pivCLASS® PACS Service and MultiPACS Service

Administration Guide

PLT-03416, Rev. D.2

March 2019

Copyright

Trademarks

Contacts

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

Americas and Corporate	Asia Pacific
611 Center Ridge Drive Austin, TX 78753 USA Phone: 866 607 7339 Fax: 949 732 2120	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)	**Brazil**
Haverhill Business Park Phoenix Road Haverhill, Suffolk CB9 7AE England Phone: 44 (0) 1440 711 822 Fax: 44 (0) 1440 714 840	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

1 About this manual

1.1 Overview

This manual covers the installation and configuration of the following HID Global pivCLASS® solution software applications:

- pivCLASS® Physical Access Control System (PACS) Service.
- pivCLASS® Physical Access Control System (PACS) MultiPACS Service.

The document also provides PACS Service administration procedures and pivCLASS Authentication Module (PAM) configuration procedures.

1.2 Intended audience

This document is intended for personnel who are responsible for installing the pivCLASS PACS Service or pivCLASS MultiPACS Service applications and performing pivCLASS PACS Service administration tasks.

1.3 Information statements

The following information statements are used in this document to alert the reader to important information.

Important: This notice is used to highlight important information about hazards or actions that could potentially impact service performance, application functionality or successful feature configuration.

Note: This note is used to highlight information of interest that needs to be brought to the reader's attention.

1.4 Conventions used

1.4.1 Vocabulary conventions

The following vocabulary conventions are used throughout this document:

Term	Description/Meaning
PACS Service	Used to refer to the pivCLASS PACS Service and/or the pivCLASS MultiPACS Service.
PACS Service application	Used to refer to the pivCLASS PACS Service software application and/or the pivCLASS MultiPACS Service software application.

1.4.2 Typographical conventions

Typographical conventions used in this document are described in the following table:

Appearance	Description
Bold	Used to highlight GUI items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are involved in a procedure or user action. For example: **File** > **Exit** **..\pivCLASS PACS Service\templates\template.xml**
Italics	Used to refer to document titles and references, for example: *pivCLASS PACS Plug-in Template XML File Specification*.

`Courier`	Used for code fragments, for example:
	`<item>`
	`  <card>[ExistingBadge]</card>`
	`</item>`

<*italics*>	Angle brackets surrounding user supplied required values, for example: <*Server name*>
[text]	Square brackets surrounding user supplied optional values, for example: [your site location name]

1.5 Related material

pivCLASS PACS Service application help can be accessed by selecting **Help** > **View Online Help** from the **pivCLASS PACS Service Administration** window. For contextual help select the keyboard key **F1** while on a specific PACS Service application form to access the associated application help information.

pivCLASS PACS Service application documentation can be accessed by selecting **Help** > **View Documentation** from the **pivCLASS PACS Service Administration** window. You will be connected to the pivCLASS documentation site where pivCLASS related documentation can be opened.

Section 2

2 pivCLASS PACS Service

2.1 Overview

This section provides a brief description of the pivCLASS PACS Service and the pivCLASS MultiPACS Service. For more detailed information on each service solution, system requirements and deployment scenarios refer to the *pivCLASS Installation Overview Guide* (PLT-02750).

2.2 pivCLASS PACS Service

The PACS Service bundle consists of multiple sub-components:

- **PACS Service:** a TCP-based service that receives data elements extracted from smart card credentials
- **PACS Plug-in:** PACS-specific code that maps card data elements to PACS card and card holder fields

Available licensable options:

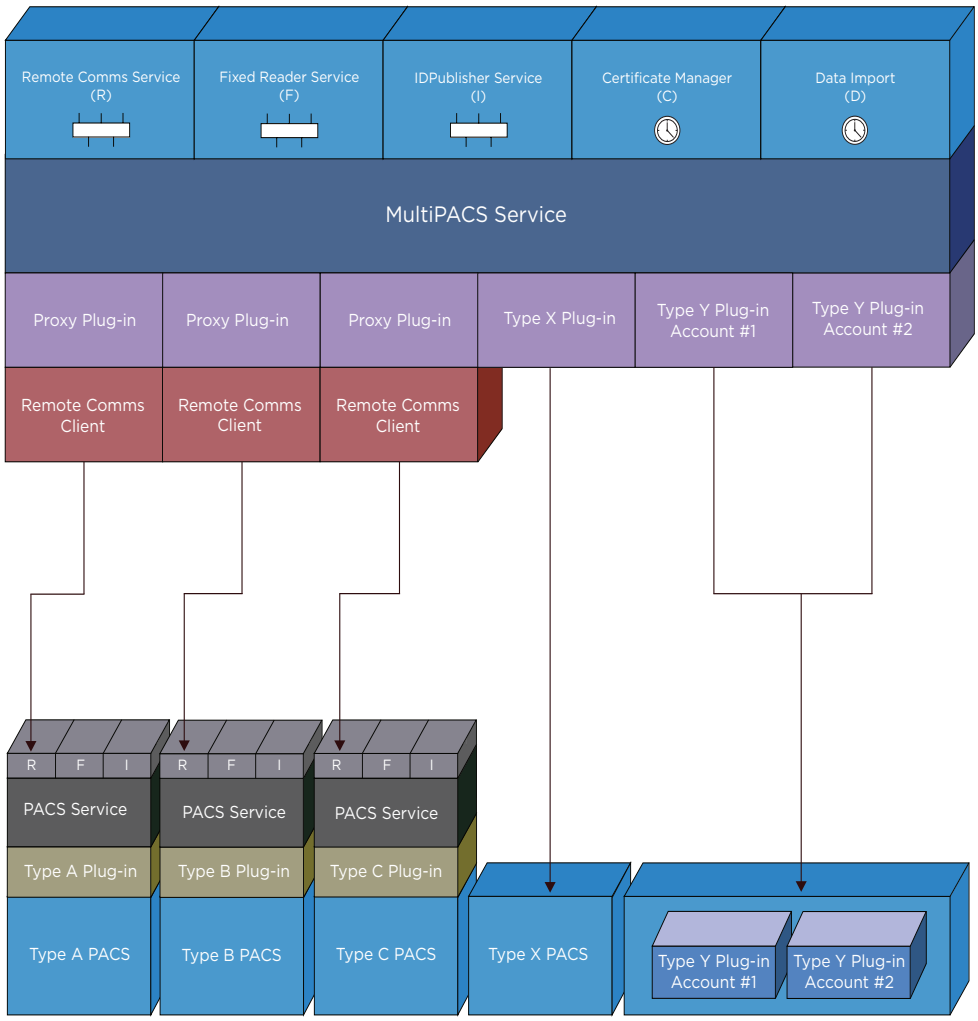
- **pivCLASS Certificate Manager:** an option that periodically re-validates the credentials that have been registered with a PACS and will suspend the PACS card's access, if needed. In most PACS, the status of a card or cardholder record changes, the access control panels are updated with this status. When a suspended PIV credential is presented to the reader, access is immediately denied. No new equipment or network drop is required at the reader.
- **pivCLASS Reader Service:** an option that provides a programmable interface to the pivCLASS PACS Service, enabling IP-based readers to request information related to a given FASC-N. Based on XML-RPC, the pivCLASS Reader Service module exposes a simple, secure API for card holder information requests, regardless of the PACS manufacturer.
- **pivCLASS IDPublisher:** this option obtains data from Human Resources Information Systems (HRIS), Identity Management Systems (IDMS), and/or Card Management Systems (CMS). It automates the provisioning and de-provisioning of users and credentials to over 25 different PACS, using a standardized web service interface.
- **Data Import:** an option that provides the ability to extract card data, access rights, user-defined cardholder information from the PACS so that it is available to pivCLASS Mobile Validator when a card is presented. Allows the operator to verify that a card is registered in the PACS and has appropriate access rights, which is ideal for use with proximity, MIFARE DESFire® and FIPS 201 cards.

2.3 pivCLASS MultiPACS Service

The MultiPACS Service bundle consists of the following sub-components:

- **Remote Communications Service:** handles all communications between pivCLASS Workstation and pivCLASS Mobile clients.
- **pivCLASS MultiPACS Proxy Plug-in:** communicates with a PACS (non-hosted) via a PACS Plug-in installed at the PACS server. A PACS Plug-in is the PACS-specific code that maps credential data elements to the PACS identity and credential fields.
- **Native PACS Plug-in:** a PACS Plug-in that is not shipped with the MultiPACS software, but is supplied to the security integrator during installation. The MultiPACS Service communicates with a hosted PACS via this PACS Plug-in.
- **Certificate Manager:** periodic credential re-validation.
- **Fixed Reader Services:** cryptographic support for fixed readers.
- **pivCLASS IDPublisher Service:** support for credential provisioning and de-provisioning by third-party applications.

The diagram below depicts the components of a MultiPACS system:



In the diagram the PACS servers designated **Type A**, **Type B**, and **Type C** are PACS configurations that require local file system or database access in order to register or suspend credentials. These PACS require an appropriate PACS Plug-in to be installed on the PACS server itself. The pivCLASS MultiPACS Proxy Plug-in exchanges data with the PACS Service at the remote end.

Type X PACS is a PACS that does not require access to its local resources. Its PACS Plug-in can be installed on the MultiPACS server.

Note: Native plug-ins are not shipped with the MultiPACS software installation package due to confidentiality constraints, however they can be obtained from HID Global support team during installation.**Type Y** PACS is a hosted system, typically partitioned by customer account or customer code. Like a **Type X** PACS Plug-in, a **Type Y** PACS Plug-in should be installed on the *M*ultiPACS server, and each plug-in must be configured with a different customer account or code.

2.3.1 Data import task

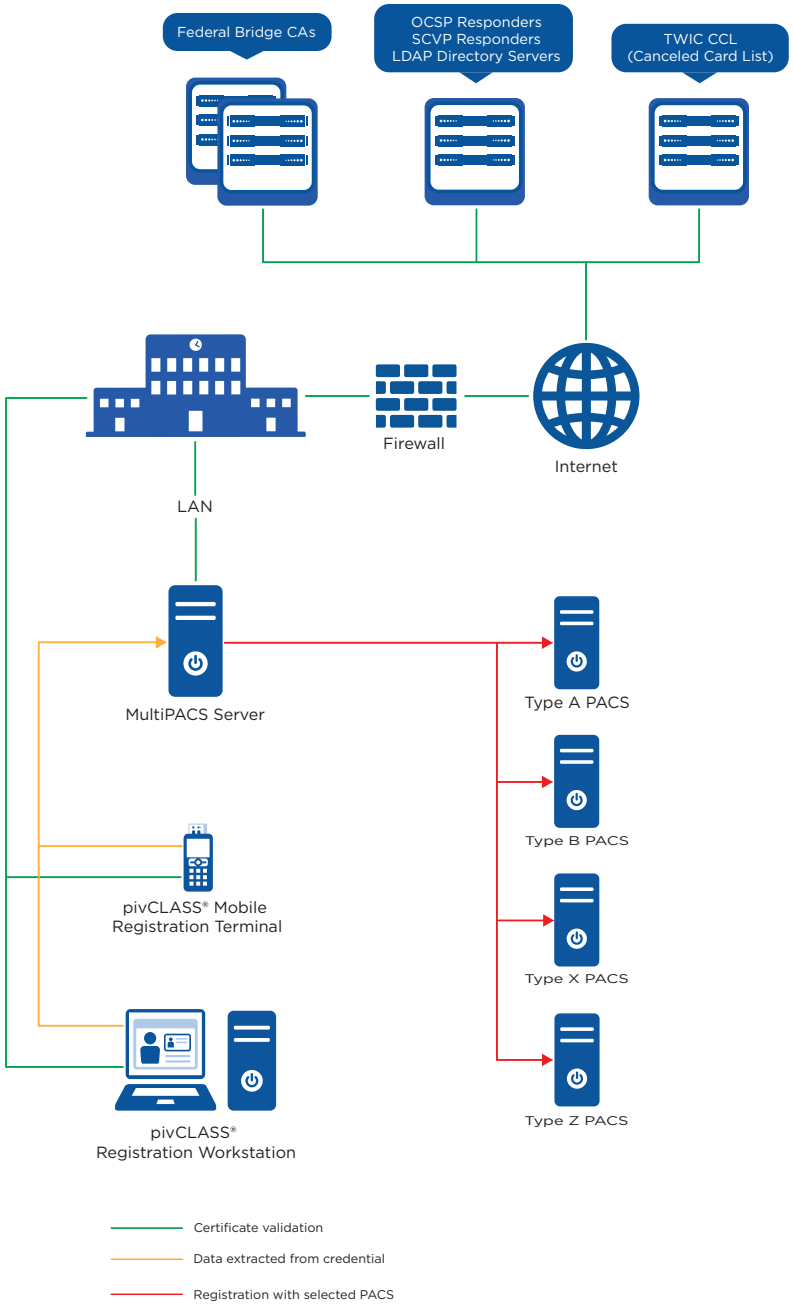
In a MultiPACS configuration, Data Import collects assignable access rights and credential active-inactive status information for credentials previously registered with each PACS, including those that were registered manually, via an IDMS feed, or another registration software product. The complete credential information, however, will only be present in MultiPACS if it was registered using pivCLASS Workstation, pivCLASS Mobile, or IDPublisher. Data Import can be executed manually or scheduled to run at periodic intervals.

2.4 MultiPACS deployment configurations

MultiPACS can be deployed in different configurations depending on the need of the customer.

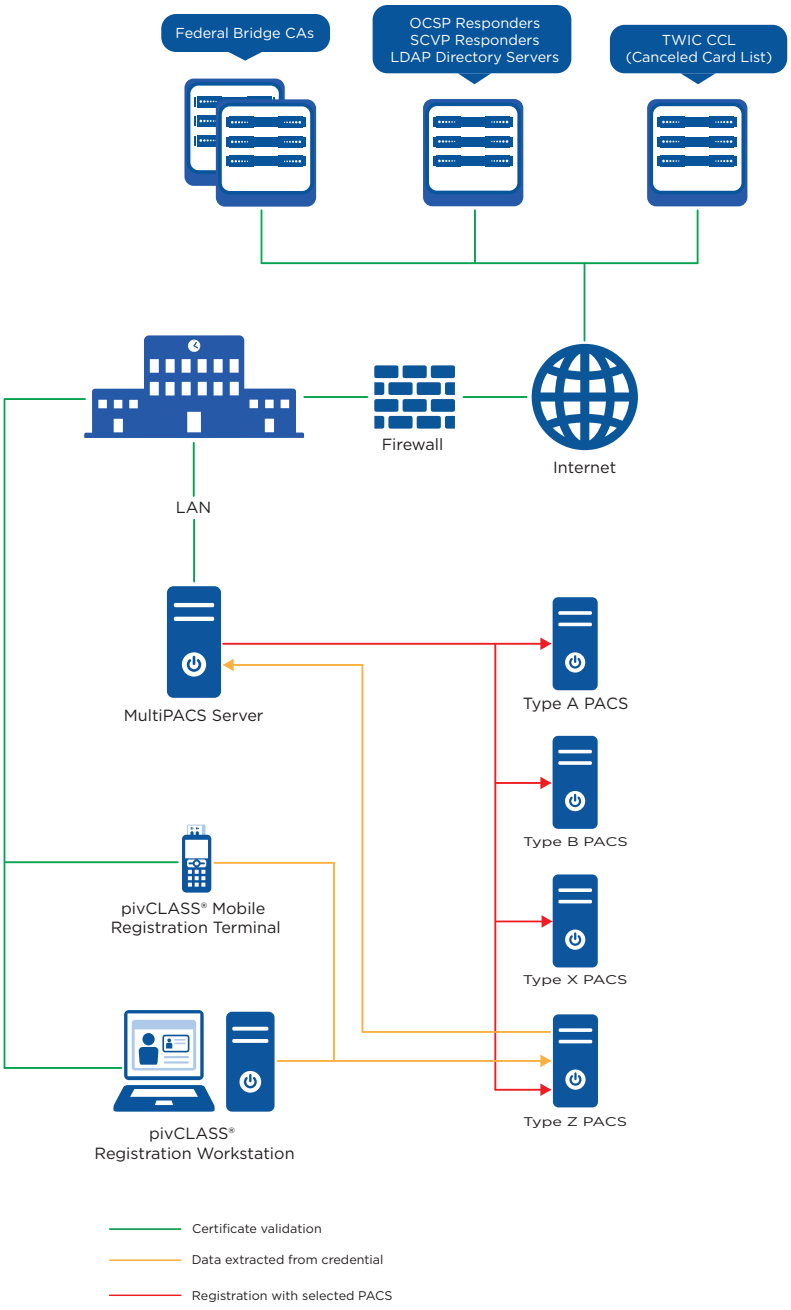
2.4.1 pivCLASS Workstation/pivCLASS Mobile Client-to-MultiPACS

When using this configuration, pivCLASS Workstation or pivCLASS Mobile clients, or both, send credential data to the MultiPACS server which in turn, pushes that data to the selected PACS.



2.4.2 pivCLASS Workstation/pivCLASS Mobile Client-to-PACS

Using the client-to-PACS configuration, pivCLASS Workstation or pivCLASS Mobile clients, or both, send credential data to a specific PACS, which forwards it to the MultiPACS server. The MultiPACS server in turn, broadcasts it to any other PACS configured to receive it.



2.4.3 MultiPACS template file

In a MultiPACS environment, where the deployment uses the same Physical Access Control System (PACS) at multiple different locations, the variables in each **template.xml** file must be modified so they are globally unique. Therefore, `Variable.1` for Location 1 cannot be the same as that used for Location 2.

In the example below, the table shows a list of template.xml file variables and a possible corresponding modified variable for use at each different location where the same PACS is deployed.

XML Template Variable	Modified variable Location 1	Modified variable Location 2	Modified variable Location 3
ExistingCardholder	ExistingCardholder.Loc1	ExistingCardholder.Loc2	ExistingCardholder.Loc3
PIN	PIN.Loc1	PIN.Loc2	PIN.Loc3
AccessRights.1	AccessRights.Loc1.1	AccessRights.Loc2.1	AccessRights.Loc3.1
AccessRights.2	AccessRights.2.Loc1.2	AccessRights.Loc2.2	AccessRights.Loc3.2
AccessRights.3	AccessRights.3.Loc1.3	AccessRights.Loc2.3	AccessRights.Loc3.3

For information regarding modifying variables and the correct formatting, refer to the *pivCLASS PACS Plug-in Template XML File Specification* (PLT-01629).

Section 3

3 Software install, uninstall, and upgrade

3.1 Installation overview

The following outlines the general process for installing the PACS Service application and upgrading the application with the purchased options.

1. Download the PACS Service application files from HID Global HTTP site. See *Section 3.2: Download files via HTTP*.
2. Install the application. See *Section 3.3: Install application*.
3. Initially configure the PACS service. See *Section 3.4 PACS Service initial setup*.
4. If required, upgrade the software license with purchased options. See *Section 3.6: Upgrade the PACS Service software*.

3.1.1 Installation and operational requirements

- The computer that hosts the PACS Service must support:
  - Microsoft Windows 10, 8.1, 7
  - Microsoft Windows Server 2016, 2012, 2008
- The PACs service must remain on a static IP or static Hostname with proper DNS routing and resolution if using panels (PAM or Embedded).

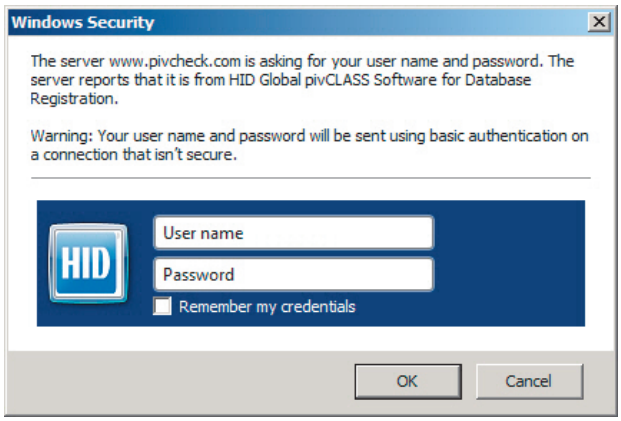
3.1.2 Security recommendations

The pivCASS PACS Service is initially installed to run as the Local System account, however the recommended best practice is to create a user, or user group, with a more restrictive set of security permissions that are sufficient to run the PACS Service. For information relating to the creation of a pivCASS PACS Service user or user group, see *Appendix C - Modify the PACS Service logon*.

3.2 Download files via HTTP

Perform the following steps to download the required application files:

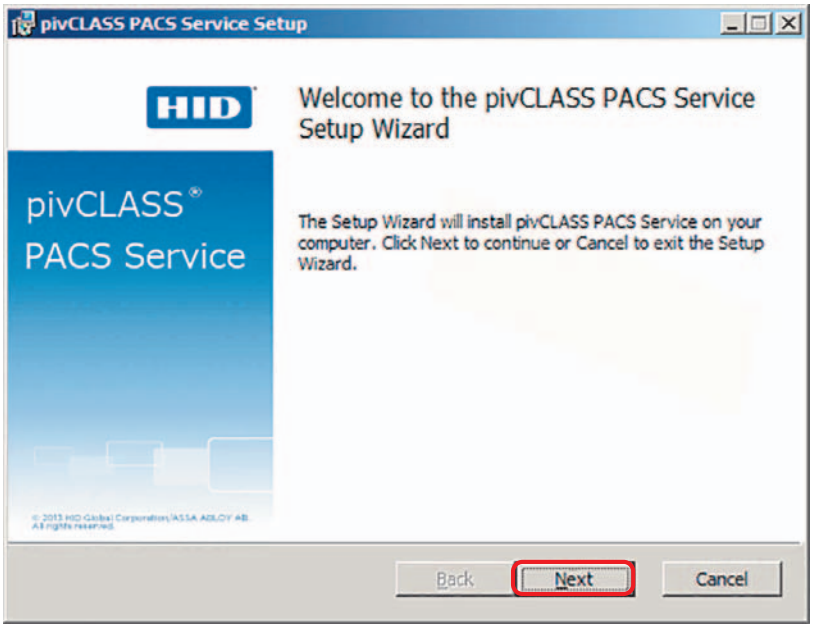
1. Open a web browser.
2. Enter the address provided in the entitlement email from HID Global. This address usually takes the form of:
   - For the PACS Service application: **http://www.pivcheck.com/<pacs name>**
   - For the MultiPACS Service application: **http://www.pivcheck.com/multipacs**
3. Enter the **Username** and **Password** provided in the entitlement email from HID Global.



4. A directory of files will be displayed. Scroll through the list and download the PACS Service application files listed in the email that apply to the configuration purchased.

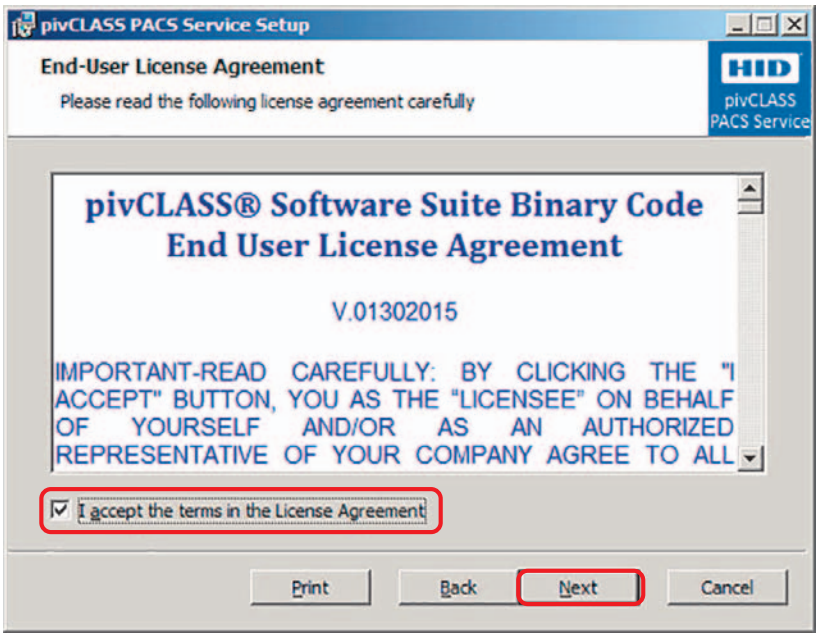
3.3 Install application

1. Double-click the downloaded PACS Service application executable file to start the Setup Wizard.
2. Click **Next** to begin the installation.

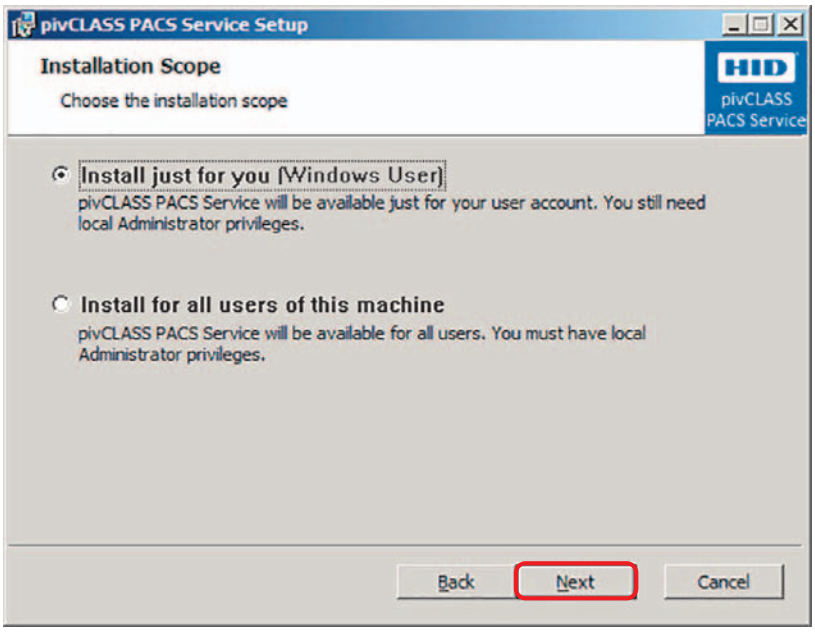


3. Read the License Agreement. Select **I accept the terms in the License Agreement**, and click **Next**.

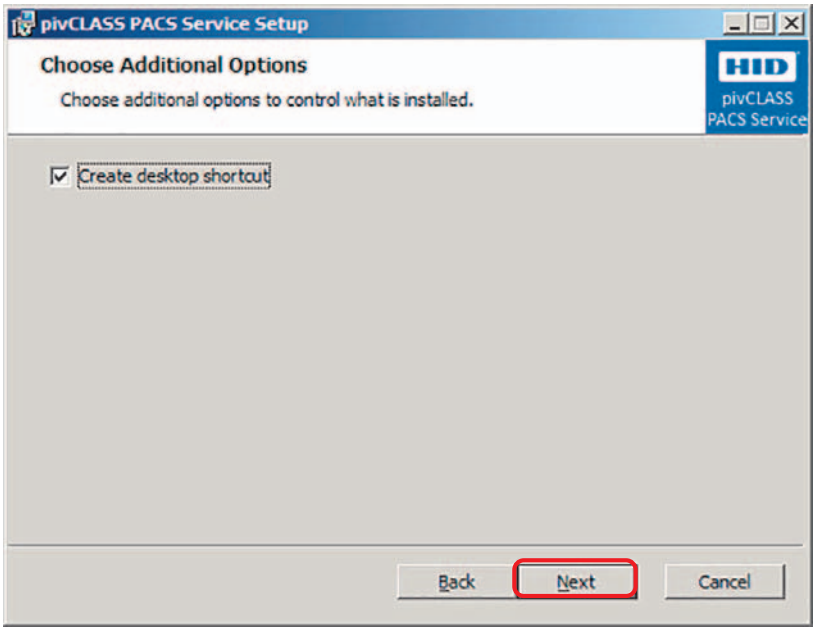
   Note: If you do not accept the license agreement, click **Cancel** to end the installation.



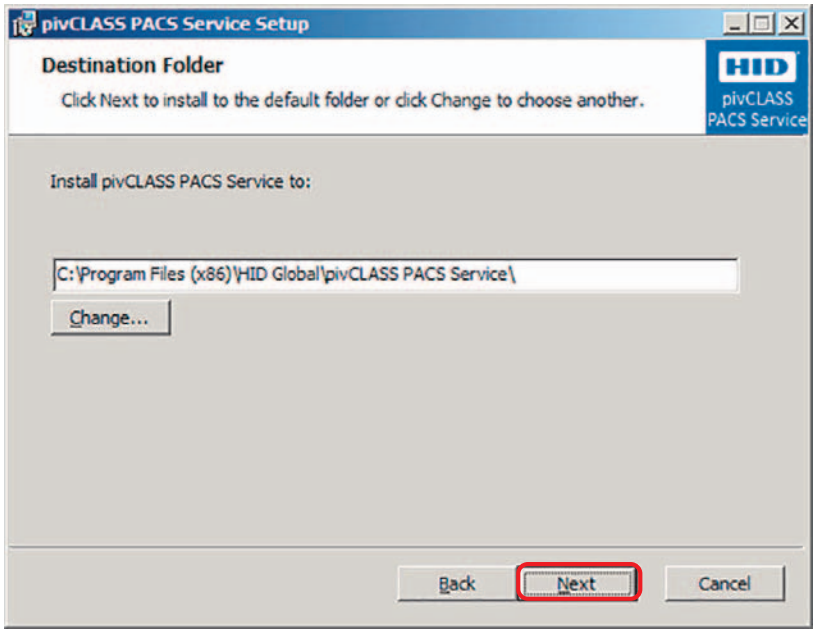
4. Select the **Installation Scope** option defined by your site administrator, and click **Next** to continue.



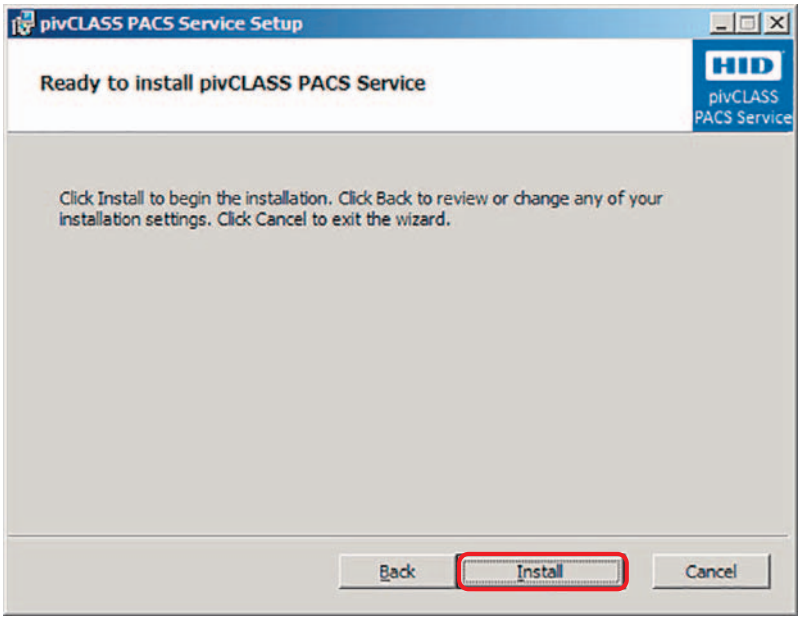
5. Select the **Create desktop shortcut** option if you want to create a pivCLASS PACS Service shortcut on your desktop. Click **Next** to continue.



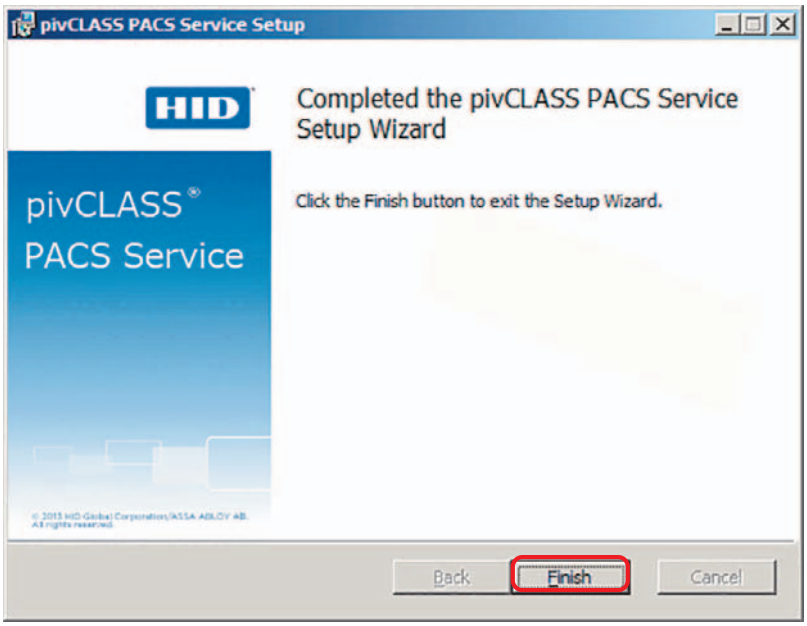
6. Set the install directory and click **Next**.



7. Click **Install**.



8. Click **Finish** to exit the Setup Wizard.



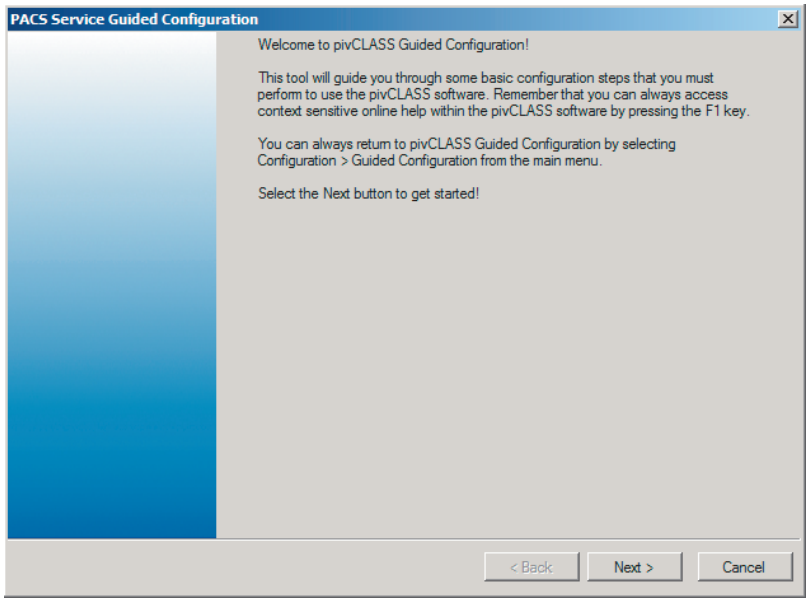
3.4 PACS Service initial setup

After software installation has finished a PACS Service Guided Configuration wizard will launch. This will guide you through basic pivCLASS configuration steps.

