HID® TRISM™ 7.x
Financial Instant Issuance
Administrator Manual

Software Version: 7.0.5200
PLT-07643, A.1
July 2025

Copyright

Trademarks

Contacts

For technical support, please visit: **https://support.hidglobal.com**.

What's new

Date	Description	Revision
July 2025	Adds secure implementation guidelines and updates to software version 7.x.	A.1

A complete list of revisions is available in **Revision history**.

Section **01**

What is TRISM 7?

1.1 What is TRISM 7?

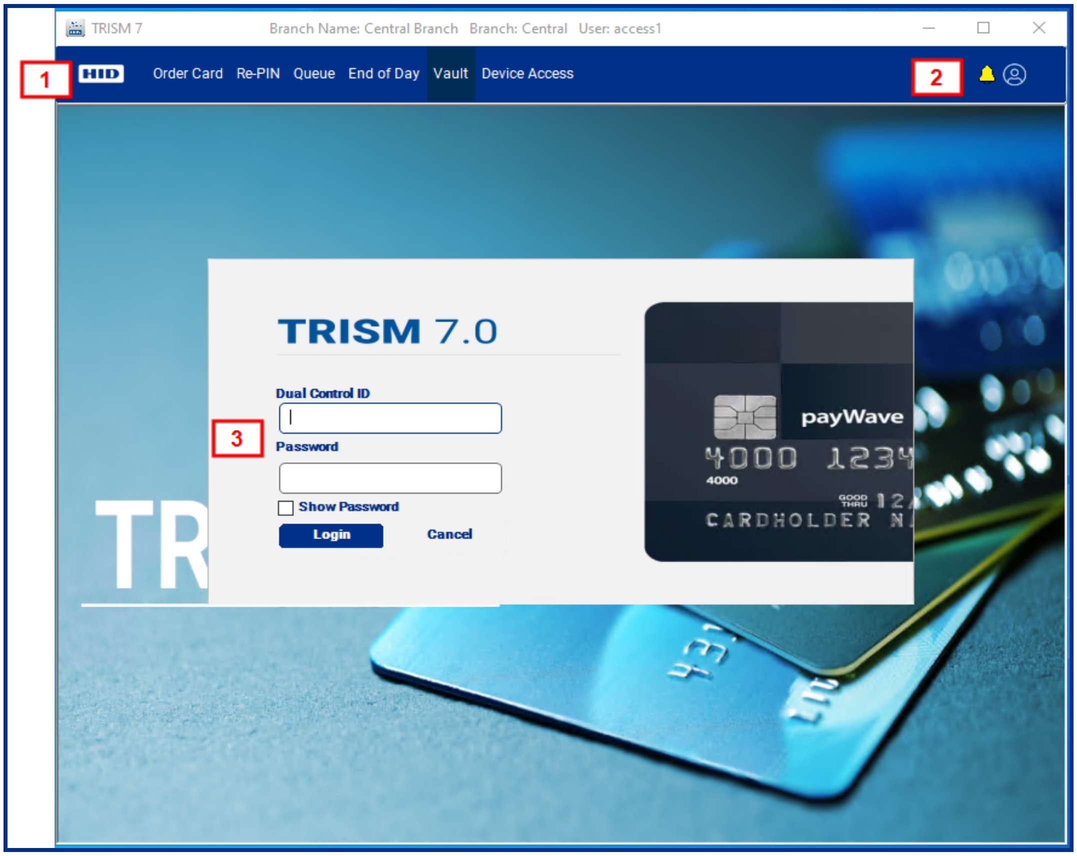
TRISM™ 7 is a unique hardware and software system that provides all the tools needed for the creation and distribution of financial cards of any kind.

Initially introduced in the late 1990s, TRISM provides instant and central issuance of Visa and Mastercard credit and debit cards to financial institutions worldwide.

TRISM works seamlessly with the PCI-certified and listed Hardware Security Module (HSM Duo and HSM XT) to ensure complete privacy of cardholders' information.

From centrally issued, pre-printed cards to customer created cards available for immediate use, TRISM 7 boasts the versatility to meet any institution's most specific demands.

1.2 TRISM 7 user interface



1. Quick launch toolbar.
2. Personal account menu.

   > **Note:** This is referred to as the **Personal icon** within this document.

3. Dual Control Login. Some TRISM features require a second user that is different than the user currently logged in (and with the appropriate permissions), to enter their login credentials.

Section 02

Installation and configuration

2.1 Installation task list

Tasks	**√**
Server	
Install SQL Server 2016+	
Configure SQL Server to accept connections	
Install HSM Manager or XT Key Management System	
Install HSM Manager	
Configure HSM	
Create Calculation Service Config file	
Install T7	
Create databases in T7	
Install and Start HID Calculation Service	
Log in as access1 and update password	
Load PIK in T7	
Add formats	
Add devices	
Install Card Printer Service	
Add vaults	
Add branches	
Set up card stock	
Edit permissions	
Workstation	
Install Client	
Install/update PIN pad drivers	
Print a card for each BIN/Card Cloning	

2.2 Secure implementation guidance

2.2.1 Intended use and operating environment

The TRISM system is intended for use within a secure local area network (LAN) environment with limited access to the internet for integration services (Cores and Activators). It is expected that the customer IT policy provides additional protection, especially when printing and sending sensitive information.

2.2.2 Dedicated server

The TRISM Server, located at the end user's facility, is designed to serve a specific function and should be exclusively dedicated to that purpose. This means that no other applications or software should be installed on the server, ensuring optimal performance and security. By maintaining this dedicated environment, the integrity and reliability of the TRISM Server operations can be preserved.

2.2.3 SQL access control

Only authorized personnel should have access to configure the TRISM settings. After the initial TRISM database instance is built with TRISM Client, it is recommended to change the TRISM Admin password for the databases. Use a strong, unique password and regularly update it according to the end user IT policy.

2.2.4 Network security

Printers, HSMs, databases, and workstations should be connected to a secure LAN with firewall protection. HID FARGO printers disable unused network protocols and services to minimize attack surfaces. HID FARGO printers use the following network ports:

- 80/TCP: Open for HTTP web page
- 443/TCP: Open for HTTPS communication for printing

2.2.5 Print job security

Print job encryption is a critical feature and is used on the HID FARGO printers, ensuring sensitive data related to print jobs is protected. The printers utilize the transport layer socket (TLS) 1.2 protocol for encryption, which is a robust standard that helps safeguard information from unauthorized access during transmission.

2.2.6 Firmware updates

Keep the printer firmware up to date to patch security vulnerabilities and improve overall device security. Authentic HID FARGO printer firmware files are encrypted and signed by HID, and only authentic files are accepted by the printer.

2.2.7 Physical security

To prevent unauthorized access, the printer and printing supplies should be physically secured in a locked room or cabinet. To deter theft or tampering, security cables or locks can also be used.

2.2.8 Software updates and scheduling

Keep the TRISM system up to date to patch security vulnerabilities and improve overall system security. All software update files are signed by HID and available for download.

2.2.9 Review preset permissions

Review all preset permissions assigned by user templates to ensure they follow the principle of least privilege. This minimizes access rights for users to the bare minimum necessary to perform their job functions.

2.2.10 Password expiration

If not utilizing Active Directory for user authentication, ensure that the password expiration settings are configured according to security best practices. Regularly update and enforce strong password policies to enhance security.

2.2.11 Hardening TRISM service server, printers, and XT HSM

Implement industry-standard hardening practices for the TRISM server, including disabling unnecessary services, applying security patches, and configuring firewalls. Secure TRISM printers by following recommended security protocols, such as enabling encryption, setting strong passwords, and regularly updating firmware.

2.2.12 Daily device inventory best practices

Implement daily device inventory checks to ensure all devices are accounted for and functioning correctly. This includes verifying device configurations and ensuring compliance with security policies. Regularly review the device inventory processes to confirm that card plastic count inventory is accurate, preventing fraudulent card creation and usage.

2.2.13 Audit logs review

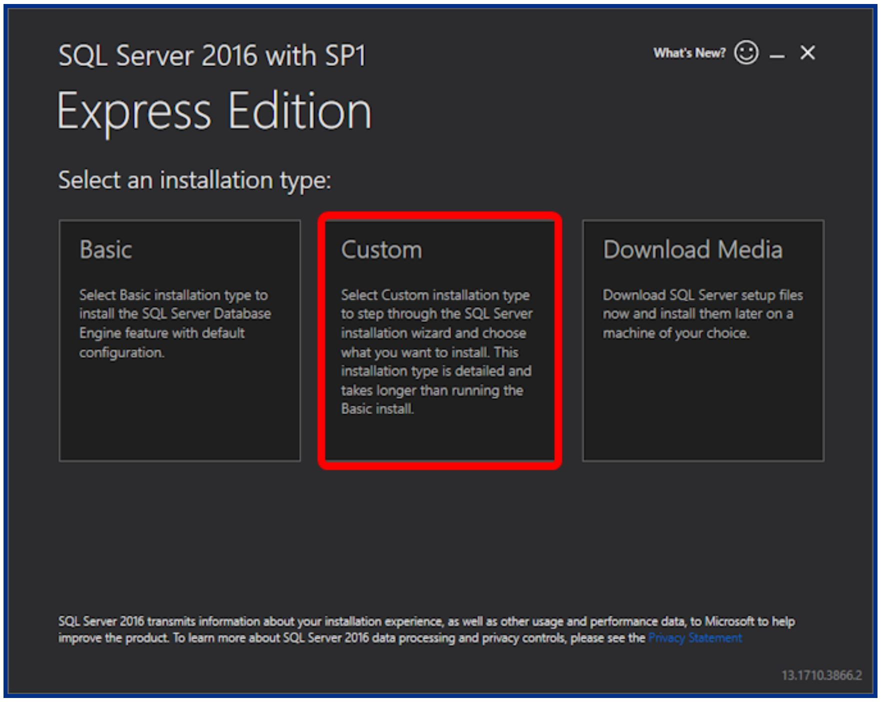
Regularly review audit logs for spoilage, card creation, and other critical activities. This helps detect and respond to any unauthorized or suspicious activities promptly.

2.2.14 Reviewing data log retention policy

Regularly review the data log retention policy to ensure it aligns with security and compliance requirements. The default data retention period is 30 days, but clients have the flexibility to adjust this period according to their needs. Ensure that the retention policy is consistently applied and that logs are securely deleted after the retention period.

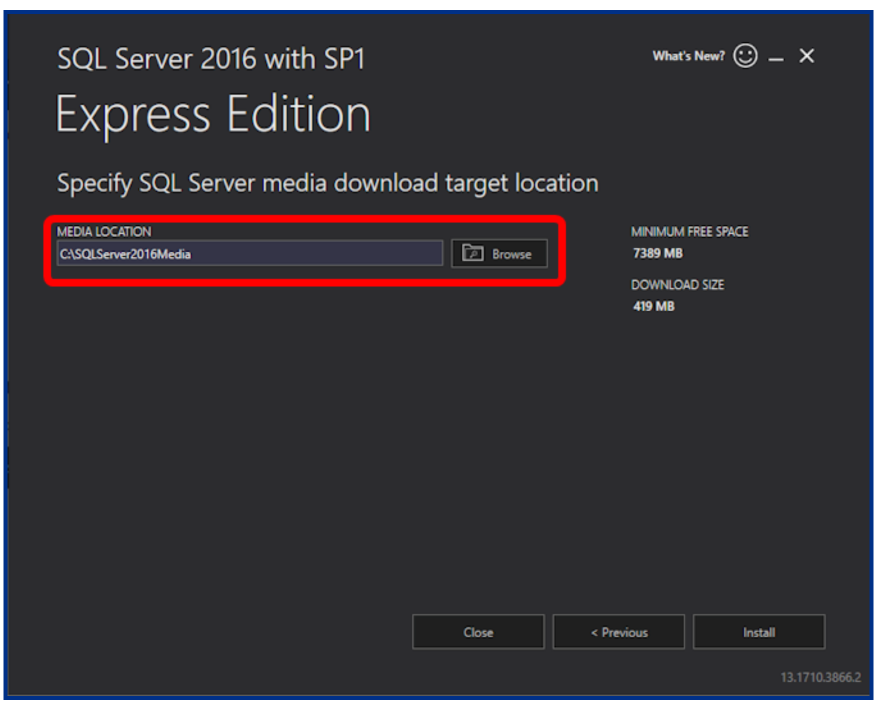
2.3 SQL server 2016 installation

1. Download the latest SQL server from the Microsoft downloads page. Select a Language, click **Download** then click **Save**.
2. Run the installer package.
3. Select the type of Install you would like. For this example, select **Custom**.

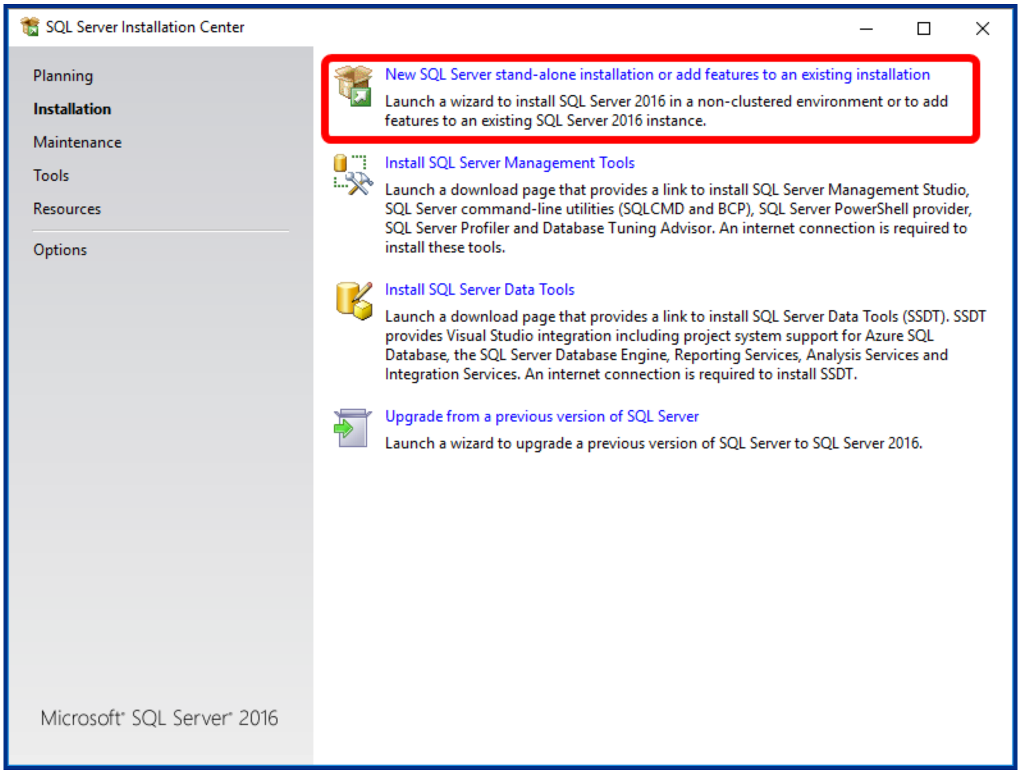


4. Choose the location for the files to be downloaded to start the install process.

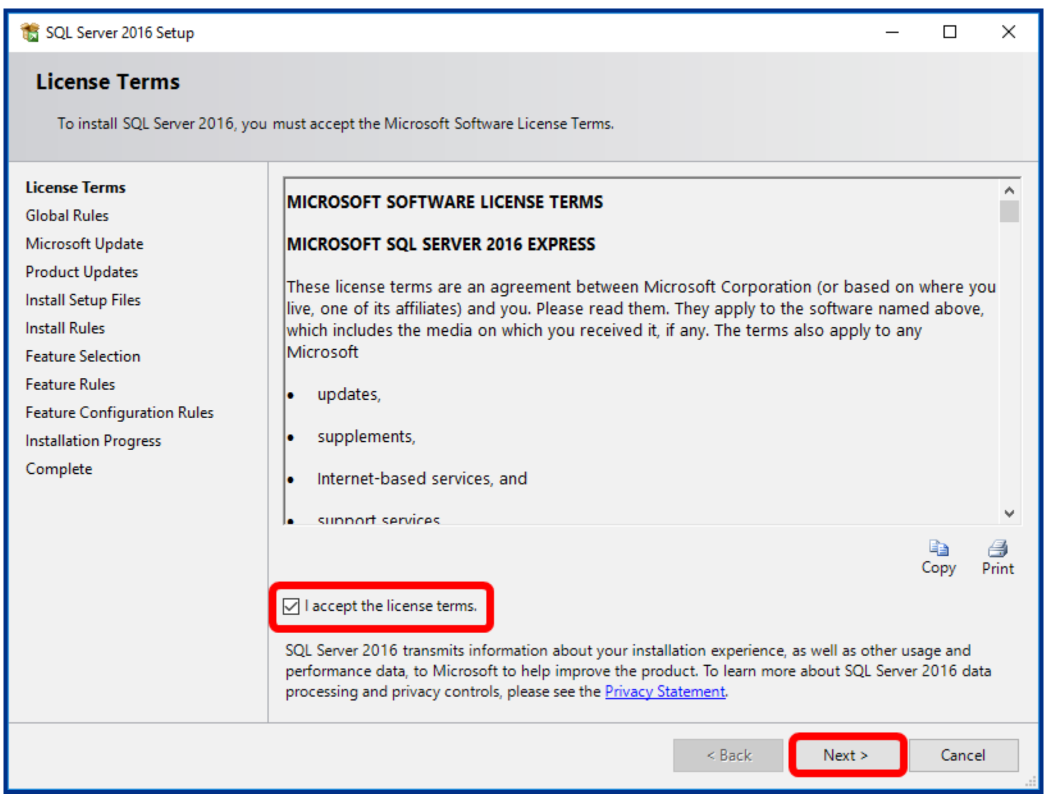
> **Note:** If you already have them downloaded this is not shown.



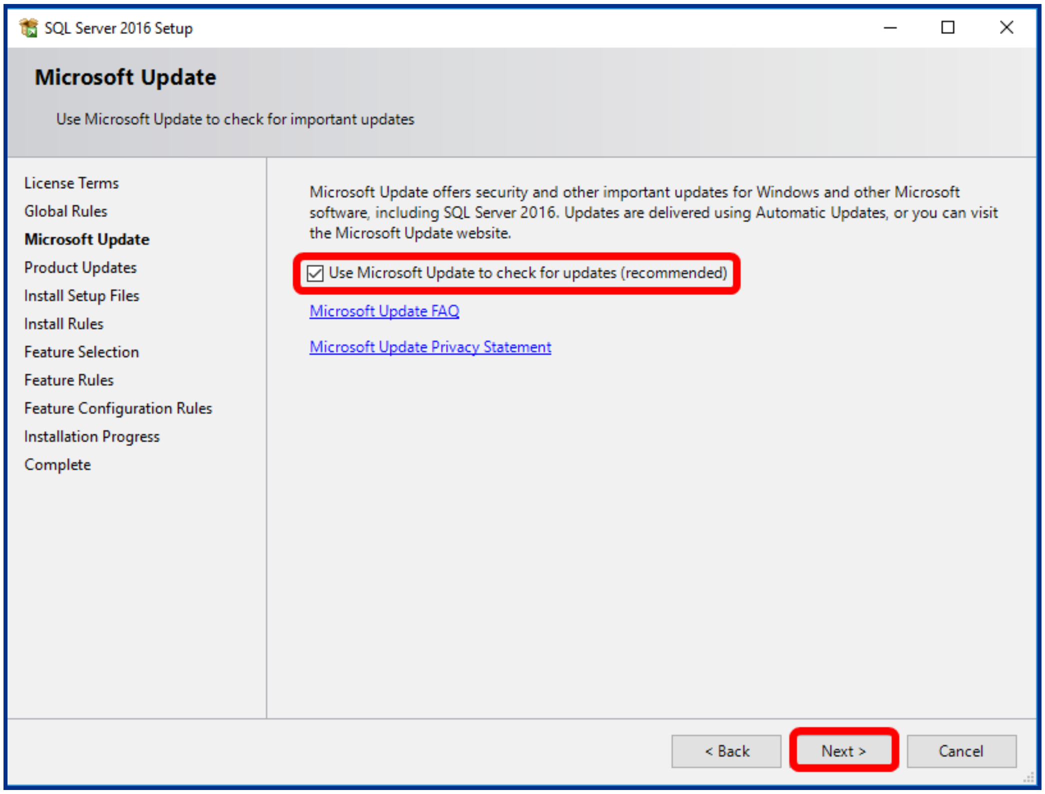
5. In the **SQL Installation Center** screen, select **New SQL Server stand-alone installation or add features to an existing installation**.



6. On the **License Terms** screen, check the **I accept the license terms** check box, then click **Next**.

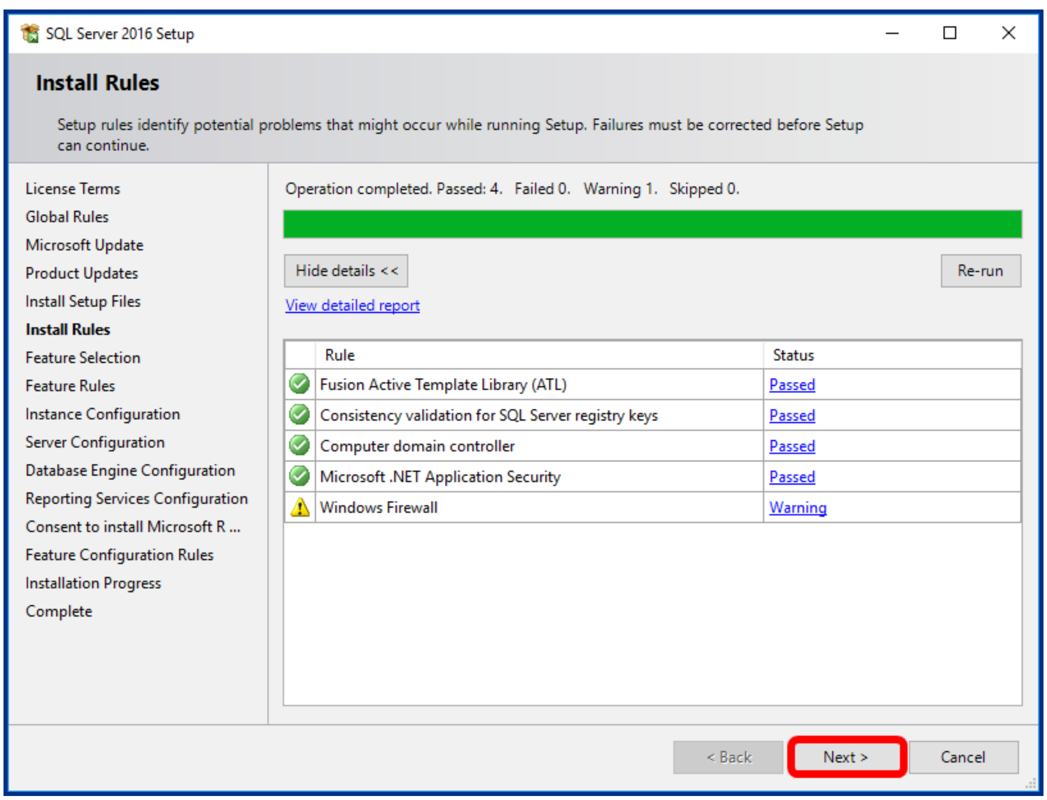


7. If prompted to install updates, select **Use Microsoft Update to check for updates** and click **Next**.

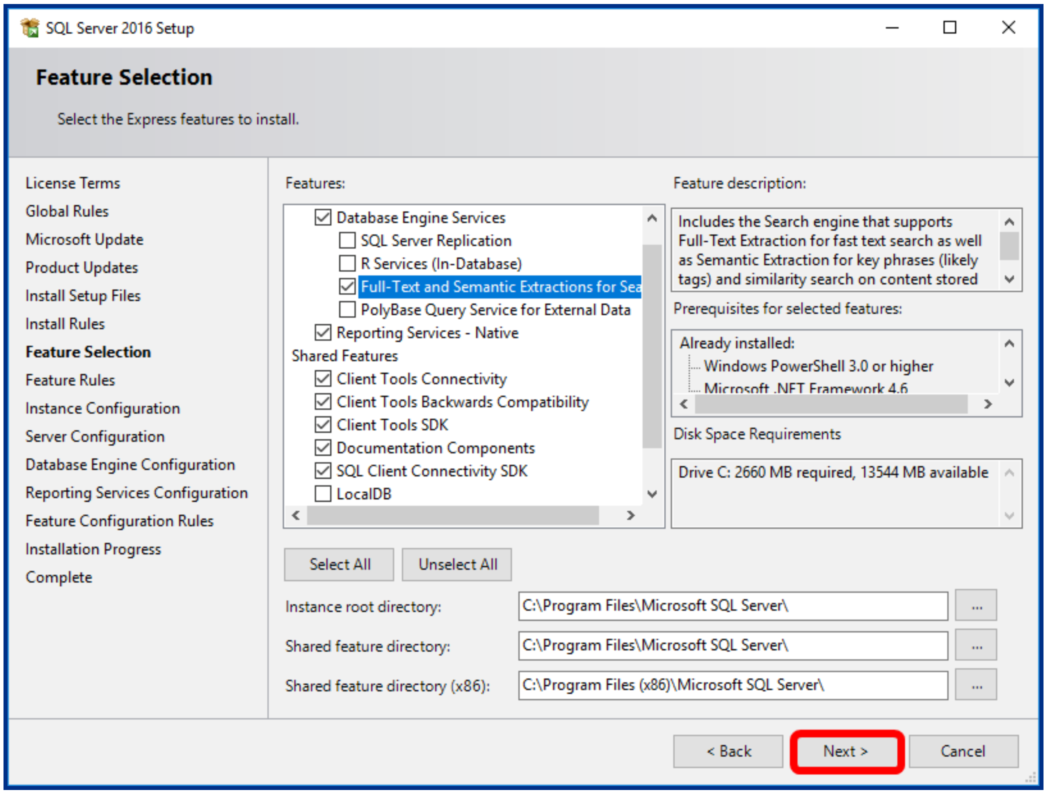


8. Verify the Rules and click **Next**.

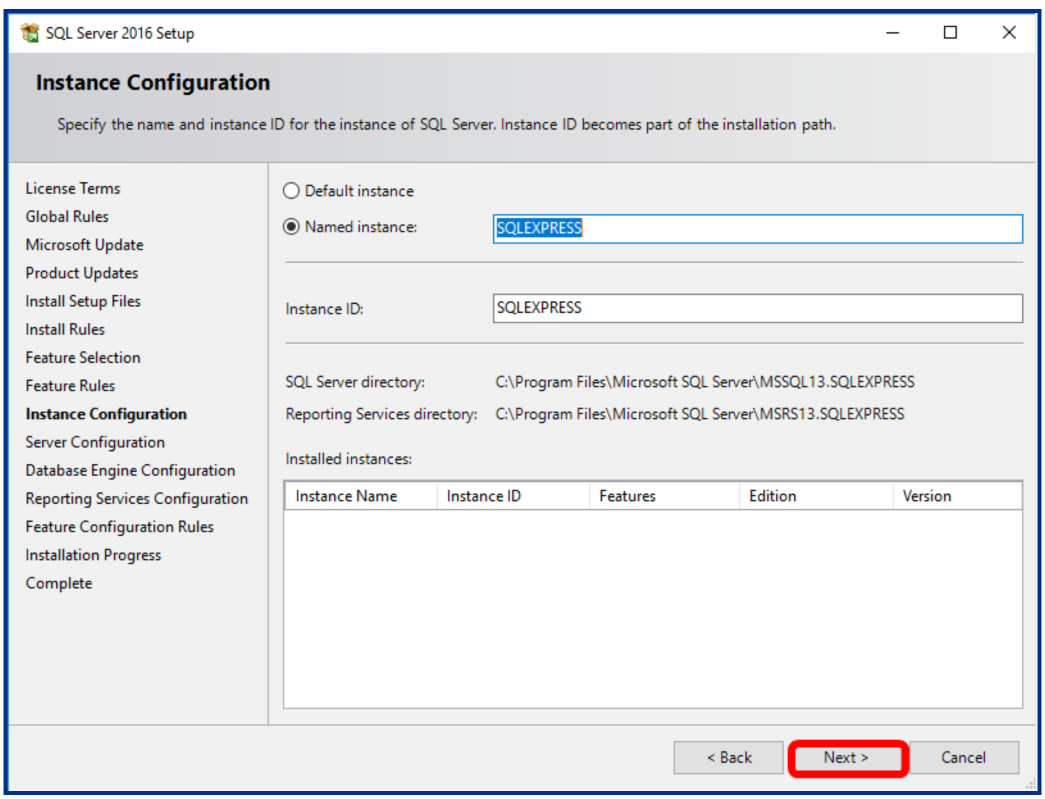
> **Note:** Windows Firewall may flag this, if so ignore until later.



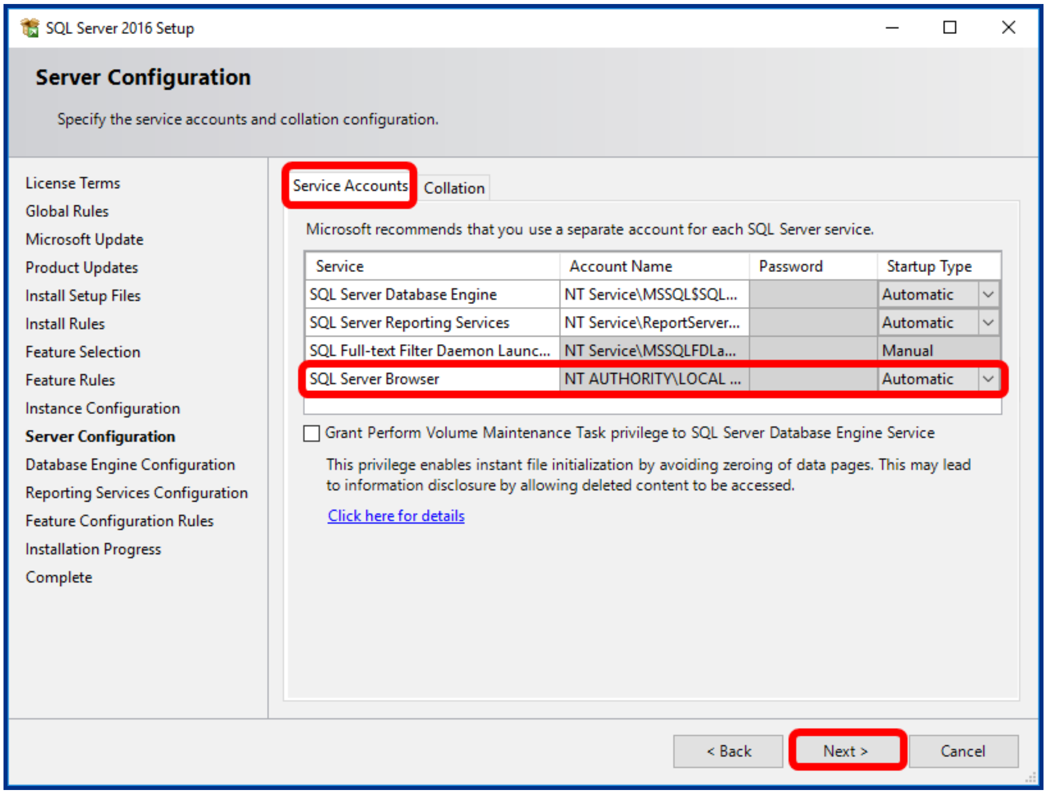
9. On the **Feature Selection** screen, leave all default values and click **Next**.



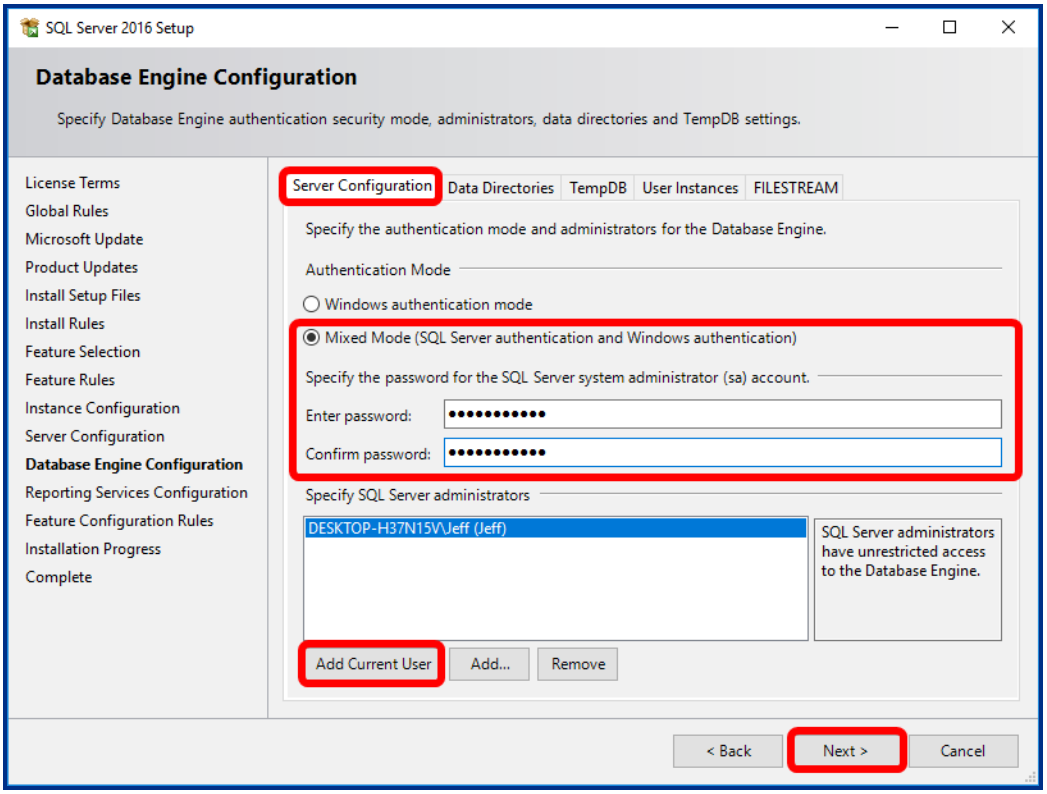
10. On the **Instance Configuration** screen, leave all default values and click **Next**.



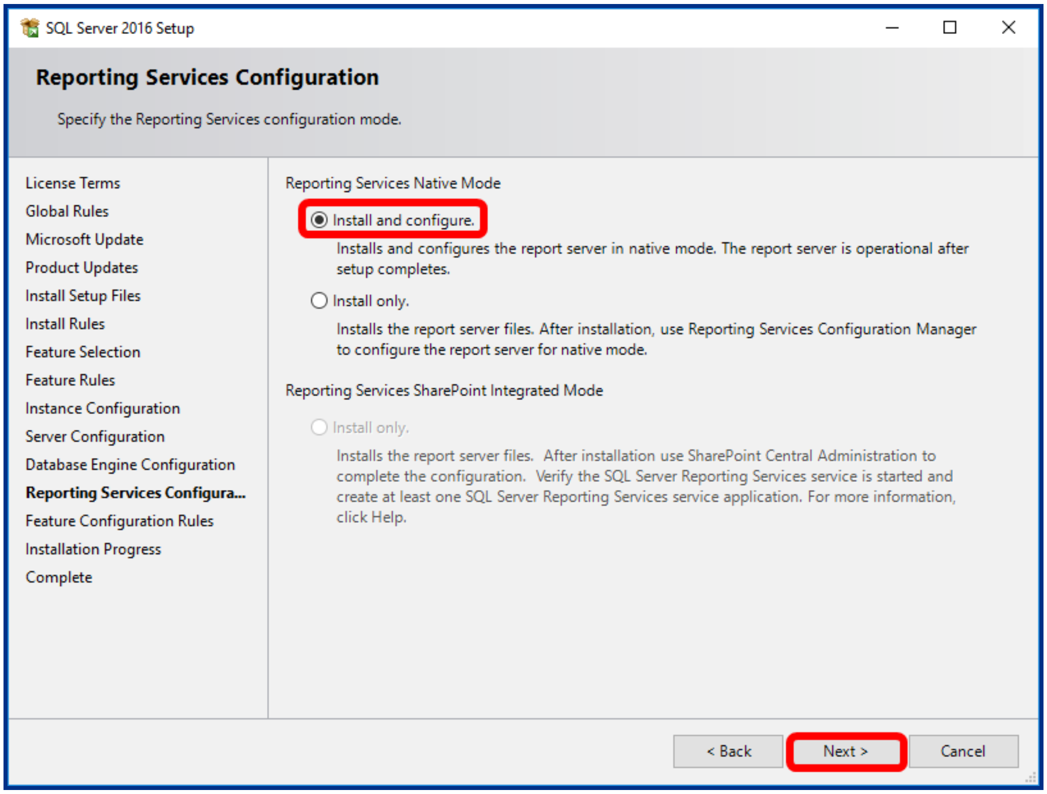
11. On the **Server Configuration** screen, select the **Service Accounts** tab. On the **SQL Server Browser**, **Startup Type** column, change the value from **Disabled** to **Automatic**. Click **Next**.



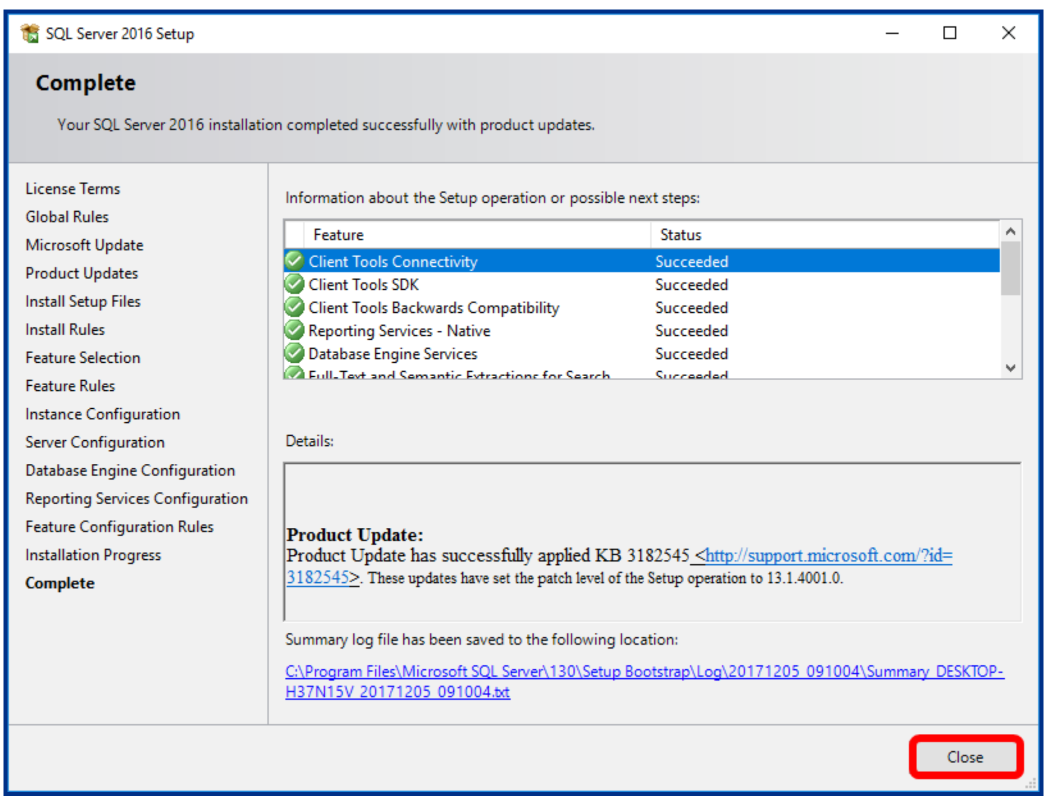
12. On the **Database Engine Configuration** screen, select the **Server Configuration** tab and select the **Mixed Mode** option. In the **Specify the password...** section, enter **DemoTeller1** in both fields. If the **Specify SQL Server administrators** box is empty, click **Add Current User**, then click **Next**.



13. When the **Reporting Services Configuration** screen is displayed, use the default **Install and configure** option. Click **Next**.



14. Wait for the installation to complete, then click **Close** to exit the SQL Server Setup window.



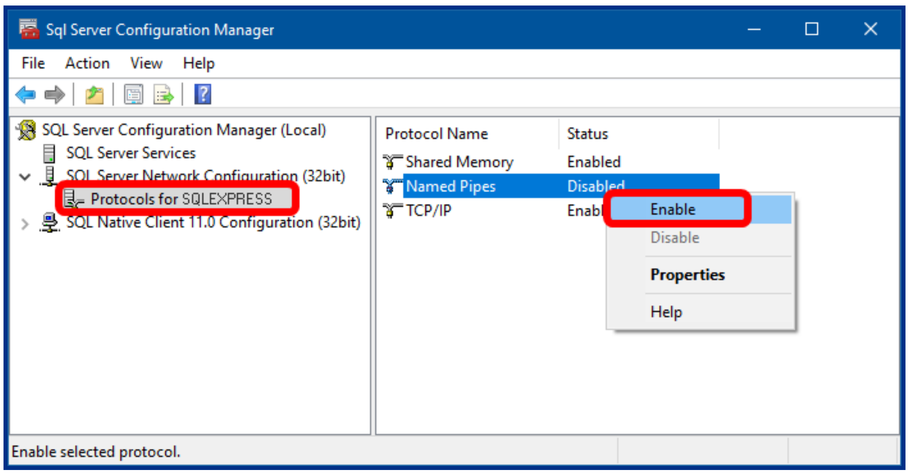
15. Close the SQL Server Installation Center window.

2.4 SQL server 2016 connection configuration

1. On Windows Server 2008 or prior, browse to **Start** > **All Programs** > **SQL Server 2016** > **Configuration Tools**, then select **SQL Server Configuration Manager**.
   OR
   On Windows Server 2012 or later, click **Windows (Start)**. Click the down arrow at the bottom of the **Start** menu, then scroll to the right and click **SQL Server Configuration Manager** to run it.

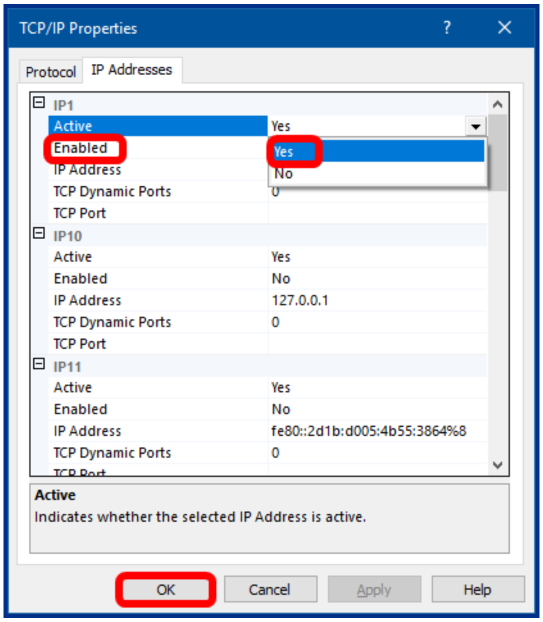
   

2. On the left-hand pane, expand **SQL Server Network Configuration**, then select **Protocols for SQLEXPRESS**.
   a. Right-click on **Named Pipes** and select **Enable**. If prompted, enter a Windows administrator password. Click **OK** on the resulting prompt.
   b. Repeat this for the **Shared Memory** and **TCP/IP** protocols, and the **VIA** protocol if listed.

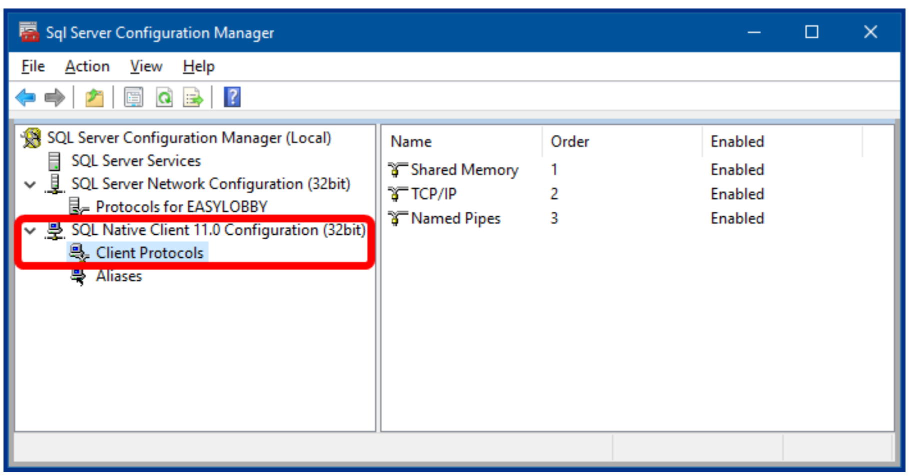
   

3. Right-click **TCP/IP** and select **Properties**.
4. In the **TCP/IP Properties** window, select the **IP Addresses** tab.

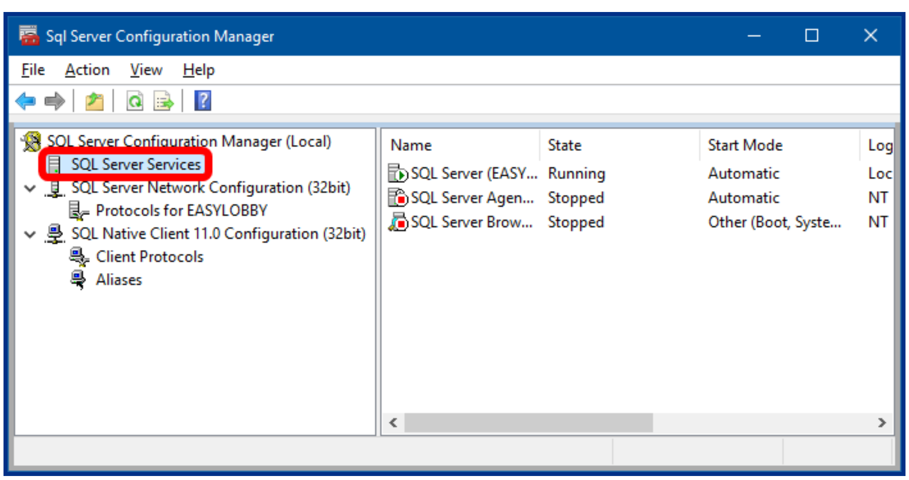
5. For every IP section (**IP1** to **IP6**), change the drop-down selection for the **Enabled** option to **Yes.** Scroll down and set the **IPALL TCP Port** to **1433**, then click **OK**.



