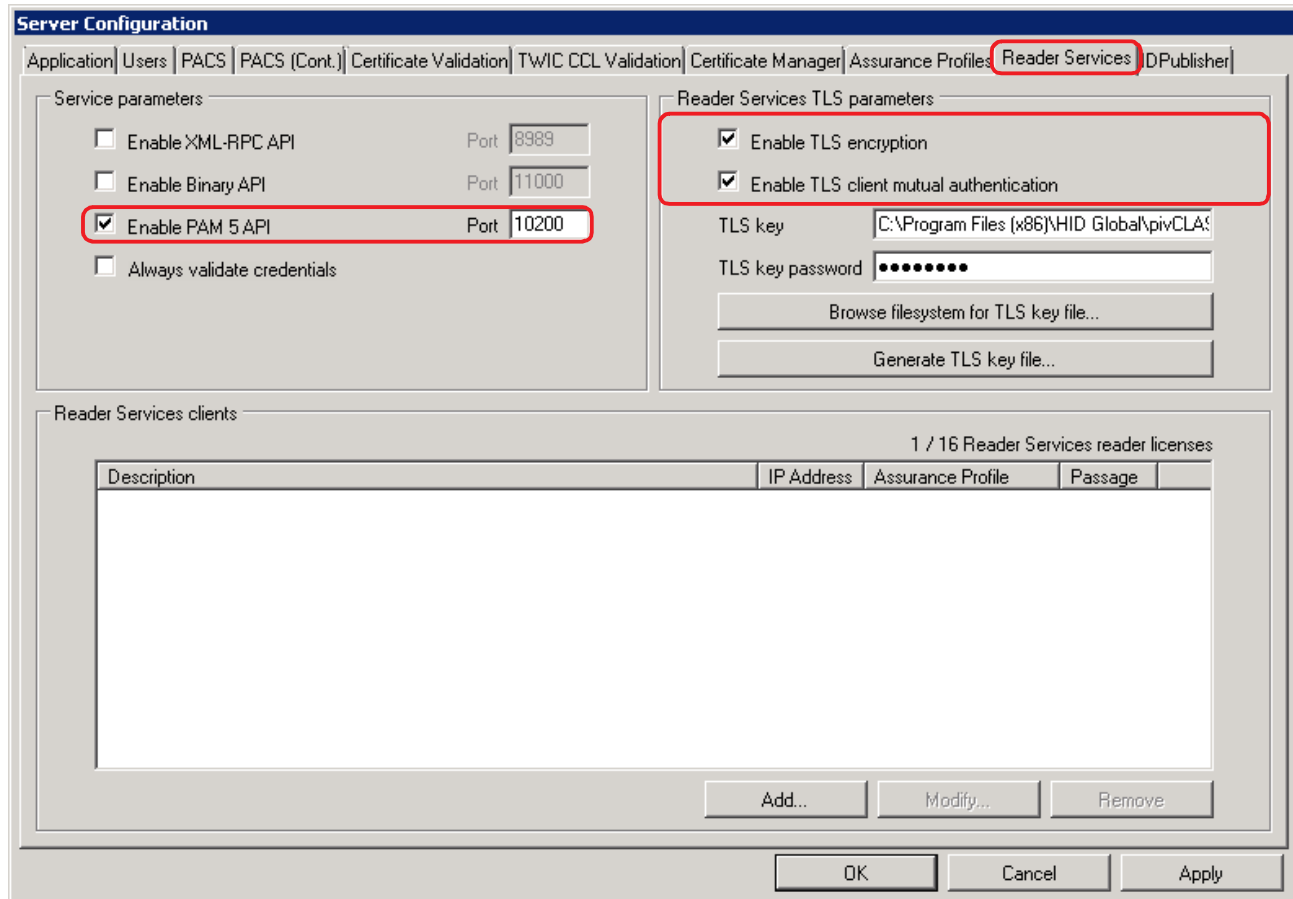
Note: Dip Switch 1 on the PAM must be in the **OFF** position for Auto Discovery Mode to be enabled, see *Section 5.2: PAM DIP switches*.

