

HID® TRISM™ 6.x

Financial Instant Issuance

Administrator Manual

Software Version: 6.3
PLT-03654, C.2
July 2025



Copyright

© 2010 - 2025 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

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

Trademarks

HID GLOBAL, HID, the HID Brick logo, TRISM, OMNIKEY, HDP, DTC, DTCii Plus, FARGO Workbench, and FARGO are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

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 6.x.	C.2

A complete list of revisions is available in [Revision history](#).

What is TRISM 6?	8
1.1 What is TRISM 6?	9
1.2 How to use this manual	9
1.3 TRISM 6 user interface	10
Installation and configuration	11
2.1 Installation task list	12
2.2 Secure implementation guidance	12
2.2.1 Intended use and operating environment	12
2.2.2 Dedicated server	12
2.2.3 SQL access control	13
2.2.4 Network security	13
2.2.5 Print job security	13
2.2.6 Firmware updates	13
2.2.7 Physical security	13
2.2.8 Software updates and scheduling	13
2.2.9 Review preset permissions	13
2.2.10 Password expiration	13
2.2.11 Hardening TRISM service server, printers, and XT HSM	13
2.2.12 Daily device inventory best practices	14
2.2.13 Audit logs review	14
2.2.14 Reviewing data log retention policy	14
2.3 SQL server 2016 installation	15
2.4 SQL server 2016 connection configuration	22
2.4.1 Remote SQL connections configuration (action by the financial institution)	24
2.5 HSM Manager	28
2.5.1 Install HSM Manager	28
2.5.2 Run HSM Manager	28
2.5.3 TRISM XT key management system	30
2.6 HSM XT installation - Mastercard CVC3 fix	32
2.6.1 Mastercard CVC3 fix overview	33
2.6.2 Omitting EFTPOS.CONFI.db during back up and restore	34
2.6.3 Mastercard CVC3 fix procedure	35
2.7 TRISM client initial installation	39
2.8 TRISM client database creation	39
2.9 Calculation service installation	43
2.10 TRISM client initial configuration	43
2.11 Calculation service configuration	45
2.11.1 HSM Duo service configuration	45

2.11.2 HSM XT service configuration	45
2.12 TRISM client configuration - server	47
2.12.1 Add license	47
2.12.2 Add formats	48
2.12.3 Add printers and embossers	50
2.12.4 Install card printer service	53
2.12.5 Configure device settings in TRISM	53
2.12.6 Device-specific setup instructions: FARGO HDPii PLUS - Ethernet	54
2.12.7 Device-specific setup instructions: FARGO HDPii PLUS - USB	55
2.12.8 Add vaults	55
2.12.9 Add branches	55
2.12.10 Setup card stock	56
2.13 TRISM client configuration: workstation	57
2.13.1 Edit permissions	57
2.13.2 Install VFI USB driver	57
2.13.3 Changing the COM port of an installed PIN Pad	57
Request	59
3.1 Order Card	60
3.2 Edit Permissions	63
3.3 Re-PIN	64
3.4 Read a Card	64
3.5 PIN mailer	65
3.6 CVV2 Calculator	65
3.7 Import	66
Queue	67
4.1 Card queue	68
Reports	69
5.1 End Of Day	70
5.1.1 Tips for balancing end of day reports	71
5.1.2 Spoil cards	72
5.1.3 Spoil other	72
5.1.4 Process End of Day for all cardstock associated to the selected branch/vault/device	73
5.2 Management	74
5.2.1 Create a customized report	74
5.2.2 Filter columns	75
5.2.3 View card details	75
5.2.4 Save a customized report	75
5.2.5 Export a report to Excel	75

5.3 Historical Card Balancing	76
5.4 Device Access	76
5.5 Spoiled Card	76
5.6 Branch Activity	76
5.7 Device Error	76
5.8 Non-Financial	77
5.9 Background	77
5.10 Remove Cardholder Data	78
Inventory	79
6.1 Device Access	80
6.1.1 Add/remove cards and change ribbon/foil	80
6.2 Vault Inventory	81
6.2.1 Add a vault	81
6.2.2 Transfer cards - send cards	81
6.2.3 Transfer cards - receive cards	82
6.2.4 Low inventory alerts	83
Configure	86
7.1 General	87
7.2 Users	89
7.2.1 Add users (without active directory)	89
7.2.2 Edit users (without active directory)	90
7.2.3 Delete users (without active directory)	90
7.3 Templates	91
7.4 Formats	92
7.4.1 General Settings	92
7.4.2 Encode Settings	93
7.4.3 Emboss Settings	94
7.4.4 EMV	95
7.4.5 Mailers	96
7.4.6 Photo Settings	96
7.4.7 Card Status	98
7.4.8 Card Class	99
7.5 Devices	100
7.5.1 Add a printer or embosser	100
7.6 Active Directory	104
7.7 Branches	105
7.7.1 Add vaults to a branch	105
7.7.2 Add devices to a branch	106
7.7.3 Add PCs/users/ranges to a branch	108

7.7.4 Add BINs to a branch	108
7.7.5 Branch Add - Quick Add feature	109
7.8 Interfaces	112
7.8.1 Interface Settings	112
7.8.2 Interface BIN Settings	113
7.9 Databases	113
7.10 Card Stock	114
7.10.1 Card Stock ID	114
7.10.2 Card Stock to BIN	114
7.10.3 Card Stock to Vault/Device	114
7.10.4 Add a new BIN or card stock	115
7.11 Theme	115
7.12 Queue Setup	116
7.13 Regions	116
7.13.1 Add a region	117
7.13.2 Add a new branch to a region	119
7.13.3 Remove a branch from a region	121
7.14 Crystal Reports licensing	122
Help	124
8.1 About	125
8.2 Support Documents	125
8.3 Data Log	126
8.4 Error Log	127
8.5 Client Information	127
8.6 Device Information	128
8.6.1 Upgrading the printer firmware	129
8.7 License	131
8.8 System Status	131
Reference	132
A.1 System requirements	133
A.2 Card layouts	134
A.3 Custom image guidelines	135
A.4 Permission descriptions	135
A.4.1 Security	135
A.4.2 Order cards	136
A.4.3 Queue	136
A.4.4 Reports	136
A.4.5 Inventory	138
A.4.6 Configure	138

A.5 Troubleshooting	139
A.5.1 EMV	139

Section 01

What is TRISM 6?

1.1 What is TRISM 6?

TRISM™ 6 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 6 boasts the versatility to meet any institution's most specific demands.

1.2 How to use this manual

The TRISM Administrator Manual is intended for use by TRISM installation and technical support only.

This manual is organized chronologically. First, you will find instructions for installation and configuration, then information pertaining to version updates or new service installation. The TRISM menus (Request, Queue, etc.) follow this and provide general instructions on how to use each of these menus. Finally, the Appendix includes post-installation information such as Template permission descriptions and troubleshooting procedures.

1.3 TRISM 6 user interface



1. Main menu.
2. Quick launch toolbar.
3. Dual Control Login: Some TRISM features require "dual control" login. A second user that is different than the user currently logged in (and with the appropriate permissions), must enter their login credentials to access these features.

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 T6	
Create databases in T6	
Install and Start HID Calculation Service	
Log in as access1 and update password	
Load PIK in T6	
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

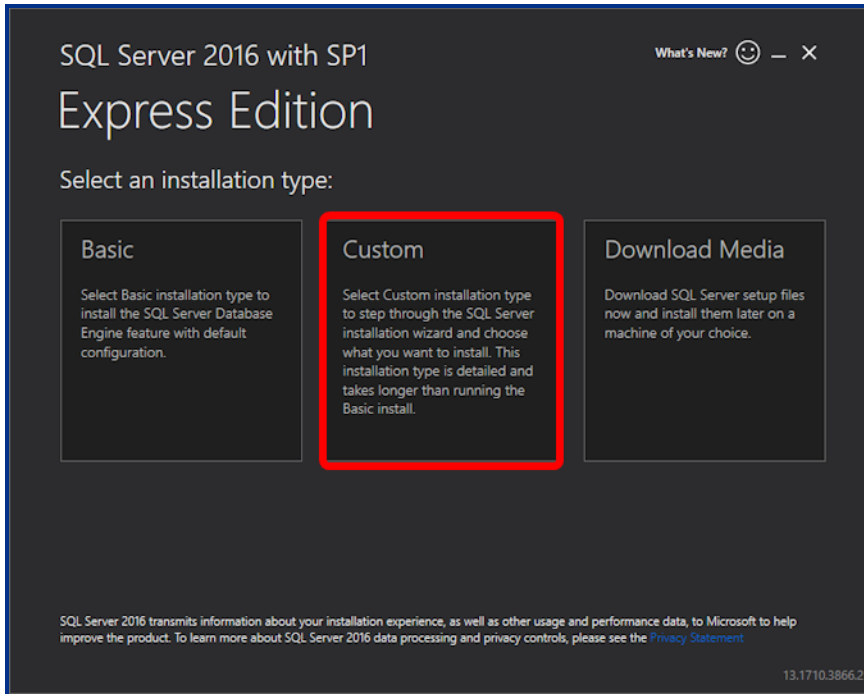
Regularly review audit logs for spoilage, card creation, and other critical activities. This helps detect and respond to any unauthorized or suspicious activities promptly.

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.

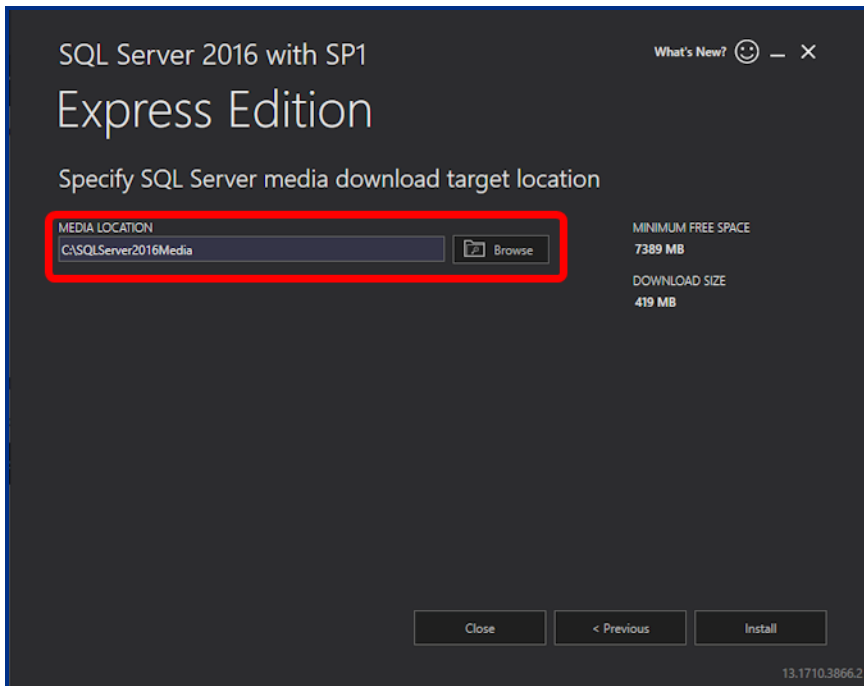
2.3 SQL server 2016 installation

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**.

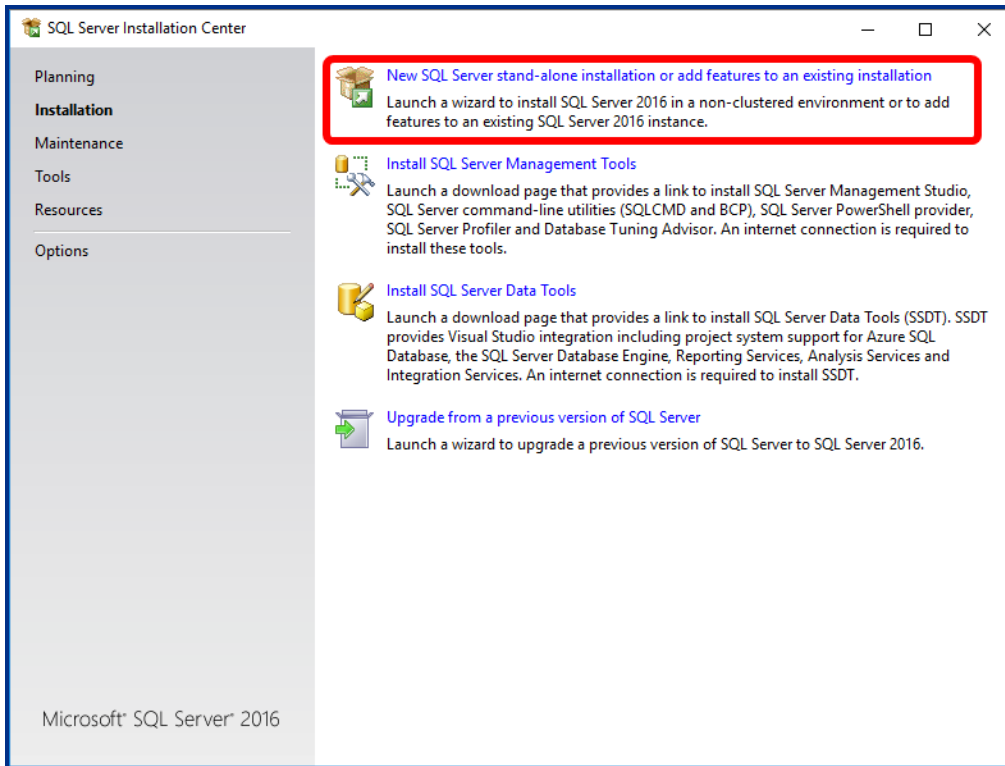


4. Choose the location for the files to be downloaded to start the install process.

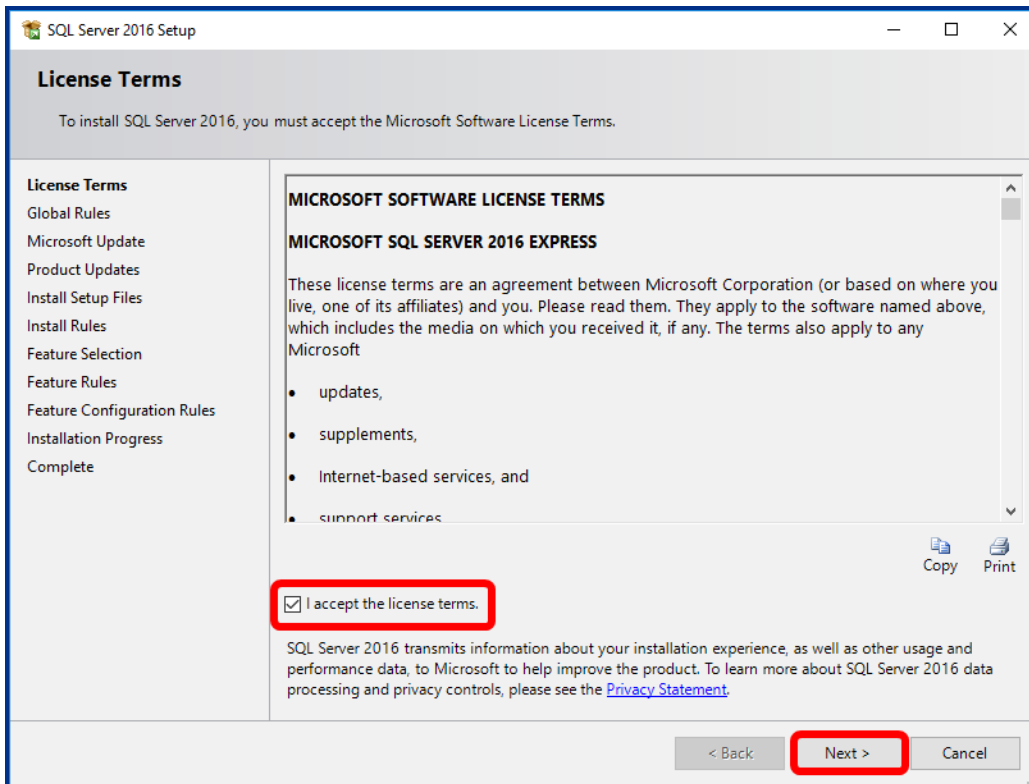
Note: If you already have them downloaded this is not shown.



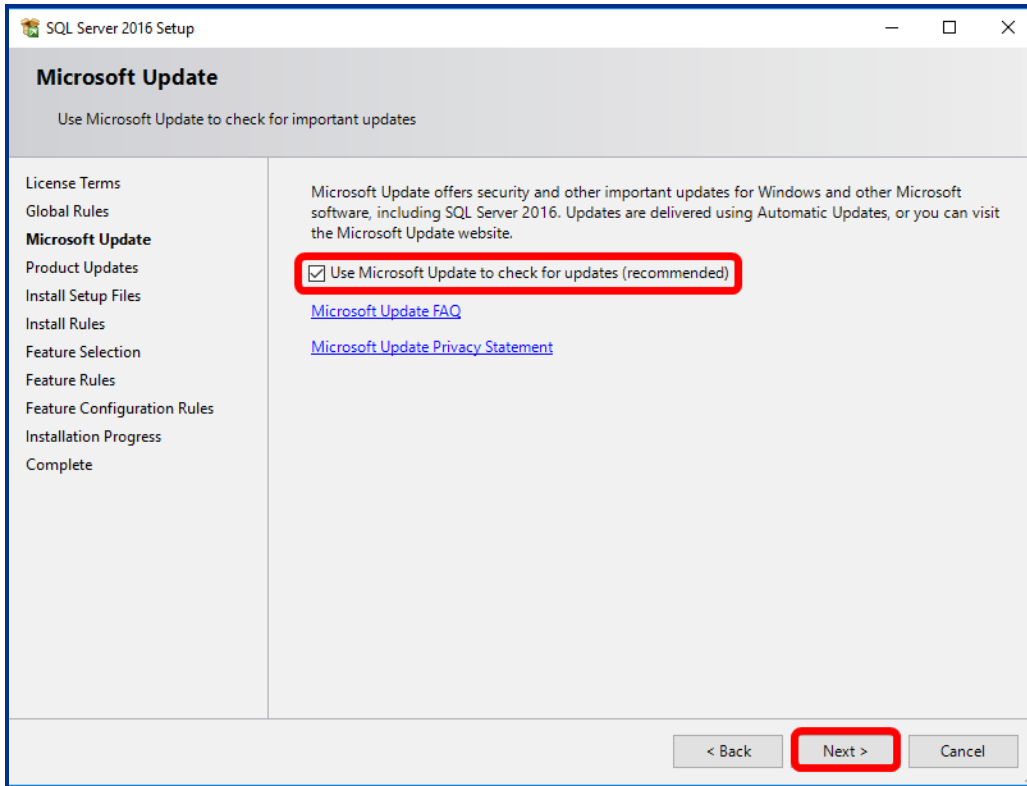
- In the **SQL Installation Center** screen, select **New SQL Server stand-alone installation or add features to an existing installation**.



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

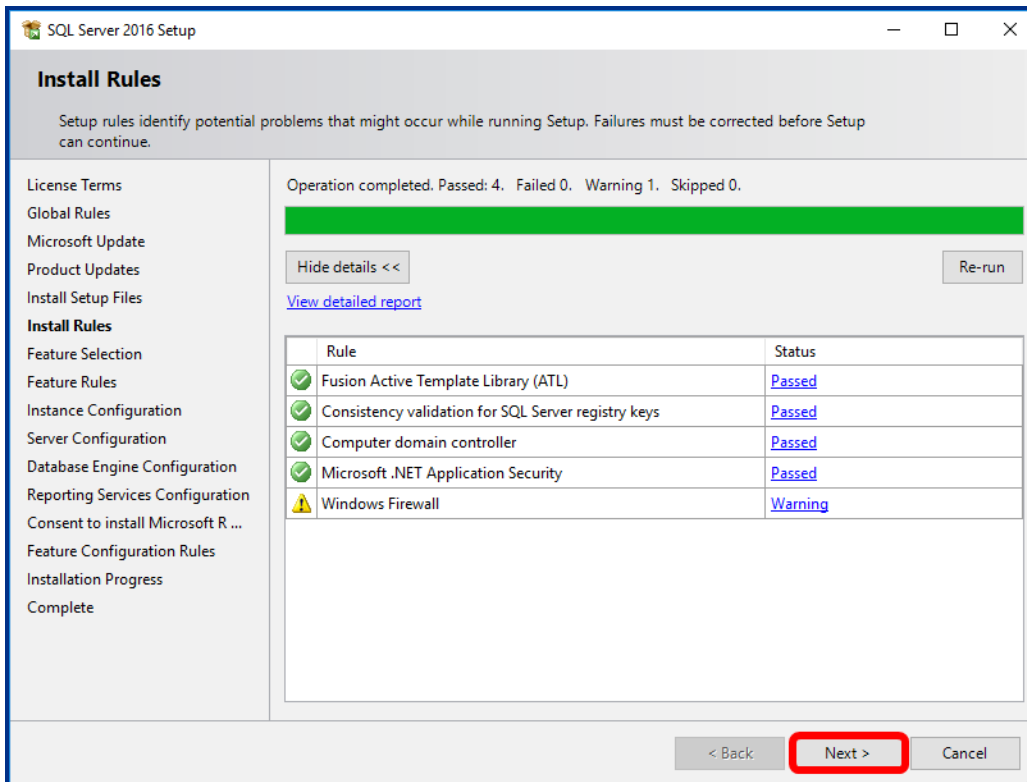


7. If prompted to install updates, select **Use Microsoft Update to check for updates** and click **Next**.



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**.