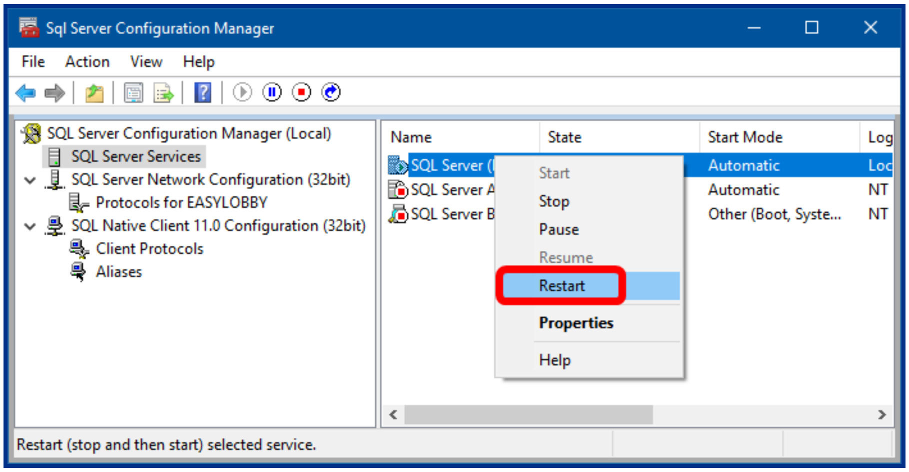
6. Repeat Step 2. for **SQL Native Client 11.0 Configuration (32bit)** and **SQL Native Client 11.0 Configuration.**



7. Select **SQL Server Services** in the left pane.



8. On the right pane, right-click **SQL Server (SQLEXPRESS)**, and select **Restart**.

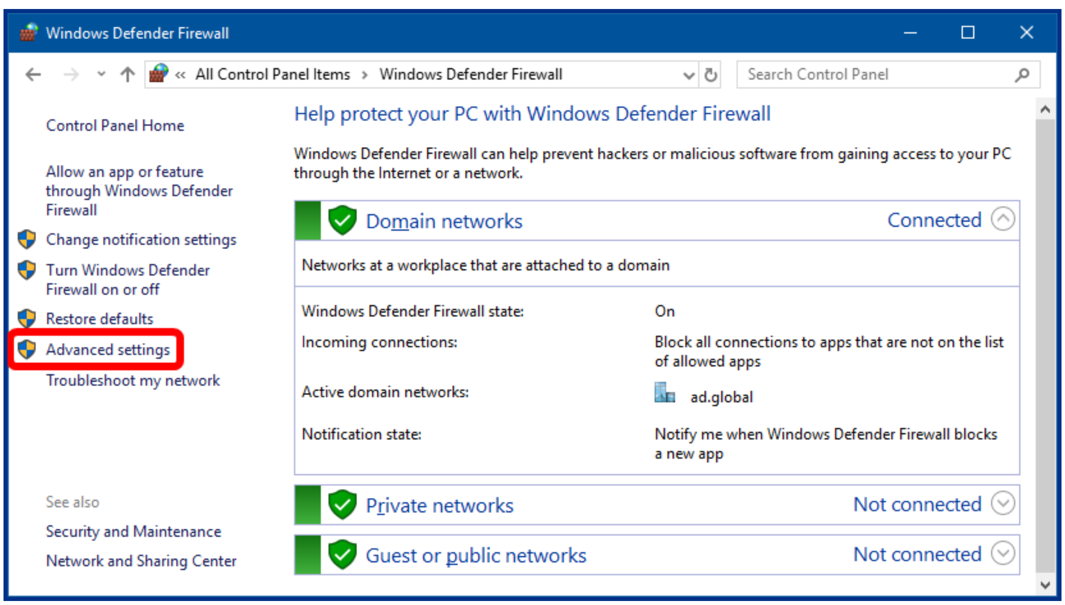


9. Once the service restart prompt disappears, close **SQL Server Configuration Manager**. Microsoft SQL Server 2016 is configured to accept connections.

2.4.1 Remote SQL connections configuration (action by the financial institution)

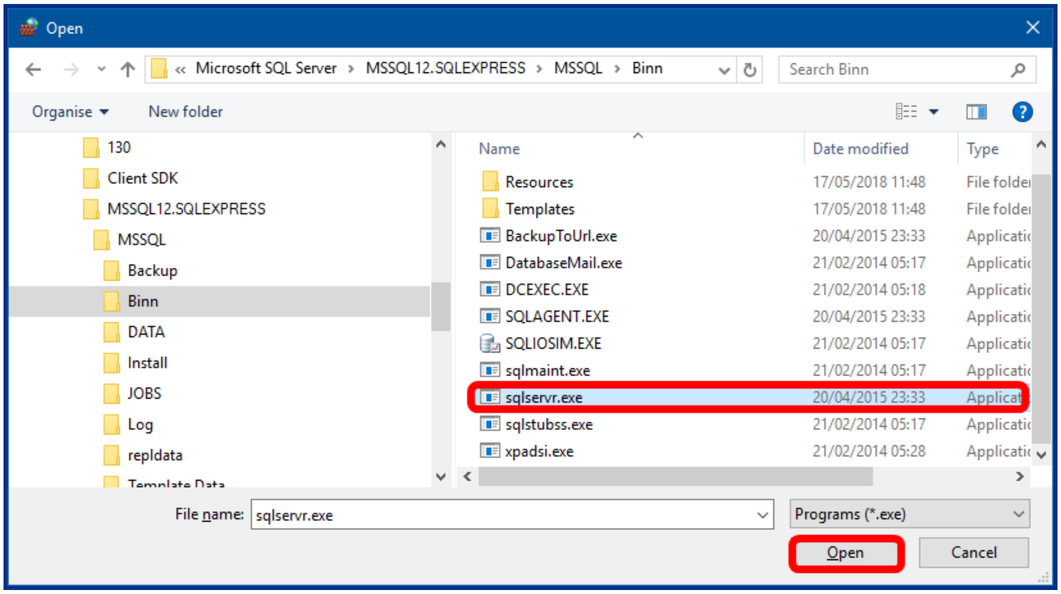
The Financial Institution must configure their firewall settings to allow remote connections to be able to contact the SQL database.

1. Ask the Financial Institution to go to the Windows Firewall settings and click **Advanced settings**.

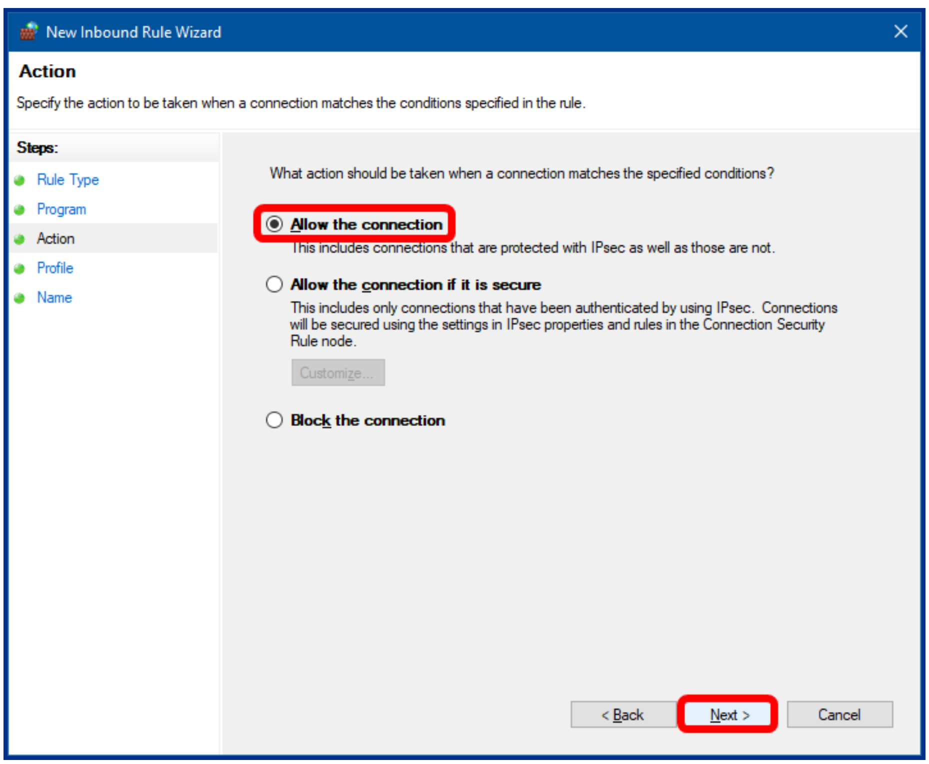


2. Click **Inbound rules** and in the **Actions** panel select **New Rule**.
3. Select **Program** and click **Next**.

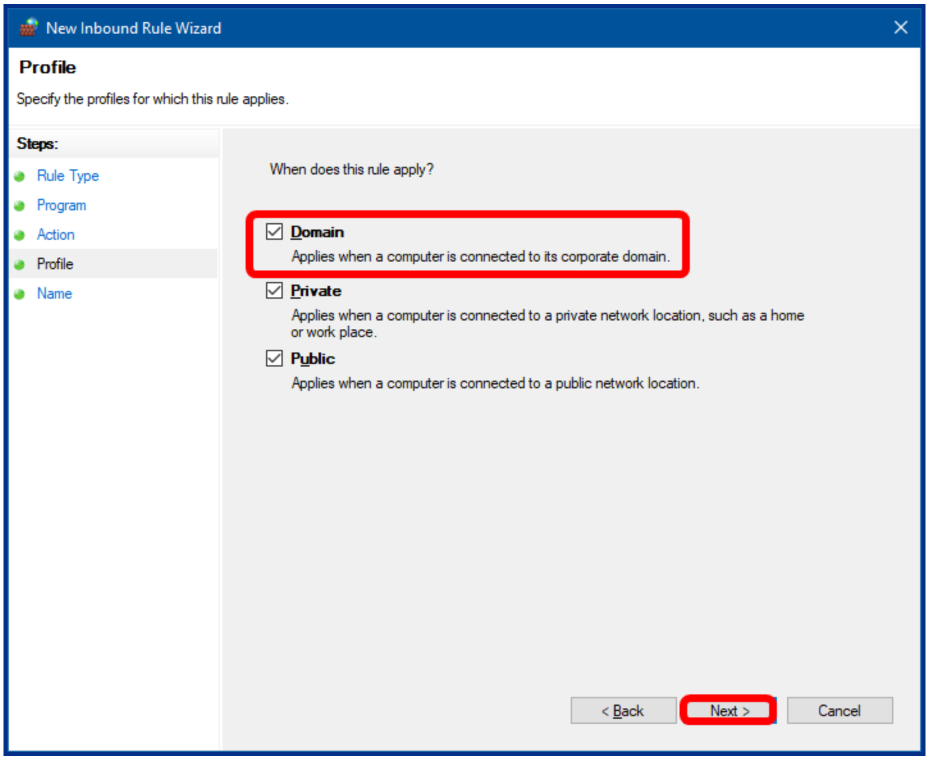
4. Browse to the Sql directory and go into the instance named folder. Go into **MSSQL**, then **Binn** and select **sqlserve.exe** (some versions are called **sqlservr.exe**). Click **Open**.



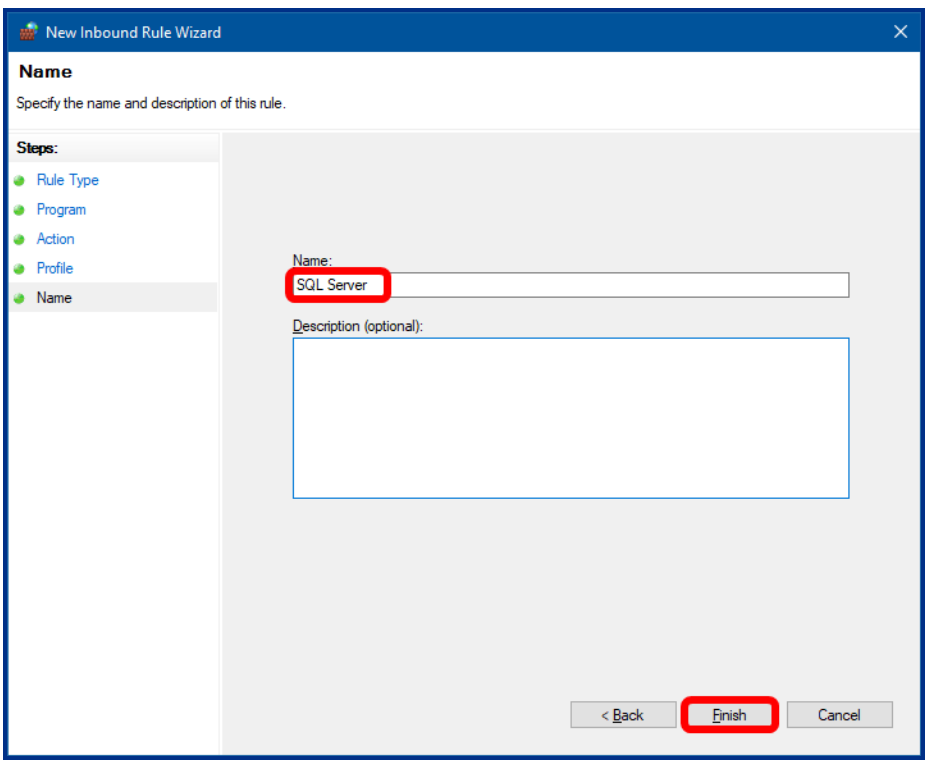
5. Select **Allow the Connection** and click **Next**.



6. Select the option for **When does the rule apply** (usually **Domain**). Click **Next.**



7. Name the rule as **SQL Server** and click **Finish.**



8. Create another rule:
    a. Select **Port** and click **Next.**
    b. Select **TCP**, select **Specific remote ports** and enter **1433**, click **Next.**
    c. Select **Allow the Connection**, click **Next.**
    d. Select the option for **When does the rule apply**, usually **Domain.**
    e. Enter a **Name** for the rule and an optional **Description**, click **Finish.**
9. Create another rule:
    a. Select **Port** and click **Next.**
    b. Select **UPD**, select **Specific remote ports** and enter **1434**, click **Next.**
    c. Select **Allow the Connection**, click **Next.**
    d. Select the option for **When does the rule apply**, usually **Domain.**
    e. Enter a **Name** for the rule and an optional **Description**, click **Finish.**
10. Create another rule:
    a. Select **Program** and click **Next.**
    b. Select Browse and select the directory for sql browser, usually:
    C:\Program Files (x86)\Microsoft SQL Server\90\Shared.
    c. Select **sqlbrowser.exe**, click **OK**, click **Next.**
    d. Select **Allow the Connection**, click **Next.**
    e. Select the option for **When does the rule apply**, usually **Domain.**
    f. Enter a **Name** for the rule and an optional **Description**, click **Finish.**

2.5 HSM Manager

> **Note:** For HSM XT see **2.5.3 TRISM XT key management system**.

2.5.1 Install HSM Manager

1. Download and run the latest HSM Manager Install package from the FTP site.
2. When prompted, click **Next**, leave all options at their default values.
3. Click **Install**, then **Finish**.
   HSM Manager is installed.

2.5.2 Run HSM Manager

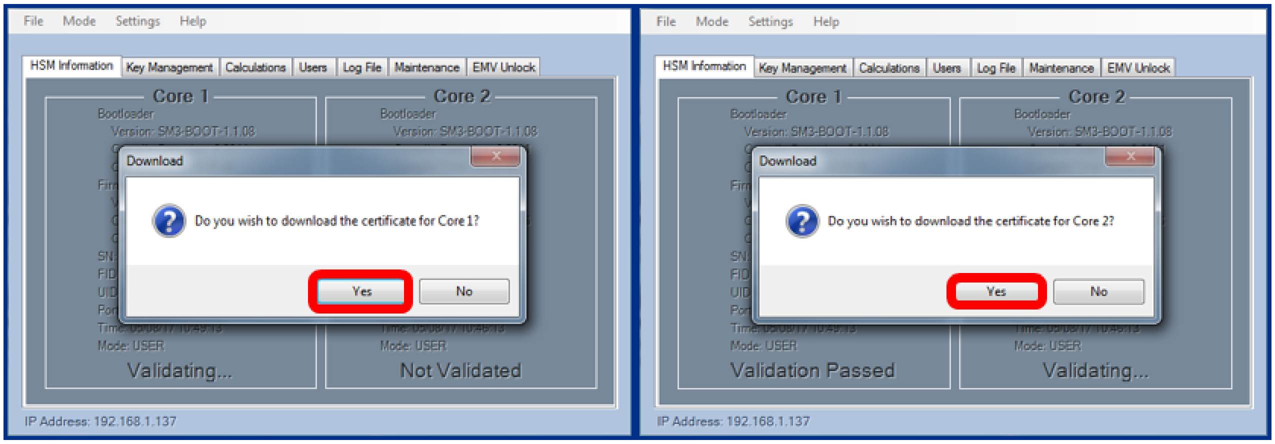
1. Run HSM Manager.
2. Enter the **HSM IP address** of the HSM and click **Save**.

   > **Note:** The ports should default to the correct settings.

3. Enter the Financial Institution (FI) **Site ID**, then click **OK**.

   > **Note:** The **Site ID** should match the FI DSI customer number (DAC), with zeros added to the left side until it is 8 digits long. For example, Customer number "817284" becomes Site ID "00817284".

4. If NOT using the same machine that was used to configure the HSM initially, a download prompt is displayed. Click **Yes**, then click **Yes** again when the prompt is displayed for the second core.

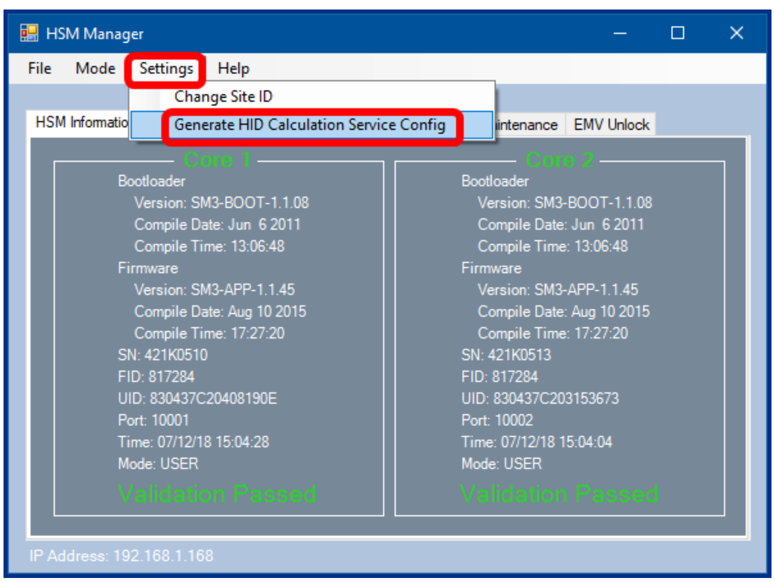


The following assumptions are:

- The target HSM has been set up and configured.
- The HSM network configuration has been completed and the HSM is reachable.
- Two or more operators/passwords have been configured in the HSM.
- The Master File Key (MFK) has been loaded.
- A PIN-Pad Derivation Key has been loaded.

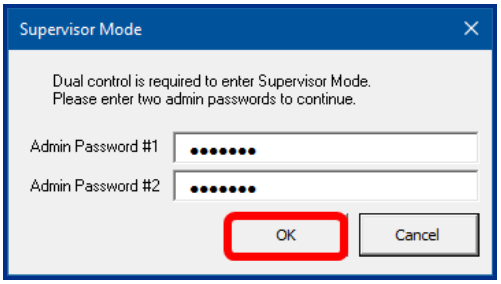
> **Note:** For instructions refer to the *TRISM Duo HSM Administrator Manual* or *HSM XT Administrator Manual*

5. Click **Settings** and then click **Generate HID Calculation Service Config**.

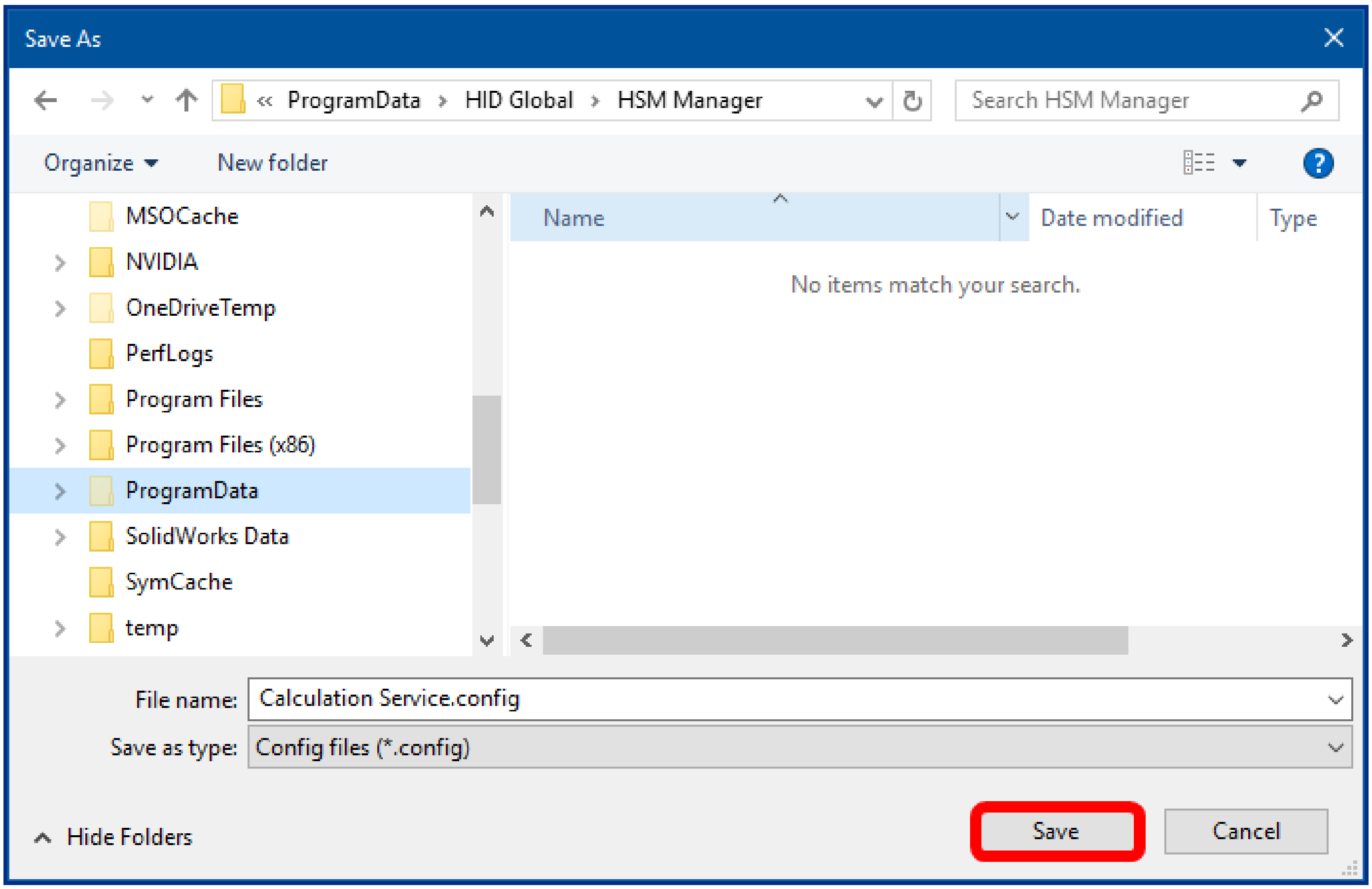


6. Set the locations for PIN Pad Derivation Key and the Database Encryption Key and click **Go**.

7. Enter a different operator password in each field and click **OK**.

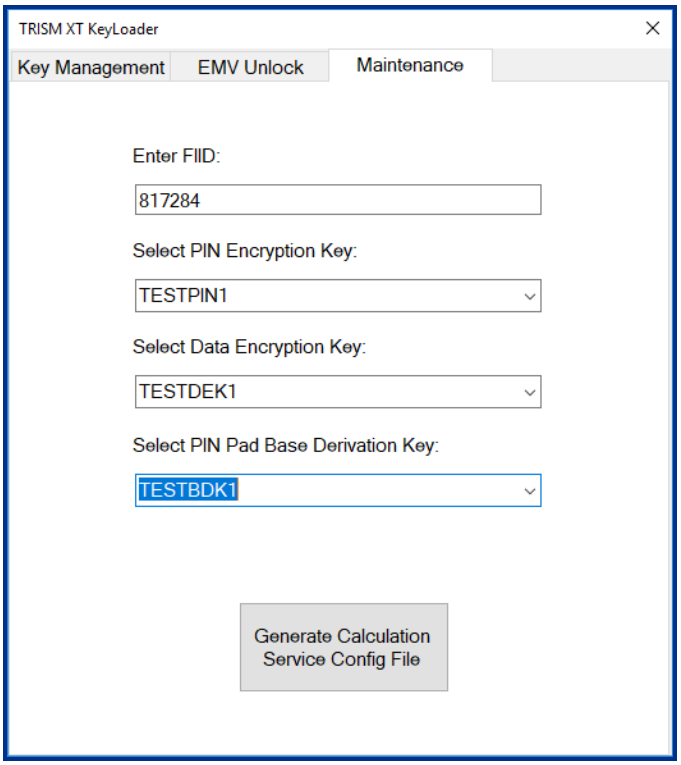


8. Save to the **C:\ProgramData\HID Global\TRISM\Calculation Service** folder. Click **Save**.



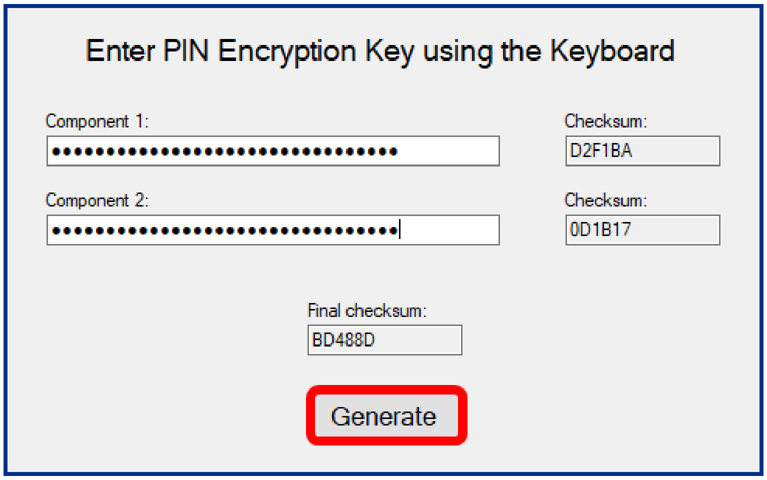
2.5.3 TRISM XT key management system

1. Copy the Calculation Service.config file created during the XT Key install (see XT Admin Guide) to **C:\ProgramData\HID Global\TRISM\HSM Manager on the TRISM Server.**
2. Launch the TRISM XT Key Management System.
3. Click **Maintenance**.
4. Enter the **Financial ID**.
5. Use the drop-down menus to select the correct key names for the required keys.
6. Once the correct information is selected click **Generate Calculation Service Configuration File**.
    a. PIN Encryption Key: Used to securely transmit PINs between the HSM and the TRISM application.
    b. Data Encryption Key: Used to derive the Database Encryption Key.
    c. PIN Pad Base Derivation Key: Used to derive the unique PIN Encryption Key used in each PIN Pad.

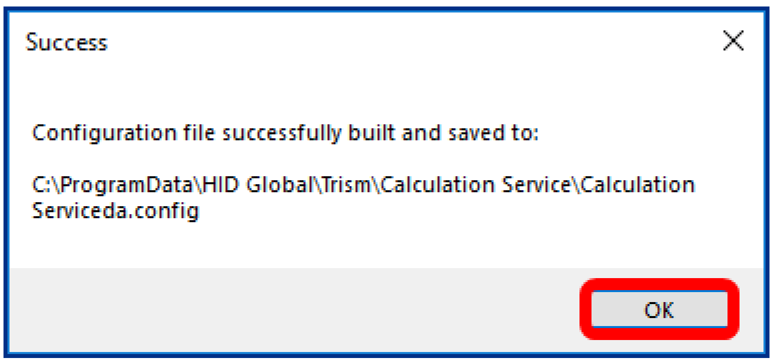


7. Locate the two PIN Encryption mailers supplied by HID Global.
8. Enter the component from each mailer into form and verify the checksums match.

9. Once both components are entered, verify the final checksum matches the final checksum in the mailer.



10. Click **Generate**.
11. Select the location and name to save the new **Calculation Service configuration file**. A message box is displayed to inform the user that the file has been successfully saved.



> **Note:** The default name and location are presented automatically. These should not be changed as this is where the HID Calculation Service searches for the configuration file.

12. Click **OK**.

For information on importing issuer certificates used for dual interface EMV chips, see Section 7.1 Generating the Issuer Key and Request File in the *TRISM HSM XT Administrators Manual* (PLT-04227).

2.6 HSM XT installation - Mastercard CVC3 fix

Using the current HSM XT firmware (4.30.3.7.mpkg), Calculation Service (6.2.1), and CLEEMV.dll (6.3), the CVC3 for the Mastercard MSD contactless path is being calculated incorrectly, even when the correct CVC3 key and MSD track layout are used.

The MSD (Mag Stripe Data) path is used on older point of sale (POS) terminals. The newer qVSCD contactless path is used by most modern terminals and does not use the MSD track or MSD CVC3 value on the chip.

> **Important: Initial key entry must be done using the currently released HSM firmware 4.30.3.7.mpkg.**

> **Note:**
> For MBK loads, the new XT firmware required for this automatically generates an MBK. When loading an MBK, KMS does not prompt to create or load one. Instead, the command to "Read MBK Cards" must be initiated using a command prompt. This is built into the instructions in section 2.6.3 Mastercard CVC3 fix procedure. The command is:
> ```
> csadm dev=<HSM XT IP> cmd-0x69,2
> ```
> Reboot CryptoServer when instructed. If the CryptoServer is not rebooted at the point the instructions in section 2.6.3 Mastercard CVC3 fix procedure state to reboot, then errors occur when trying to perform any calculations or chip unlock. The error is reported as: **B07C0013 - No MBK Loaded**. Rebooting the CryptoServer through the **Manage** menu in cat.jar, resolves the issue. This is the same error that occurs when updating the firmware if **Update** is used instead of **New Installation**.

The following materials are required from HID Global:

- HSM XT FW: PaymentSserver-Hybrid-Se2-Series-4.30.3.7.mpkg
  The initial key entry must be done using this package.
- HSM XT FW: PaymentSserver-Hybrid-Se2-Series-4.33.3.0.mpkg
- HID Key Management System v6.2.4 or later
- HID Calculation Service 6.2.2.0
- HID Card Printer Service v6.3.22 or higher (contains CLEEMV.dll v6.2 or higher)
- **XT Setup** and **User Add** call has been completed.

The following materials are required from the financial institution:

- Physical access to the HSM XT with the key pad
- 2 MBK smart cards
- All keys
- HSMAdmin1 and HSMAdmin2 key files and passwords
- XTUser1 and XTUser2 passwords
- KeyHolder passwords

2.6.1 Mastercard CVC3 fix overview

Note: These steps are provided for reference only. See section **2.6.3 Mastercard CVC3 fix procedure** for the complete list of instructions.

1. Load all keys using current released HSM firmware 4.30.3.7.mpkg.
2. Re-enter any CVC3 keys as **Type IMK-DAC**.

   Most keys use an existing key as the CVC3 key (either the MDK-AC or a CVV). To re-enter the same key as a different type, the XT must first be put into NON mode.

   a. Create backups (omit EFTPOSCONFI.db)
   b. Put XT into PCI NON mode.
   c. Reload MBK.
   d. Enter keys.
   e. Create backups.
3. Create new backups (omit EFTPOSCONFI.db).
4. Update firmware using **New Installation**.

   New Installation wipes all keys, MBK keys, and non ADMIN users. Only HSADMIN1 and HSADMIN2 users remain.
5. In the CryptoServer Administration Tool, select **Manage** > **Reboot CryptoServer**.
6. Force XT to read and load current MBK smart cards.

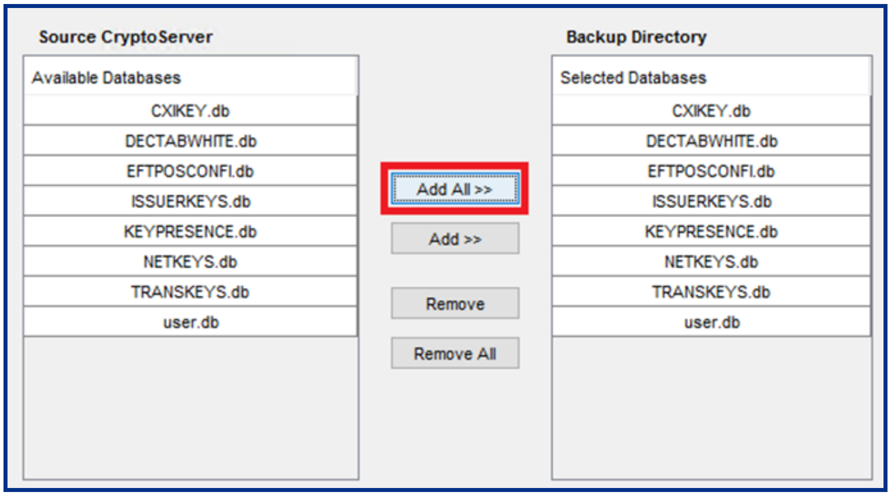
   New firmware auto generates MBK and you need to force the XT to load the MBK stored on the two smart cards.
7. Restore backups omitting the EFTPOSCONFI.db.
8. Set XT to V2 mode. This is like setting to NON mode, keys are wiped. MBK should remain.
9. Restore backups omitting the EFTPOSCONFI.db.
10. In the CryptoServer Administration Tool, select **Manage** > **Reboot CryptoServer**.
11. Complete key installation tasks.
12. Create final backups including the EFTPOSCONFI.db.
13. Update HID Calculation Service.
14. Update CLEEMV.dll in HID Card Printer Service.

2.6.2 Omitting EFTPOSCONFI.db during backup and restore

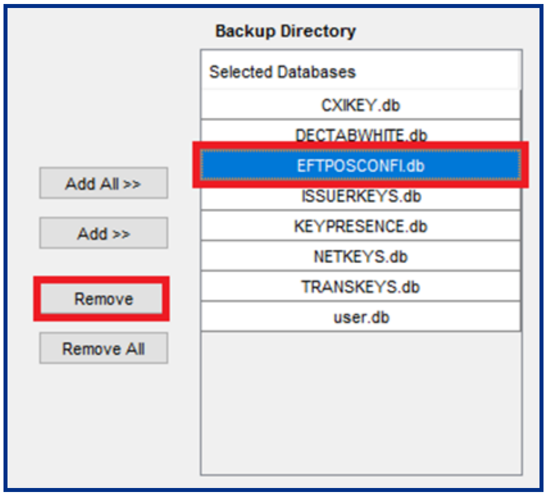
EFT POS CONFIG contains the NON, V2, V3 mode of the HSM XT. If a backup is made in V3 mode, then when it is restored, it puts the HSM back into V3 mode. If the XT is already in V2 mode, EFTPOSCONFI.db can be backed up for future restoration.

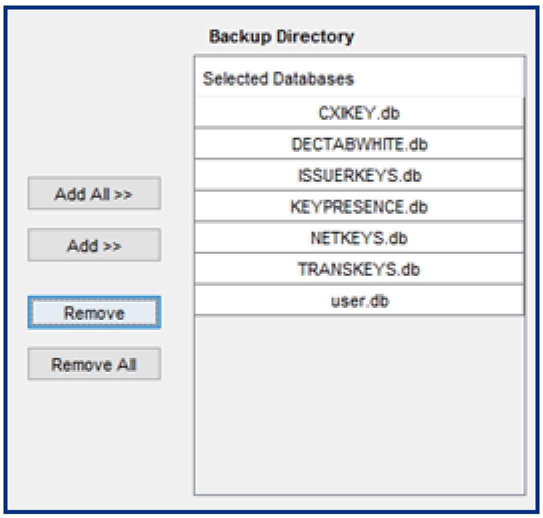
When creating a backup and restoring prior to setting to V2 mode:

1. Click **Add All**.



2. From the **Backup Directory** list, click **EFTPOSCONGI.db** to highlight and click **Remove**.





When making final backups after the firmware update and the XT is in V2 mode, back up all databases including EFTPOSCONFI.db.If keys need to be restored to the XT in the future or to a DR XT, the restore puts the XT in the proper V2 mode.

2.6.3 Mastercard CVC3 fix procedure

Key Entry

1. Update HID Key Management System to latest version.
   Download and update CLEEMV.dll to 6.1.32 minimum in C:\Program Files (x86)\HID Global\TRISM\Key Management System.

   > **Note:** If using the installed CLEEMV.dll, Chip Unlock fails.

2. Enter all keys as normal, following the usual guides except the CVC3 key(s).

   > **Note:** This must be done using the current released HSM firmware 4.30.3.7.mpkg.

   CVC3 key entry on this firmware (see **Re-entering CVC3 keys as type IMK-DAC in NON PCI mode**), is entered as IMK-DAC type, and not IMK-AC type.

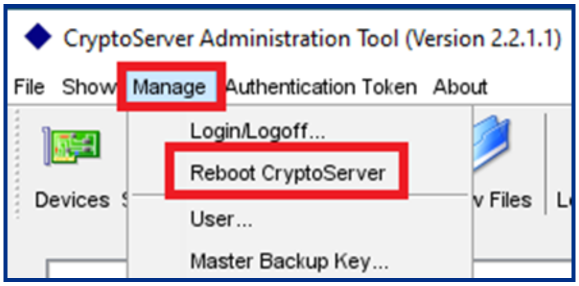
Re-entering CVC3 keys as type IMK-DAC in NON PCI mode

1. Launch cat.jar, and create back-ups omitting EFTPOSCONFI.db HSM XT.
2. On the PC or server where KMS is installed, launch a command prompt and type the following and press **Enter**:
```
CD C:\Program Files (x86)\HID Global\TRISM\Key Management System\
```
3. Set the XT into PCI NON mode. At the command prompt, type the following and press **Enter**:
```
csadm dev=<HSM XT IP> Logonpass=XTUser1,ask Logonpass=XTUser2,ask cmd=0x7c,0x5b,3,'"NON"'
```
   a. You are prompted to enter the password for XTUser1, then XTUser2. There is not a visual indication that typing occurred.
      If successful, you will see **ANSW:**
   b. Verify the mode. Type the following and press **Enter**:
```
csadm dev=<HSM XT IP> cmd=0x7c,0x49
```
      If **RN** is displayed, the XT is in NON PCI mode.
   c. Leave the command prompt open.

      Note: Setting the XT to PCI NON mode erases keys that have been entered, including the MBK.
4. Re-load the MBK.
   a. Launch KMS.
   b. At the prompt to create and load a MBK, click **No**. (You are reloading an existing MBK.)
   c. At the prompt to plug in the keypad and gather the MBK cards, click **Yes**.
   d. At the keypad prompts to import the MBK, enter the following:
      1. PINPad screen: Import new key. Press **OK/Cancel**.
      2. PINPad screen: Insert 1. card. Press **OK/Cancel**.
      3. PINPad screen: Enter PIN. (Should be **123456.**)
      4. PINPad screen: Insert 2. card. Press **OK/Cancel**.
      5. PINPad screen: Enter PIN. (Should be **123456**.)
   e. HSM XT restarts and KMS prompts to log in. Press **Cancel**.
   f. The keys have been wiped and need to be restored.
5. Log in to reconnect to the HSM XT in cat.jar and restore back-ups.
   If EFTPOSCONFI.db was backed up, remove it from the restore list.
6. Log in to the HSM XT using KMS and load the CVC3 keys as **Type: IMK-DAC**
   The naming convention is C3XXXX01.
   If keys are entered through a KEK, then re-enter the KEK as **DAC Type - Hex: 08**.
   KMS shows a blank type after KEK is loaded, but keys loaded using it show as type DAC.
7. Once key entry tasks are completed, log into cat.jar, and create new back-ups (omitting EFTPOSCONFI.db)

Updating firmware/setting to V2 mode/restoring backups

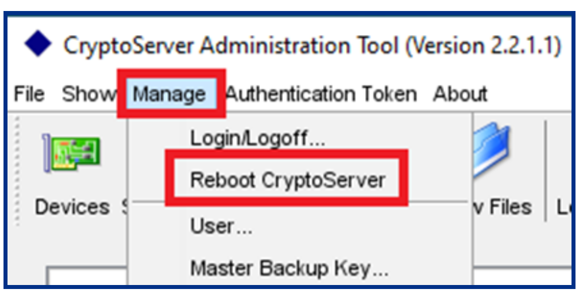
1. Update the firmware to PaymentServer-Hybrid-Se2-Series-4.33.3.0.mpkg - HSM XT - Installing/Updating Firmware.
    a. Use **New Installation**.
    HSMAdmin1 and HSMAdmin2 users remain, all other Users/Keys/MBK are deleted.
    b. Reboot the CryptoServer by selecting **Manage** > **Reboot CryptoServer**.



2. Force XT to read MBK from cards.
    a. Return to the command prompt. Type the following and press **Enter**:

```
csadm dev=<HSM XT IP> cmd=0x69,2
```

    The command prompt shows a blinking cursor.
    b. The keypad prompts to import the MBK, enter the following:
        1. PINPad screen: Import new key. Press **OK/Cancel**.
        2. PINPad screen: Insert 1. card. Press **OK/Cancel**.
        3. PINPad screen: Enter PIN. (Should be **123456**.)
        4. PINPad screen: Insert 2. card. Press **OK/Cancel**.
        5. PINPad screen: Enter PIN. (Should be **123456**.)
    c. When completed, the CMD prompt shows **ANSW:**
3. Restore backups omitting the EFTPOSCONFI.db - EFT POS Config file.
    a. EFT POS Config - stores the NON, V2, V3 mode - If backups were made in V3, then when restored, it puts the HSM back into V3.
    b. The HSM XT must remain in PCI V2 mode.
4. In the CryptoServer Administration Tool, reboot the CryptoServer by selecting **Manage** > **Reboot CryptoServer**.



5. Set the XT to PCI mode V2.
   a. Return to the command prompt. Type the following and press **Enter**:

   ```
   csadm dev=<HSM XT IP> Logonpass=XTUser1,ask Logonpass=XTUser2,ask
   cmd=0x7c,0x5b,2,'"V2"'
   ```

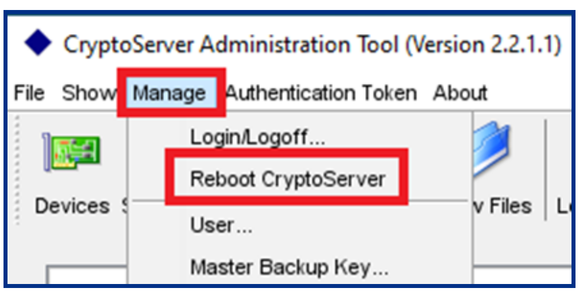
   b. When you press **Enter**, you are prompted to enter the password for XTUser1, then XTUser2. There is not a visual indication that typing occurs.
   c. Check the PCI mode. Type the following and then press **Enter**:

   ```
   csadm dev=<HSM XT IP> cmd=0x7c,0x49
   ```

   A response of R2 indicates the XT is in PCI mode V2.
6. Reload the MBK.
   a. Return to the command prompt. Type the following and press **Enter**:

   ```
   csadm dev=<HSM XT IP> cmd=0x69,2
   ```

   The command prompt shows a blinking cursor.
   b. The keypad prompts to import the MBK, enter the following:
      1. PINPad screen: Import new key. Press **OK/Cancel**.
      2. PINPad screen: Insert 1. card. Press **OK/Cancel**.
      3. PINPad screen: Enter PIN. (Should be **123456**.)
      4. PINPad screen: Insert 2. card. Press **OK/Cancel**.
      5. PINPad screen: Enter PIN. (Should be **123456**.)
   c. When completed, the CMD prompt shows **ANSW:**
7. Restore backups again omitting the EFTPOSCONFI.db.
   a. Setting to V2 Mode will wipe keys, so backups need to be restored again.
   b. MBK should remain loaded and untouched.
8. In the CryptoServer Administration Tool, reboot CryptoServer by selecting **Manage** > **Reboot CryptoServer**.



9. Launch KMS and log in to verify all keys are present. Complete any remaining key installation tasks.
10. Log into cat.jar and create final backups including the EFTPOSCONFI.db.

2.7 TRISM client initial installation

1. Download the appropriate latest TRISM client Web Installer package and run when prompted.
2. On the **Install Requirements** screen, click **Install**.
3. On the **SAP Crystal Reports** installer, click **Next** and accept the license agreement when prompted.
4. On the **TRISM 7** installer, click **Next** and accept the license agreement when prompted. Leave all fields at their default values.

TRISM 7 is installed.

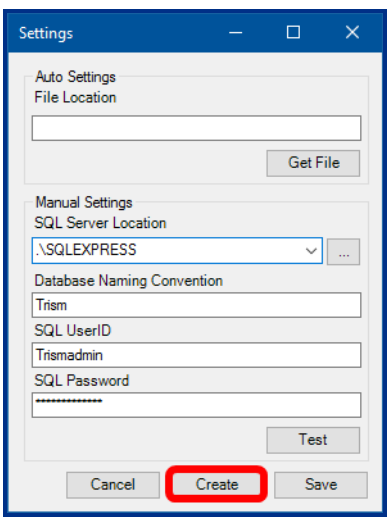
2.8 TRISM client database creation

This section assumes:

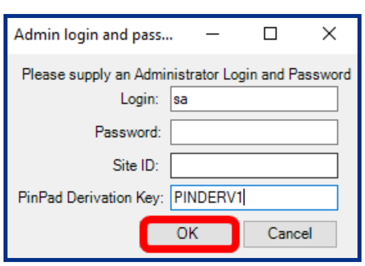
- SQL Server 2016+ and SQL Server Management Studio have been installed and have been configured via SQL Server Configuration Manager.
- TRISM Client has been installed and updated to the appropriate version.

1. Run the TRISM Client.
2. With the TRISM Client log in window displayed, press **Alt** on the keyboard to display the **Settings** button on the bottom right corner of the window. Click **Settings**.

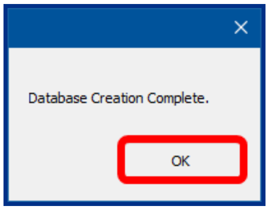
3. In the **Settings** window, verify that the **SQL Server Location** field is correct, then click **Create**.



4. Enter **sa** as the **Login**. Enter the password used on the SQL install, the 8 digit Site ID, and the location of the PINpad Derivation Key then click **OK**.