5.5.1 Panel API communication options

Before you begin check the panel API communication options in the PACS Service application:

1. Start the PACS Service application and select **Configuration > Edit Service Settings**.
2. Select **Reader Services** tab and ensure the **Enable PAM 5 API** option is selected.
Note: If the default port number 10200, is not accepted, enter a new port number in the **Port** field. Record the port number and retain it for later use to configure the PAM.
3. It is recommended that the **Enable TLS encryption** and **Enable TLS client mutual authentication** options are selected to encrypt communication the PACS Service and API client.

For additional information on PACS Service encrypted communication and TLS parameter options, select F1 while on the **Reader Services** tab to access the relevant *PACS Service Online Help* topic.



Server Configuration

Application | Users | PACS | PACS (Cont.) | Certificate Validation | TWIC CCL Validation | Certificate Manager | Assurance Profiles | **Reader Services** | DPublisher

Service parameters

- ☐ Enable XML-RPC API Port: 8989
- ☐ Enable Binary API Port: 11000
- ☒ **Enable PAM 5 API** Port: **10200**
- ☐ Always validate credentials

Reader Services TLS parameters

- ☒ Enable TLS encryption
- ☒ Enable TLS client mutual authentication
- TLS key: C:\Program Files (x86)\HID\Global\pivCLA...
- TLS key password:
- Browse filesystem for TLS key file...
- Generate TLS key file...