SQL Server 2016 Setup

Feature Selection

Select the Express features to install.

License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Installation Progress
Complete

Features:

- ☒ Database Engine Services
 - ☐ SQL Server Replication
 - ☐ R Services (In-Database)
 - ☒ Full-Text and Semantic Extractions for Search
 - ☐ PolyBase Query Service for External Data
- ☒ Reporting Services - Native

Shared Features

- ☒ Client Tools Connectivity
- ☒ Client Tools Backwards Compatibility
- ☒ Client Tools SDK
- ☒ Documentation Components
- ☒ SQL Client Connectivity SDK
- ☐ LocalDB

Feature description:

Includes the Search engine that supports Full-Text Extraction for fast text search as well as Semantic Extraction for key phrases (likely tags) and similarity search on content stored

Prerequisites for selected features:

Already installed:

- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

Disk Space Requirements

Drive C: 2660 MB required, 13544 MB available

Select All Unselect All

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

< Back **Next >** Cancel

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

SQL Server 2016 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Installation Progress
Complete

☐ Default instance

☒ Named instance: **SQLEXPRESS**

Instance ID: **SQLEXPRESS**

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL13.SQLEXPRESS

Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS13.SQLEXPRESS

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

< Back **Next >** Cancel

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**.

SQL Server 2016 Setup

Server Configuration
Specify the service accounts and collation configuration.

License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Installation Progress
Complete

Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQL\$SQL...		Automatic
SQL Server Reporting Services	NT Service\ReportServer...		Automatic
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL ...		Automatic

☐ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service
This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.
[Click here for details](#)

< Back **Next >** Cancel

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**.

SQL Server 2016 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Installation Progress
Complete

Server Configuration Data Directories TempDB User Instances FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

☐ Windows authentication mode

☒ Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: [Masked]

Confirm password: [Masked]

Specify SQL Server administrators

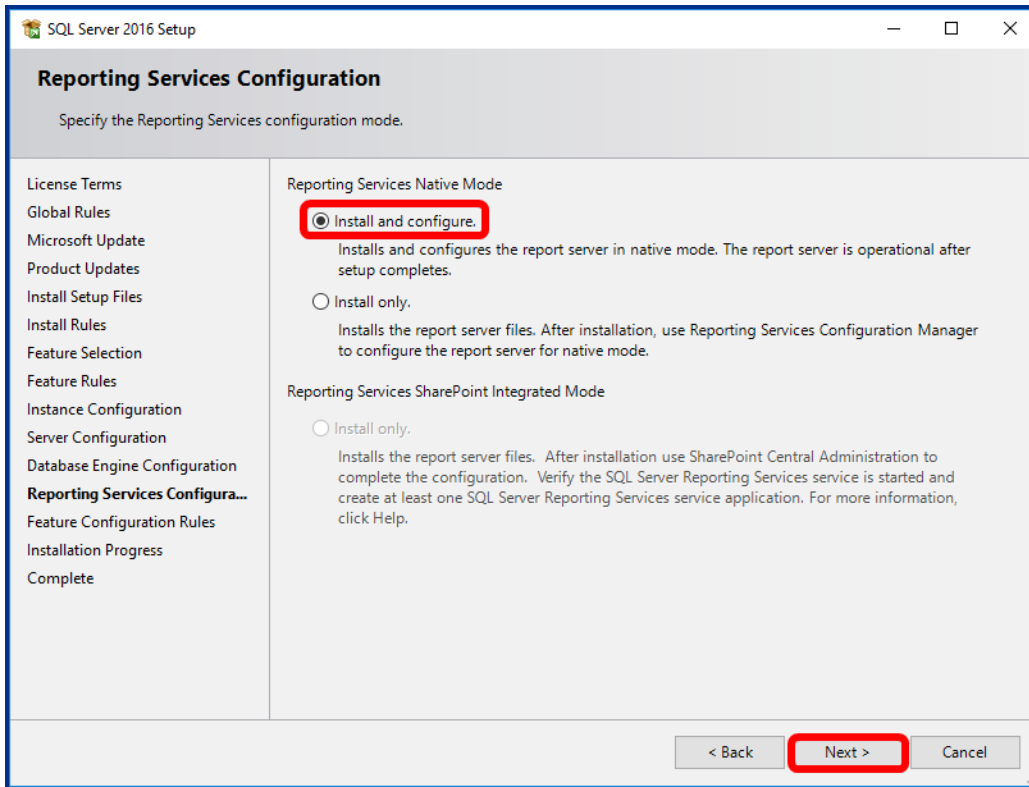
DESKTOP-H37N15V\Jeff (Jeff)

SQL Server administrators have unrestricted access to the Database Engine.

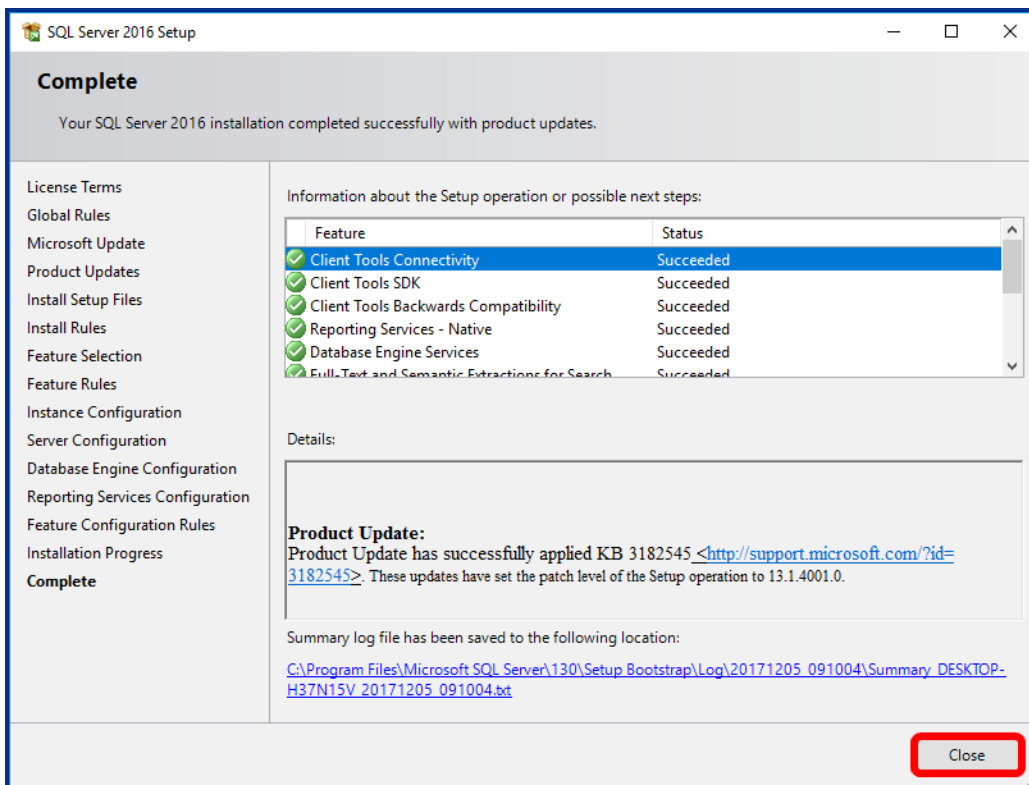
Add Current User Add... Remove

< Back **Next >** Cancel

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.



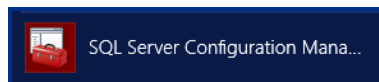
15. Close the SQL Server Installation Center window.

2.4 SQL server 2016 connection configuration

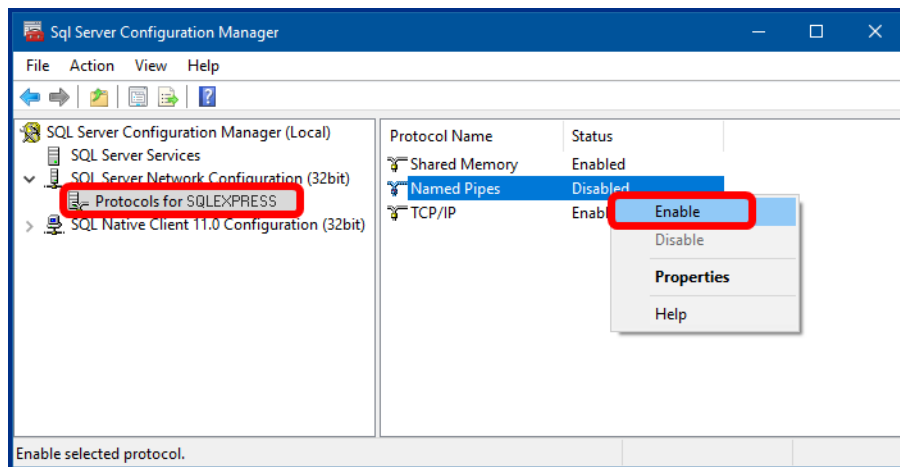
1. On Windows Server 2008 or prior, browse to **Start > All Programs > SQL Server 2016 > Configuration Tools**, then select **SQL Server Configuration Manager**.

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.

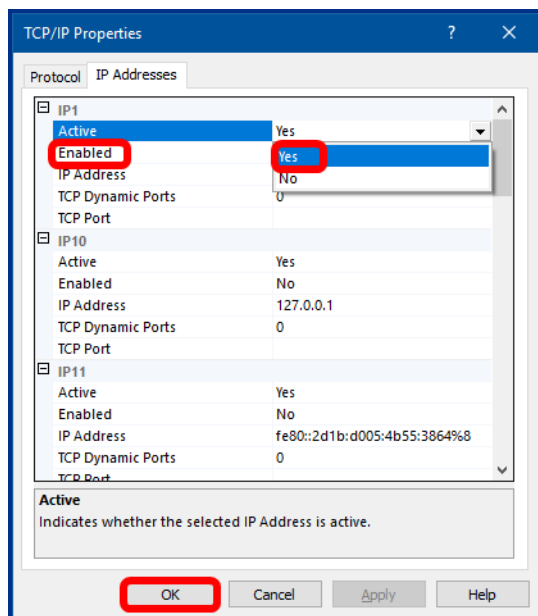


2. On the left-hand pane, expand **SQL Server Network Configuration**, then select **Protocols for SQLEXPRESS**.
 - a. Right-click on **Named Pipes** and select **Enable**. If prompted, enter a Windows administrator password. Click **OK** on the resulting prompt.
 - b. Repeat this for the **Shared Memory**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

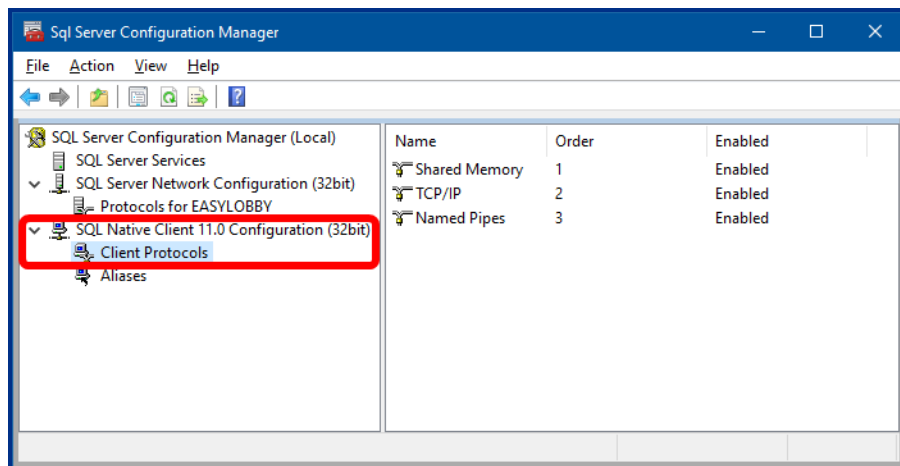


3. Right-click **TCP/IP** and select **Properties**.
4. In the **TCP/IP Properties** window, select the **IP Addresses** tab.

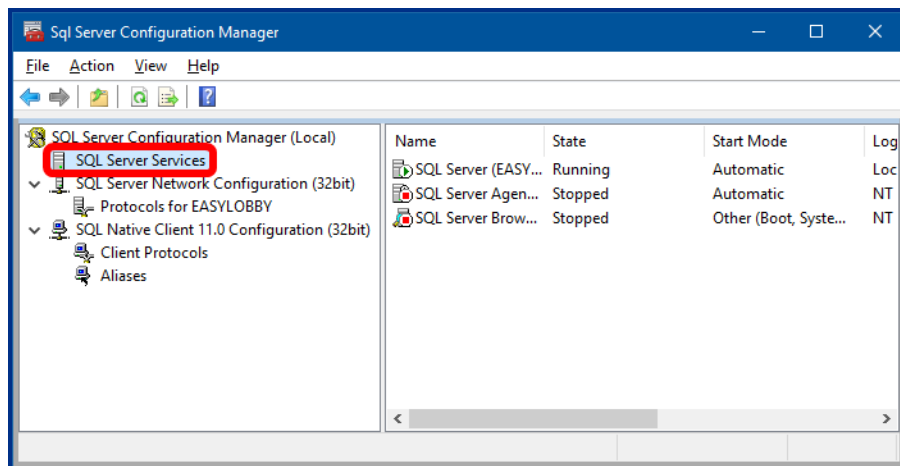
- For every IP section (**IP1** to **IP6**), change the drop-down selection for the **Enabled** option to **Yes**. Scroll down and set the **IPALL TCP Port** to **1433**, then click **OK**.



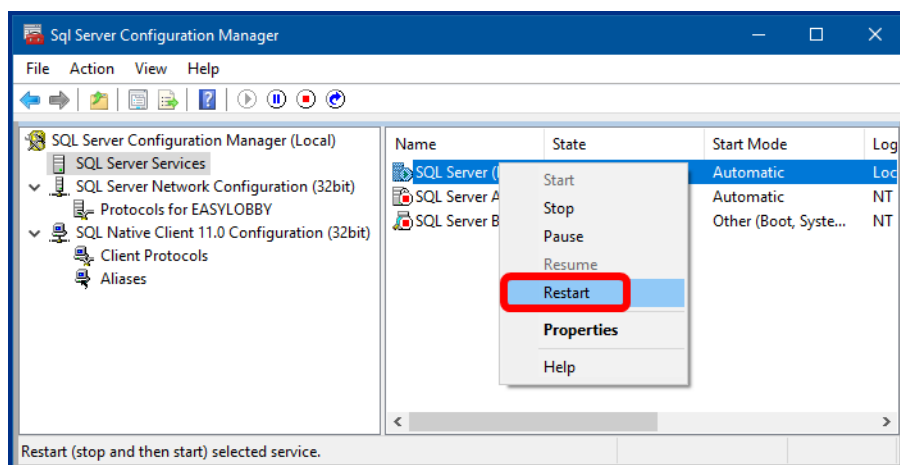
- Repeat Step 2. for **SQL Native Client 11.0 Configuration (32bit)** and **SQL Native Client 11.0 Configuration**.



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



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

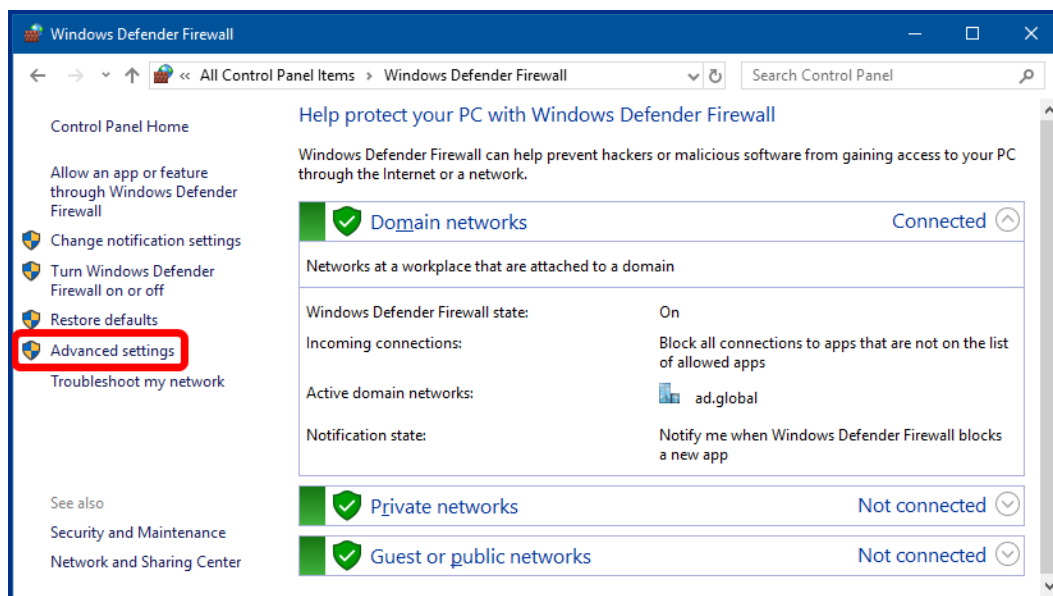


- Once the service restart prompt disappears, close **SQL Server Configuration Manager**. Microsoft SQL Server 2016 is now configured to accept connections.

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

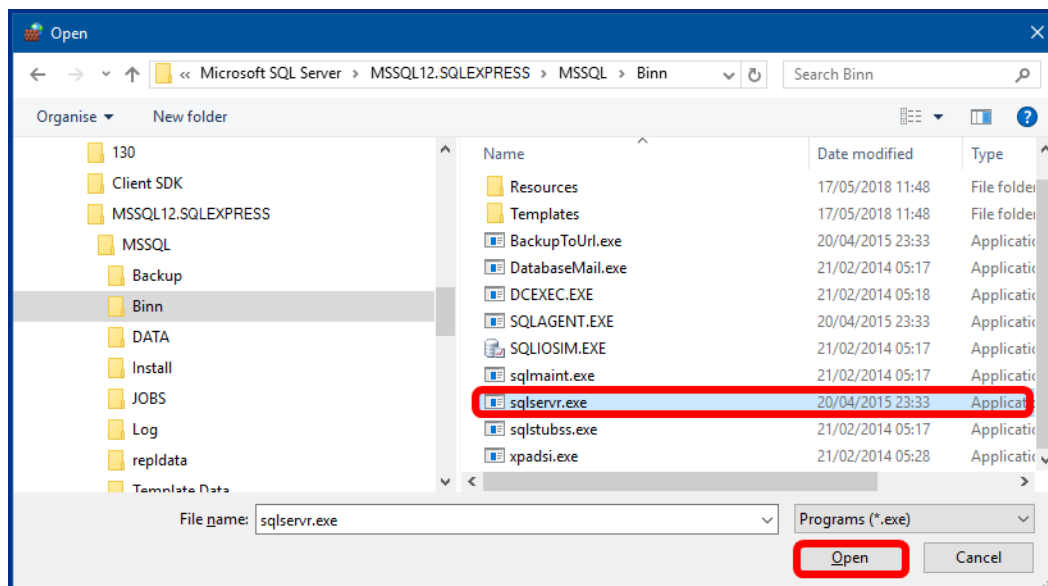
The Financial Institution must configure their firewall settings to allow remote connections to be able to contact the SQL database.