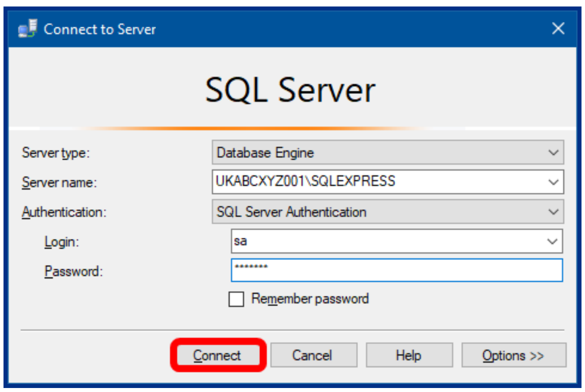


5. Once database creation is completed, a **Database Creation Complete** prompt is displayed. Click **OK**, then click **Cancel** on the TRISM Client log-in form to close TRISM Client.

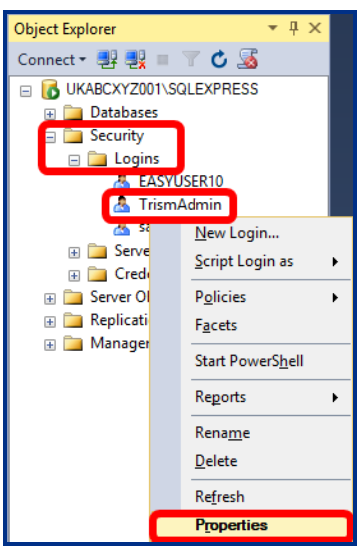


The TRISM databases and "trismadmin" user have been created. The software is installed.

6. Run the SQL Server Management Studio software. The **Connect to Server** form is displayed.
   - Verify that the selected SQL server/instance in the **Server name** drop-down menu is correct.
   - In the **Authentication** drop-down menu, verify **SQL Server Authentication** is selected.
   - Enter **sa** as the login and password used on SQL install, then click **Connect**.

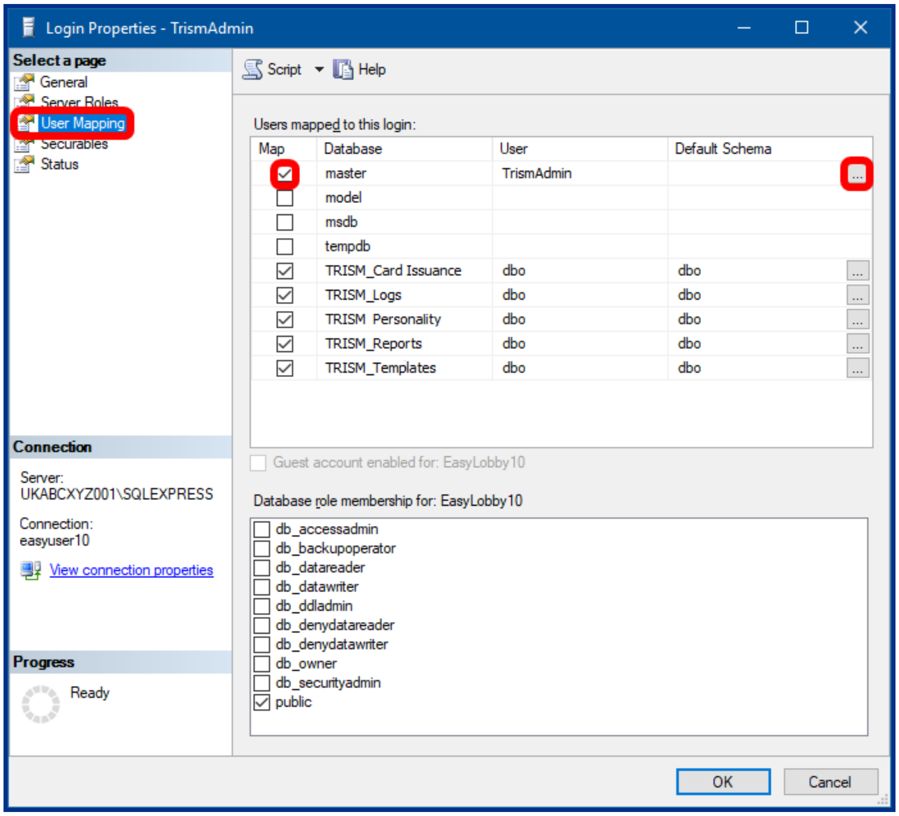


7. On the **Object Explorer** panel, on the left side of the **Connect to Server** window, expand the **Security** folder, then expand the **Logins** folder. Right-click on the **trismadmin** login and select **Properties**.

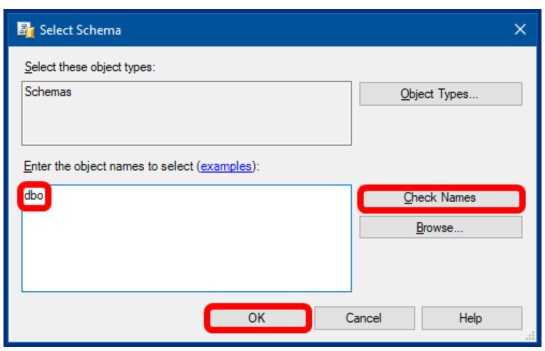


8. In the **Login Properties** window, in the **Select a page** section, select **User Mapping**.
9. In the table, select **Map** on the **master** database row.

10. On the same row, click ... in the **Default Schema** column.



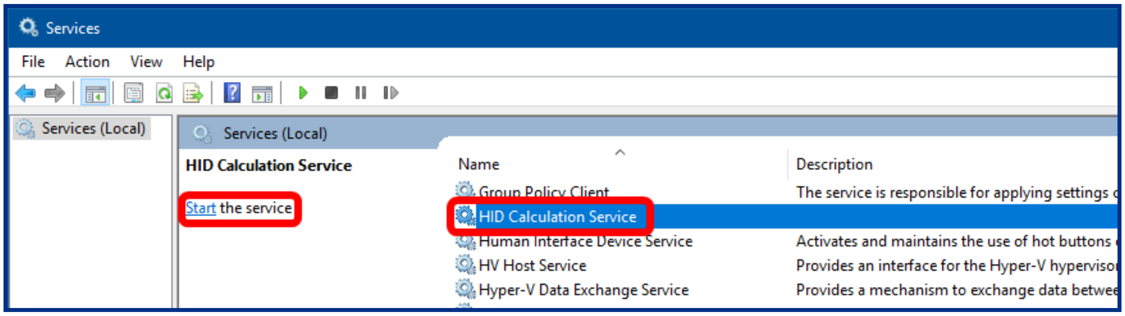
11. In the **Enter the object names to select** text box, type **dbo** and click **Check Names.** The **dbo** text changes to **[dbo].** Click **OK.**



12. In the **Login Properties** window, click **OK.**
13. Close the SQL Server Management Studio.

2.9 Calculation service installation

1. Download and run the HID Calculation Service Installer and any updates in the Current Version location on the FTP Site.
2. Start the **HID Calculation Service**.



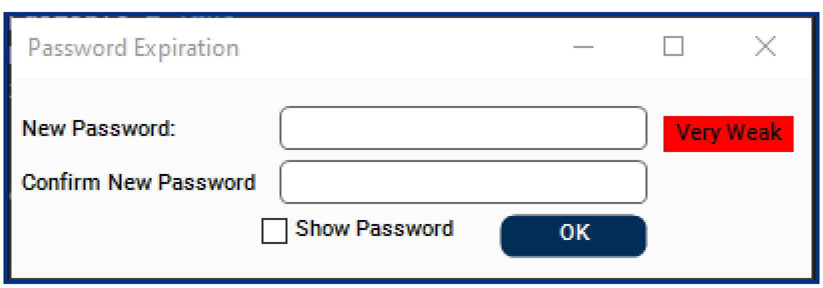
2.10 TRISM client initial configuration

This section assumes that:

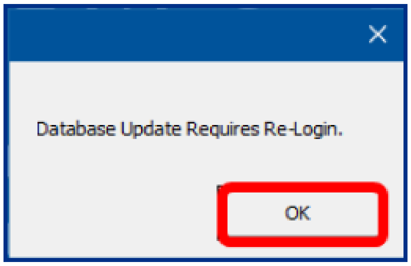
- The HSM has been installed and configured.
- The TRISM Client Database Creation has been completed.
- HID Calculation Service has been installed and started.

1. Run TRISM Client (T6).
2. Enter **access1** as the **User ID** and have the FI enter password of **1234567**. Click **Login**.

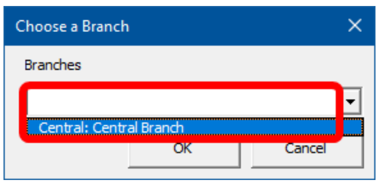
3. You are asked to enter and re-enter a new password. This is the permanent password for the **access1** login. See **7.2.1 Add users (without active directory)** for an explanation of the password strength meter. Click **Create**.



4. You are prompted to login, click **OK**. The Database is updated to whatever version you are currently running. There is a chance that it requires a re-login after the update.

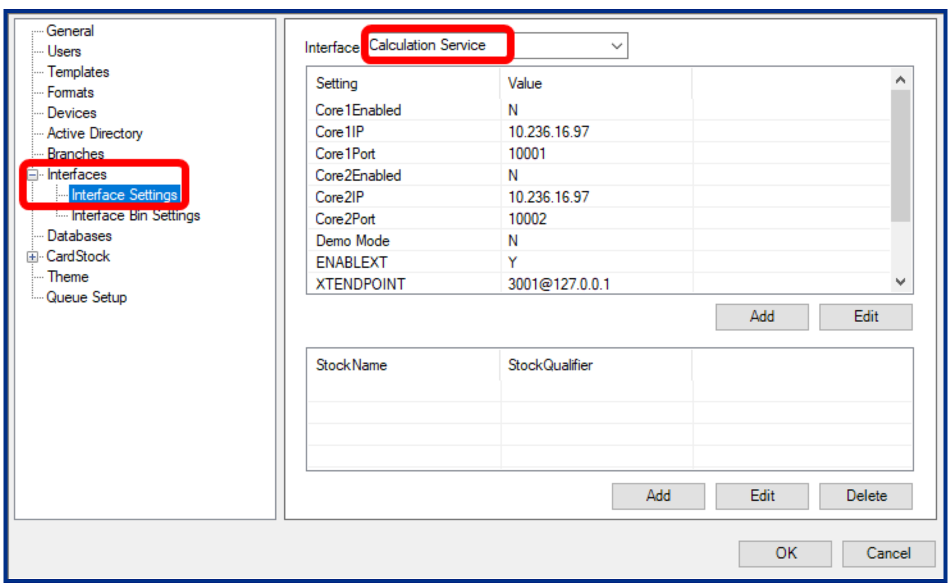


5. A **No Branch Found Please Select a Branch From the list** prompt is displayed. Click **OK**.
6. Select **Central:Central Branch** in the **Branches** drop-down menu and click **OK**.



2.11 Calculation service configuration

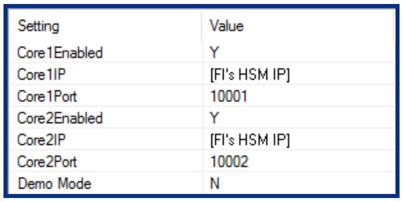
1. In TRISM 7, select the **Personal icon** > **Configure** > **Interfaces** > **Interface Settings**.
2. Select **Calculation Service** from the drop-down menu.



2.11.1 HSM Duo service configuration

Change the Core1 and Core2 settings to point to the HSM cores, using the true IP address of the HSM.

> **Note:** Do not change the **Demo Mode** value on a customer settings. This should only be changed to **Y** on a demo system that is not using an HSM.

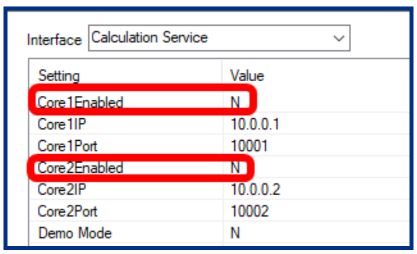


Setting	Value
Core1Enabled	Y
Core1IP	[FI's HSM IP]
Core1Port	10001
Core2Enabled	Y
Core2IP	[FI's HSM IP]
Core2Port	10002
Demo Mode	N

The Calculation Service has been set up correctly if the **Data Log** displays **Core1** and **Core2** have come online. This should happen within 60 seconds of changing the **Core1** and **Core2** settings.

2.11.2 HSM XT service configuration

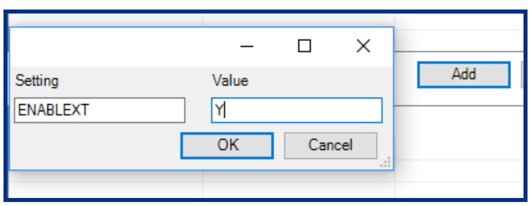
1. Set **Core1Enabled** and **Core2Enabled** to **N**



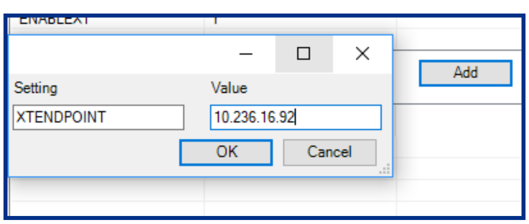
Interface: Calculation Service

Setting	Value
Core1Enabled	N
Core1IP	10.0.0.1
Core1Port	10001
Core2Enabled	N
Core2IP	10.0.0.2
Core2Port	10002
Demo Mode	N

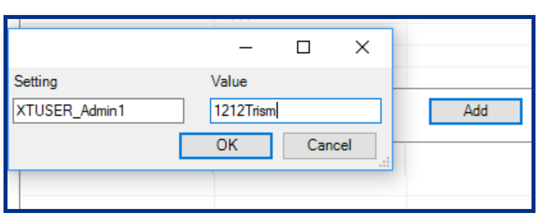
2. Values need to be manually added: ENABLEXT, XTENDPOINT, 2 Admin Users created during HSM XT Installation
3. Click **Add**, for **Setting**, enter **ENABLEXT**, for **Value**, enter **Y**, and click **OK**.



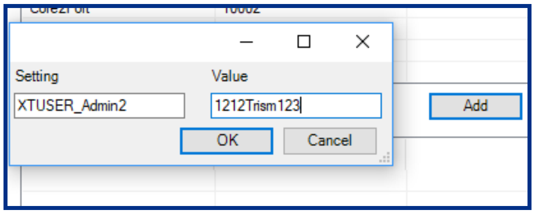
4. Click **Add**, for **Setting**, enter **XTENDPOINT**, for **Value**, enter **[IP of HSM XT]**, and click **OK**.



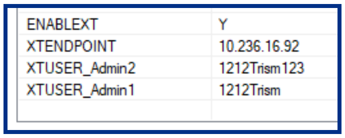
5. Click **Add**, for **Setting**, enter **XTUSER_[adminuser1]**, for **Value**, enter **[pw for adminuser1]**, and click **OK**.



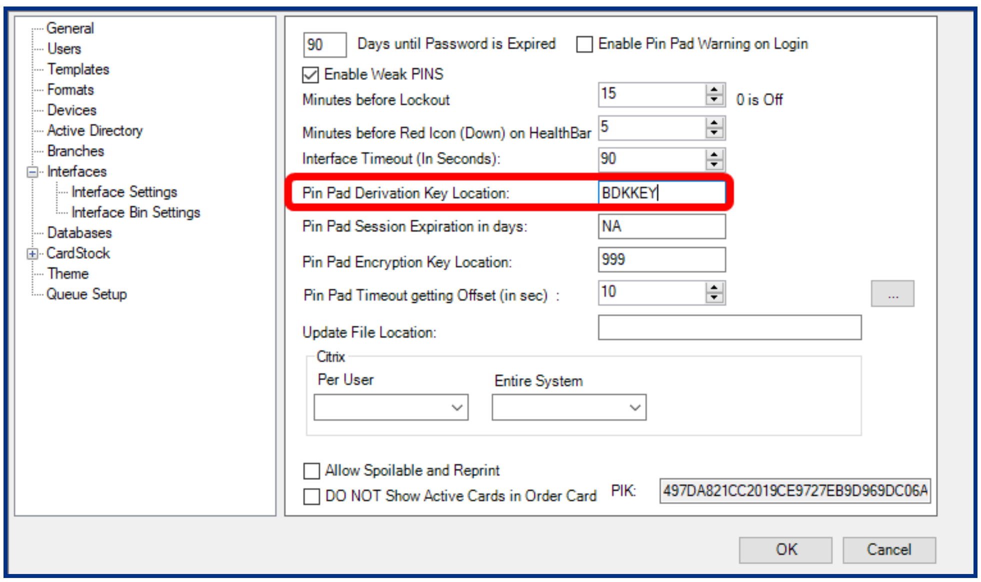
6. Click **Add**, for **Setting**, enter **XTUSER_[adminuser2]**, for **Value**, enter **[pw for adminuser2]**, and click **OK**.



7. All Settings have been added.



8. Restart the **HID Calculation Service**.
9. Close TRISM Manager and select **Yes** on the Are you sure you want to exit? message box.
10. Log into TRISM Manager.
    a. Go to **Configure** > **General**.
    b. In **PIN Pad Derivation Key Location,** enter the name of the **BDK (PinPad Derivation Key)** as entered during the HSM XT Key Install.



2.12 TRISM client configuration - server

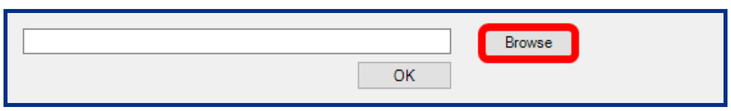
2.12.1 Add license

The following configuration must be carried out on the server on which the initial TRISM installation was completed.

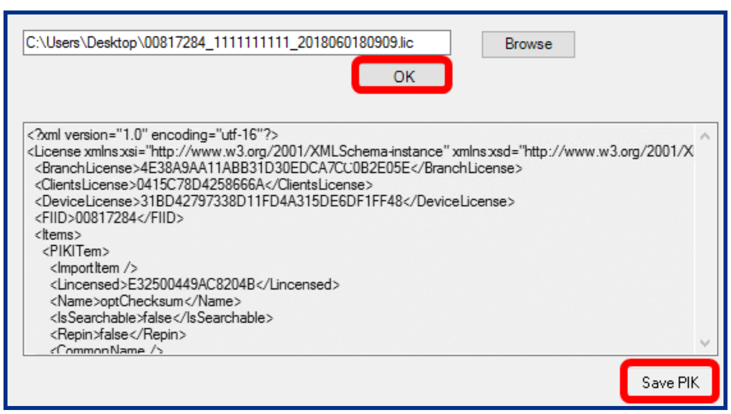
1. In the TRISM login menu, enter the login ID **Access1** and the configured password. Click **Login**.

   > **Note:** If you log in with **installer1**, the password is **1212Trism**. If you log in with **installer2** the password is **1212Trism123**.

2. Click **Help** on the main menu and select **License**.
3. In the **License** window, click **Browse**.



4. Locate the appropriate license file (*.lic), select it and click **Open**.
5. Back in the **License** window, click **OK**. The text box in the body of the License form populates with the opened license's XML.

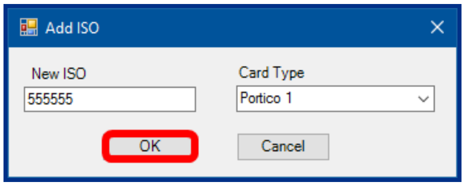


6. Click **Save PIK**. The **PIK has been Saved** prompt is displayed.
7. Click **OK**.
8. Repeat this process for any other license files (branch, device, PIN pad, and so on).

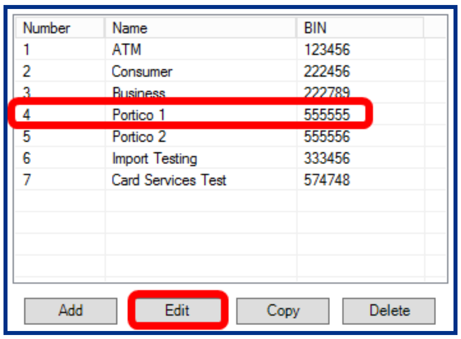
   TRISM Client Initial Configuration is completed.

2.12.2 Add formats

1. In the **Configure** menu, select **Formats.** Select one of the pre-loaded BINs (ATM or Visa Debit), then click **Copy.**
2. Enter the BIN in the **New ISO** field, then select a card type from the drop-down menu or enter a new card type. Click **OK**.

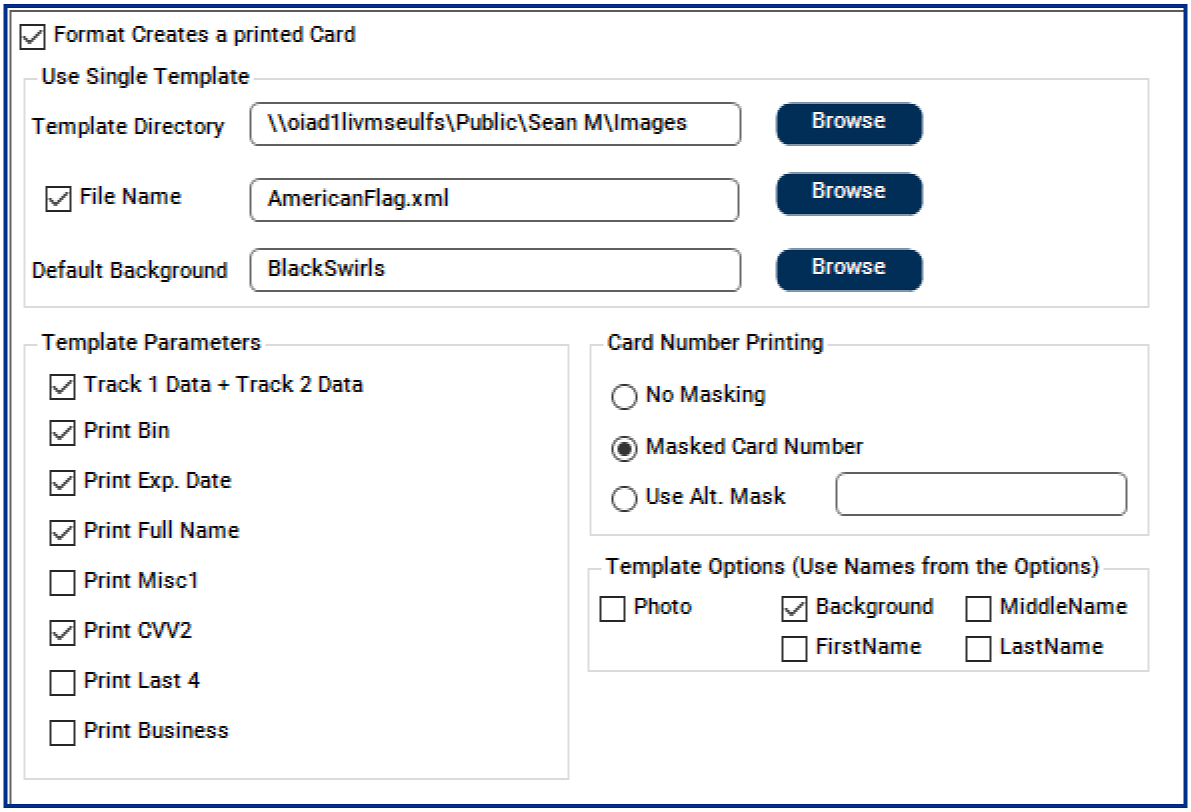


3. Navigate back to the **Personal icon** > **Configure** > **Formats** and select the BIN you just created, then click **Edit.**



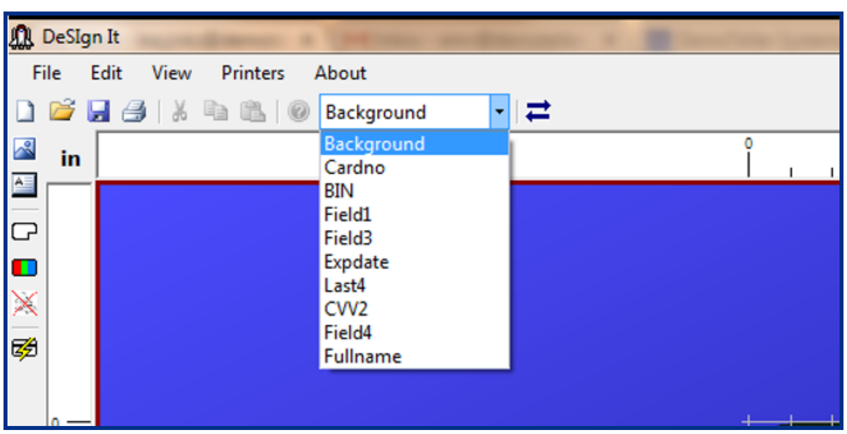
4. Expand the **Encode Settings** menu and configure the track layouts.

5. Expand the **Photo Settings** menu and select the **General** tab:



- Select **Format Creates a printed Card** option.
- In the **Template Directory** field, enter the UNC path of the folder containing the card background images and XMLs.
- If using a single file XML, select the **File Name** box and click **Browse**. Navigate to the Images folder (same as the UNC path above) and select the desired XML.

6. In **Template Parameters**, select the parameters that are used in the XML. To check what parameters are used in the XML, open the XML in **DeSign-It** and expand the drop-down menu to view the parameters.



7. In **Template Options**, check the items for which the FI has a PIK:
   - Photo = cardholder picture printed on card.
   - Background = custom or galleried images printed on card.

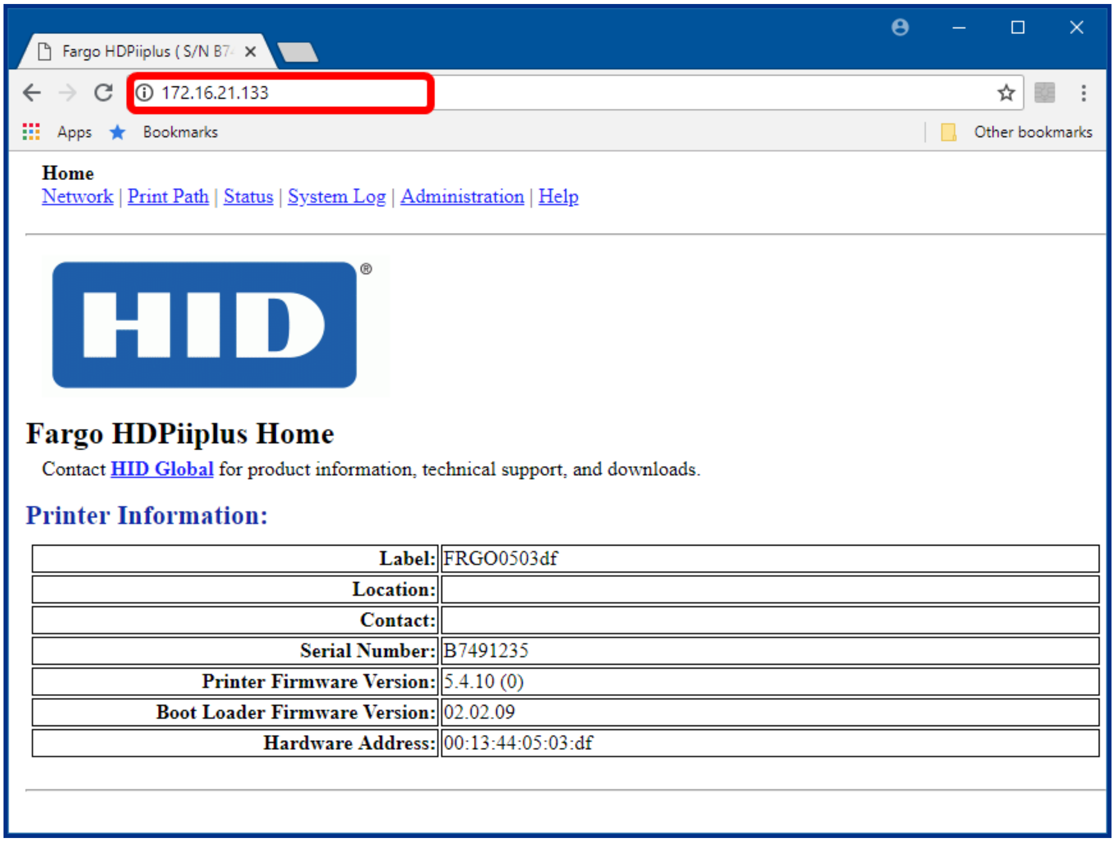
Note: If an error is displayed regarding missing fonts, download the appropriate fonts from the FTP site.

8. If any of the **Template Options** above were selected, select the **Advanced** tab under **Photo Settings**. If the FI is using custom images, select **Enable Background Selection** and **Enable Custom Backgrounds**, then enter the Images folder's UNC path.

2.12.3 Add printers and embossers

Drivered printers

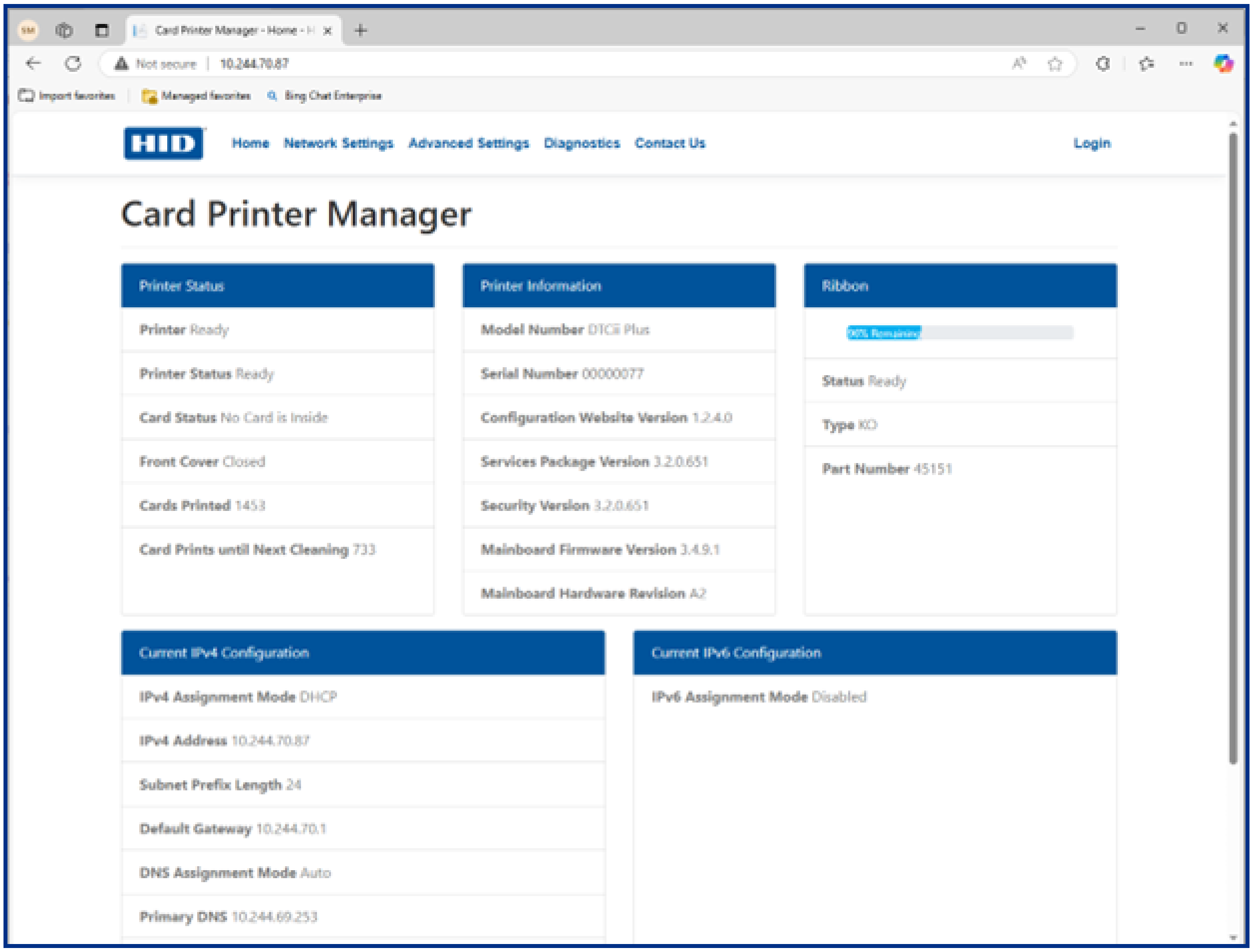
1. Verify connectivity to printer by entering the printer IP address in the address bar of a web browser.



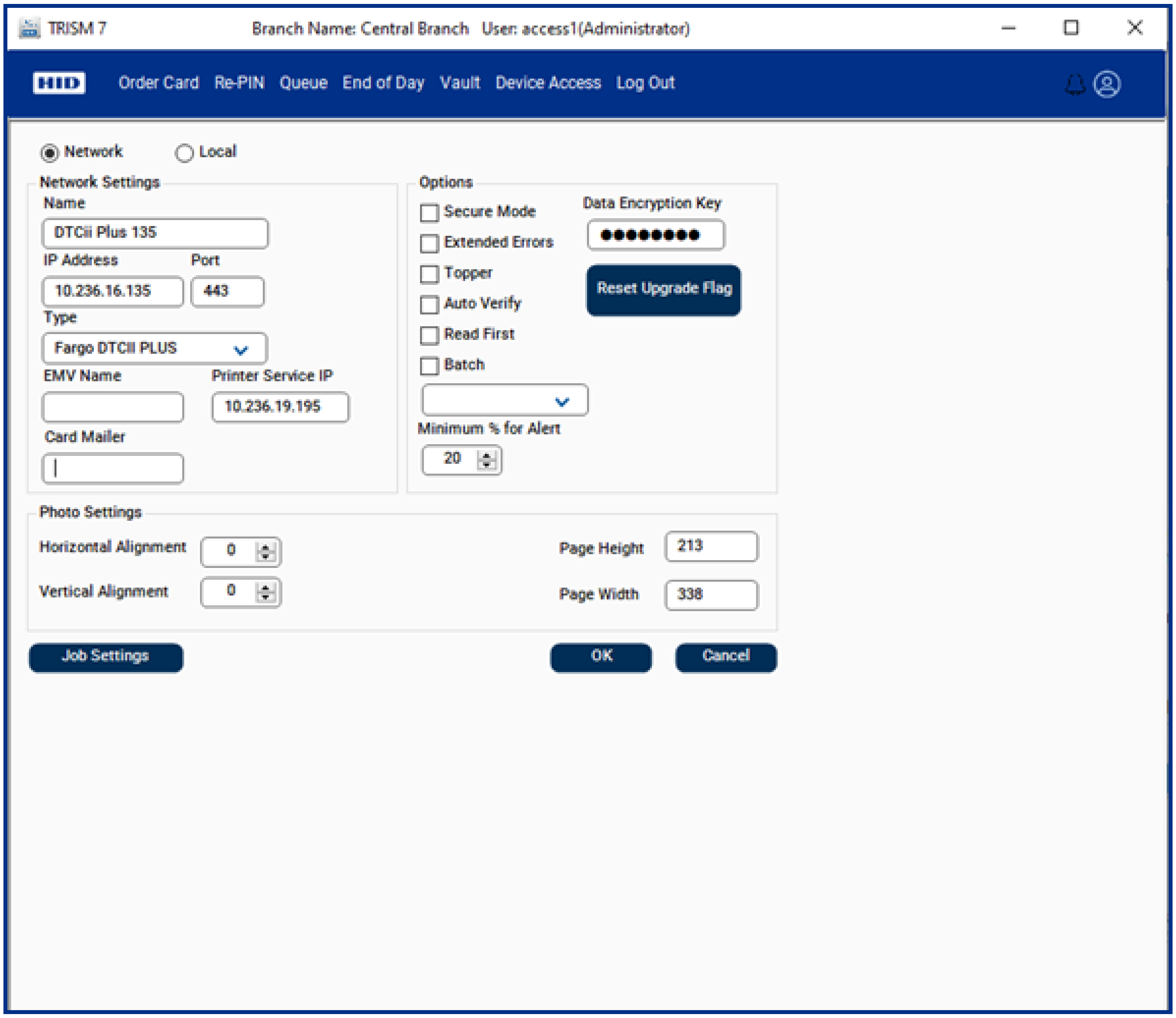
2. Install the printer and smart card reader drivers. Download the following from the FTP site as required:
   - FARGO® HDPii Plus
   - FARGO DTCii
   - HID OMNIKEY® Card Reader USB
   - Evolis Primacy: Evolis Premium Suite and Identive MultiSlot-CLOUD Driver Installer
3. Configure settings in **Windows Printer** properties and **Evolis Printer** properties or **FARGO Workbench**.
4. Add printers to the TRISM client. Note that the printer name in TRISM, and its corresponding name in Windows Devices and Printers, must match exactly. It is advised to copy the name from Windows Devices and Printers and paste it into the name field in TRISM.

Driverless printers

1. Verify connectivity to the printer by entering the printer IP address in the address bar of a web browser.



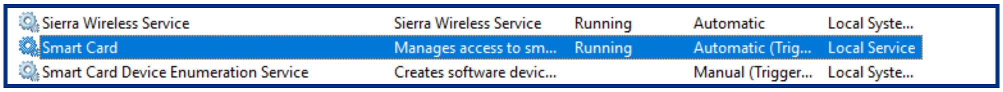
2. Go to the **Personal icon** > **Configure** > **Devices** and click **Add**.



3. With **Network** selected, configure the device as follows:
   Name: The desired name for the printer.
   IP Address: IP address of the printer.
   Port: Because SSL is enabled on the printer, set the port to **443**.
   Type: Fargo DTCii PLUS or **Fargo HDP600ii**.
   Printer Service IP: The IP of the server where the HID Card Printer Service is installed and running.
   Minimum % for Alert: If the financial institution desires to enable low ribbon/film warnings, set the minimum% of ribbon/film remaining to trigger alerts.
4. Click **OK** to save.
5. At the **Device Added Successfully** prompt, click **OK**.
6. At the **You must Restart Card Printer Service** prompt, click **OK**.

2.12.4 Install card printer service

1. Download and run the 7.0 HID Card Printer Service from the FTP site.
2. By default, Windows has Smart Card service disabled. To enable this service, go into services, right-click **Smart Card**, set it to automatic, and start the service.



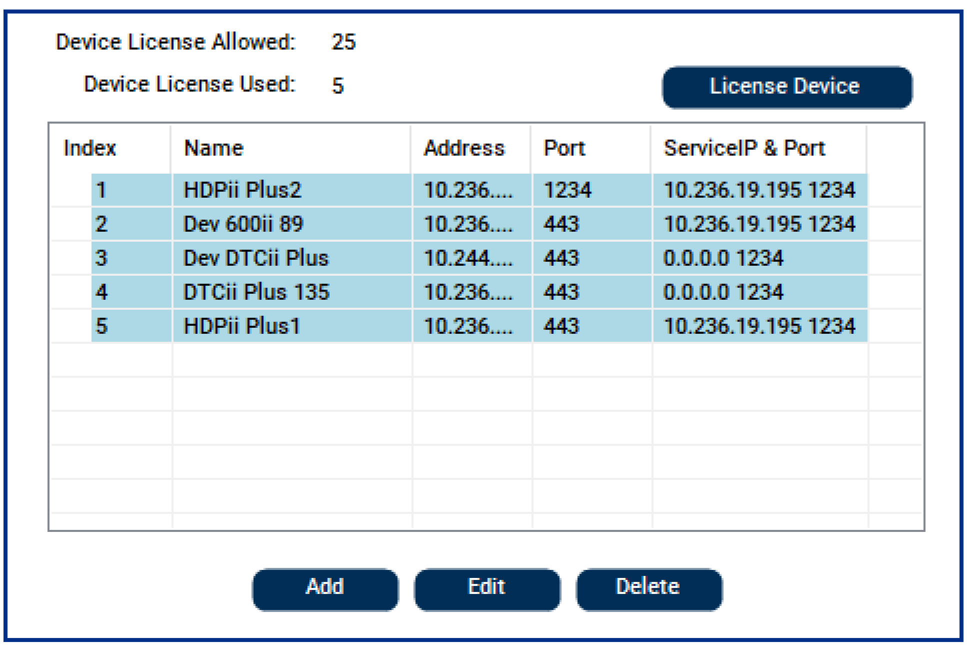
3. Start the Card Printer Service to populate the Card Printer Service interface settings in TRISM. An error is displayed. Click **OK** and proceed to the next step.
4. To configure the Card Printer Service in TRISM, select the **Personal icon** > **Configure** > **Interfaces** > **Interface Settings** and select **Card Printer Service**.
5. Enter the domain username and password. The password returns an encrypted value in the setting field.
6. Select the **Personal icon** > **Configure** > **Interfaces** > **Interface Bin Settings** and select **Card Printer Service**.
7. Enter the **EMV key locations**.
8. Repeat steps 4. to 7. for each BIN.
9. Save EMV template file to **C:\ProgramData\HID Global\TRISM\Card Printer Service**.

> **Note:**
> If this folder does not exist, create it.
> The default template name extension in interface settings vs. actual (.xml vs. .txt). They must match.

10. Restart the Card Printer Service.
11. Verify the Card Printer Service is running in the TRISM Data Log.

2.12.5 Configure device settings in TRISM

1. On the main menu, click **Configure**. On the side menu, click **Devices**.



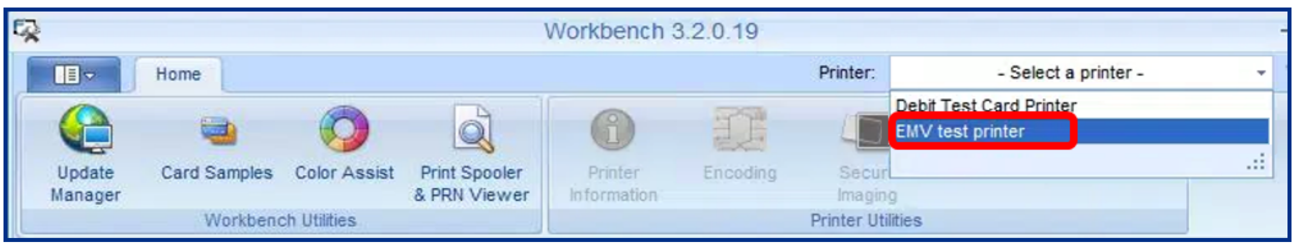
2. Select a device and click **Edit**.
3. Select the correct device type from the **Type** drop-down menu.

4. Enter a unique printer IP address and port number for each device.
5. Printer Service IP = the IP from where the card printer service is running.
6. Edit photo settings according to device, if applicable.
7. Verify page height = 213 and page width = 338.
8. Click **OK.**
9. Continue to the device-specific printer setup instructions.

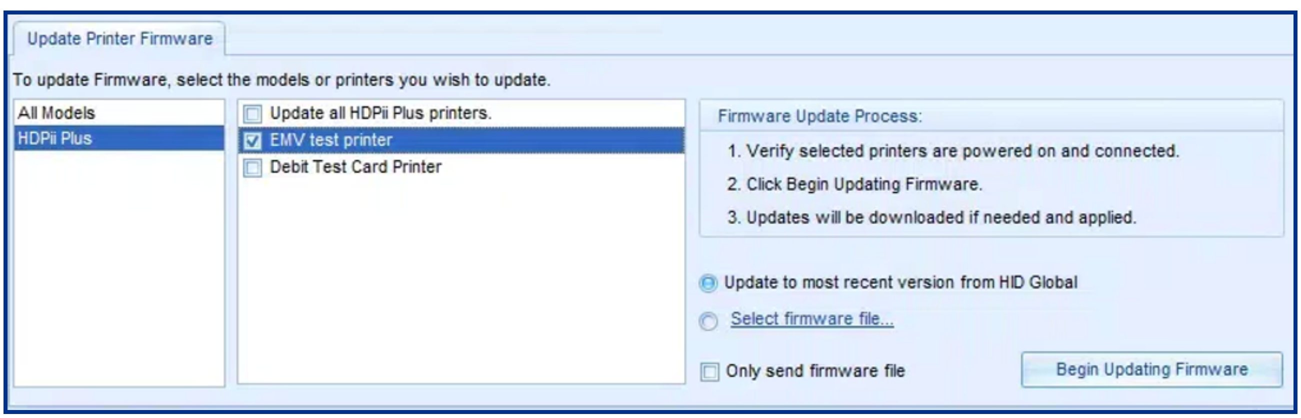
2.12.6 Device-specific setup instructions: FARGO HDPii PLUS - Ethernet

The following must be performed from the console, not an RDP session.

1. Download HID OMNIKEY Ethernet driver (32- and 64-bit).
2. Open the OMNIKEY 5121 Ethernet Encoder Utility (this may be located in the Start menu and not on the desktop). Click **File** and select **Add New Encoder**.
3. Select **Use Dynamic IP Configuration**, click **OK**.
4. Click **Install.** This can take a few minutes. A timer appears by the reader in **Devices and Printers**.
5. Install up to nine additional devices.
6. Install and run **FARGO Workbench**.
7. Download the latest firmware update from the FTP site.
8. In **FARGO Workbench**, select the printer from the drop-down menu.



9. Click the **Printer Information icon**, then click **Update Manager**. Select the box corresponding to the printer, then select **Select firmware file…** and browse to the firmware downloaded from the FTP site. Click **Begin Updating Firmware**.



10. The printer LCD may prompt to begin updating firmware. If so, have the FI personnel press the right button.

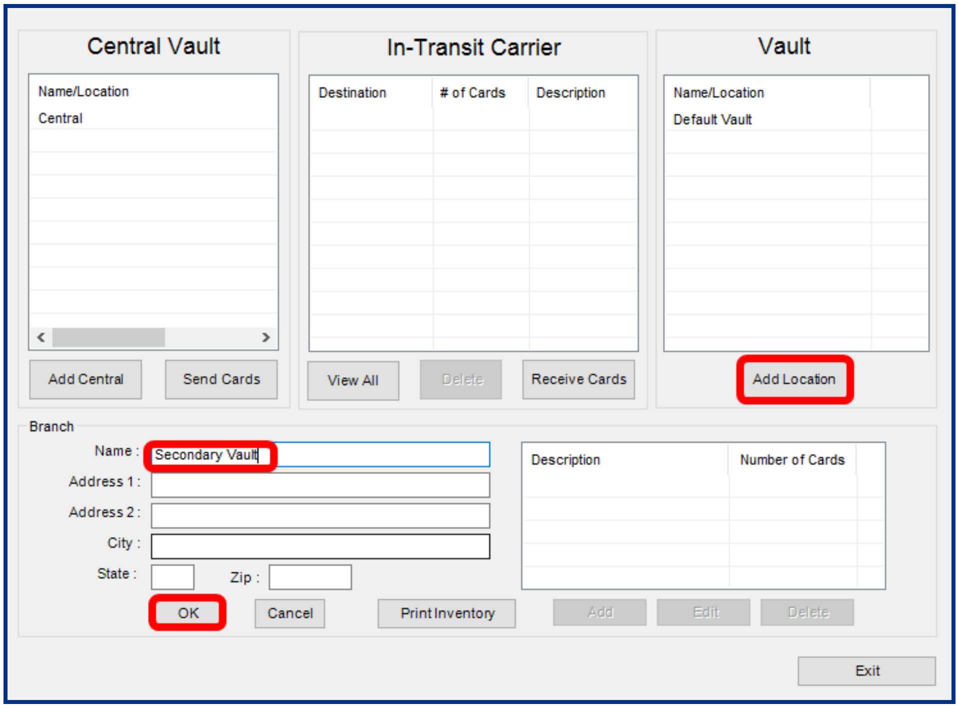
2.12.7 Device-specific setup instructions: FARGO HDPii PLUS - USB

Follow the FARGO HDPii Plus-Ethernet instructions above. In TRISM device settings, enter 127.0.0.1 as the IP address. In the EMV Name field, enter the name of the EMV encoder.