Reader Services clients

1 / 16 Reader Services reader licenses

Description	IP Address	Assurance Profile	Passage

Add... Modify... Remove

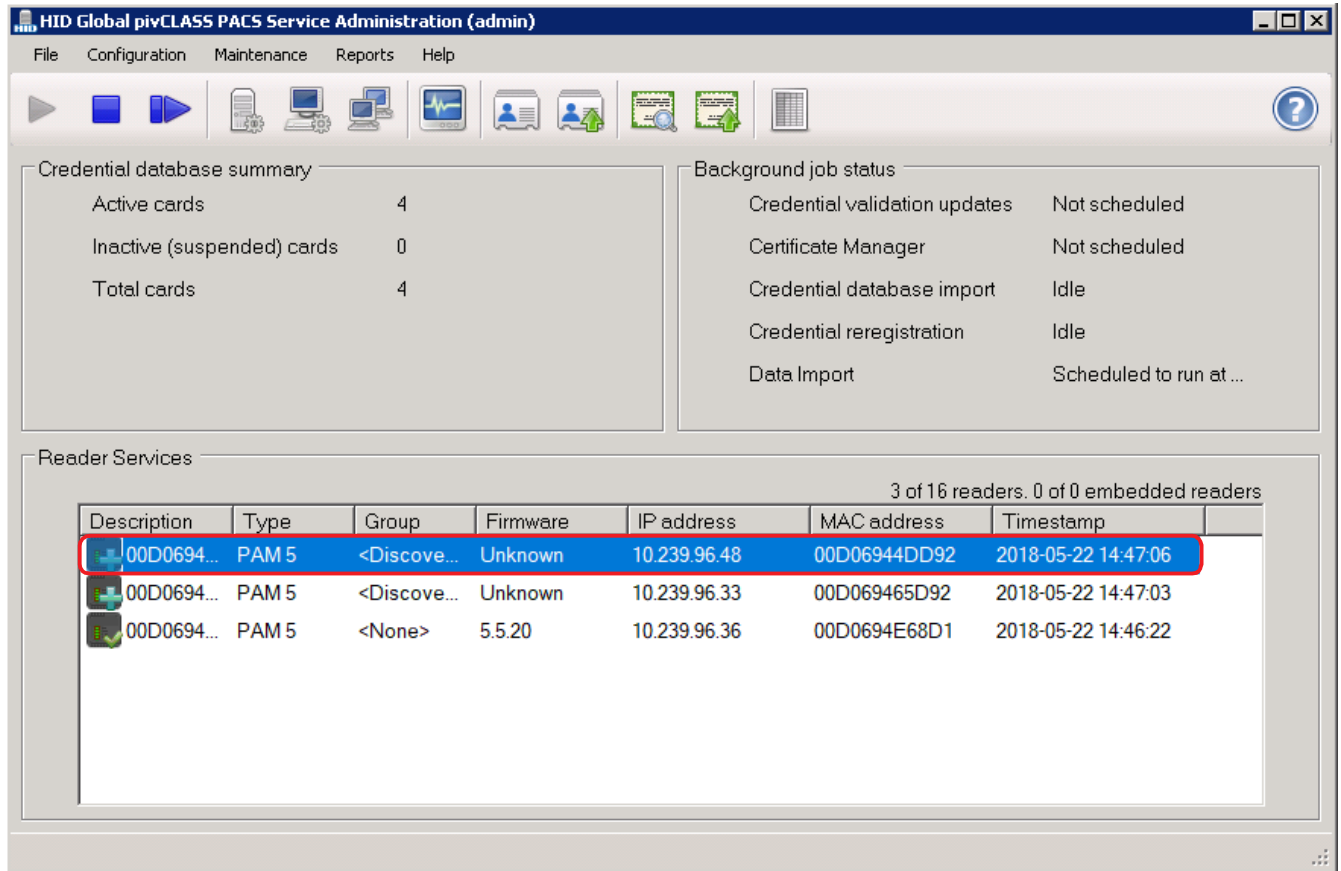
OK Cancel Apply

5.5.2 Add automatically discovered PAM

1. Install the PAM and power it on.
2. Start the PACS Service application.

Discovered PAMs are displayed in the **Reader Services** status window.

3. Double click on a discovered panel entry to launch the **Panel** form.



Credential database summary

Active cards	4
Inactive (suspended) cards	0
Total cards	4

Background job status

Credential validation updates	Not scheduled
Certificate Manager	Not scheduled
Credential database import	Idle
Credential reregistration	Idle
Data Import	Scheduled to run at ...