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

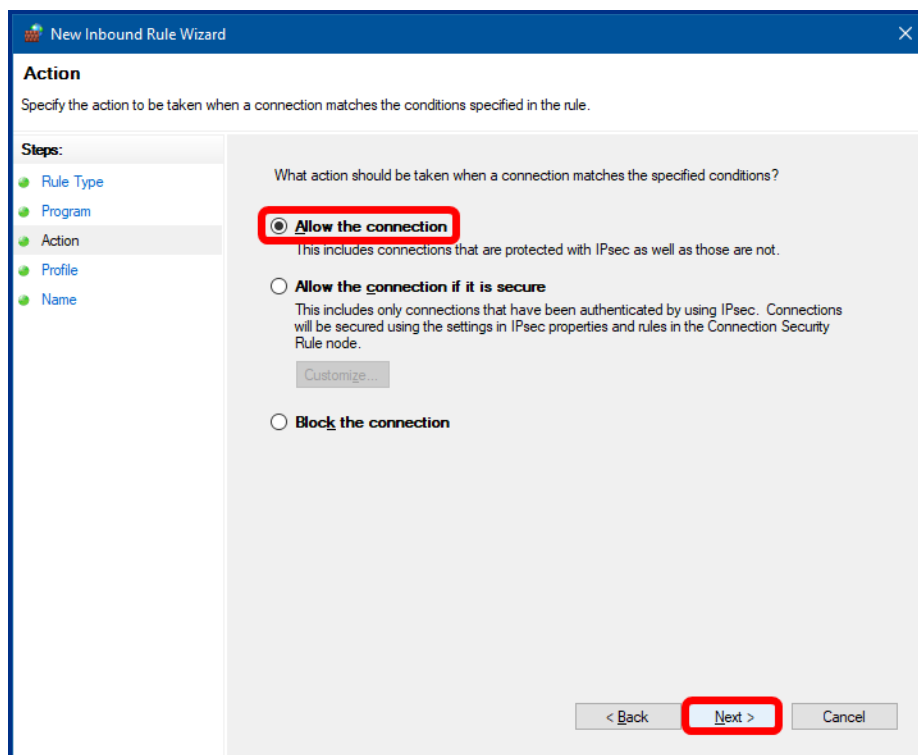


- Click **Inbound rules** and in the **Actions** panel select **New Rule**.
- Select **Program** and click **Next**.

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



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



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

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile' (highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and contains three checked options: **Domain** (highlighted with a red box), **Private**, and **Public**. Each option has a description: 'Applies when a computer is connected to its corporate domain.', 'Applies when a computer is connected to a private network location, such as a home or work place.', and 'Applies when a computer is connected to a public network location.' At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

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

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile', and 'Name' (highlighted). The main area has a 'Name:' label followed by a text box containing 'SQL Server' (highlighted with a red box). Below it is a 'Description (optional):' label followed by a large empty text area. At the bottom, there are three buttons: '< Back', 'Finish' (highlighted with a red box), and 'Cancel'.

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 **UDP**, 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](#).

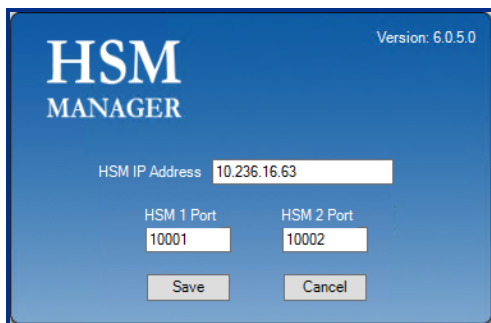
2.5.1 Install HSM Manager

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

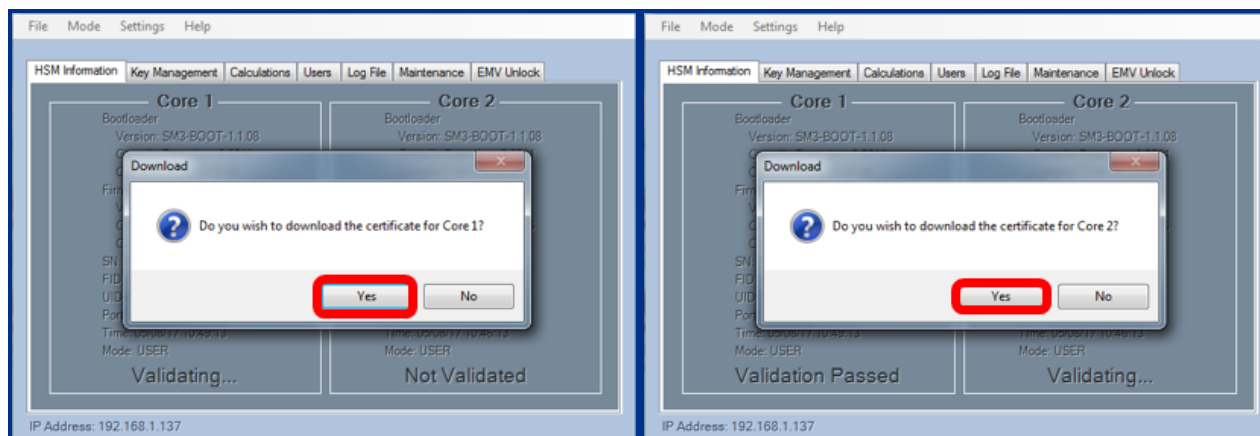


3. Enter the Financial Institution (FI) **Site ID**, then click **OK**.

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".



- 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.

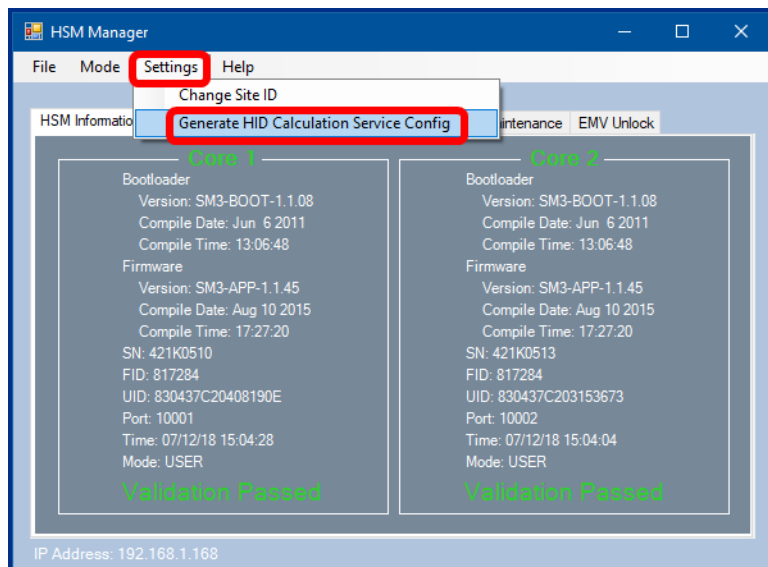


The following assumptions are:

- 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.

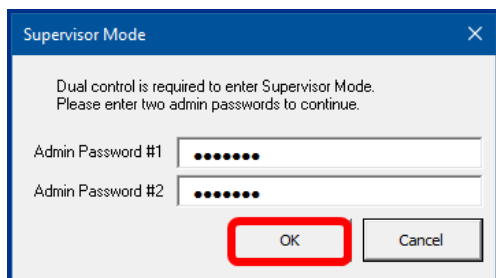
Note: For instructions refer to the *TRISM Duo HSM Administrator Manual* or *HSM XT Administrator Manual*

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

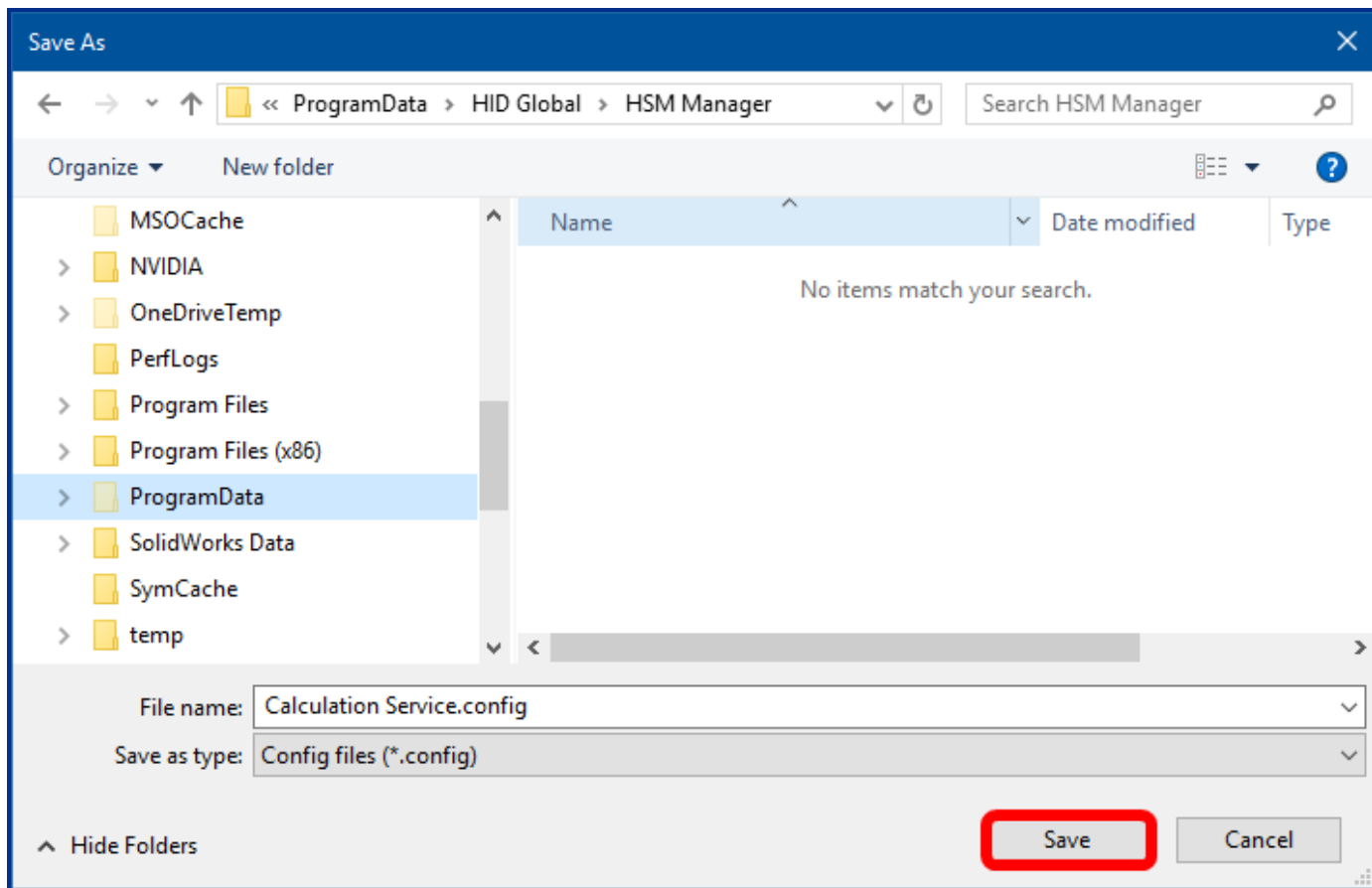


- Set the locations for PIN Pad Derivation Key and the Database Encryption Key and click **Go**.

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



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



2.5.3 TRISM XT key management system

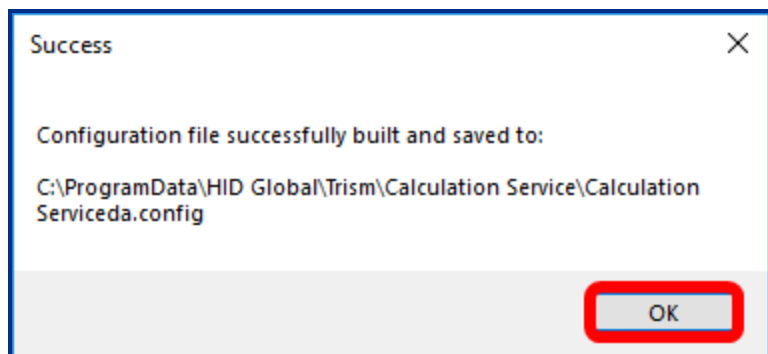
- Copy the Calculation Service.config file created during the XT Kky install (see XT Admin Guide) to **C:\ProgramData\HID Global\TRISM\HSM Manager on the TRISM Server**.
- Launch the TRISM XT Key Management System.
- Click **Maintenance**.
- Enter the **Financial ID**.
- Use the drop down menus to select 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**.

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: 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 **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 **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
- HSMAAdmin1 and HSMAAdmin2 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 [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 EFTPOSCONF.db)
 - b. Put XT into PCI NON mode.
 - c. Reload MBK.
 - d. Enter keys.
 - e. Create backups.
3. Create new backups (omit EFTPOSCONF.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 EFTPOSCONF.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 EFTPOSCONF.db.
10. In the CryptoServer Administration Tool, select **Manage > Reboot CryptoServer**.
11. Complete key installation tasks.
12. Create final backups including the EFTPOSCONF.db.
13. Update HID Calculation Service.
14. Update CLEEMV.dll in HID Card Printer Service.

2.6.2 Omitting EFTPOSCONF.db during back up 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, EFTPOSCONF.db can be backed up for future restoration.

When creating a back up and restoring prior to setting to V2 mode:

1. Click **Add All**.

Source CryptoServer

Available Databases

CXIKEY.db

DECTABWHITE.db

EFTPOSCONF.db

ISSUERKEYS.db

KEYPRESENCE.db

NETKEYS.db

TRANSKEYS.db

user.db

Backup Directory

Selected Databases

CXIKEY.db

DECTABWHITE.db

EFTPOSCONF.db

ISSUERKEYS.db

KEYPRESENCE.db

NETKEYS.db

TRANSKEYS.db

user.db

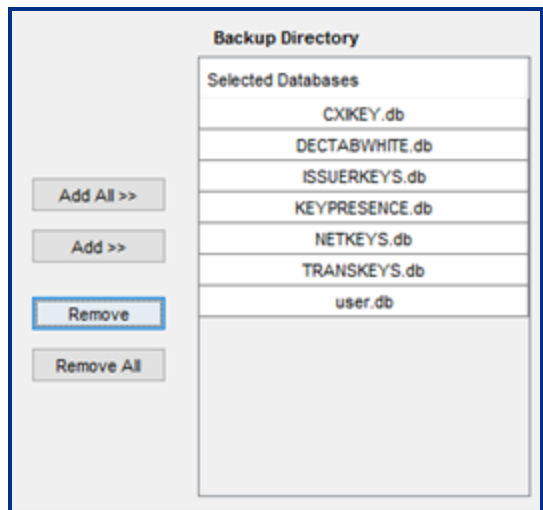
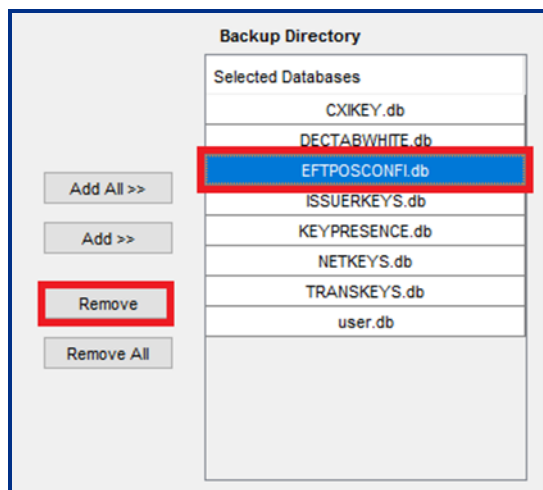
Add All >>

Add >>

Remove

Remove All

- From the **Backup Directory** list, click **EFTPOSCONFI.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

- 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.

- 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 EFTPOS.CONFI.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.

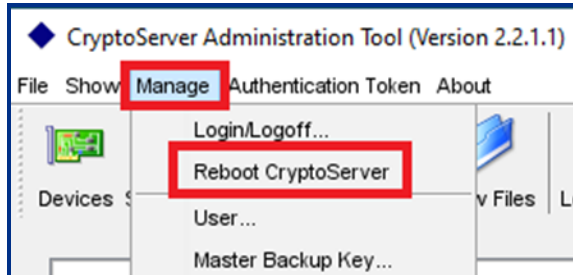
- c. Leave the command prompt open.

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 EFTPOS.CONFI.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 EFTPOS.CONFI.db)

Updating firmware/setting to V2 mode/restoring backups

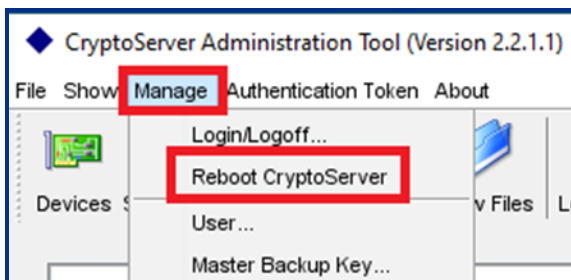
1. Update the firmware to PaymentServer-Hybrid-Se2-Series-4.33.3.0.mpkg - HSM XT - Installing/Updating Firmware.
 - a. Use **New Installation**.
HSMAdmin1 and HSMAdmin2 users remain, all other Users/Keys/MBK are deleted.
 - b. Reboot the CryptoServer by selecting **Manage > Reboot CryptoServer**.



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 EFTPOSCONF1.db - EFT POS Config file.
 - a. EFT POS Config - stores the NON, V2, V3 mode - If back ups 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:

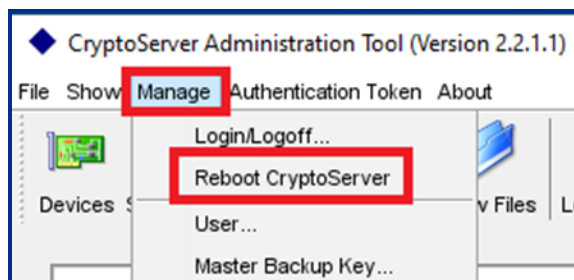
1. PINPad screen: Import new key. Press **OK/Cancel**.
2. PINPad screen: Insert 1. card. Press **OK/Cancel**.
3. PINPad screen: Enter PIN. (Should be **123456**.)
4. PINPad screen: Insert 2. card. Press **OK/Cancel**.
5. PINPad screen: Enter PIN. (Should be **123456**.)

- c. When completed, the CMD prompt shows **ANSW**:

7. Restore backups again omitting the EFTPOSCONF.db.

- a. Setting to V2 Mode will wipe keys, so back-ups 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 EFTPOSCONF.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 **Microsoft SQL Server 2008 R2 Native Client** installer, click **Next** and accept the license agreement when prompted. Leave all fields at their default values.
5. On the **TRISM 6** installer, click **Next** and accept the license agreement when prompted. Leave all fields at their default values.

TRISM 6 is now 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**.



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

The screenshot shows the 'Settings' window with the 'Manual Settings' section expanded. The 'SQL Server Location' is set to '.SQLEXPRESS'. The 'Database Naming Convention' is 'Trism'. The 'SQL UserID' is 'Trismadmin'. The 'SQL Password' is masked with asterisks. The 'Create' button is highlighted with a red box.

- 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**.

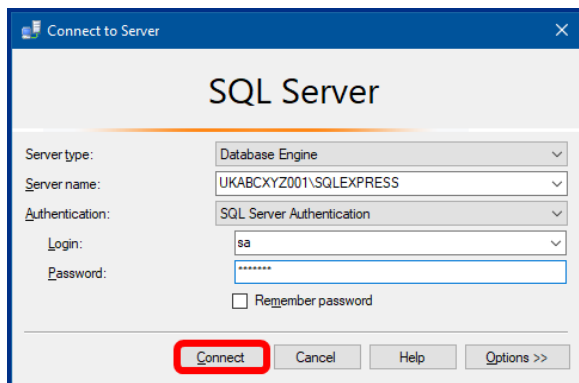
The screenshot shows the 'Admin login and pass...' window. The 'Login' field is 'sa'. The 'Password' field is empty. The 'Site ID' field is empty. The 'PinPad Derivation Key' field is 'PINDERV1'. The 'OK' button is highlighted with a red box.

- 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.

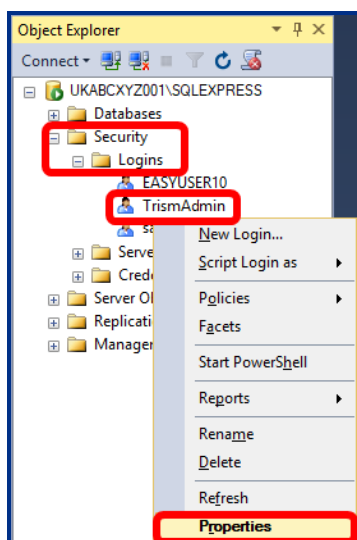
The screenshot shows a 'Database Creation Complete.' prompt with an 'OK' button highlighted by a red box.