2.12.8 Add vaults

> **Note:** There is typically one vault per printer.

1. On the main menu, click **Inventory** > **Vault Inventory**.
2. In the **Vault** section, click **Add Location**.
3. Enter a vault name and click **OK**.

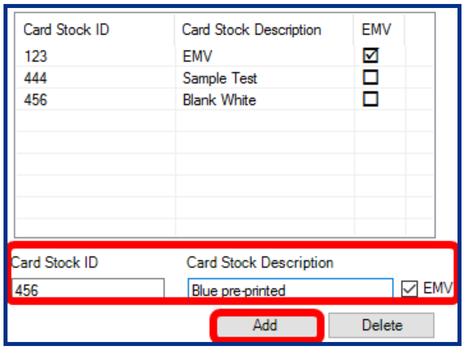


2.12.9 Add branches

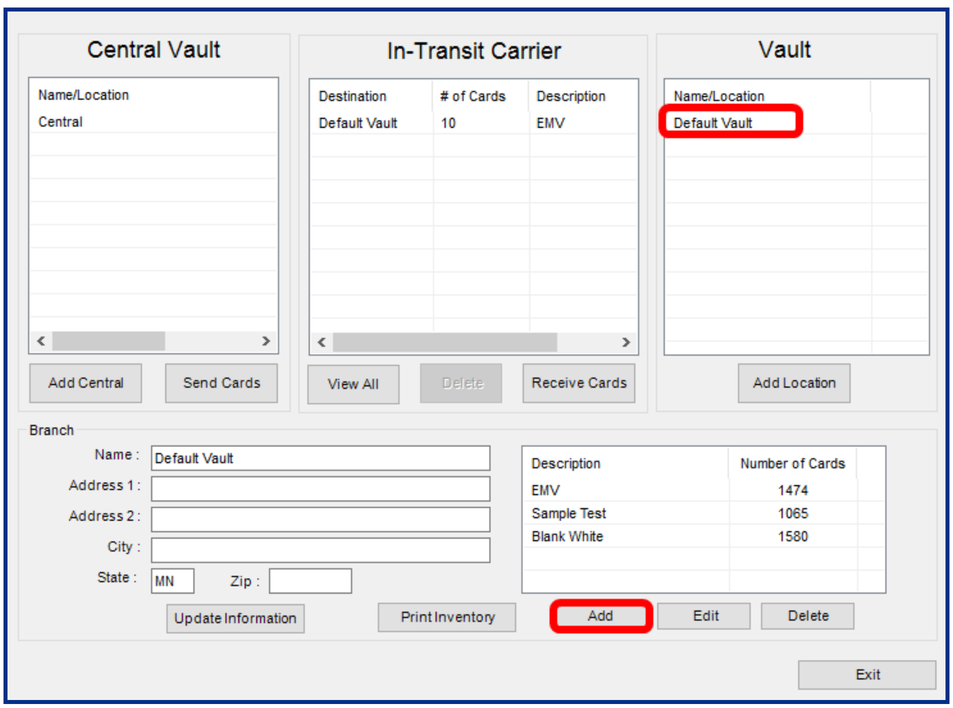
1. On the main menu, click the **Personal icon** > **Configure** > **Branches**.
2. Click **Add**.
3. Enter the Branch ID, Branch Name, and address (if available) for one of the FI's branches, then click **OK**.
4. Repeat this process for the remaining branches.

2.12.10 Setup card stock

1. Select the **Personal icon** > **Configure** > **CardStock** > **CardStock ID**, enter a **Card Stock ID** and **Card Stock Description** (for example, blank white or pre-printed). Check the **EMV** option if the cardstock has an EMV chip. Click **Add**.



2. Select the **Personal icon** > **Configure** > **CardStock** > **CardStock to BIN**, select the card stock you just created in the first drop-down menu (if it is not listed, close and re-open TRISM client).
3. Select the **BIN** to use with the cardstock in the bottom drop-down menu, then click **Add**. The card stock and BIN are now linked.
4. Select the **Personal icon** > **Inventory** > **Vault Inventory**, select a **Vault** and click **Add**. Select the cardstock and enter a quantity (this can be changed later).



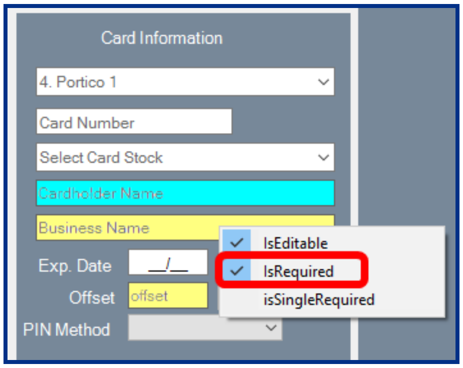
5. In the **Personal icon** > **Configure** > **CardStock** > **CardStock to Vault/Device**, select the cardstock and the vault and device to be linked. Select a **State** (usually **Ready - card will print immediately after ordering**) and click **Add**.

2.13 TRISM client configuration: workstation

The following configuration must be performed at a workstation with a PIN pad plugged in. For information about the PIN pad, see **2.13.3 Changing the COM port of an installed PIN Pad**.

2.13.1 Edit permissions

1. On the main menu, click the **Personal icon** > **Request** > **Edit Permissions**.
2. Right-click the **Cardholder Name** field and select **IsRequired**.



2.13.2 Install VFI USB driver

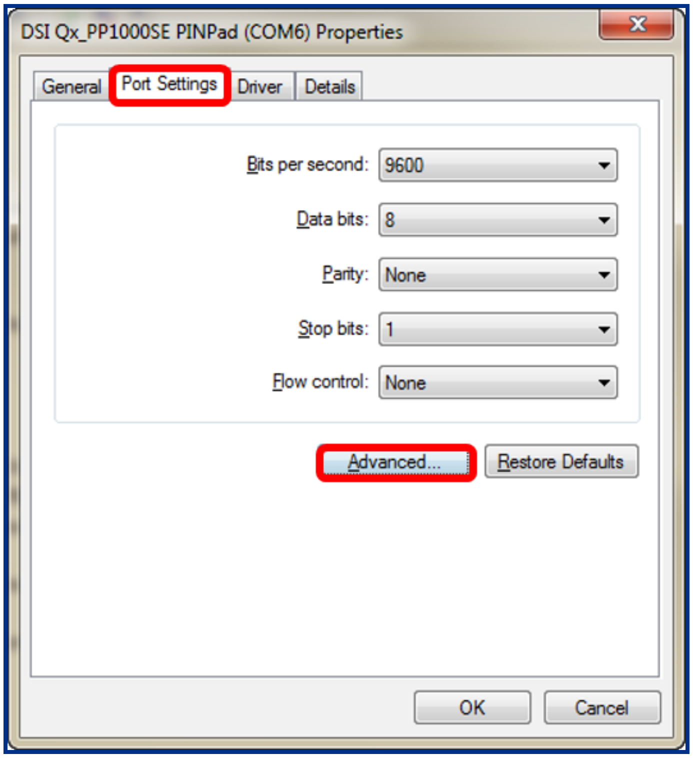
To install the Vx USB driver (VFI_USB_Driver_2.0.X.msi):

1. Download the **VFI_USB_Driver_Installer_2.X.X.X_BX** zip file from the FTP site.
2. Extract the contents of the zip file to any folder.
3. Right-click the **silent.bat** file in the extracted folder, and run as administrator.
4. Wait for the install to finish.
5. Connect the Vx PINpad to the workstation.

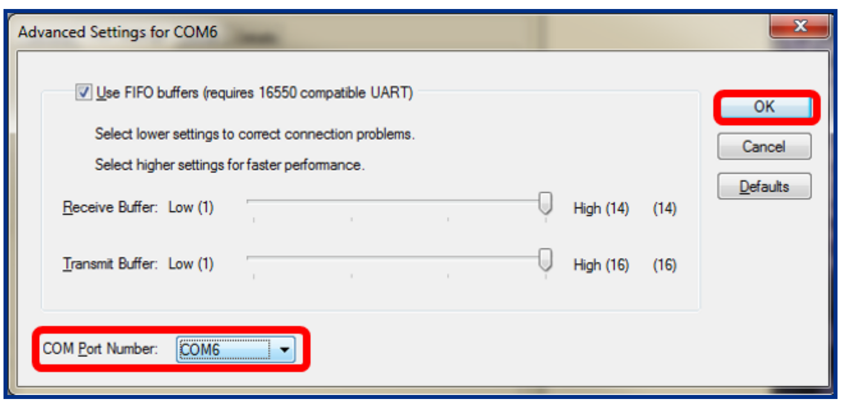
2.13.3 Changing the COM port of an installed PIN Pad

1. If you want to use a PIN Pad in conjunction with TRISM client software that is running under Microsoft Terminal Services or Citrix, then you most often need to select a specific COM port for the PIN Pad that is to be used across all workstations. To do this, right-click on the PIN Pad in the **Device Manager** and once again select **Properties**.

2. In the **Properties** window, select the **Port Settings** tab and click **Advanced**.



3. Select the appropriate COM port that you wish to use in the **COM Port Number** drop-down menu and click **OK** to save your settings.



4. Unplug the PIN Pad from the USB port, then plug it back in once to ensure that it is registering on the newly assigned COM port in your remote environment.

Note: If you encounter problems with the driver installation, ensure that the Microsoft **USBSER.SYS** (USB-to-Serial) system file is in the **C:\Windows\System 32\Driver** folder. If it is not, then you can copy it over from another computer on your network. If you do not have another machine on your network that has this file, then you can try using the **USBSER.SYS** file that was included in the PIN Pad driver **.zip** file.

Section **03**

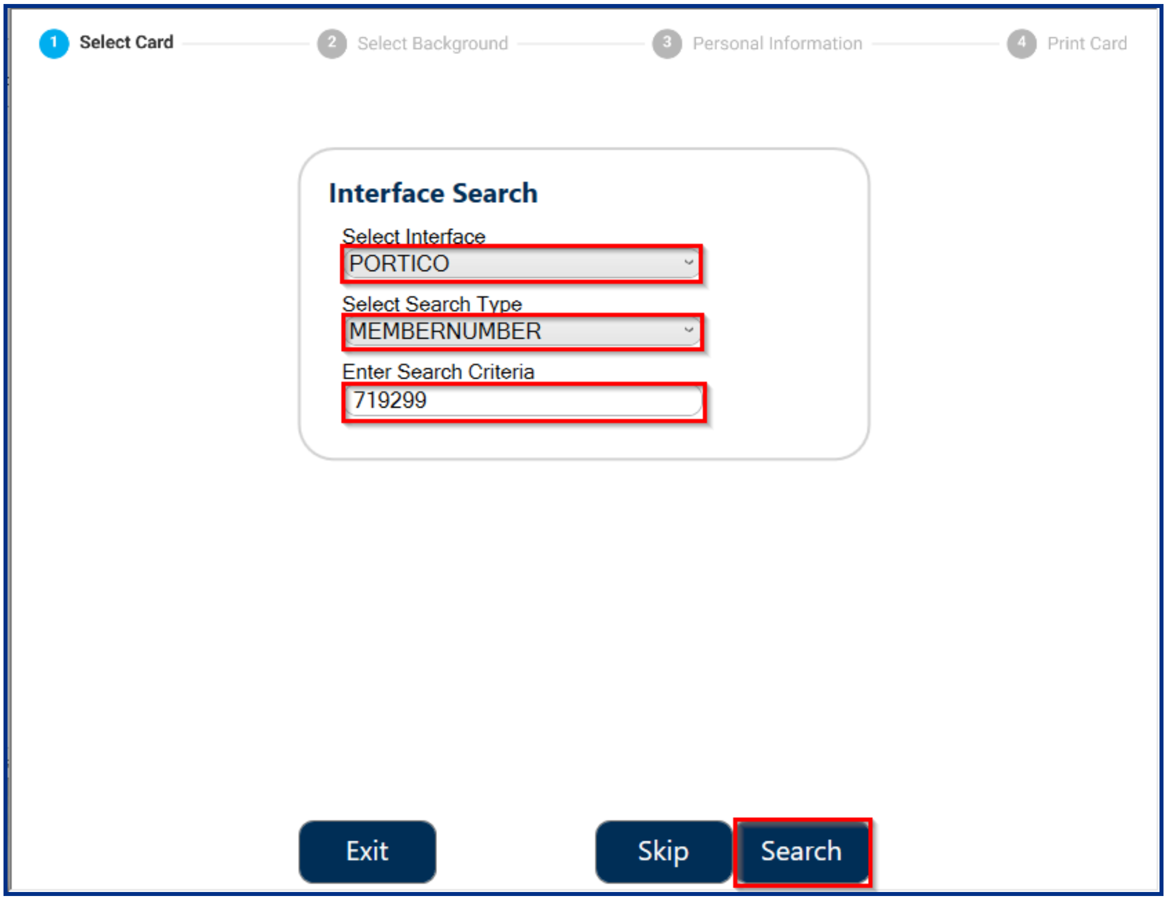
Request

3.1 Order Card

1. Interface search

   a. From the **Quick launch** toolbar, click Order Card or click the **Personal icon** > **Request** > **Order Card**.

   b. The Interface Search window is displayed. Select the appropriate BIN from the **Select Interface** drop-down menu.



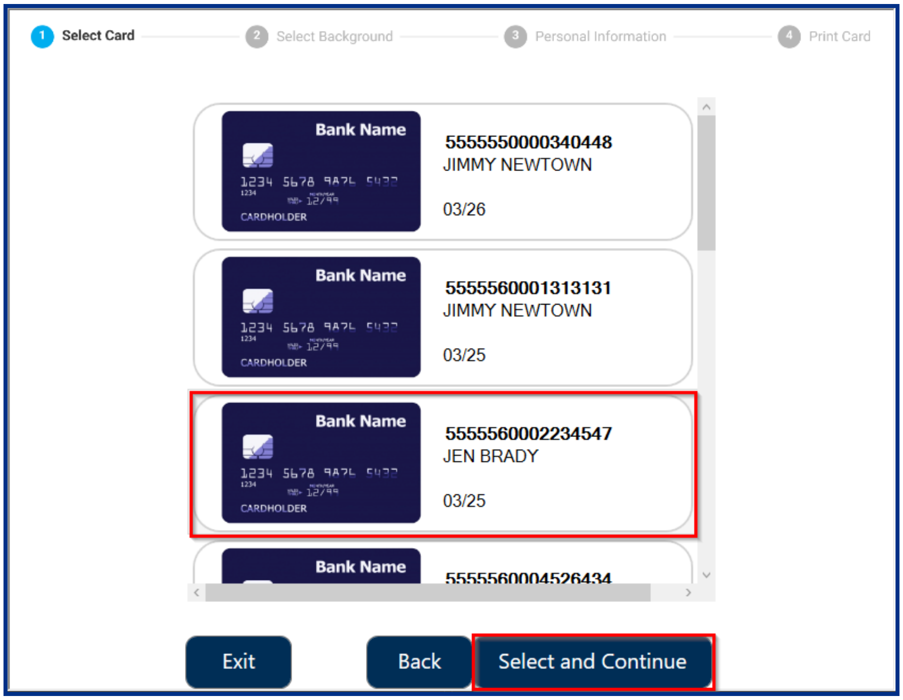
- **If a core/processor interface is used**: select the interface, search by member or card number, and enter the member or card number. **If searching by card number**, the cardholder's information is populated in the information fields. **If searching by member number**, select the corresponding account in the bottom menu, then the account's information is populated in the information fields.
- **If a core/processor interface is not used**: complete the address information, security information, and contact information fields. After step 3.c, click **Accounts** in the **Account Information** menu, then enter the **customer's account number** and **ChkSavDesignator**. One account must have **Primary** selected.

   c. Select the search type from the **Select Search Type** drop-down menu.

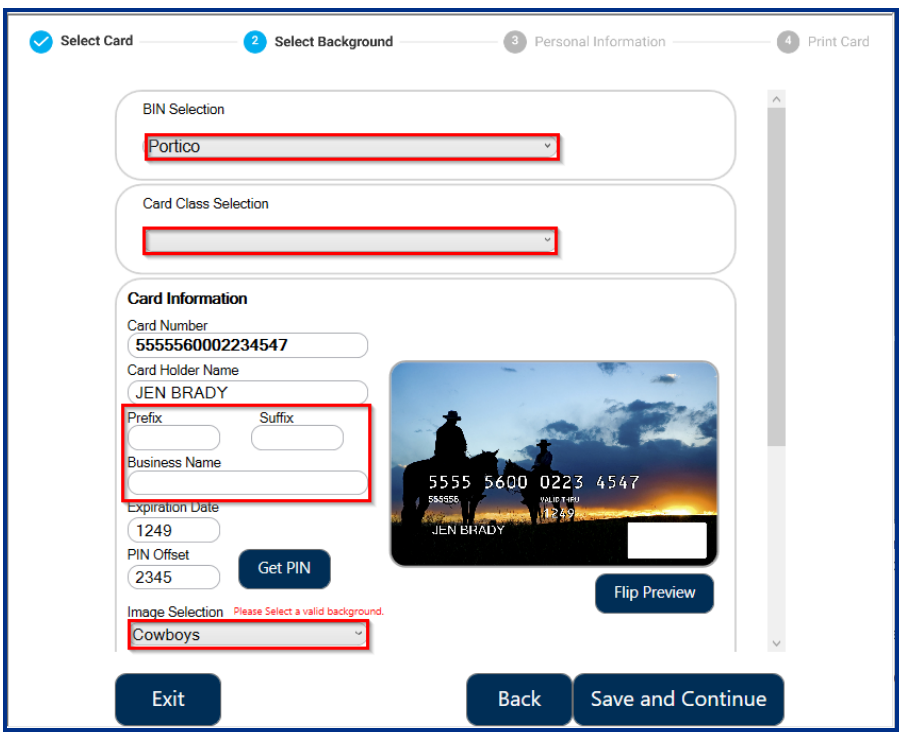
   d. Enter the search criteria in the **Enter Search Criteria** drop-down menu.

   e. Click **Search**.

2. The search results are displayed. Select the appropriate account number, then click **Select and Continue**.



3. Card information

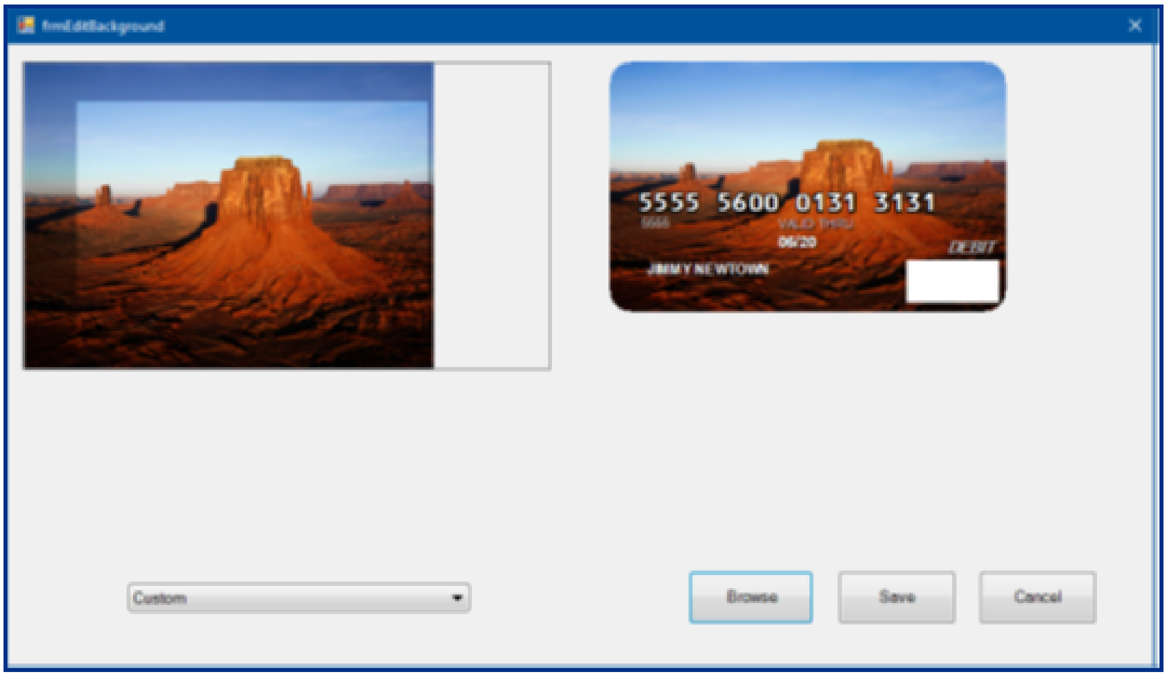


a. Select a BIN from the **BIN Selection** drop-down menu.
b. Select a card class (if any) from the **Card Class Selection** drop-down menu.
c. If not automatically generated, enter **Prefix/Suffix/Business Name** (if any) in the provided fields. Also enter the card's **Expiration Date**, if not automatically generated.
d. Select a PIN method.

   e. Click **Get PIN**. The PIN is generated if specified, otherwise, the PIN pad beeps.

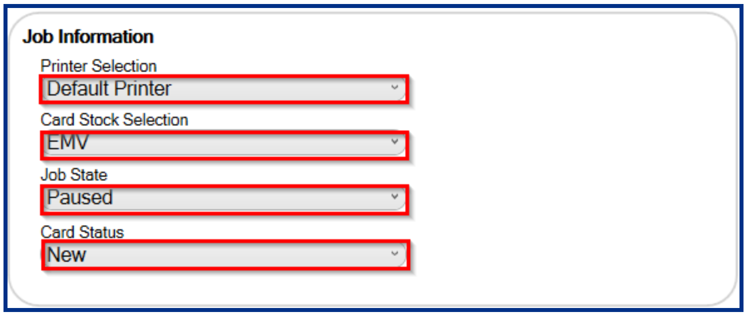
      > **Note:** The Verifone Vx805 and P200 PIN pads do not have the beep functionality.

   f. Enter the desired PIN on the PIN pad. Press the green **Enter** button. The PIN pad beeps again. Re-enter the PIN and press the green **Enter** button to confirm the PIN.
   g. The card's offset is displayed after the PIN is entered.
4. Personalizing and Previewing Cards – See section **A.3 Custom image guidelines** for image guidelines.
   a. Select a gallery image from the drop-down menu or click **Personalize**. If only one image is in the gallery destination folder, that image displays automatically.

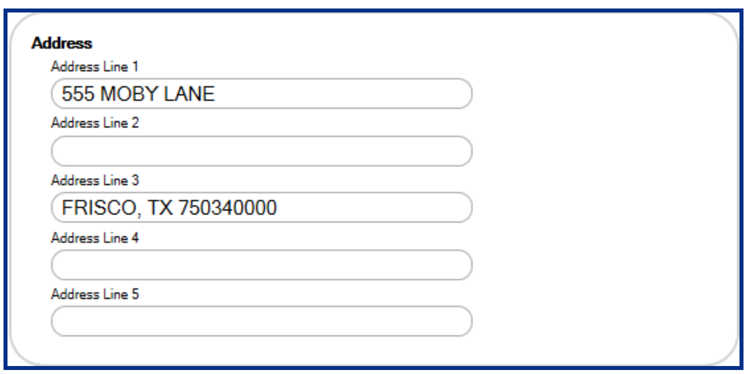


   b. Click **Browse** and navigate to the folder containing the custom image.
   c. Select the image and click **Open**.
   d. To crop the image, click and drag an area on the image on the left.
   e. If applicable, select the desired template from the drop-down menu in the bottom left of the screen.
   f. Click **Save** when personalization is complete.
   g. Click **Back** to preview the backside of the card.

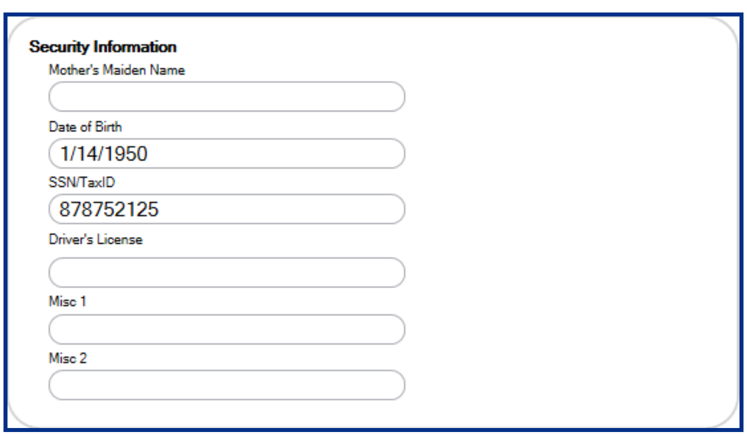
5. Job Information



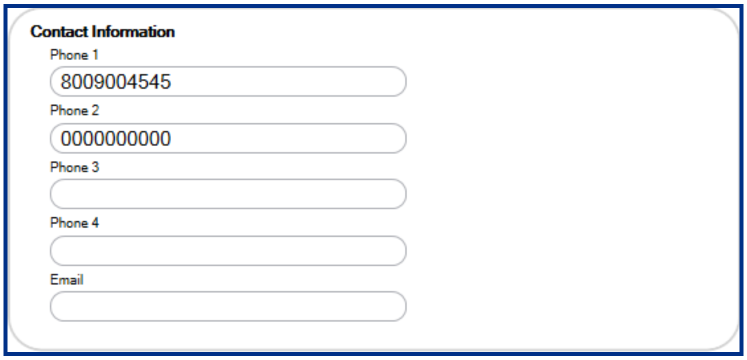
   a. Select a printer from the **Printer Selection** drop-down menu.
   b. Select a card stock from the **Card Stock Selection** drop-down menu.
   c. Select a state from the **Job State** drop-down menu.
      - **Ready:** card prints immediately upon completion.
      - **Paused:** card does not print until state is changed to Ready in the Queue.
      - **Manual:** card does not print until it is manually fed into printer (not available with all printers).
   d. Select a card status from the **Card Status** drop-down menu.
6. Click **Save and Continue**.
7. Fill in any missing Address Information.



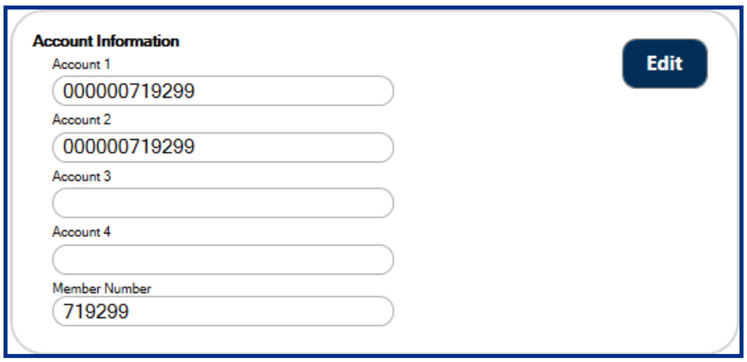
8. Fill in any Security Information.



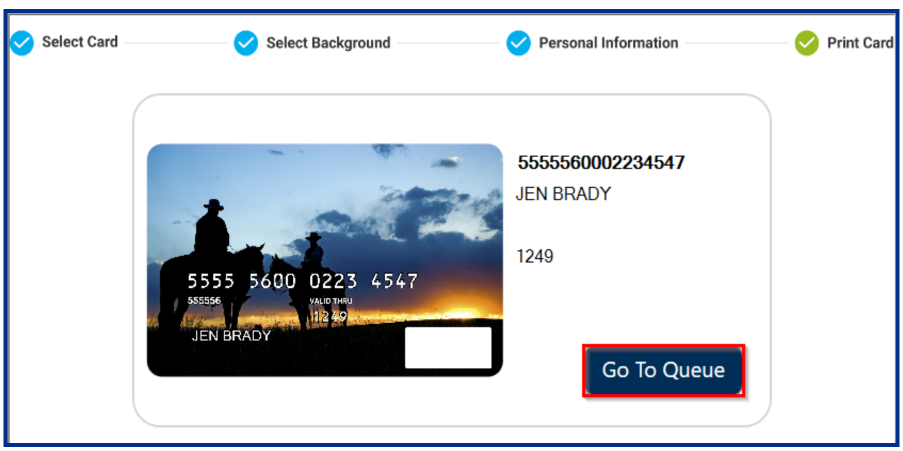
9. Fill in any contact Information.



10. Fill in any account information.



11. Click **Save and Continue**.
12. Click **Go To Queue** to view the newly created card.

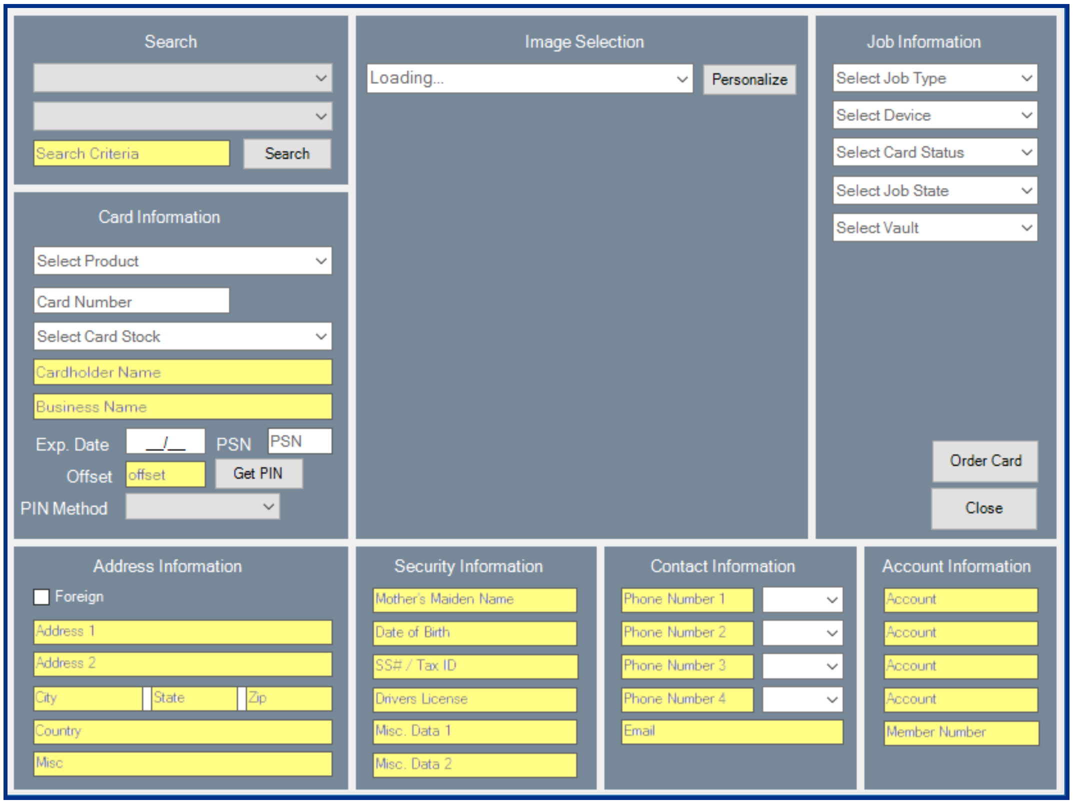


3.2 Edit Permissions

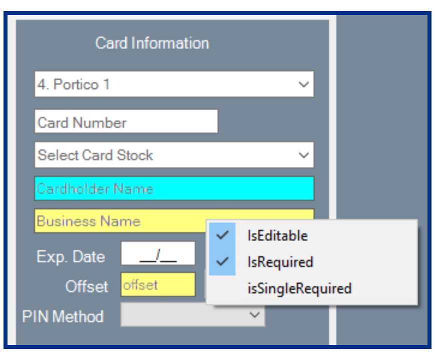
The **Edit Permissions** window allows a user to make certain fields in the **Order Card** window editable or required.

On the main menu, click the **Personal icon** > **Request** > **Edit Permissions**. Select a card type to edit its permissions.

In the following screen, the fields highlighted in yellow have editable permissions.

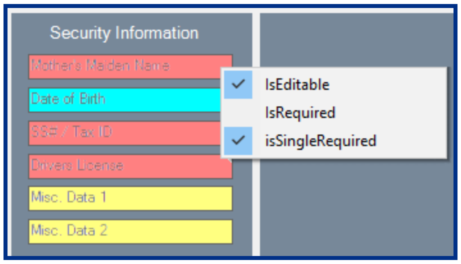


You can change the colors of the **Editable**, **Required** and **Single Required** fields in **7.11 Theme**.



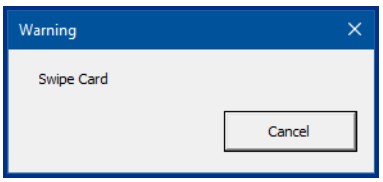
- **IsEditable**: enables input of text.
- **IsRequired**: field must be filled to complete request.
- **IsSingleRequired**: one out of all Single Required fields per panel must be completed.

For example, in the Security Information panel, **Mother's Maiden Name**, **SS#/Tax ID**, and **Drivers License** are single required, so one of these three fields must be completed to process the request.



3.3 Re-PIN

1. On the main menu, click the **Personal icon** > **Request** > **Re-PIN**.
   - If the PINpad has a card reader, a window prompts you to swipe the card to re-PIN.

   - If a card reader is not used or the card is not available, the **Order Card** form is displayed for card number information entry.
2. Select the PIN method, enter or generate the PIN.
3. Click **Complete**.

3.4 Read a Card

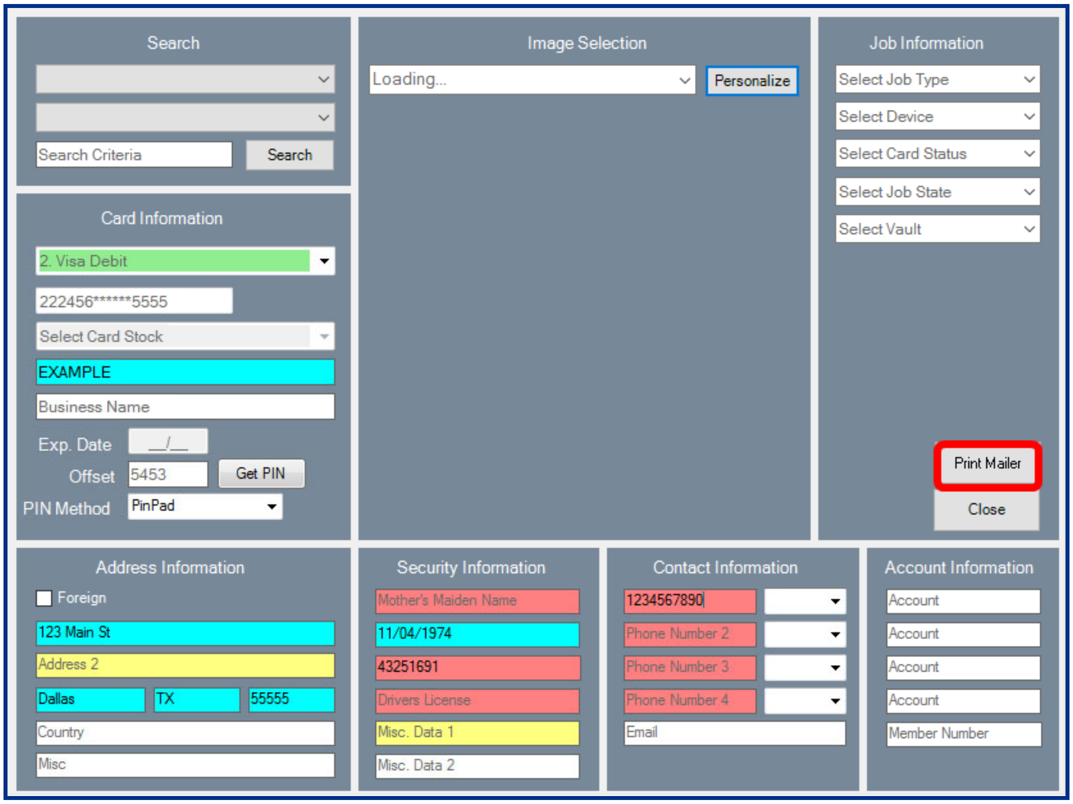
On the main menu, click the **Personal icon** > **Request** > **Read a Card**.

If a PINpad with a card reader or USB card reader is detected, you can swipe a card to display its track data (Card Number, Format Code, Expiration Date, and so on).

Field Name	Data
Format Code	B
Card Number	5555560002234547
Name	^BRADY/JEN
Expiration Date	2006
Service Code	101
Member Number	1
Offset	3386
Misc. Data	0000000000
CVV	123
Misc. Data	000000

3.5 PIN mailer

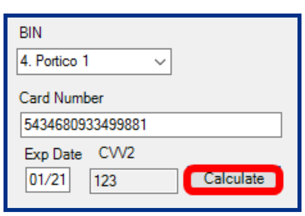
On the main menu, click the **Personal icon** > **Request** > **PIN Mailer**. A PIN mailer can be printed from this window if one is not printed at the time of card creation.



1. In the **Search** area of this window,
    a. In the first drop-down box, select an **Interface** (if there is more than one available).
    b. In the second drop-down box select a **Search Criteria Type** (if there is more than one available).
    c. In the **Search Criteria** field, enter the required information and click **Search**.
2. In the **Card Information** area of this window, select the desired card number to populate the customer information.
3. Click **Print Mailer**.

3.6 CVV2 Calculator

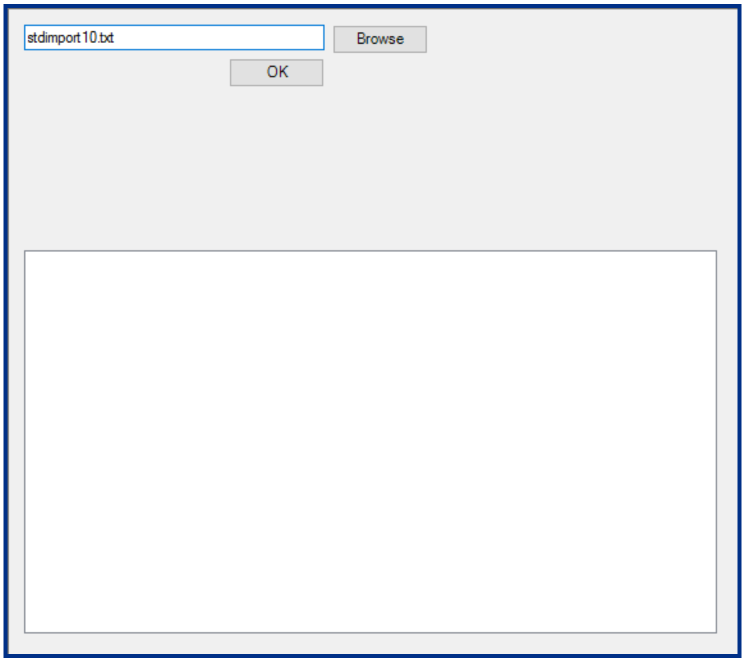
1. On the main menu, click the **Personal icon** > **Request** > **CVV2 Calculator**.
2. Verify the keys entered in HSM Manager are correct.



3. Enter the BIN, card number, and expiration date of an existing card.
4. Click **Calculate**. If the CVV2 on the card and the generated CVV2 match, the keys are correct.

3.7 Import

1. On the main menu, click the **Personal icon** > **Request** > **Import > Standard** (or an alternative).



2. Click **Browse** to select your import file.
3. Click **OK.**

   A list of failed cards shows in the list view with the error per card. Any card not in this list view is successful and in the queue depending on your format settings.

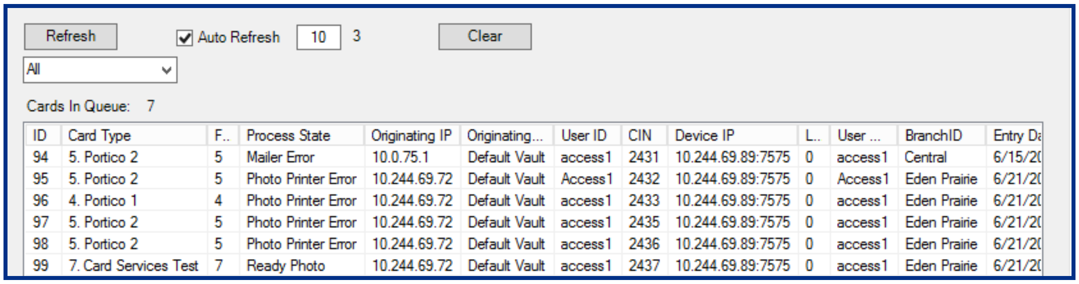
Section 04

Queue

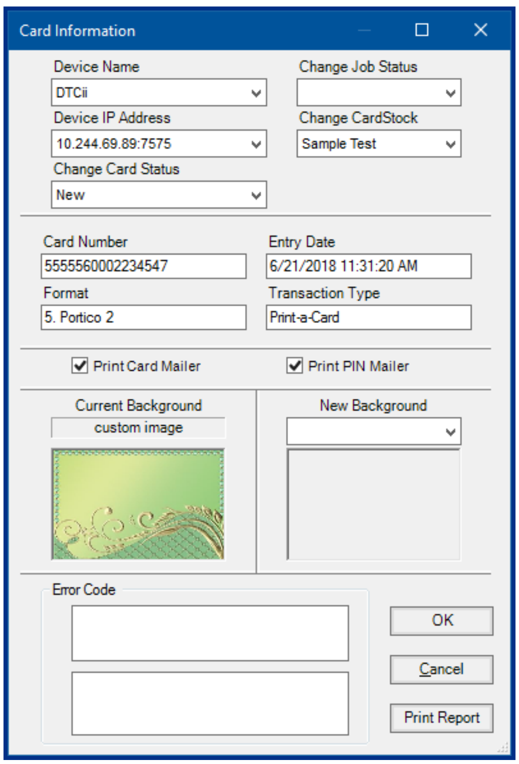
4.1 Card queue

The queue displays all cards that have been ordered and have not yet printed.

On the main menu, click Queue.



Double-click an item in the queue to display the Card Information window:



Note: If a Card Information window is open at another workstation or branch, the card cannot be printed, deleted, or changed. In the process state in the queue, this shows as "Trism locked".

- **Change Job Status** allows you to select the card status as ready photo, paused photo, manual photo, or card verified.
- To delete a card from the queue, select it and press **Delete** on your keyboard.

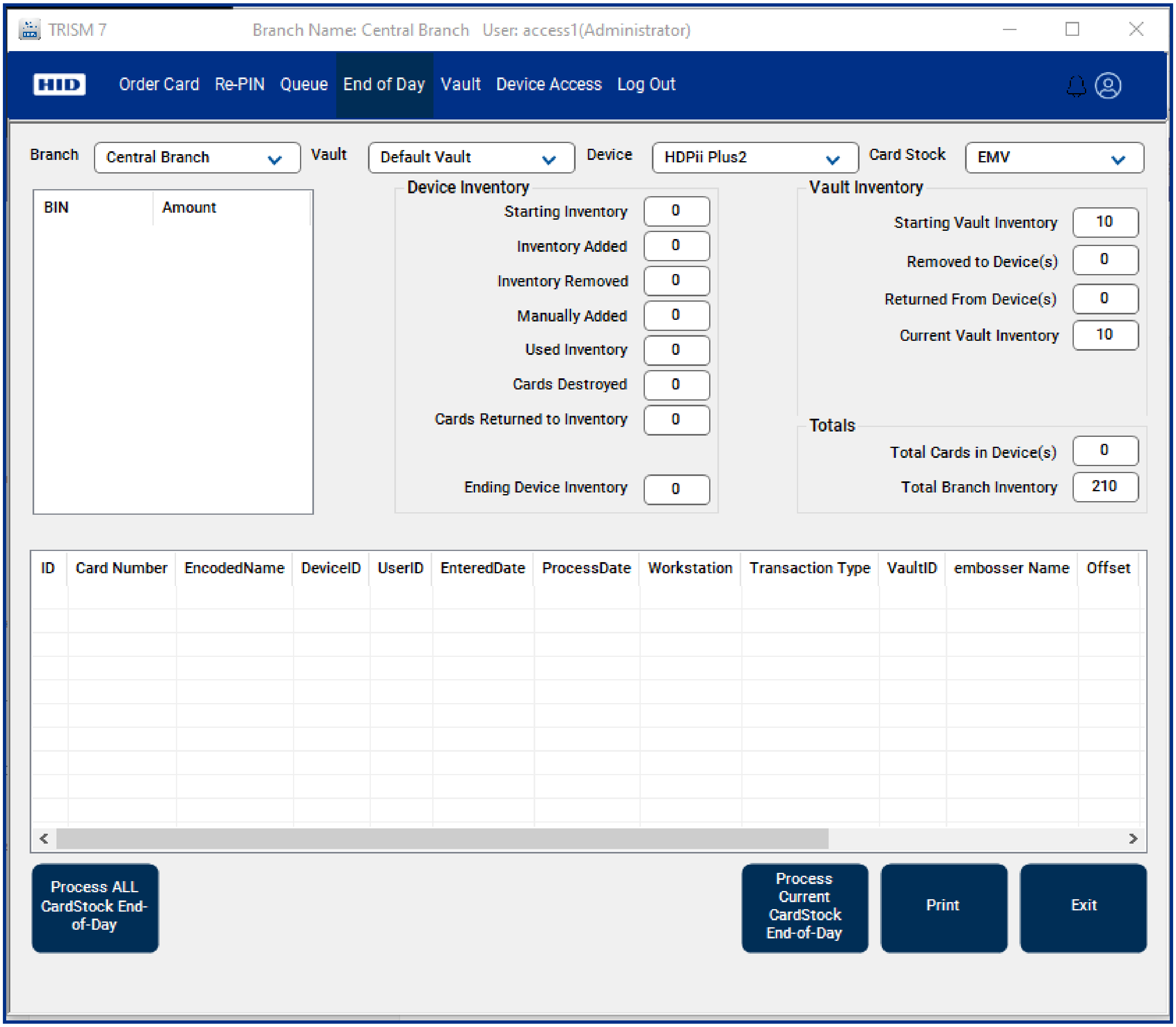
Section 05

Reports

5.1 End Of Day

On the main menu, click the **Personal icon** > **Reports** > **End Of Day**, or click End of Day.

The **End of Day** report displays all cards and inventory changes made that day in selected devices and vaults. The table with the headers **BIN** and **Amount** show the quantity of each card type issued that day.