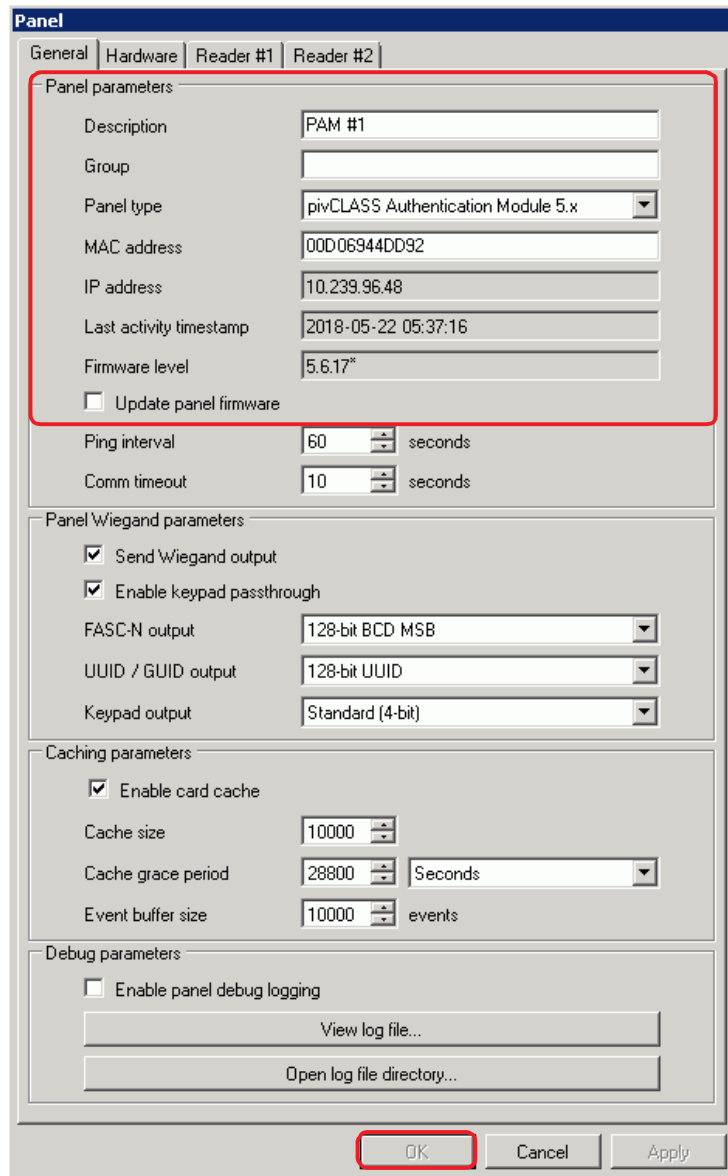
Reader Services

3 of 16 readers. 0 of 0 embedded readers

Description	Type	Group	Firmware	IP address	MAC address	Timestamp
00D0694...	PAM 5	<Discove...	Unknown	10.239.96.48	00D06944DD92	2018-05-22 14:47:06
00D0694...	PAM 5	<Discove...	Unknown	10.239.96.33	00D069465D92	2018-05-22 14:47:03
00D0694...	PAM 5	<None>	5.5.20	10.239.96.36	00D0694E68D1	2018-05-22 14:46:22

- On the **General** tab of the **Panel** form, enter the panel parameters and click **OK** to add the panel to the list of configured panels.

Note: Select the **Update panel firmware** option to indicate that the panel firmware should be updated when the panel is connected. The option is disabled if the panel already has the latest firmware level.



To modify any of the panel parameters, double click on the displayed panel entry in the **Reader Services** status window.

Note: For detailed information on panel configuration parameters, select F1 while on the **Panel** dialog box to access the relevant *PACS Service Online Help* topic.

Section 6

6 Troubleshooting

This chapter provides troubleshooting hints and tips if you encounter problems with your pivCLASS Authentication Module (PAM).

6.1 LED activity

The following table lists the LED indicators of the PAM.

LED	Purpose
POWER	Indicates power to the PAM is on/off. The LED turns GREEN when power is ON.
TAMPER	Indicates the tamper status. Normal (input shorted) is OFF. If the tamper line is activated (input is open), the LED turns RED. Verify the tamper circuit, or jumper the input if not used.
PW_FAIL	Indicates the power failure input status. Normal (input shorted) is OFF. If the power fail line is activated (input is open), the LED turns RED. Verify the power fail circuit or jumper if the input is not used.
FAULT	Indicates if the PAM is online with Reader Services. If the PAM is online then the LED is GREEN, if the PAM is offline/not configured then the LED turns RED.
READER1 READER2	Indicates the corresponding reader port is configured or in use. The LED will be off if the reader is not configured. If the reader is configured, the LED switches from solid green to solid red every 15 seconds while the PAM attempts to communicate with the reader. Once the PAM has successfully communicated with the reader, the LED blinks green, indicating that the PAM is polling for smart cards. When a card is detected, the LED briefly turns red while data is read from the card. Once card processing is complete, the LED returns to blinking green.
RS-485	Normal is OFF.

When the PAM starts:

- In non auto discovery mode: READER 1, READER 2 and RS-485 LEDs turn red, then off.
- In auto discovery mode: READER 1, READER 2 and RS-485 LEDs will light up in a three sequenced scanning pattern:
 - red slow scan (searching for a DHCP address)
 - red fast scan (searching for a PACS Service)
 - green fast scan (PACS Service found)

6.2 Resetting to factory defaults

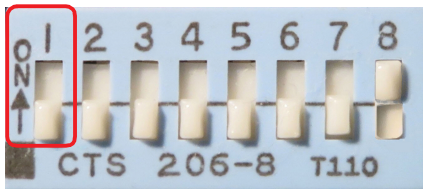


WARNING

Resetting the PAM to factory defaults permanently erases all configuration settings (including logs, keys and cached validation data). It also returns the module to the factory default IP address (192.168.0.222, with subnet mask 255.255.255.0). These changes are non-recoverable.