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

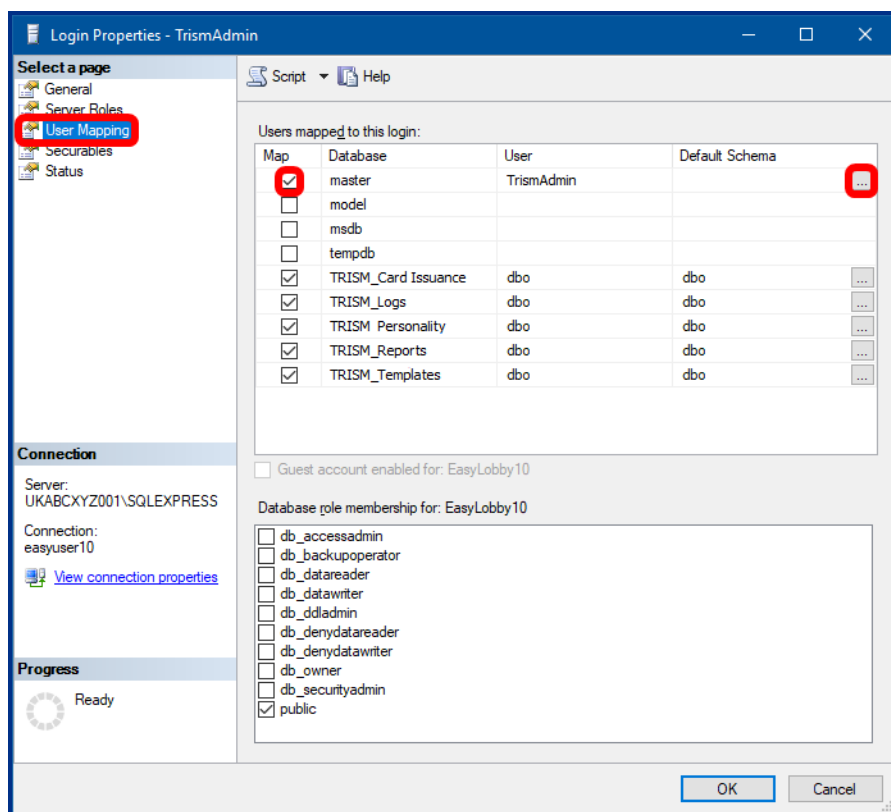


7. On the **Object Explorer** panel, on the left side of the **Connect to Server** window, expand the **Security** folder, then expand the **Logins** folder. Right-click on the **trismadmin** login and select **Properties**.

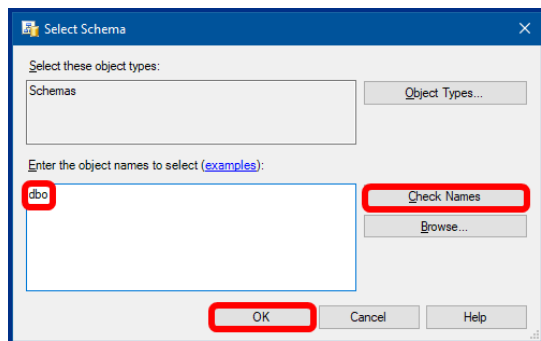


8. In the **Login Properties** window, in the **Select a page** section, select **User Mapping**.
9. In the table, select **Map** on the **master** database row.

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



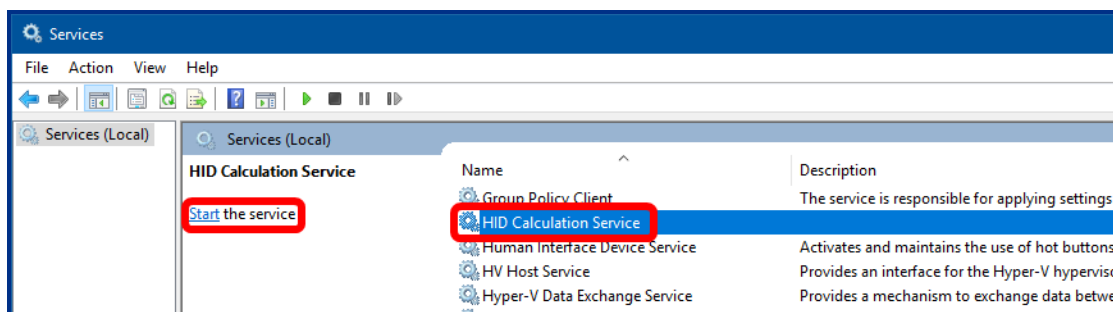
11. In the **Enter the object names to select** text box, type **dbo** and click **Check Names**. The **dbo** text changes to **[dbo]**. Click **OK**.



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

2.9 Calculation service installation

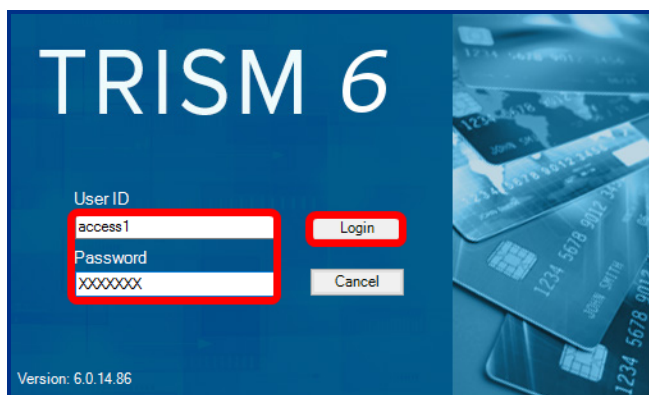
1. Download and run the HID Calculation Service Installer and any updates in the Current Version location on the FTP Site.
2. Start the **HID Calculation Service**.



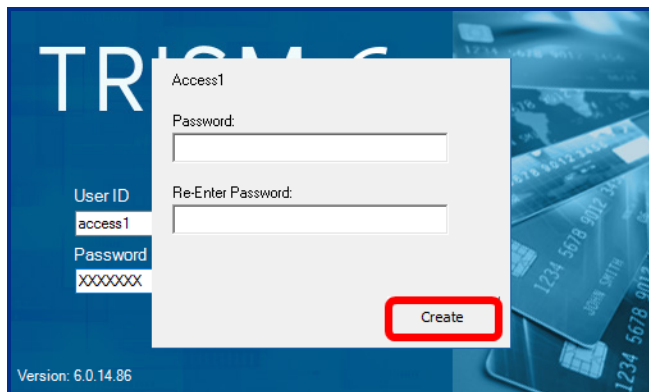
2.10 TRISM client initial configuration

This section assumes that:

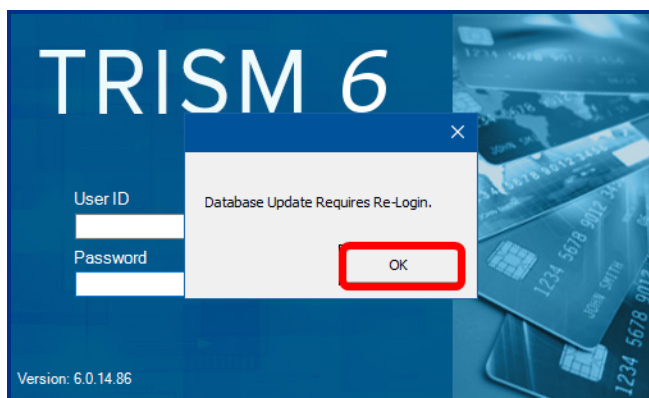
- The HSM has been installed and configured.
 - The TRISM Client Database Creation has been completed.
 - HID Calculation Service has been installed and started.
1. Run TRISM Client (T6).
 2. Enter **access1** as the **User ID** and have the FI enter password of **1234567**. Click **Login**.



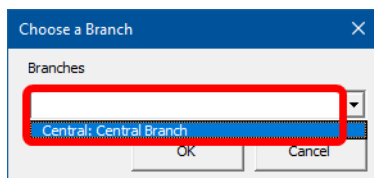
3. You are now asked to enter and re-enter a new password. This is the permanent password for the **access1** login. Click **Create**.



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 6, select **Configure > Interfaces > Interface Settings**.
2. Select **Calculation Service** from the drop-down menu.

The screenshot shows the 'Interface Settings' window for the 'Calculation Service'. On the left, a tree view shows the navigation path: General > Users > Templates > Formats > Devices > Active Directory > Branches > Interfaces > Interface Settings. The 'Interface' dropdown is set to 'Calculation Service'. The main table lists settings and their values:

Setting	Value
Core1Enabled	N
Core1IP	10.236.16.97
Core1Port	10001
Core2Enabled	N
Core2IP	10.236.16.97
Core2Port	10002
Demo Mode	N
ENABLEXT	Y
XTENDPOINT	3001@127.0.0.1

Below the table are 'Add' and 'Edit' buttons. At the bottom are 'OK' and 'Cancel' buttons. There is also a section for 'StockName' and 'StockQualifier' with 'Add', 'Edit', and 'Delete' buttons.

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**

The screenshot shows the 'Interface Settings' window for the 'Calculation Service'. The 'Interface' dropdown is set to 'Calculation Service'. The main table lists settings and their values:

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

The 'Core1Enabled' and 'Core2Enabled' rows are highlighted with red boxes. Below the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom are 'OK' and 'Cancel' buttons.

2. Values need to be manually added: ENABLEXT, XTENDPOINT, 2 Admin Users created during HSM XT Installation

- Click **Add**, for **Setting**, enter **ENABLEXT**, for **Value**, enter **Y**, and click **OK**.

Setting	Value
ENABLEXT	Y

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

Setting	Value
XTENDPOINT	10.236.16.92

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

Setting	Value
XTUSER_Admin1	1212Trism

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

Setting	Value
XTUSER_Admin2	1212Trism123

- All Settings have been added

ENABLEXT	Y
XTENDPOINT	10.236.16.92
XTUSER_Admin2	1212Trism123
XTUSER_Admin1	1212Trism

- Restart the **HID Calculation Service**.
- 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.

The screenshot shows the 'General' configuration window in TRISM Manager. The left sidebar lists various settings categories. The main area contains several configuration options. The 'Pin Pad Derivation Key Location' field is highlighted with a red rectangle and contains the text 'BDKKEY'. Other visible fields include 'Days until Password is Expired' (90), 'Enable Weak PINS' (checked), 'Minutes before Lockout' (15), 'Minutes before Red Icon (Down) on HealthBar' (5), 'Interface Timeout (In Seconds)' (90), 'Pin Pad Session Expiration in days' (NA), 'Pin Pad Encryption Key Location' (999), 'Pin Pad Timeout getting Offset (in sec)' (10), and 'Update File Location' (Citrix Per User). At the bottom, there are checkboxes for 'Allow Spoilable and Reprint' and 'DO NOT Show Active Cards in Order Card', and a 'PIK' field containing a long alphanumeric string.

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**.

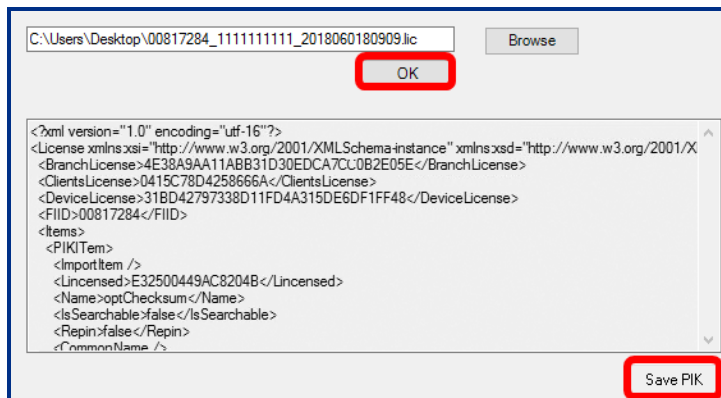
The screenshot shows the TRISM 6 login screen. The 'Login ID' field contains the text 'Access1' and the 'Password' field contains 'xxxxxxxx'. The 'Login' button is highlighted with a red rectangle. The background of the login screen features a blue gradient with a stylized image of a credit card.

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

The screenshot shows the 'License' window. It contains a text input field for the license file path and a 'Browse' button, which is highlighted with a red rectangle. There is also an 'OK' button at the bottom.

4. Locate the appropriate license file (*.lic), select it and click **Open**.

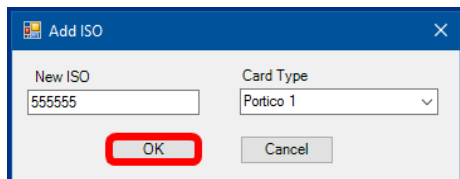
- Back in the **License** window, click **OK**. The text box in the body of the License form populates with the opened license's XML.



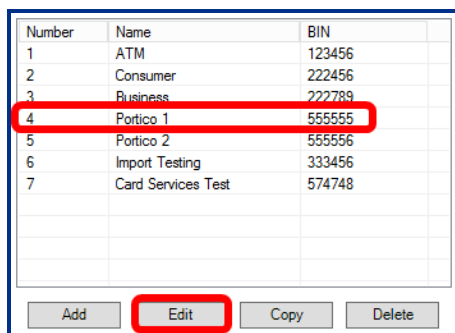
- Click **Save PIK**. The **PIK has been Saved** prompt is displayed.
 - Click **OK**.
 - Repeat this process for any other license files (branch, device, PIN pad, etc.).
- TRISM Client Initial Configuration is now completed.

2.12.2 Add formats

- In the **Configure** menu, select **Formats**. Select one of the pre-loaded BINs (ATM or Visa Debit), then click **Copy**.
- 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**.



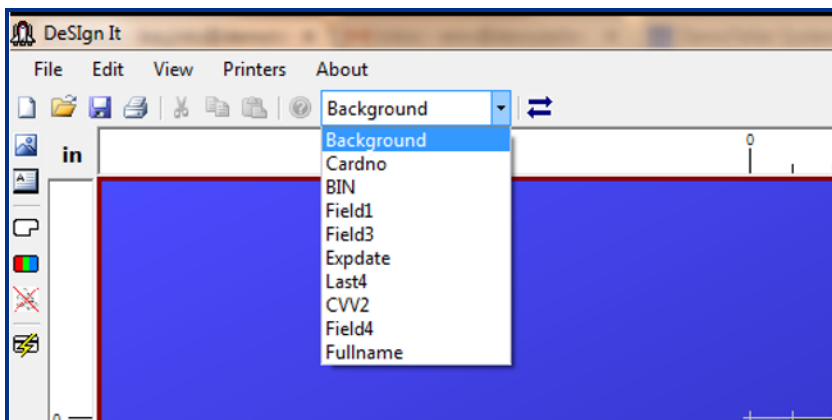
- Navigate back to **Configure > Formats** and select the BIN you just created, then click **Edit**.



- 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.

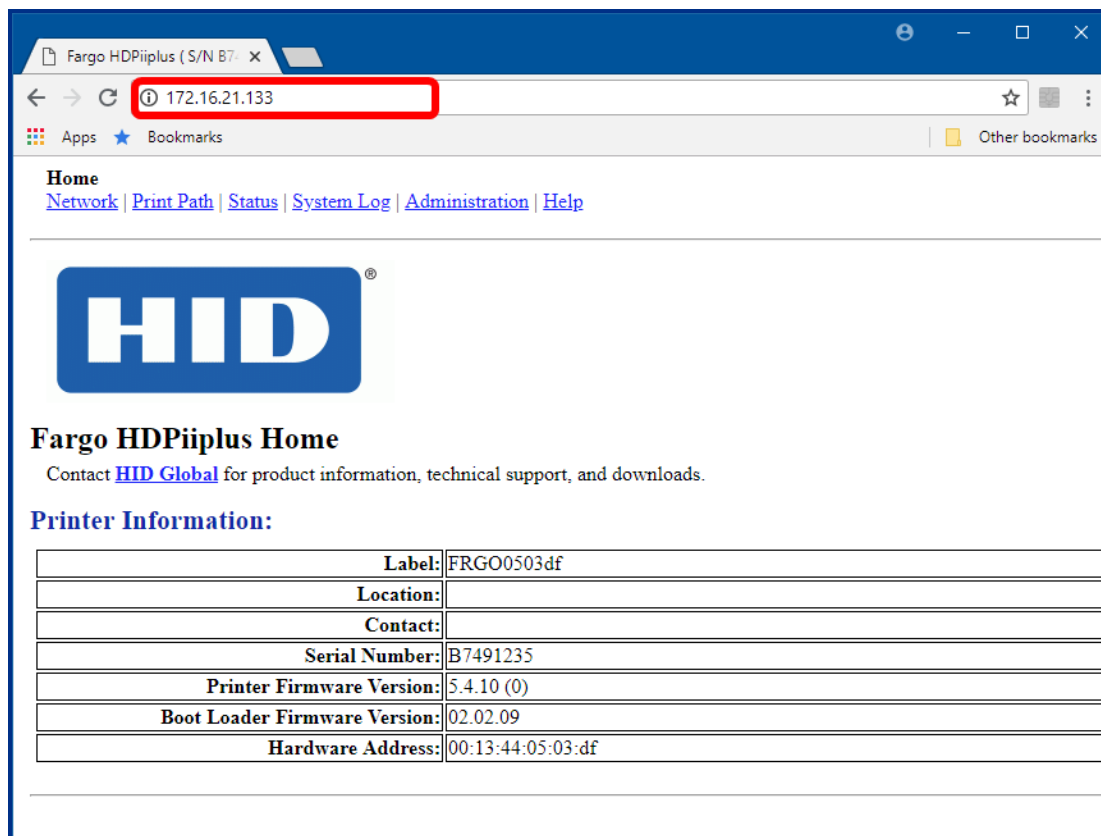
Note: If an error is displayed regarding missing fonts, download the appropriate fonts from the FTP site.

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

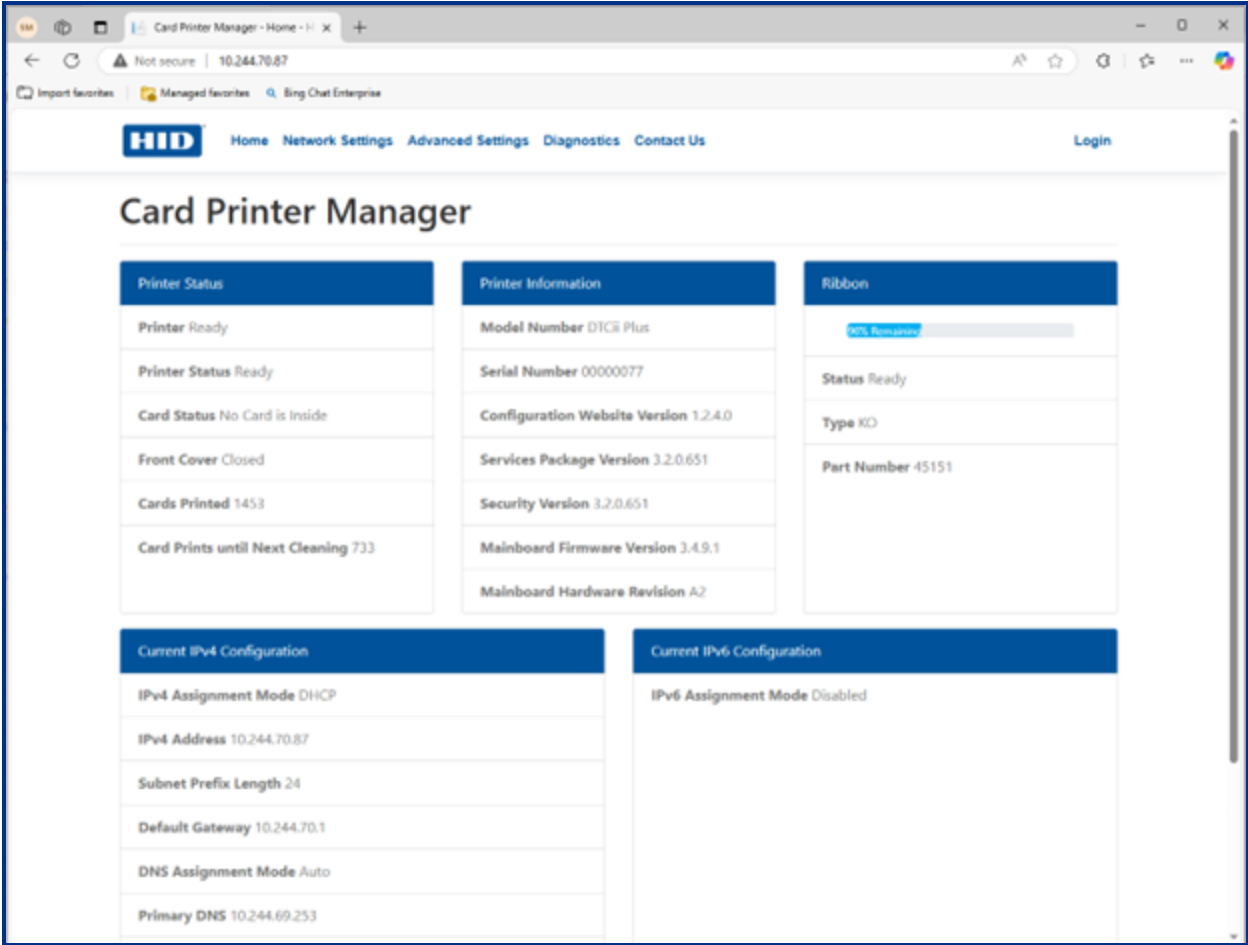
1. Verify connectivity to printer by entering the printer's IP address in the address bar of a web browser.