Field	Description
Device Inventory	
Starting Inventory	Quantity of cards in device at the beginning of the day (only greater than zero if cards are not removed at end of previous day).
Inventory Added	Quantity of cards added to device throughout the day.
Inventory Removed	Total quantity of cards removed from vault device.
Manually Added	Quantity of cards inserted manually into the printer using the exception feed slot.
Used Inventory	Quantity of cards not destroyed or returned to inventory; successfully printed cards issued to customers.
Cards Destroyed	Quantity of cards destroyed in the Spoil Card menu.
Cards Returned to Inventory	Quantity of cards returned in the Spoil Card menu.
Ending Device Inventory	Sum of the above quantities.
Vault Inventory	
Starting Vault Inventory	Quantity of cards in vault since last processed end-of-day.
Removed to Device(s)	Quantity of cards added to devices in Device Access.
Returned from Device(s)	Quantity of cards removed from devices via Device Access and returned to vault.
Current Vault Inventory	Quantity of cards in vault.
Total Cards in Device(s)	Quantity of cards in all devices.
Total Branch Inventory	Sum of cards in devices and vault(s).

If the Ending Device Inventory and/or Total Cards in Device(s) is greater or less than zero, the following window is displayed:

- Click **Yes** to process End-of-Day.
- Click **No** to return to the End-of-Day Report screen.

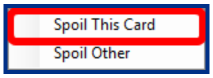
5.1.1 Tips for balancing end of day reports

- Balance the end-of-day report every day. Never start the day with a device inventory greater or less than zero.
- Do not wait until the end of the business day to spoil cards. Spoil them as soon as they are incorrectly printed. Otherwise, it is easy to lose track of misprinted cards and causes difficulty balancing the end of day report.
- Use the Device Access function to account for added or removed cards even if the device is unlocked manually. Not using Device Access is a guaranteed way to end the day with a negative device inventory.
- The queue should be empty at the end of day. All cards in the queue should either be printed and verified or deleted.

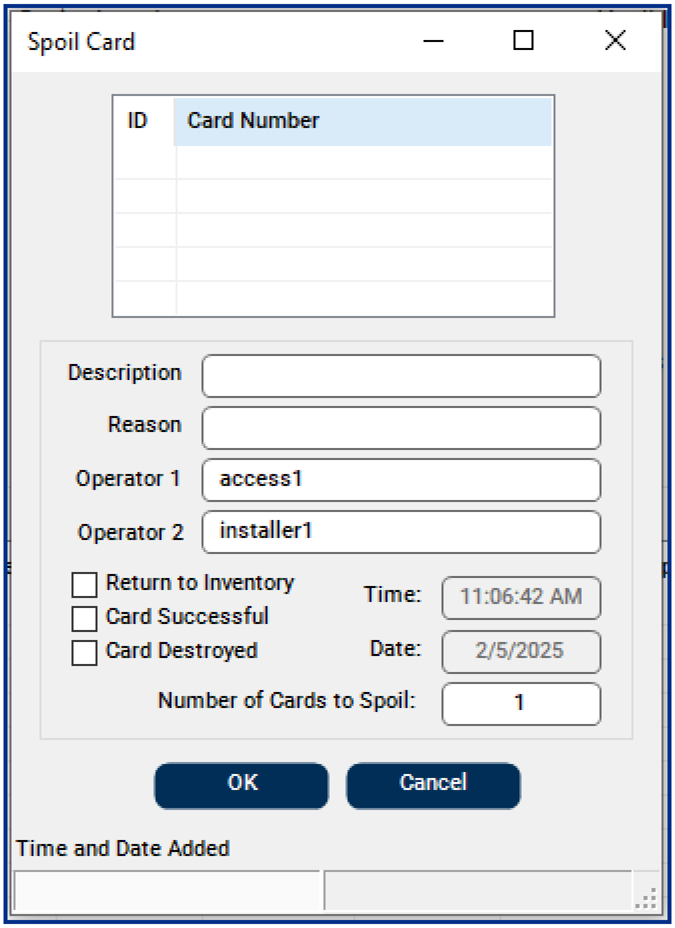
5.1.2 Spoil cards

A misprinted card that cannot be issued is considered "spoiled." A spoiled card is highlighted in red.

1. Right-click a card in the **End of Day** report:



2. Select **Spoil This Card** to display the following window:



3. Enter a description of the spoiled card and the reason for spoilage. Select from the following options:

Field	Description
Return to Inventory	The card was ejected clean/unencoded and can be used again. Will add 1 back into Vault Inventory.
Card Successful	The card did print or a card was accidentally printed. Subtracts 1 from Vault Inventory.
Card Destroyed	The card was damaged during printing or was destroyed after printing. Subtracts 1 from Vault Inventory.

4. Click **OK**.

5.1.3 Spoil other

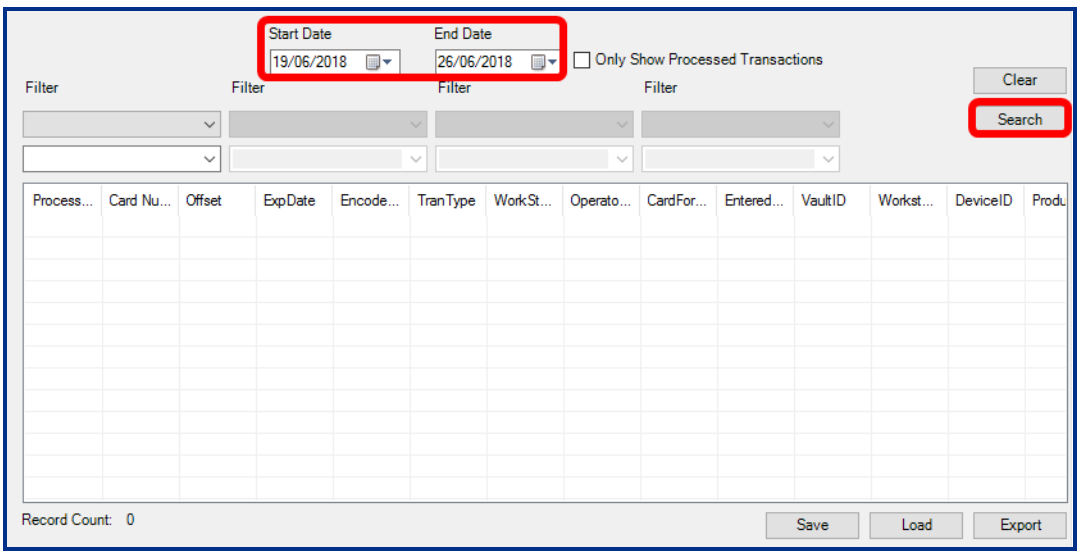
If inventory needs adjusting without the need to spoil a printed card, this can be achieved through selecting **Spoil Other**. Right-click anywhere in the field where printed cards are displayed and select **Spoil Other**. The same process as a regular spoil applies. Additionally, multiple cards can be spoiled at once.

- To add a card back to the Vault Inventory, select **Return to Inventory**.
- To subtract a card from the Vault Inventory, select **Card Destroyed**.
- If spoiling multiple cards at once enter the quantity in the **Number of Cards to Spoil** field.

5.2 Management

Reports with user-specified information can be created in the **Management** tab.

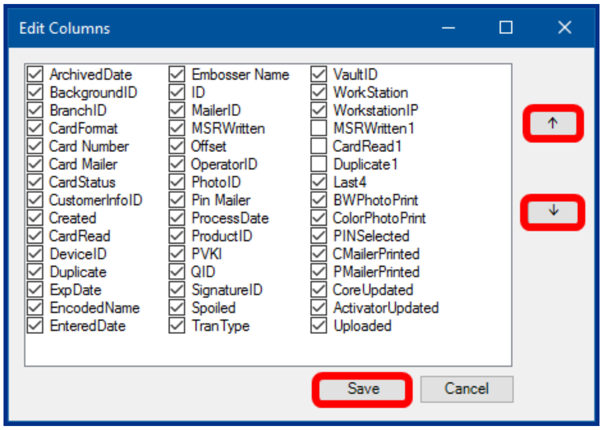
1. On the main menu, click the **Personal icon** > **Reports** > **Management**.
2. Select the **Start Date** and **End Date** to specify a range of cards to display. The **Start Date** should be set one day prior to the date of card verification.



3. Click **Search** to populate the list of cards.

5.2.1 Create a customized report

1. Select which columns are printed by right-clicking anywhere in the card information field and then selecting **Add/Remove Columns**.
2. Select or clear the boxes to display columns. To change the column order, select a column name and click the up or down arrows.



3. Click **Save** to apply your changes, then click **Search** to apply them.
   If this does not change the default column view, select a date range in which transactions were processed.

5.2.2 Filter columns

1. Select a column field from the first **Filter** drop-down menu.
2. Enter the filter criterion in the field below (only one criterion per filter). Filters must match the intended field name exactly.

   > **Note:** Only one filter field is initially enabled. The following filters are enabled once preceding filters are designated.

3. Click **Search** to apply the specified filters.

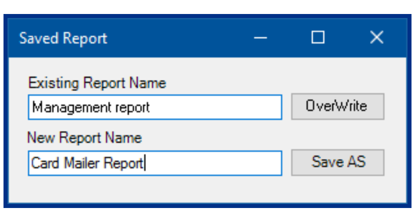
5.2.3 View card details

Right-click a card and select **Details**.

5.2.4 Save a customized report

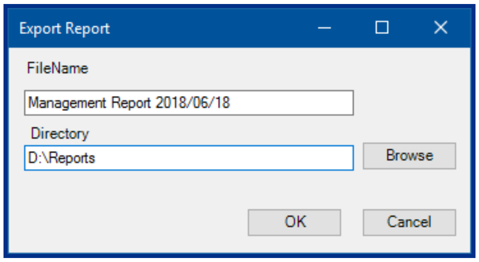
Click **Save**.

- To save over an existing saved report, click **OverWrite**.
- To save a new report, click **Save AS**.



5.2.5 Export a report to Excel

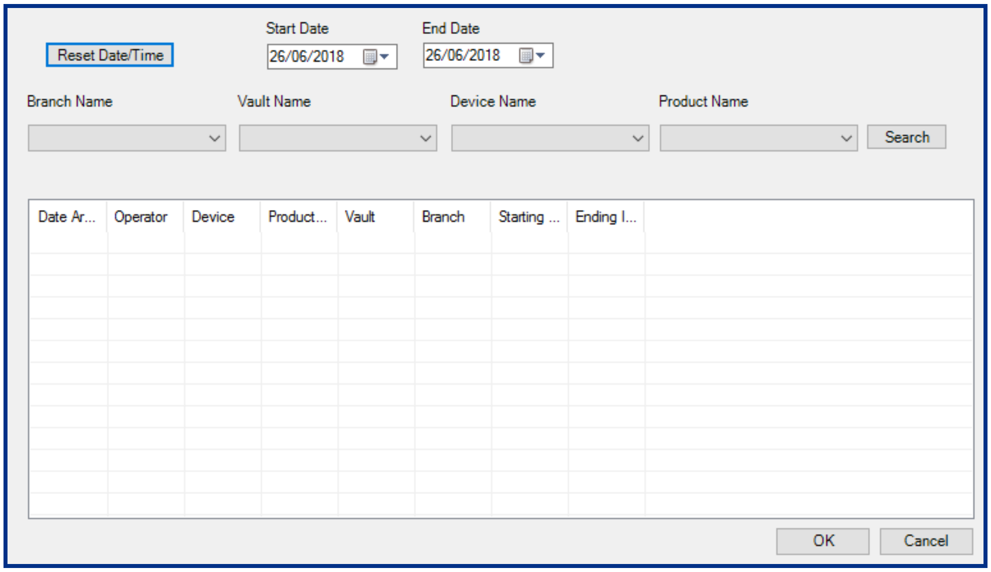
1. Click **Export**.
2. Enter a filename in the **FileName** field, then click **Browse** to select a location to save the file.
3. Click **OK**.



5.3 Historical Card Balancing

Reports summarizing cards printed per branch, device, card stock, and/or operator can be printed.

1. On the main menu, click **Reports** > **Historical Card Balancing**.



2. Select a date range, branch, vault, device, and/or product in the drop-down menus to narrow the search.
3. Click **Search** to generate the historical report.

Reset Date/Time changes the start and end dates to the current date.

5.4 Device Access

On the main menu, click the **Personal icon** > **Reports** > **Device Access** to display a list of all device access activity for a specified printer/embosser within a specified date range.

5.5 Spoiled Card

On the main menu, click the **Personal icon** > **Reports** > **Spoiled Card** to create a report of all spoiled cards for a specified branch within a specified date range.

5.6 Branch Activity

On the main menu, click the **Personal icon** > **Reports** > **Branch Activity** to create a report of all cards printed at the branch in which the workstation creating the report is located.

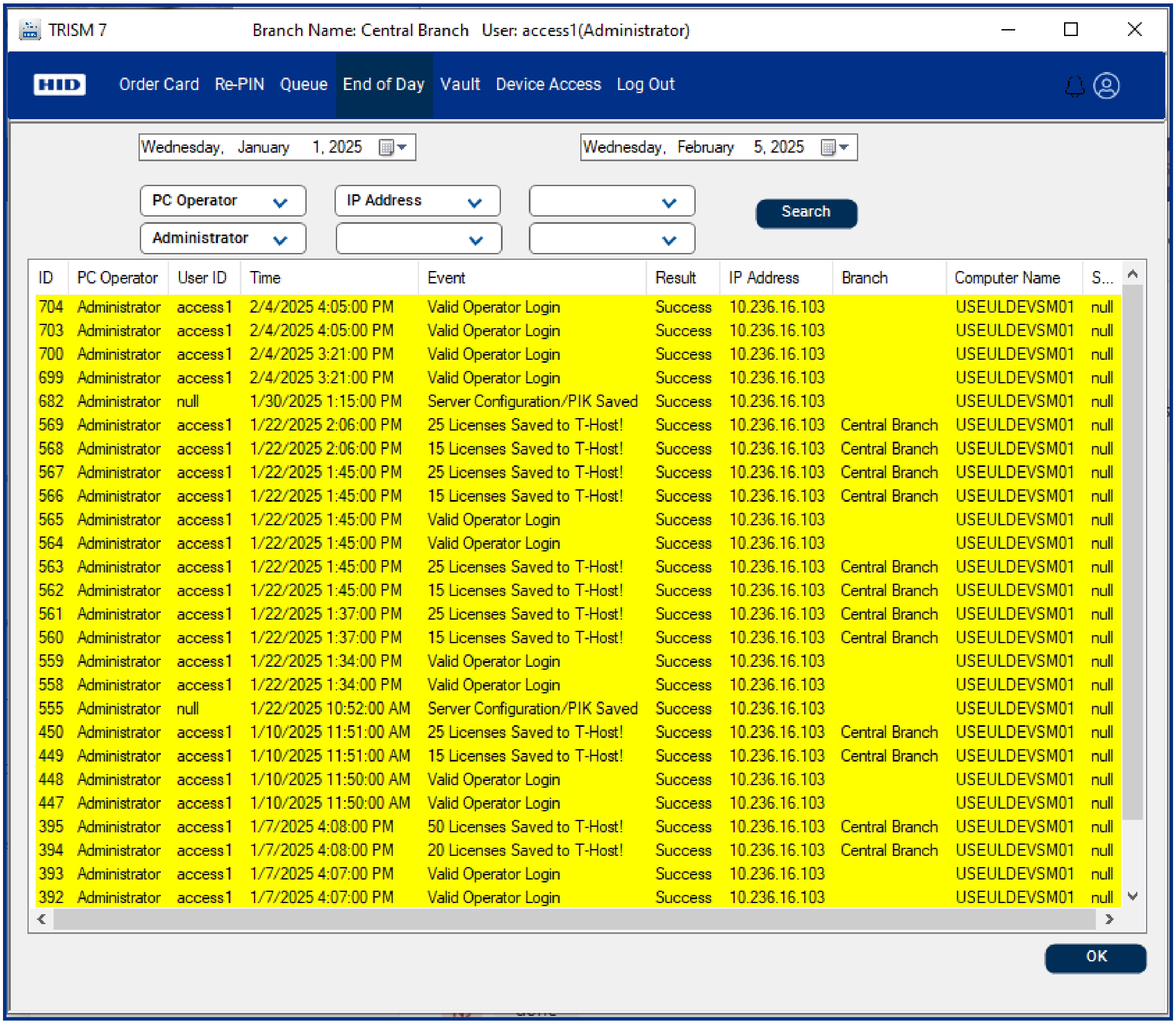
5.7 Device Error

On the main menu, click the **Personal icon** > **Reports** > **Device Error** to create a report of all device errors for a specified printer within a specified date range.

5.8 Non-Financial

Displays TRISM activity per PC Operator, User ID, TRISM ID, Event, Result, IP Address, Branch, or Computer Name.

1. On the main menu, click the **Personal icon** > **Reports** > **Non-Financial**.
2. Select a field in the top row of drop-down menus, then select or manually enter search criteria in the drop-down menu below it.
3. Click **Search** to display results.



ID	PC Operator	User ID	Time	Event	Result	IP Address	Branch	Computer Name	S...
704	Administrator	access1	2/4/2025 4:05:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
703	Administrator	access1	2/4/2025 4:05:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
700	Administrator	access1	2/4/2025 3:21:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
699	Administrator	access1	2/4/2025 3:21:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
682	Administrator	null	1/30/2025 1:15:00 PM	Server Configuration/PIK Saved	Success	10.236.16.103		USEULDEVSM01	null
569	Administrator	access1	1/22/2025 2:06:00 PM	25 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
568	Administrator	access1	1/22/2025 2:06:00 PM	15 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
567	Administrator	access1	1/22/2025 1:45:00 PM	25 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
566	Administrator	access1	1/22/2025 1:45:00 PM	15 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
565	Administrator	access1	1/22/2025 1:45:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
564	Administrator	access1	1/22/2025 1:45:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
563	Administrator	access1	1/22/2025 1:45:00 PM	25 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
562	Administrator	access1	1/22/2025 1:45:00 PM	15 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
561	Administrator	access1	1/22/2025 1:37:00 PM	25 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
560	Administrator	access1	1/22/2025 1:37:00 PM	15 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
559	Administrator	access1	1/22/2025 1:34:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
558	Administrator	access1	1/22/2025 1:34:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
555	Administrator	null	1/22/2025 10:52:00 AM	Server Configuration/PIK Saved	Success	10.236.16.103		USEULDEVSM01	null
450	Administrator	access1	1/10/2025 11:51:00 AM	25 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
449	Administrator	access1	1/10/2025 11:51:00 AM	15 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
448	Administrator	access1	1/10/2025 11:50:00 AM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
447	Administrator	access1	1/10/2025 11:50:00 AM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
395	Administrator	access1	1/7/2025 4:08:00 PM	50 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
394	Administrator	access1	1/7/2025 4:08:00 PM	20 Licenses Saved to T-Host!	Success	10.236.16.103	Central Branch	USEULDEVSM01	null
393	Administrator	access1	1/7/2025 4:07:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null
392	Administrator	access1	1/7/2025 4:07:00 PM	Valid Operator Login	Success	10.236.16.103		USEULDEVSM01	null

5.9 Background

On the main menu, click the **Personal icon** > **Reports** > **Background** to display a list of all background images printed within a specified date range.

5.10 Remove Cardholder Data

Customers may wish to have their data removed from the system, especially in cases of General Data Protection Regulation (GDPR). To remove data from the system, use the Customer Information Section from the database.

To enable this feature, you must access the permissions and select the **Customer Removal** check box. Once this feature is enabled, you can access the **Customer Removal** screen to remove all records or specific records from the database.

1. Select the **Personal icon** > **Reports** > **Remove Cardholder Data**.
2. On the **Customer Removal** screen you can search all records or a specific record.
   - To search all records, leave the **Name** field blank and click **Search.**
   - To search for a specific name, enter the first, middle, and last name in the **Name** field and click **Search**.

   Any information that matches the search criteria is displayed.
3. Select the records you wish to remove and click **Delete**. The user information is removed, and the screen is refreshed with a new list of applicable search criteria.

> **Important: The record of the transaction remains in the database but all information pertaining to the customer is removed. This includes photo information.**

Section 06

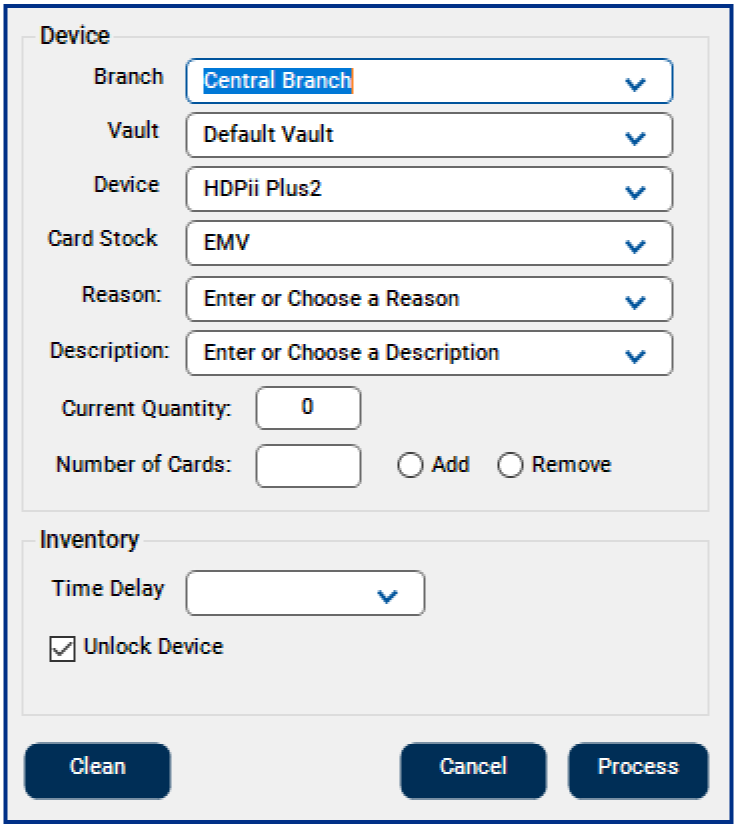
Inventory

6.1 Device Access

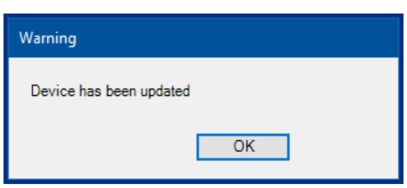
6.1.1 Add/remove cards

Each time a printer or embosser is opened, it must be accounted for in the Device Inventory.

1. On the main menu, click the **Personal icon** > **Inventory** > **Device Access**, or click Device Access.



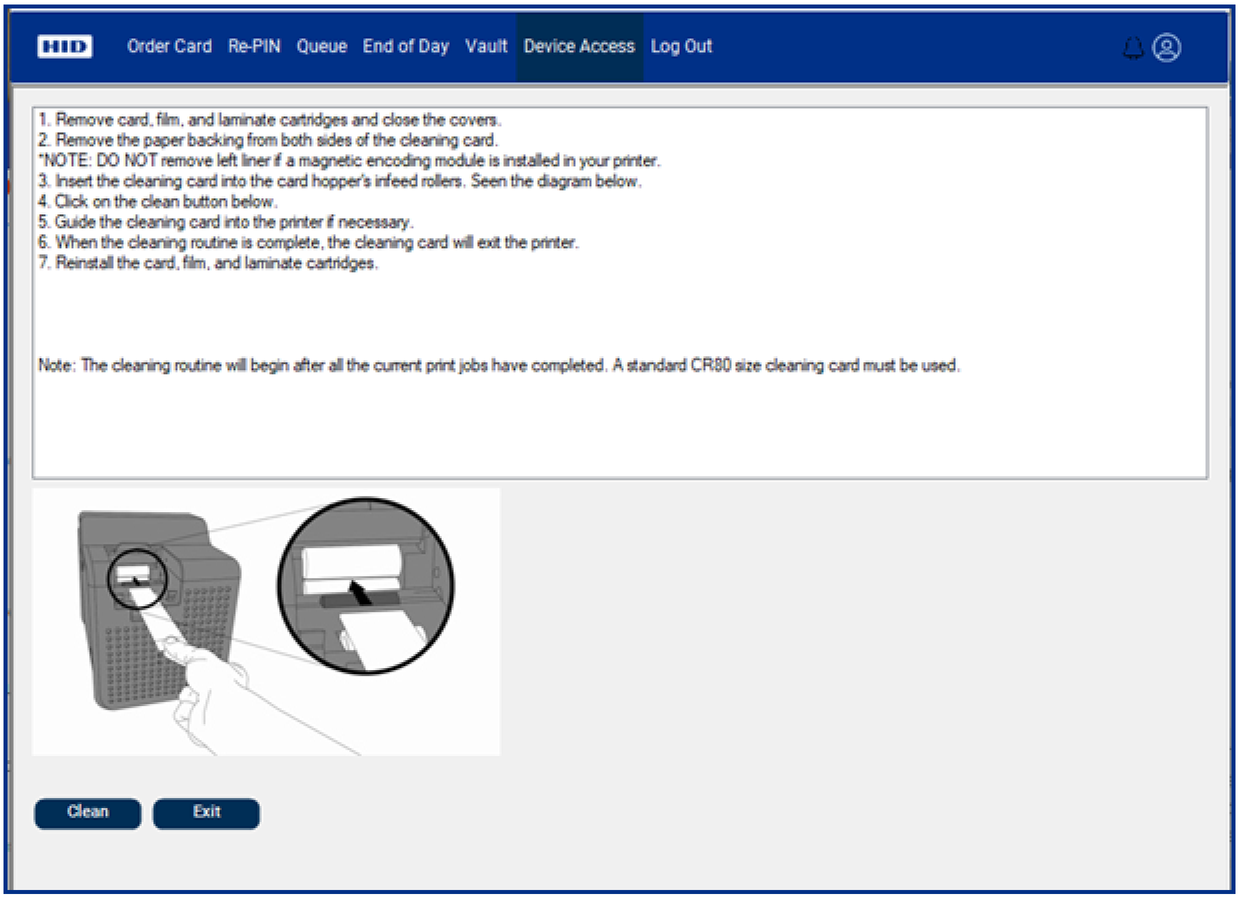
2. The **Branch**, **Vault**, and **Device** defaults to whatever values were assigned to the branch. Select other values if necessary.
3. If adding or removing cards, select **Card Stock**.
4. Select **Add** or **Remove**. Selecting **Remove** automatically generates a reason, description, and number of cards.
5. Enter a **Reason** for opening and a **Description** of the actions performed or choose a reason and description from the drop-down menus.
6. Enter the **Number of Cards** to add or remove, if any.
7. Select a time delay for unlocking the device. Longer delays should be used if the device is not near the workstation.
8. Click **Process**.



6.2 Printer cleaning

1. On the main menu, click the **Personal icon** > **Inventory** > **Device Access**, or click Device Access.
2. On the **Device Access** screen, click **Clean**.
3. Follow the instructions provided in the text box at the top of the **Printer Cleaning** screen.

> **Note:** The cleaning instructions are specific to each printer type.



4. Repeat as many times as necessary to completely clean the printer.
5. When finished, click **Exit**.

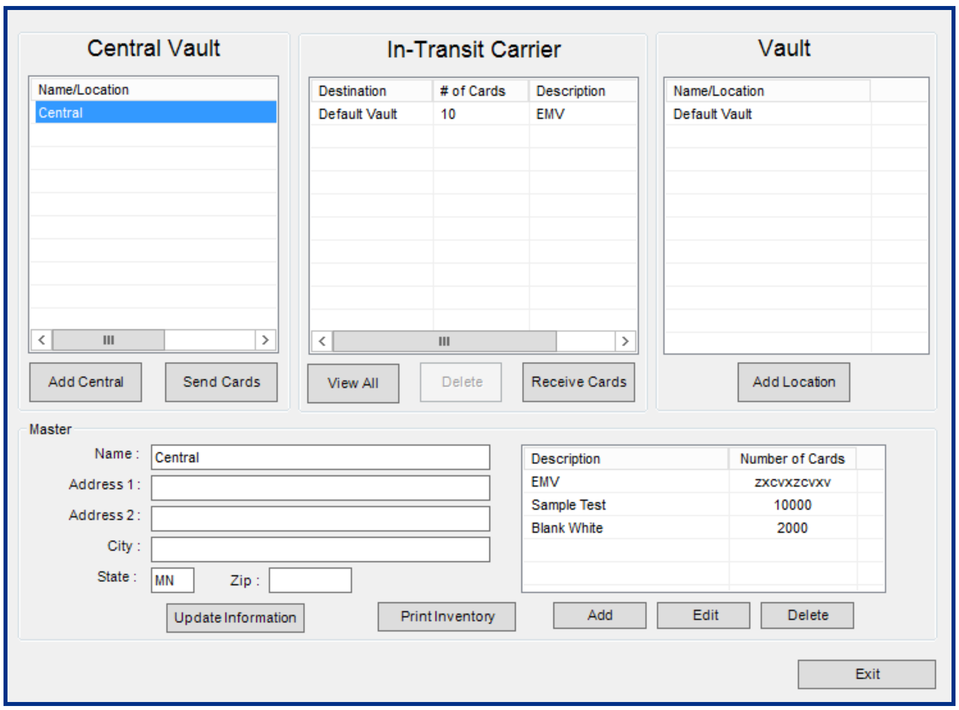
6.3 Vault Inventory

Vault Inventory shows the number of cards in each vault (central or branch). It also allows you to track shipments of cards between the central vault and a branch vault. A central vault is not required, but at least one branch vault is required. That vault can be shared by multiple branches if necessary (Central Issuance).

6.3.1 Add a vault

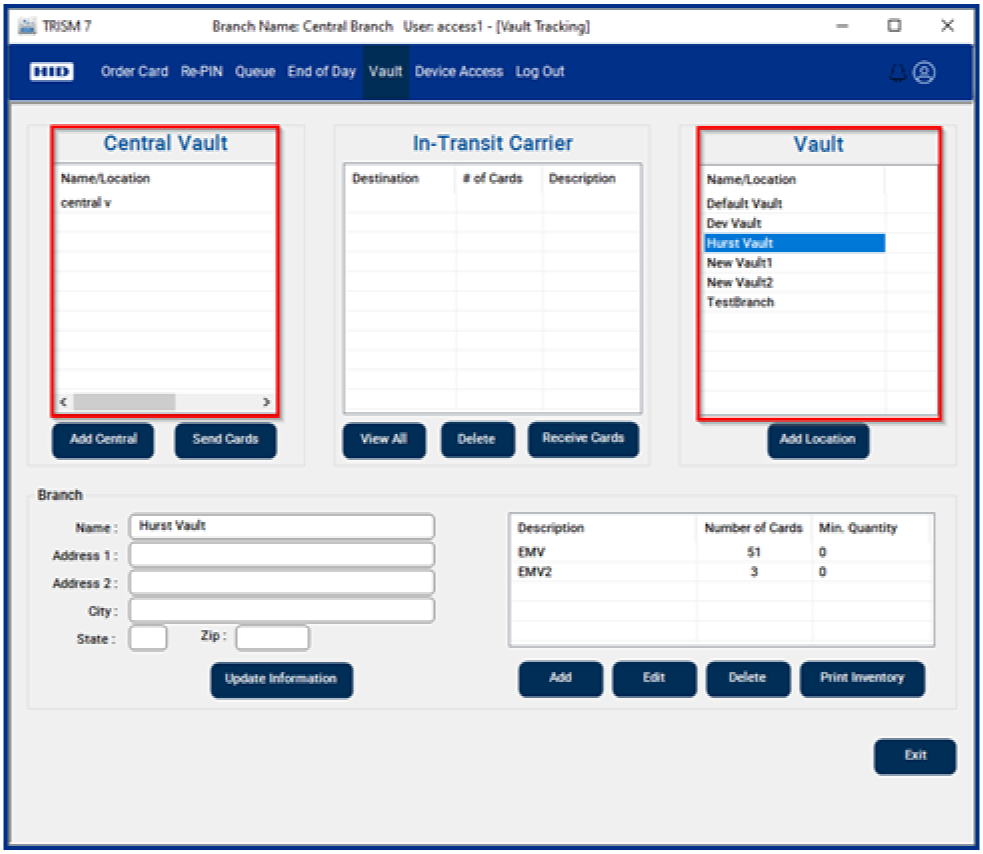
1. On the main menu, click the **Personal icon** > **Inventory** > **Vault Access**, or click 

.
2. Click **Add Central** in the Central Vault display or **Add Location** in the Vault display.
3. Enter the required name and address fields (optional).
4. Click **OK**.

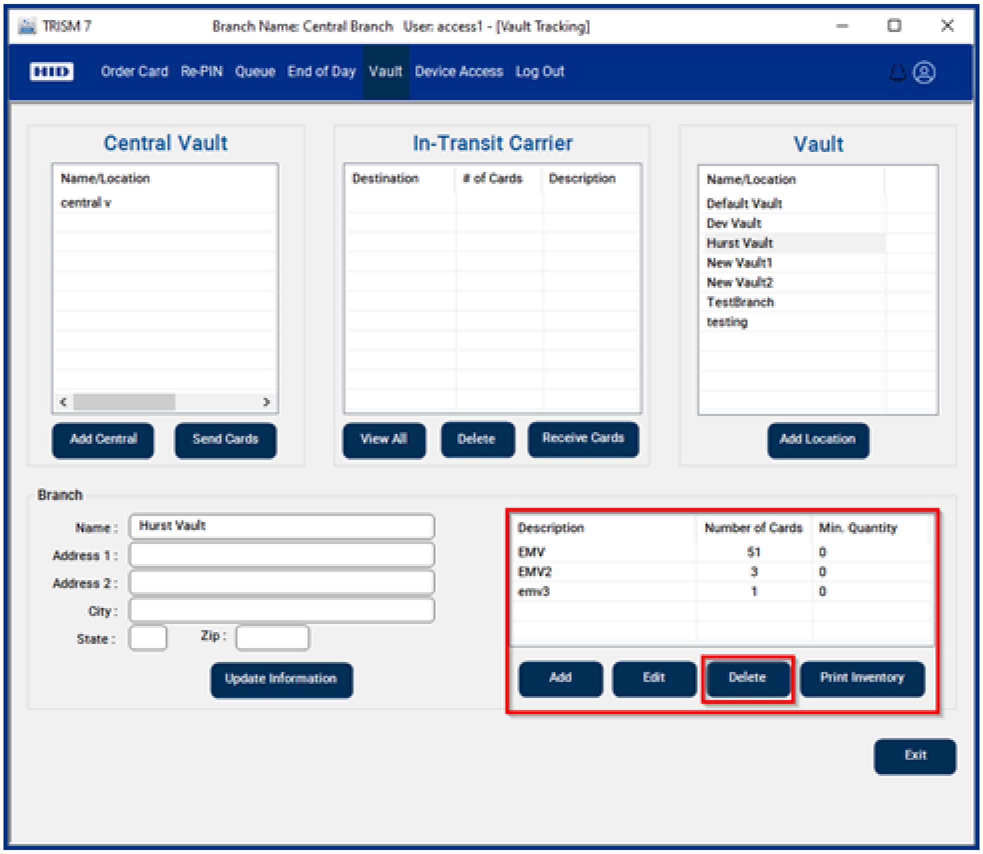


6.3.2 Delete a vault

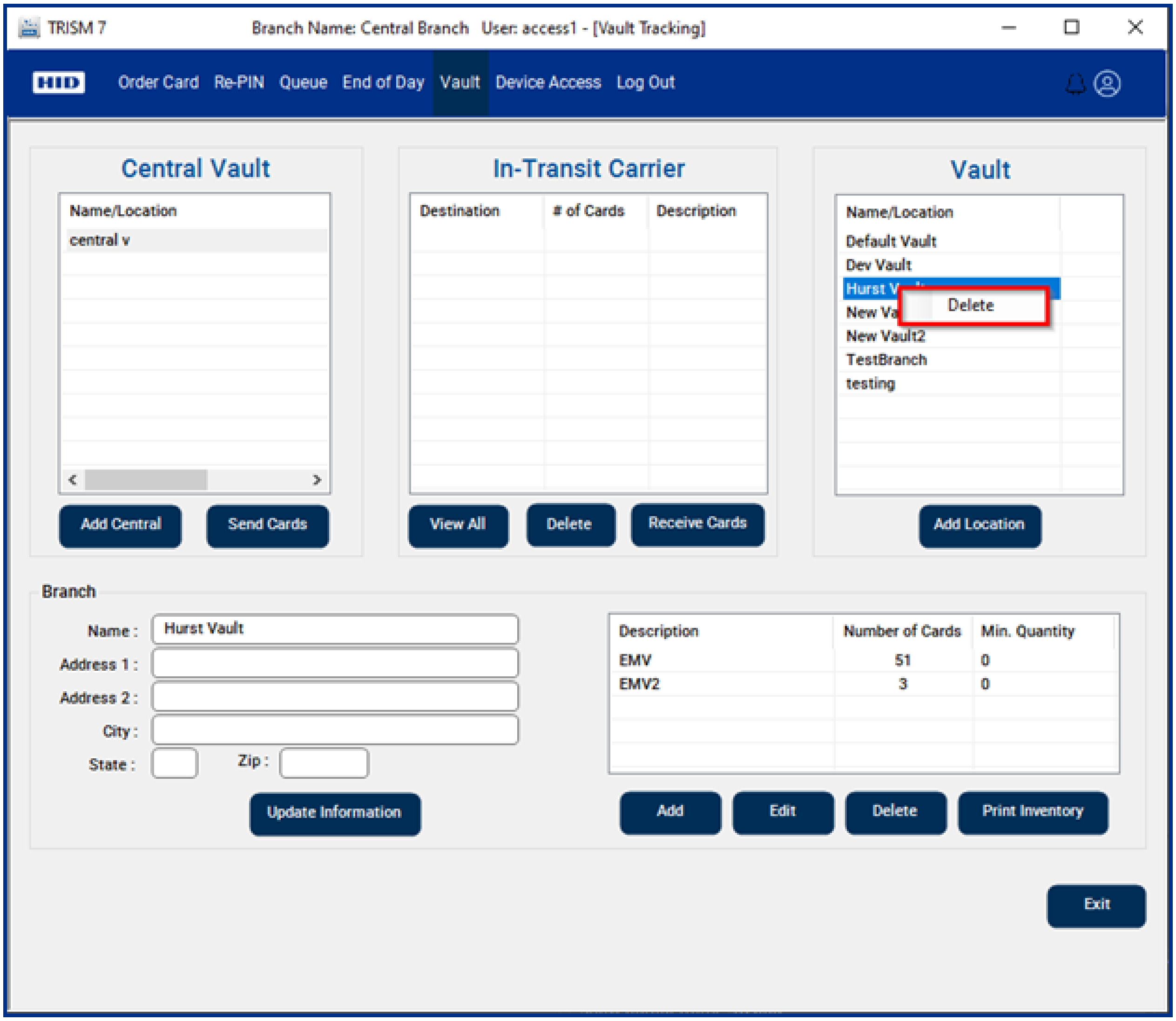
1. Detach the vault to be deleted from any branches and printers.
2. From the quick launch toolbar, select **Vault** and log in with Dual Control when prompted.
3. Select the central Vault/Vault to be deleted.



4. Select each cardstock entry and click Delete.



5. Right-click on the vault to be deleted and click **Delete**.

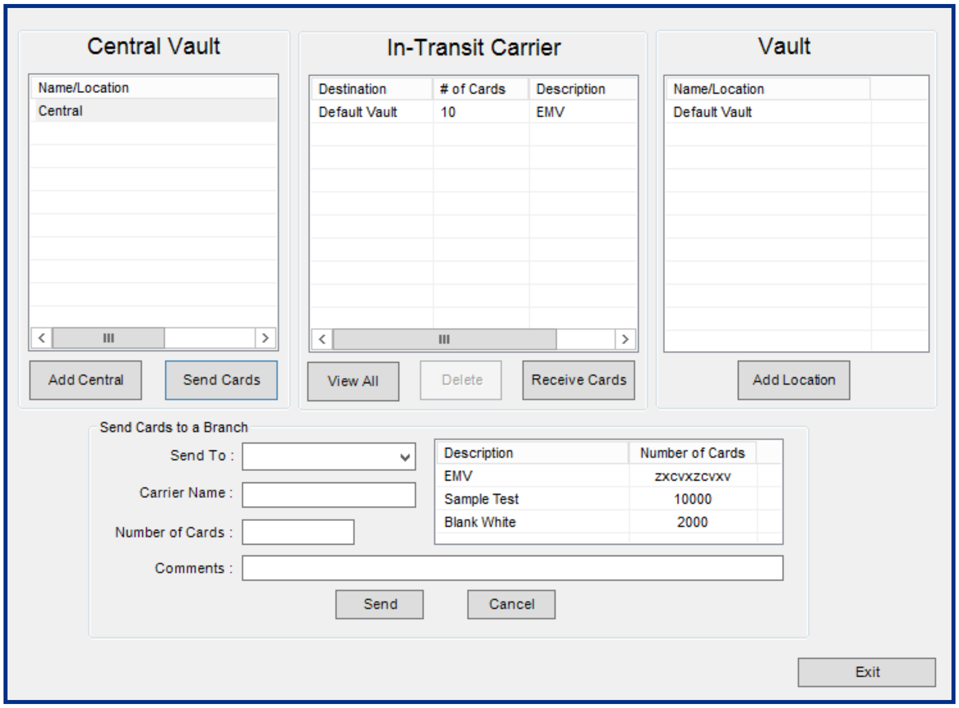


The vault is removed from the list.

6.3.3 Transfer cards - send cards

1. Select a central vault, then click **Send Cards**.
2. Select the recipient branch's vault from the **Send To** drop-down menu.
3. Enter the **Carrier Name**, **Number of Cards** to send, and any additional comments.
4. Select the type of cards stock to send.
5. Click **Send**.

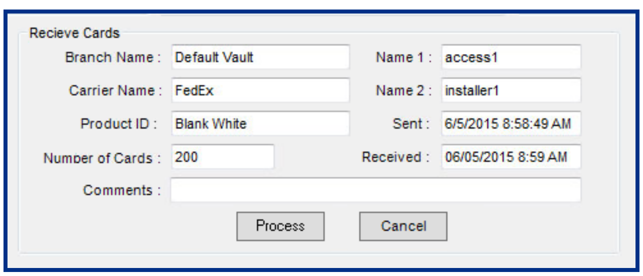
6. The shipment order is displayed under the **In-Transit Carrier** menu.



6.3.4 Transfer cards - receive cards

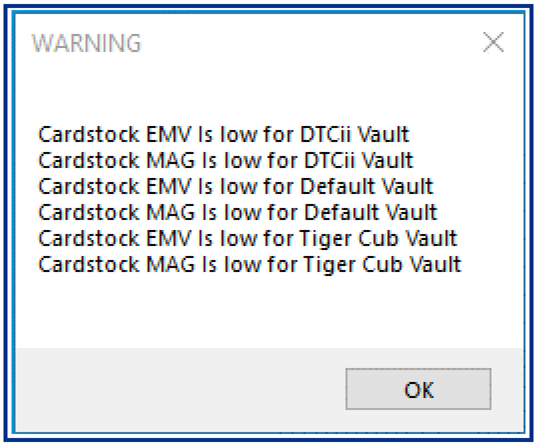
1. Select the received order under the **In-Transit Carrier** menu.
2. Click **Receive Cards**, then **Process**.

   The order is removed from the In-Transit Carrier menu and the cards are added to the vault inventory.



6.3.5 Low inventory alerts

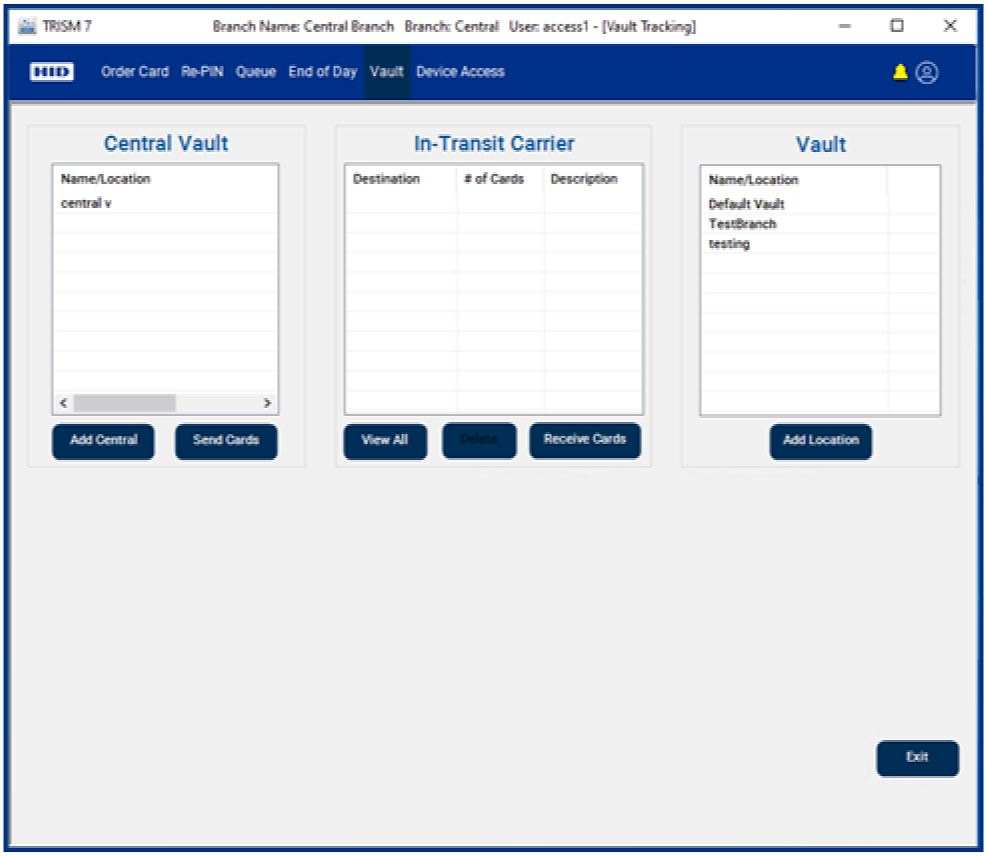
If TRISM is used for tracking inventory, the TRISM client can be set up for low inventory warnings. These warnings are displayed upon login. Low inventory alerts notify you when the branch vault is running low on card stock. You can set the inventory levels for each individual vault location. Then, in the User Template, you can enable the alerts. When the low inventory levels are set up and enabled, the following warning is displayed:



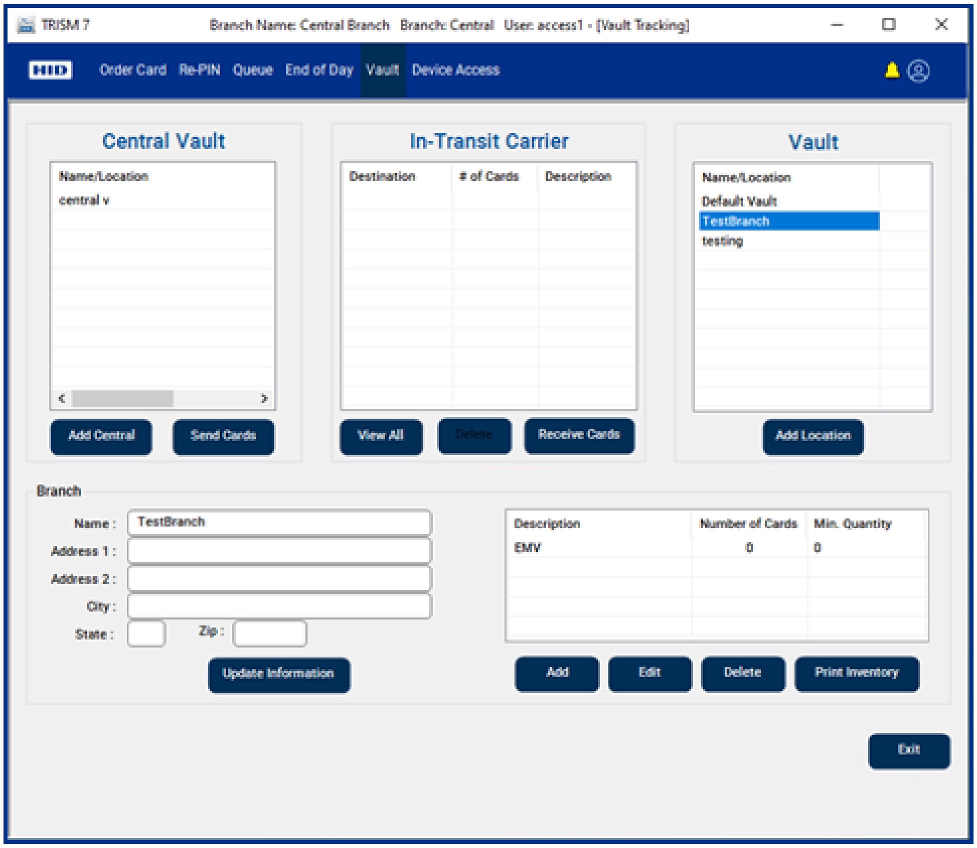
Note: To set up the low inventory alerts you must have a Dual Control user ready with the same permissions.