To reset the PAM to factory default settings, perform the following steps:

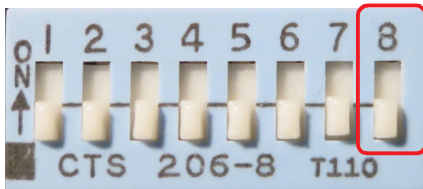
1. Remove power from the PAM.
2. Set DIP switch 8 to **ON** with all other switches **OFF**.



3. Apply power to the PAM, see *Section 4.8: Applying power*.
4. Wait until FAULT, READER 1, READER 2 and RS-485 LEDs flash red/green/red/green continuously. The PAM has successfully been reset to factory defaults.

To reconfigure the PAM, perform the following steps:

1. Remove power from the PAM.
2. Set DIP switch 8 to **OFF**.



3. Apply power to the PAM.
4. Configure the PAM, see *Section 5 PAM configuration*.

6.3 Troubleshooting configuration problems

If there are PAM operation problems, follow these steps to troubleshoot the problem:

- Examine the PAM configuration (**Setup Mode** page).
- Enable debug message logging and download the logs using the pivCLASS Reader Services.

Important: Enabling debug logging will cause a large increase in the size of the log file and a possible decrease in system performance. It is therefore recommended that debug logging should only be enabled for short troubleshooting periods and then turned off.

- Consult your provider.

6.3.1 Troubleshoot pivCLASS Reader Services communication

If the PAM is not communicating with the Reader Services, verify the following:

- The network cable is good between the module and the hub/switch/server.
- The Reader Services is up and running.
- The Reader Services IP address is correctly specified in the PAM **Setup Mode**.
- The Reader Services TCP port is correctly specified in the PAM **Setup Mode**.
- The PAM routes IP traffic to the pivCLASS Reader Services (contact your network administrator for assistance).
- SSL is enabled for PAM communications and that certificates are correctly installed on the PAM/Server.

6.3.2 Wiegand output problems

If the PACS panel is reporting **Invalid card format** or otherwise not recognizing a known and registered credential verify that the PAM is installed with the ground lug connected to earth ground or power supply ground, see *Section 4.7 Connecting to the power supply*.

6.3.3 Troubleshoot communication issues

The following provides information on possible issues that may cause breaks in communication between the PAM Rev. A (91000ABNNN and 91000ANNN) and the pivCLASS Service.

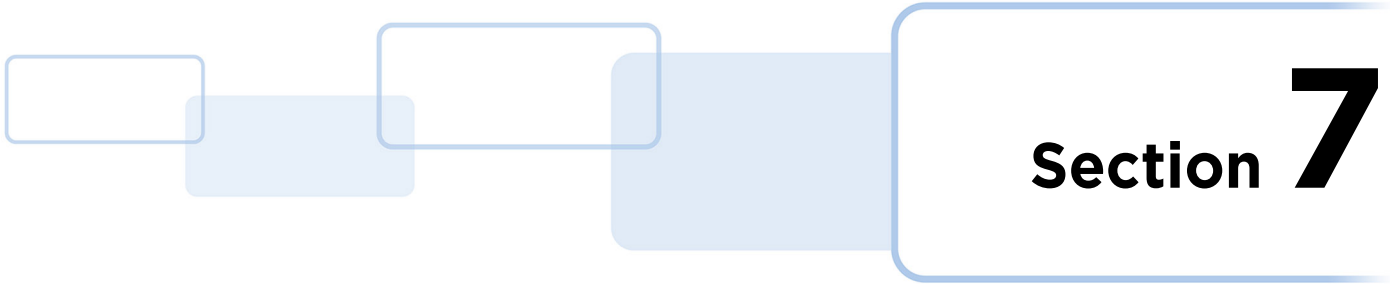
Note: PAM Rev. B (91000BBNNN and 91000BNNN) contain updates to address these issues.