2. Install the printer and smart card reader drivers. Download the following from the FTP site as required:
 - FARGO® HDP®ii Plus
 - FARGO DTC®ii
 - 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.



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

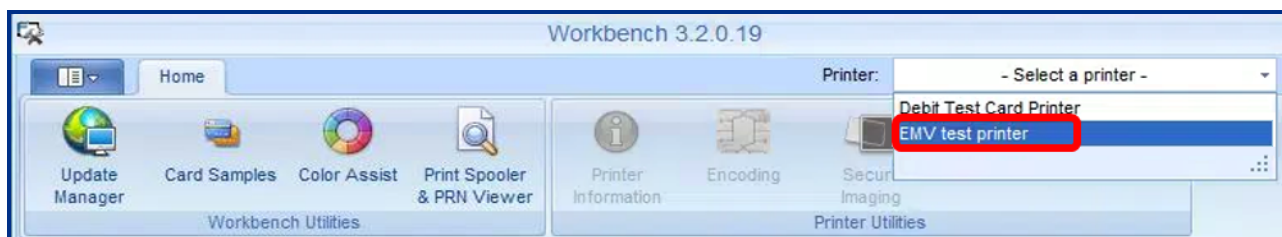
- With **Network** selected, configure the device as follows:
Name: The desired name for the printer.
IP Address: IP address of the printer.
Port: Because SSL is enabled on the printer, set the port to **443**.
Type: **Fargo DTCii PLUS** or **Fargo HDP600ii**.
Printer Service IP: The IP of the server 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.
- Click **OK** to save.
- At the **Device Added Successfully** prompt, click **OK**.
- At the **You must Restart Card Printer Service** prompt, click **OK**.

8. Click **OK**.
9. Continue to the device-specific printer setup instructions.

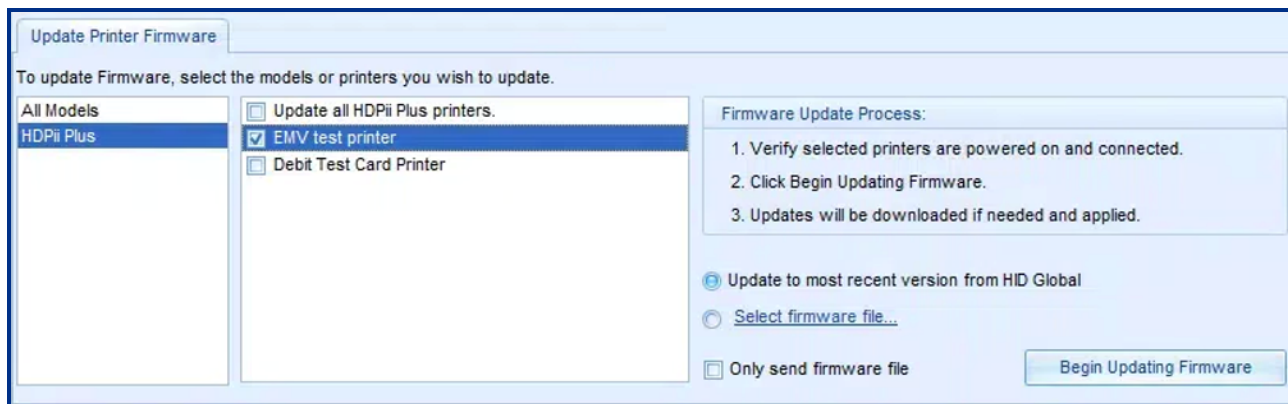
2.12.6 Device-specific setup instructions: FARGO HDPii PLUS - Ethernet

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**.

The screenshot displays the TRISM software interface with three main sections: Central Vault, In-Transit Carrier, and Vault. The Vault section is active, showing a table with columns for Name/Location and a description. The 'Add Location' button is highlighted with a red box. Below the Vault section, the 'Branch' section is visible, with the 'Name' field containing 'Secondary Vault' and the 'OK' button highlighted with a red box. The 'In-Transit Carrier' section shows a table with columns for Destination, # of Cards, and Description. The 'Central Vault' section shows a table with columns for Name/Location and a description. The 'Vault' section shows a table with columns for Name/Location and a description. The 'Branch' section shows fields for Name, Address 1, Address 2, City, State, and Zip, along with buttons for OK, Cancel, Print Inventory, Add, Edit, and Delete.

2.12.9 Add branches

1. On the main menu, click **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 **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**.

Card Stock ID	Card Stock Description	EMV
123	EMV	☒
444	Sample Test	☐
456	Blank White	☐

Card Stock ID	Card Stock Description	EMV
456	Blue pre-printed	☒

2. Select **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 **Inventory > Vault Inventory**, select a **Vault** and click **Add**. Select the cardstock and enter a quantity (this can be changed later).

Central Vault

Name/Location
Central

In-Transit Carrier

Destination	# of Cards	Description
Default Vault	10	EMV

Vault

Name/Location
Default Vault

Branch

Name :

Default Vault

Address 1 :

Address 2 :

City :

State :

MN

Zip :

Description

Number of Cards

EMV	1474
Sample Test	1065
Blank White	1580

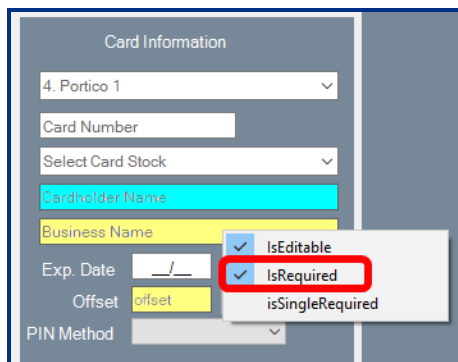
5. In **Configure > CardStock > CardStock to Vault/Device**, select the cardstock and the vault and device to be linked. Select a **State** (usually **Ready - card will print immediately after ordering**) and click **Add**.

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 **Request > Edit Permissions**.
2. Right-click the **Cardholder Name** field and select **IsRequired**.



2.13.2 Install VFI USB driver

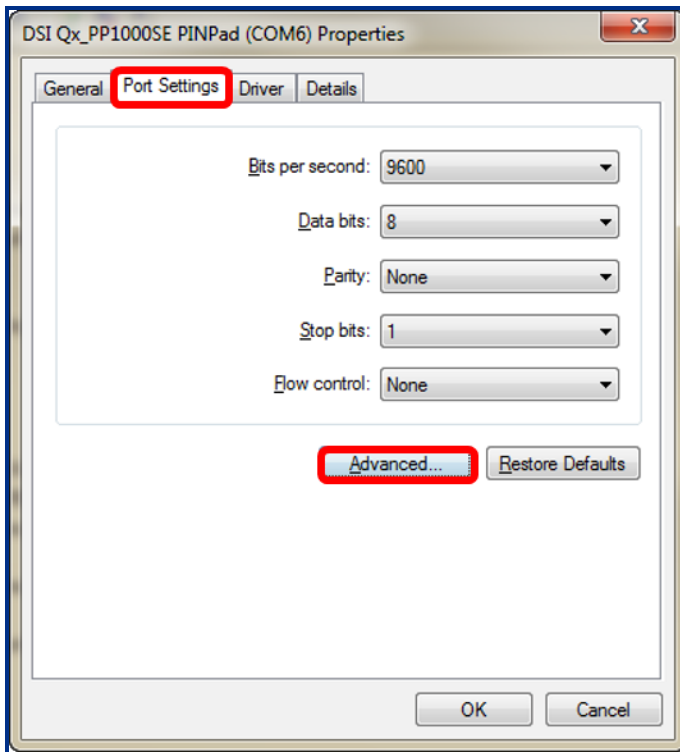
To install the Vx USB driver (VFI_USB_Driver_2.0.X.msi):

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.

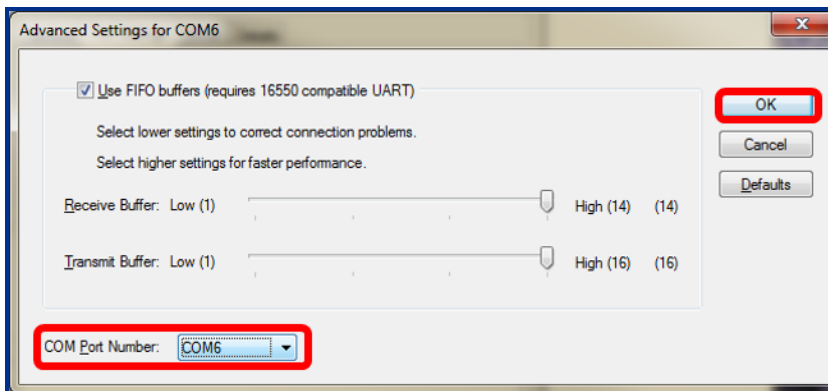
2.13.3 Changing the COM port of an installed PIN Pad

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**.

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



- 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.



- 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 **USB.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 **USB.SYS** file that was included in the PIN Pad driver **.zip** file.

Section 03

Request

3.1 Order Card

1. On the main menu, click **Request > Order Card**, or click .
2. Select the appropriate BIN in the **Select Product** drop-down menu (highlighted in red).

Note: Only select a BIN if you are going to manually enter the information.

3. **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 [4.c](#), click **Accounts** in the Account Information menu, then enter the customer's account number and ChkSavDesignator. One account must have **Primary** selected. The **Accounts** button only appears when using Mastercard dps.

ChkSavDesignator Values:

- D = checking
- S = savings

Account 1

☐ Primary

Number

TypeID

ChkSavDesignator

Descriptor

Balance

Status

4. Card Information

- Click **Get Card #** to automatically generate the card number (if **Auto Card Number** is enabled in the BIN's format settings) or enter it manually.
- Select the card stock from the drop-down menu.
- Enter the customer's name, business name (if desired), and the card's expiration date, if not automatically generated.
- Select the PIN method.
- 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.

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.

- The card's offset is displayed after the PIN is entered.

Search

Portico

Member Number

719299

Card Information

5. Portico 2

5555560001313131

Sample Test

JIMMY NEWTOWN

Business Name

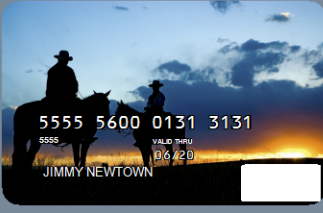
Exp. Date

Offset

PIN Method

Image Selection

Cowboys



Job Information

Print

DTCii

New

Ready

Default Vault

Card and Pin Mailer

Address Information

☐ Foreign

553 MOBY LANE

Address 2

RR500 TX 7503-0000

Country

Misc

Security Information

Motion's Maiden Name

37491860

578552128

Drivers License

Misc. Data 1

Misc. Data 2

Contact Information

8000000000 Home

0000000000 Work

Phone Number 3

Phone Number 4

Email

Account Information

75

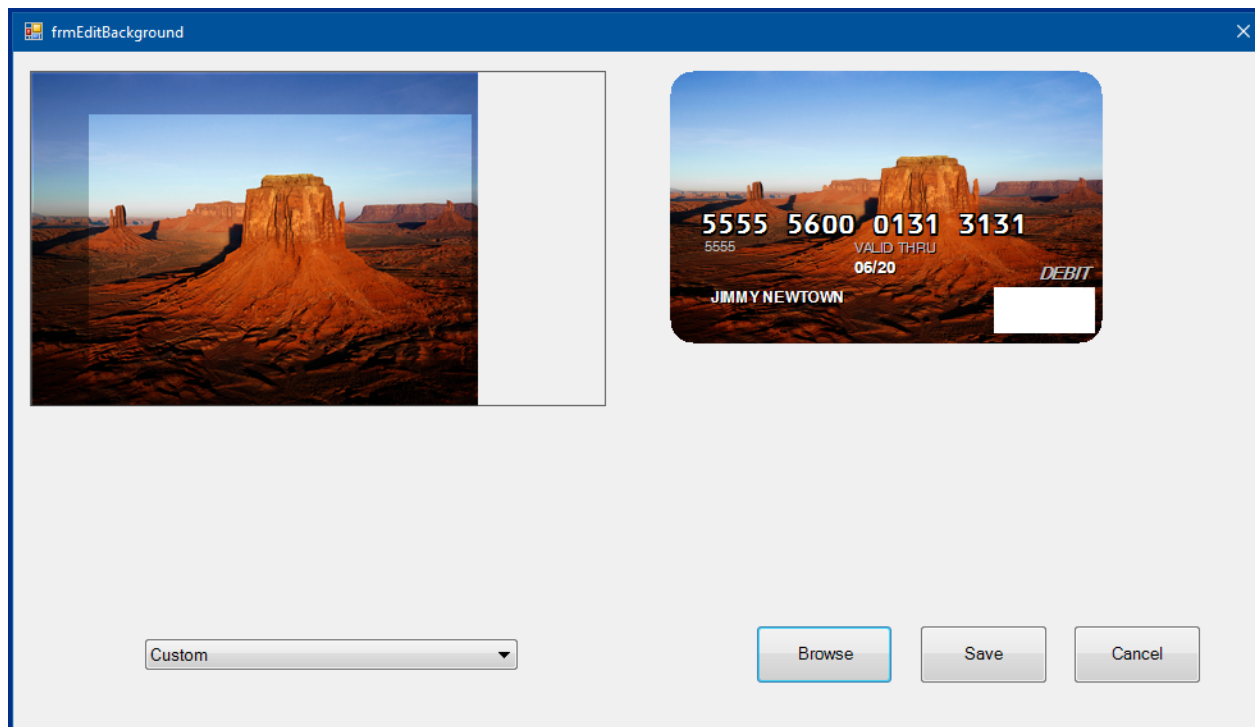
01

Account

Account

719299

5. Personalizing and Previewing Cards – See [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 back of the card.
6. Job Information

Select the following information from the drop-down menus:

 - a. Device: Card Printer
 - b. Card Status
 - c. Job Status:
 - **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).
7. Click **Complete** when all required fields are entered, and personalization is complete.

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 **Request > Edit Permissions**. Select a card type to edit its permissions.

The fields highlighted in yellow on the following screen have editable permissions.

The screenshot shows the 'Edit Permissions' window with several sections:

- Search:** Includes a search bar and a 'Search' button. The 'Search Criteria' field is highlighted in yellow.
- Card Information:** Includes fields for 'Select Product', 'Card Number', 'Select Card Stock', 'Cardholder Name' (highlighted in yellow), 'Business Name' (highlighted in yellow), 'Exp. Date', 'PSN', 'Offset' (highlighted in yellow), 'Get PIN', and 'PIN Method'.
- Image Selection:** Includes a 'Loading...' dropdown and a 'Personalize' button.
- Job Information:** Includes dropdowns for 'Select Job Type', 'Select Device', 'Select Card Status', 'Select Job State', and 'Select Vault'. It also has 'Order Card' and 'Close' buttons.
- Address Information:** Includes a 'Foreign' checkbox, 'Address 1', 'Address 2', 'City', 'State', 'Zip', 'Country', and 'Misc' fields. The address fields are highlighted in yellow.
- Security Information:** Includes fields for 'Mother's Maiden Name', 'Date of Birth', 'SS# / Tax ID', 'Drivers License', 'Misc. Data 1', and 'Misc. Data 2'. These fields are highlighted in yellow.
- Contact Information:** Includes dropdowns for 'Phone Number 1' through 'Phone Number 4' and an 'Email' field. These fields are highlighted in yellow.
- Account Information:** Includes fields for 'Account' (multiple instances) and 'Member Number'. These fields are highlighted in yellow.

You can change the colors of the **Editable**, **Required** and **Single Required** fields in [7.11 Theme](#).

The screenshot shows the 'Card Information' section with a tooltip for the 'Cardholder Name' field. The tooltip contains the following settings:

- ☒ IsEditable
- ☒ IsRequired
- ☐ isSingleRequired

- **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.

Security Information

Mother's Maiden Name

State of Birth

SS# / Tax ID

Drivers License

Misc. Data 1

Misc. Data 2

IsEditable

IsRequired

isSingleRequired

3.3 Re-PIN

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

Warning

Swipe Card

Cancel

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

3.4 Read a Card

On the main menu, click **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 in this window if one is not printed at the time of card creation.

The screenshot shows the PIN Mailer window with the following sections:

- Search:** Includes a dropdown menu, a search criteria field, and a 'Search' button.
- Card Information:** Includes a dropdown menu for card type (e.g., '2 Visa Debit'), a card number field (e.g., '222456*****5555'), a 'Select Card Stock' dropdown, a 'Business Name' field, an 'Exp. Date' field, an 'Offset' field (e.g., '5453'), a 'Get PIN' button, and a 'PIN Method' dropdown (e.g., 'PinPad').
- Image Selection:** Includes a 'Loading...' dropdown and a 'Personalize' button.
- Job Information:** Includes dropdown menus for 'Select Job Type', 'Select Device', 'Select Card Status', 'Select Job State', and 'Select Vault'. A 'Print Mailer' button is highlighted with a red box, and a 'Close' button is below it.
- Address Information:** Includes a 'Foreign' checkbox, an 'Address 1' field (e.g., '123 Main St'), an 'Address 2' field, a 'City' field (e.g., 'Dallas'), a 'State' field (e.g., 'TX'), a 'Zip' field (e.g., '55555'), a 'Country' field, and a 'Misc' field.
- Security Information:** Includes fields for 'Mother's Maiden Name', 'Date of Birth' (e.g., '11/04/1974'), 'Drivers License', 'Misc. Data 1', and 'Misc. Data 2'.
- Contact Information:** Includes fields for 'Phone Number 1' (e.g., '1234567890'), 'Phone Number 2', 'Phone Number 3', 'Phone Number 4', and 'Email'.
- Account Information:** Includes fields for 'Account' (multiple) and 'Member Number'.

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

3.6 CVV2 Calculator

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

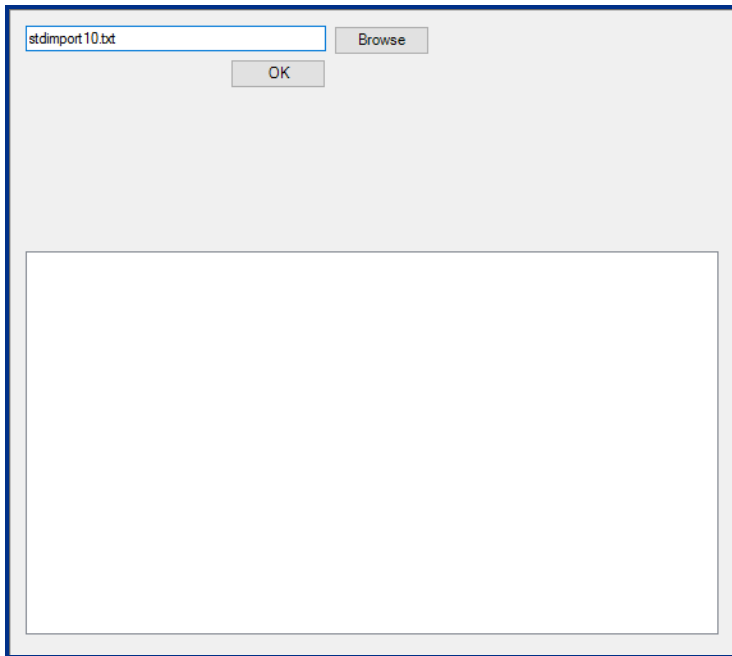
The screenshot shows the CVV2 Calculator window with the following fields:

- BIN:** A dropdown menu (e.g., '4. Portico 1').
- Card Number:** A text field (e.g., '5434680933499881').
- Exp Date:** A date field (e.g., '01/21').
- CVV2:** A text field (e.g., '123').
- Calculate:** A button highlighted with a red box.

- Enter the BIN, card number, and expiration date of an existing card.
- 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 **Request > Import > Standard** (or an alternative).



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

A list of failed cards is shown 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**, or click .

Refresh ☒ Auto Refresh 10 3 Clear All ▼ Cards In Queue: 7												
ID	Card Type	F..	Process State	Originating IP	Originating...	User ID	CIN	Device IP	L...	User ...	BranchID	Entry De
94	5. Portico 2	5	Mailer Error	10.0.75.1	Default Vault	access1	2431	10.244.69.89:7575	0	access1	Central	6/15/20
95	5. Portico 2	5	Photo Printer Error	10.244.69.72	Default Vault	Access1	2432	10.244.69.89:7575	0	Access1	Eden Prairie	6/21/20
96	4. Portico 1	4	Photo Printer Error	10.244.69.72	Default Vault	access1	2433	10.244.69.89:7575	0	access1	Eden Prairie	6/21/20
97	5. Portico 2	5	Photo Printer Error	10.244.69.72	Default Vault	access1	2435	10.244.69.89:7575	0	access1	Eden Prairie	6/21/20
98	5. Portico 2	5	Photo Printer Error	10.244.69.72	Default Vault	access1	2436	10.244.69.89:7575	0	access1	Eden Prairie	6/21/20
99	7. Card Services Test	7	Ready Photo	10.244.69.72	Default Vault	access1	2437	10.244.69.89:7575	0	access1	Eden Prairie	6/21/20

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

Card Information

Device Name

DTCii

Device IP Address

10.244.69.89:7575

Change Card Status

New

Change Job Status

Change Card Stock

Sample Test

Card Number

5555560002234547

Entry Date

6/21/2018 11:31:20 AM

Format

5. Portico 2

Transaction Type

Print-a-Card

☒ Print Card Mailer

☒ Print PIN Mailer

Current Background

custom image



New Background

Error Code

OK

Cancel

Print Report

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".