Note: To exit the Guided Configuration wizard you can select **Cancel** at any time during the configuration setup process.

Follow the instructions presented within the Guided Configuration wizard to:

1. Configure Admin user password and SSO (Single Sign-On)
2. Carry out PACS Service license download or manually enter the PACS Service license key
3. Configure PACS headend connectivity
4. View recommendations to further customize your PACS Service



To ensure your configuration options are valid, you will not be allowed to transition to the next step until the current step is successfully completed.

3.5 Install license key

The license key is bound to the computer it was initially generated from, therefore any changes to the hardware configuration (for example, motherboard, CPU) will result in the need for a new license key. In the scenario where the software is used in a VM and the VM hardware changes or the VM is moved to a different machine, please contact Technical Support (see Contacts section) and request for the license to be moved to the new configuration.

Note: A 30 day trial license can be installed if the system is unregistered. A trial license consists of a fully functional pivCLASS Validation Workstation allowing the user to evaluate card validation and biometric verification. However the trial version does not contain the license for the biometric matcher, and does not support PACS integration.

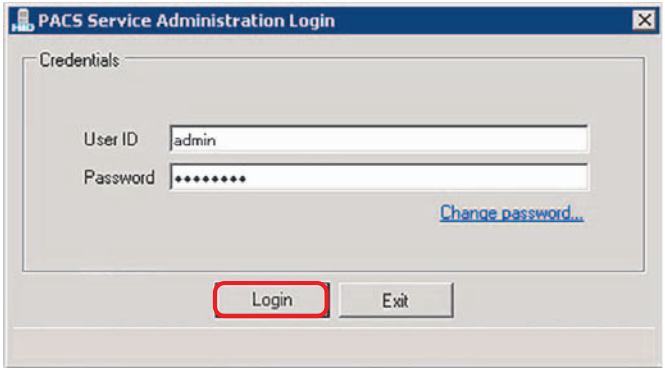
3.5.1 Register the PACS Service application System ID

In order to install and activate a permanent application software license the System ID of the pivCLASS PACS Service application firstly needs to be registered with HID Global. Once this has been done the license key can be downloaded or manually entered (depending on Internet availability) for access to purchased options and upgrades.

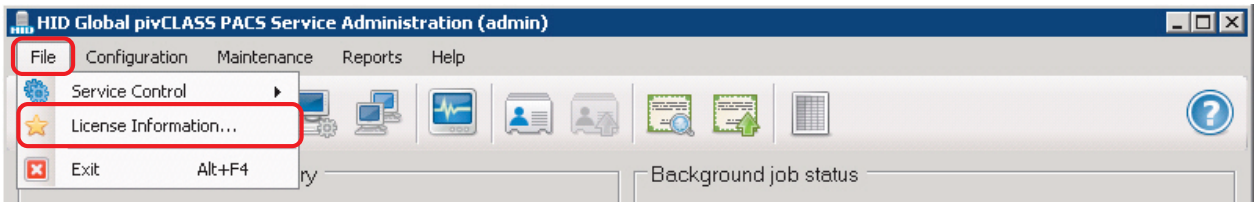
To register the System ID with HID Global:

1. Launch the PACS Service application.
2. On the login screen, enter the default User ID (*admin*) and Password (*password*).

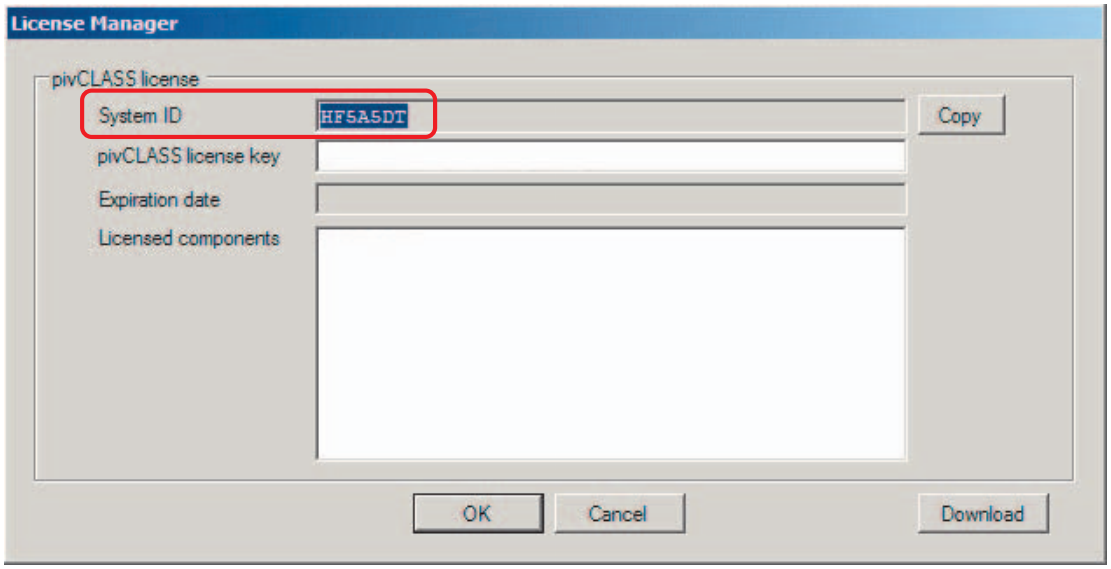
   Note: The default password should be changed as soon as possible for security reasons. See *Section 3.9 Change password*.
3. Click **Login**..



4. From the pivCLASS PACS Service application, select **File**> **License Information**.



5. In the **License Manager** window, make a note of the **System ID**



6. Email the following information to **pivCLASSSupport@hidglobal.com**
   - Name
   - Company
   - System ID (from the License Manager window)
   - Workstation System ID (if applicable)
   - End User/Customer Site Name as identified in the fulfillment email
   - End User/Customer location (city, state)
   - PO/SO number (if applicable)
   - PO/SO number of PAMs are on (if applicable for Reader Services)

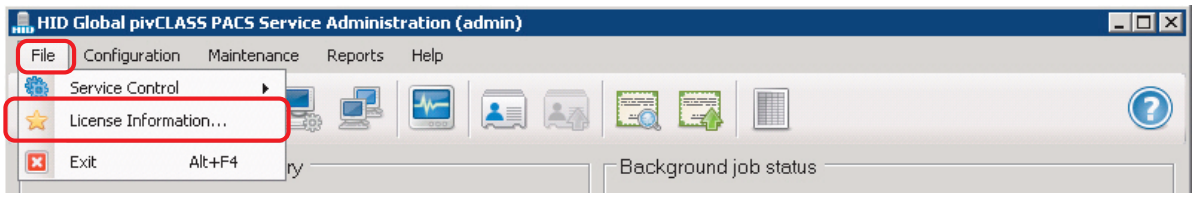
   Note: This information will be entered into the database with the System ID and License Key.

HID Global will send a confirmation email within a business day (although usually within a few hours), including a permanent license key along with any program options your site may have purchased.

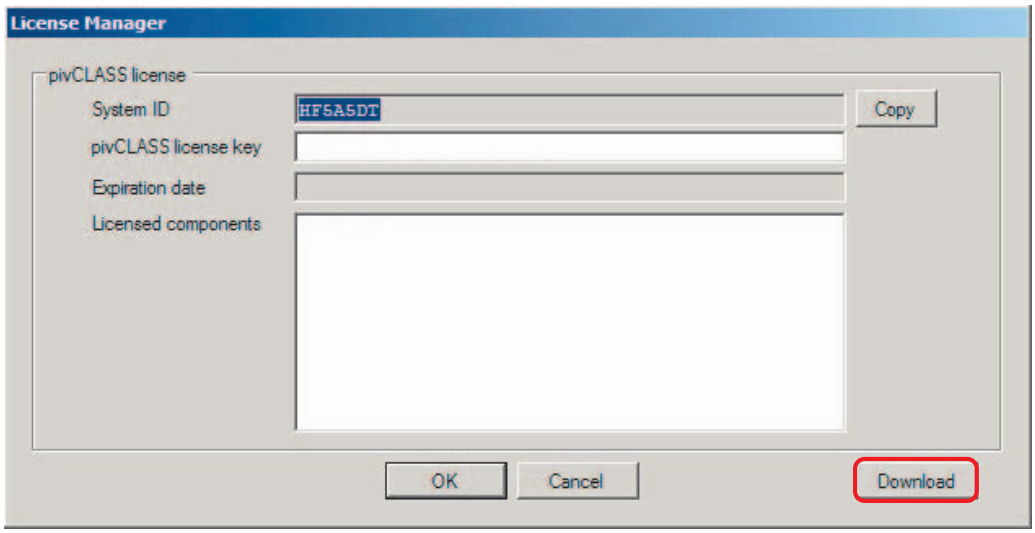
3.5.2 Download and install license key

Once you have received the license confirmation email from HID Global, if an internet connection is available, the license key can be downloaded and installed.

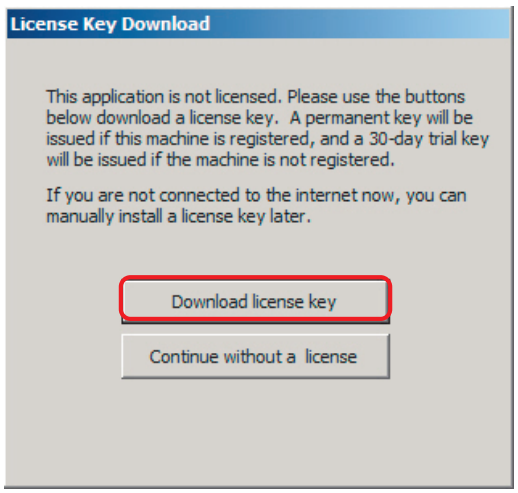
1. Launch the PACS Service application.
2. From the pivCLASS PACS Service application, select **File** > **License Information**.



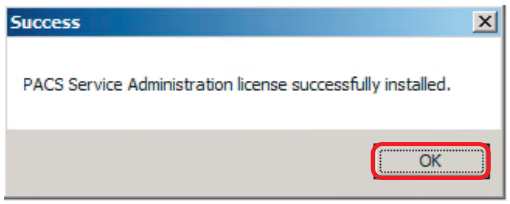
3. In the **License Manager** window, click **Download**.



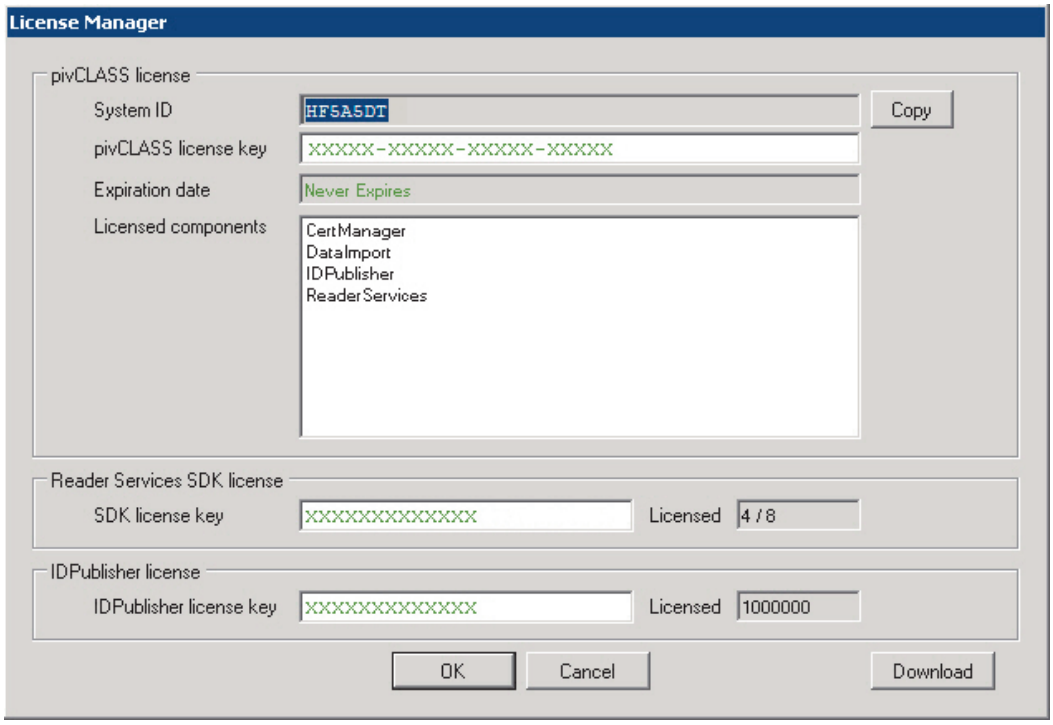
4. In the **License Key Download** dialog, click **Download license key**.



5. When the license key has installed, click **OK**.



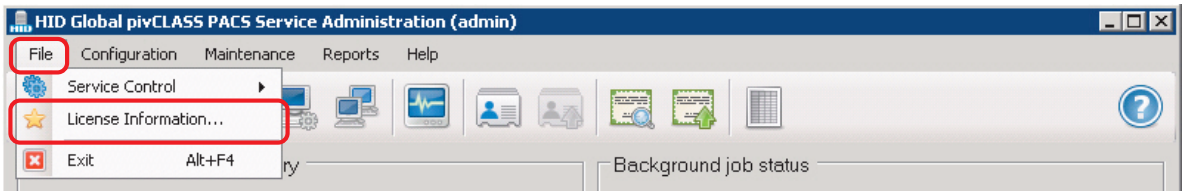
The full working version of the pivCLASS PACS Service and all the purchased option will be available.



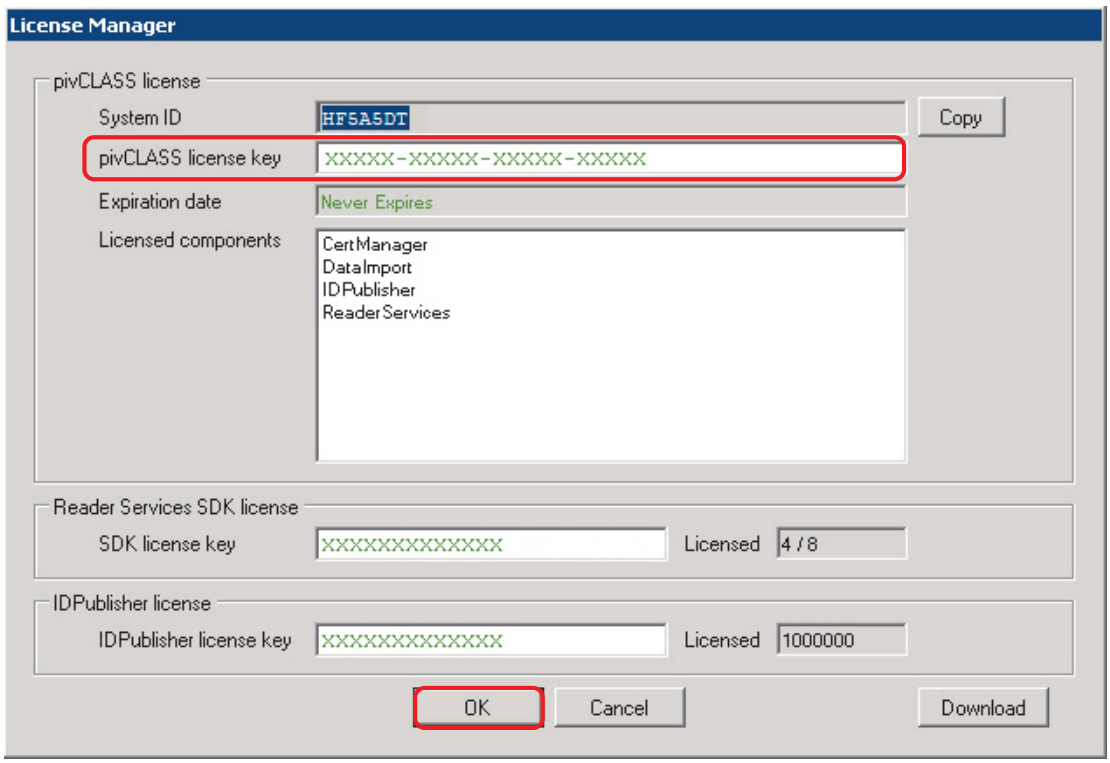
3.5.3 Manually enter license key

If no internet connection is available, you can manually enter the permanent license key contained in the confirmation email form HID Global.

1. From the pivCLASS PACS Service application, select **File** > **License Information**.



2. In the **License Manager** window, enter the permanent license keys provided by HID Global into the appropriate fields and click **OK**.



The full working version of the pivCLASS PACS Service and all the purchased option will be available.

3.6 Upgrade the PACS Service software

There are multiple ways to upgrade to the latest release of the PACS Service application. The method the user selects will depend upon network connectivity and whether the software is properly licensed. The user can:

- Request the PACS Service application to upgrade the software, see*Section 3.6.1 Software download*.
- Use a web browser to download the software installation files, see*Section 3.2 Download files via HTTP*, and install it manually.
- From a different machine with internet access, use a web browser to download the software installation files, see*Section 3.2 Download files via HTTP*. Copy the installation files onto a removable or network drive accessible by the machine the PACS Service is installed on, see *Section 3.6.2 Install an executable file from a removable or network drive*.

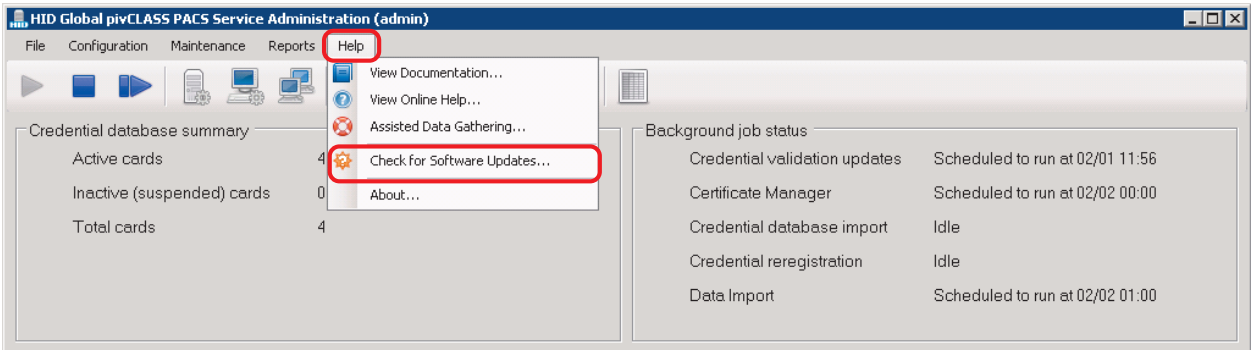
Note: The newest version of available pivCLASS PACS Service may not be FICAM approved for the system installed. If there is a requirement to use only FICM approved versions please refer to PACS Approved Product List to determine the correct version:

https://www.idmanagement.gov/approved-products-list-pacs-products/

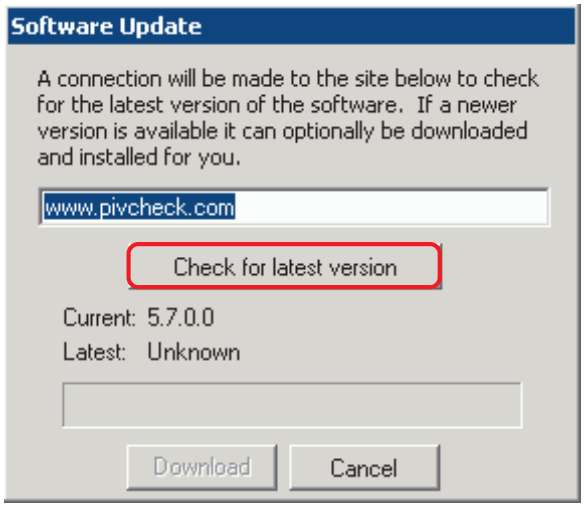
3.6.1 Software download

This method, requires an Internet connection and a licensed copy of the software (revision 1.1.5.0 or later).

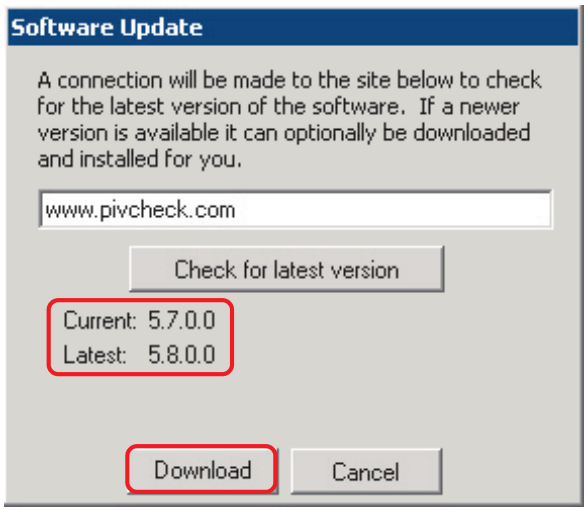
1. Select **Help** > **Check for Software Updates**.



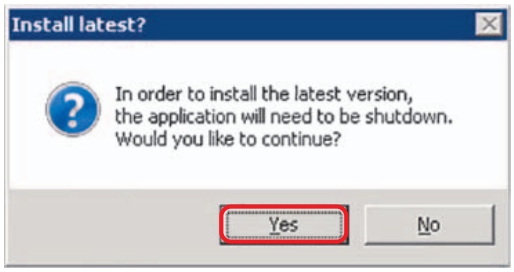
2. Click **Check for latest version**.



3. If a newer version is available, it will be displayed. Click **Download** to begin the process.



4. When the download is complete, click **Yes** to shutdown and restart the system.



5. The normal install will start, see *Section 3.3: Install application*.

3.6.2 Install an executable file from a removable or network drive

1. Copy the executable file onto the removable drive.
2. Insert the removable drive into one of the standard USB ports of your computer.
3. Double-click the Device icon within My Computer.
4. The removable drive will appear as a Hard Drive in this directory.
5. Double-click on the Hard Drive directory to reveal the pivCLASS PACS Service **.msi** file.
6. Copy the **.msi** file from the **My Computer\Hard Disk** directory to the My **Computer\Temp** directory.
7. Double-click the **.msi** file and follow the installation wizard instructions to complete the installation.

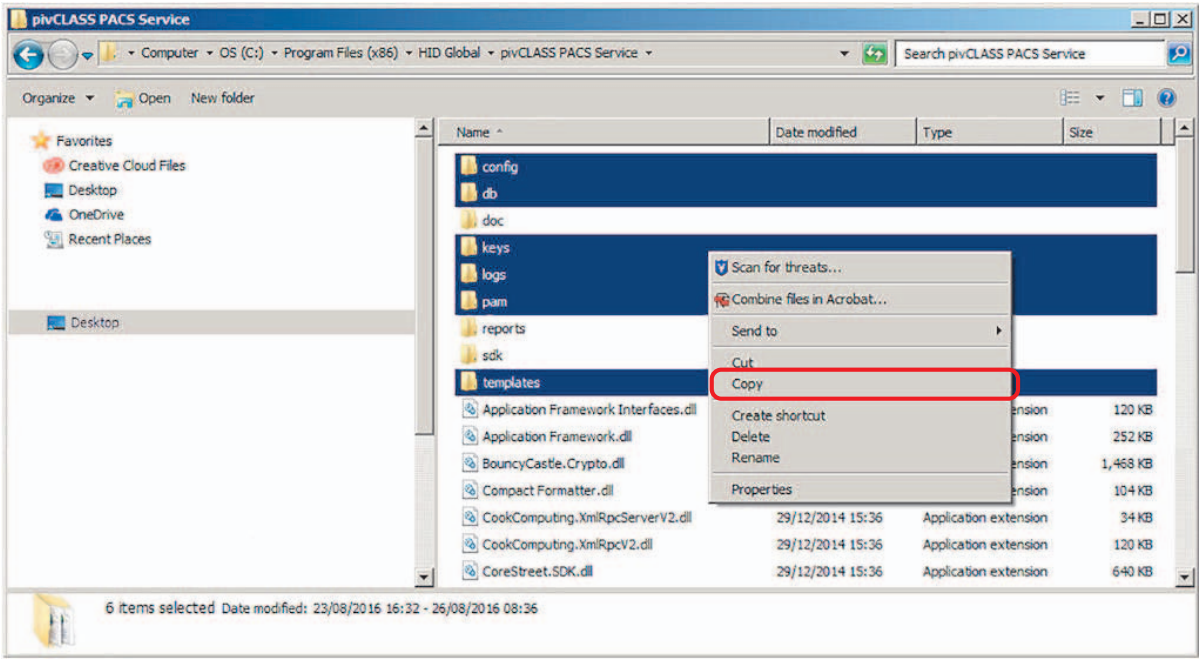
3.7 Apply saved configuration settings

The pivCLASS PACS Service allows the user to save and reuse configuration settings. The following procedure outlines how to save all of the settings for backup/recovery purposes or in order to have a mirror setup on another server.

1. Navigate to the directory where the PACS Service application is installed.

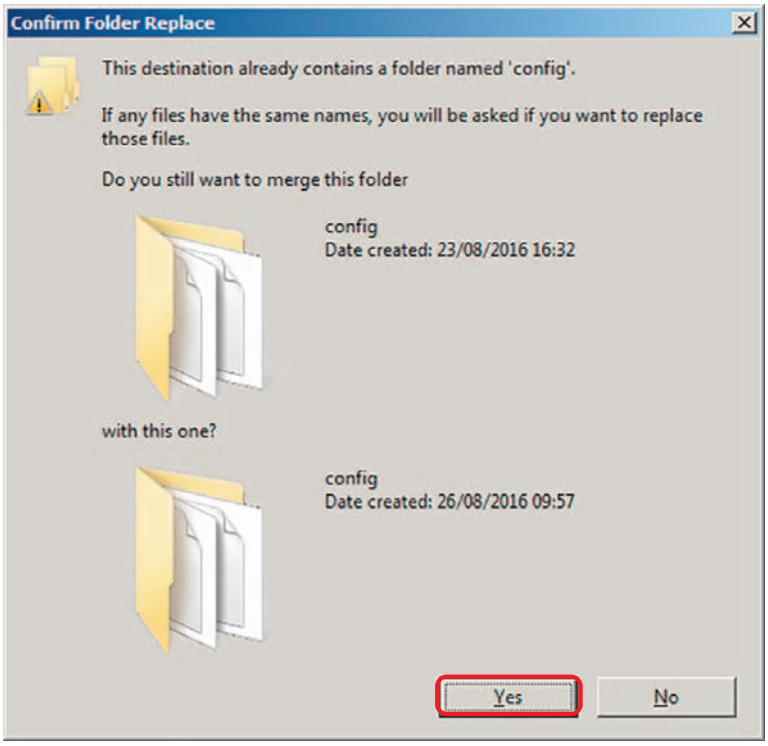
   Note: The default directory will differ depending on the operating system.

2. Select the following highlighted folders in the installation directory:
   - **config**
   - **db**
   - **keys**
   - **logs**
   - **pam**
   - **templates**
3. Right-click and select **Copy**.



4. Navigate to the new PACS Service application installation directory, and paste (**Ctrl-V**) the file(s).

5. Click **Yes** to confirm folder replacement. When the PACS Service is run the configuration settings will be applied.



3.8 Upgrading the PAM software from pre 5.x to 5.x

To upgrade the pivCLASS Authentication Module (PAM) software from pre 5.x to 5.x, there are two possible methods:

- Create an SD Card Image (requires a PC and SD card reader/writer)
- Order an upgrade kit from HID Global

3.8.1 Upgrade instructions

1. Power down the PAM
2. Remove the front panel
3. Remove the SD card from the PAM (located on the top right)
4. Update the firmware on the SD card. See *Section 3.8.2: Creating a SD Card image* for details
5. Replace the card in the PAM
6. Power up the system

3.8.2 Creating a SD Card image

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

1. Install the following tools:
   - 7-zip from: http://7-zip.org/download.html
   - HDD Raw Copy Tool from: http://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:

   http://www.pivcheck.com/*<folder>*/firmware
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 2 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. Double-click the file.
8. Click **Continue**.
9. Select the SD card as the destination.
10. Click START to begin the sector copy.
11. When complete, the SD card can be removed and is available for use in a PAM.

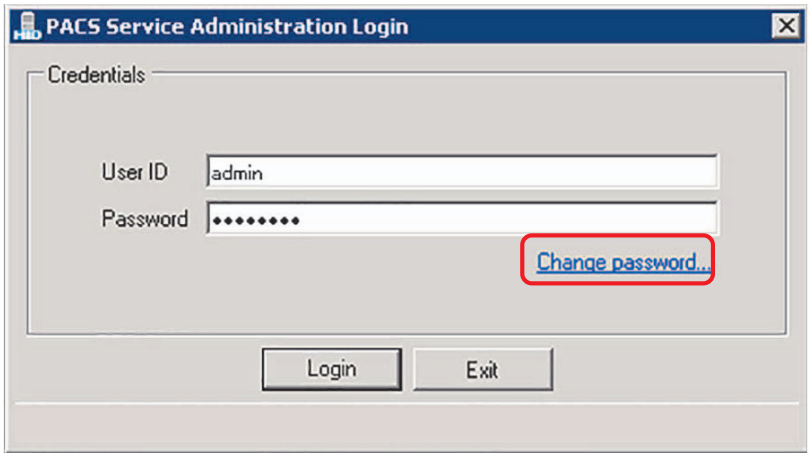
    Note: After booting, the PAM will be returned to factory defaults.

3.9 Change password

The Admin password should be changed immediately for security reasons.

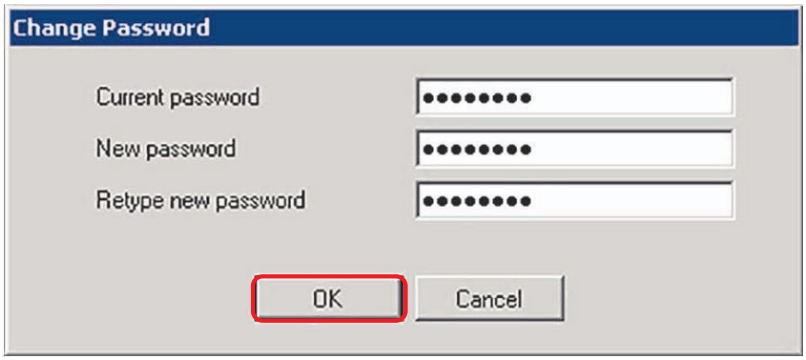
To change a password:

1. Launch the PACS Service application.
2. On the **PACS Service Administration Login** window, click **Change password**.



3. Enter the **Current Password**, and **New Password** (twice to confirm).

   Note: Password must be a minimum of 8 characters.
4. Click **OK**.



3.9.1 Reset password

To reset your pivCLASS PACS Service password if it is lost or forgotten:

1. Try to log into the PACS Service application using the default User ID and Password:
   - User ID: **admin**
   - Password: **password**
2. If the default user User ID and Password does not work then delete the **settings.bin** file to return the application to initial installation defaults.

WARNING
Deleting the settings.bin file will return the PACS Service application to initial installation defaults. All previous stored settings will be lost.

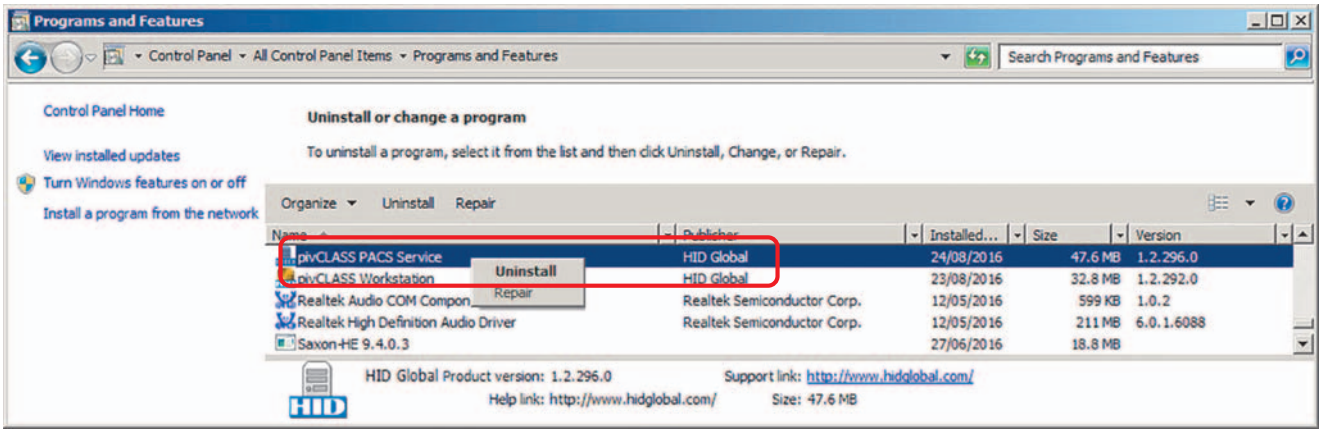
1. Stop the PACS Service application.
2. Browse to the PACS Service application **config** folder, normally:

   C:\Program Files (x86)\HID Global\pivCLASS PACS Service\config
3. Delete the **settings.bin** file (contains all pivCLASS PACS Service settings).
4. Log into the PACS Service application using the default User ID and Password:
   - User ID: **admin**
   - Password: **password**
5. For security reasons change the default login password, see*Section 3.9 Change password*.