Issue	Description	Solution/Workaround
Noise on power input to PAM	Some power sources are not well filtered and cause noise to be passed to the power input on the PAM. This noise then couples onto the Ethernet communications causing network communication issues.	Use a UL 294 rated PACS power supply as directed in the user manual and required by UL. Note: A linear or switching power supply with lossy linear post regulator filter is likely to provide the best results. We do not recommend the use of low cost two-prong switching supplies with very high noise and ripple i.e. exceeding 10%.
PAM ground lug not connected	The PAM is installed and the built in ground lug is not connected to an electrical ground causing a fluctuating ground reference on the system, primarily impacting the Ethernet communications.	Connect the ground lug to an electrical ground on the same circuit as the PAM power supply. Doing so will make sure the PAM is grounded and no ground loops are generated.

Issue	Description	Solution/Workaround
"Green" power dropping voltage	Newer Ethernet switches with "Green" power can cause a drop in line voltage for the Ethernet communications which a Rev A PAM was unable to handle.	If using a Rev A PAM, it is recommended to disable the "Green" or auto power negotiation for the port the PAM is connected to.
PoE capable switch is being used	The Ethernet port on the PAM is not compatible with PoE.	If using a Rev B PAM, it is recommended to turn off the POE power on the port being used. If using a Rev A PAM, turn off the POE capability for the port in the switch the PAM is connected to or use a switch without POE.
Gig-E switch fails to auto-negotiate	Gig-E/Gigabit Switch is used that does not successfully auto-negotiate speed connection with PAM.	Adjust the setting of the port the PAM is connected to a 10/100MB port. If issues are still encountered attempt to set the port to 100MB full duplex. If that does not result in improvements then utilize 10MB full duplex. If issues are still encountered it is recommended to try a different brand or model of Ethernet switch. Note: Testing showed no issues with business grade switches, similarly with consumer grade TRENDnet, NETGEAR, and 3Com switches. Issues were encountered with business grade D-Link and consumer grade Dell Gigabit switches. Worst case, use a 10/100 switch for the first connection from the PAM. Note: This applies to Rev A PAMs only. There are no known issues with Gig-E switches for Rev B PAMs.
Enterprise fibre-capable switch connections	Inability to connect to the PAM through multiple fiber channel connected switches.	Verify that the standard MTU is 1500 and that Port speed is set to 10/100.

6.4 Swapping a PAM

If for any reason you need to swap a PAM or the SD card, contact your Technical Support organization.



Section 7

7 Regulatory

The pivCLASS Authentication Module (PAM) is certified compliant with the following standards.

Federal Communications Commission (FCC) Part 15, Class A

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada

This device complies with Industry Canada ICES-003. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux ICES-003. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

UL 294 Access Control System Units

- Listed for use only within the protected area.
- Mount only in a UL 294 Listed sheet metal enclosure measuring not less than 16 x 16 x 3.5 inch (406 x 406 x 89 mm), such as the Bosch model D8103.
- A UL Listed Tamper switch must be used in the enclosure.
- The GPIO, Console and unused RS-485 ports were not evaluated by UL. No connections are supported.
- PAM has been evaluated for use with pivCLASS and iCLASS SE readers and EdgePlus Controllers.
- Connect only to a UL Listed ALVY or APHV, regulated, power limited power supply rated 12 to 24 V DC (with an output voltage range of 10.2 to 26.2 V DC), 1.2 Amp minimum.

CE Marking

HID Global hereby declares that this product is in compliance with the essential requirements and other relevant provisions of Directives 2014/30/EU (EMC) and 2014/35/EU (LVD).