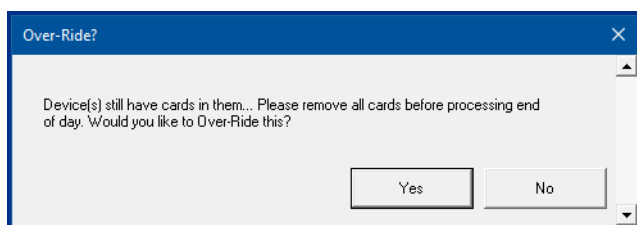
- **Change Job Status** allows you to select the card status as ready photo, paused photo, manual photo, or card verified.
- To delete a card from the queue, select it and press **Delete** on your keyboard.

Section 05

Reports

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 added manually during the order card process.
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.

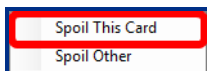
5.1.1 Tips for balancing end of day reports

- 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 the 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:

 The "Spoil Card" dialog box is shown. It contains the following fields and controls:

- ID / Card Number:** A dropdown menu showing "5555560004526434".
- Queue ID:** A text box containing the number "2".
- Description:** An empty text box.
- Reason:** An empty text box.
- Operator 1:** A text box containing "Access1".
- Operator 2:** A text box containing "Installer1".
- Return to Inventory:** An unchecked checkbox.
- Card Successful:** An unchecked checkbox.
- Card Destroyed:** An unchecked checkbox.
- Time:** A text box showing "12:29:03".
- Date:** A text box showing "26/06/2018".
- Buttons:** "OK" and "Cancel" buttons at the bottom.
- Footer:** A label "Time and Date Added" above an empty field.

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.

- To add a card back to the Vault Inventory, select **Return to Inventory**.
- To subtract a card from the Vault Inventory, select **Card Destroyed**.

5.1.4 Process End of Day for all cardstock associated to the selected branch/vault/device

1. On the **End of Day** window, select the desired **Branch**, **Vault**, and **Device**.
2. Click **Process ALL Card Stock End-of-Day**.

Trism 6 Branch Name: Central Branch: Central User: mike

File Request Queue Reports Inventory Configure Help

Log Out Order Card RePIN Queue End of Day Vault Device Access Help

Branch Central Vault DTCi Vault Device T3 Office DTCi Card Stock MAG

BIN	Amount
555555	1

Device Inventory

Starting Inventory 0

Inventory Added 1

Inventory Removed 0

Manually Added 0

Used Inventory 1

Cards Destroyed 0

Cards Returned to Inventory 0

Ending Device Inventory 0

Vault Inventory

Starting Vault Inventory -1

Removed to Device(s) 1

Returned From Device(s) 0

Current Vault Inventory -2

Total Cards in Device(s) 0

Total Branch Inventory 2

ID	Card Number	EncodedName	DeviceID	UserID	EnteredDate	ProcessDate	Workstation	Transaction Ty
1	555555*****0448	NEWTOWN/JIMMY	10.236.16.81:3000	mike	8/28/2020 9:19:41 AM	8/28/2020 9:23:48 AM	AAHID2P1WZM2	PRINT-A-CARD

Process ALL CardStock End-of-Day

Process Current CardStock End-of-Day

Print

3. Select **Print** or **Cancel** on the **Print** window depending on if a paper copy is desired. One prompt is presented for each cardstock processed.
4. After the final **Print** window is resolved, click **OK** on the **Process Completed Successfully** window.

5.2 Management

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

1. On the main menu, click **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.

The screenshot shows the Management report interface. At the top, there are two date pickers: 'Start Date' (19/06/2018) and 'End Date' (26/06/2018), both highlighted with red boxes. To the right of these is a checkbox labeled 'Only Show Processed Transactions'. Below the date pickers are four 'Filter' dropdown menus. To the right of the filters is a 'Clear' button and a 'Search' button, which is highlighted with a red box. Below the filters is a table with columns: Process..., Card Nu..., Offset, ExpDate, Encode..., TranType, WorkSt..., Operato..., CardFor..., Entered..., VaultID, Workst..., DeviceID, and Produ... The table is currently empty. At the bottom left, it says 'Record Count: 0'. At the bottom right, there are 'Save', 'Load', and 'Export' buttons.

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 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.

The screenshot shows the 'Edit Columns' dialog box. It contains a list of columns with checkboxes. The columns are: ArchivedDate, BackgroundID, BranchID, CardFormat, Card Number, Card Mailer, CardStatus, CustomerInfoID, Created, CardRead, DeviceID, Duplicate, ExpDate, EncodedName, EnteredDate, Embosser Name, ID, MailerID, MSRWritten, Offset, OperatorID, PhotoID, Pin Mailer, ProcessDate, ProductID, PVKI, QID, SignatureID, Spoiled, TranType, VaultID, WorkStation, WorkstationIP, MSRWritten1, CardRead1, Duplicate1, Last4, BWPhotoPrint, ColorPhotoPrint, PINSelected, CMailerPrinted, PMailerPrinted, CoreUpdated, ActivatorUpdated, and Uploaded. The 'Save' button at the bottom is highlighted with a red box. There are also up and down arrows on the right side of the list, which are also highlighted with red boxes.

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.

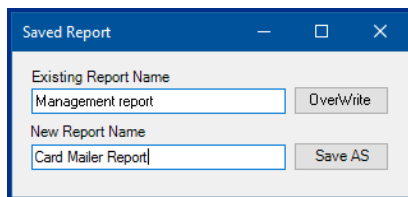
5.2.3 View card details

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

5.2.4 Save a customized report

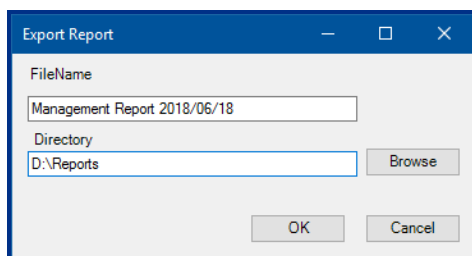
Click **Save**.

- 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 **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 **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 **Reports > Branch Activity** to create a report of all cards printed at the branch in which the workstation creating the report is located.

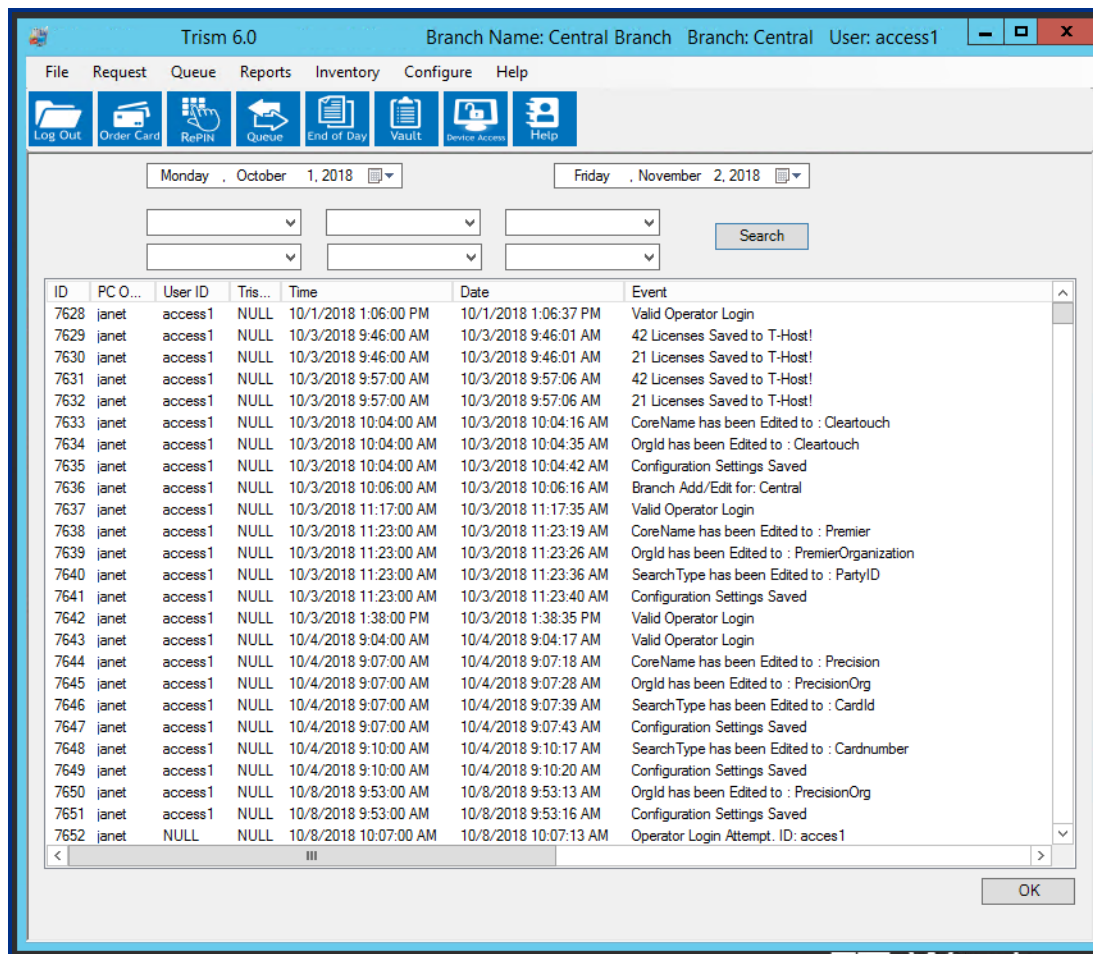
5.7 Device Error

On the main menu, click **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 **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.



5.9 Background

On the main menu, click **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 specific records from the database.

1. Select **Reports > Remove Cardholder Data**.
2. On the **Customer Removal** screen, you can search for 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

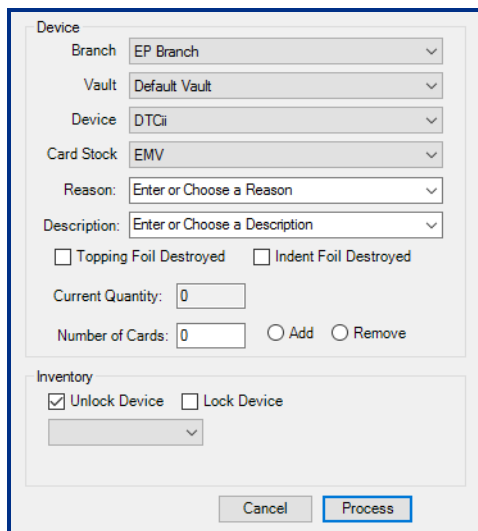
Inventory

6.1 Device Access

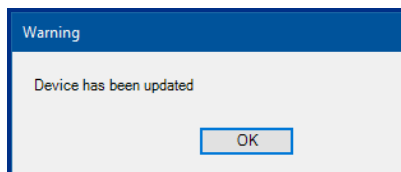
6.1.1 Add/remove cards and change ribbon/foil

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

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



2. The **Branch**, **Vault**, and **Device** default 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**.

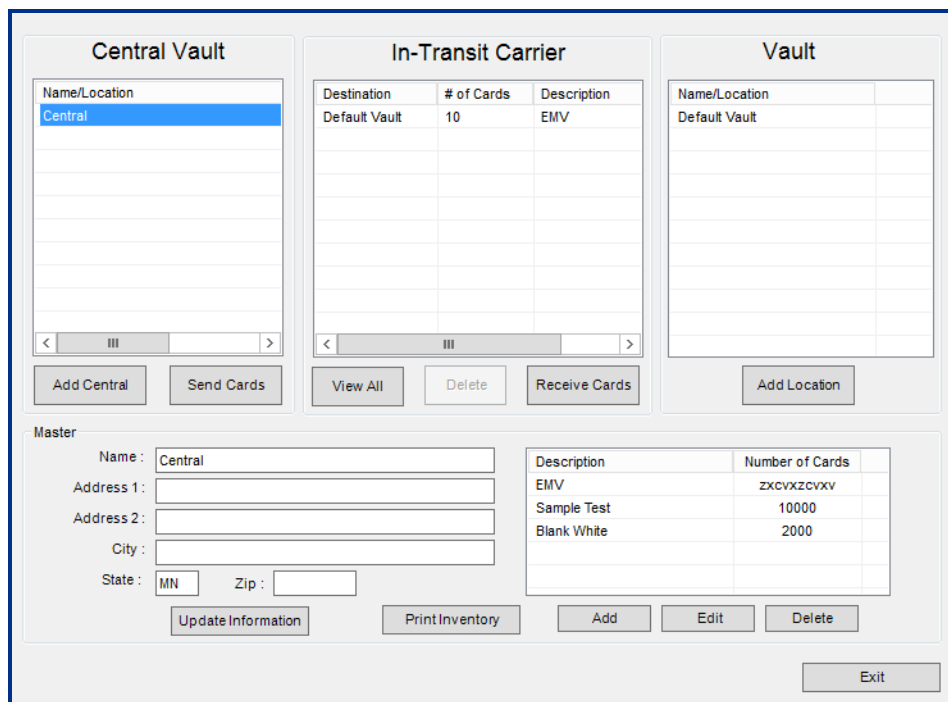


6.2 Vault Inventory

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).

6.2.1 Add a vault

1. On the main menu, click **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**.



The screenshot displays the Vault Inventory application interface, which is divided into three main sections: Central Vault, In-Transit Carrier, and Vault.

Central Vault: This section contains a table with the header "Name/Location" and a single entry "Central". Below the table are navigation buttons: "< III >". At the bottom of this section are two buttons: "Add Central" and "Send Cards".

In-Transit Carrier: This section contains a table with the following data:

Destination	# of Cards	Description
Default Vault	10	EMV

Below the table are navigation buttons: "< III >". At the bottom of this section are three buttons: "View All", "Delete", and "Receive Cards".

Vault: This section contains a table with the header "Name/Location" and a single entry "Default Vault". Below the table are navigation buttons: "< III >". At the bottom of this section is one button: "Add Location".

Master: This section contains a form for entering vault information. It includes fields for "Name" (set to "Central"), "Address 1", "Address 2", "City", "State" (set to "MN"), and "Zip". Below these fields are three buttons: "Update Information", "Print Inventory", and "Add". To the right of the form is a table showing card inventory:

Description	Number of Cards
EMV	ZXCXVZCXXV
Sample Test	10000
Blank White	2000

Below the card inventory table are three buttons: "Add", "Edit", and "Delete". At the bottom right of the entire interface is an "Exit" button.

6.2.2 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**.

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

Central Vault

Name/Location
Central

< III >

Add Central Send Cards

In-Transit Carrier

Destination	# of Cards	Description
Default Vault	10	EMV

< III >

View All Delete Receive Cards

Vault

Name/Location
Default Vault

Add Location

Send Cards to a Branch

Send To :

Carrier Name :

Number of Cards :

Comments :

Description	Number of Cards
EMV	zxcvzxzcvxv
Sample Test	10000
Blank White	2000

Send Cancel

Exit

6.2.3 Transfer cards - receive cards

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

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

Receive Cards

Branch Name : Default Vault

Carrier Name : FedEx

Product ID : Blank White

Number of Cards : 200

Comments :

Name 1 : access1

Name 2 : installer1

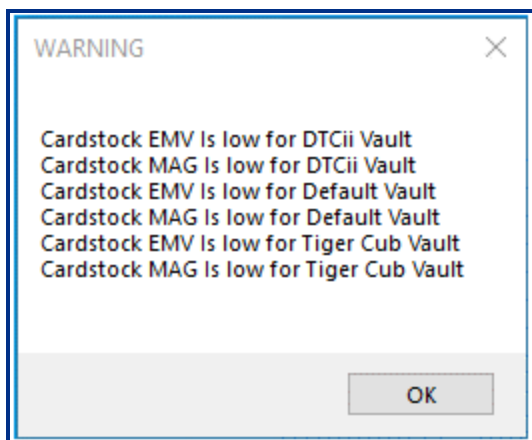
Sent : 6/5/2015 8:58:49 AM

Received : 06/05/2015 8:59 AM

Process Cancel

6.2.4 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  and log in with a Dual Control user when prompted.

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

TRISM 6

Branch Name: Central Branch Branch: Central User: access1 - [Vault Tracking]

File

Request

Queue

Reports

Inventory

Configure

Help

Log Out

Order Card

RePIN

Queue

End of Day

Vault

Device Access

Help

Central Vault

Name/Location
Central

Add Central

Send Cards

In-Transit Carrier

Destination	# of Cards	Description

View All

Delete

Receive Cards

Vault

Name/Location
Default Vault
East Side Vault
West Side Vault

Add Location

Branch

Name :

West Side Vault

Address 1 :

Address 2 :

City :

State :

Zip :

Update Information

Print Inventory

Add

Edit

Delete

Exit

Description	Number of Cards	Min. Quantity
EMV	0	0

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**.

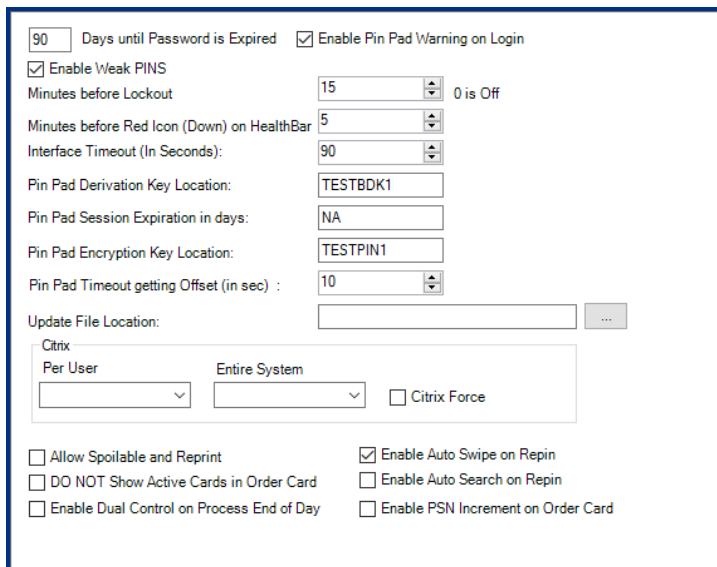
6. The Edit Stock window is displayed. Enter a number or use the up and down arrows to increase or decrease the **Minimum Number for Alert** and click **Update**.
7. Repeat these steps for each vault and card stock.

Section **07**

Configure

7.1 General

On the main menu, click **Configure**. On the side menu, click **General**.



90 Days until Password is Expired ☒ Enable Pin Pad Warning on Login

☒ Enable Weak PINS

Minutes before Lockout: 15 0 is Off

Minutes before Red Icon (Down) on HealthBar: 5

Interface Timeout (In Seconds): 90

Pin Pad Derivation Key Location: TESTBDK1

Pin Pad Session Expiration in days: NA

Pin Pad Encryption Key Location: TESTPIN1

Pin Pad Timeout getting Offset (in sec) : 10

Update File Location: ...