3.10 Uninstall PACS Service software

To uninstall the PACS Service application:

1. Select **Start** > **Control Panel**.
2. Double-click **Programs and Features**.
3. Right-click **pivCLASS PACS Service**, and select **Uninstall**.
4. Click **Yes** to verify the uninstall.



This page is intentionally left blank.

Section 4

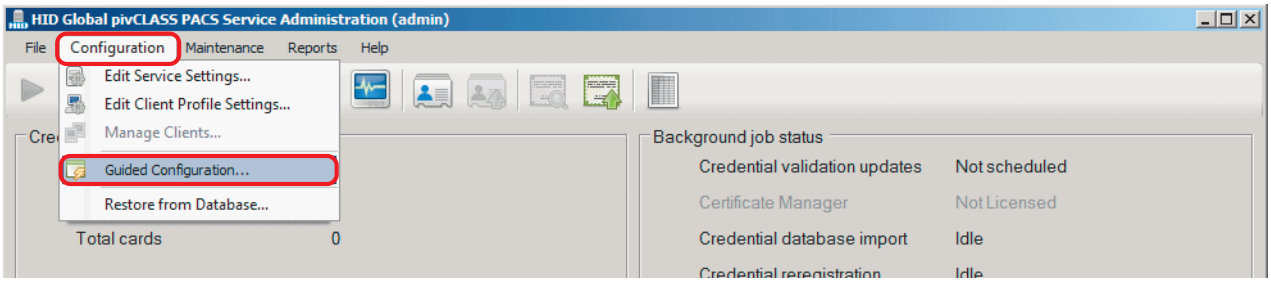
4 pivCLASS PACS Service administration

4.1 Overview

This section provides administration procedures used to run, configure and maintain the PACS Service. For detailed information on the PACS Service application user interface, configuration screens and configuration parameter groups refer to the PACS Service application help.

4.2 PACS Service Guided Configuration

Although the PACS Service Guided Configuration wizard will start when the PACS Service application is initially started, you can access the Guided Configuration wizard at any point by selecting **Configuration** > **Guided Configuration** from the PACS Service application main menu.



Follow the instructions presented within the Guided Configuration wizard to guide you through the most basic pivCLASS configuration steps:

1. Configure Admin user password and SSO (Single Sign-On)
2. Carry out PACS Service license download or manually enter the PACS Service license key
3. Configure PACS headend connectivity
4. View recommendations to further customize your PACS Service

To ensure your configuration options are valid, you will not be allowed to transition to the next step until the current step is successfully completed.

Note: To exit the Guided Configuration wizard you can select **Cancel** at any time during the configuration setup.

4.3 Credential database configuration

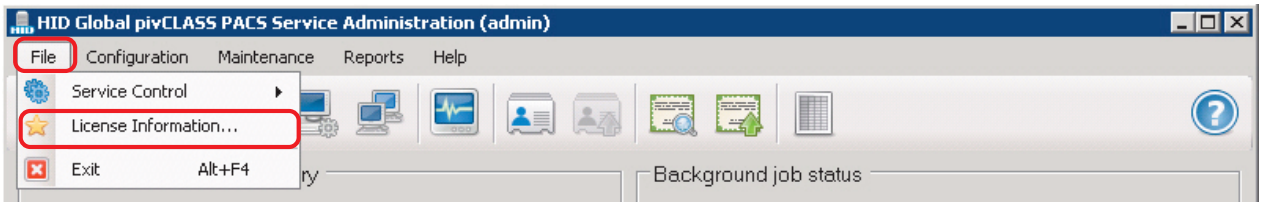
4.3.1 Restore the PACS Service configuration from an existing database

The PACS Service automatically backs up all configuration files and stores them in the Credential Database when changes are made. This includes the **settings.bin** file, **template** file, **PAM configuration** files, etc.

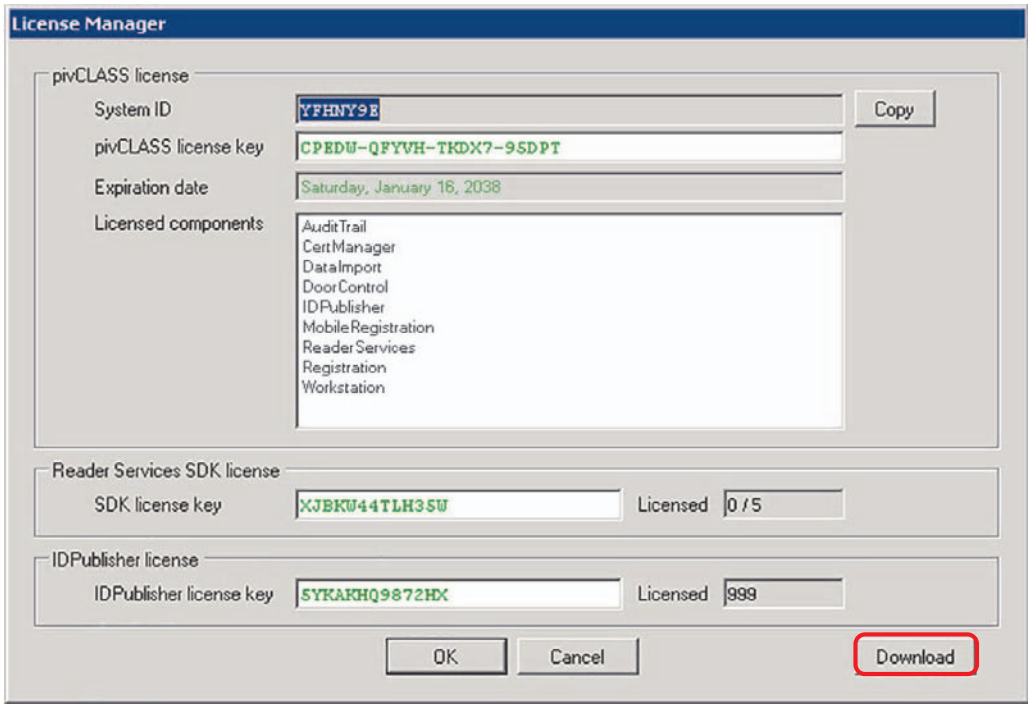
Important: Make a backup of the original working pivCLASS database before continuing with the following procedure.

The following procedure assumes PACS Service application is installed on a new machine from scratch and that an existing credential database has been configured at the host.

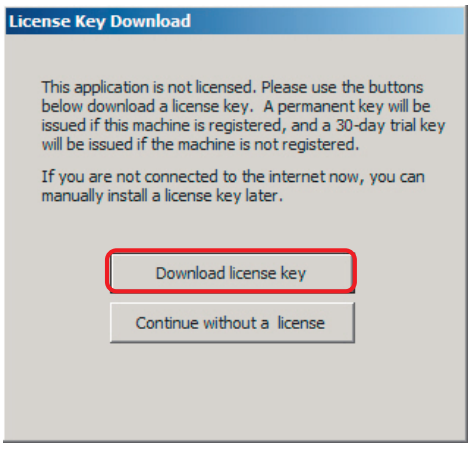
1. Launch the PACS Service application.
2. Go to **File** > **License Information**.



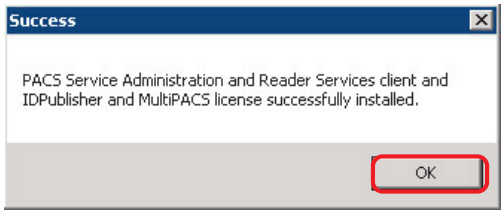
3. In the **License Manager** window click **Download**.



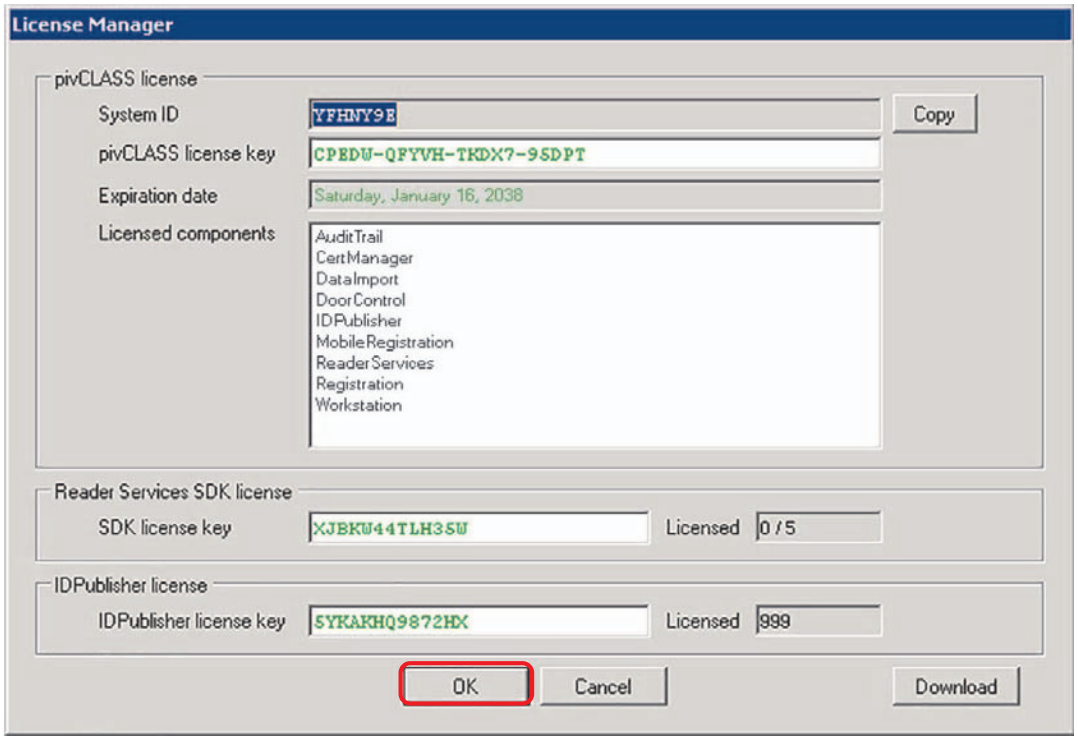
4. Click **Download license key**.



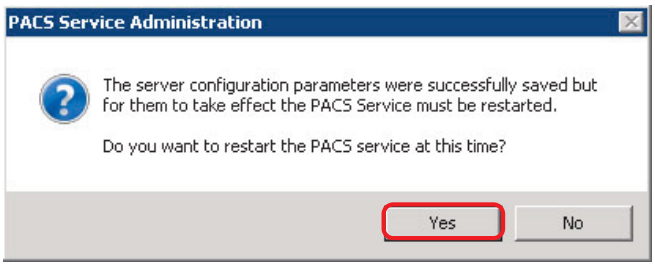
5. Once the License Key install is complete, the **Success** window will display. Click **OK**.



6. In the **License Manager** window, click **OK**.



7. Click **Yes** to restart PACS Service.

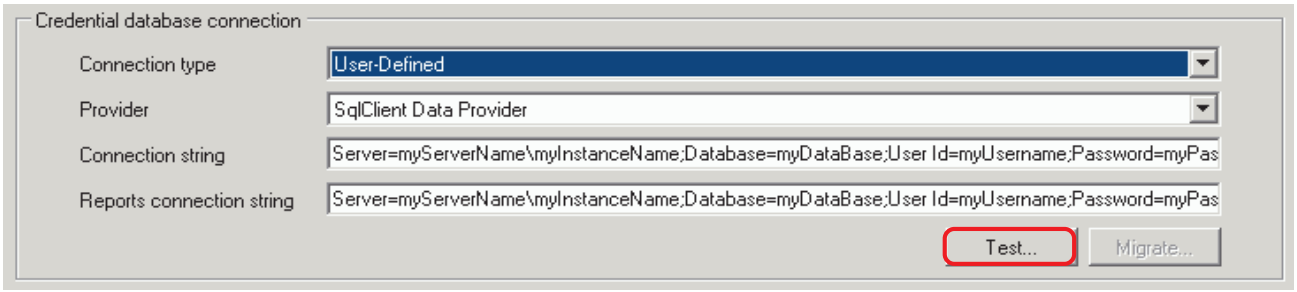


8. To configure the PACS Service to point to an existing credential database, in the **PACS Service Administration** window select, **Configuration** > **Edit Service Settings**.
9. On the **Application** tab, in the **Credential database parameters** section, select a **Connection type** from the drop-down list and, if prompted, enter the settings associated with the connection type.

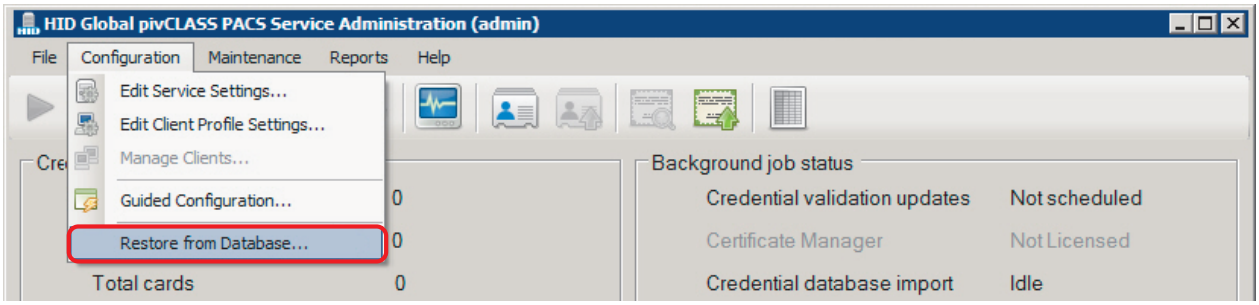
   Note: For a full description of connection type settings, while on the **Application** tab, select the keyboard key F1 to access the relevant *pivCLASS PACS Service Application Online Help*. For more information on database connection, see *Section 4.3.2 Credential database connection*.

10. Click **Test** to verify the connection.

    If successful a message states that the database settings have been validated. Click **OK**.



11. In the **Server Configuration** window, click **OK** to accept the new settings.
12. Select **Configuration** > **Restore from Database**.



13. When prompted click **Yes** to restore the configuration files from the database.

    The PACS Service will now be running with a previously working configuration.

4.3.2 Credential database connection

Although the pivCLASS PACS Service is provided with a *Firebird* open source database installed this should only be used for test and evaluation purposes and is not recommended for normal PACS Service operational environments.

In order to setup a different database provider you must first, create an empty database, select an appropriate data provider, and define a connection string to access that database. PACS Service access to this database should include database administrative rights, since tables will need to be created, altered, and dropped over the lifetime of the system.

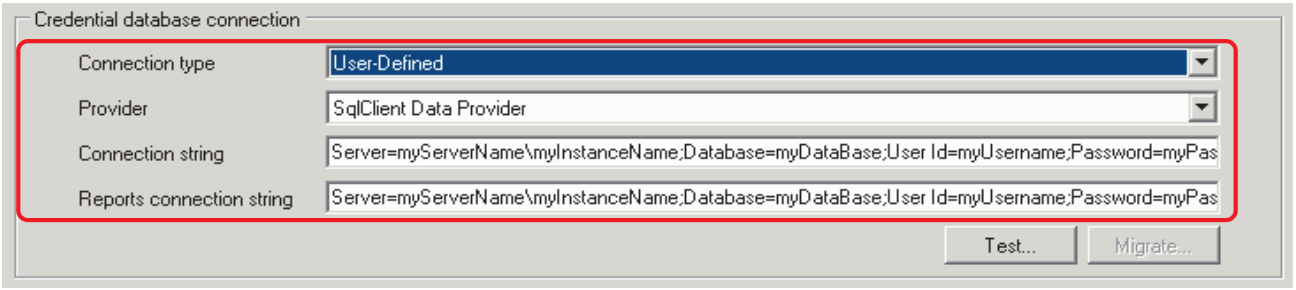
Many PACS ship with a database server instance installed. pivCLASS has been certified to co-locate its database on the PACS server instance. Simply create an empty pivclass database within the PACS database server instance.

Note: If your PACS does not use Microsoft SQL Server, and you do not have access to Microsoft SQL Server Standard or Enterprise Edition, we suggest that you download and install Microsoft SQL Server Express with Management Studio. For download and installation instructions, see the following URL:

http://www.microsoft.com/express/database/

Credential database connection settings

For a full description of connection type settings, while on the **Application** tab, select the keyboard key F1 to access the relevant *pivCLASS PACS Service Application Online Help*.



Connection type:

- **Firebird:** The default Firebird database parameters are used. No additional configuration information is required. The Firebird database should only be used for test and evaluation purposes. It is not recommended for normal PACS Service operational environments.
- **Microsoft SQL Server:** This connection type prompts for basic connection information for SQL Server connectivity. Separate authentication options are available for reports so the PACS Service can execute reports under a different database user with restricted permissions.
- **User-Defined:** This connection type prompts you to select the desired database provider and enter your own database connection string and reporting database connection string.

  Note: While on the **Application** tab select the keyboard key F1 to access the relevant *pivCLASS PACS Service Application Online Help* topic and a description of the settings for each **Connection type**.

Provider: Serves as a bridge between and application and a data provider. Select a data provider from the drop-down list to set up a database connection.

Connection string: Enter the connection string for the selected provider. This contains the information that the provider needs to know in order to establish a connection to the database. For example, connecting to a SQL Server instance:

```
Server=myServerName\myInstanceName;Database=myDataBase;User Id=myUsername;Password=myPassword;
```

For more information about connections strings and connection string examples, refer to:

https://www.connectionstrings.com/

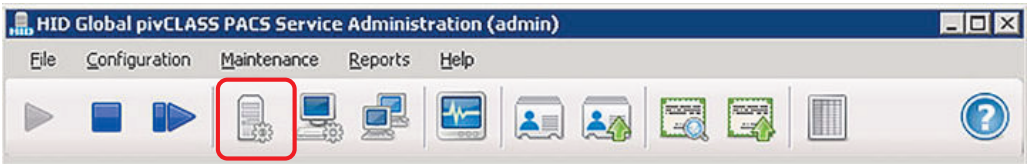
Reports connection string: An additional reports database connection string can be entered for the specified database provider. The the PACS Service will use this connection string to execute reports. A blank entry configures the PACS Service to use the connection string specified in the **Connection String** field.

4.3.3 Modify the PACS Service log on

The PACS Service is initially installed to run as the Local System account. In some instances a temporary administrative account is created for installations and may not have the appropriate access to the database. To assure the correct access is used to connect to the database you can use the Window Services applet to configure the PACS Service with the desired account logon credentials. See *Appendix C - Change the PACS Service user account logon*.

4.3.4 Configure PACS Service to point to an existing credential database

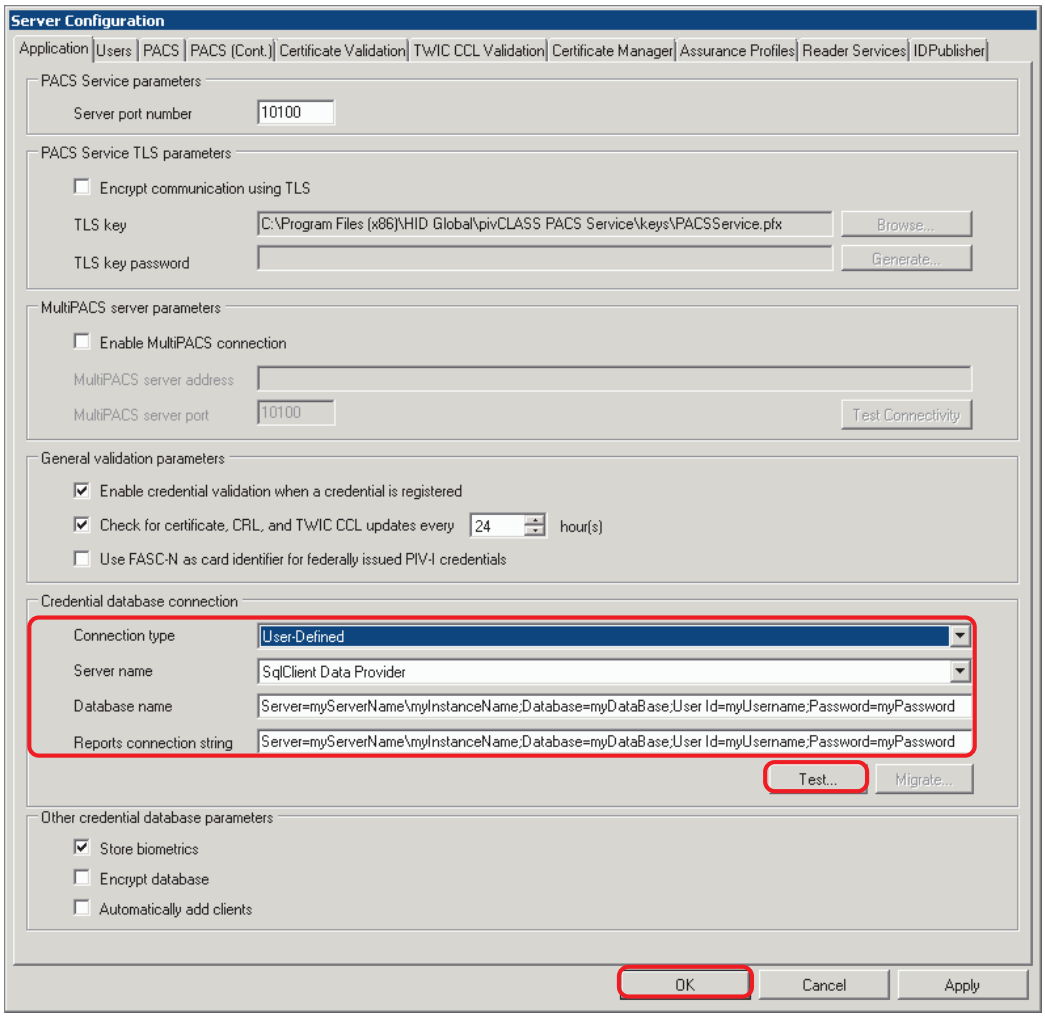
1. In the **PACS Service Administration** menu bar select the **Configure PACS Service** icon.



2. In the **Server Configuration** window select the **Application** tab.
3. In the **Credential database parameters** section, select a **Connection type** from the drop-down list and, if prompted, enter the settings associated with the connection type.

   Note: For a full description of connection type settings, while on the **Application** tab, select the keyboard key F1 to access the relevant *pivCLASS PACS Service Application Online Help*. For more information on database connection, see *Section 4.3.2 Credential database connection*.

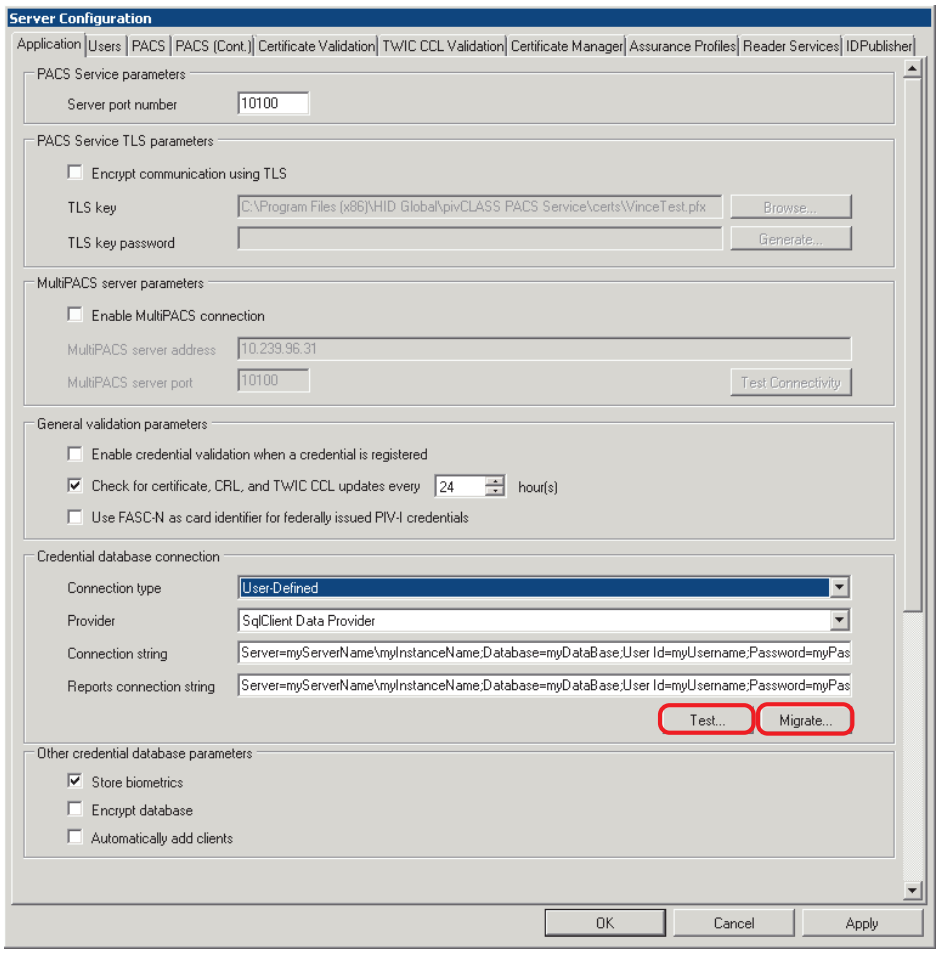
4. Click **Test** to verify the connection. If successful a message will state that the database settings have been validated.
5. Click **OK** to accept the new settings.



4.3.5 Migrate a Credential Database to another Database

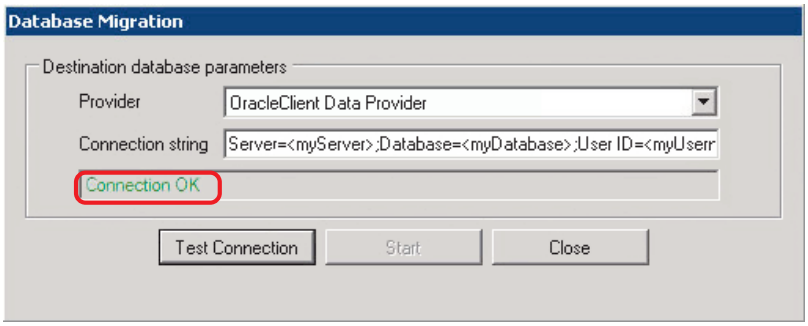
To migrate existing deployments to another database provider carry out the following:

1. After entering all of the current credential database parameters, click **Test**.
2. If the test is successful, the **Migrate** button is enabled. Click **Migrate**.



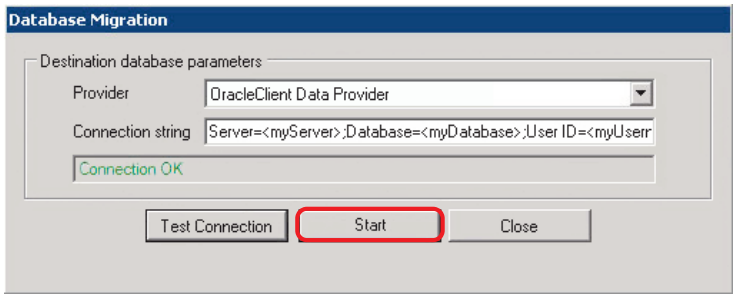
3. Select the new database provider from the **Provider** drop-down menu.
4. Enter the **Connection string** for the selected provider.
5. Click **Test Connection**.

   If the test is successful a `Connection OK` message will display.



6. Click on the **Start** button.

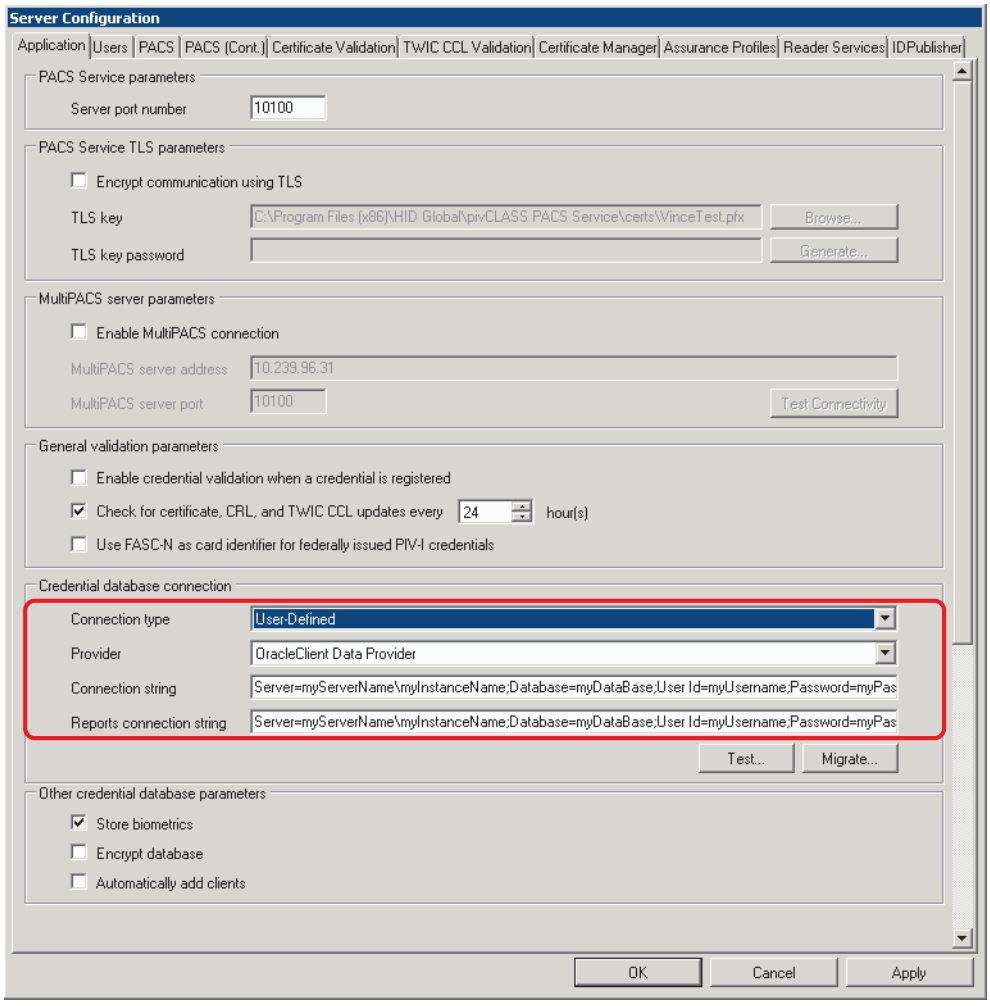
   All data from the source pivCLASS credential database will be copied to the destination database. During this time you will see messages displayed, indicating which tables are being created and the number of rows that have been inserted in them.



7. When complete, a message **Completed copying tables to destination database** is displayed. Click **Finish**.

   Note: Messages displayed can be copied and pasted into a text editor.

   The **Credential database parameters** fields on the **Application** tab, will now display the new provider information.



4.4 User and account administration

The User form is used to create and manage accounts for pivCASS operators and administrators.

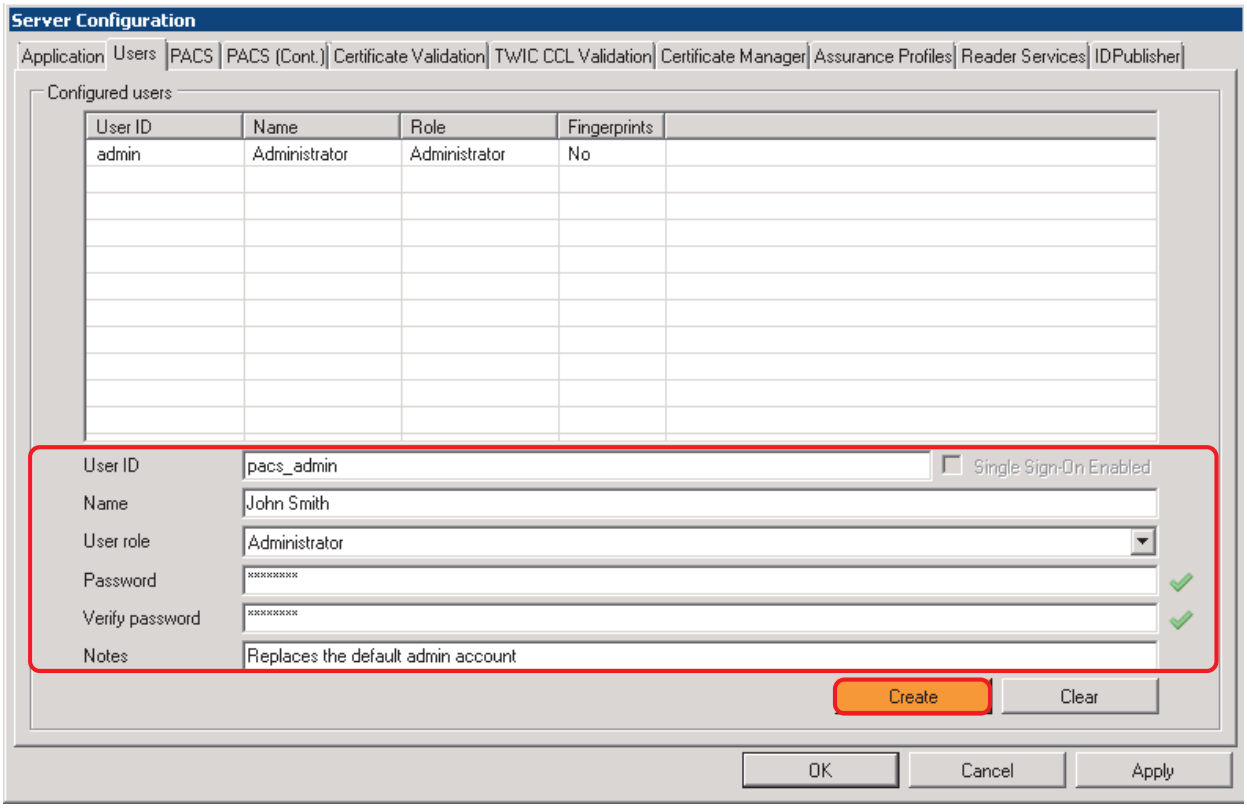
Note: An administrative user account comes pre-installed (User ID = *admin*, Password = *password*).