1. Log in to TRISM with a user account that has the necessary permissions to access and edit vaults.
2. On the main menu, select Vault and log in with a Dual Control user when prompted.

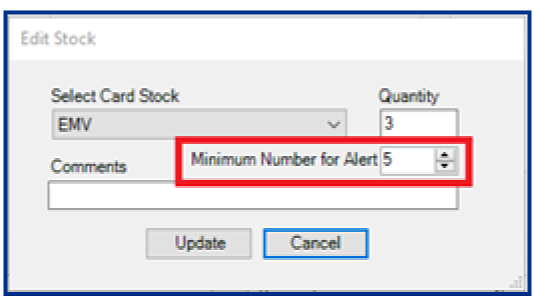
3. The Vault information is displayed. Select a Vault location.



4. The Branch information is displayed and the current minimum number of cards remaining before the alert is enabled is displayed in the **Min. Quantity** column.



5. To edit the minimum number of cards remaining before the alert, double-click the card stock name or select the card stock name and click **Edit**.



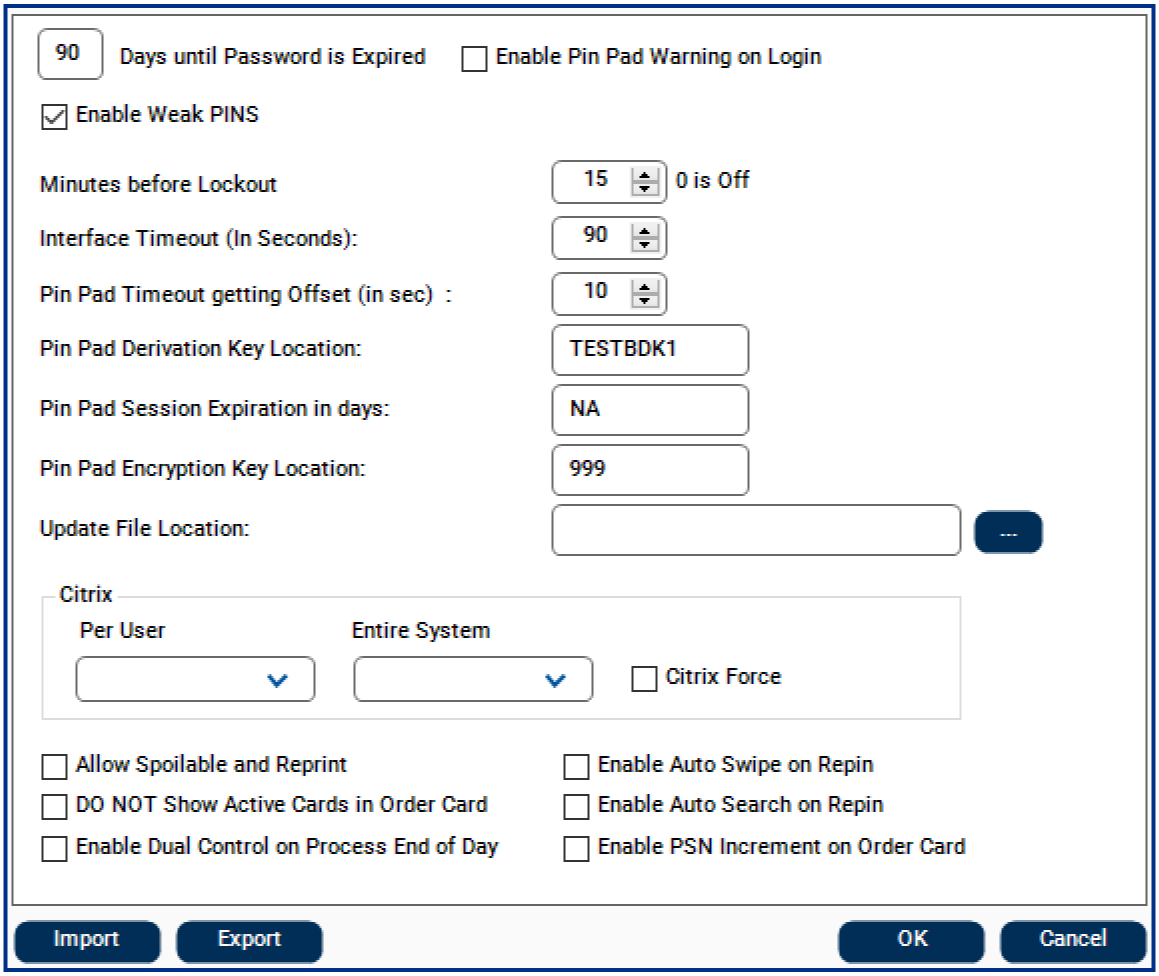
6. The Edit Stock window is displayed. Enter a number or use the up and down arrows to increase or decrease the **Minimum Number for Alert** and click **Update**.
7. Repeat these steps for each vault and card stock.

Section 07

Configure

7.1 General

On the main menu, click the **Personal icon** > **Configure.** On the side menu, click **General.**



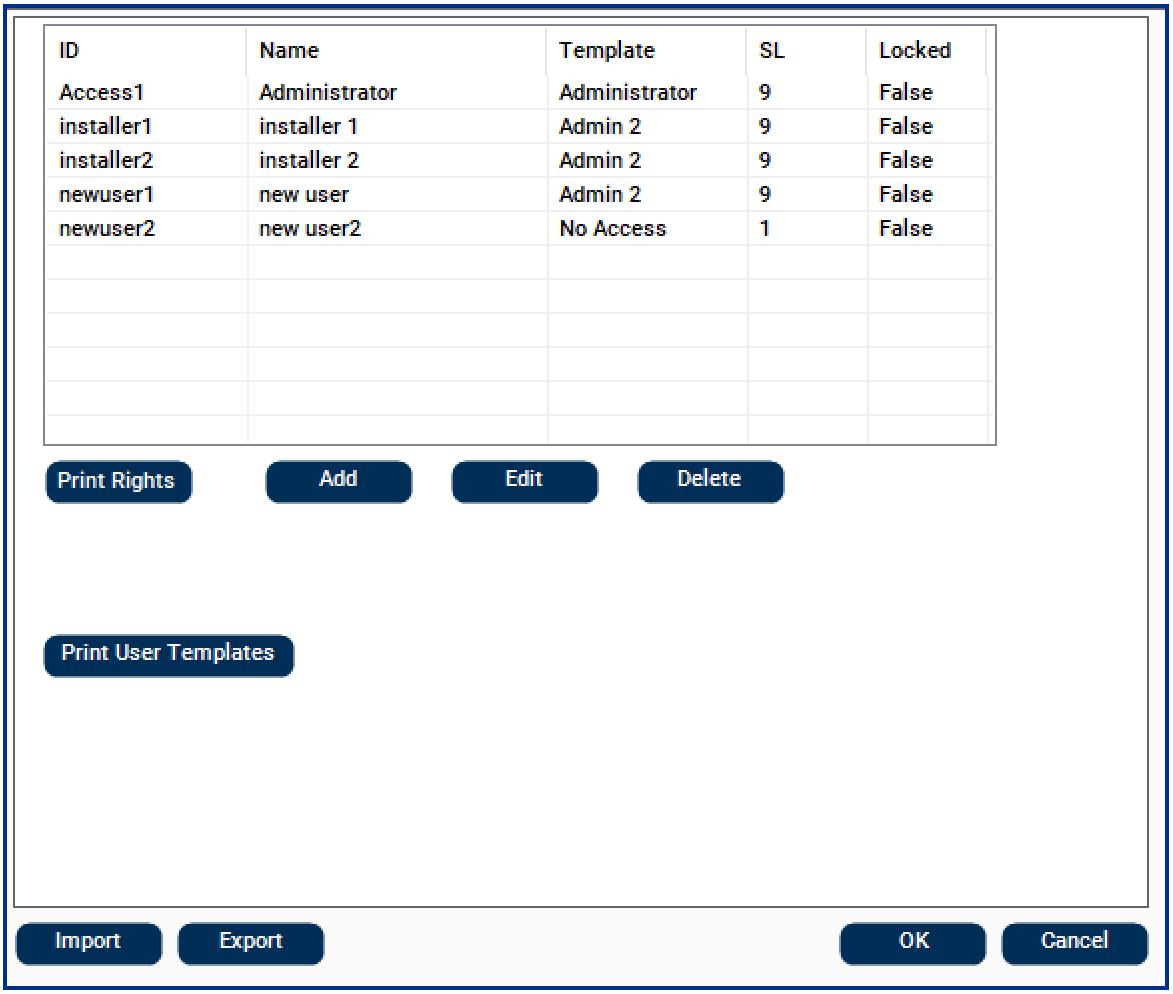
Field	Description
Days until Password is Expired	Applies only to non-Active Directory users. User passwords are valid for this number of days. Users are prompted to select a new password upon expiration.
Enable Pin pad Warning on Login	Display warning message that no PIN pad is plugged in to the computer upon TRISM login.
Enable Weak PINS	If checked, weak PINs (1111, 1234, 4321, and so on.) are allowed.
Minutes before Lockout	After the specified number of minutes, the user must re-enter login credentials to continue using TRISM. Must be same user that is currently active, otherwise TRISM must be restarted to log in as a different user.
Pin Pad Derivation Key Location	Numerical location of PIN Pad Derivation Key in HSM Manager.
Pin Pad Timeout getting Offset	After PIN is entered: if offset is not generated after the specified number of seconds, PIN pad times out.
Update File Location	Where TRISM update files are downloaded.
Citrix	**Per User**: Select port if assigned per user. **Entire System**: Select port if assigned for entire system.

Field	Description
Allow Spoilable and Reprint	When the card status is changed to Ready in the Queue, a message box asks if a card has already been printed from the specified request. If yes, another transaction is created that may be spoiled.
DO NOT Show Active Cards In Order Card	If using an interface to find customer information, only the customer's inactive or expired cards will populate in the search results.

7.2 Users

The following user configuration is not used when **Active Directory** is enabled, except for the administrative users **access1**, **installer1**, and **installer2**.

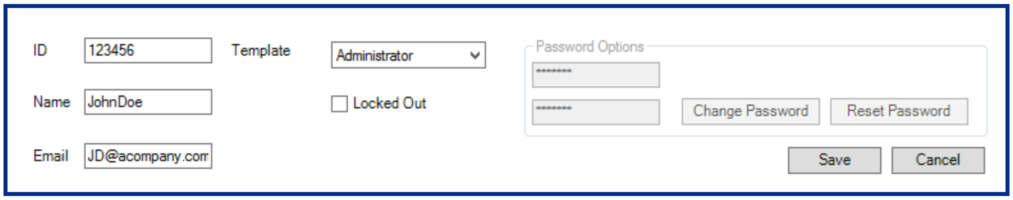
On the main menu, click the **Personal icon** > **Configure.** On the side menu, click **Users**.



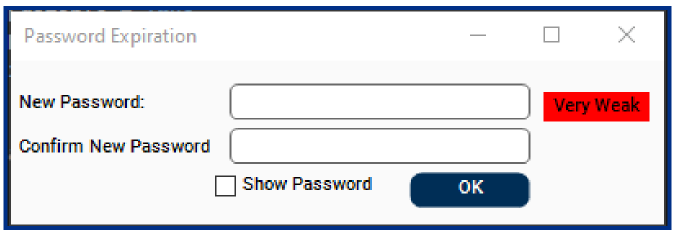
Field	Descriptions
Print Rights	Print a list of all the selected user’s template permissions.
Print User Template	Print a list of all TRISM users and their corresponding templates.

7.2.1 Add users (without active directory)

1. Click **Add**, and enter the user ID, Name, and select a template.
2. Click **Save**.



New user password selection



When you log in as a new user, you must use the default password **1234567**. When you click **Login**, a window opens and prompts you to change your password.

Enter the new password and click **OK**. You must then enter your new password in the login screen. There is a minimum requirement of 12 characters for passwords. The password strength meter indicates the strength of the password. Point values are assigned to the characters and the meter updates as characters are entered or deleted. Point values are noncumulative for each case. Point values are:

- Capital letters: 2 points
- Lowercase letters: 2 points
- Numbers: 1 point
- Special characters (!@#$%^&*): 3 points
- Length of at least 12 characters: 5 points
- Length greater than 15 characters (not cumulative with length at least 12 characters): 10 points

As point values are accumulated, the strength of the password is measured in colors on the strength meter. Point values are scored as:

- Up to 5 points: Very weak (red)
- Between 6 and 10 points: Weak (orange)
- Between 10 and 15 points: Good (yellow)
- Greater than 15 points: Very strong (green)

Alternatively, users can be entered using the Active Directory function.

7.2.2 Edit users (without active directory)

Select a user and click **Edit**. Make the desired changes and click **Save**.

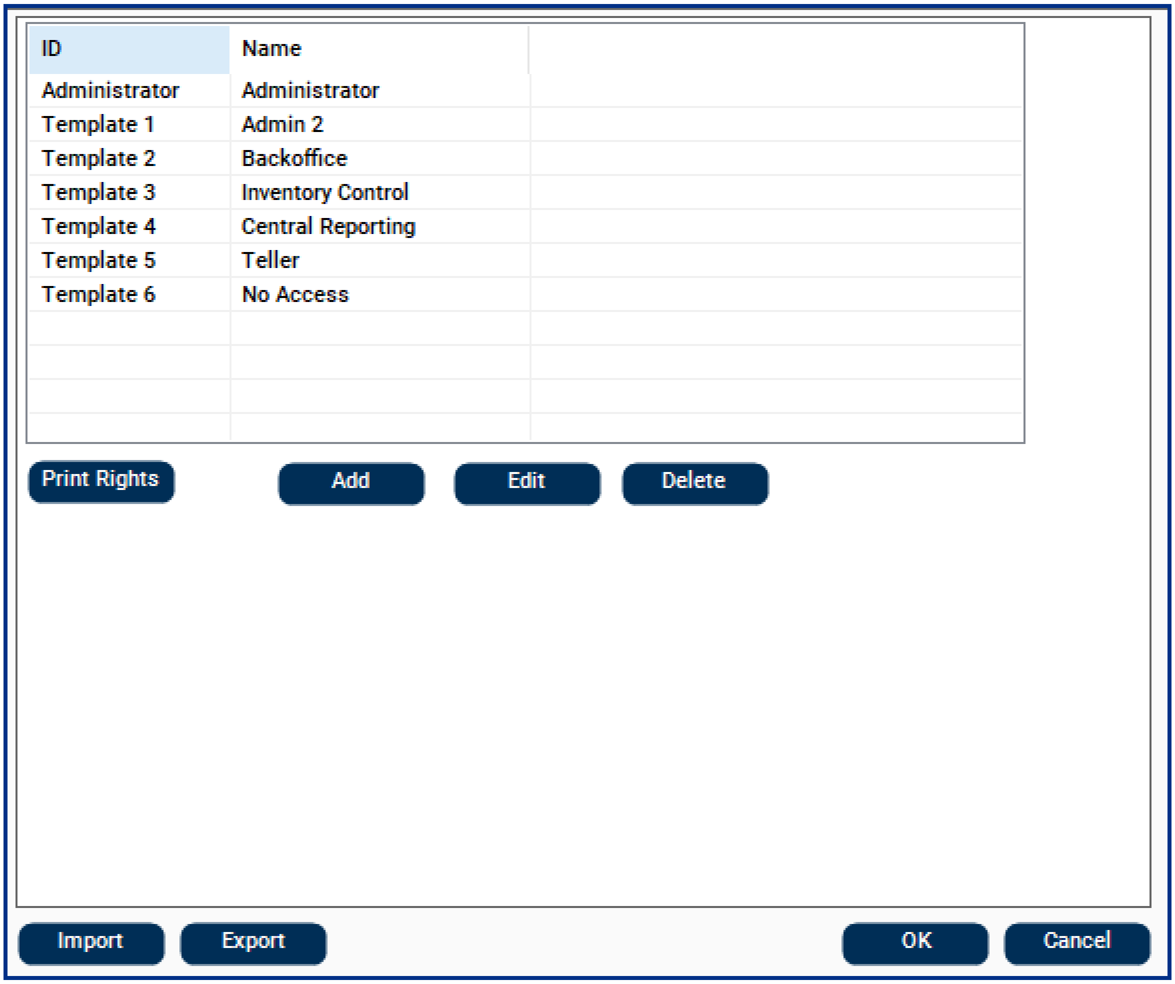
7.2.3 Delete users (without active directory)

Select a user and click **Delete**.

7.3 Templates

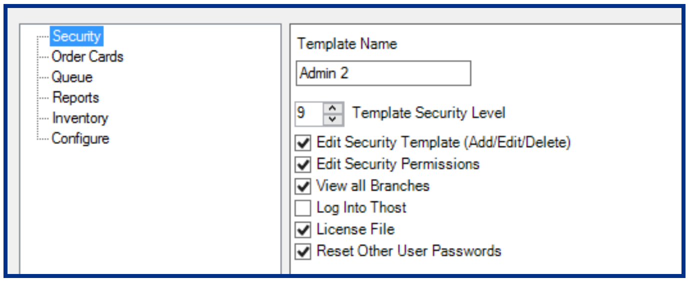
A template can be used to automatically assign a user a specific set of permissions. See section **A.4 Permission descriptions** for permission descriptions. The administrator template cannot be edited or deleted.

On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Templates**.



Field	Description
Print Rights	Print a list of all user permissions associated with the selected template.
Add	Add new templates.
Edit	Enable or disable permissions of the selected template.
Delete	Delete a User Template from the list. Only templates added by the financial institution can be deleted. **Administrator**, **Admin 2**, **Backoffice**, **Inventory Control**, **Central Reporting**, and **Teller** cannot be deleted.

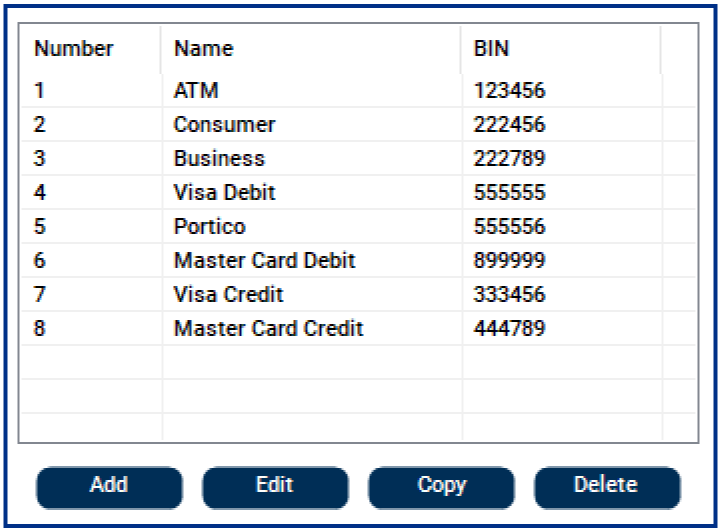
Each template, with the exception of **Administrator**, can be edited by selecting the template from the list and clicking **Edit**. Each of the options in this menu opens a list of permissions that can be enabled and disabled by clicking their respective check boxes.



7.4 Formats

Card types (for example, Mastercard, Visa, Visa EMV, and so on.) are added in the **Formats** menu. Card and mailer formats can also be edited in the **Formats** menu to customize placement of text and pictures.

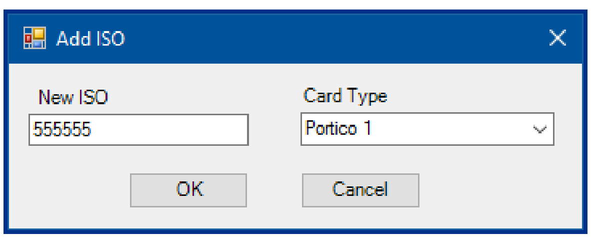
On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats**.



Number	Name	BIN
1	ATM	123456
2	Consumer	222456
3	Business	222789
4	Visa Debit	555555
5	Portico	555556
6	Master Card Debit	899999
7	Visa Credit	333456
8	Master Card Credit	444789

To add a card type:

1. Click **Add**.
2. Enter the card's **ISO** or **BIN** number, then select or manually enter the **Card Type**.
3. Click **OK**.

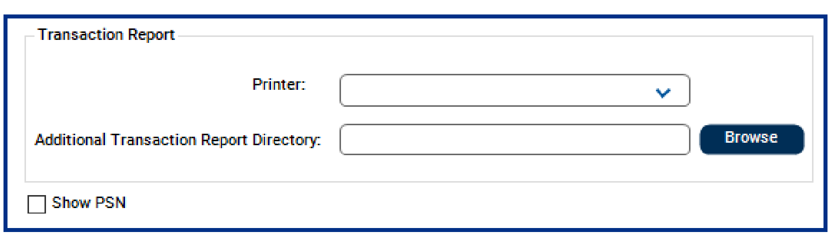


7.4.1 General Settings

To display the general settings:

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats**.
2. Select a card type in the list and click **Edit**.
3. On the side menu, click **General Settings**.

BINs cannot be added to branches until their formats are completed.



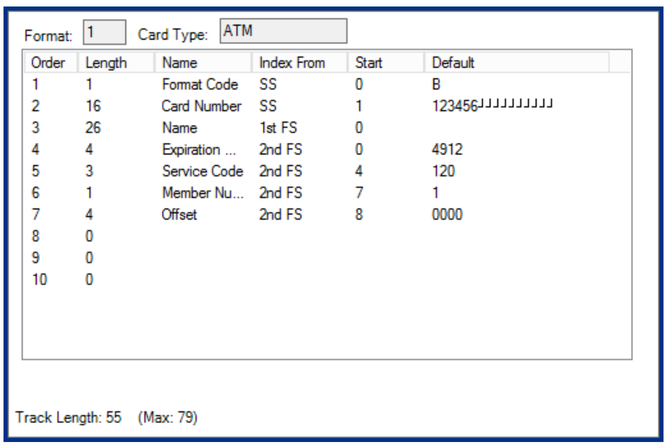
Field	Description
Print Report for Every Queued Transaction	All transactions sent to the queue print a hard-copy report to the printer selected in the drop-down menu.
Additional Transaction Report Directory	All items in the selected folder are printed in addition to transaction reports.
Show PSN	Shows the PSN control on the Order Card screen. Some financial institutions will need to manually update the PSN. Other financial institutions will wish to hide this control.

7.4.2 Encode Settings

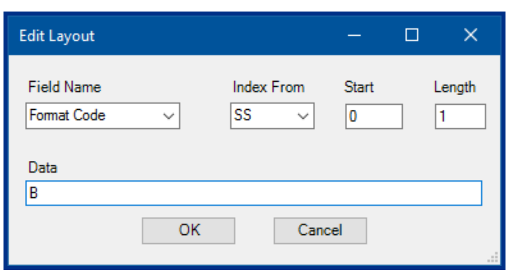
The **Encode Settings** determine the information and placement of information written to the cards' magnetic stripe. To display the encode settings:

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats.**
2. Select a card type in the list and click **Edit.**
3. On the side menu, click **Encode Settings**.

Track 1/Track 2 Layout

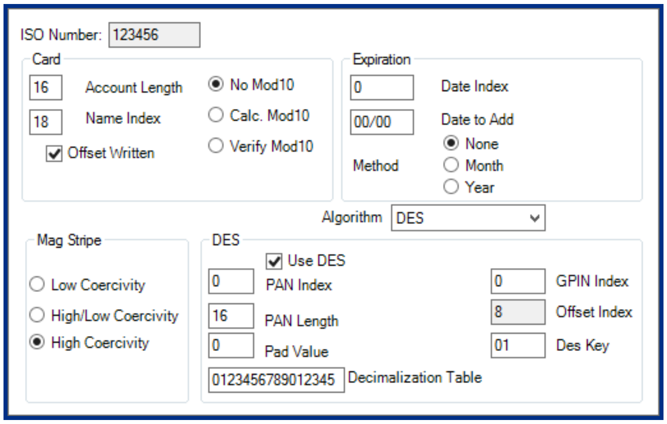


1. To edit the settings, double-click the field to be changed to display the following window:



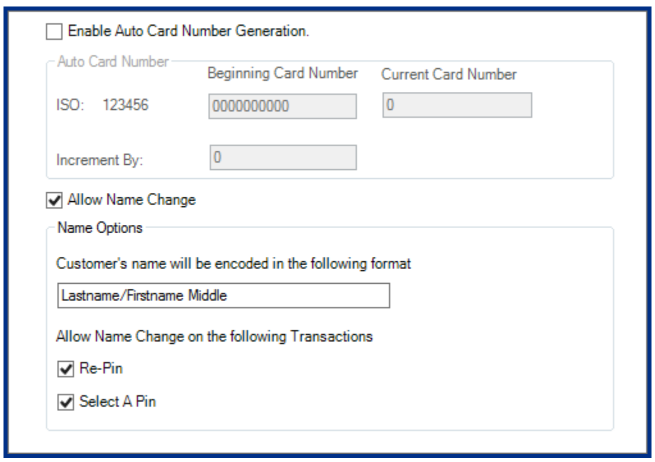
2. Click **OK** when editing is completed.

Track 1/Track 2 Parameters



Auto Card Number

Card numbers can be generated automatically by TRISM in the **Auto Card Number** menu. Check the **Enable Auto Card Number Generation** box to edit card number settings.



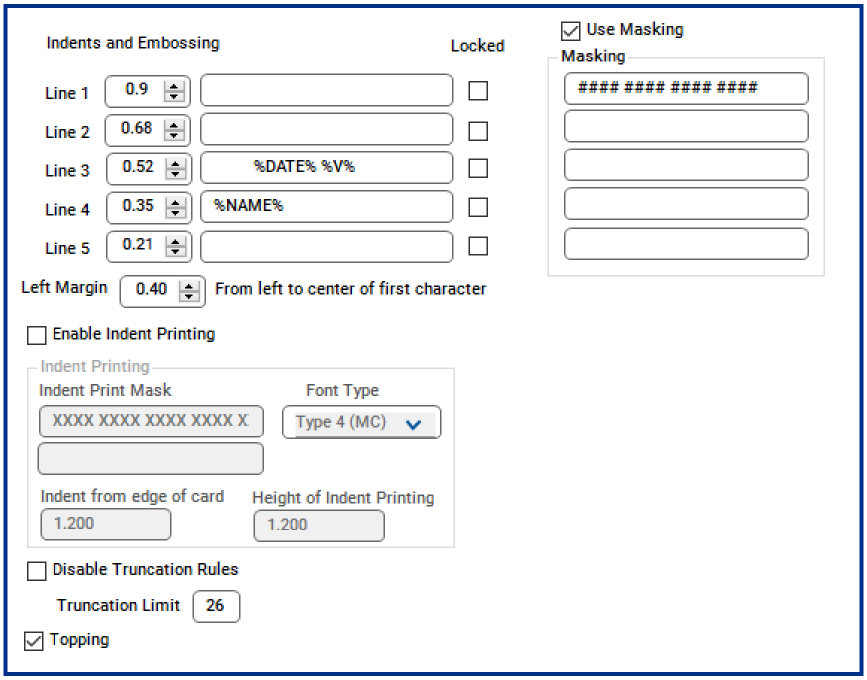
Field	Description
Beginning Card Number	First card number used.
Current Card Number	Last card number printed.
Increment By	Determines by what increment card numbers increase.
Allow Name Change on the following Transactions	Allows modification to an existing customer's name.

7.4.3 Emboss Settings

To display the emboss settings:

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats.**
2. Select a card type in the list and click **Edit.**

3. On the side menu, click **Emboss Settings**.



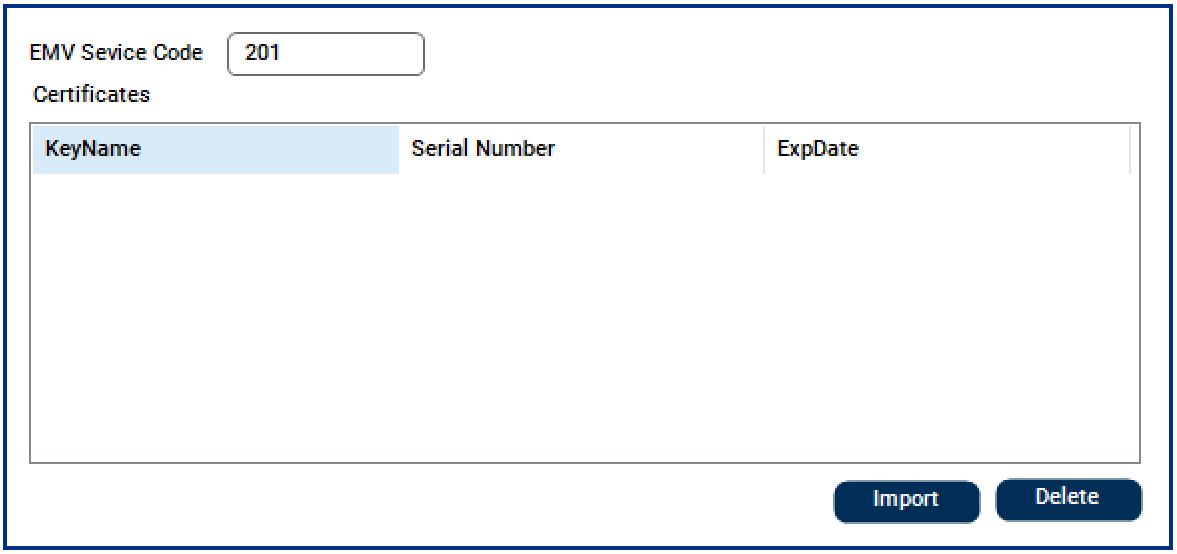
Field	Description
Indents and Embossing	Enter the size of the indentation applied to text on the card.
Use Masking	Check this box to hide certain lines of text from displaying on the Order Card window when cards are being created.
Disable Truncation Rules	Customer names are not shortened automatically.
Topping	Check this box if topping foil is used on embossed card text.

7.4.4 EMV

To display the EMV service code, which indicates that the card is an EMV chip card.

1. On the main menu, click the **Personal icon** > **Configure.** On the side menu, click **Formats.**
2. Select a card type in the list and click **Edit.**

3. On the side menu, click **EMV**.



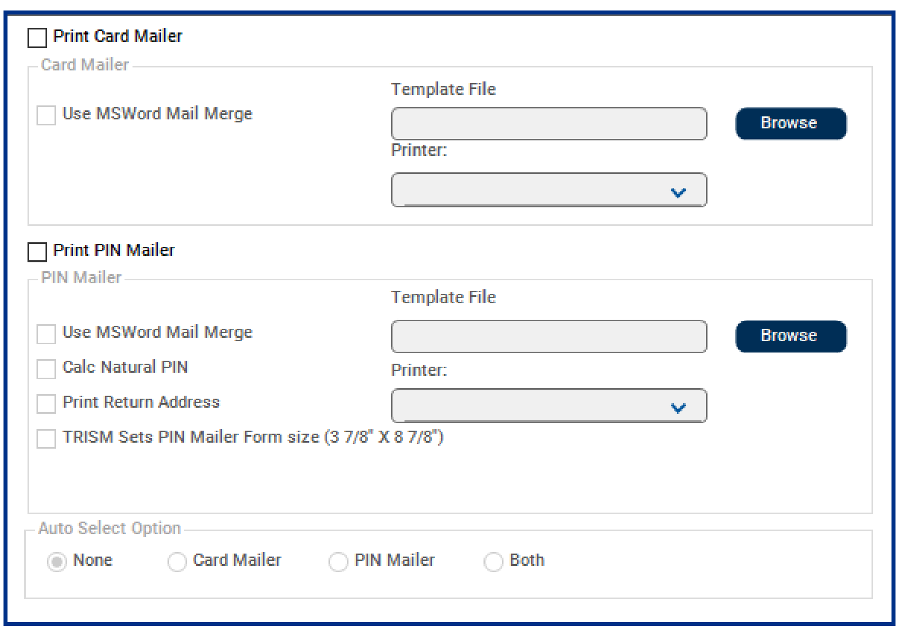
For information on importing issuer certificates used for dual interface EMV chips, see section 7.2 Import the Issuer Certificate File into the TRISM Client in the *TRISM HSM XT Administrators Manual* (PLT-04227).

7.4.5 Mailers

> **Note:** This option is only available if you are licensed for mailers.

To display the Mailers settings:

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats**.
2. Select a card type in the list and click **Edit**.
3. On the side menu, click **Mailers**.



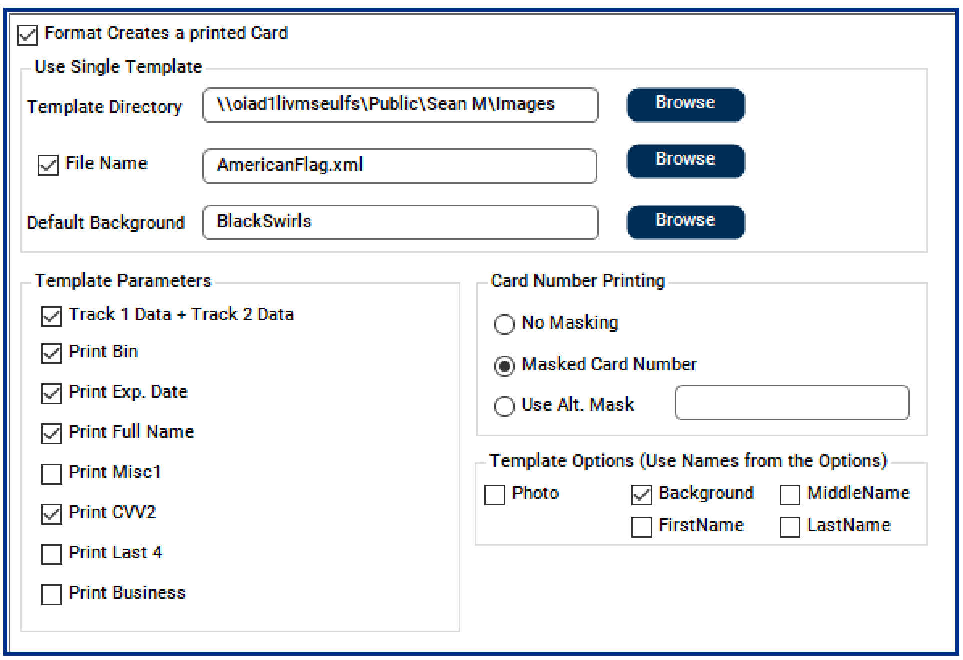
Field	Description
Print Card Mailer	Enables printing of mailers upon card print.
Use MSWord Mail Merge	Use mailer templates from Microsoft Word documents.
Print PIN Mailer	Enables printing of mailers upon card print.
Use MSWord Mail Merge	Use mailer templates from Microsoft Word documents.
Calc Natural PIN	Automatically generate a PIN for which the offset is 0000. When this is not enabled, the offset is determined based on a randomly generated PIN.
Print Return Address	Include the branch's address on the PIN mailer.
Auto Select Option	Specifies a default mailer option, so the teller does not have to make a manual selection each time.

7.4.6 Photo Settings

Configure **.xml** files, card number layout, photo IDs, and custom backgrounds. To display the photo settings:

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats**.
2. Select a card type in the list and click **Edit**.
3. On the side menu, click **Photo Settings**.

General

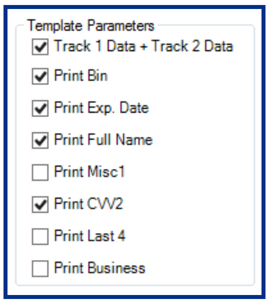


Field	Description
Use Single Template	
Template Directory	Sets the image gallery location. Click Browse. The file location should be accessible to every user. It is recommended the image gallery is saved in a folder with a name matching the BIN, within the specified card type folder. For example: \\Server Name\Images\Card Type\BIN
Default Background	Select a background image to automatically populate the Order Card screen.

Field	Description
Card Number Printing	
No Masking	Select for 18-digit cards to disable spacing between numbers.
Masked Card Number	Separate a 16-digit card number into 4 blocks of 4 digits.
Use Alt. Mask	Enter a string of "#" signs consistent with the desired spacing of card digits.

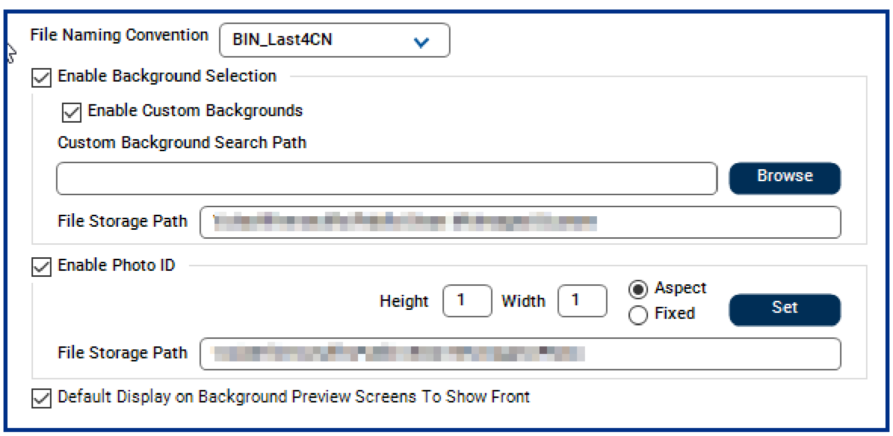
Template Parameters and Template Options

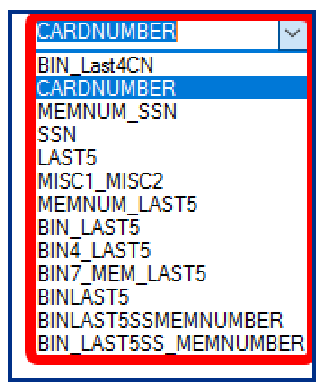
Check the fields that the card format **.xml** file contains.



Advanced

From the **File Naming Convention** drop-down menu, select which cardholder information indicator is used to name the image files.





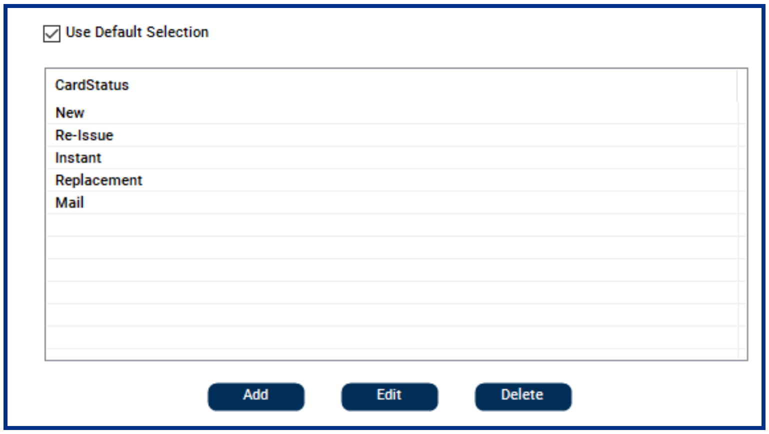
Field	Description
Enable Background Selection	Enable the gallery card selection drop-down menu in the Order Card screen. **Enable Custom Backgrounds:** Show the Personalize button in the Order Card screen. **Custom Background Search Path:** Folder in which custom backgrounds will be saved.
Enable Photo ID	Show **Take Photo** button in the Order Card screen.

7.4.7 Card Status

The card status for each format is chosen in the **Order Card Job Information** panel. Use the default selection.

To display the card status settings:

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats**.
2. Select a card type in the list and click **Edit.**
3. On the side menu, click **Card Status**.



Card Status	Definition
Instant	Activates card and updates offset/exp.date when end user has already added a card record and it is being pulled back into TRISM.
New	Adds skeletal record, activates card, and updates offset/exp.date.
Re-Issue	Updates offset/exp.date.
Replacement	Makes no changes and does not communicate any new data (for example, just prints a card).
Mail	Used in conjunction with the default statuses (for example, Instant Mail, New Mail, Re-Issue, and Replacement). Adds skeletal card record, updates offset/exp.date, and does not activate card.

7.4.8 Card Class

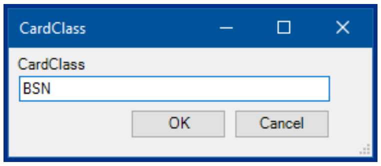
When there is more than one card class assigned to a BIN, the card class for each format is chosen in the **Order Card Job Information** panel.

To display the card class settings:

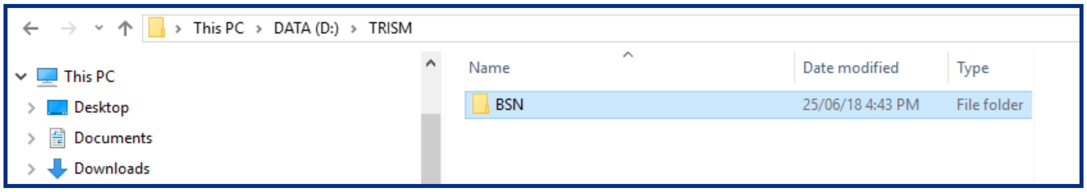
1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Formats.**
2. Select a card type in the list and click **Edit.**
3. On the side menu, click **Card Class**.

Adding a Card Class to a BIN:

1. Click **Add** and enter the card class name. Click **OK**.



2. In Windows Explorer, navigate to the BIN template directory. Create a folder with a name that exactly matches the card class name.

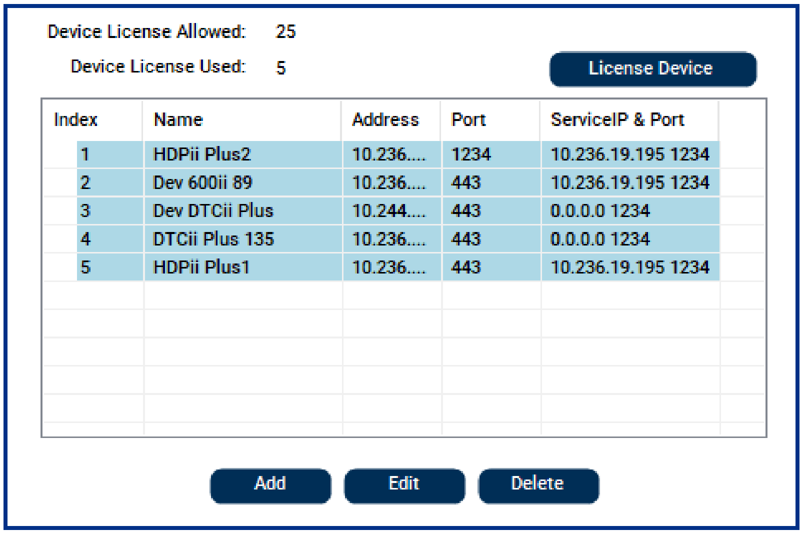


3. Add the desired image and xml file to the card class folder. If using different xml files for each image, add all necessary xml files.
4. If another BIN is using the same card class, copy the card class folder and paste it in the other BIN folder. It is important that each card class folder is updated when the contents of one is modified.

7.5 Devices

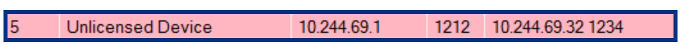
The **Devices** tab displays a list of all printers and embossers configured with TRISM.

On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Devices**.

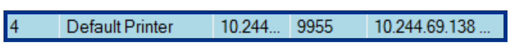


Each device must be licensed. For instructions on adding a device license, see section **8.7 License**.

An unlicensed device is highlighted in red. Select the device from the Devices list and click **License Device**.



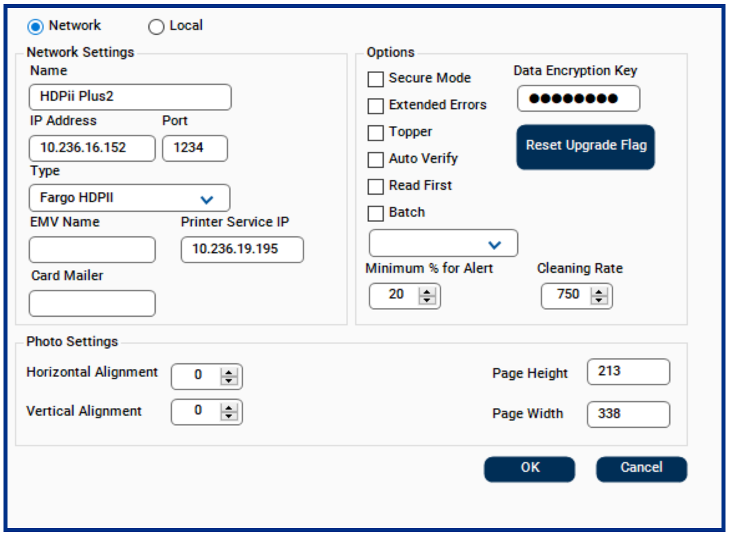
A licensed device is highlighted in blue.