Citrix

Per User Entire System ☐ Citrix Force

☐ Allow Spoilable and Reprint ☒ Enable Auto Swipe on Repin

☐ DO NOT Show Active Cards in Order Card ☐ Enable Auto Search on Repin

☐ Enable Dual Control on Process End of Day ☐ Enable PSN Increment on Order Card

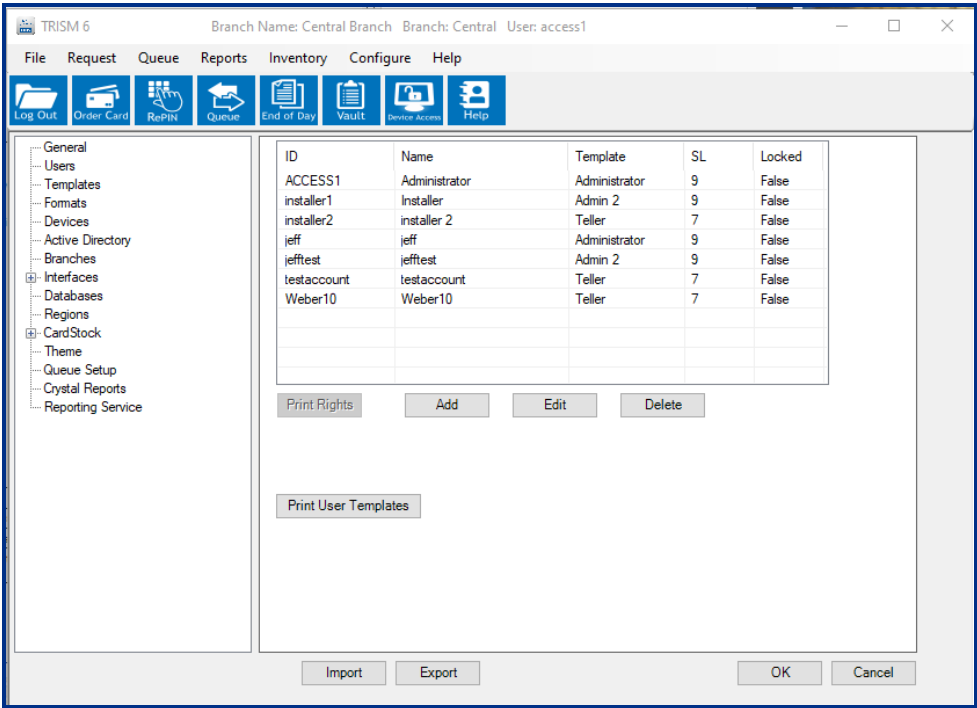
Field	Description
Days until Password is Expired	Applies only to non-Active Directory users. User passwords are valid for this number of days. Users are prompted to select a new password upon expiration.
Enable Pin Pad Warning on Login	Display warning message that no PIN pad is plugged in to the computer upon TRISM login.
Enable Weak PINS	If checked, weak PINs (1111, 1234, 4321, etc.) 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 login as a different user.
Minutes before Red Icon (Down) on Healthbar	Allows you to set a time frame before a System Status turns from green to red on the System Status Window (see 7.8 System Status).
Interface Timeout (in Seconds)	
Pin Pad Derivation Key Location	Numerical location of PIN Pad Derivation Key in HSM Manager.
Pin Pad Session Expiration in days	
Pin Pad Encryption Key Location	
Pin Pad Timeout getting Offset (in secs)	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.
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.

Field	Description
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.
Enable Dual Control on Process End of Day	Requires a second admin user for the user to process the End of Day report.
Enable Auto Swipe on Repin	
Enable Auto Seach on Repin	
Enable PSN Increment on Order Card	Choose to have the Pa Sequence Number incremented when a card is being ordered.

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 **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)

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

ID

123456

Template

Administrator

Name

JohnDoe

☐ Locked Out

Email

JD@acompany.com

Password Options

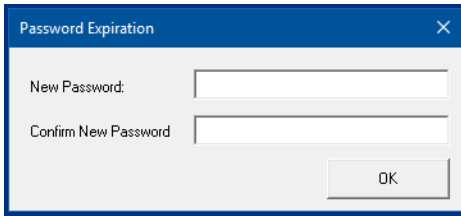
Change Password

Reset Password

Save

Cancel

New user password selection

A screenshot of a 'Password Expiration' dialog box. The dialog has a blue title bar with the text 'Password Expiration' and a close button (X). Inside the dialog, there are two text input fields. The first field is labeled 'New Password:' and the second field is labeled 'Confirm New Password:'. Below the second field is an 'OK' button.

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 in the provided fields and click **OK**. You must then enter your new password in the login screen. All passwords must be at least 8 characters long and include at least three of the following:

- Capital letter
- Lowercase letter
- Number
- Special character (!@#\$%^&*).

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 [A.1 System requirements](#) for permission descriptions. The administrator template cannot be edited or deleted.

On the main menu, click **Configure**. On the side menu, click **Templates**.

General

Users

Templates

Formats

Devices

Active Directory

Branches

Interfaces

Databases

CardStock

Theme

Queue Setup

ID	Name
Administrator	Administrator
Template 1	Admin 2
Template 2	Backoffice
Template 3	Inventory Control
Template 4	Central Reporting
Template 5	Teller

Print Rights

Add

Edit

Delete

OK

Cancel

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.

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.

Security

Order Cards

Queue

Reports

Inventory

Configure

Template Name

Admin 2

9

Template Security Level

☒ Edit Security Template (Add/Edit/Delete)

☒ Edit Security Permissions

☒ View all Branches

☐ Log Into Thost

☒ License File

☒ Reset Other User Passwords

7.4 Formats

Card types (for example, Mastercard, Visa, Visa EMV, etc.) 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 **Configure**. On the side menu, click **Formats**.

Number	Name	BIN	
1	ATM	123456	
2	Consumer	222456	
3	Business	222789	
4	Portico 1	555555	
5	Portico 2	555556	
6	Import Testing	333456	
7	Card Services Test	574748	

Add

Edit

Copy

Delete

To add a card type:

- Click **Add**.
- Enter the card’s **ISO** or **BIN** number, then select or manually enter the **Card Type**.
- Click **OK**.

Add ISO

New ISO

555555

Card Type

Portico 1

OK

Cancel

7.4.1 General Settings

To display the general settings:

- On the main menu, click **Configure**. On the side menu, click **Formats**.
- Select a card type in the list and click **Edit**.
- On the side menu, click **General Settings**.

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

Transaction Report

Printer:

Additional Transaction Report Directory

Browse

☐ Show PSN

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 **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

Format: Card Type:

Order	Length	Name	Index From	Start	Default
1	1	Format Code	SS	0	B
2	16	Card Number	SS	1	1234567890123456
3	26	Name	1st FS	0	
4	4	Expiration ...	2nd FS	0	4912
5	3	Service Code	2nd FS	4	120
6	1	Member Nu...	2nd FS	7	1
7	4	Offset	2nd FS	8	0000
8	0				
9	0				
10	0				

Track Length: 55 (Max: 79)

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

Edit Layout

Field Name	Index From	Start	Length
Format Code	SS	0	1
Data			
B			
OK		Cancel	

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

Track 1/Track 2 Parameters

ISO Number: 123456

Card

16 Account Length ☒ No Mod10
18 Name Index ☐ Calc. Mod10
☒ Offset Written ☐ Verify Mod10

Expiration

0 Date Index
00/00 Date to Add
☒ None
☐ Month
☐ Year

Method

Algorithm DES

Mag Stripe

☐ Low Coercivity
☐ High/Low Coercivity
☒ High Coercivity

DES

☒ Use DES
0 PAN Index 0 GPIN Index
16 PAN Length 8 Offset Index
0 Pad Value 01 Des Key
0123456789012345 Decimalization Table

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.

☐ Enable Auto Card Number Generation.

Auto Card Number

Beginning Card Number Current Card Number

ISO: 123456 0000000000 0

Increment By: 0

☒ Allow Name Change

Name Options

Customer's name will be encoded in the following format

Lastname/Firstname Middle

Allow Name Change on the following Transactions

☒ Re-Pin
☒ Select A Pin

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 **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**.

Indents and Embossing

Locked

☒ Use Masking

Line 1

0.9

☐

Masking

####

Line 2

0.68

☐

Line 3

0.52

%DATE% %V%

☐

Line 4

0.35

%NAME%

☐

Line 5

0.21

☐

Left Margin

0.40

From left to center of first character

☐ Enable Indent Printing

Indent Printing

Indent Print Mask

####

1234 5678 9012 3456 CV2

Indent from edge of card

1.200

Font Type

Type 4 (MC)

☐ Disable Truncation Rules

Truncation Limit

26

☒ Topping

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.

- On the main menu, click **Configure**. On the side menu, click **Formats**.
- Select a card type in the list and click **Edit**.
- On the side menu, click **EMV**.

EMV Service Code

201

Certificates

KeyName	Serial Number	ExpDate
TEST ISSUER KEY 01	111111	12/1/2028

Import

Delete

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 6.1 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:

- On the main menu, click **Configure**. On the side menu, click **Formats**.
- Select a card type in the list and click **Edit**.
- On the side menu, click **Mailers**.

☐ Print Card Mailer

Card Mailer

☐ Use MSWord Mail Merge

Template File

Browse

Printer:

☐ Print Pin Mailer

PIN Mailer

☐ Use MSWord Mail Merge

Template File

Browse

☐ Calc Natural PIN

☐ Print Return Address

Printer:

☐ Trism Sets PIN Mailer Form size (3 7/8" X 8 7/8")

Auto Select Option

☒ None
 ☐ Card Mailer
 ☐ PIN Mailer
 ☐ Both

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:

- On the main menu, click **Configure**. On the side menu, click **Formats**.
- Select a card type in the list and click **Edit**.
- On the side menu, click **Photo Settings**.

PLT-03654, C.2

96

July 2025

General

☒ Format Creates a printed Card

Use Single Template

Template Directory

\\WIN-ZHSOL64AR4V\Users\Public\XML - HFS

Browse

☒ File Name

Portico.xml

Browse

Default Background

Browse

Template Parameters

☒ Track 1 Data + Track 2 Data
 ☒ Print Bin
 ☒ Print Exp. Date
 ☒ Print Full Name
 ☐ Print Misc1
 ☒ Print CVV2
 ☐ Print Last 4
 ☐ Print Business

Card Number Printing

☐ No Masking
 ☒ Masked Card Number
 ☐ Use Alt. Mask

XXXX XXXX XXXX XXXX

Template Options (Use Names from the Options)

☐ Photo
 ☒ Background
 ☐ MiddleName
 ☐ FirstName
 ☐ LastName

Original Card Inventory

Default Embosser

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.
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.

Template Parameters

☒ Track 1 Data + Track 2 Data
 ☒ Print Bin
 ☒ Print Exp. Date
 ☒ Print Full Name
 ☐ Print Misc1
 ☒ Print CVV2
 ☐ Print Last 4
 ☐ Print Business

PLT-03654, C.2

97

July 2025

Advanced

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

File Naming Convention

BIN_LAST5

☒ Enable Background Selection

☒ Enable Custom Backgrounds

Custom Background Search Path

Browse

File Storage Path

\Images\Custom

☐ Enable Photo ID

Height

1

Width

1

☒ Aspect
 ☐ Fixed

Set

File Storage Path

\Images\Photo

CARDNUMBER

BIN_Last4CN

CARDNUMBER

MEMNUM_SSN

SSN

LAST5

MISC1_MISC2

MEMNUM_LAST5

BIN_LAST5

BIN4_LAST5

BIN7_MEM_LAST5

BINLAST5

BINLAST5SSMEMNUMBER

BIN_LAST5SS_MEMNUMBER

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:

- On the main menu, click **Configure**. On the side menu, click **Formats**.
- Select a card type in the list and click **Edit**.
- On the side menu, click **Card Status**.

☒ Use Default Selection

CardStatus

Instant

New

Re-Issue

Replacement

Mail

Add

Edit

Delete

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 (i.e., 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

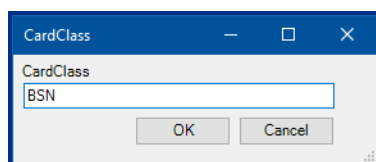
When there is more than one card class assigned to a BIN, the card class for each format is chosen in the **Order Card Job Information** panel.

To display the card class settings:

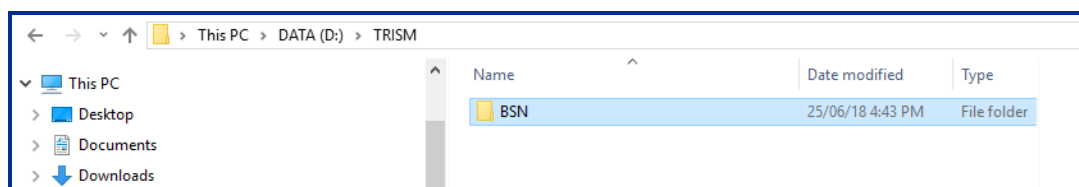
1. On the main menu, click **Configure**. On the side menu, click **Formats**.
2. Select a card type in the list and click **Edit**.
3. On the side menu, click **Card Class**.

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 are modified.

7.5 Devices

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

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

Device License Allowed: 20
Device License Used: 4 License Device

Index	Name	Address	Port	ServiceIP & Port
1	DTCii	10.244....	7575	10.244.69.138 1234
2	Printer B6060933	10.244....	1235	10.244.69.138 1234
3	Printer B4210100	10.244....	10100	10.244.69.138
4	Printer B5240113	10.244....	9955	10.244.69.138

Add Edit Delete

Each device must be licensed. For instructions on adding a device license, see [8.7 License](#).

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

5	Unlicensed Device	10.244.69.1	1212	10.244.69.32 1234
---	-------------------	-------------	------	-------------------

A licensed device is highlighted in blue.

4	Default Printer	10.244...	9955	10.244.69.138 ...
---	-----------------	-----------	------	-------------------

7.5.1 Add a printer or embosser

1. Install the printer according to the manufacturer's instructions.
2. In the TRISM 6 **Devices** window, click **Add**.
3. If the printer is accessed via a network or wireless connection, select **Network**.

☒ Network ☐ Local

Network Settings

Name: DTCii Plus Brance 4

IP Address: 10.236.16.203 Port: 0

Type: Fargo DTCII PLUS

EMV Name: Printer Service IP: 10.236.16.73

Card Mailer:

Options

☐ Secure Mode ☐ Extended Errors ☐ Topper ☐ Auto Verify ☐ Read First ☐ Batch

Data Encryption Key:

Minimum % for Alert: 0

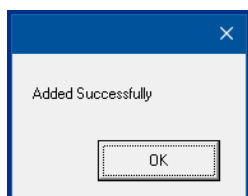
Photo Settings

Horizontal Alignment: 0 Vertical Alignment: 0

Page Height: 213 Page Width: 338

Job Settings OK Cancel

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 6 **Devices** window, click **Job Settings**.

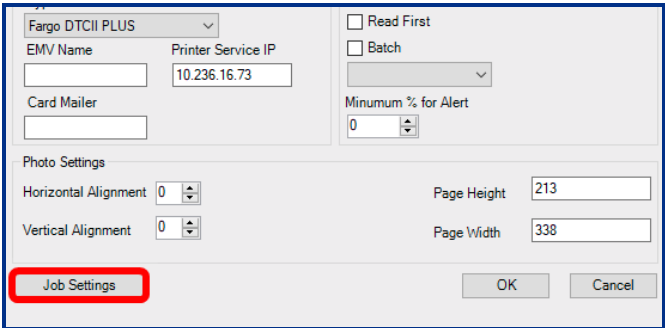
2. The following form is displayed to adjust the settings for the HDP600ii printer.

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.

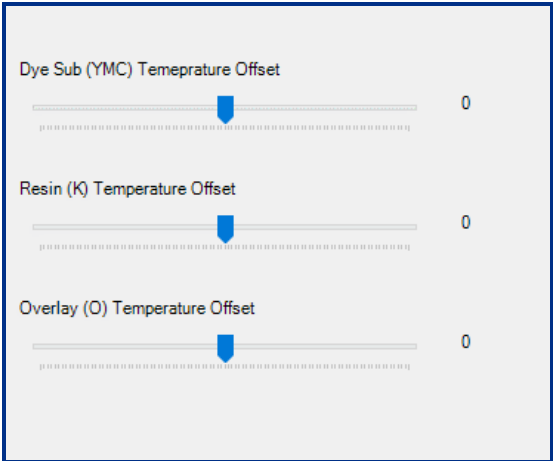
Job Settings for DTCii Plus Printer

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

- In the TRISM 6 **Devices** window, click **Job Settings**.



- 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's **Active Directory** can be automatically entered in TRISM. If Active Directory is enabled, usernames and passwords cannot be changed using TRISM 6. The computer in use must be part of a domain, not a workgroup. If the computer is part of a workgroup, 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 6 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.

☒ Enable Active Directory
☐ Use Nested Groups
 Domain
 Trism.test.com
 Get Domain Groups

Settings
 Users
 Template
 Template Group
 Set Clear
 Previous Groups

OK Cancel

7.7 Branches

Each branch must be licensed. For instructions on adding a branch license, see [8.7 License](#).

- On the main menu, click **Configure**. On the side menu, click **Branches**.

Branch License Allowed: 21

Branch License Used: 2

License Branch

BranchID	Branch Name
Central	Central Branch
Eden Prairie	EP Branch

Add

Edit

Delete

Quick Add

- 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

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

Branch ID

Central

Address 1

City

Branch Name

Central Branch

Address 2

State

Zip

Vaults

Description

Default Vault

Add

Remove

Devices

Description

DTCi

Printer B6060933

Printer B4210100

Printer B5240113

Add

Remove

PC's/Users/Ranges

Description

Tablet3

TRISM_QA01

USMINL-BDSVZF2

nuvision

USMINL-3ZGJD12

SurfacePro

USMINS-TRISM01

ADMIN01

USMINL-3ZGJD12

Add

Remove

BINS

Description

1. ATM

2. Consumer

3. Business

4. Portico 1

5. Portico 2

6. Import Testing

7. Card Services Test

Add

Remove

OK

Cancel

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

Description	
Default Vault	
Central	

Add New OK Cancel

- 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**.
- Enter the vault name and location, then click **OK**.
- To add card stock to a vault, select the vault and click **Add**.
- Select the card stock to add, enter the quantity of cards, and any comments required by your financial institution. Click **Add**.

Select Card Stock: Blank White Quantity: 400

Comments: Added 6/26/2018 by John Smith

Add Cancel

- The vault inventory is updated.

Branch

Name: New Vault

Address 1: 123 Main St

Address 2:

City: Anyville

State: MN Zip: 10203

Description	Number of Cards
Blank White	400

Update Information Print Inventory Add Edit Delete

7.7.2 Add devices to a branch

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

Description	
DTCii	
Printer B6060933	
Printer B4210100	
Printer B5240113	

Add Remove

- Select an existing device and click **OK** or click **Add New** to set up a new device (see [7.5.1 Add a printer or embosser](#)).

Description	
DTCii	
Printer B6060933	
Printer B4210100	
Printer B5240113	
Matica 8300 XID QA	

Add New OK Cancel

- To make one of the devices this branch prints to by default, select the device from the **Devices** list and click **Make Default**. This step is not required.

Branch ID: Central Address 1: City: State: Zip:

Branch Name: Central Branch Address 2:

Vaults

Description
Central
Default Vault

Add Remove

Devices

Description
DTCii Card Printer
Fargo
HDPI6600
T3 DTCii plus

Add Remove **Make Default**

PC's/Users/Ranges

Description
AAHIDGNCZN93
tablet3
Demo Tablet6
DESKTOP-H37N15V
USEULL-D9M3JR2
WIN-T730Q3898KS
Demo Tablet2
tablet2

Add Remove

BINS

Description
1. ATM
2. Consumer
3. Business
4. Portico
5. portico2
6. Precision
7. consumer copy2
17. jeffcontactless

Add Remove

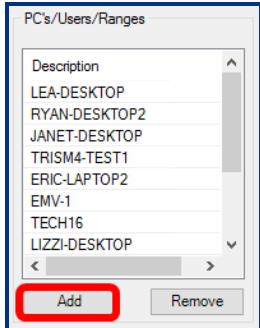
* Yellow Background on a Device Notes it is the Default Printer for this Branch.

OK Cancel

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.



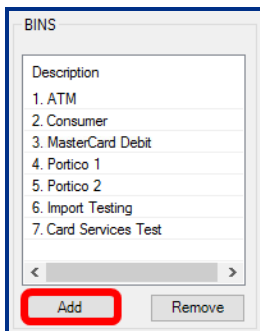
3. Select the method and enter the PC Name, IP Address/Range, or User Name and click **OK**.

7.7.4 Add BINs to a branch

Before adding BINs to a branch, the BINs must be set up. See [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.