4.4.1 Create a new user

1. Click **Clear**.
2. Enter the user information:
   - Enter a unique user ID in the **User ID** field (must be at least two characters).

     Note: pivCLASS supports Single Sign-On for Windows. If the **Single Sign-On Enabled** option is selected the User ID will be matched against the Windows credential.
   - Enter the full name of the user in the **Name** field.
   - Select Administrator or Operator in the **User Role** field. HID Global recommends that users log into the pivCLASS Workstation application as "Operator" for day to day use of the application unless administration privileges are required.
   - Enter a secure password in the **Password** field (must be at least eight characters).
   - Re-enter the same password in the **Verify Password** field.
3. Click **Create**.

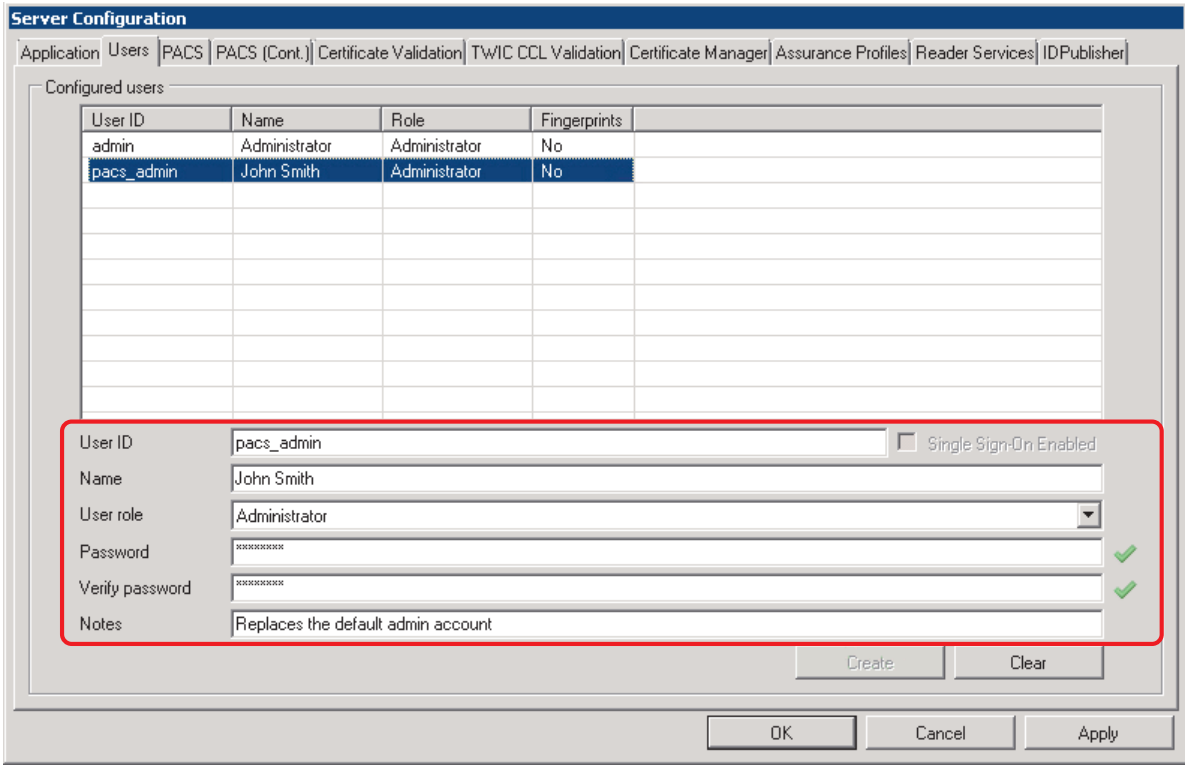
   A new user is added to the **Configured users** list.



4.4.2 Update user information

To update user information:

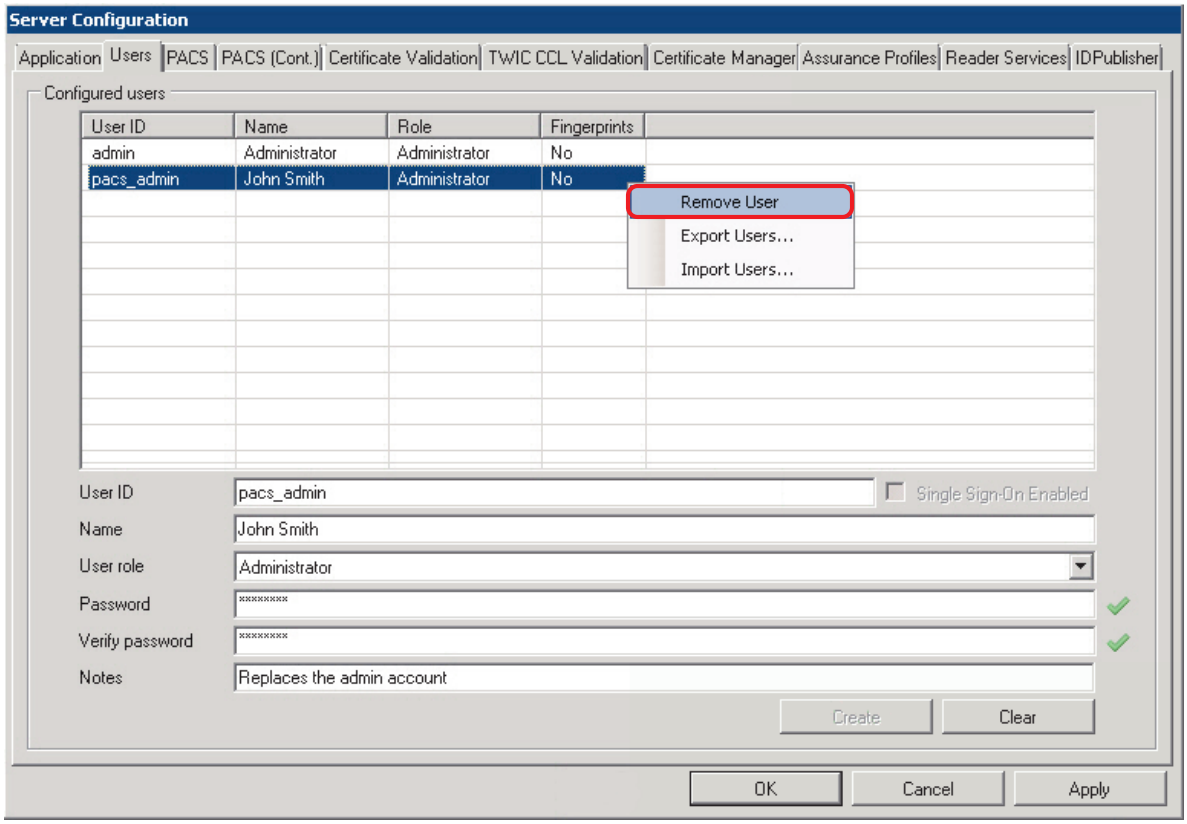
1. Select a **User** from the list
2. Edit the information in the fields below. All changes are added as they are made.



4.4.3 Remove a user

1. To remove a client user account from the system, right-click on a **User** from the list.
2. Select **Remove User** from the drop-down menu.

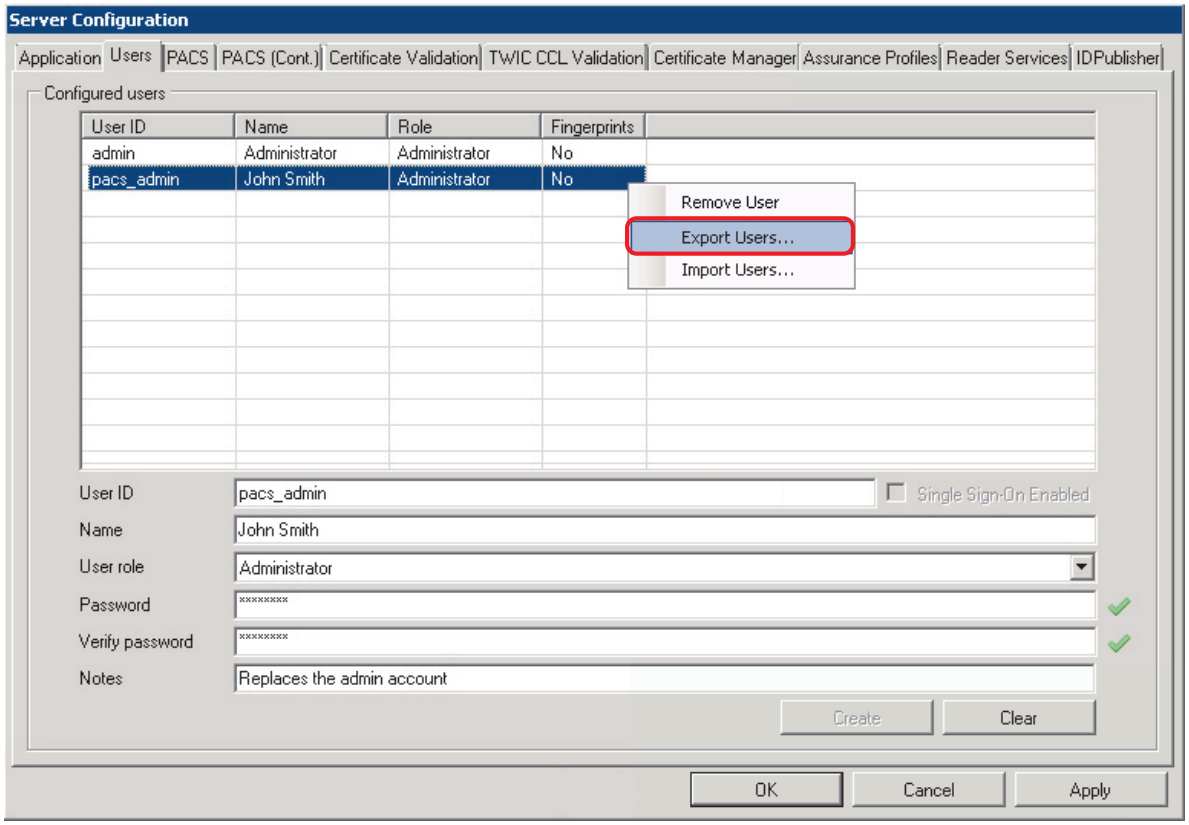
   The user is removed from the list.



4.4.4 Export users

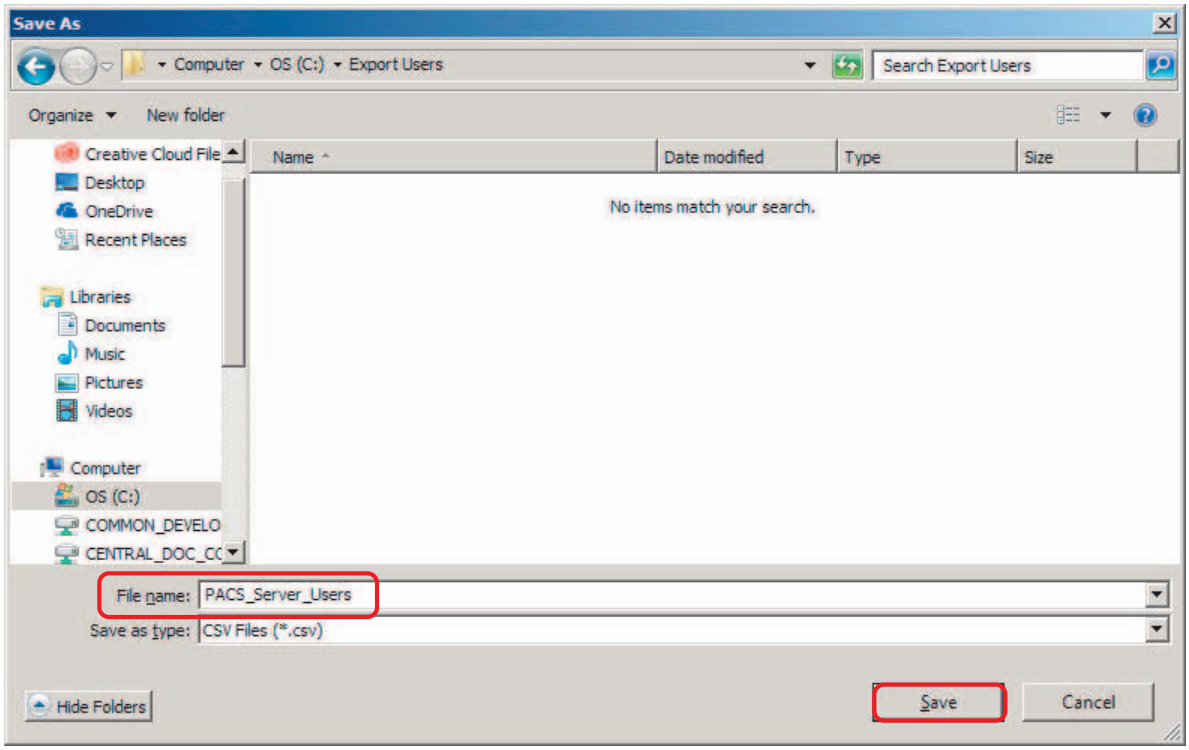
Users configured in the PACS server can be exported to a Comma Separated Values (**.csv**) file.

1. Right-click in the **Configured users** area.
2. Select **Export Users** from the drop-down menu.



3. Navigate to the folder to create the **.CSV** file.

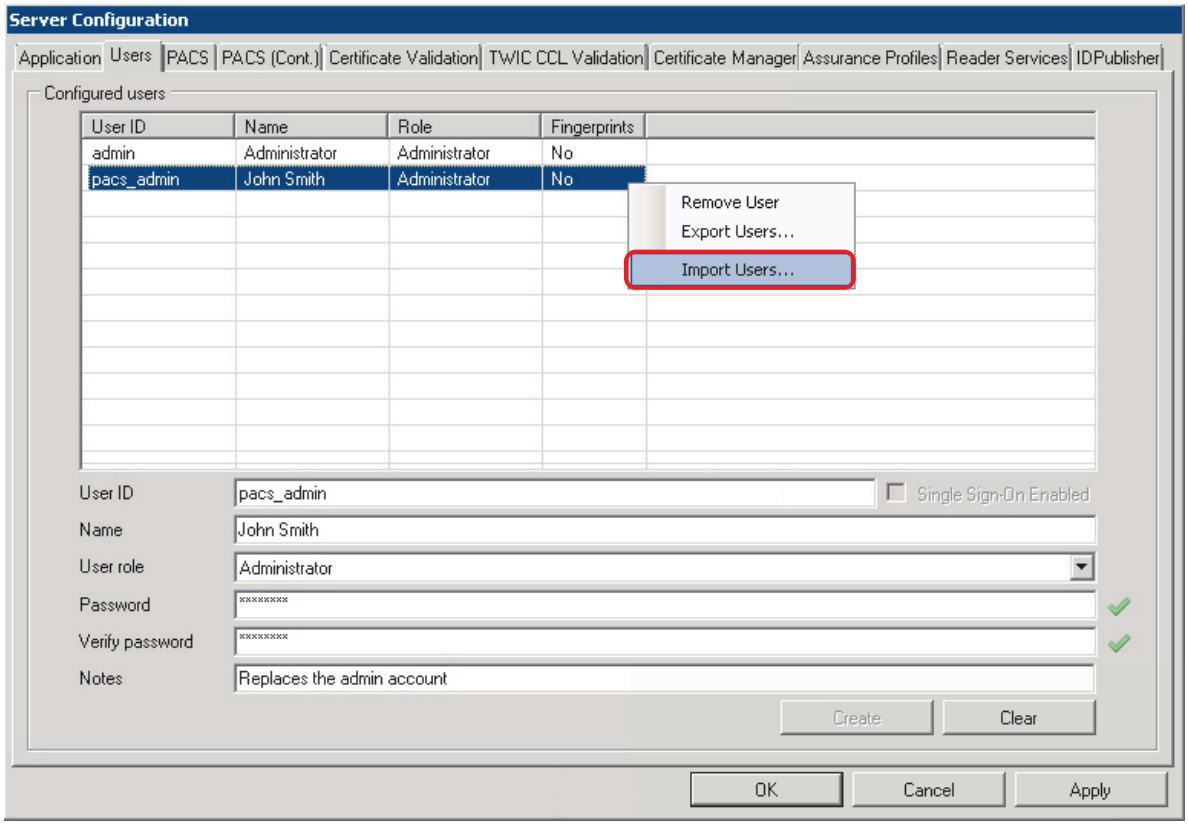
   Note: The passwords will be saved in encrypted form. If imported into another server, the passwords will need to be reset.



4.4.5 Import users

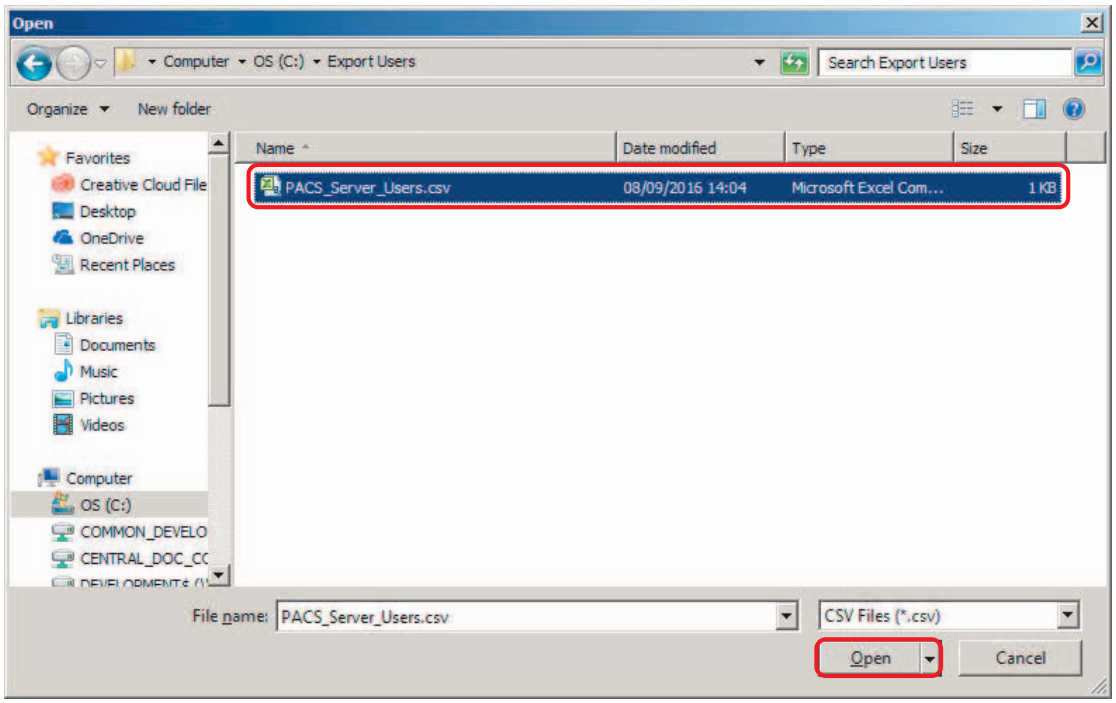
Users can be imported from a Comma Separated Value (**.CSV**) file.

1. Right-click in the **Configured users** area.
2. Select **Import Users** from the drop-down menu.



3. Navigate to the **.CSV** file that contains the Users to import.
4. Select the file and click **Open**.

   Note: The passwords will be saved in encrypted form. If imported into another server, the passwords will need to be reset.



Note: The file must include the following column headers in the first row:

```
UserId, Name, Description, Password, Role, SSO, Workstation, Mobile
```

The values in each column should correspond to the column header as illustrated in the example below:

```
admin, Administrator, Administrator, cGFzc3dvcmQ=, Administrator, FALSE, TRUE, TRUE,
Operator, Operator, Operator, b3BlcmF0b3I=, Operator, FALSE, TRUE, TRUE
```

5. Click **OK** when complete.

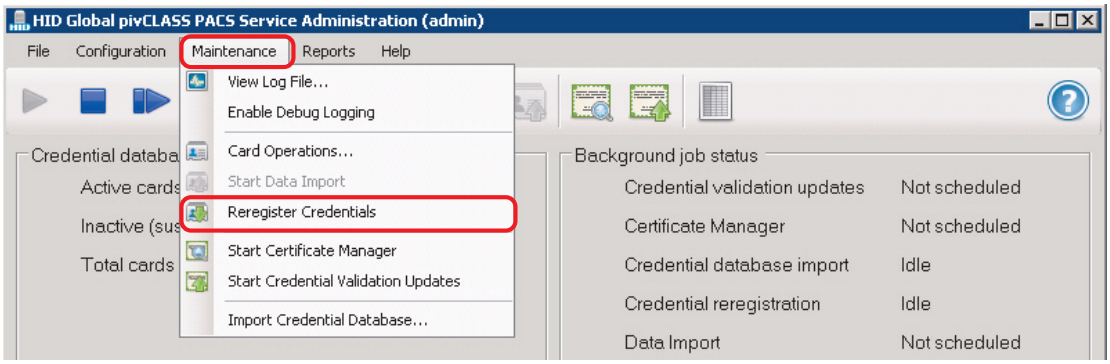
4.5 Credential administration

4.5.1 Reregister Credentials

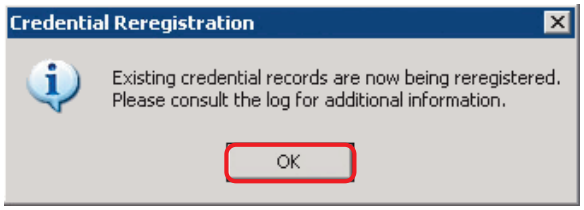
Credential Reregistration allows the PACS Service to register existing credential information again. This may be necessary if the credential information in the PACS has become stale. However this is most valuable when a new PACS connector is added in a MultiPACS environment, with none of the previously registered credential information.

To re-register existing credential information perform the following:

1. In the **PACS Service Administration** window, select **Maintenance** > **Reregister Credentials**.



2. The **Credential Reregistration** window will appear. Click **OK**.

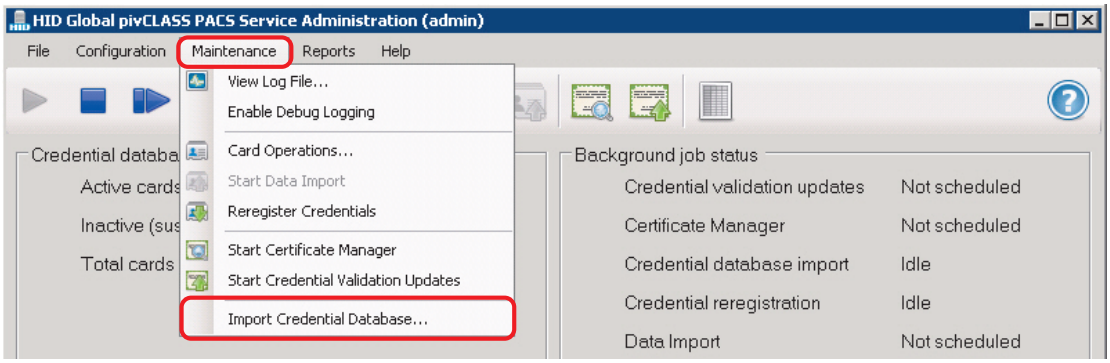


4.5.2 Import Credential Database

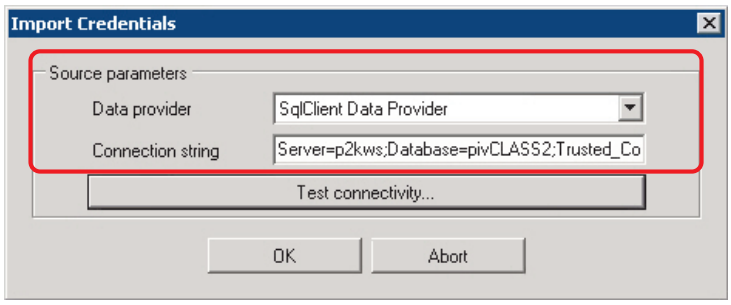
The **Import Credential Database** option allows the administrator to load the PACS Service with credential records from another pivCLASS database.

To import a credential database:

1. In the **PACS Service Administration** window, select **Maintenance** > **Import Credential Database**.

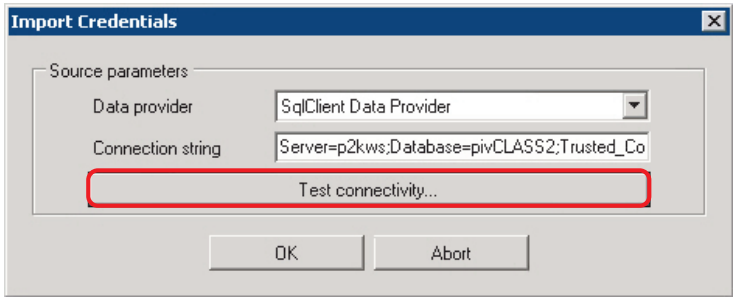


2. Enter the Source parameters.

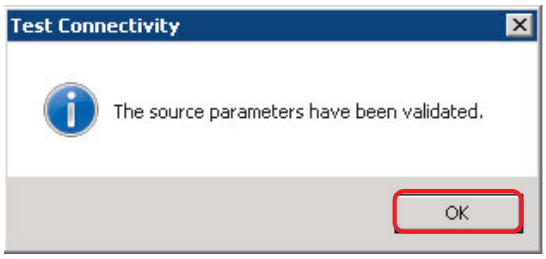


Option	Description
Data provider	A data provider serves as a bridge between an application and a data source. To set up a new database connection, select the data provider you will be using from the **Data Provider** drop-down list.
Connection string	Enter the connection string parameters for the database listed above.

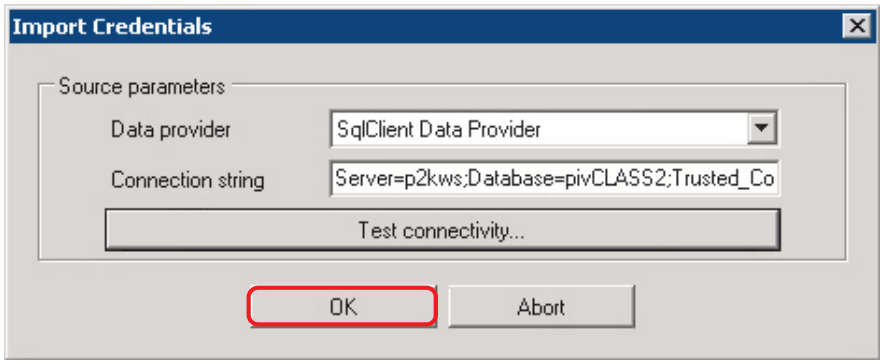
3. Click **Test connectivity** to test whether the entered **Data provider** and **Connection string** parameters can be used to open a database connection.



4. If the source parameters are validated, click **OK**.



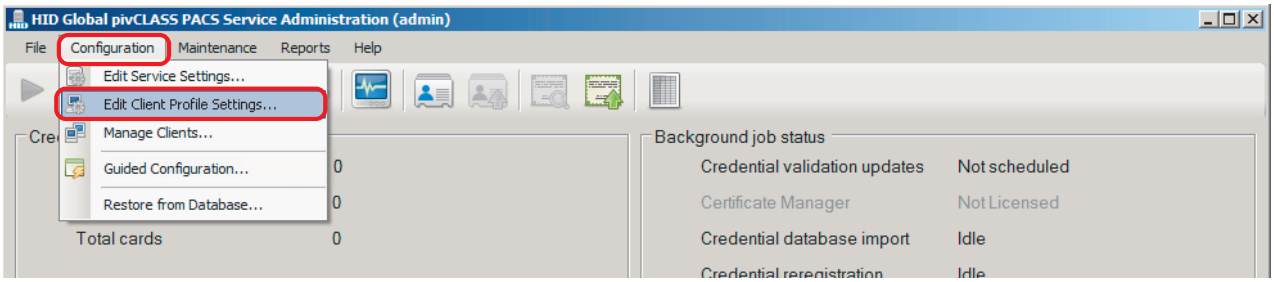
5. Click **OK** to begin the import of credential information.



4.6 Client profile configuration

Client profiles are a set of configuration policies managed by the PACS Server. These policies are pushed out to pivCLASS and pivCLASS Mobile clients whenever they synchronize with the server.

To access and configure client profile parameters select, **Configuration** > **Edit Client Profile Settings**.



The values entered in the set of **Client Configuration** dialogs control the behavior of all mobile and desktop clients.

- **Application:** Configure general client parameters, fingerprint verification parameters, and the settings that control the files sent from the PACS Service to pivCLASS clients.
- **pivCLASS Mobile:** Configure settings for pivCLASS Mobile clients.
- **Users:** Create and edit accounts for pivCLASS operators and administrators.
- **Certificate Validation:** Configure general certificate validation parameters and the authentication method for credential verification of authenticity and revocation status.
- **TWIC CCL Validation:** Configure general TWIC CCL parameters and the settings for TWIC CCL download.

Note: For a detailed description of client profile parameters, while on any of the above **Client Configuration** dialogs, select the keyboard key F1 to access the relevant *pivCLASS PACS Service Application Online Help* topic.

4.6.1 Upgrade Clients using Synchronize Data

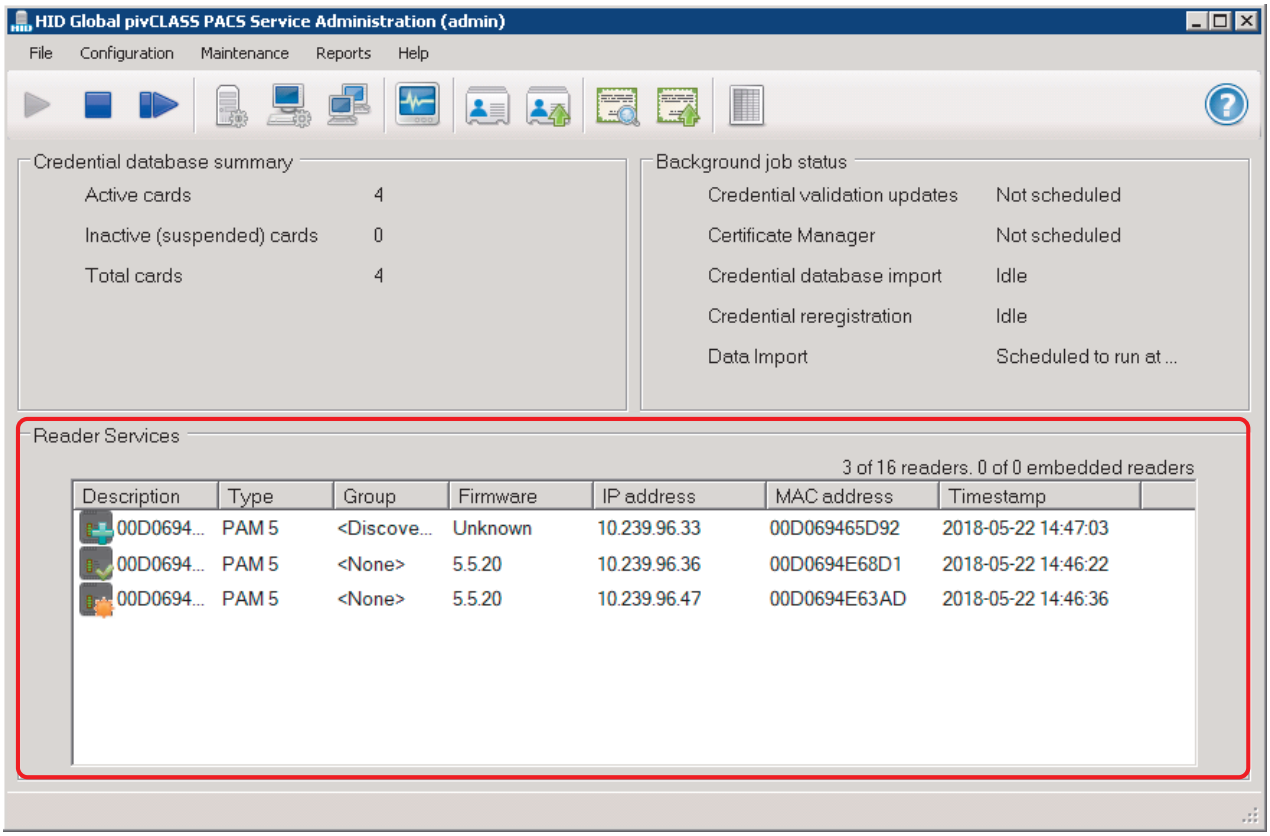
To upgrade pivCLASS or pivCLASS Mobile clients connected to a particular PACS Plug-in, place the pivCLASS Validation Workstation **.msi** files and/or **pivCLASS Mobile Validator.exe** install files in a directory named **clientsw** (client software) within the PACS Plug-in installation directory.

Note: Create this directory if it does not exist.

When a client performs a synchronize data, the server will look for newer version of software in the client software directory and send it back to the client. The client will behave similar to how the check for software updates feature works.

4.7 Reader Services administration

The **Reader Services** status area on the pivCLASS PACS Service application main window displays status information about pivCLASS Authentication Modules (PAMs) and pivCLASS Embedded Authentication devices.