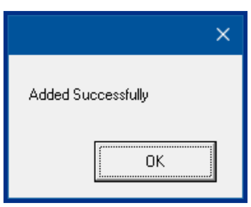
7.5.1 Add a printer or embosser

1. Install the printer according to the manufacturer's instructions.
2. In the TRISM 7 **Devices** window, click **Add**.

3. If the printer is accessed via a network or wireless connection, select **Network**.



4. Enter the printer **Name**, **IP Address**, a **Port** unique to the printer, **Type** (photo printer, embosser), and UNC path of the **Card Mailer** printer (if applicable).
5. Set the **Horizontal** and **Vertical Alignment** fields to **6** (HDPii Plus printers only).
6. Ensure the **Page Height** is **213** and the **Page Width** is **338**.
7. If an embosser is being used, select the desired options in the **Options** area:
   - **Secure Mode**: Enter embosser's data encryption key to encrypt information sent to embosser.
   - **Extended Errors**: View a detailed log of any embosser errors.
   - **Topper**: Check if a foil topping is imprinted on card numbers and names.
   - **Auto Verify**: After a card is printed, it is automatically verified that it has printed correctly. This is recommended when printing large quantities of cards.
   - **Read First**: Not used.
   - **Batch:** Not used.
8. When all required information has been added, click **OK**.

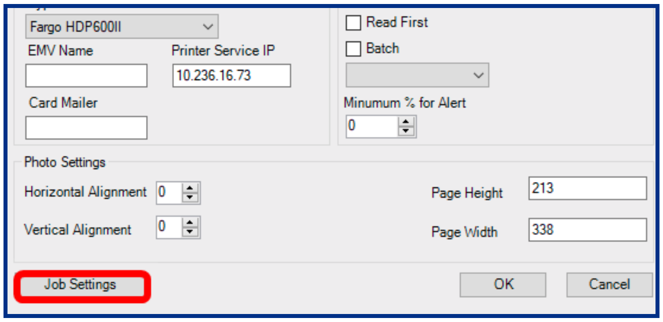


9. Restart Card Printer Service after adding, deleting, or changing a device.

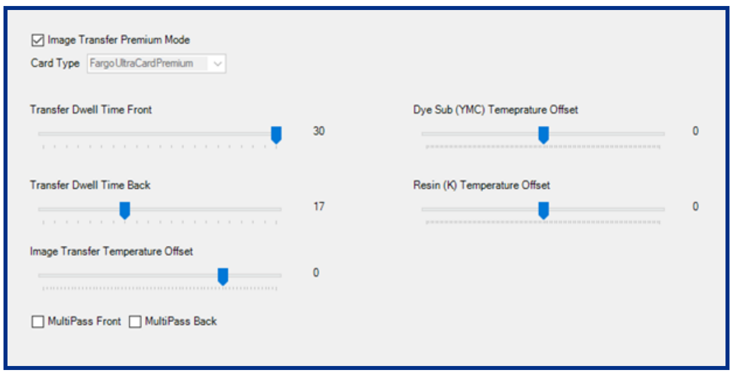
Job Settings for HDP600ii Printer

Additional job settings can be configured for the HDP600ii printer.

1. In the TRISM 7 **Devices** window, click **Job Settings**.



2. The following form is displayed to adjust the settings for the HDP600ii printer.

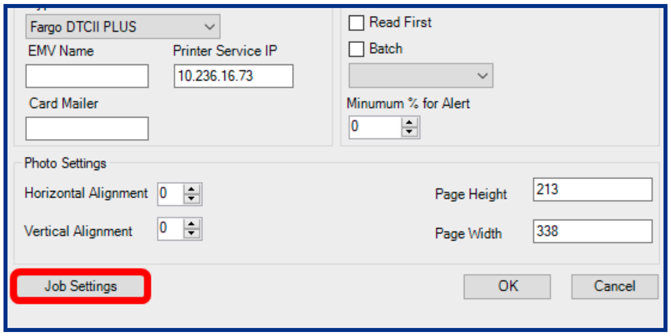


Field	Description
Image Transfer Premium Mode	When this option is selected, you can specify the type of card used in the printer. When the **Card Type** is selected, the **Transfer Dwell Time Front**, **Transfer Dwell Time Back**, and **Image Transfer Temperature Offset** settings are automatically set to the optimum values. If this field is not selected, these settings are not applied.
Transfer Dwell Time Front	Sets the speed at which the card moves through the transfer section in the printer. This setting affects the front of the card transfer speed.
Transfer Dwell Time Back	Sets the speed at which the card moves through the transfer section of the printer. This setting affects the back of the card transfer speed.
Image Transfer Temperature Offset	Sets the temperature of the transfer roller when applying the film to the card.
Dye Sub (YMC) Temperature Offset	Controls the temperature of the print head when printing the Yellow, Magenta, and Cyan panels onto the card. Increase the setting to darken the image and decrease the setting to lighten the image.
Resin (K) Temperature Offset	Controls the temperature of the print head when printing the black resin panel onto the card. Increase the setting to darken the image and decrease the setting to lighten the image.
MultiPass Front	When enabled, a second layer of film is applied to the front of the card. This should not be used if the inhibit panel is being used on the front of the card.
MultiPass Back	When enabled, a second layer of film is applied to the back of the card. This should not be used if the inhibit panel is being used on the back of the card.

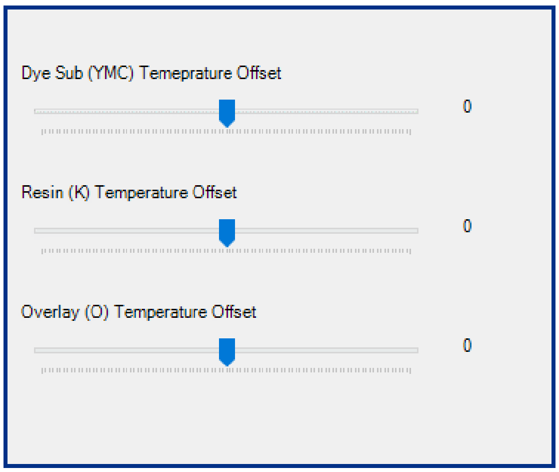
Job Settings for DTCii Plus Printer

Additional job settings can be configured for the DTC®ii Plus printer.

1. In the TRISM 7 **Devices** window, click **Job Settings**.



2. The following form is displayed to adjust the settings for the DTCii Plus printer.



Field	Description
Dye Sub (YMC) Temperature Offset	Controls the temperature of the print head when printing the Yellow, Magenta, and Cyan panels onto the card. Increase the setting to darken the image and decrease the setting to lighten the image.
Resin (K) Temperature Offset	Controls the temperature of the print head when printing the black resin panel onto the card. Increase the setting to darken the image and decrease the setting to lighten the image.
Overlay (O) Temperature Offset	Controls the temperature of the print head when applying the overlay material onto the card.

7.6 Active Directory

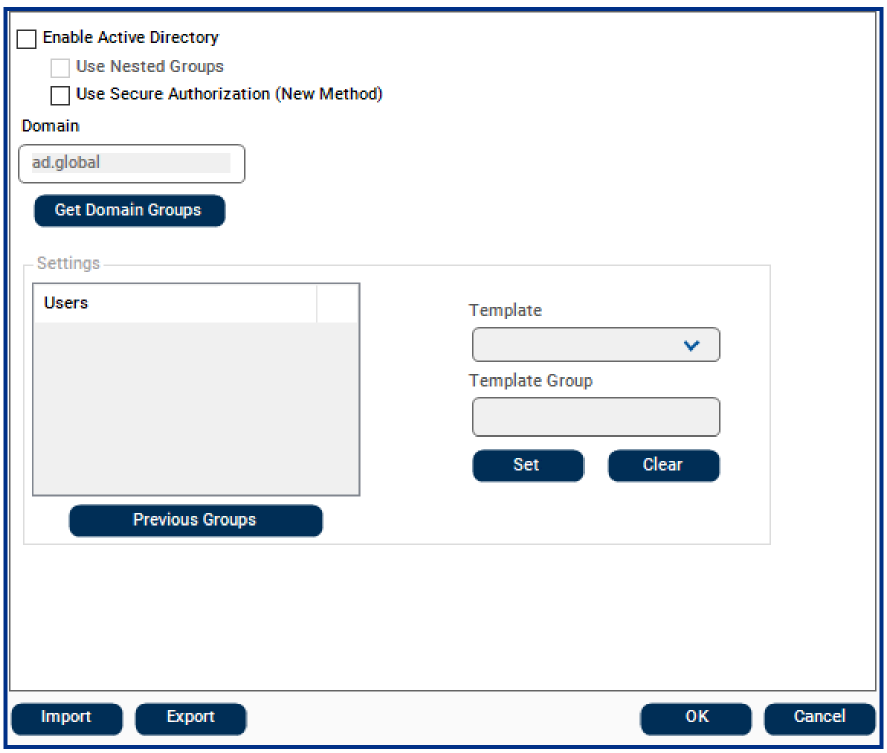
All users that are part of a network **Active Directory** can be automatically entered in TRISM. If Active Directory is enabled, user names and passwords cannot be changed using TRISM 7. The computer in use must be part of a domain, not a work group. If the computer is part of a work group, do not change any active directory settings.

On the main menu, click **Configure**. On the side menu, click **Active Directory**.

When Active Directory is enabled, the only non-active directory logins that may be used are:

- Access1
- Installer1
- Installer2

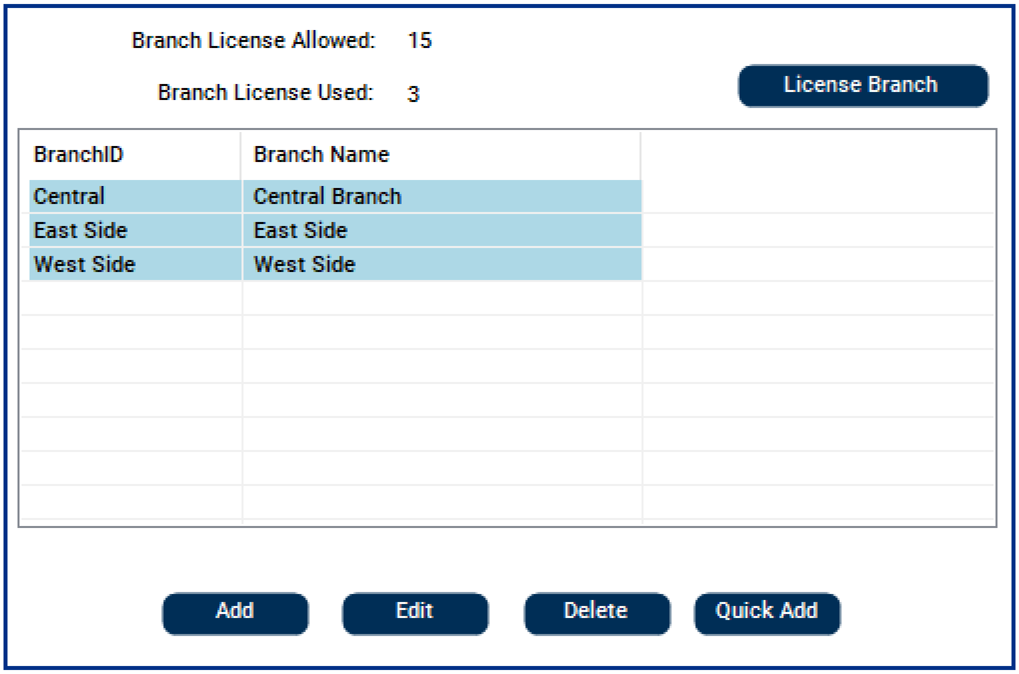
1. Check **Enable Active Directory**. TRISM 7 automatically searches and enters the domain name.
2. Click **Get Domain Groups** to display all groups in the Users window.
3. Select a group in the **Users** window and choose a template from the drop-down menu.
4. Click **Set** to save the template to the selected domain group.
   The domain group selected is displayed in the **Template Group** field.



7.7 Branches

Each branch must be licensed. For instructions on adding a branch license, see section **8.7 License**.

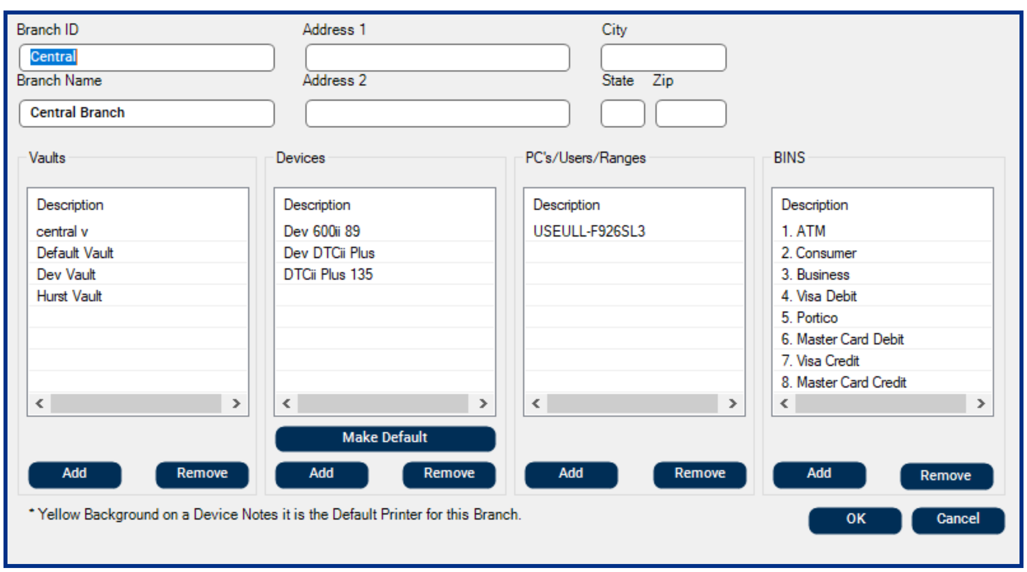
1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Branches**.



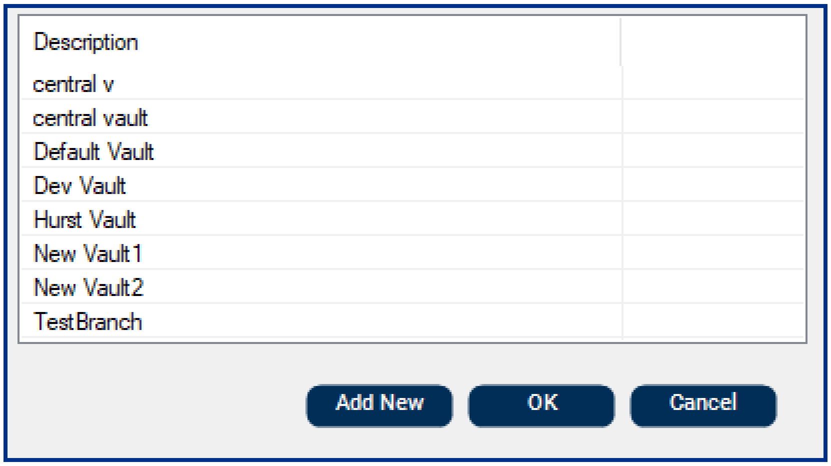
2. Select an unlicensed branch highlighted in red and click **License Branch**. A licensed branch is highlighted in blue.

7.7.1 Add vaults to a branch

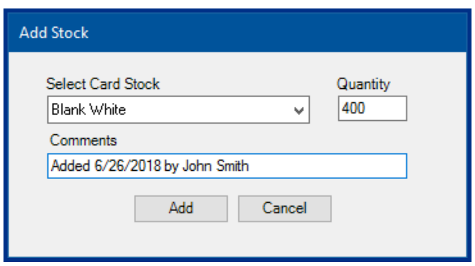
1. Select a branch and click **Edit**.
2. Click **Add** under the list of **Vaults**.



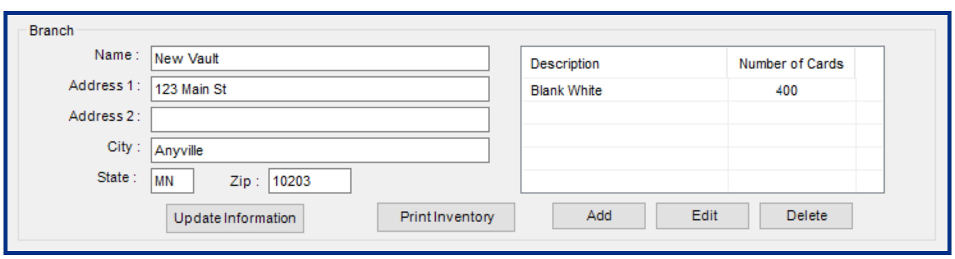
3. Click **Add New**. Dual control is enforced for accessing vaults, so a second user must enter their login credentials.



4. To add a central vault (the vault in which inventory is usually stored for distribution to branches), click **Add Central**. To add a non-central vault (no inventory is taken from a non-central vault and sent to other branches), click **Add Location**.
5. Enter the vault name and location, then click **OK**.
6. To add card stock to a vault, select the vault and click **Add**.
7. Select the card stock to add, enter the quantity of cards, and any comments required by your financial institution. Click **Add**.

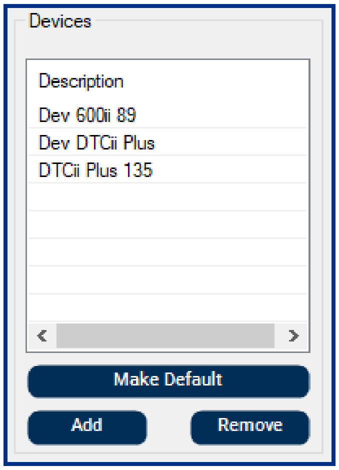


8. The vault inventory is updated.

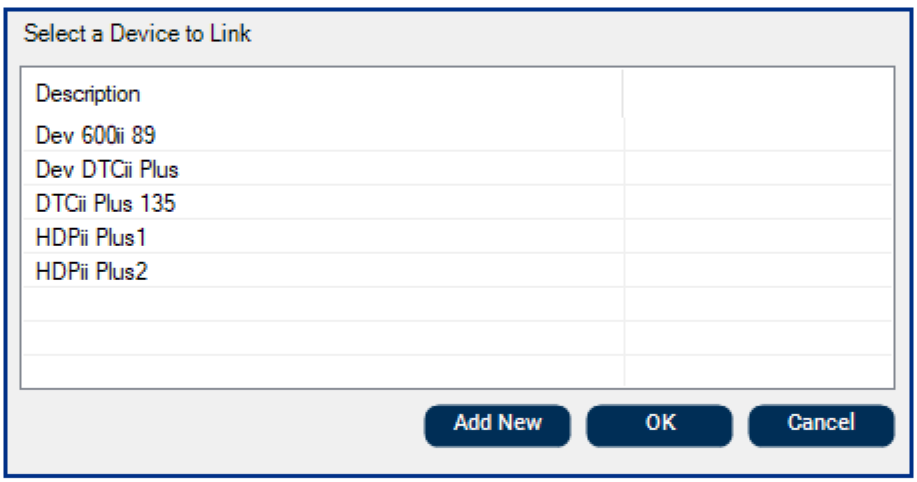


7.7.2 Add devices to a branch

1. Select a branch and click **Edit**.
2. Click **Add** under the list of devices.



3. Select an existing device and click **OK** or click **Add New** to set up a new device. For more information, see section **7.5.1 Add a printer or embosser**

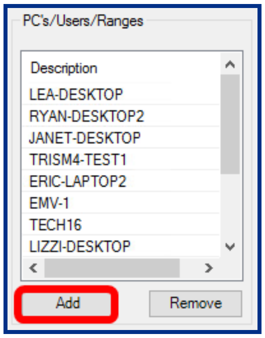


Note: To make one of the devices in the list a default device for the branch, select the device from the list and click **Make Default**. That device now has a yellow background.

7.7.3 Add PCs/users/ranges to a branch

The following procedure is used only to add users when **Active Directory** is enabled.

1. Select a branch and click **Edit**.
2. Click **Add** under the **PC's/Users/Ranges** list.



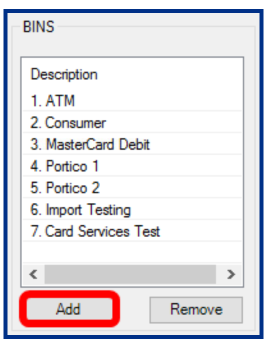
3. Select the method and enter the PC Name, IP Address/Range, or User Name, and click **OK**.

7.7.4 Add BINs to a branch

Before adding BINs to a branch, the BINs must be set up. See section **7.4 Formats**.

The following procedure is used only if different branches use different BINs. If all branches use the same BINs, do not add BINs to any branches. When the BINs list is blank, the branch automatically displays all BINs when ordering a card.

1. Select a branch and click **Edit**.
2. Click **Add** under the **BINS** list.



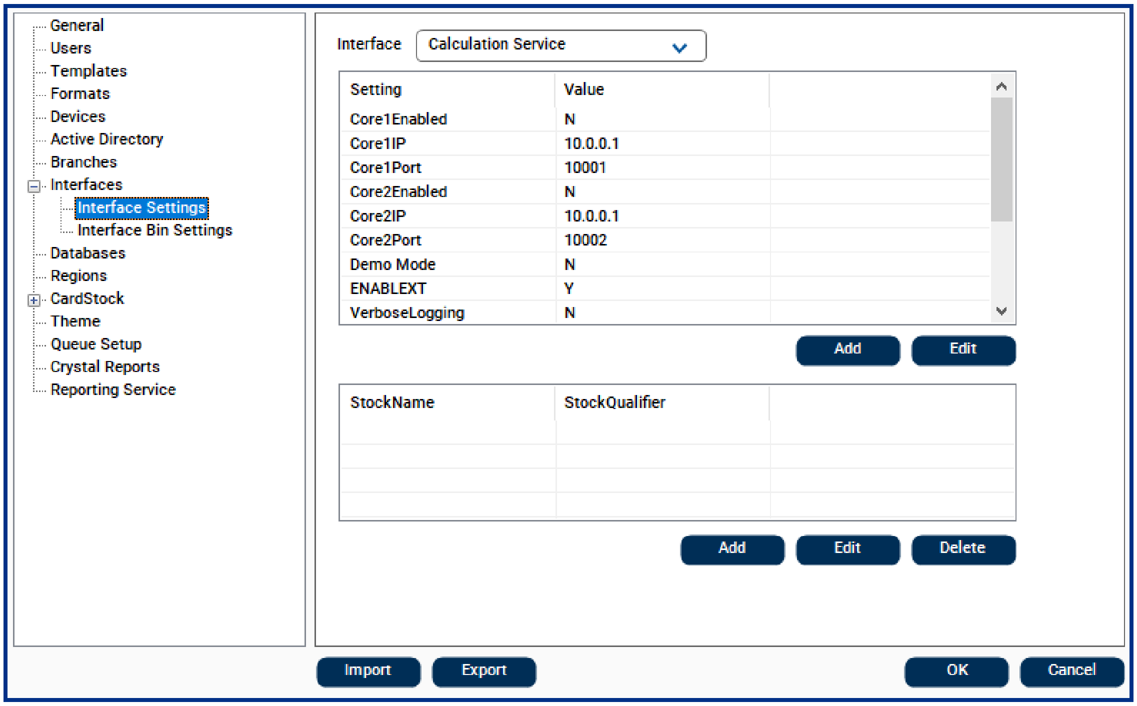
3. Select a BIN and click **OK**.

7.8 Interfaces

7.8.1 Interface Settings

Interface settings and values are determined by each individual interface and are generally not edited by financial institution personnel.

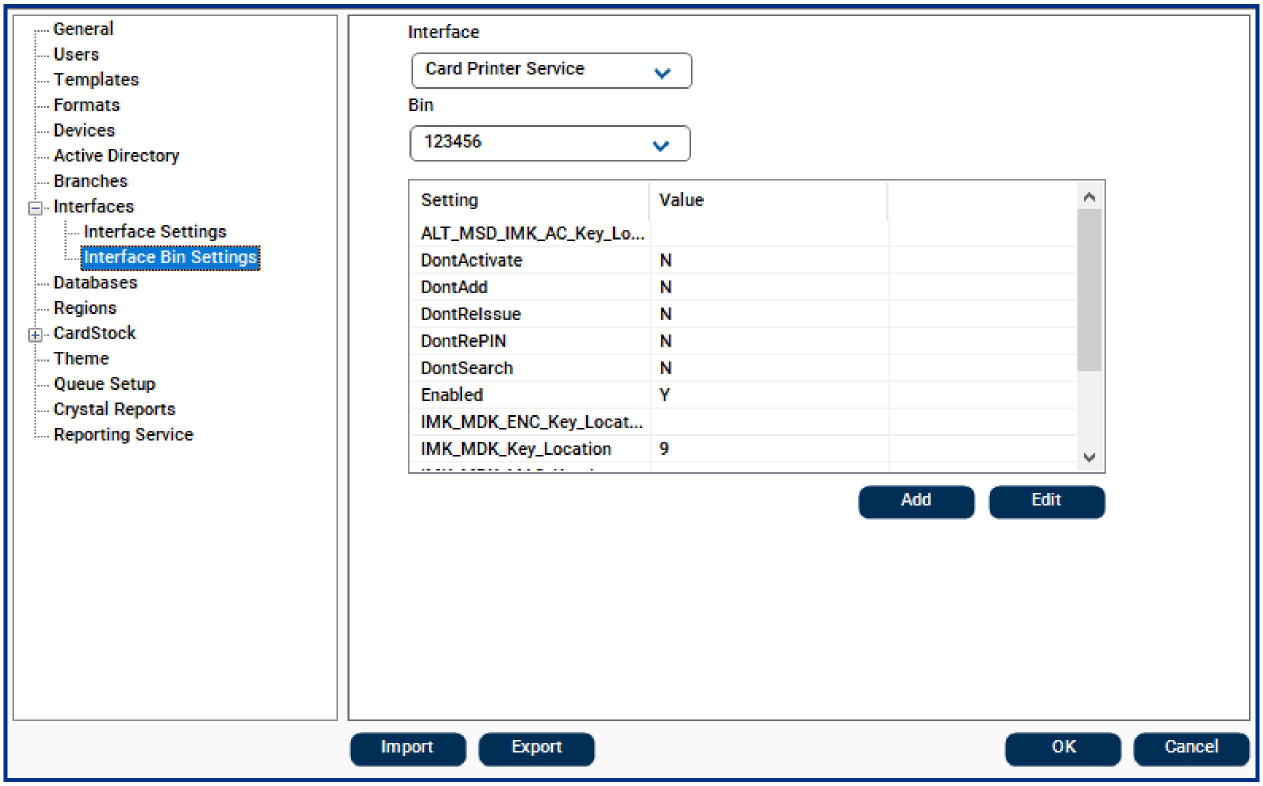
On the main menu, click the **Personal icon** > **Configure.** On the side menu, click **Interfaces**.



7.8.2 Interface BIN Settings

Interface BIN settings determine what actions can be performed by each BIN. Interface BIN settings and values are determined by each individual interface and generally not edited by financial institution personnel.

On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Interfaces** > **Interface BIN Settings**.



7.9 Databases

Change logging options for SQL databases.

On the main menu, click the **Personal icon** > **Configure.** On the side menu, click **Databases**.

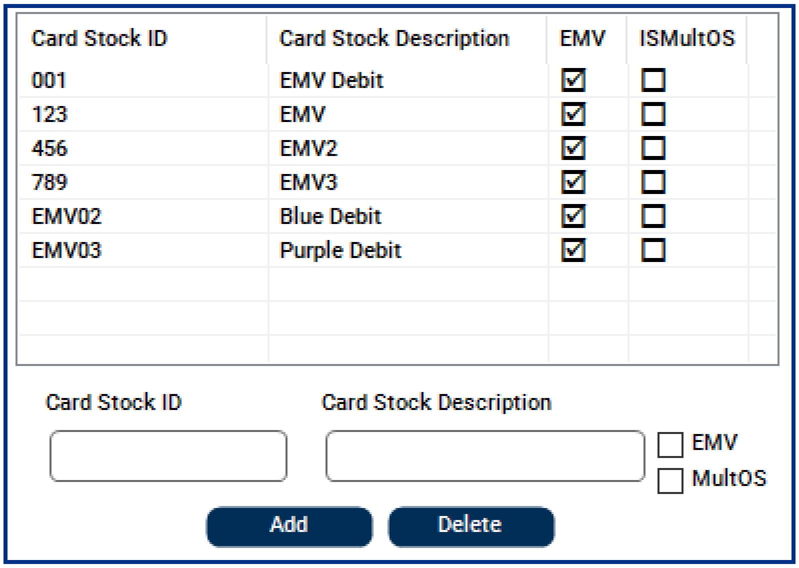
7.10 Card Stock

On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Card Stock**.

7.10.1 Card Stock ID

To add different card stocks to the inventory menus:

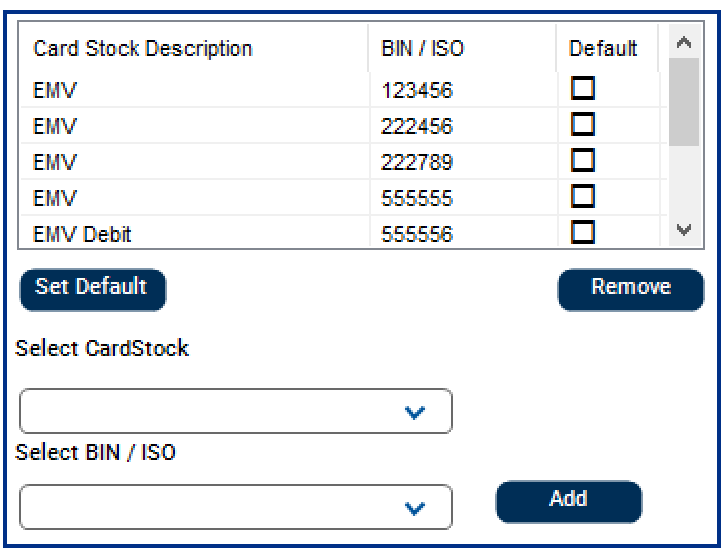
1. Enter the new card stock ID (may be alphanumeric) and description in the fields.
2. Select **EMV** if the card has a chip. Select **ISMultOS** if the card has Chip Card Plug In (CCPI). Click **Add**.



7.10.2 Card Stock to BIN

To set the BIN number to be printed on each card stock type:

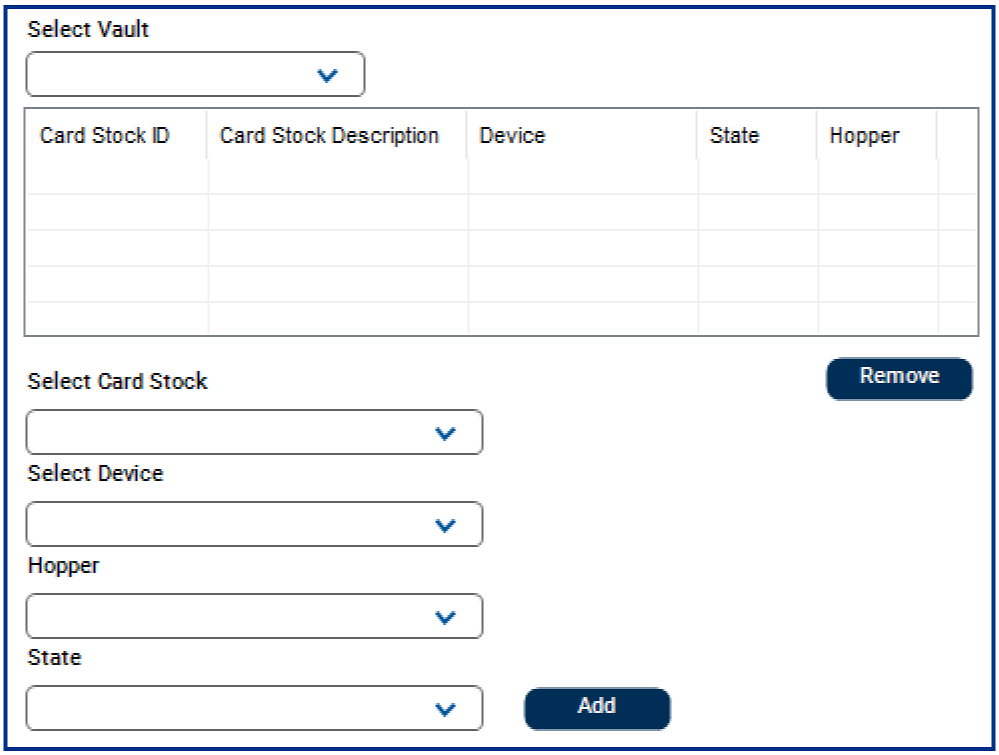
1. Select the card stock in the drop-down menu.
2. Select the BIN in the drop-down menu, then click **Add**.



7.10.3 Card Stock to Vault/Device

Track the addition of card types to printers and embossers.

1. Select the vault that contains the card stock to be added, then select the card stock from the drop-down menu.
2. Select the printer or embosser to which card stock is to be added.
3. Select the card stock default state/status. Select the card stock default state/status. The default selections are:
   - **Ready**: the card prints immediately upon completion.
   - **Paused**: the card does not print until the state is changed to Ready or Manual in the Queue.
   - **Manual**: the card does not print until it is manually fed into the printer using the exception feed slot. This is not available on some printer models.
4. Click **Add**, then **OK**.



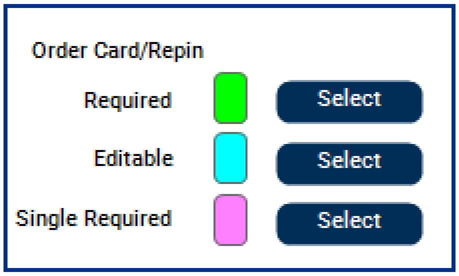
7.10.4 Add a new BIN or card stock

1. If adding a new BIN, add a new format (see section **7.4 Formats**).
2. Add a new card stock ID (see section **7.10.1 Card Stock ID**).
3. Link the new card stock ID to the appropriate BIN (see section **7.10.2 Card Stock to BIN**).
4. If you are using different BINs for different branches, add the BIN to the branch (see section **7.7.4 Add BINs to a branch**). If you are using the same BINs for all branches, go to the next step.
5. Add card stock to the branch vault (see section **7.7.4 Add BINs to a branch**).
6. Link the new card stock to the vault and device (see section **7.10.3 Card Stock to Vault/Device**).
7. Card stock can be added to devices in Device Access (see section **6.1 Device Access**).

7.11 Theme

Allows you to customize the text box color of the **Edit Permissions**, **Order Card**, and **Re-PIN** menus.

Click **Select** to choose a color, then click **OK** to apply changes.



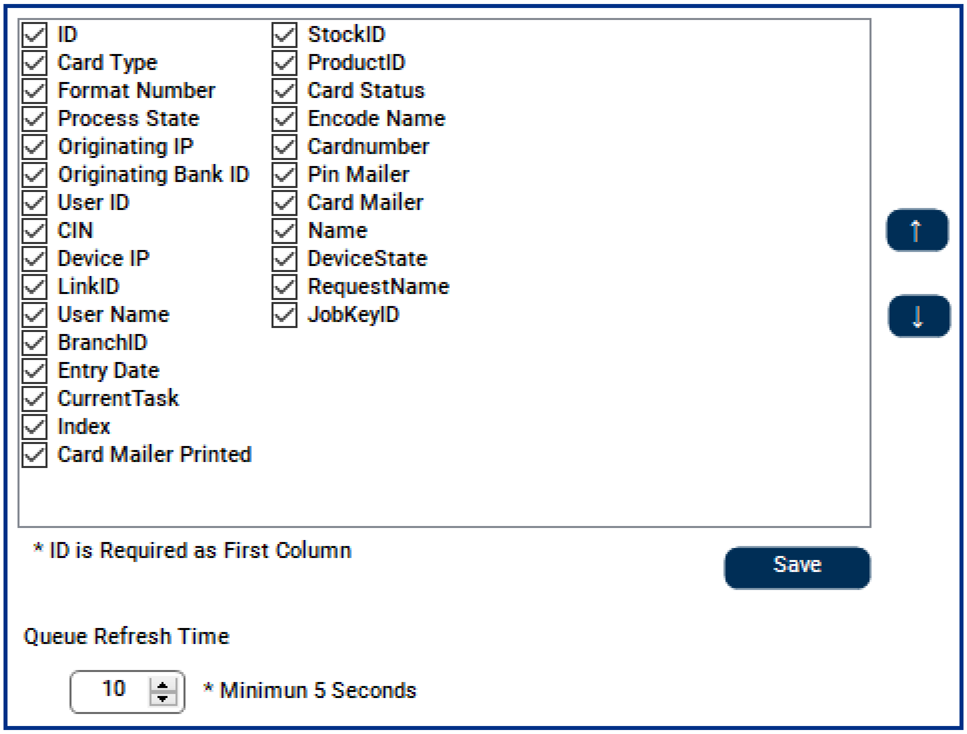
7.12 Queue Setup

Change the order in which columns are displayed in the Queue.

1. On the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Queue Setup**.
2. Select a field and click the arrows to change its order.

    Note: The ID field must be first and must be checked.

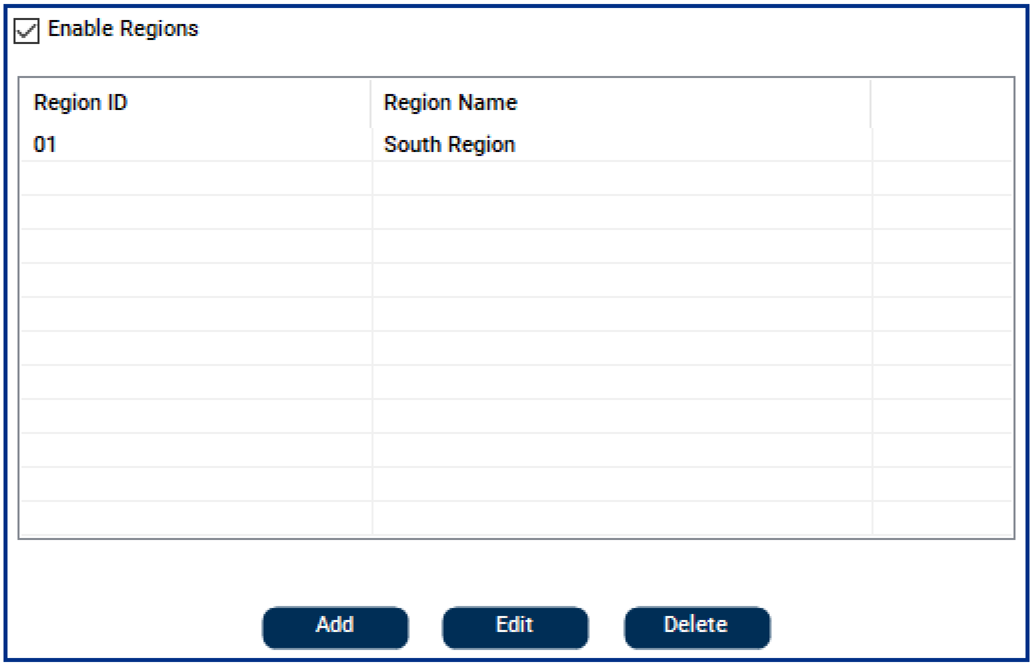
3. Clear the check box to hide the field in the Queue.
4. Click **Save**.



7.13 Regions

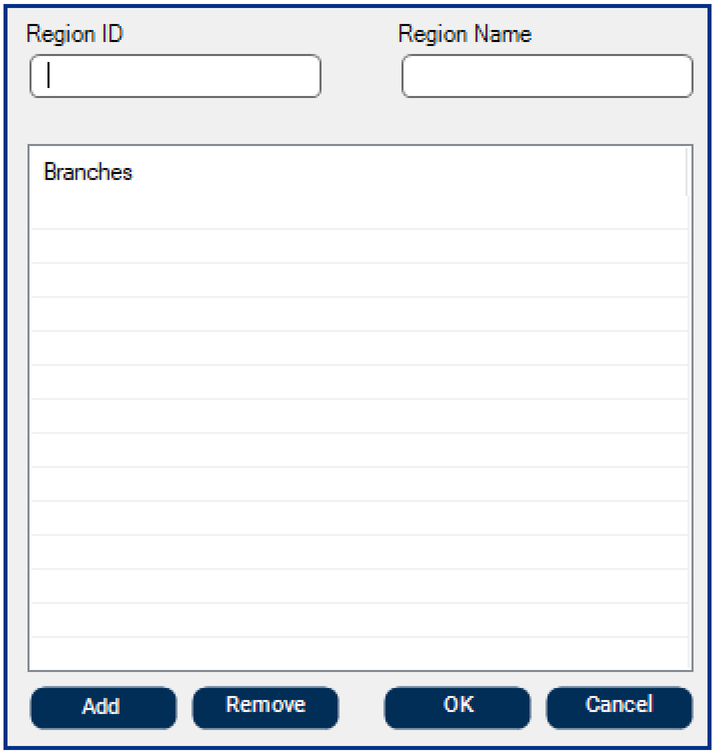
Regions are groups of branches that are linked together to allow you, with correct permissions, access to the regional queue and devices. They also allow you to redirect jobs to any other device in the region.

To manage the regions setup, on the main menu, click the **Personal icon** > **Configure**. On the side menu, click **Regions**.