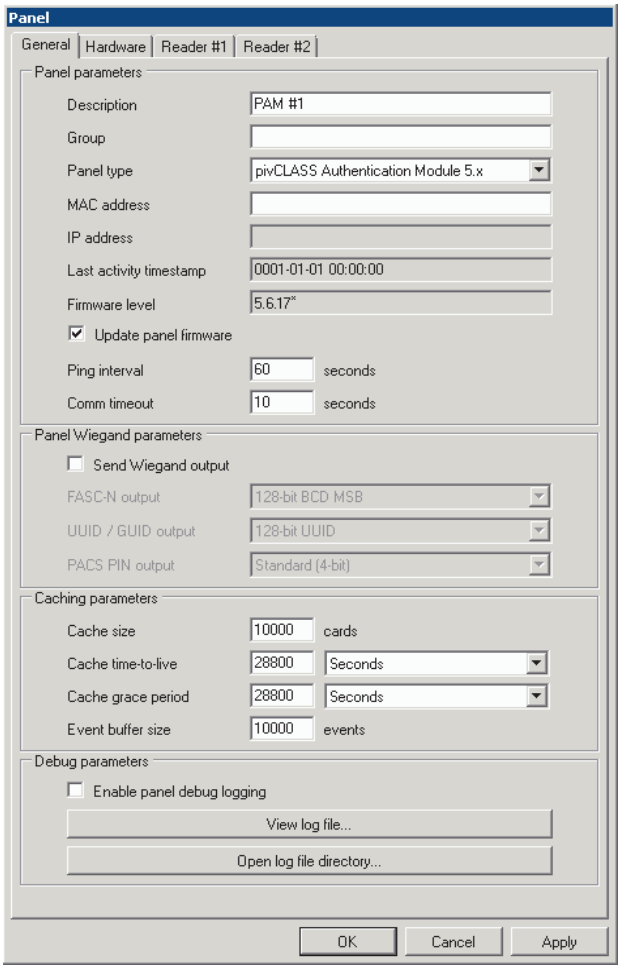


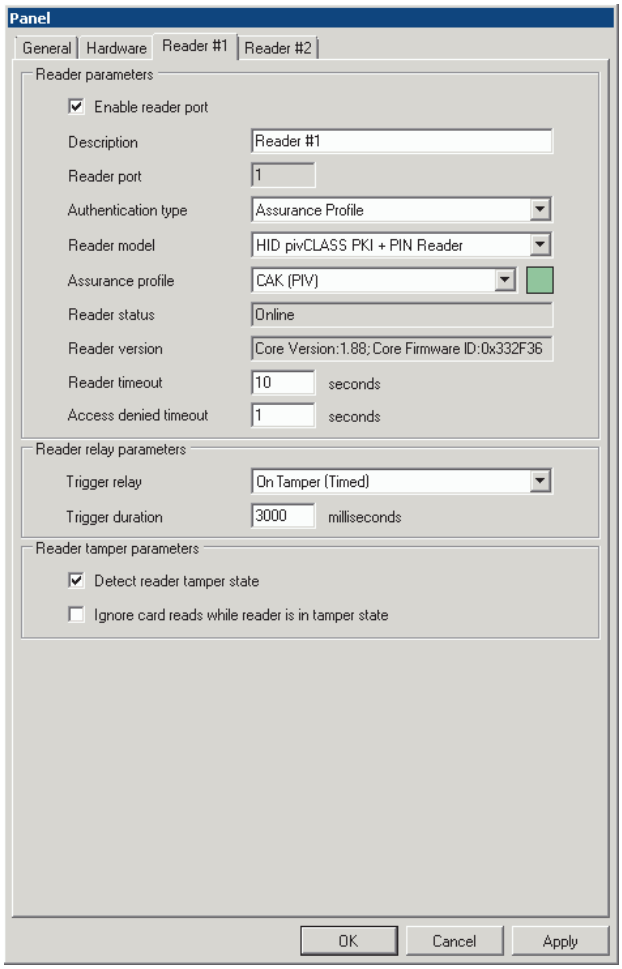
Status icon	Description
	This panel icon indicates the device is a pivCLASS Embedded Authentication device.
	This panel icon indicates the device is a pivCLASS Authentication Module (PAM).
	This symbol on a panel icon indicates that the panel has been flagged for firmware updates.
	This symbol on a panel icon indicates the panel has not sent a ping message to the PACS Service within the number of seconds indicated by its configured ping interval. The PACS Service considers this panel offline.
	This symbol on a panel icon indicates the panel is sending ping messages to the PACS Service. The PACS Service considers this panel online.
	This symbol on a panel icon indicates the panel is in discovery mode and waiting to be added to the PACS Service.
	This symbol on a panel icon indicates that a configuration change was made to the PAM but the PAM has yet to be made aware of it.

4.7.1 Panel/Reader parameters

Double click on a displayed panel icon in the **Reader Services** status area to access general Panel and Reader configuration parameters.

For detailed information on panel/reader configuration parameters select F1 while on the **General** form or the **Reader#1**/**Reader# 2** form to access the relevant *pivCLASS PACS Service Application Online Help* topic.

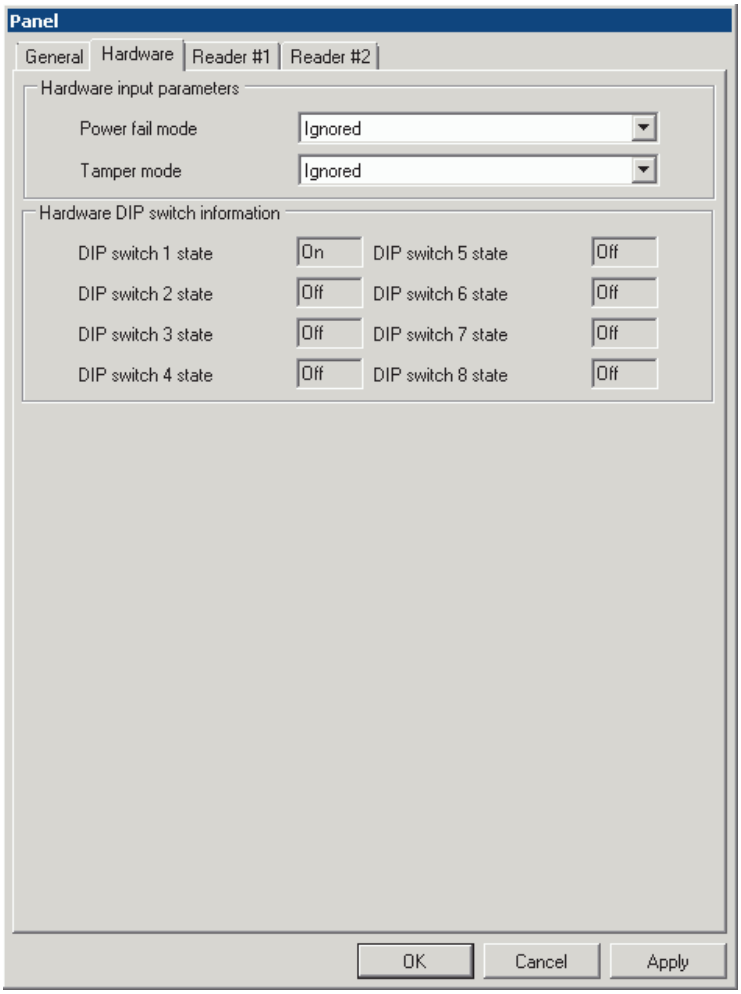




For instructions on how to setup the PACS Service to PAM communication path and add a PAM within Reader Services (manually or via auto discovery), refer to the *pivCLASS Authentication Module Installation and Configuration Guide* (PLT-01628).

4.7.2 Hardware status information

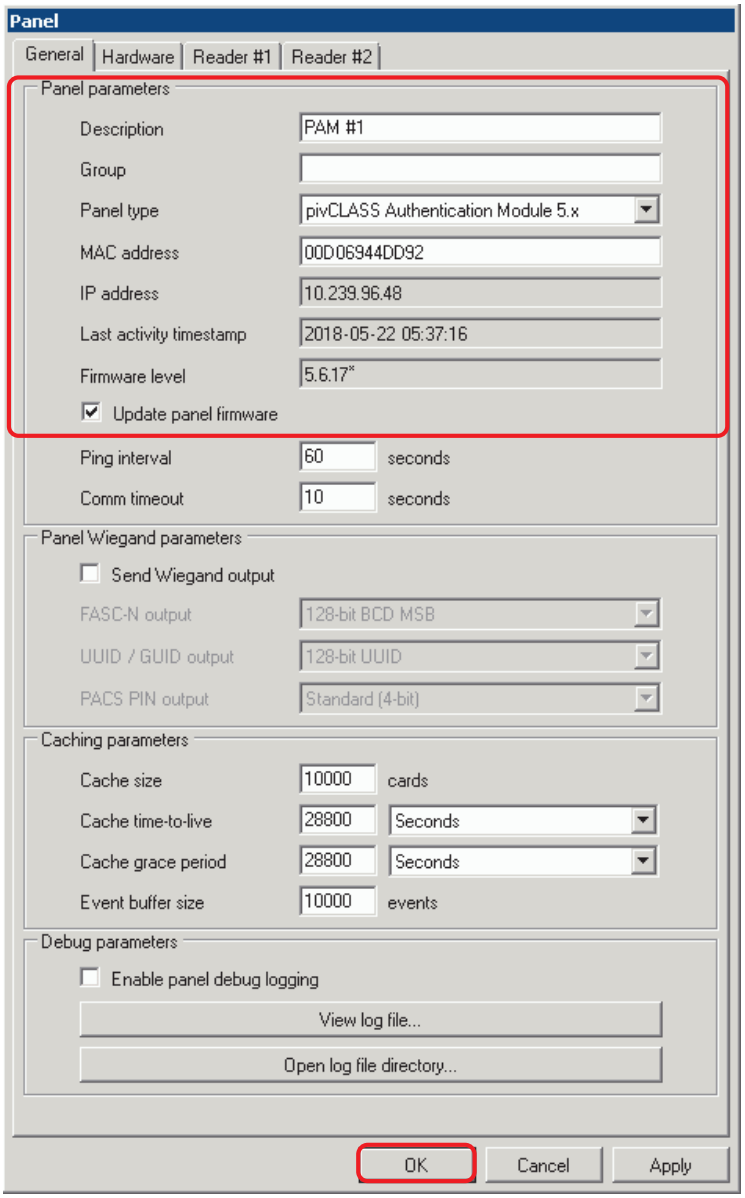
Select the **Hardware** tab on the **Panel** form to set the options for power fail mode and tamper mode and to view panel DIP switch status information (PAM 5 only).



4.7.3 Panel auto discovery

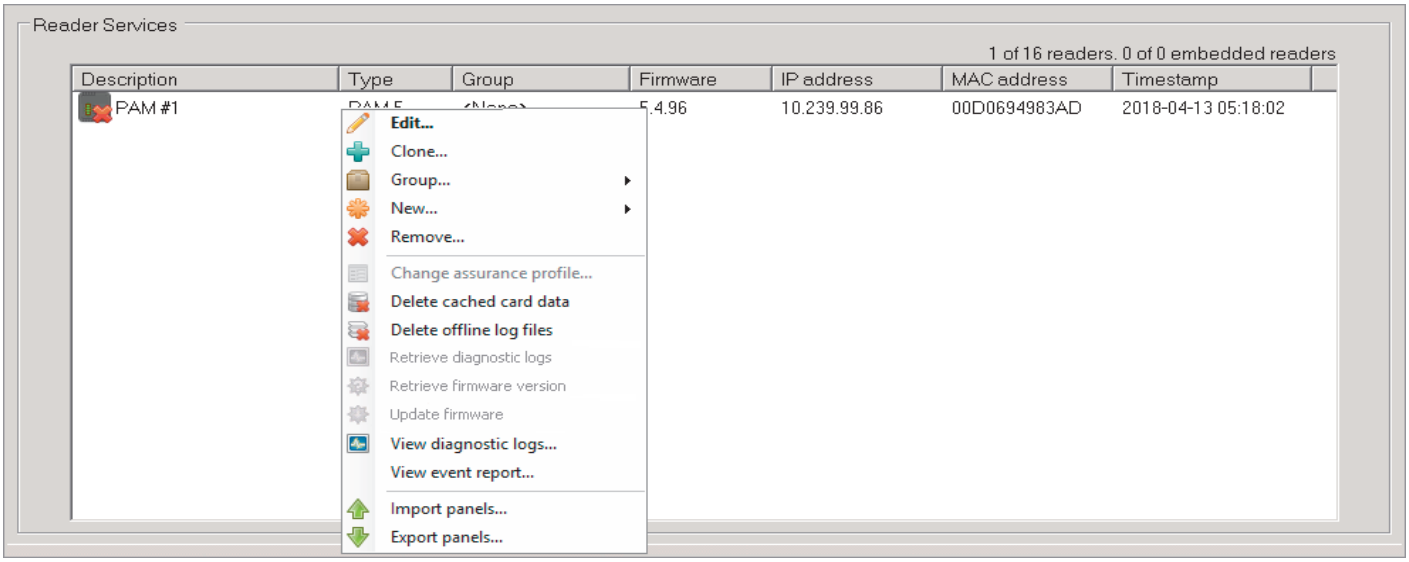
Double click on a displayed discovered panel icon [ ] in the **Reader Services** status area to launch the **Panel** form. On the **General** tab, enter the panel parameters and click **OK** to add the panel to the list of configured panels.

Note: Select the **Update panel firmware** option (PAM 5 only) 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.



4.7.4 Reader Services functions

Right click in the **Reader Services** status area on the pivCLASS PACS Service application main window to access Reader Services related functions. Some functions are only available for certain panel types.



Menu option	Description
Edit	View or modify panel parameters for a selected panel.
Clone (PAM 4, PAM5, Embedded)	Make a copy of the selected panel. The newly created panel record is assigned a unique lock ID and description.
Group (PAM 4, PAM5, Embedded)	Move a panel to a panel group.
New	Create a new panel. The newly created panel record is assigned a unique lock ID and description.
Remove	Remove a selected panel.
Change assurance profile (PAM 4, PAM5)	Change the assurance profile of a selected panel.
Delete cached card data (PAM5, Embedded)	Instructs selected panels to remove any cached card information, including certificates, TWIC privacy keys, and biometrics
Delete offline log files (PAM5, Embedded)	Instructs selected panels to remove any logging information stored while the panel was offline and pending upload to the PACS Service
Retrieve diagnostic logs (PAM)	Download the diagnostic logs for a PAM (PAM 4 only). Diagnostic logs are located in a directory named according to the selected PAM's lock ID in the **\pam\debugfiles** directory beneath the PACS Service application directory.
Retrieve firmware version (PAM 4)	Query a PAM for its current firmware version (PAM 4 only).
Update firmware (PAM 4, PAM5)	Upload firmware update files to the selected PAM (PAM 4 and PAM 5). Firmware update files are located in the **\pam\firmware** directory beneath the PACS Service application directory.

Menu option	Description
View diagnostic logs (PAM5, Embedded)	Open the Log Viewer to view the log file in real-time (PAM 5 and Embedded PAM).
View event report (PAM 4, PAM5, Embedded)	Open a Reports window displaying a log of PAM events. There is a limit of 100 total records returned regardless of the number of selections made. Records are ordered by timestamp, most recent first.
Import panel	Load saved panels, panel groups, and readers from a .CSV file. The user is prompted to select the name and filesystem location of the .CSV file.
Export panels	Save configured panels, panel groups, and readers to a .CSV file. The user is prompted to select the name and filesystem location of the .CSV file.

4.8 Log file administration

By default, the PACS Service application and the pivCLASS Workstation application logs system messages to the logs directory beneath their respective installation directories. It is sometimes useful to refer to this log when attempting to troubleshoot system errors.

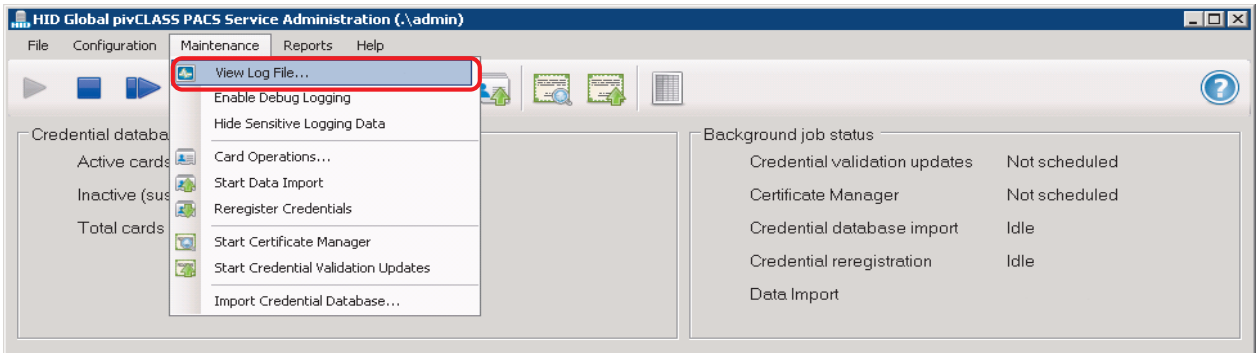
The scope of the system messages captured can be configured using the **log4net.xml** file in the install directory. For more information, refer to the Log Viewer topic in the *PACS Service Application Online Help*.

To learn more about log4net refer to:

http://logging.apache.org/log4net/

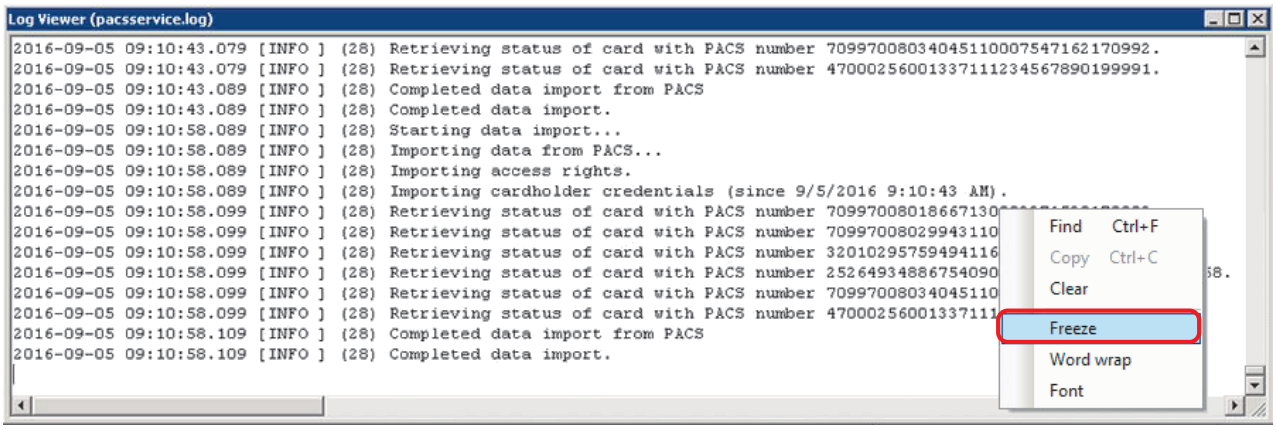
4.8.1 View the PACS Service log

Select **Maintenance** > **View Log File** from the PACS Service Administration window to launch **Log Viewer**.



The **Log Viewer** window displays the most recent **pacsservice.log** containing event information messages for service events.

Note: The **Log Viewer** displays the logging in real time therefore the display is updated as log messages are being generated. Right-click in the **Log viewer** window and select **Freeze** to pause real time updating in order to review displayed log entries.



4.8.2 Turn on Debug Logging

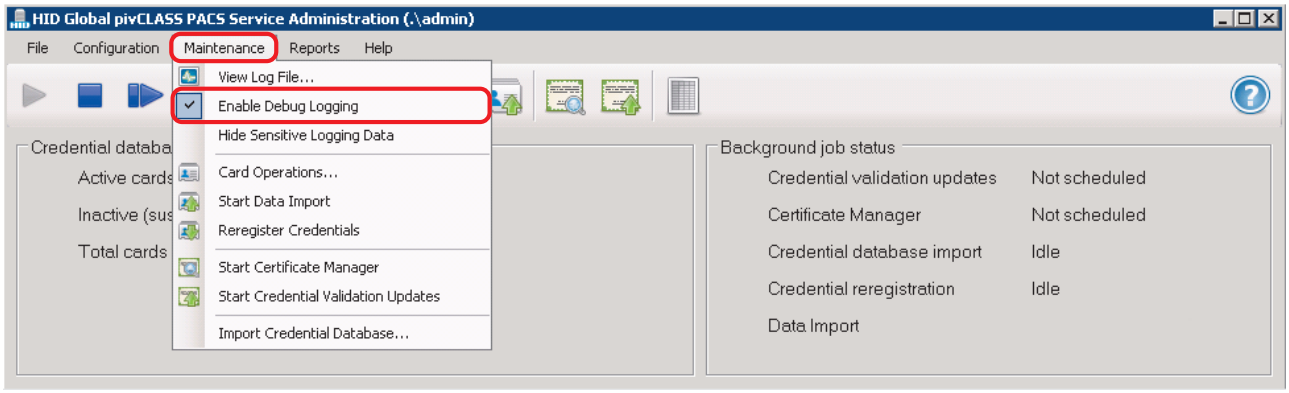
By default event messages in the log file are informational only. If a card, registration, client, server or system error is received, a prompt may appear to **Enable Debug Logging**. Enabling debug logging will assist troubleshooting issues by recording advanced debugging messages.

Important: Enabling debug logging will cause a large increase in the size of the log file. Debug logging should only be enabled for short troubleshooting periods and then turned off.

To enable debug logging:

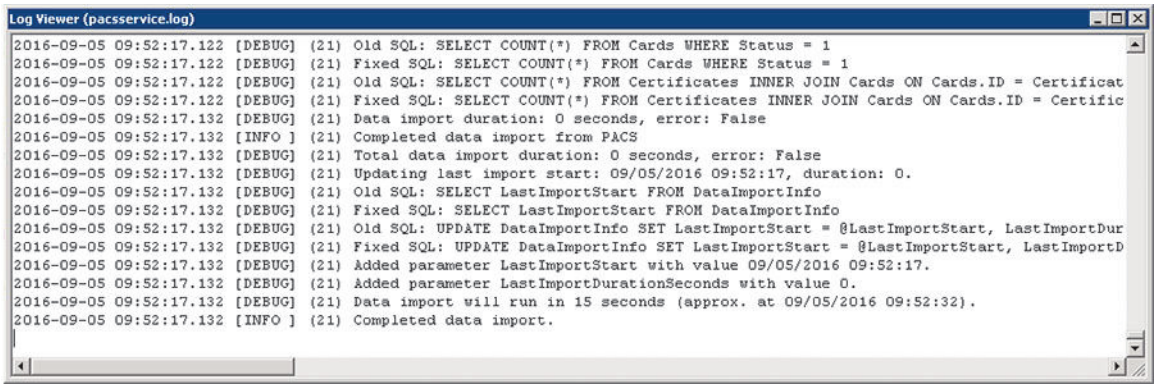
1. In the **PACS Service Administration** window, select **Maintenance** > **Enable Debug Logging**

   A check mark box will appear next to the **Enable Debug Logging** menu item to indicate that the option is turned on.



2. In the **PACS Service Administration** window, select **Maintenance** > **View Log File**.

   The **Log Viewer** window displays debug messages and event information messages for service events.

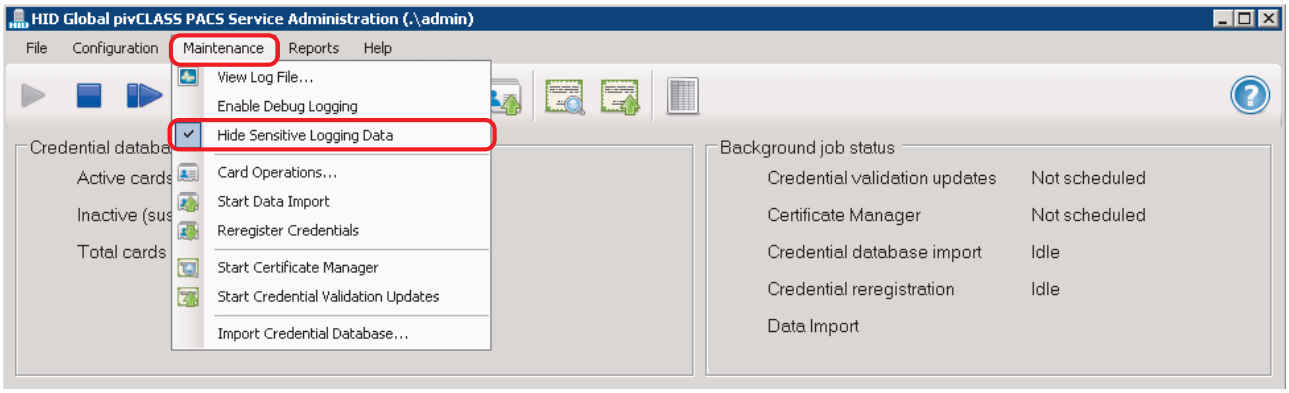


4.8.3 Redact Personal Information from log files

As an option certain sensitive Personally Identifiable Information (PII) can be obfuscated in the log file. This is useful when there is a need to share log files with others and there is a concern about PII contained in the files.

To enable this option, from the **PACS Service Administration** main window, select **Maintenance** > **Hide Sensitive Logging Data**.

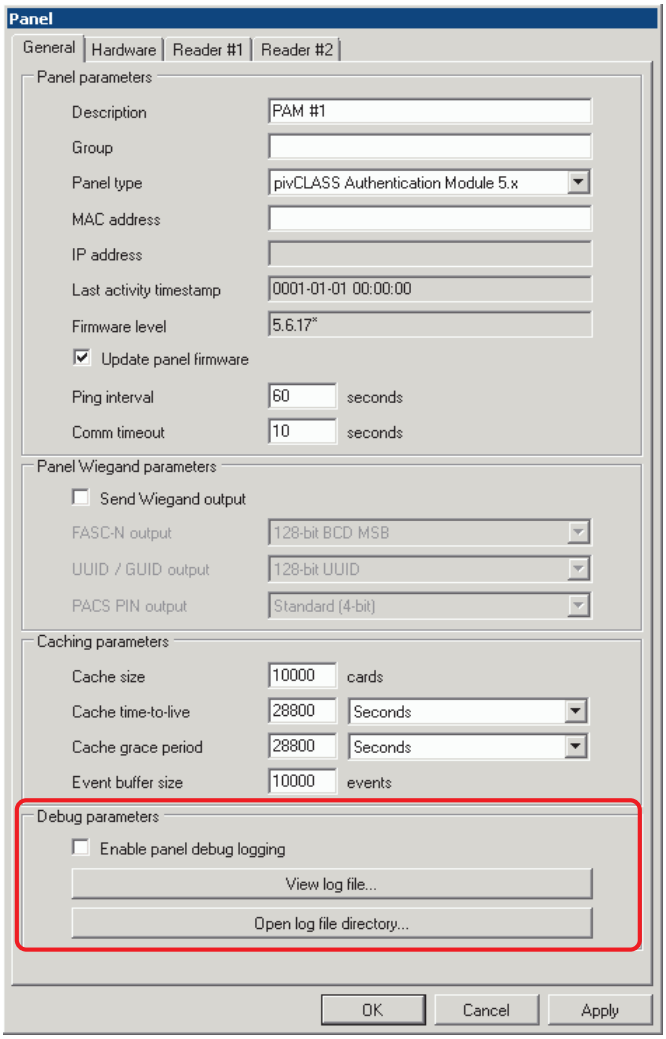
A check mark box will appear next to the **Hide Sensitive Logging Data** menu item to indicate that the option is enabled.



4.8.4 Panel log file

Double click on a displayed panel icon in the **Reader Services** status area to access the **Panel** form.

The **Debug parameters** section provides options for debug logging, viewing panel logs, and opening the log file directory.



4.8.4.1 Enable panel debug logging

By default message entries in the log file are informational only. However when a problem occurs selecting the **Enable panel debug logging** option configures the PAM to write additional debugging messages to its log. HID Technical Support may request the administrator to enable this option to assist with troubleshooting.

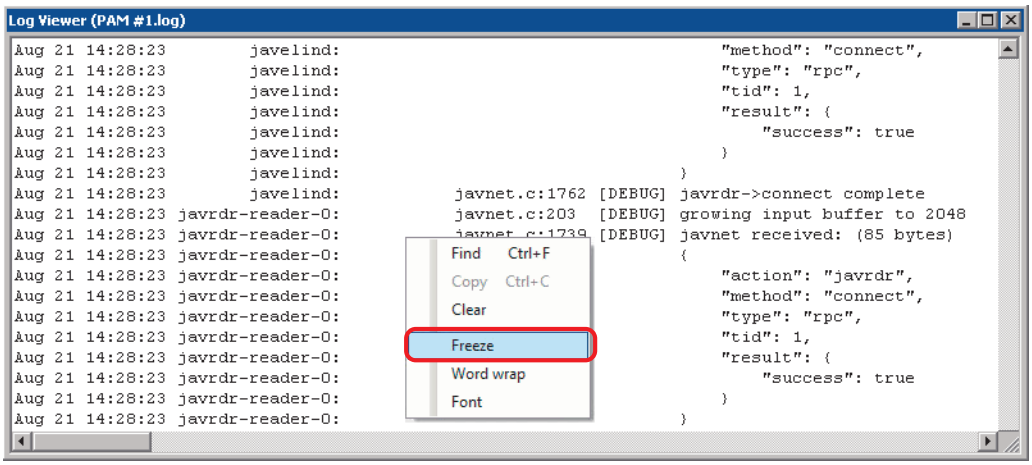
Important: Enabling debug logging will cause a large increase in the size of the log file. Debug logging should only be enabled for short troubleshooting periods and then turned off.

4.8.4.2 View log file

Select **View log file** to launch **Log Viewer**.

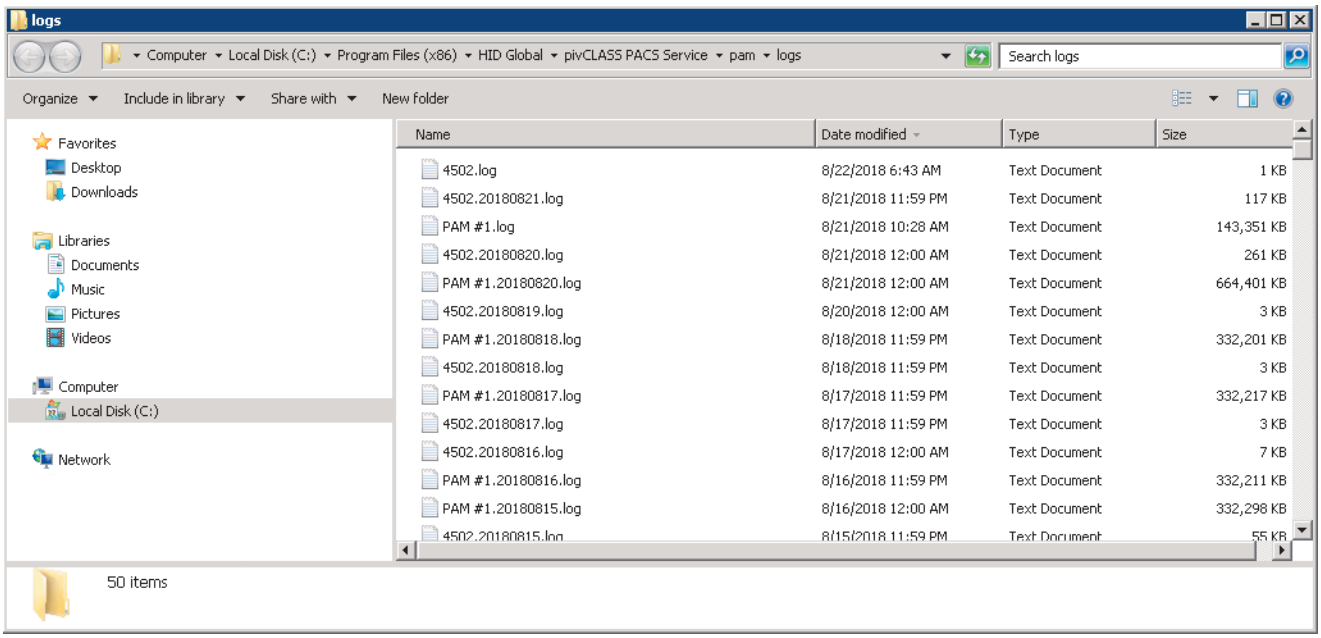
The **Log Viewer** window displays the **PAM.log** for the selected panel.

Note: The **Log Viewer** displays the logging in real time therefore the display is updated as log messages are being generated. Right-click in the **Log viewer** window and select **Freeze** to pause real time updating in order to review displayed log entries.



4.8.4.3 Open log file directory

Select **Open log file directory** to open the log file directory used by the selected panel.



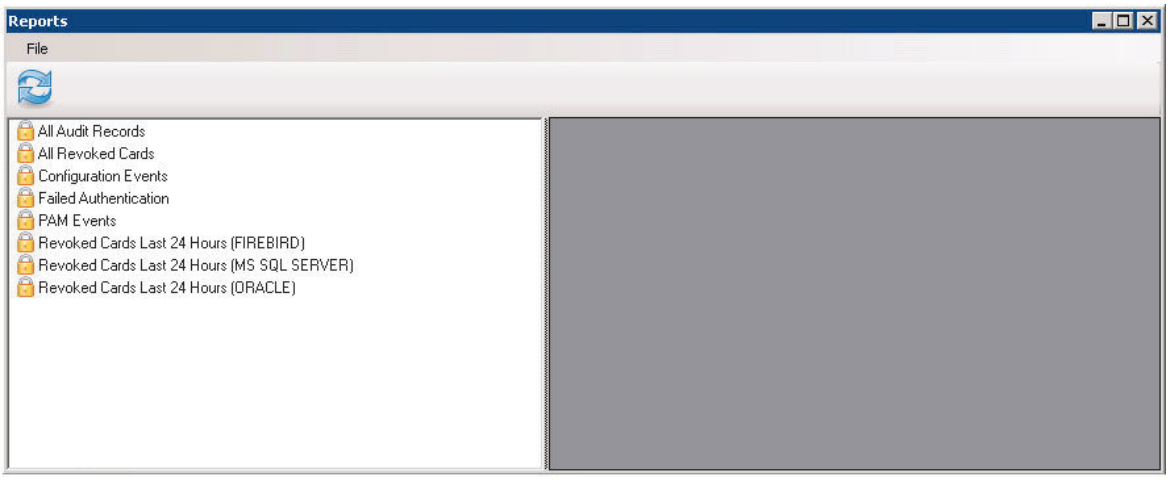
4.9 Reports administration

4.9.1 Reports

The **Audit Log** is a record of PIV credential validation history. Every pivCLASS Workstation and pivCLASS Mobile client records the outcome of all card validation sessions. These sessions can be uploaded to the PACS server where they can be reviewed in the form of **Audit Log Reports**. Sessions can be sent in real-time or in batch mode.

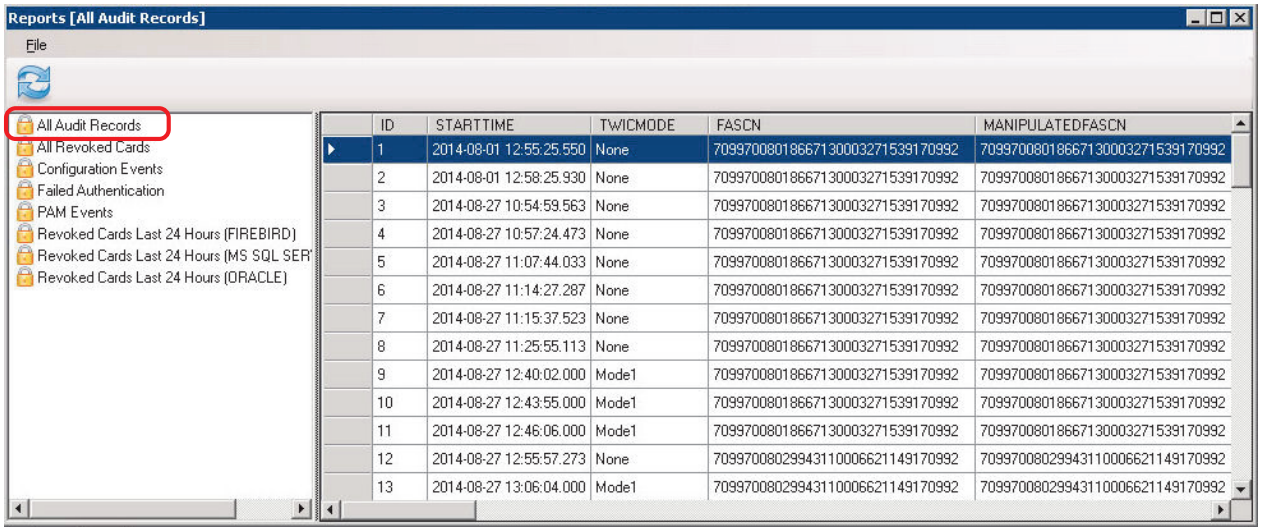
Note: For more information on exporting audit logs, see **Exporting Audit Logs** in the pivCLASS Validation Work Station or pivCLASS Mobile Validator User Manuals.

1. Select **Reports** > **Reports**. The **Reports** window is opened.

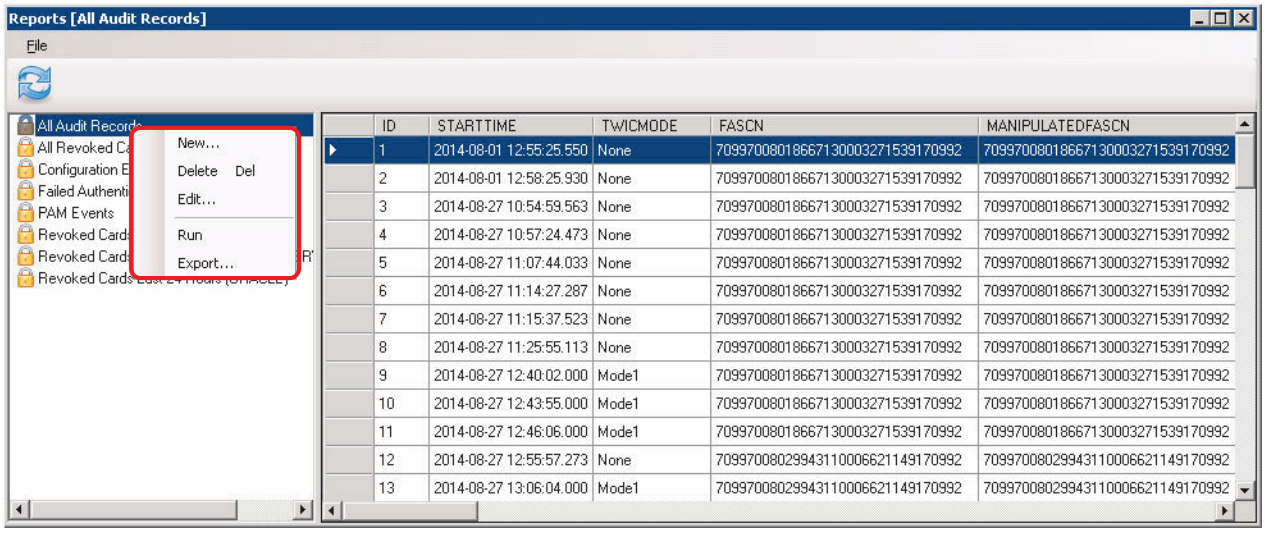


2. Double-click on a **Report** to display the report events log.

   Note: Default reports are denoted with a lock icon.



3. Right-click on a selected **Report** to display additional options.



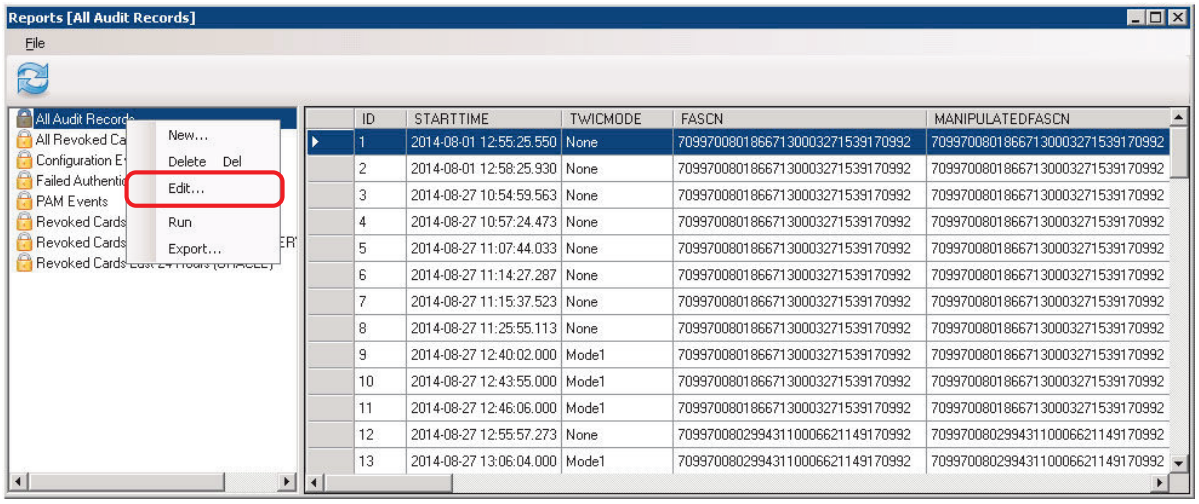
4.9.2 Edit option

The listed default **Report** queries can be edited.

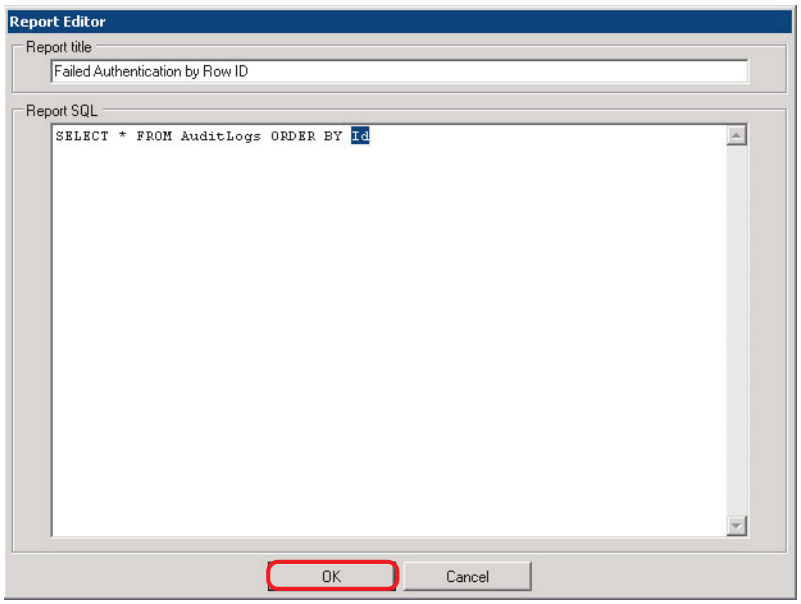
Note: Any updates are saved as a new report query, as default report queries cannot be overwritten.

To edit an existing **Report** query and save the edited report to a new query report:

1. Right-click a report from the list, and select **Edit**.



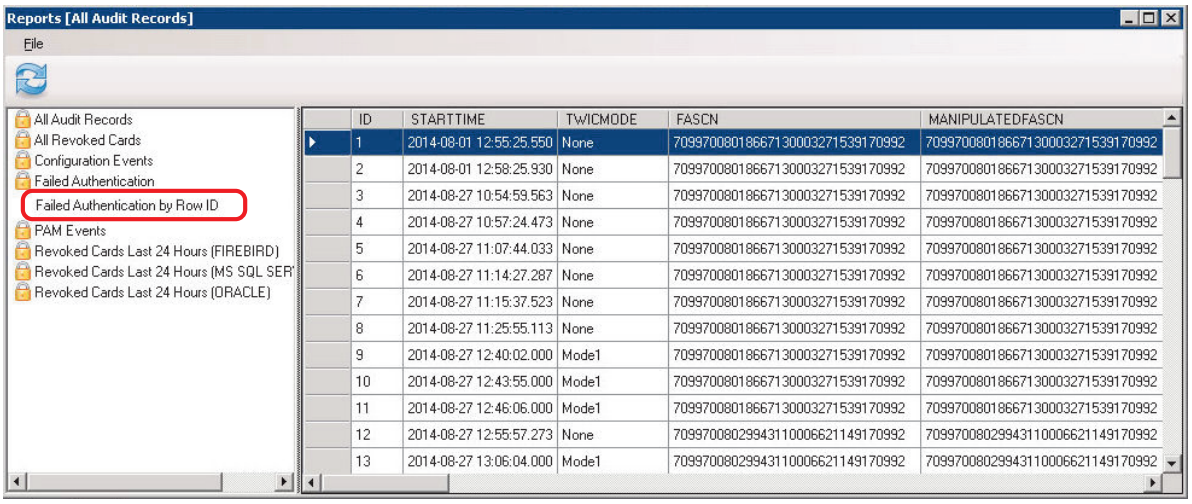
2. In the **Report Editor** window, modify the query, enter a new **Report title** for the Report and click **OK**.



3. The new report will be added to the list of reports.

This page is intentionally left blank.

Note: A lock does not appear next to this new report (indicating it is not a default report).

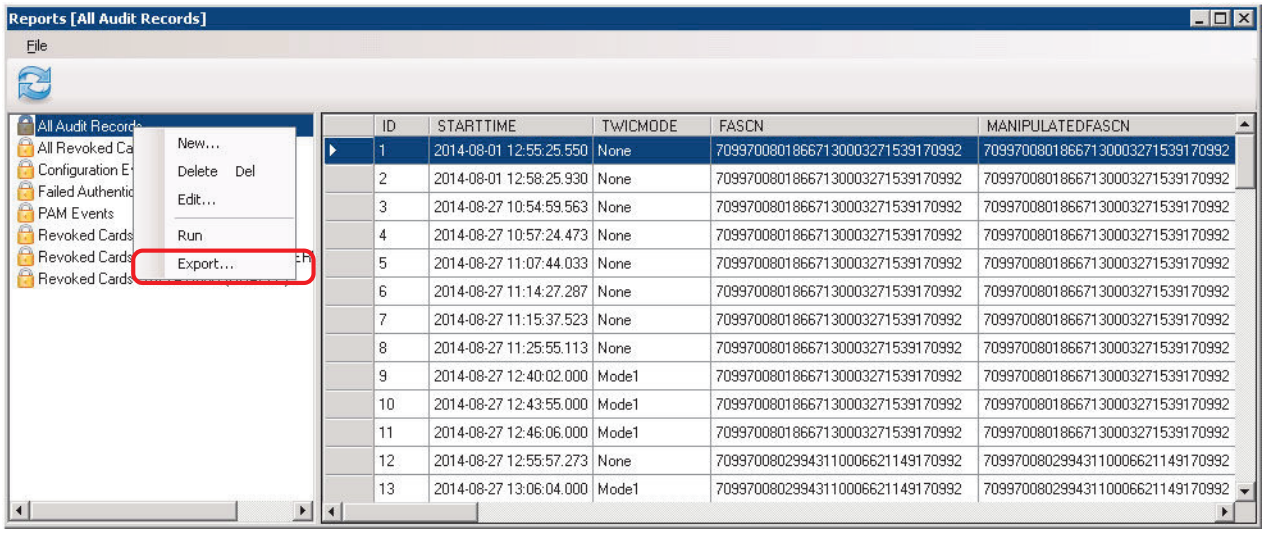


4.9.3 Export option

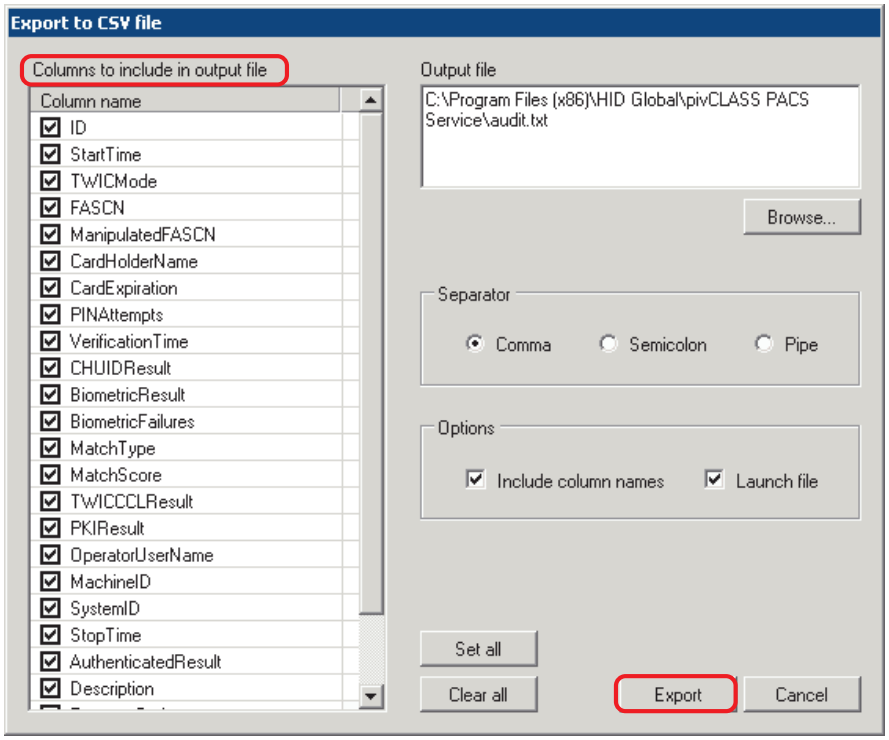
A listed **Report** can be exported to a Comma Separated Value (**.CSV**) file.

To export a report to a **.CSV** file:

1. Right-click a report from the list, and select **Export**.



2. In the **Export to CSV file** window, select the table columns to include in the output file from **Columns to include in output file**. Click **Export**.



The saved data will be rendered in Notepad, as shown in the example below.

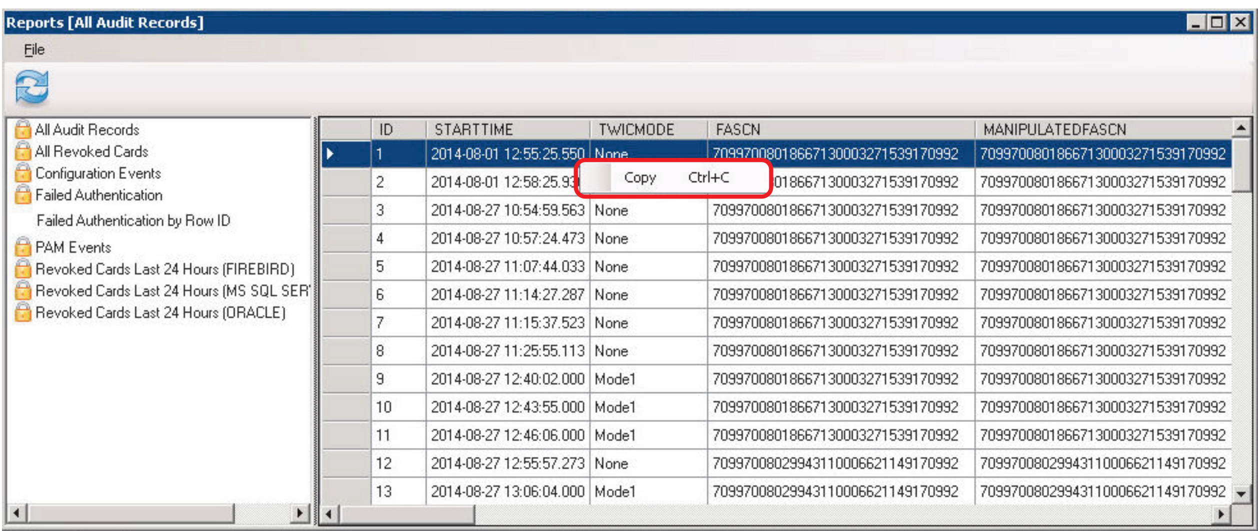
```
"ID","StartTime","TWICMode","FASCN","CardHolderName","CardExpiration","PINAttempts","VerificationTime","CHUIDResult","Biome
tricResult","BiometricFailures","MatchType","MatchScore","TWICCCLResult","PKIResult","OperatorUserName","MachineID","StopTi
me","AuthenticatedResult","Description","Added","RFU1","RFU2","RFU3","SystemID","ManipulatedFASCN","PassageOption","Passage
Result"
"1","27Apr2011 14:05:06","None","70997008010993120000505370170992","FONTANA, ROBERT A","06Apr2013 00:00:00","1","27Apr2011
14:05:21","Ok","Not Configured","0","Identix","-1","Not Configured","Not Configured","Administrator","7F64ECQ","27Apr2011
14:06:40","Authenticated","","13May2011 08:41:21","","","","","","",""
"2","29Apr2011 00:54:18","None","47000000000336110001002324147001","Bill MSOHSEVENTYONE","08Jun2015
00:00:00","1","29Apr2011 00:54:34","Ok","Not Configured","0","Identix","-1","Not
Configured","Revoked","Administrator","7F64ECQ","29Apr2011 00:54:44","Not Authenticated","Blacklist verification failed:
SCVP response indicates non-valid certificate: certPathConstructFail, NotValid, No Valid Cert Path","13May2011
08:41:21","","","","","","",""
"3","29Apr2011 01:16:41","None","47000000000336110001002324147001","Bill MSOHSEVENTYONE","08Jun2015
00:00:00","1","29Apr2011 01:16:56","Ok","Not Configured","0","Identix","-1","Not
Configured","Revoked","Administrator","7F64ECQ","29Apr2011 01:16:59","Not Authenticated","Blacklist verification failed:
SCVP response indicates non-valid certificate: certPathConstructFail, NotValid, No Valid Cert Path","13May2011
08:41:21","","","","","","",""
"4","29Apr2011 01:22:55","None","47000000000336110001002324147001","Bill MSOHSEVENTYONE","08Jun2015
00:00:00","1","29Apr2011 01:23:15","Ok","Not Configured","0","Identix","-1","Not
Configured","Revoked","Administrator","7F64ECQ","29Apr2011 01:46:41","Not Authenticated","Blacklist verification failed:
SCVP response indicates non-valid certificate: certPathNotValid, NotValid, Invalid Cert Policy","13May2011
08:41:21","","","","","","",""
"5"."29Apr2011 01:46:42"."None"."47000000000336110001002324147001"."Bill MSOHSEVENTYONE"."08Jun2015
```

4.9.4 Export option #2

The following is another option to save report output data to a file:

1. Select a row(s) to copy.
2. Right-click and select **Copy**.

This page is intentionally left blank.



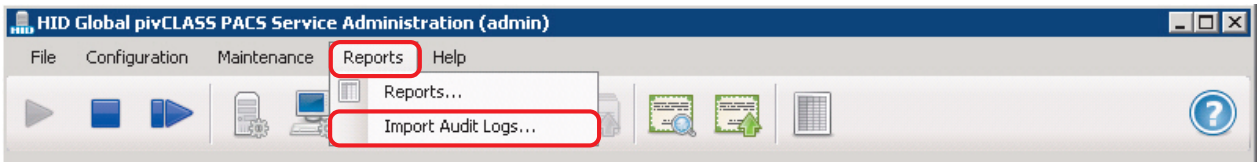
3. This will copy the selected rows to the Windows Clipboard. This information can be pasted into an editor or spreadsheet.

   Note: If pasting into Microsoft Excel, set the cell type to **Text** before the paste.

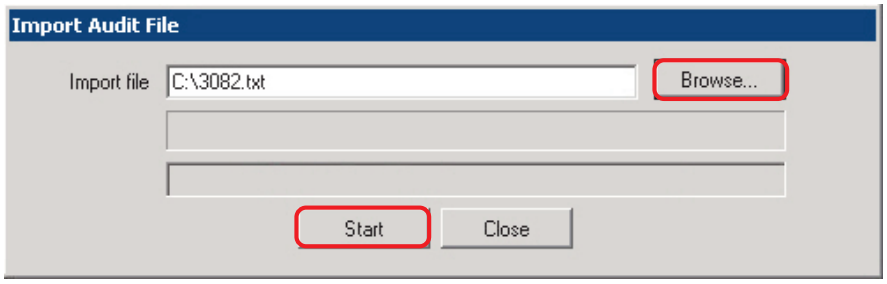
4.9.5 Import Audit Logs

To import a previously exported audit log file from a pivCLASS Workstation or pivCLASS Mobile client.

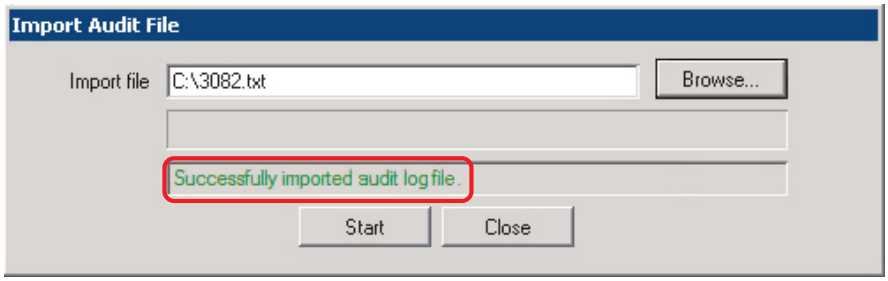
1. From the **PACS Service Administration** window select **Reports** > **Import Audit Logs**.



2. Click **Browse** to locate and select an audit log file to import.
3. Click **Start** to begin the import process.



4. The import may take several minutes. A message indicating a successful import should display.



This page is intentionally left blank.

Section 5

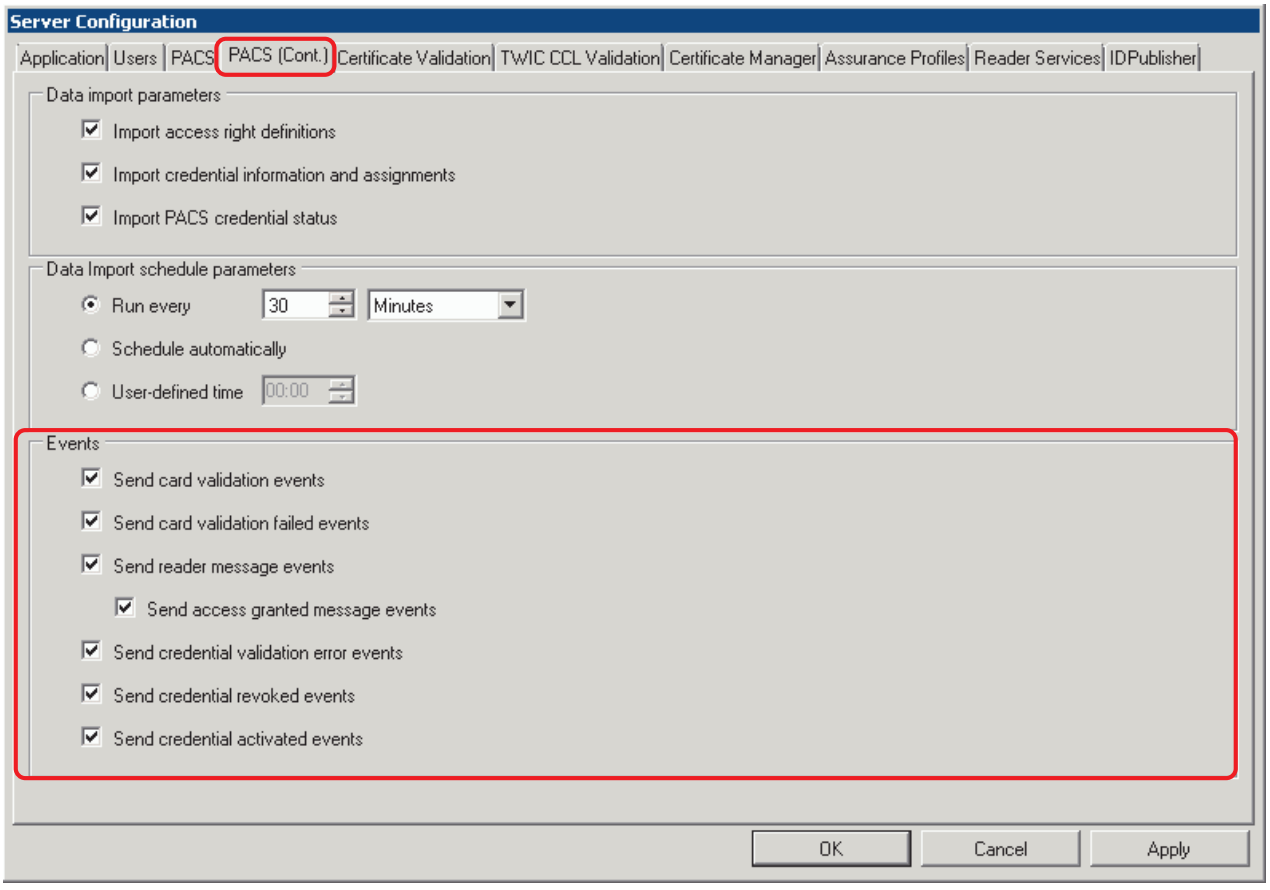
5 PACS events

5.1 Overview

Events are triggered as a result of a specific action. By default, when such events occur, the event is logged in the pivCLASS log file but not sent to the PACS. However events can be configured so that the corresponding event is sent to the PACS. The PACS will then handle the event using its standard alarm or event system.

5.1.1 Configuring Events

The PACS Service configurable event options are located on the **Configuration** > **Edit Service Settings** > **PACS (Cont.)** tab.



Option	Description
Send Card Validation Events	Select this option to send events to the PACS when a credential passes validation
Send Card Validation Failed Events	Select this option to send events to the PACS when a credential fails validation
Send Reader Message Events	Select this option to allow PAMs and fixed readers to publish messages to the PACS using Reader Services
Send Access Granted Message Events	Select this option to send "Access Granted" messages from PAMs and fixed readers to the PACS regardless of whether the PACS panel also sends its own PACS specific access granted message. **Note:** This option is not recommended for use with PAMs.
Send Credential Validation Error Events	Select this option to send a message to the PACS that an error occurred when a credential was checked by the Certificate Manager.
Send Credential Revoked Events	Select this option to send a message to the PACS that a credential has been determined to be revoked according to the Certificate Manager
Send Credential Activated Events	Select this option to send a message to the PACS that a credential has been activated after it was determined to be revoked by the Certificate Manager

Section 6

6 Assurance profiles

Pre-configured Assurance Profiles are available to assist sites in creating their own security policies.

		Check TWIC Canceled Card List	Match Fingerprint	Perform CAK Authentication	Perform PIV Authentication	Perform Secure Messaging Authentication	PIN-to-PACS	Require Registration	Require TWIC	Secure Messaging CAK Fallback	Validate CAK Certificate	Validate CHUID Signature Certificate	Validate Fingerprint Template Signature Certificate	Validate PIV Certificate	Validate Secure Messaging Signature Certificate	Verify CHUID	Verify Fingerprint Template	Verify PIN
1	CHUID (TWIC)							✓	✓			✓				✓		
2	CAK (TWIC)			✓				✓	✓		✓							
3	CHUID + BIO (TWIC)		✓					✓	✓			✓	✓			✓	✓	
4	CHUID + CAK + BIO (TWIC)		✓	✓				✓	✓		✓	✓	✓			✓	✓	
5	CHUID (PIV)							✓				✓				✓		
6	PKI + PIN (PIV)				✓			✓						✓				✓
7	PKI + PIN + BIO (PIV)		✓		✓			✓					✓	✓			✓	✓
8	CAK (PIV)			✓				✓			✓							
9	CHUID + CAK (PIV)			✓				✓			✓	✓				✓		
10	CAK + BIO (PIV)		✓	✓				✓			✓		✓				✓	
11	Card ONLY (no PKI)																	
12	Card + PIN (no PKI)																	✓
13	Card + PACS PIN (no PKI)						✓											
14	Card + PIN + BIO (no PKI)		✓															✓
15	Secure Messaging (PIV)					✓		✓		✓					✓			

Operational Mode	Description
Check TWIC Canceled Card List	Indicates that the PAM must perform a local search of the TWIC Canceled Card List (CCL) using the FASC-N of the presented card. Non-TWIC cards will never appear on the TWIC CCL and will therefore, always pass this check.
Match Fingerprint	Indicates that readers assigned this assurance profile must prompt the cardholder for a biometric sample and attempt to match it against the biometric templates stored on the card.
Perform CAK Authentication	Indicates that readers assigned this assurance profile must perform card authentication by issuing a challenge to the credential using the public key associated with its card authentication certificate and verifying the response that is returned.
Perform PIV Authentication	Indicates that readers assigned this assurance profile must perform PKI authentication by issuing a challenge to the credential using the public key associated with its PIV authentication certificate and verifying the response that is returned.
Perform Secure Messaging Authentication	Indicate that readers assigned this assurance profile must perform Secure Messaging authentication. Secure Messaging is an optional feature and is not supported by all smart card credentials.
PIN to PACS[1]	Indicates that readers assigned this assurance profile must prompt the cardholder for their PACS PIN and submit this PIN to the PACS for verification. **Note:** It is very important to recognize that the PIN the cardholder must enter is the PIN they were assigned in the PACS and not the PIN used to access their smart card credential. These two PINs are virtually guaranteed to differ in form and content.
Require Registration	Indicates that a credential must be registered with pivCLASS for access to be granted at the door. If this option is 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 **pam\certs** directory beneath in the pivCLASS PACS Service directory.
Require TWIC	Indicates that readers assigned this assurance profile must reject credentials that do not contain a TWIC applet.
Secure Messaging CAK Fallback	Indicates that readers should fallback to CAK authentication if the credential does not support the Secure Messaging feature. When this option is selected and a smart card credential is presented that does not support Secure Messaging, the PAM will perform the following translations before continuing: • The selected state of the **Perform Secure Messaging Authentication** option is temporarily assigned to the **Perform PKI CAK** option • The selected state of the **Validate Secure Messaging Signature Certificate** option is temporarily assigned to the **Validate Card Authentication Certificate** option.
Validate CAK Certificate	Indicates that readers assigned this assurance profile must validate the Secure Messaging signature certificate and check its revocation status using OCSP, SCVP, or up-to-date CRLs.
Validate CHUID Signature Certificate	Indicates that readers assigned this assurance profile must validate the CHUID signature certificate and check its revocation status using OCSP, SCVP, or up-to-date CRLs.
Validate Fingerprint Template Signature Certificate	Indicates that readers assigned this assurance profile must validate the fingerprint template signature certificate and check its revocation status using OCSP, SCVP, or up-to-date CRLs.

Operational Mode	Description
Validate PIV Authentication Certificate	Indicates that readers assigned this assurance profile must validate the PIV authentication certificate and check its revocation status using OCSP, SCVP, or up-to-date CRLs.
Validate Secure Messaging Signature Certificate	Indicates that readers assigned this assurance profile must validate the Secure Messaging signature certificate and check its revocation status using OCSP, SCVP, or up-to-date CRLs.
Verify CHUID	Indicates that readers assigned this assurance profile must read the entire CHUID from the credential, verify its signature, and assert that the expiration date it contains has not already passed.
Verify Fingerprint Template	Indicates that readers assigned this assurance profile must verify the fingerprint templates found on the credential.
Verify PIN	Indicates that readers assigned this assurance profile should prompt the operator to enter their PIN, preferably using SPE (Secure PIN Entry), and use this PIN to unlock the card.

PIN to PACS Features/Requirements[1]

- Maximum PIN length: 15 digits
- PIN entry timeout: 15 seconds
- PACS PIN retries: Not supported
- Termination character: Pound (#)
- PIV cards only (PIN to PACS will not work for legacy card pass through)

Note: If the PAM denies access, due to an authorization failure, the PAM may still prompt for PACS PIN. If the card is left in the slot after the PAM denies access the LCD may continue to prompt for PACS PIN.

This page is intentionally left blank.

Section 7

7 Troubleshooting

This section provides information related to viewing and collecting diagnostic messages that can assisting in troubleshooting issues when pivCLASS® system problems occur. The section also provides lists of log messages, PAM error codes definitions and, event messages.

7.1 Logs and events

The pivCLASS® system provides features for generating and viewing both informative and diagnostic messaging through logs and events on the pivCLASS PACS server. These logs and events provide useful information about patterns of use and system performance, and can assist when troubleshooting issues.