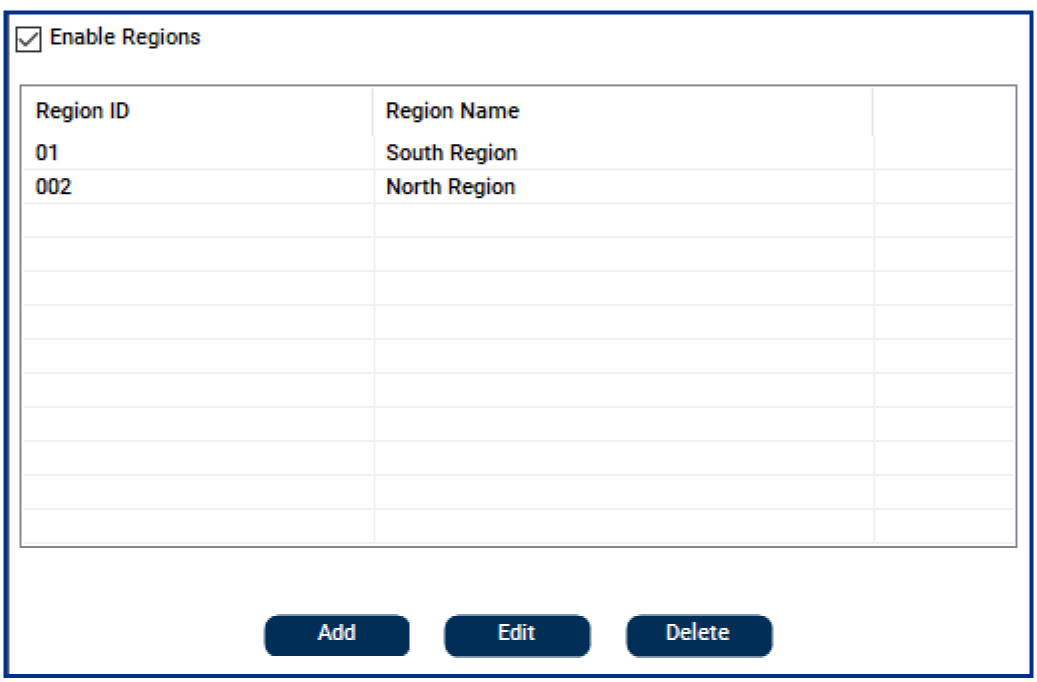
7.13.1 Add a region

1. On the Regions configuration screen, click **Add**.
2. Enter a **Region ID**, **Region Name**, and click **OK**.

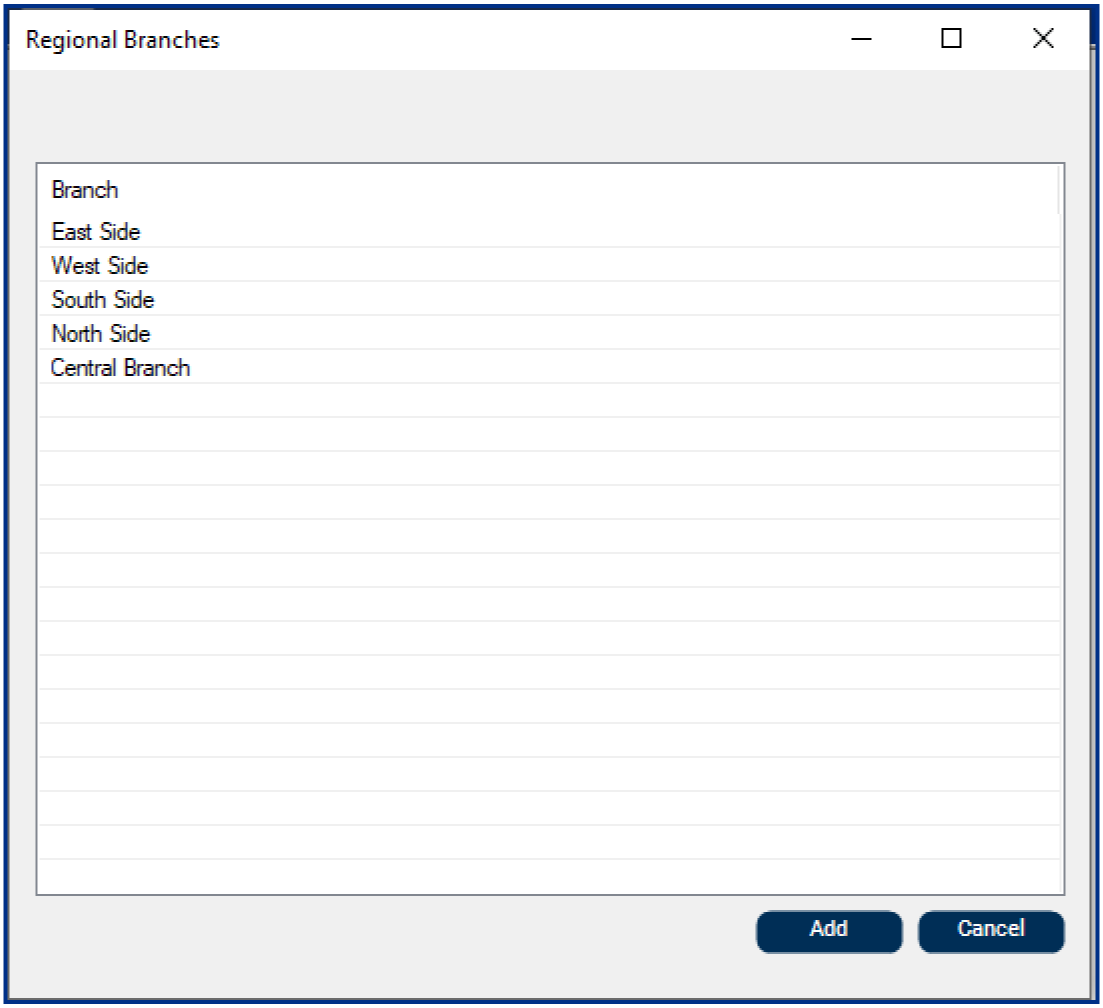


7.13.2 Add a new branch to a region

1. On the Regions configuration screen, select a region and click **Edit**.

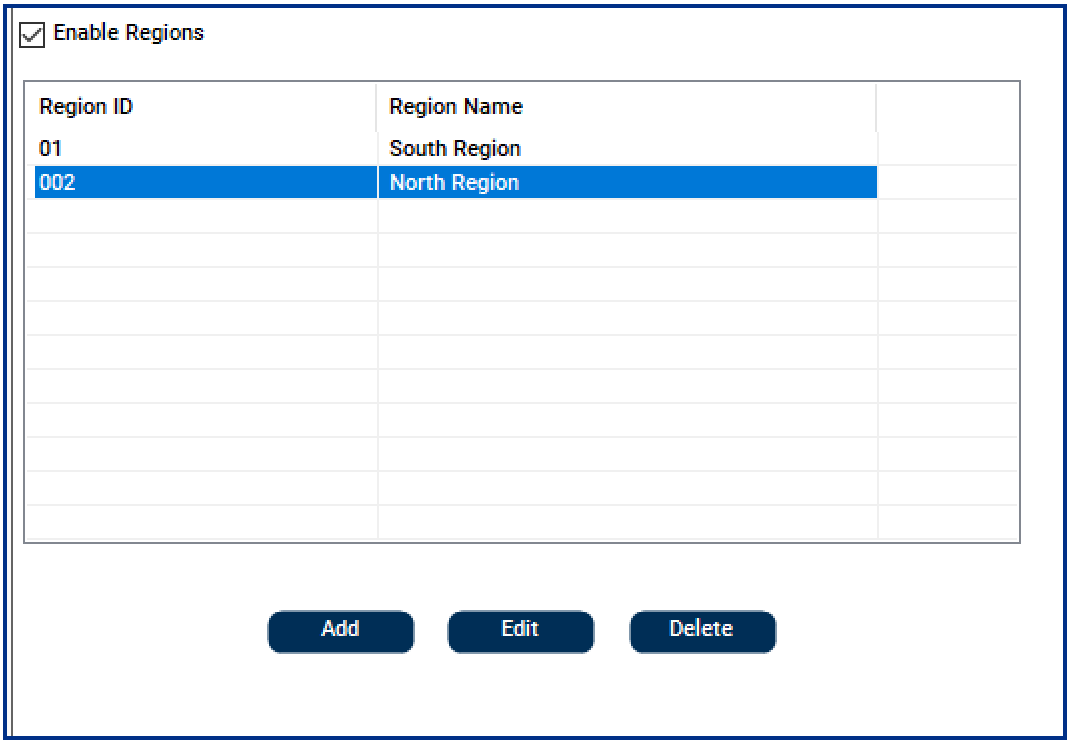


2. On the Edit screen, click **Add**.
3. From the list, select the branch to add to the region and click **Add**.

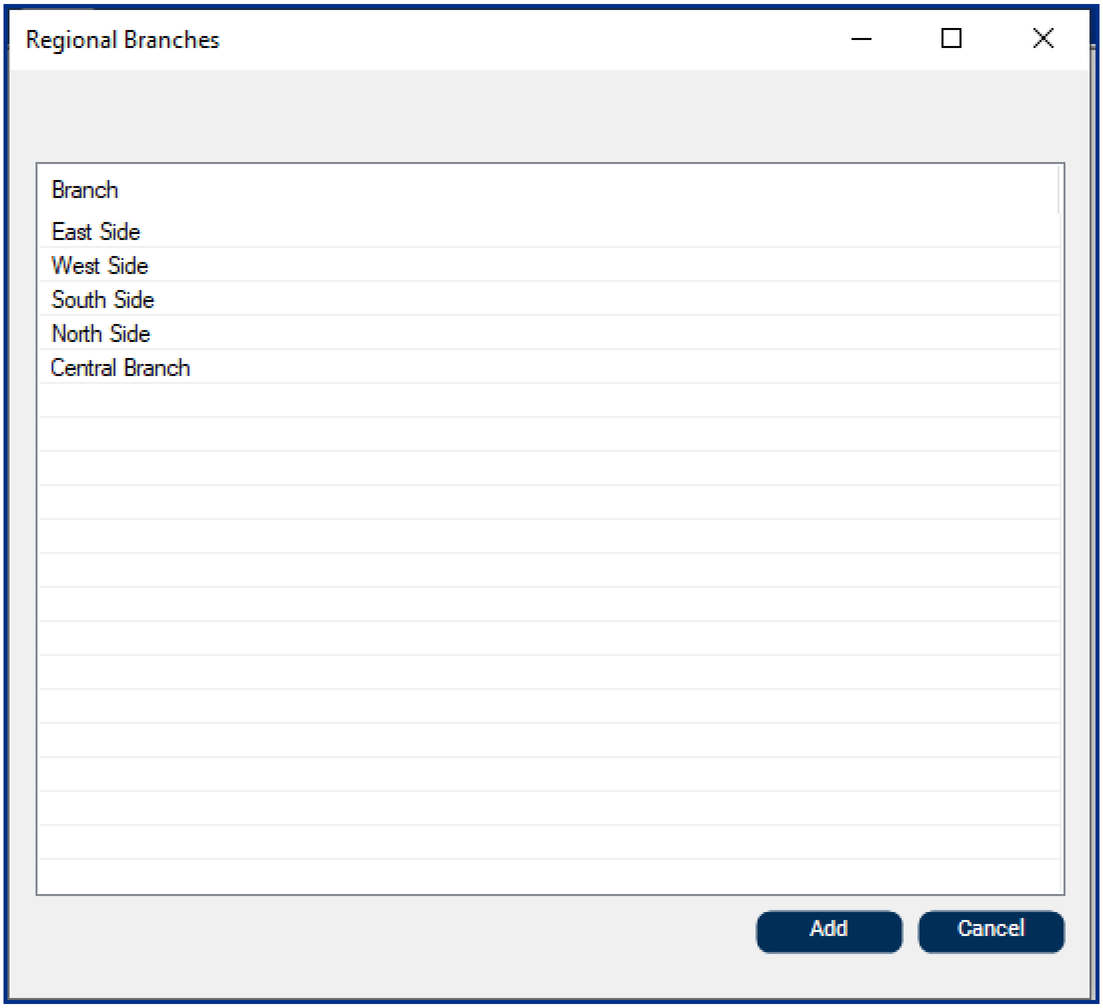


7.13.3 Remove a branch from a region

1. On the Regions configuration screen, select a region and click **Edit**.



2. Select the branch to remove from the region and click **Remove**.



Section 08

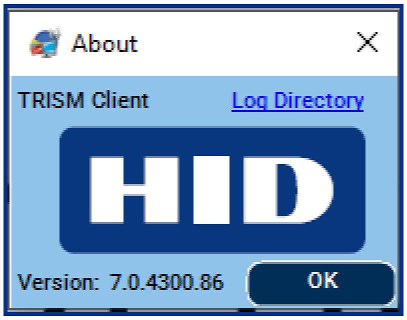
Help

8.1 About

View the version of TRISM 7 currently installed.

On the main menu, click the **Personal icon** > **Help** > **About**.

To view TRISM data and error logs, click **Log Directory**.



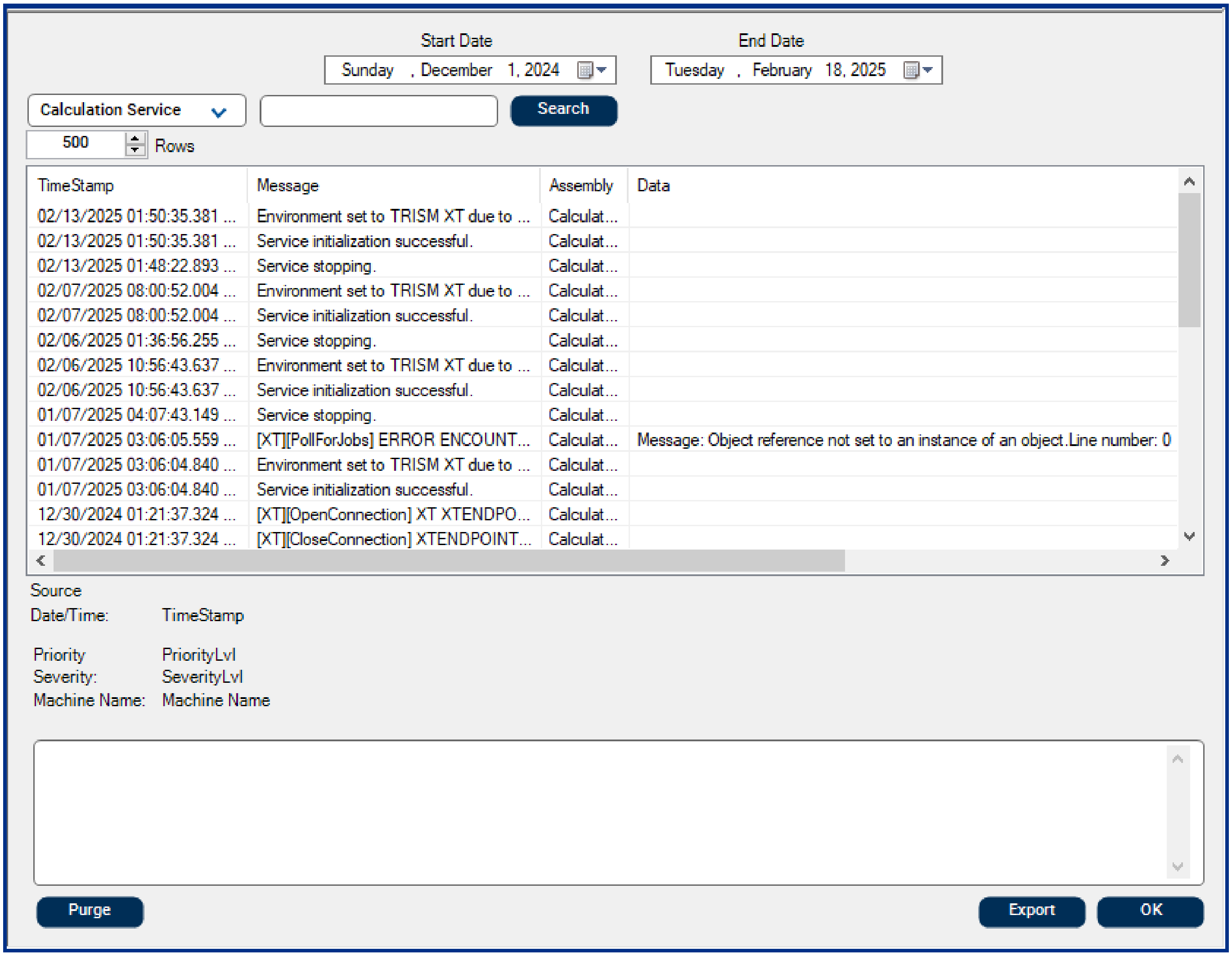
8.2 Support Documents

View TRISM support documents such as the user manual and daily procedures.

8.3 Data Log

View the log of all actions performed by third party services.

1. On the main menu, click the **Personal icon** > **Help** > **Data Log**.
2. Select the dates to search by in the **Start Date** and **End Date** drop-down menus.
3. Select the service in which to view the log.
4. Logs can be queried using search terms with the AND, OR, and NOT filter expressions. To utilize this feature, enter the desired words into the search field and click **Search**.

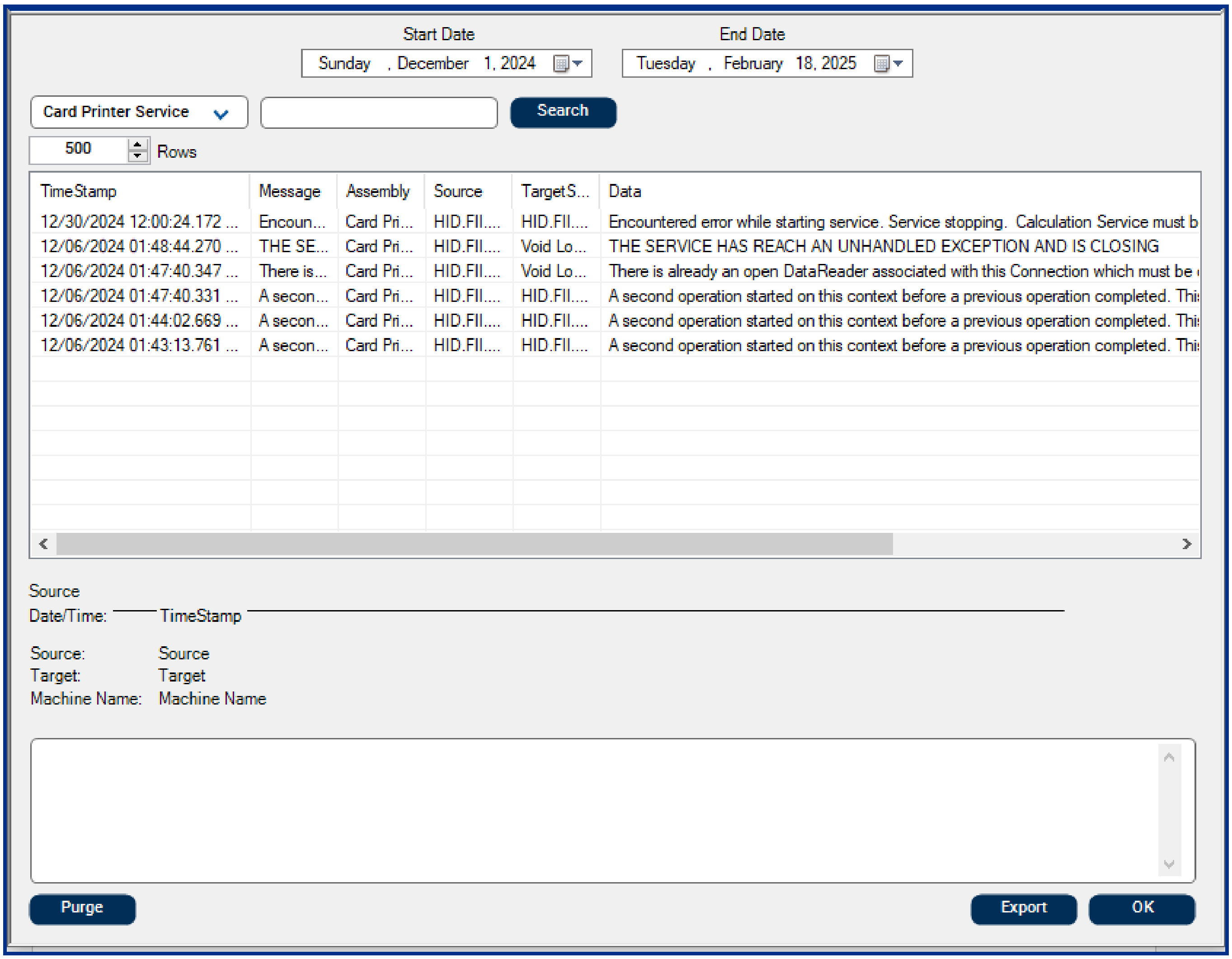


Button	Description
Purge	Deletes the log.
Export	Exports log to a notepad file.

8.4 Error Log

View the log of all errors encountered by third party services.

1. On the main menu, click the **Personal icon** > **Help** > **Error Log**.
2. Select the dates to search by in the **Start Date** and **End Date** drop-down menus.
3. Select the service in which to view the log. Click **Search**.
4. Logs can be queried using search terms with the AND, OR, and NOT filter expressions. To utilize this feature, enter the desired words into the search field and click **Search**.
5. Click **Purge** to delete the log.



8.5 Client Information

On the main menu, click the **Personal icon** > **Help** > **Client Information**.

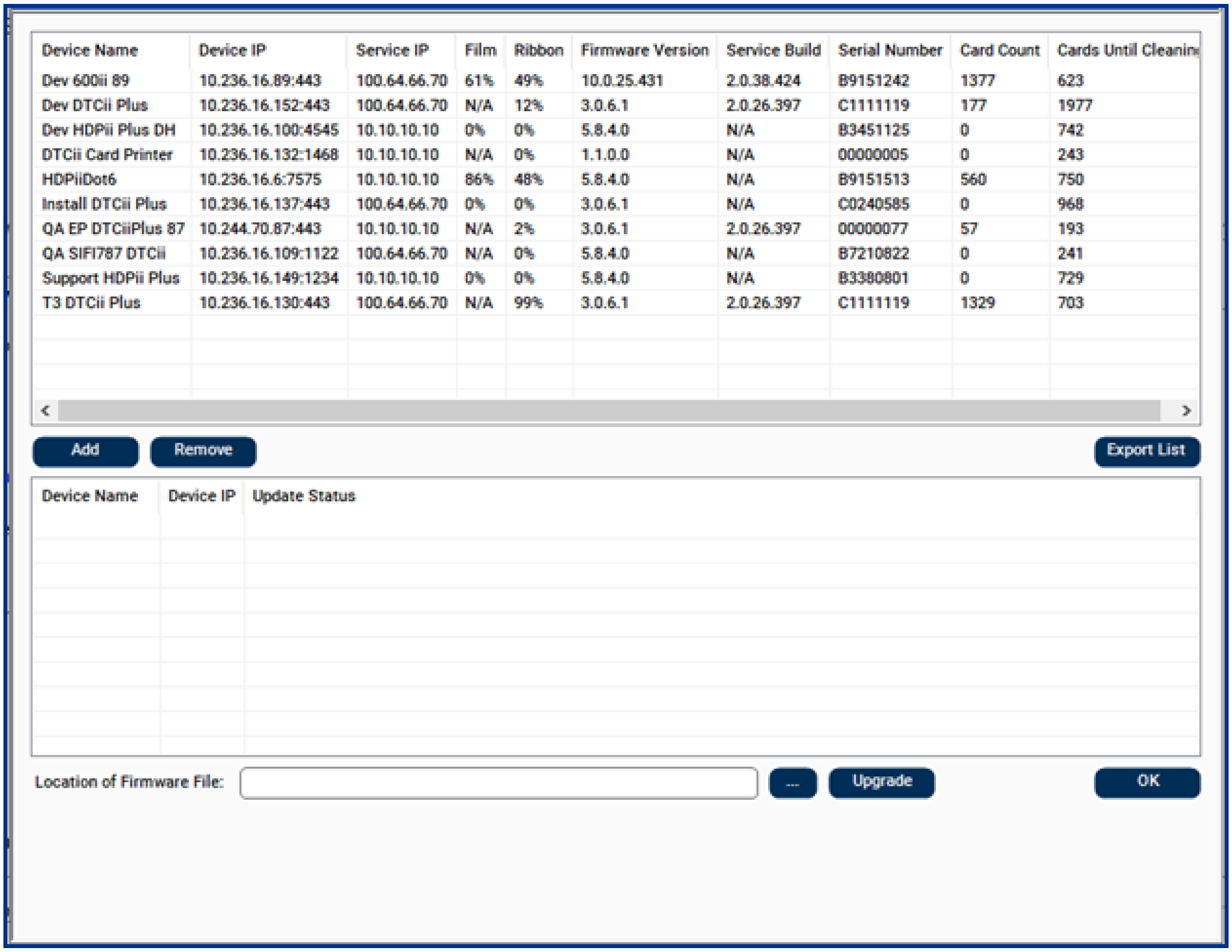
Client Information displays a list of each TRISM workstation and the following information associated with each workstation:

- User ID
- TRISM Version
- Last Login
- Last Logout
- PIN Pad Serial Number

8.6 Device Information

The Device Information screen is used to display information about currently configured driverless printers such as the HDP600ii and DTCii Plus.

On the main menu, click the **Personal icon** > **Help** > **Device Information**.



Device Name	Device IP	Service IP	Film	Ribbon	Firmware Version	Service Build	Serial Number	Card Count	Cards Until Cleanin
Dev 600ii 89	10.236.16.89:443	100.64.66.70	61%	49%	10.0.25.431	2.0.38.424	B9151242	1377	623
Dev DTCii Plus	10.236.16.152:443	100.64.66.70	N/A	12%	3.0.6.1	2.0.26.397	C1111119	177	1977
Dev HDPii Plus DH	10.236.16.100:4545	10.10.10.10	0%	0%	5.8.4.0	N/A	B3451125	0	742
DTCii Card Printer	10.236.16.132:1468	10.10.10.10	N/A	0%	1.1.0.0	N/A	00000005	0	243
HDPiiDot6	10.236.16.6:7575	10.10.10.10	86%	48%	5.8.4.0	N/A	B9151513	560	750
Install DTCii Plus	10.236.16.137:443	100.64.66.70	0%	0%	3.0.6.1	N/A	C0240585	0	968
QA EP DTCiiPlus 87	10.244.70.87:443	10.10.10.10	N/A	2%	3.0.6.1	2.0.26.397	00000077	57	193
QA SIFI787 DTCii	10.236.16.109:1122	100.64.66.70	N/A	0%	5.8.4.0	N/A	B7210822	0	241
Support HDPii Plus	10.236.16.149:1234	10.10.10.10	0%	0%	5.8.4.0	N/A	B3380801	0	729
T3 DTCii Plus	10.236.16.130:443	100.64.66.70	N/A	99%	3.0.6.1	2.0.26.397	C1111119	1329	703

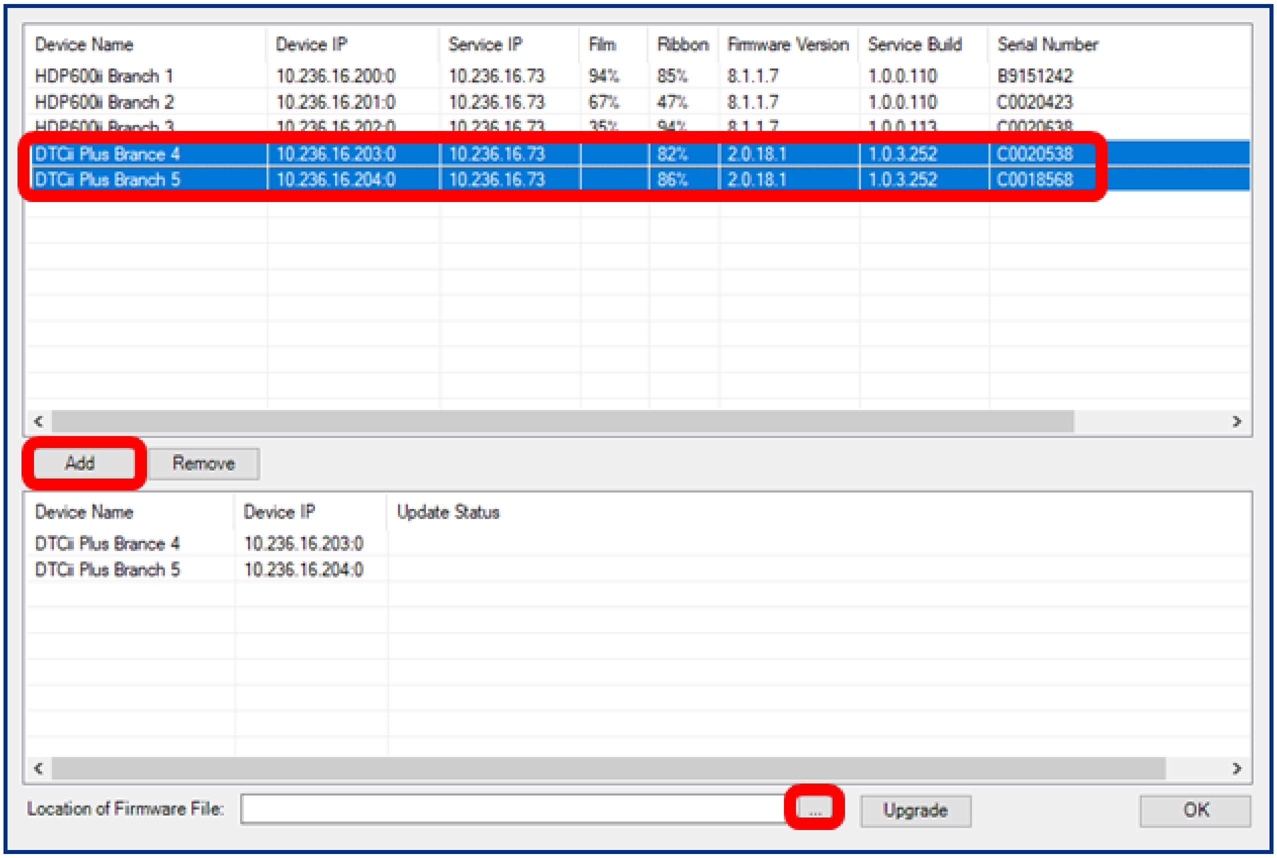
Device Information lists each printer and the following information associated with each printer:

- Device Name: The logical printer name in TRISM
- Device IP: The network IP address of the printer
- Service IP: The network IP address of the print server. (The server running the Card Printer Service.)
- Film: The percentage of transfer film left on the spool
- Ribbon: The percentage of ribbon left on the spool
- Firmware Version: The printer firmware version
- Service Build: The printer software build version
- Serial Number: The serial number of the printer
- Card Count: The number of cards currently in the printer
- Cards Until Cleaning: The number of cards that can be printed before the printer must be cleaned.

8.6.1 Upgrading the printer firmware

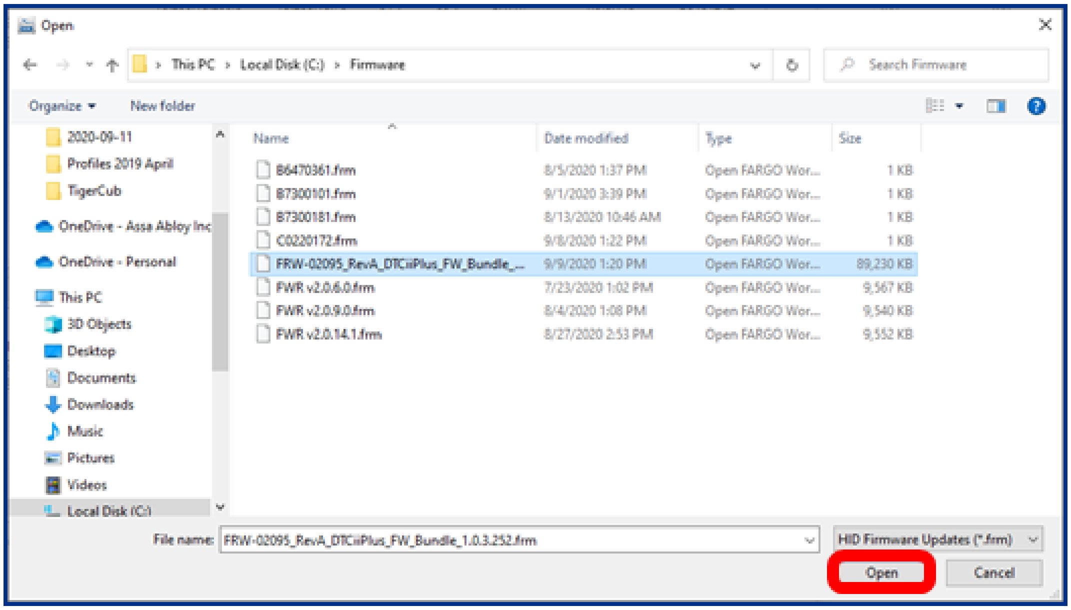
To upgrade the printer to a new firmware version, you need to have the firmware file on the system running the TRISM Client.

1. Select the printers to be updated and click **Add**. The selected printers are added to the update list that is displayed in the lower table.



2. Select the firmware file to install on the printers. Click **...** (Browse) to navigate to the firmware file on the TRISM Client.

3. Select the firmware file to install and click **Open**.



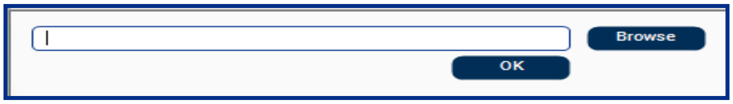
4. Once the printers and firmware are selected, click **Upgrade** to begin the upgrade.

> **Note:** During the upgrade process, a status meter displays the percent completed of the firmware package to the device being upgraded. In additionm if you attempt to exit the **Device Information** screen an error message is dispayed until all selected devices are fully upgraded.

8.7 License

All licenses (for example, device, PIN pad, MSR, workstation, and so on) are loaded into TRISM in this window.

1. On the main menu, click the **Personal icon** > **Help** > **License**.
2. Click **Browse** to navigate to the license file.
3. Click **OK**.

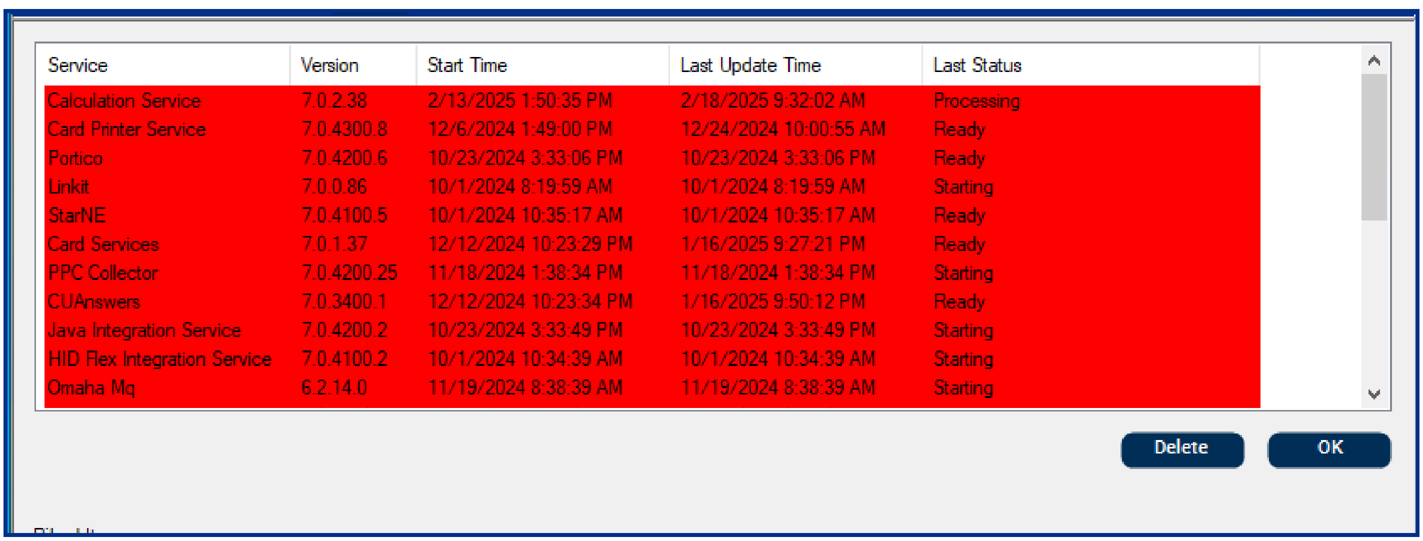


4. Click **Save PIK**.

8.8 System Status

Displays the **Version**, **Start Time**, **Last Update Time**, and **Last Status Time** of each service.

On the main menu, click the **Personal icon** > **Help** > **System Status**.



Service	Version	Start Time	Last Update Time	Last Status
Calculation Service	7.0.2.38	2/13/2025 1:50:35 PM	2/18/2025 9:32:02 AM	Processing
Card Printer Service	7.0.4300.8	12/6/2024 1:49:00 PM	12/24/2024 10:00:55 AM	Ready
Portico	7.0.4200.6	10/23/2024 3:33:06 PM	10/23/2024 3:33:06 PM	Ready
Linkit	7.0.0.86	10/1/2024 8:19:59 AM	10/1/2024 8:19:59 AM	Starting
StarNE	7.0.4100.5	10/1/2024 10:35:17 AM	10/1/2024 10:35:17 AM	Ready
Card Services	7.0.1.37	12/12/2024 10:23:29 PM	1/16/2025 9:27:21 PM	Ready
PPC Collector	7.0.4200.25	11/18/2024 1:38:34 PM	11/18/2024 1:38:34 PM	Starting
CUAnswers	7.0.3400.1	12/12/2024 10:23:34 PM	1/16/2025 9:50:12 PM	Ready
Java Integration Service	7.0.4200.2	10/23/2024 3:33:49 PM	10/23/2024 3:33:49 PM	Starting
HID Flex Integration Service	7.0.4100.2	10/1/2024 10:34:39 AM	10/1/2024 10:34:39 AM	Starting
Omaha Mq	6.2.14.0	11/19/2024 8:38:39 AM	11/19/2024 8:38:39 AM	Starting

- **Green**: status table in database is running.
- **Red**: status table has not been updated for five minutes. Red status does not indicate that the service is down.

Appendix A

Reference

A.1 System requirements

A typical TRISM installation consists of a server or virtual machine (Host) and one or more workstations. A dedicated server or VM is strongly recommended to prevent network downtime, as aspects of installation, setup, configuration, and updates may require system reboots. The server must be provided by the financial institution. The hardware and software requirements for TRISM installations are listed in the following table.

	Server (Host)	Workstation (Client)
Minimum processor speed	2.0 GHz	2.0 GHz
Minimum available RAM	16 GB	4 GB
Available hard disk space	50 GB	10 GB
Video resolution	SVGA (1024 × 768)	SVGA (1024 × 768)
Operating system	Microsoft Windows 2019, 2022	Microsoft Windows 11
Database software	Microsoft SQL Server 2017, 2019, 2022 Standard Express, or Enterprise	N/A

Note:

- A dedicated server or virtual server with a dedicated SQL Server instance is strongly recommended. High volumes of printers or mixed printer environments or embossers may require additional print servers.
- It is recommended to use the Standard or Enterprise edition of SQL Server in an environment containing 25 or more branches.

A.2 Card layouts

Refer to the following guidelines when setting up card formats.

Card Layouts	
Card size	3 3/8" × 2 1/8"
Bleed	1/8" optimal; 3/32" minimum
Clearance	Text/logos at least 3/32" from edge of card, brand marks, magnetic stripe, EMV chip, or signature panel
Visa Specifications	
Visa brand mark	9.75 mm × 20.5 mm
Distance from right of brand mark to right edge of card	2 mm
Distance from bottom of brand mark to bottom edge of card	2 mm
MasterCard Specifications	
MasterCard brand mark	11.3 mm × 19.25 mm
Distance from right of brand mark to right edge of card	2 mm
Distance from bottom of brand mark to bottom edge of card	3 mm
Custom Images	
Image file type	.jpeg, .bmp
Aspect ratio	3:2
Minimum resolution	1015 × 640

A.3 Custom image guidelines

Your financial institution reserves the right to determine, in its sole discretion, whether a submitted image is accepted or rejected. All images submitted must have the consent of the owner including those images downloaded from the internet.

Any images that contain the following items are not accepted:

- Company names, logos, slogans, third party brands, trademarks, copyrighted items, or any image which may be protected by trademark or copyright.
- Professional athletes, politicians, celebrities, public figures (excluding permission-based photos of you, your family members, or friends photographed with a famous person).
- Depictions of illegal activities or otherwise inappropriate behavior.
- Addresses, phone numbers, social security numbers or other personal identification numbers, URL addresses.
- Items that may be considered obscene, offensive, indecent, provocative, nude, semi-nude, lewd, or otherwise inappropriate images, including profanity.
- Political affiliations or other socially sensitive images.
- Racially sensitive material.
- Artwork which was created by a third party for which you have not obtained permission from the owner to use.
- Cartoon or other characters for which express permissions have not been obtained. This includes images that you have not created and do not have permission to use.
- Any other image which is deemed unacceptable and reflects negatively on the branding message of your financial institution.

A.4 Permission descriptions

A.4.1 Security

Permission	Description
Template Security Level	Determines if you can reset a user's password when you have the Add User permission or locks the account if you have the Edit User permission.
Edit Security Template (Add/Edit/Delete)	Allows you to add, edit, or delete templates.
Edit Security Permissions	Allows you to edit a template. This is specifically for modifying the templates without having the ability to add or remove the templates.
View All Branches	Allows you to access all branches even if the system is configured to only show your branch. This is useful for users who float.
License File	Allows you to see the License Section and allows you to add/update the licenses with the supplied file.
Reset Other User Passwords	Allows you to reset other user's passwords. **Note:** This does not apply to systems configured with Active Directory.
Import Configuration	Allows you to import a saved configuration file.
Export Configuration	Allows you to export and save a configuration file to import later.
View Regional Branches (Regional Queue)	Allows you to access regional branches even if the system is configured to only show your branch. This is useful for users who float.

A.4.2 Order cards

Permission	Description
View Order Card	Allows you to access the **Order Card** option from the **Request** menu on the main toolbar and to access the **Order Card** button on the quick launch toolbar.
View Actions	Allows you to access the **Request** menu on the main toolbar.
Edit Permissions	Allows you to access the **Request** > **Edit Permissions** option on the main toolbar.
RePIN a Card	**With PIN Verification**: Allows you to see the **Request** > **Re-PIN** option. **Override**: No longer used. **Enforce Card**: Allows you to see the Re-PIN screen. Card must be swiped to re-PIN. Re-PIN is not possible if card is not present.
Order Card Express	Order Card screen opens automatically upon log in.
PIN Mailer Only	Allows you to access the **Request** > **PIN Mailer** option on the main toolbar.
Print Transaction Report	Allows you to access the Transactional Print screen when you successfully order a card. The Transactional Report is a sign off sheet the customer signs to state they had a card made. Many financial institutions do not use this or have their own.
Hide Customer Info on Transaction Report	Allows you to access the **Print Transactional Report** option to mask the customer data on the report. This is for security.
Read a Card	Allows you to access the **Request** > **Read a Card** option on the main toolbar.
CVV2 Calculator	Allows you to access the **Request** > **CVV2 Calculator** option on the main toolbar.
Auto Select First Card Status	Allows you to have the Card Status in Order Card to automatically be populated with the first option. This is for improved automation.

A.4.3 Queue

Permission	Description
View Queue	Allows you to access the **Queue** menu on the main toolbar and to access the **Queue** button on the quick launch toolbar.
Edit Card	Allows you to edit card records in the Queue.
Delete Cards	Allows you to delete card records in the Queue.
Delete from any Branch	Allows you to delete cards from other branches and requires you to have the View All Branches permission.
Purge Queue Requests	Allows you to access the **Purge Queue Request** button on the quick launch toolbar to delete all pending queue requests. This is used to troubleshoot systems that have a lot of traffic in the queue.

A.4.4 Reports

Permission	Description
View Reports	Allows you to access the **Reports** menu from the main toolbar and the **Reports** button on the quick launch toolbar.
View Local Reports	Allows you to see the predefined reports as well as custom reports that have been saved.

Permission	Description
Run End of Day Reports	Allows you to access the **End of Day** option in the **Reports** menu of the main toolbar and the **End of Day button** on the quick launch toolbar.
Use Classic View	Allows you to view the End of Day report in the classic format. This is the default view.
Run End of Day Reports	**User:** Allows you to run the End of Day report in user mode. This report displays individual branch options only. **Admin:** Allows you to run the End of Day report in Admin mode which shows all branches and formats.
Show Mask Card Number	Shows masked card numbers through the entire TRISM system. This does not include some logs that have this data.
Force EOD Masked Card Number	Allows you to have all card numbers on the end of day report masked. This is for security.
View Non-Financial Reports	Allows you to have access to the Non-Financial report in the **Reports** menu of the main toolbar.
View Individual Reports	Allows you to access the Management Reports Section that allows you to save/load reports created by the financial institution.
View Existing Reports	Allows you to see the Historical Card Balance Report in the **Reports** menu of the main toolbar.
Print Reports	Allows you to print reports.
View Data Log	Allows you to access the **Data Log** option in the **Help** menu of the main toolbar.
View Error Log	Allows you to access the **Error Log** option in the **Help** menu of the main toolbar.
View Client Information	Allows you to access the **Client Information** option in the **Help** menu of the main toolbar.
Device Access	Allows you to access the Device Access report in the **Reports** menu of the main toolbar.
Vault Supply	Allows you to access the Vault Supply Tracking report in the **Reports** menu of the main toolbar.
Device Error	Allows you to access the Device Error report in the **Reports** menu of the main toolbar.
Spoiled Card	Allows you to access the Spoiled Card report in the **Reports** menu of the main toolbar.
Spoiled Card For all Branches	Allows you to access the Spoiled Card report with all branches available in the **Reports** menu of the main toolbar.
Branch Activity	Allows you to access the Branch Activity report in the **Reports** menu of the main toolbar.
Device Access Report (CardStock)	Allows you to access the Device Access report from the **Profile** > **Reports** menu.
Background	Allows you to have access to the Background report from the **Profile** > **Reports** menu.
Historical Transfers	Allows you to have access to the Historical Transfers report from the **Profile** > **Reports** menu.
Historical Vault	Allows you to have access to the Historical Vault report from the **Profile** > **Reports** menu.
Historical Central Vault	Allows you to have access to the Historical Central Vault report from the **Profile** > **Reports** menu.
Customer Removal	Allows you to have access to the Customer Removal tool from the **Profile** > **Reports** menu.
Device Cleaning Report	Allows you to have access to the Device Cleaning Report from the **Profile** > **Reports** menu.

A.4.5 Inventory

Permission	Description
View Inventory	Allows you to access the **Profile** > **Inventory** menu.
Device Unlock	Allows you to access the **Device Unlock** function (card add and removal) from the **Profile** > **Inventory** menu.
View Card Stock	No longer used.
View Vault Inventory	Allows you to access the **Inventory** > **Vault Inventory** option from the **Profile** > **Inventory** menu. **Central View:** Allows you to access the left side of the Vaults which contain all the Central Vaults in the Vault Inventory screen. • **Central Admin**: Allows you to access the **CardStock** options (add, edit, or remove) and allows you to Send Transfers. This also allows you to add more Central Vaults. • **Central User**: Allows you to have access to Central Branch Transfers in the transfers section of the Vault Inventory screen. **Branch View:** Allows you to view the right side of the Vaults which contain Branch Level Vaults in the Vault Inventory screen.
View all Vaults	Allows you to view all vaults in the Vault Access screen.
Show Alerts (Notifications)	**Ribbon/Film Alert:** Allows you to be notified once the film or ribbon has fallen below a certain percentage. **Cardstock Alert:** Allows you to get notified once the cardstock inventory amount drops below a given value.

A.4.6 Configure

Permission	Description
View Settings	Allows the user to access the Configure option on the main toolbar
User Editing	**Add User:** Allows you to access the Add User button in the User section of the Configuration screen. **Edit User:** Allows you to access the Edit User button in the User section of the Configuration screen. **Delete User:** Allows you to access the Delete User button in the User section of the Configuration screen.
Card Stock	**Add**: Allows you to add cardstock to vaults in the Vault Inventory screen. **Delete**: Allows you to delete cardstock to vaults in the Vault Inventory screen. **Edit**: Allows you to edit cardstock to vaults in the Vault Inventory screen. **Rename**: No longer used. **Process:** No longer in used.
General Edit	Allows you access to the **General** option on the left side of the Configuration screen.
User Editing	Allows you access to the **Users** option on the left side of the Configuration screen.
Template Editing	Allows you access to the **Templates** option on the left side of the Configuration screen.
Format Editing	Allows you access to the **Formats** option on the left side of the Configuration screen.
Device Editing	Allows you access to the **Devices** option on the left side of the Configuration screen.
Active Directory Edit	Allows you access to the **Active Directory** option on the left side of the Configuration screen.
Interface Editing	Allows you access to the **Interfaces** option on the left side of the Configuration screen.
CardStock Editing	Allows you access to the **CardStock** option on the left side of the Configuration screen.
Branch Editing	Allows you access to the Branches option on the left side of the Configuration screen. **Add**: Allows you to add branches in the Branch section of the Configuration screen. **Edit**: Allows you to edit branches in the Branch section of the Configuration screen. **Delete**: Allows you to delete branches in the Branch section of the Configuration screen.
Printers	**Add**: Allows you to add printers in the Devices section of the Configuration screen. **Edit**: Allows you to edit printers in the Devices section of the Configuration screen. **Remove**: Allows you to remove printers in the Devices section of the Configuration screen.
Formats	**Add**: Allows you to add formats in the Formats section of the Configuration screen. **Edit**: Allows you to edit formats in the Formats section of the Configuration screen. **Remove**: Allows you to remove formats in the Formats section of the Configuration screen.
Show Healthbar	Allows you to see the red and green status lights in the main toolbar.
Show System Status Table	Allows you to access the **Help** > **System Status** option of the main toolbar.
Crystal Reports Editing	Allows you to enable or disable Crystal Reports licensing when used in a Citrix, Terminal Services, or VDI environment.

Permission	Description
Region Editing	Allows you to add, remove, or edit regions. Branches can be set to belong to certain regions. **View all Branches** option in the **Security** tab must not be selected to use this option. **Add:** Allows you to add new regions. **Edit:** Allows you to edit existing Region(s): • Region name • Branches in region - add/remove **Delete:** Allows you to delete Regions.

A.5 Troubleshooting

A.5.1 EMV

Issue	Possible Causes or Resolutions
Job stuck in Ready Photo	• Card Printer Service is not running • Printer name in Windows Devices and Printers is not identical to the device name in TRISM client[1] • Printer device type is not correct in TRISM Devices[1] • Incorrect Card Printer Service IP in TRISM Devices[1] • Card Printer Service not running as local admin • Card Printer Service domain login is incorrect [1]Any changes to devices in the configuration menu require the Card Printer Service to be restarted.
Offset printing in place of expiration date	• Verify **offset written** is checked for both Track 1 and Track 2 encode settings
Photo Printer Error	• Verify printer is available from web interface, if not, reset printer • Verify EMV Card stock is in the device hopper and loaded correctly • Verify all fonts are loaded on the server by pulling in .xml using DeSignIt (especially if you just moved the EMV.xmls into place) • Verify EMV template is in: **C:\ProgramData\HID Global\TRISM\Card Printer Service**
Photo Printer Error: Failure to select AID Card Manager	• EMV reader could not engage EMV chip
Photo Printer Error: Failure to install AID Card Manager	• EMV reader could not write to the chip. Chip is either used or defective.
Printer offline in Windows Devices & Printers	• This is normal for Silex printers in TRISM 7 and they should still work correctly.
No settings for Card Printer Service in Interface Settings	• EMV is not PIK'd - load new PIK
PINpad not Found	Ensure that there is a valid HID PIN pad connected and restart the TRISM client. If you are still getting this error, there may be an issue with the PIN pad. It may have lost its keys or the driver may be incorrect. If you are a PINPadless workstation and are getting this error, verify that your workstation license is in C:\programdata\HID Global\TRISM\.

Revision history

Date	Description	Revision
July 2025	Adds secure implementation guidelines and updates to software version 7.x.	A.1
June 2024	Initial release.	A.0

hidglobal.com

For technical support, please visit: https://support.hidglobal.com

PLT-07643, Rev. A.1