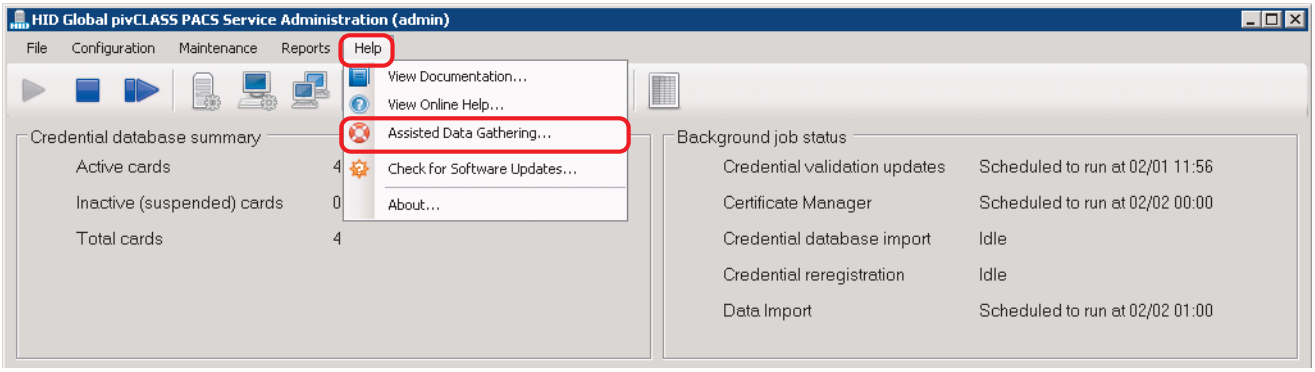
For detailed information about viewing logs, turning on debug logging, and omitting certain data, such as Personally Identifiable Information (PII), from logs, see *Section 4.8 Log file administration*.

For information about configuring event options, see *Section 5 PACS events*.

7.2 Collect troubleshooting data

If error conditions occur in the pivCLASS System, and technical assistance is required, the pivCLASS PACS Administration application allows the user to collect important debugging data from the pivCLASS environment, via a data gathering wizard, and package the resulting information. The packaged debug information can then be emailed (or uploaded) to pivCLASS Technical Support to assist with troubleshooting issues.

To access the **Assisted Data Gathering** wizard select **Help** > **Assisted Data Gathering** from the pivCLASS PACS Service application main menu and follow the instructions presented in the wizard to create, gather, and package debugging information related to an issue or problem.



7.3 Log/Event messages and error codes

The following tables list log messages, event messages, and PAM error codes.

7.3.1 Log messages for card validation errors

Each of the log messages listed below will occur during an access request transaction (for example, when a card is presented to a reader).

Note: In cases where the Reader Display Message can have multiple causes the only way to identify which failure occurred is to check the pivCLASS PAM debug logs, the pivCLASS Embedded Authentication debug logs, or the PACS Service debug logs.

Log Message	Reader Display Message
CHUID expiration date has passed	Invalid Card
CHUID signature is invalid	Invalid Card
Failed to decode challenge response	Invalid Card
challenge and response length not equal	Invalid Card
Decrypted challenge does NOT equal original challenge data	Invalid Card
CHUID Card ID does not match Card Authentication Cert	Invalid Card
CHUID Card ID does not match PIV Authentication Key	Invalid Card
Failed to read Fingerprint Template from card	Invalid Card
No TPK present in database	Invalid Card
Could not decrypt TWIC fingerprint template	Invalid Card
Fingerprint Not Before date has not been reached	Invalid Card
Fingerprint Not After date has passed	Invalid Card
Failed to read TPK from card	Invalid Card
Failed to select PIV applet	Invalid Card
Card does not support Secure Messaging	Invalid Card
Card found on TWIC CCL	Invalid Card
Certificate Not Before date has not been reached	Invalid Card
Certificate Not After date has passed	Invalid Card
Certificate status cannot be determined	Invalid Card
Card not registered in Pacs Service Database	Invalid Card
Card passed validation successfully	Valid Card

7.3.2 PAM/Embedded Authentication error codes

Value	Name	Meaning
1001	JVR_ERROR_CARD_INIT	Smart card failed to initialize
1002	JVR_ERROR_CARD_NOPIV	Smart card does not support the PIV applet
1003	JVR_ERROR_CARD_CHUID_READ	Failed to read CHUID from card
1004	JVR_ERROR_CERT_READ	Failed to read certificate from card
1005	JVR_ERROR_FINGERPRINT_READ	Failed to read fingerprint template from card
1006	JVR_ERROR_CARD_NOTWIC	Card does not contain the TWIC applet but the assurance profile requires it
1007	JVR_ERROR_TPK_READ	Failed to read TPK element from TWIC card
1008	JVR_ERROR_CARD_NOT_REGISTERED	Presented card is not registered in the PACS Service database
2001	JVR_ERROR_CHUID_DECODE	Failed to decode CHUID
2002	JVR_ERROR_CHUID_DECODE_TLV	Failed to decode CHUID BER TLV data
2003	JVR_ERROR_CHUID_DECODE_SIGNATURE	Failed to decode CHUID signature
2004	JVR_ERROR_CHUID_EXPIRED	CHUID has expired
2005	JVR_ERROR_CHUID_SIGNATURE_INVALID	CHUID signature was not valid
3001	JVR_ERROR_CERT_VALIDATION	Certificate was not valid
3002	JVR_ERROR_CERT_NOT_BEFORE	Certificate “not before” time has not been reached
3003	JVR_ERROR_CERT_NOT_AFTER	Certificate “not after” time has passed
3004	JVR_ERROR_CERT_STATUS_INVALID	Certificate status is not valid
3005	JVR_ERROR_CERT_STATUS_EXPIRED	Cached certificate status has expired
3006	JVR_ERROR_CERT_STATUS_UNKNOWN	Certificate status cannot be determined from cache or server
4001	JVR_ERROR_VERIFY_PIN	PIN verification failed
4002	JVR_ERROR_VERIFY_PIN_DIRECT	PIN verification failed
5001	JVR_ERROR_INTERNAL_AUTHENTICATE	Internal Authenticate process (cryptographic challenge/response) failed
6001	JVR_ERROR_CARD_ID_CROSSCHECK	Card ID numbers are not consistent across all analyzed data elements
7001	JVR_ERROR_FINGERPRINT_DECODE_TLV	Fingerprint template malformed
7002	JVR_ERROR_FINGERPRINT_DECODE_SIGNATURE	Fingerprint template has missing or invalid signature
7003	JVR_ERROR_FINGERPRINT_NOT_BEFORE	Fingerprint template not before time has not been reached
7004	JVR_ERROR_FINGERPRINT_NOT_AFTER	Fingerprint template “not after” time has passed
7005	JVR_ERROR_FINGERPRINT_MISSING_FASCN	Fingerprint signature is missing the FASC-N
7006	JVR_ERROR_FINGERPRINT_INVALID_FASCN	Fingerprint template FASC-N does not match signature FASC-N

Value	Name	Meaning
7007	JVR_ERROR_FINGERPRINT_MISSING_GUID	Fingerprint signature is missing the GUID
7008	JVR_ERROR_FINGERPRINT_SIGNATURE_INVALID	Fingerprint signature does not match template data
7009	JVR_ERROR_FINGERPRINT_MATCH_FAILED	Live biometric failed to match template
8001	JVR_ERROR_SECURE_MESSAGING_QUERY	Secure Messaging query failed
8002	JVR_ERROR_SECURE_MESSAGING_DECODE	Decoding of the SM reply failed
8003	JVR_ERROR_SECURE_MESSAGING_AUTH	Authentication of the reply failed
9001	JVR_ERROR_TWIC_CCL_CHECK	Either the card is on the TWIC CCL or there was a problem processing the CCL
9002	JVR_ERROR_COMM_PACS_SERVICE	There was an error communicating with the PACS Service system
9003	JVR_ERROR_INTERNAL_PACS_SERVICE	The PACS Service returned an unexpected error code
9004	JVR_ERROR_COMM_READER	There was an error communicating with the reader
9005	JVR_ERROR_COMM_CARD	There was an error communicating with the card

7.3.3 Events associated with general operation

The following events are not associated with an access request transaction (for example, when a card is presented to a reader). They occur at any time and will not result in a Reader Display Message.

PAM and Embedded Authentication:

- EVENT_READER_ONLINE
- EVENT_READER_OFFLINE
- EVENT_PACS_SERVICE_ONLINE
- EVENT_PACS_SERVICE_OFFLINE

PAM only:

- EVENT_TAMPER_TRIGGERED
- EVENT_TAMPER_RESET
- EVENT_POWER_FAIL_TRIGGERED
- EVENT_POWER_FAIL_RESET
- EVENT_READER_TAMPER_TRIGGERED
- EVENT_READER_TAMPER_RESET

Appendix A

A User feedback at the reader

When available, the pivCLASS® system provides both informative and diagnostic messaging through the use of a reader display.

A.1 Reader display messages

The following table lists the pivCLASS Authentication Module (PAM)/pivCLASS Embedded Authentication device reader display messages currently implemented.

Text Message	Triggering Event	Notes
Card Detected	Card is detected by reader.	
Configuring System	Indicates a change on the server side that affects the PAM or reader configuration.	
Insert Card	Reader requires card to be inserted in the contact slot.	
Present Card	Reader will accept a card to be read from the contact or contactless interface.	
Remove Card	Card has been processed. Remove card from the reader.	
Door Unlocked	Cardholder enrolled, card valid and cardholder authorized for access. Signal returned from the panel indicating the door strike was triggered.	
Enter PACS PIN	Prompt user to enter a PACS PIN.	
Access Granted	Cardholder enrolled, card valid and cardholder authorized for access.	
Access Denied	Cardholder enrolled, card valid but cardholder NOT authorized for access.	Check the PACS Service and PAM debug logs for details of the failure.
Valid Card	Cardholder enrolled, card valid but cardholder authorized for access.	
Invalid Card	Unsuccessful validation. Multiple reasons for this message: • Cardholder not enrolled • Certificate revoked • Signature validation check failed	
Invalid PIN	Incorrect PIN	

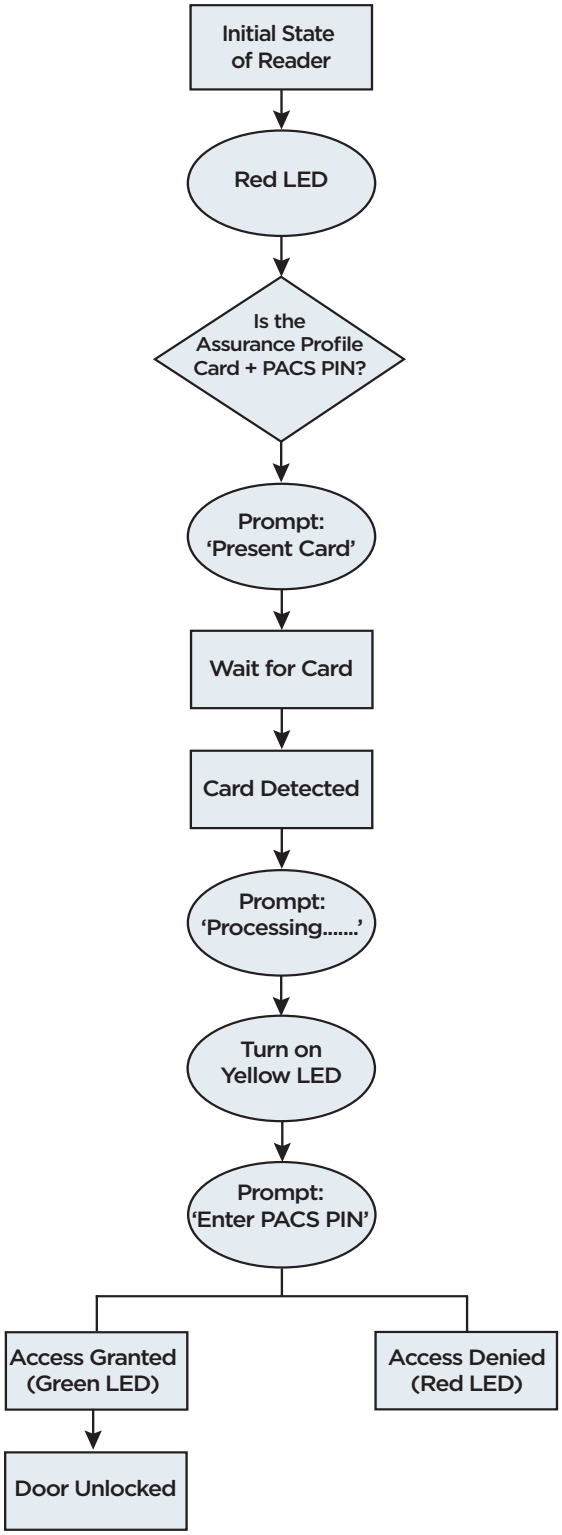
Text Message	Triggering Event	Notes
Processing.....	Validating the card.	
Match Failed Remove finger from sensor	Fingerprint match failed.	
Match Failed	Fingerprint match failed.	
Enter Card PIN	Prompt user to enter a PACS PIN.	
(n) finger	(n) represents the FP template from the card.	The display indicates which finger to use

A.2 Reader beeper and LED states

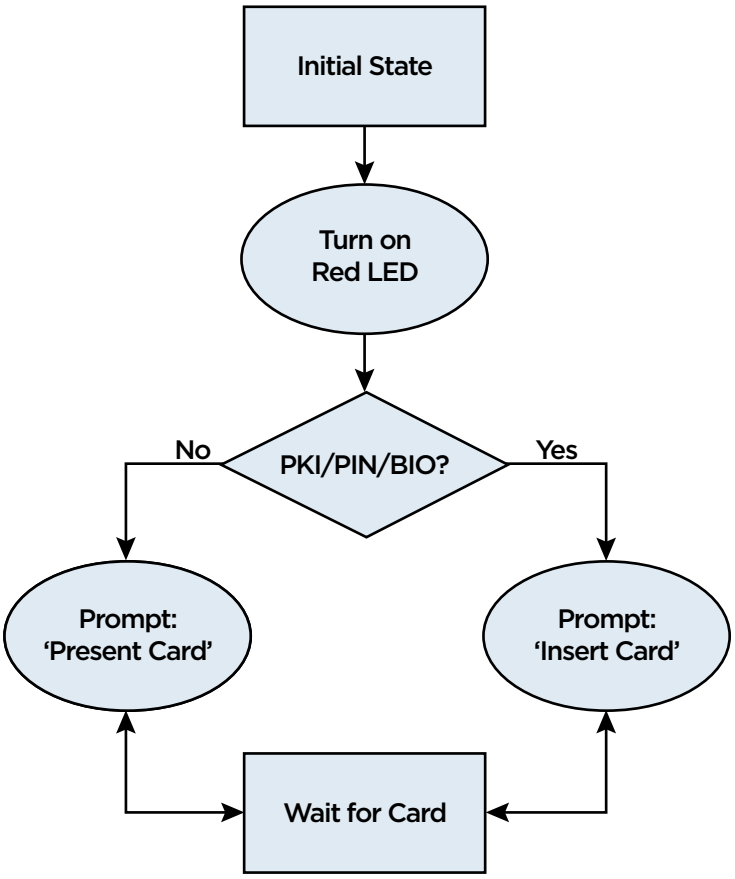
- Green - door unlocked (If PACS configured and access granted). Reader not able to detect the state of the door, just Green LED trigger.
- Red - door locked (or Standby/Idle). Reader not able to detect the state of the door, just Red LED trigger.
- Yellow - processing card (Processing Card)
- 1 beep - good (Compatible card was read)
- 3 beeps and flash Blue LED- card communication error indicated (If PACS configured and access denied > Card Valid Access Denied)

The following sections describe the different pivCLASS reader LED behavior.

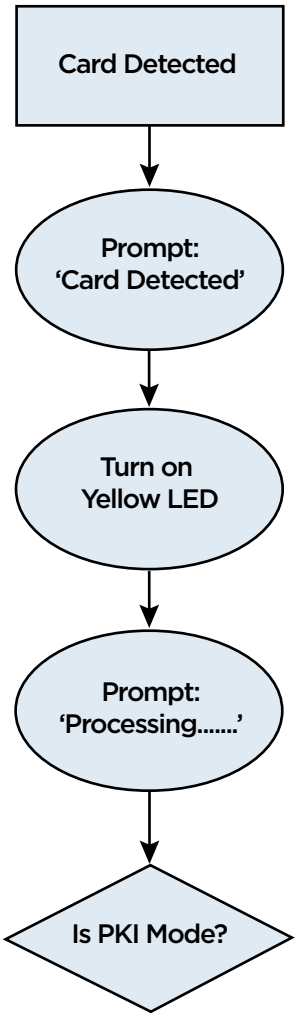
LED PIN to PACS (No PKI)



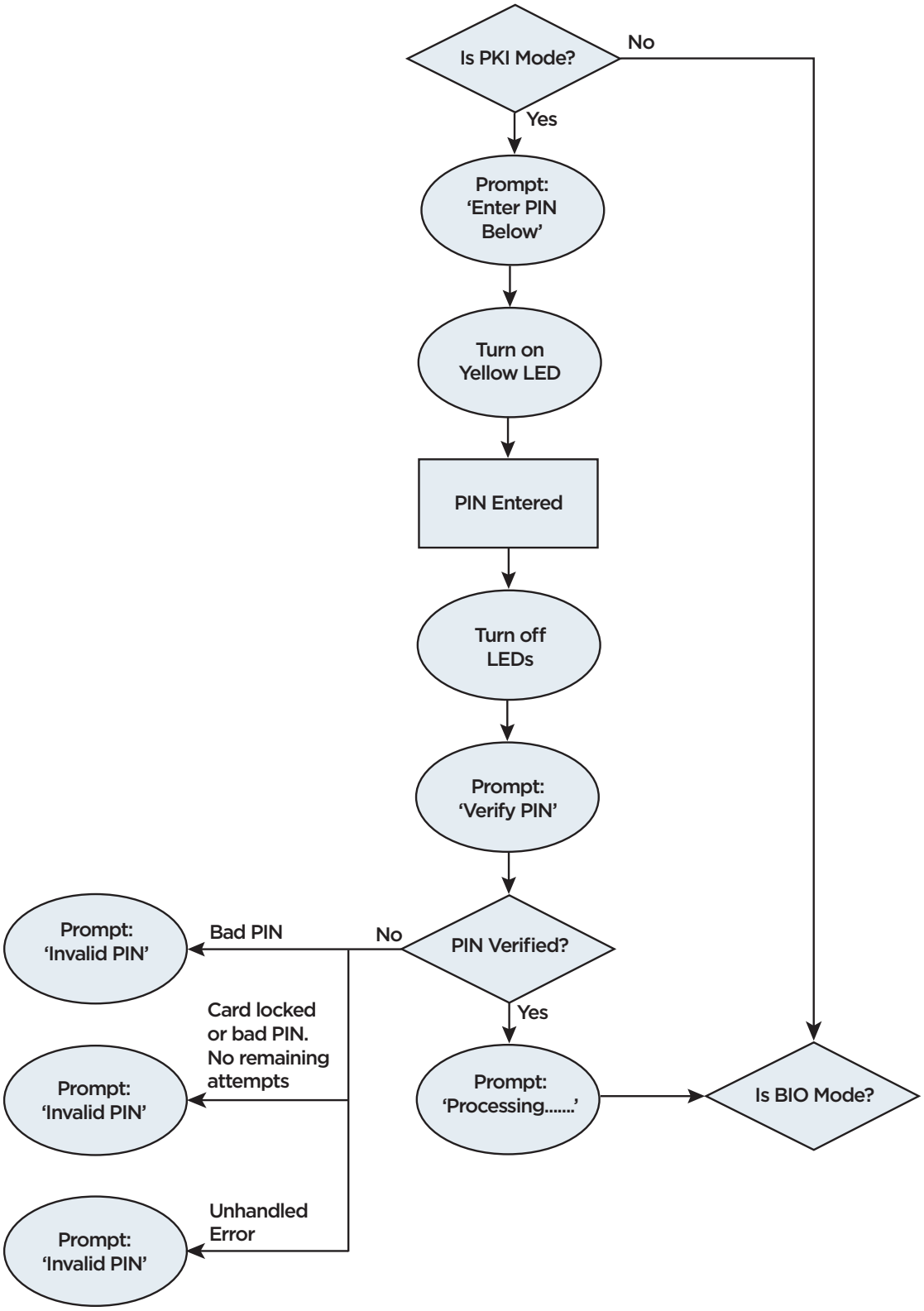
LED Initial State (PKI)



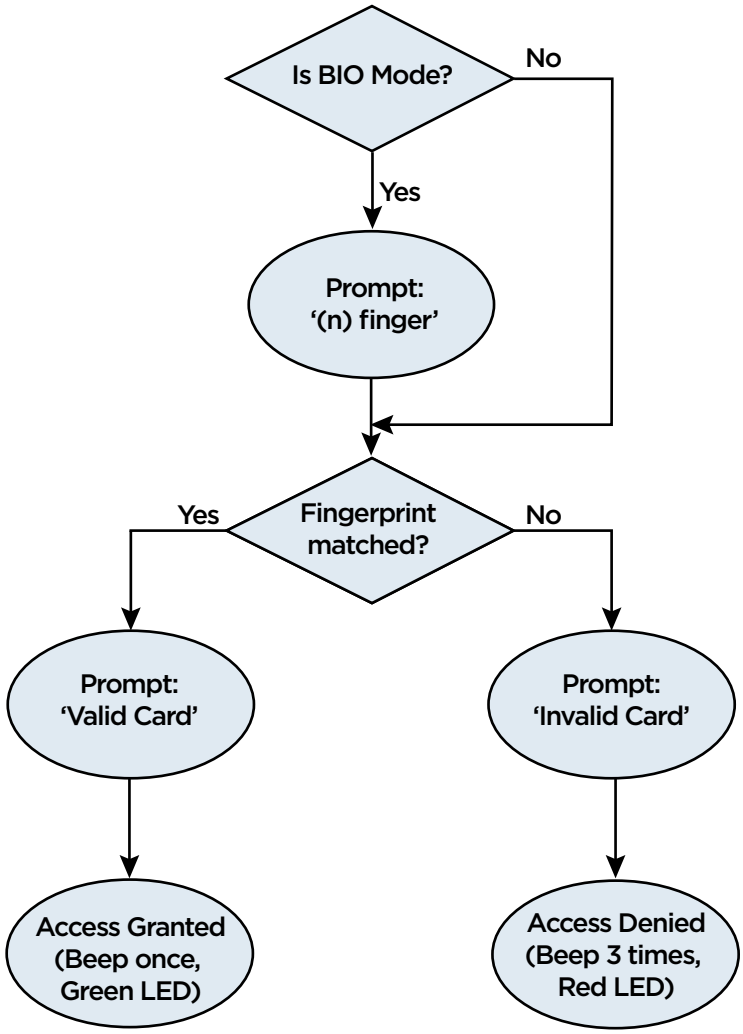
LED Card Detected



LED PIN Entry



LED Biometrics Behavior



This page is intentionally left blank.

Appendix B

B Optional configuration

B.1 SQL Server Database connection fails to connect

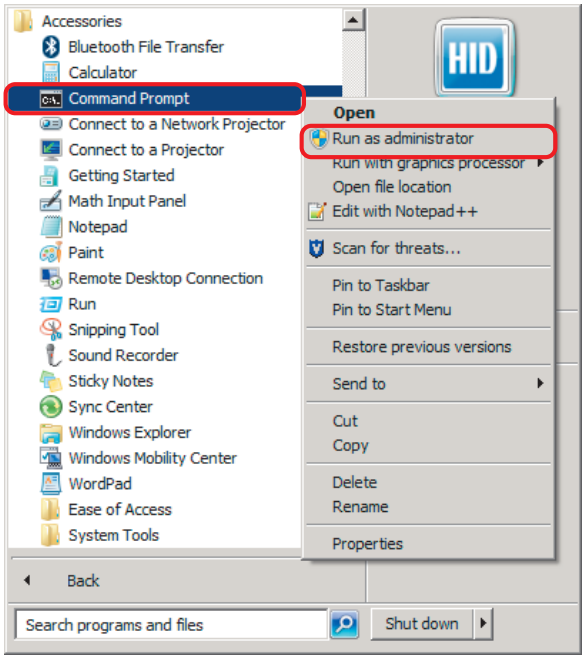
This applies to a PACS Service that is configured to use SQL as a database provider. During a system reboot, the SQL Server may take too long to start causing the PACS Service to terminate. If the PACS Service terminates, it does not automatically try to restart.

The following procedures will assist to determine the existing dependencies, how to obtain the SQL server instance name, then how to construct the command line to add the dependency from this information.

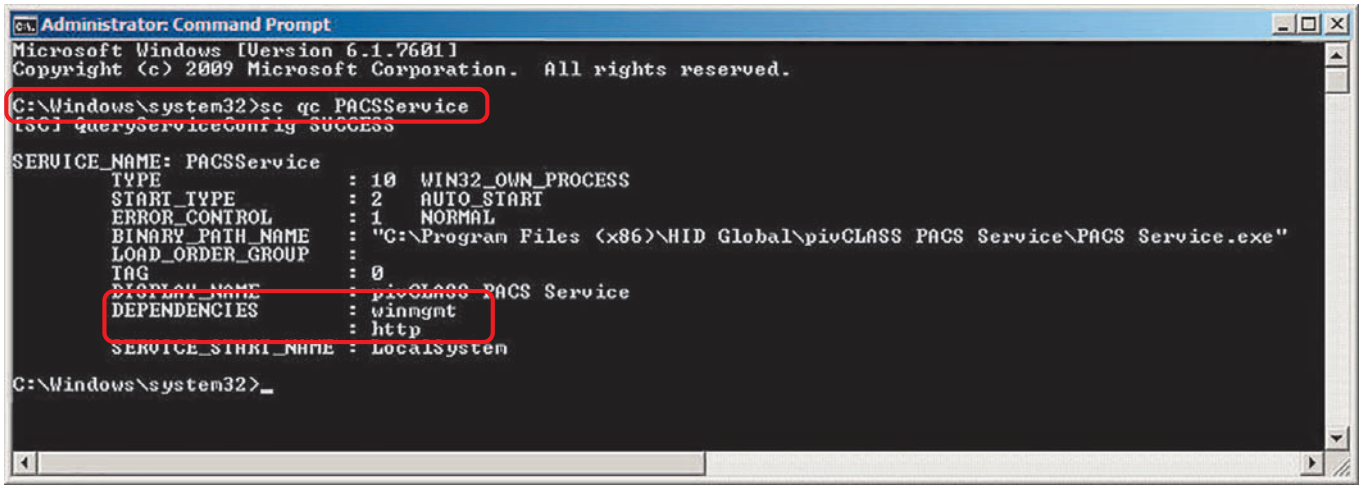
Note: Reinstalling or updating the PACS Service will reset any existing dependencies. This following procedure will have to be repeated after each install or upgrade.

B.2 How to determine the existing dependencies

1. On the computer running the PACS Service and SQL Server, launch a command window with Administrator privileges. Select **Start** > **Accessories**.
2. Right-click on the **Command Prompt** menu option and select **Run as administrator**. The command prompt console will open.

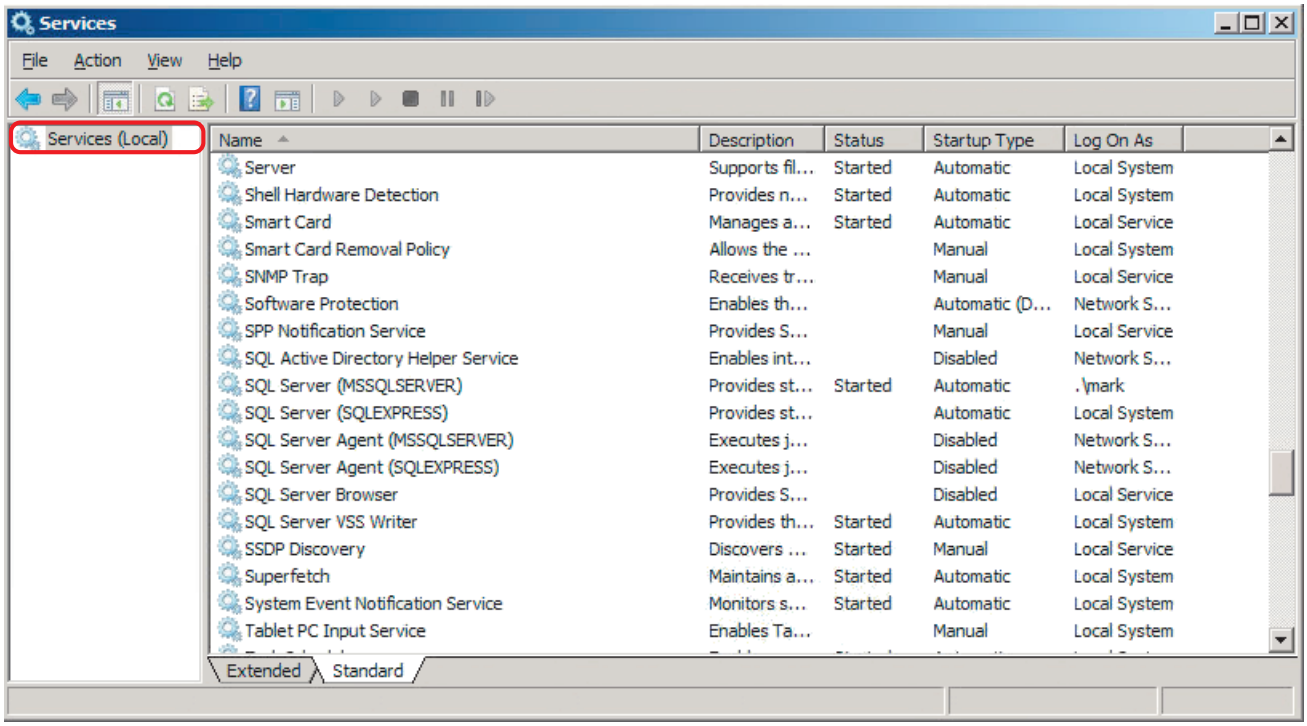


3. At the command line type, `sc qc PACSService`, then press **Enter**. The existing dependencies will be displayed.

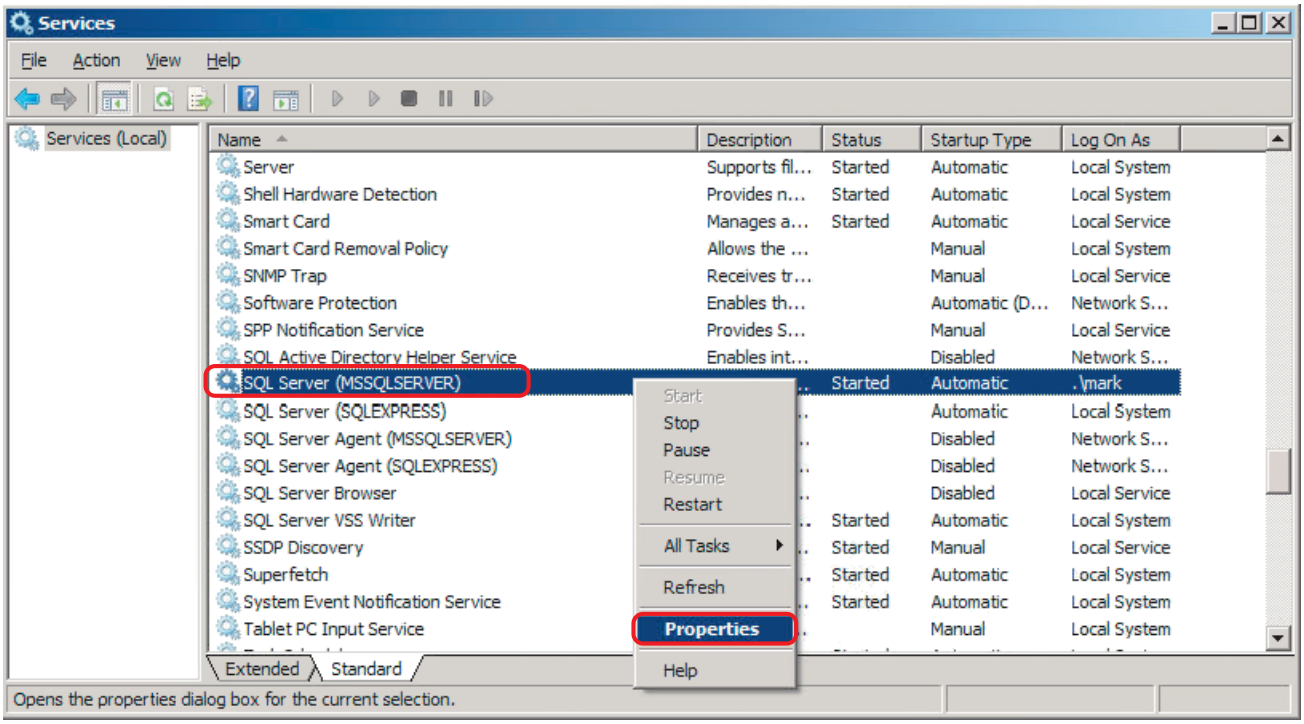


B.2.1 How to obtain the SQL Server instance Service Name

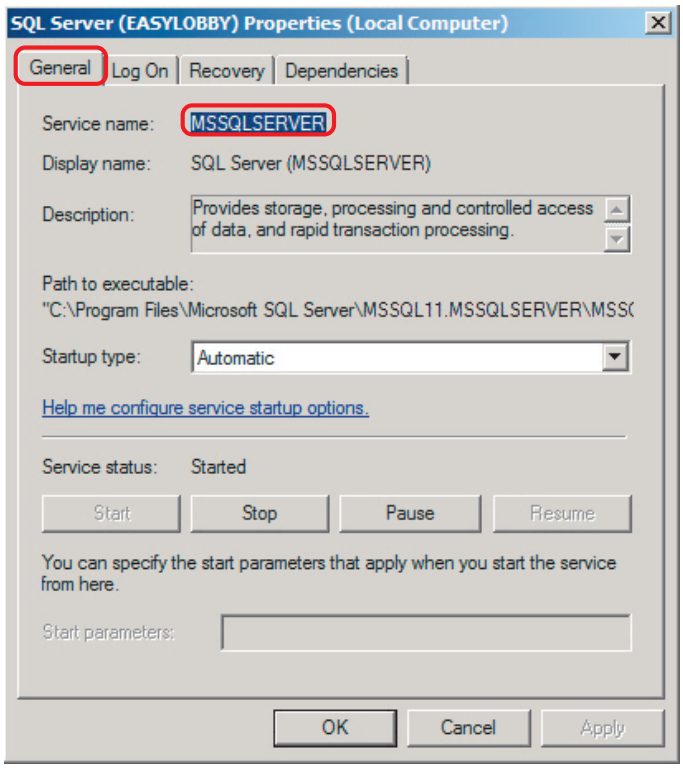
1. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.



2. Right-click on the desired service, and select **Properties**.



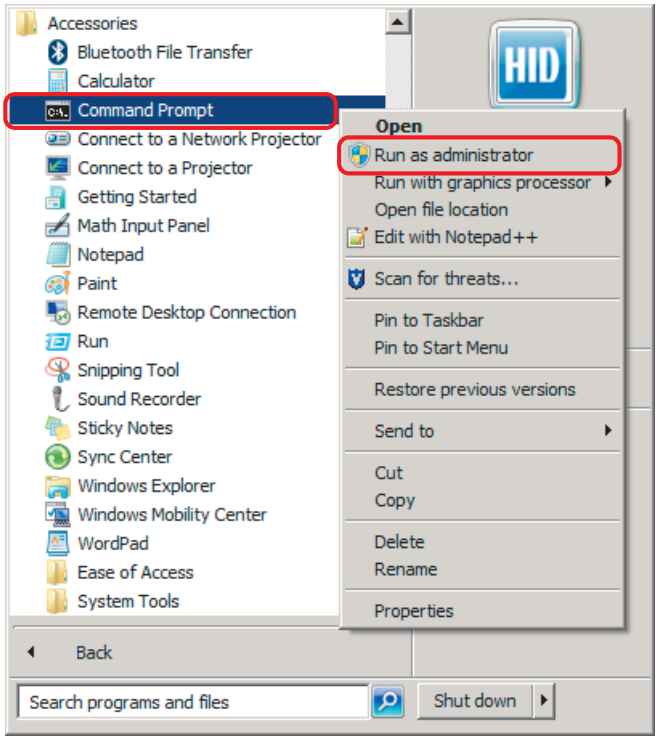
3. The **Service name** is displayed at the top on the **General** tab.



B.2.2 How to construct the command line to add the dependency

The correct solution is to set the service dependencies properly such that the PACS Service is dependent upon the database service. In the case where SQL Server is being used and SQL Server is installed on the same machine as the PACS Service, the PACS Service should be dependent upon the SQL Server service.

1. On the computer running the PACS Service and SQL Server, launch a command window with administrator privileges. Select **Start** > **Accessories**.
2. Right-click on the **Command Prompt** menu option and select **Run as administrator**. The command prompt console will open.

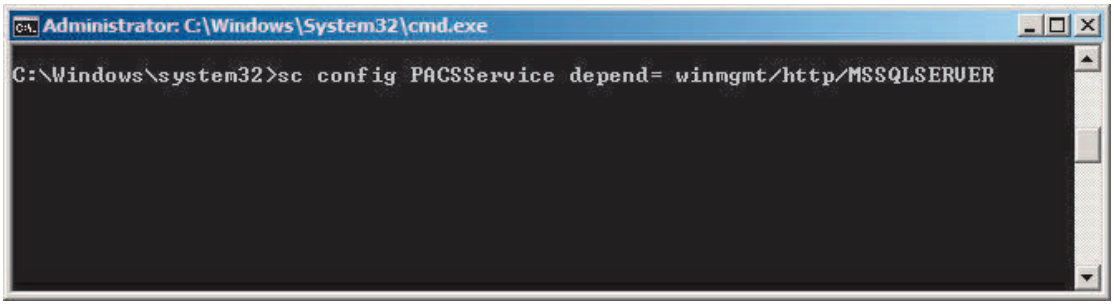


3. At the command line type the following string and press **Enter**:

   ```
   sc config PACSService depend= winmgmt/http/<SQL Server Instance Service Name>
   ```

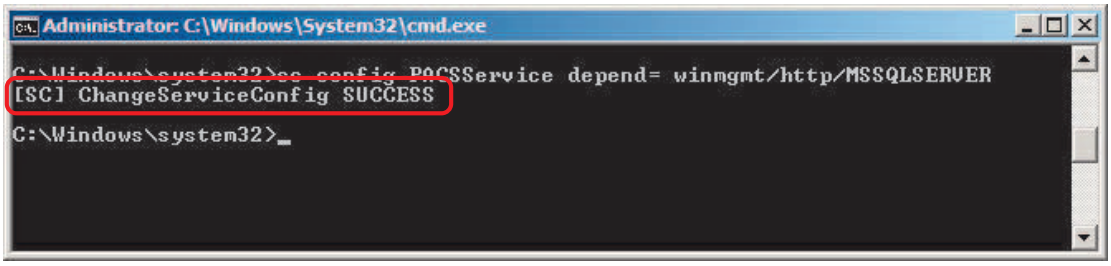
   where `winmgmt` and `http` are the existing dependencies separated by a `/`, and `<SQL Server Instance Service Name>` is the name of the SQL Server instance obtained in the previous section.

Important: Each time you want to add a new dependency, the string must contain all of the existing dependencies separated by a forward slash (/). If you fail to enter the existing dependencies, they will be removed from the list.



4. If the command was successful then the following should display:

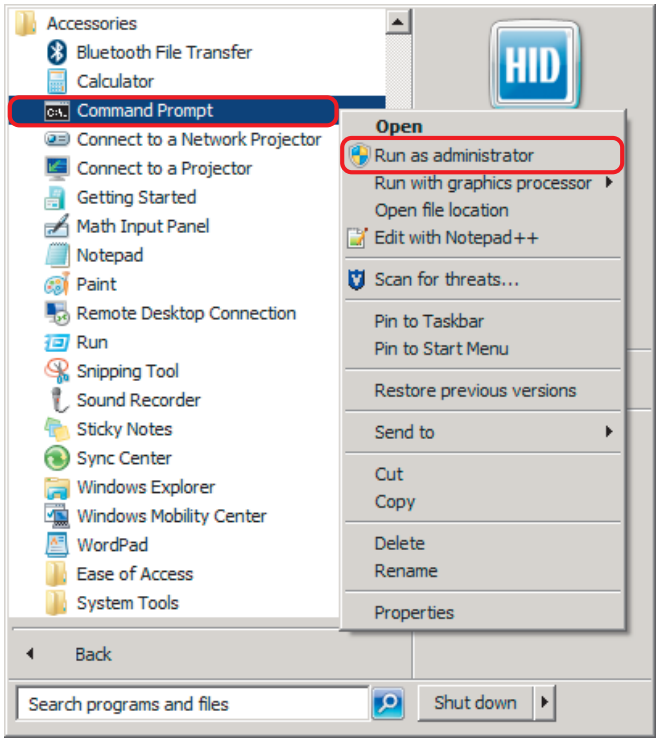
   ```
   [SC] ChangeServiceConfig SUCCESS
   ```



5. Now the dependency on the SQL Server instance running in order for the PACS Service to run has been set.

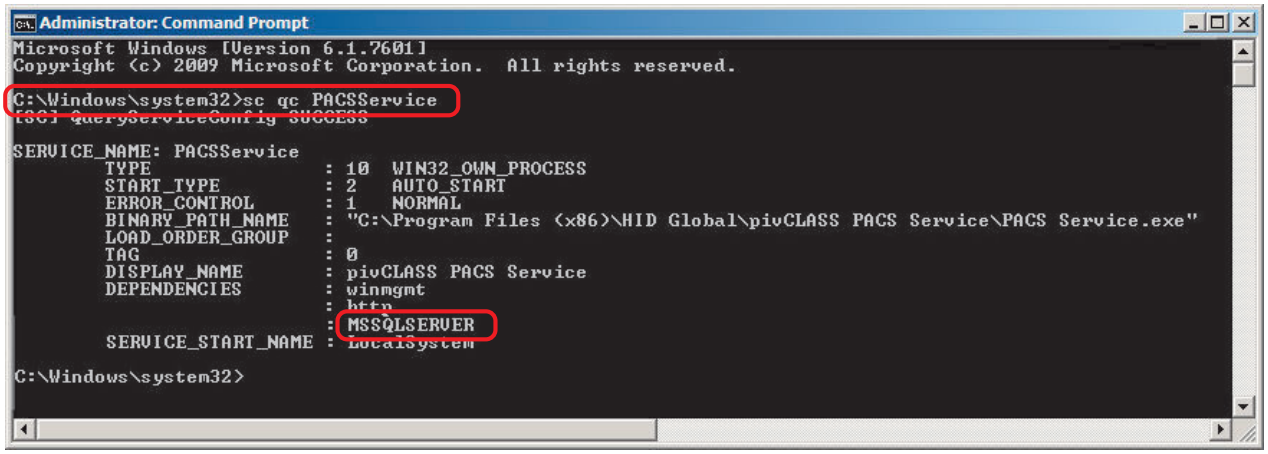
B.2.3 Checking for the new dependency

1. On the computer running the PACS Service and SQL Server, launch a command window with Administrator privileges. Select **Start** > **Accessories**.
2. Right-click on the **Command Prompt** menu option and select **Run as administrator**. The command prompt console will open.



3. At the command line type, `sc qc PACSService`, then press **Enter**.

   The <`SQL Server Instance Service Name`> previously added should be displayed against the list of **Dependencies**.



B.2.4 Connecting through a Web Proxy (no authentication)

1. Stop the PACS Service.
2. Copy the text from between the lines below specifying the proxy IP address and port:

```
------------------------------------------------------------------------------
<system.net>
   <defaultProxy>
      <proxy proxyaddress="http://192.168.1.10:3128" bypasslocal="false" />
   </defaultProxy>
</system.net>
------------------------------------------------------------------------------
```

3. Paste this portion of the XML into the <configuration> section of the following files in the PACS Service installation directory:
   - **PACS Service Administration.exe.config**
   - **PACS Service.exe.config**
4. Save the files.
5. Restart the PACS Service.

B.2.5 Connecting through a Web Proxy (Windows user authentication)

Set the `useDefaultCredentials="true"` on the <defaultProxy> element if the Windows user account is to be used to authenticate with the proxy.

1. Stop the PACS Service.
2. Copy the text from between the lines below specifying the proxy IP address and port:

```
------------------------------------------------------------------------------
<system.net>
   <defaultProxy useDefaultCredentials="true">
      <proxy proxyaddress="http://192.168.1.10:3128" bypasslocal="false" />
   </defaultProxy>
</system.net>
------------------------------------------------------------------------------
```

3. Paste this portion of the XML into the <configuration> section of the following files in the PACS Service installation directory:
   - **PACS Service Administration.exe.config**
   - **PACS Service.exe.config**
4. Save the files.
5. Restart the PACS Service.

   Note: If after completing the above steps a connection is failing through the web proxy configured at the site. Contact the IT Department and request assistance.

Appendix C

C Modify the PACS Service logon

The pivCASS PACS Service is initially installed to run as the Local System account, however the recommended best practice is to create a user, or user group, with a more restrictive set of security permissions that are sufficient to run the PACS Service. The following sections provide information and recommended suggestions that will assist in creating a user or user group.

Note: The following procedures are intentionally generic due to the various Windows operating systems that the PACS Service can run on and the different network configurations the system can be deployed on.

C.1 Configure user account to have "Log on as a service" permissions

Any user that is created to run the pivCLASS PACS Service (the service name is PACSService) must have the ability to start and stop the service. One method to achieve this would be to add the user or user group to the **Log on as a service** policy:

1. Log onto the computer with administrative privileges.
2. Open the **Control Panel** and select **Administrative Tools**.
3. Double click **Local Security Policy** to open the Management Console.
4. Expand the **Local Policies** option and click on **User Rights Assignment**.
5. In the right pane, right click on **Log on as a service** and select **Properties**.
6. On the **Local Security Setting** tab select **Add User or Group**.
7. In the **Select Users, Computers, Service Accounts, or Groups** dialog, find the user you wish to enter and click **OK**.
8. In the **Log on as a service Properties** dialog, click **OK** to save changes.

C.2 Establish access control list url reservations for HTTP prefixes

As the PACS Service registers HTTP prefixes for the PAM, PACSServiceSDK and IDPublisher, a new user would need to establish access control list (acl) url reservations for the HTTP prefixes. One method to achieve this would be to use netsh (Network Shell) to run a `http add urlacl` command, for example:

```
http add urlacl url=http://*:8081/IDPublish user=Domain_or_Host_name\user_name
```

The default HTTP url prefixes are:

- `http://*:8081/IDPublish`
- `http://*:10200/PAM`
- `http://*:8080/PACSServiceSDK`

C.3 Grant NTFS permissions

The PACS Service user or user group will need Windows standard NTFS modify permissions on the installation directory of the PACS Service and all sub directories and files in the installation directory tree.

To set Windows standard NTFS permissions:

1. On your machine navigate to the PACS Service installation directory, normally:

   C:\Program Files (x86)\HID Global\pivCLASS PACS Service

2. Right click on the installation directory and select **Properties**.
3. Select the **Security** tab.
4. Under **Group or user names**, select a group or user and click **Edit**.
5. Under **Permissions or Administrators**, select **Allow** or **Deny** for any of the available permissions.
6. When the permission options are set click **OK**.

C.4 Configure DML, DDL, and TCL permissions

The PACS Service user account, or any account that is configured to connect to and use the credential database, will need full database DML (Data Manipulation Language) permissions, DDL (Data Definition Language) permissions, and TCL (Transactional Control Language) permissions.

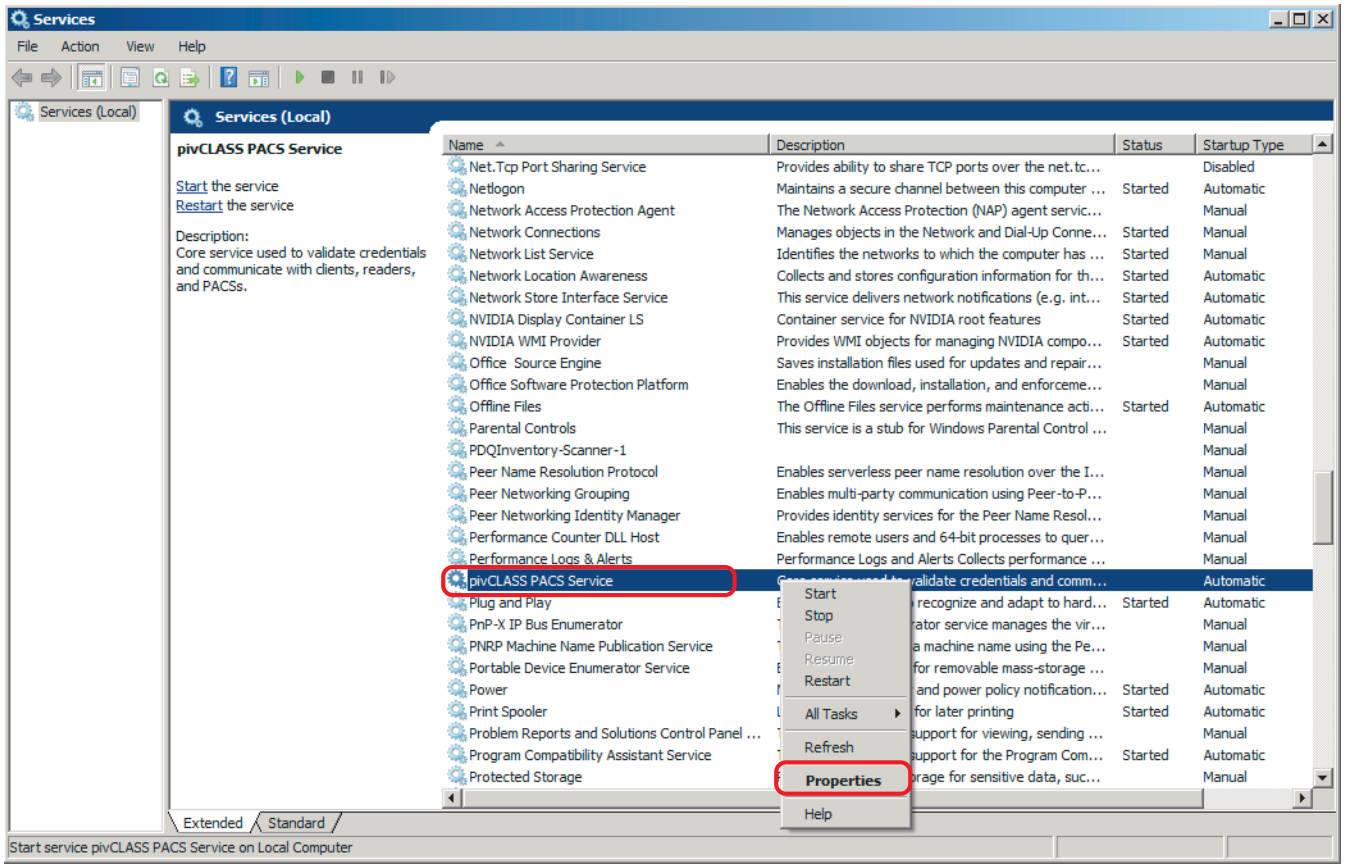
The methods for configuring DML, DDL, and TCL permissions vary from platform to platform and you will have to consult your DBMS specific documentation for the exact procedure.

C.5 Change the PACS Service user account logon

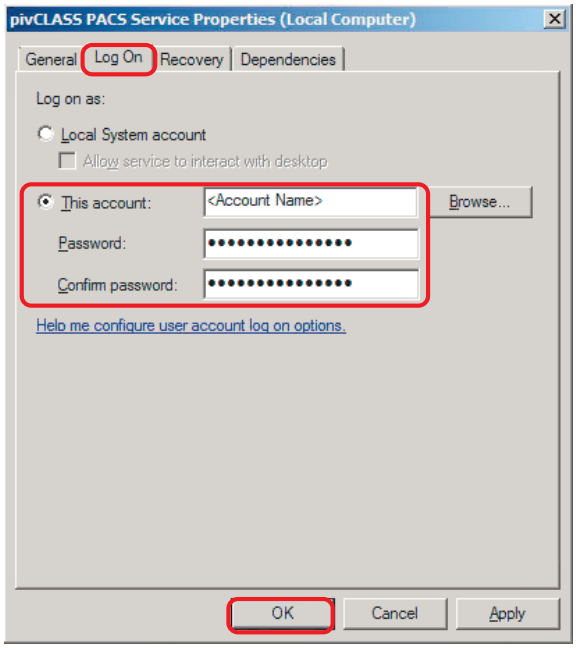
Note: This applies to the **Application** tab and the **PACS** tab for plug-ins that use an ADO.NET database connection.

In some instances a temporary administrative account is created for installations and therefore may not have the appropriate access to the database. To assure the correct access is used to connect to the database use the Window Services applet to configure the PACS Service with the desired account logon credentials.

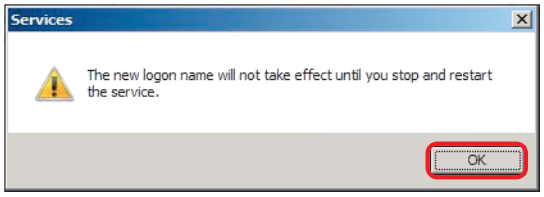
1. In the PACS Service application configure the **Application** tab and/or the **PACS** tab with a connection string that allows read access to the database when running as the desired service account.
2. At this point, the PACS Service is still configured to Log on as the local system account. On the **PACS Service Administration** window click **File** > **Service Control** > **Stop**.
3. Exit the PACS Service application.
4. Use the Windows Services applet to configure the PACS Service with the desired account log on credentials. Select the **Start** > **Control Panel** > **Administrative Tools** > **Services**.
5. Right-click on **pivCLASS PACS Service** and select **Properties**.



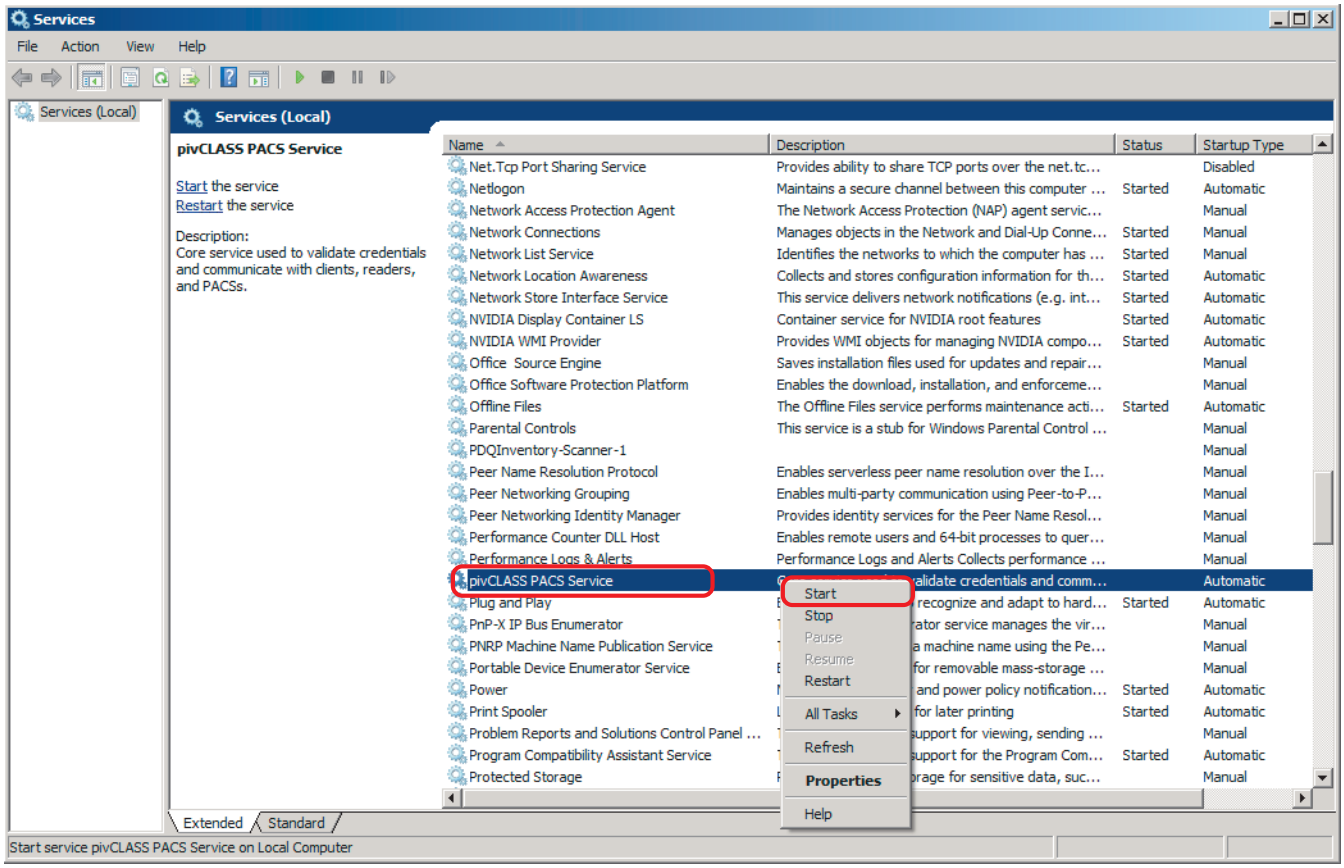
6. Select the **Log On** tab.
7. Select **This account** and enter the desired account's credentials.
8. Click **OK**.



9. Click **OK** to stop and restart the Service.



10. Right-click on **pivCLASS PACS Service** and select **Start**.



From this point forward, the PACS Service will be able to access the Credential and PACS databases, including across reboots.

Note: Any account that accesses the pivCLASS PACS Service application will not be able to stop/start the service, nor will it be able to configure connection strings.

Note: If connection strings are modified on the **Application** or **PACS** configuration tabs to a different database, or to an incorrect location, there may be issues when restarted as the service itself is configured using the log on credentials described above.

On a software upgrade the user will be prompted for the Windows account information for the service account if it has been changed from the default (Local System).

This page is intentionally left blank.

Appendix D

D Reference documents

Document Title	Publisher	Date
Federal Information Processing Standard Publication 201-2 (FIPS 201-2) Personal Identity Verification (PIV) of Federal Employees and Contractors	NIST, US Department of Commerce	Sept. 2013
NIST PIV Program web site	http://csrc.nist.gov/groups/SNS/piv/	
NIST Special Publication 800-63-1 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology	NIST, US Department of Commerce	Dec. 2011
NIST Special Publication 800-73-3 Interfaces for Personal Identity Verification - Part 1: End-Point PIV Card Application Namespace, Data Model, and Representation	NIST, US Department of Commerce	Feb. 2010
NIST Special Publication 800-76-1 Biometric Data Specification for Personal Identity Verification	NIST, US Department of Commerce	Jan. 2007
NIST Special Publication 800-78-3 Cryptographic Algorithms and Key Sizes for Personal identity Verification	NIST, US Department of Commerce	Dec. 2010
NIST Special Publication 800-79-1 Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCIs)	NIST, US Department of Commerce	Jun. 2008
NIST Special Publication 800-85A-2 PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-2 Compliance)	NIST, US Department of Commerce	Jul. 2010
NIST Special Publication 800-85B PIV Data Model Test Guidelines	NIST, US Department of Commerce	Jul. 2006
NIST Special Publication 800-85B-1 PIV Data Model Conformance Test Guidelines	NIST, US Department of Commerce	Sept. 2009
NIST Special Publication 800-87 Rev 1 Codes for Identification of Federal and Federally-Assisted Organizations	NIST, US Department of Commerce	Apr .2008
NIST Special Publication 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)	NIST, US Department of Commerce	Nov. 2008
TWIC Reader Hardware and Card Application Specification Version 1.1.1	US Dept of Homeland Security, Transportation Security Administration	May 2012

Document Title	Publisher	Date
TWIC Technical Advisory TA-2008-TWIC001-V1.0 TWIC Reader Functionality Augmentation	US Dept of Homeland Security, Transportation Security Administration	Sept. 2008
TWIC Technical Advisory TA-2009-TWIC001-V1.0 Format for a TWIC Card with no Fingerprint Biometric Data	US Dept of Homeland Security, Transportation Security Administration	Mar. 2009
TWIC Technical Advisory TA-2011-TWIC001-V1.0 Name Change of “HOTLIST” to “CANCELED CARD LIST”	US Dept of Homeland Security, Transportation Security Administration	Feb. 2011
TWIC Technical Advisory TA-2012-TWIC001-V1.0 Clarification of the May 2008 Reader Hardware and Card Application Specification	US Dept of Homeland Security, Transportation Security Administration	May 2012
TWIC Technical Advisory TA-2013-TWIC001-V1.0 Removing Expired TWIC Cards from the Canceled Card List (CCL)	US Dept of Homeland Security, Transportation Security Administration	Feb. 2013
TWIC Technical Advisory TA-2009-TWIC002-V1.0 Additional Error Code Definitions for TWIC Cards	US Dept of Homeland Security, Transportation Security Administration	Mar. 2008
TWIC Technical Advisory TA-2011-TWIC002-V1.0 Release of new TWIC Card and Card Applications	US Dept of Homeland Security, Transportation Security Administration	Jul. 2011
TWIC Technical Advisory TA-2012-TWIC002-V1.0 Renewal of TWIC Intermediary Certificate Authority Certificates TWICCA1 and TWICCA2	US Dept of Homeland Security, Transportation Security Administration	May 2012
TWIC Technical Advisory TA-2013-TWIC002-V1.0 Clarification of Fixed Reader Environmental Requirements	US Dept of Homeland Security, Transportation Security Administration	Jul. 2013
TWIC Technical Advisory TA-2012-TWIC003-V1.0 New Content Signing Certificate for TWIC Cards	US Dept of Homeland Security, Transportation Security Administration	May 2012
TWIC Technical Advisory TA-2013-TWIC003-V1.0 Clarification of TWIC Reader Safety Requirements	US Dept of Homeland Security, Transportation Security Administration	Jul. 2013
TWIC Technical Advisory TA-2012-TWIC004-V1.0 Addition of TWIC Intermediary Certificate Authority TWICCA3	US Dept of Homeland Security, Transportation Security Administration	Dec. 2012
TWIC Technical Advisory TA-2013-TWIC004-V1.0 Clarification of TWIC Reader PACS Interface	US Dept of Homeland Security, Transportation Security Administration	Jul. 2013
TWIC Technical Advisory TA-2013-TWIC005-V1.0 New Location for the Canceled Card List (CCL)	US Dept of Homeland Security, Transportation Security Administration	Sept. 2013
Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials	Smart Card Alliance Publication Number: PAC-07002	Sept. 2007

Glossary

Term	Description
Administrator	An administrator is an individual authorized to manage one or more desktop or mobile biometric terminals. Administrators are provided additional functionality based on their login credentials.
API	Application Programming Interface
APL	Approved Products List
BIO	Biometric
CAK	Card Authentication Key
Cardholder	A cardholder is an individual who has been issued a credential.
CCL	Canceled Card List
Certificate Authority (CA)	A CA is an entity that issues digital certificates to organizations or individuals. The CA is usually well known and universally trusted. A CA may authorize other entities to issue certificates on its behalf, thereby creating or extending a chain of trust. Certificates contain a digital version of this chain so software can verify that each node on the chain of trust is a valid CA. This process is known as Certificate Path Validation.
Certificate Revocation List (CRL)	A CRL is a list of certificates that have been revoked before their expiration by a Certificate Authority.
CHUID	Cardholder Unique Identifier
Desktop Biometric Terminal	A Desktop Biometric Terminal is a standard desktop PC, integrated with the following components: • FIPS 201 compliant smart card reader capable of reading PIV-II compliant cards over its contact interface • FIPS 201 compliant fingerprint capture device
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
IDRC	Intelligent Dual Reader Controller
Mobile Biometric Terminal	A Mobile Biometric Terminal is a mobile, hand-held reader configured with the following components: • FIPS 201 compliant smart card reader capable of reading PIV-II compliant cards over its contact or contactless smart card interface • FIPS 201 compliant fingerprint capture device
Online Certificate Status Protocol (OCSP)	The OCSP defines a series of messages between software applications that need to verify whether the issuing CA has revoked an x.509 digital certificate. An OCSP server does not check the validity of any of the certificates in the chain of certificates associated with the end entity (certificate in question).

Term	Description
Personal Identity Verification (PIV)	FIPS 201 PIV is a two-part standard, referred to as PIV-I and PIV-II, respectively: • Defines the processes and infrastructures that are used in establishing a person's identity and issuing them a credential • Defines technical interoperability requirements for those credentials to be used in a variety of applications
Physical Access Control System (PACS)	A PACS refers to an integrated unit of software, data, firmware, microcontrollers, and ingress/egress devices that control human access to areas within a facility. A PACS head-end usually consists of one or more servers that communicate with field devices to which doors, turnstiles, and access readers are physically connected.
PII	Personal Identifying Information
PKI	Public Key Infrastructure
RSA	RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem.
Server-based Certificate Validation Protocol (SCVP)	SCVP defines a series of messages between software applications that need to verify whether the issuing CA has revoked an x.509 digital certificate. An SCVP server checks the validity of all of the certificates in the chain of certificates associated with the end-entity and can return additional information to enable a relying party (client) to make more intelligent decisions regarding the certificate.
SSO	Single Sign-On
TPK	TWIC Privacy Key
Transportation Worker Identification Credential (TWIC)	The TWIC is a standard that is intended to address the unique needs of transportation workers, most notably within the maritime industry. TWIC breeder documents and biometric data are gathered and processed by systems that comply with FIPS 201 PIV-I. TWIC cards are required to be PIV-II compliant and can be read by any PIV-II compliant smart card reader. The TWIC standard diverges from the PIV-II standard in that it provides for contactless card-reader biometric data exchange, whereas the FIPS 201 PIV-II standard states that biometric data retrieval can only be performed while the card is in physical contact with the reader. The two main factors that drive this are: • TWIC cards are used in high traffic areas, where a mistyped or forgotten PIN creates delays • A corrosive maritime environment can impact contact-based readers
TWIC Privacy Key (TPK) (TWIC cards only)	The TWIC privacy key is used to protect cardholder privacy when transmitting biometric templates over a TWIC contactless interface. An application acquires the TPK from the card's magnetic stripe, the smart card's TPK container, or from a server on a network. pivCLASS Mobile Validator retrieves this key when the smart card is inserted into the contact reader.
User (Operator)	A user is an individual that has been authorized to operate a mobile biometric terminal. pivCLASS Validation Workstation and pivCLASS Mobile Validator enables its extraction and data import functions after it determines the individual logging into the system is authorized to perform user-level functions.

Revision History

Date	Description	Revision
March 2019	Updates implemented: ■ *Section 4.7.4 Reader Services functions*. Update for added functions. ■ *Section 7 Troubleshooting*. Added section for Assisted Data Gathering feature. ■ *Section 1.5 Related material*. Updated section to describe access to pivCLASS documentation.	D.2
November 2018	Updates implemented: ■ *Section 2 pivCLASS PACS Service*. Standardized graphics. ■ *Section 3.1.2 Security recommendations*. Added text for PACS Service user login security recommendations. ■ *Section 3.4 PACS Service initial setup* and *Section 4.2 PACS Service Guided Configuration*. Added new sections for Guided Configuration functionality. ■ *Section 4.3 Credential database configuration*. Updated sub-sections for the more simplified presentation of PACS Service database connection settings. ■ *Section 4.7.1 Panel/Reader parameters*, *Section 4.7.2 Hardware status information*, *Section 4.7.3 Panel auto discovery*, and *Section 4.8.4 Panel log file*. Updated Panel dialog box screenshots. ■ *Appendix C - Modify the PACS Service logon*. Updated section to provide information and recommended suggestions relating to PACS Service user/user group logon security.	D.1