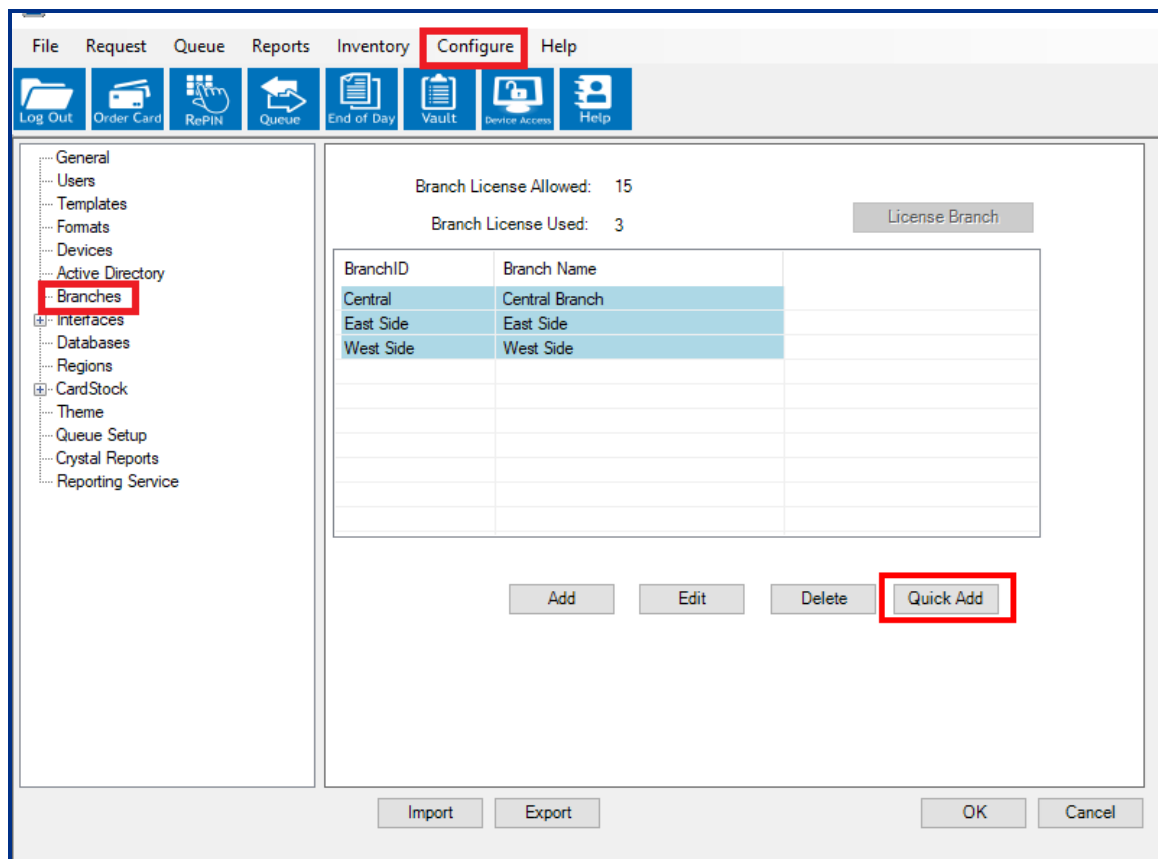
3. Select a BIN and click **OK**.

7.7.5 Branch Add - Quick Add feature

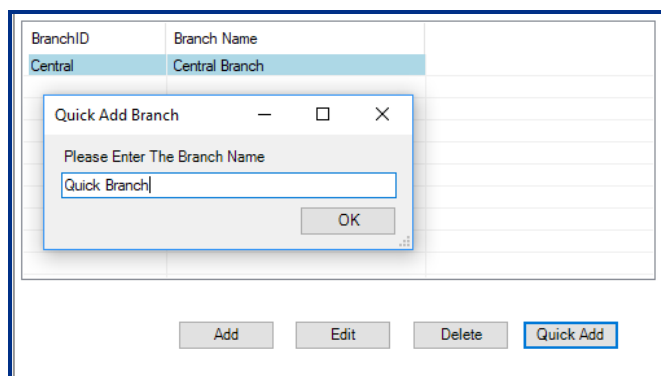
The Quick Add feature adds efficiency for configuring a new device, branch, and vault.

Note: Using this feature assumes the printer has been installed on the server.

1. Log in to TRISM using the User ID for the administrator level.
2. On the main menu, click **Configure**. On the side menu, click **Branches**. Click **Quick Add**.

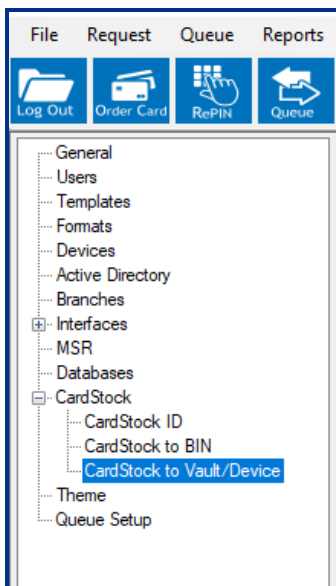


3. Enter a **Branch Name** and click **OK**.



The branch name is added. In addition, a vault and device with similar names are added to the branch.

4. Click **OK**.
5. On the **Configuration** screen, click **Devices**. A new printer was added with the name you created in step 3. Select the device and click **Edit**.
6. Edit the following fields to configure the printer:
 Name: The name exactly as it is displayed in Devices and Printers.
 IP Address: IP of the installed printer.
 Port: Any number. This setting is not used, but must be filled in.
 Type: Type of printer.
 Print Service IP: IP address of where the printer is installed, and the Card Printer Service is running.
 Photo Settings: Set both the **Horizontal** and **Vertical Alignment** to **6**.
 Click **OK** and restart **Card Printer Service**.
7. A matching vault was created with card stock added in step 3. If new card stock is created, that stock is automatically added to each vault.
8. On the **Configuration** screen, click **CardStock** > **CardStock to Vault/Device**.



9. From the **Select Vault** list, select the new vault.

10. Select the **Card Stock**, **Device**, **Hopper**, and **State**. Click **Add**.

Select Vault
Quick Branch

Card Stock ID	Card Stock Description	Device	State	Hopper	

Remove

Add

Select Card Stock
EMV

Select Device
Quick Branch Printer

Hopper
1

State
Ready

The card stock is now linked to the vault and device.

The branch and printer have been configured.

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 **Configure**. On the side menu, click **Interfaces**.

... General
 ... Users
 ... Templates
 ... Formats
 ... Devices
 ... Active Directory
 ... Branches
 ... Interfaces
 Interface Settings
 Interface Bin Settings
 ... Databases
 + CardStock
 ... Theme
 ... Queue Setup

Interface Portico

Setting	Value
BRANCHID	000
CREDITUNIONID	22222
LOGGINGMAX	100
LOGGINGMIN	0
OVERIDEACTIVATION	N

Add Edit

StockName	StockQualifier
Blank white	654321

Add Edit Delete

OK Cancel

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

General

Users

Templates

Formats

Devices

Active Directory

Branches

Interfaces

Interface Settings

Interface Bin Settings

Databases

CardStock

Theme

Queue Setup

Interface

Card Printer Service

Bin

123456

Setting	Value
DontActivate	N
DontAdd	N
DontReIssue	N
DontRePIN	N
DontSearch	N
Enabled	Y

Add

Edit

OK

Cancel

7.9 Databases

Change logging options for SQL databases.

On the main menu, click **Configure**. On the side menu, click **Databases**.

Logs

Days to Keep: 30

Purge Time: (24h Format) 02:00

7.10 Card Stock

On the main menu, click **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, then click **Add**.

Card Stock ID	Card Stock Description	EMV
123	EMV	☒
444	Sample Test	☐
456	Blank White	☐

Card Stock ID

Card Stock Description

☐ EMV

456

Blue pre-printed

☒ EMV

Add

Delete

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**.

Card Stock Description	BIN / ISO
EMV	222456
EMV	123456
EMV	222789
Blank White	222456

Select CardStock

Remove

EMV

Select BIN / ISO

555556

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 (not available with all printers).

4. Click **Add**, then **OK**.

Select Vault

Default Vault

Card Stock ID	Card Stock Description	Device	State	Hopper
123	EMV	DTCii	Paused	1
123	EMV	Printer B6060933	Paused	1
123	EMV	Printer B4210100	Paused	1
123	EMV	Printer B5240113	Paused	1
444	Sample Test	DTCii	Ready	1

Select Card Stock

Remove

Select Device

Add

Hopper

State

7.10.4 Add a new BIN or card stock

- If adding a new BIN, add a new format (see [7.4 Formats](#)).
 - Add a new card stock ID (see [7.10.1 Card Stock ID](#)).
 - Link the new card stock ID to the appropriate BIN (see [7.10.2 Card Stock to BIN](#)).
 - If you are using different BINs for different branches, add the BIN to the branch (see [7.7.4 Add BINs to a branch](#)). If you are using the same BINs for all branches, go to the next step.
 - Add card stock to the branch vault (see [7.7.4 Add BINs to a branch](#)).
 - Link the new card stock to the vault and device (see [7.10.3 Card Stock to Vault/Device](#)).
 - Card stock can now be added to devices in Device Access (see [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.

From the main menu, select **Configure**, then from the side menu, click **Theme**.

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

Order Card/Repin

Required

Select

Editable

Select

Single Required

Select

7.13.1 Add a region

1. On the Regions configuration screen, click **Add**.

General
Users
Templates
Formats
Devices
Active Directory
Branches
+ Interfaces
Databases
Regions
+ CardStock
Theme
Queue Setup
Crystal Reports

☒ Enable Regions

Region ID	Region Name
01	South Region

Add Edit Delete

OK Cancel

2. Enter a **Region ID**, **Region Name**, and click **OK**.

The screenshot shows a dialog box for configuring a region. At the top, there are two input fields: "Region ID" and "Region Name". Both fields are empty and have a red rectangular highlight around them. Below these fields is a large, empty text area labeled "Branches". At the bottom of the dialog box, there are four buttons: "Add", "Remove", "OK", and "Cancel". The "OK" button is highlighted with a red rectangular border.

7.13.2 Add a new branch to a region

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

☒ Enable Regions

Region ID	Region Name	
01	South Region	
002	North Region	

Add

Edit

Delete

2. On the Edit screen, click **Add**.

3. From the list, select the branch to add to the region and click **Add**.

Regional Branches

Branch

das

Test12

sdasadsad

Add Cancel

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

☒ Enable Regions

Region ID	Region Name
01	South Region
002	North Region

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

Region ID: 12345

Region Name: North West

Branches:

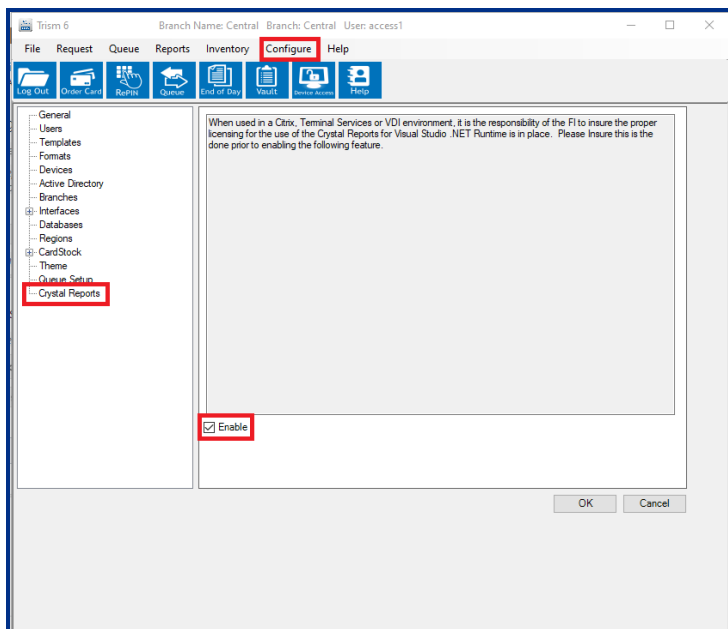
- Central Branch
- Test Branch

Buttons: Add, Remove, OK, Cancel

7.14 Crystal Reports licensing

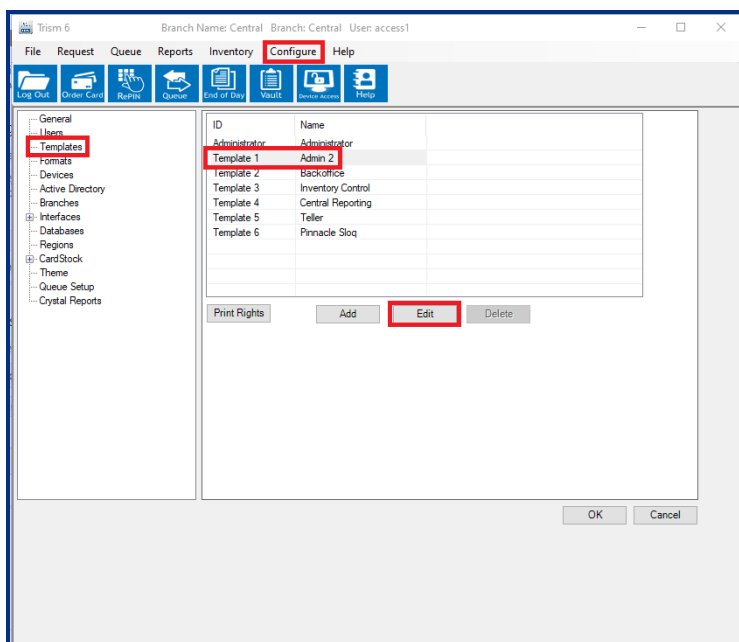
Crystal Reports version 13.026 requires a license agreement to be accepted if using Citrix/remote environments. TRISM Client 6.2 and above detects if the Client is launched in a remote session and disables Crystal Reports from being used if the license acceptance has not been checked. Card production can still occur but when Crystal Reports is called to print a report, a message is displayed stating Crystal Reports is not licensed.

To enable the license agreement, select **Configure > Crystal Reports** and select **Enable**.

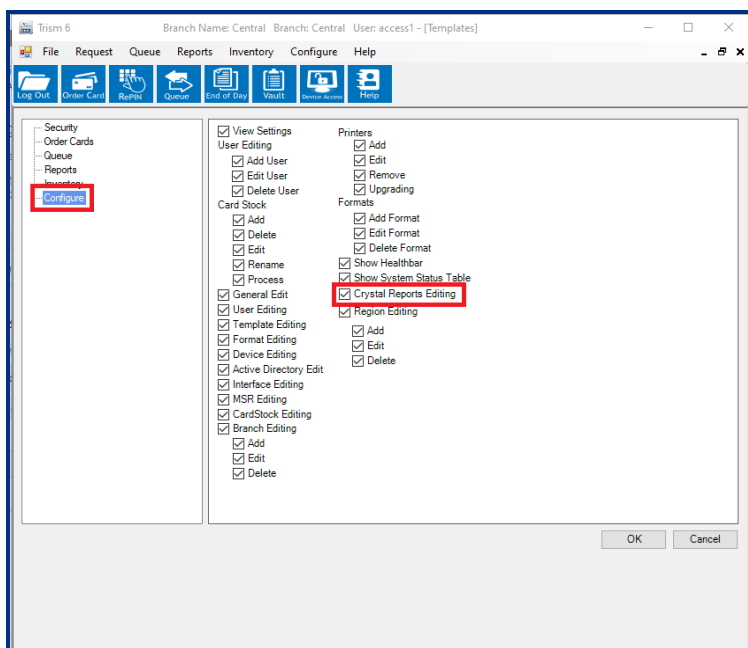


By default, this setting is disabled in all User Templates. If the financial institution does not log in with Access1, then the setting must be enabled in a User Template to show the settings, then disabled to remove it.

To enable the setting, select **Configure > Template**, select the template and click **Edit**.



Select **Crystal Reports Editing** and click **OK**.



The financial institution should then log into TRISM with a user on the edited template to enable the setting.

Section 08

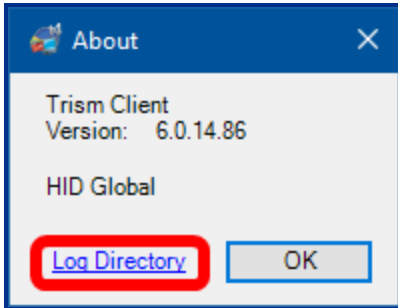
Help

8.1 About

View the version of TRISM 6 currently installed.

On the main menu, click **Help** > **About**, or click .

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.

- On the main menu, click **Help > Data Log**.
- Select the dates to search by in the **Start Date** and **End Date** drop-down menus.
- Select the service in which to view the log. Click **Search**.

Start Date

End Date

01 June 2018

27 June 2018

HID TRISM Monitor

Search

500 Rows

Time Stamp	Message	Assembly	Data
4/1/2015 8:43:05 AM	Legacy logging method all check dat...	DSI BP...	Encountered exception while calling trismwsservicehost.Open() Messa
4/1/2015 8:43:02 AM	Starting Service - Version = 4.1.0.3009	DSI BP...	
4/1/2015 8:29:15 AM	Legacy logging method all check dat...	DSI BP...	Encountered exception while calling trismwsservicehost.Open() Messa
4/1/2015 8:28:57 AM	Starting Service - Version = 4.1.0.3009	DSI BP...	

Source

Date/Time: TimeStamp

Priority PriorityLvl

Severity: SeverityLvl

Machine Name: Machine Name

Purge

Export

OK

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 **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. Click **Purge** to delete the log.

Start Date: 27 June 2018 End Date: 27 June 2018

Calculation Service: Search

500 Rows

TimeStamp	Message	Assembly	Source	TargetS...	Data
5/26/2015 8:22:37 AM	Invalid li...	DSI Ultr...	DSI Inte...	Demotel...	
5/26/2015 8:22:37 AM	Invalid li...	DSI Ultr...	DSI Inte...	Demotel...	
5/21/2015 5:54:59 AM	Invalid li...	DSI Ultr...	DSI Inte...	Demotel...	
5/21/2015 5:54:59 AM	Invalid li...	DSI Ultr...	DSI Inte...	Demotel...	
5/20/2015 1:48:29 PM	Invalid li...	DSI Ultr...	DSI Inte...	Demotel...	
5/20/2015 1:48:29 PM	Invalid li...	DSI Ultr...	DSI Inte...	Demotel...	

Source: Date/Time: Timestamp

Source: Source

Target: Target

Machine Name: Machine Name

Purge Export OK

8.5 Client Information

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

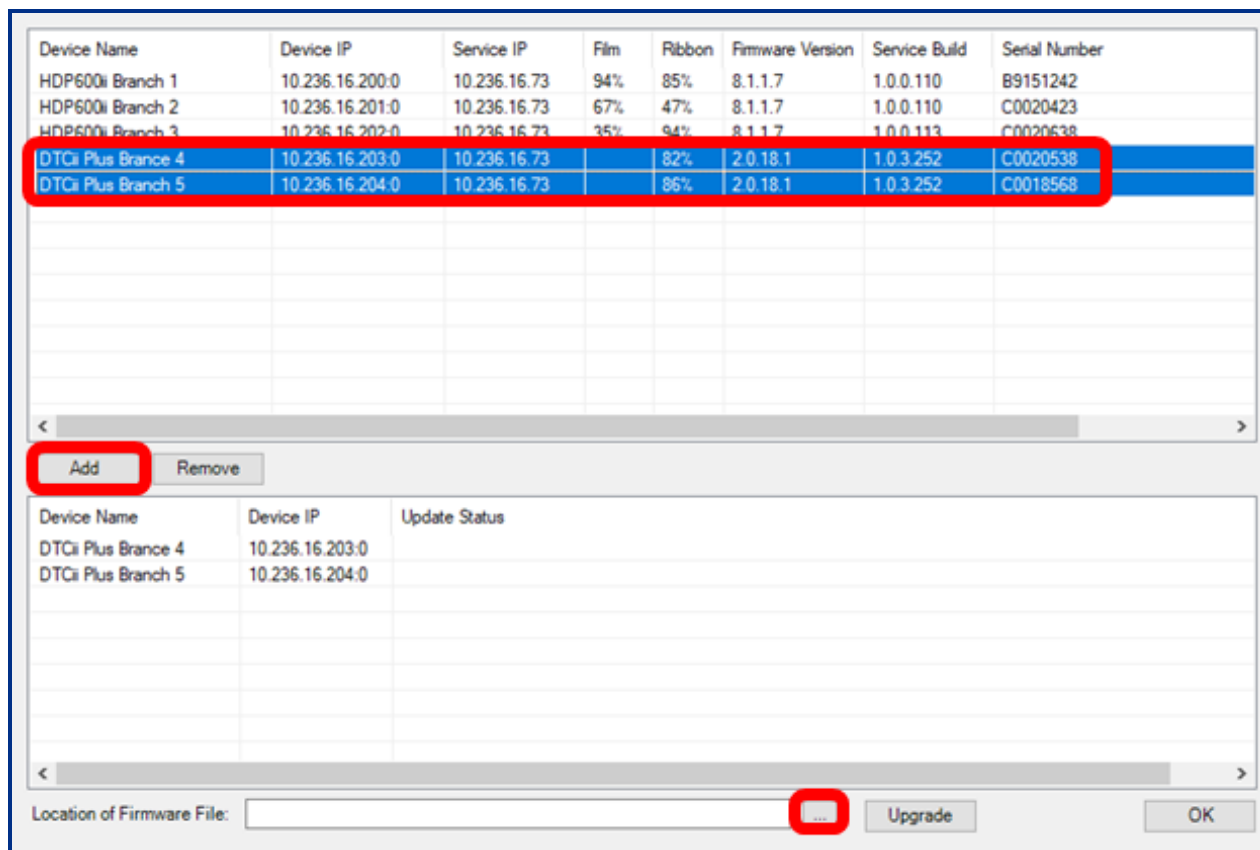
Client Information displays a list of each TRISM workstation, and the following information associated with each workstation:

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

8.6.1 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.



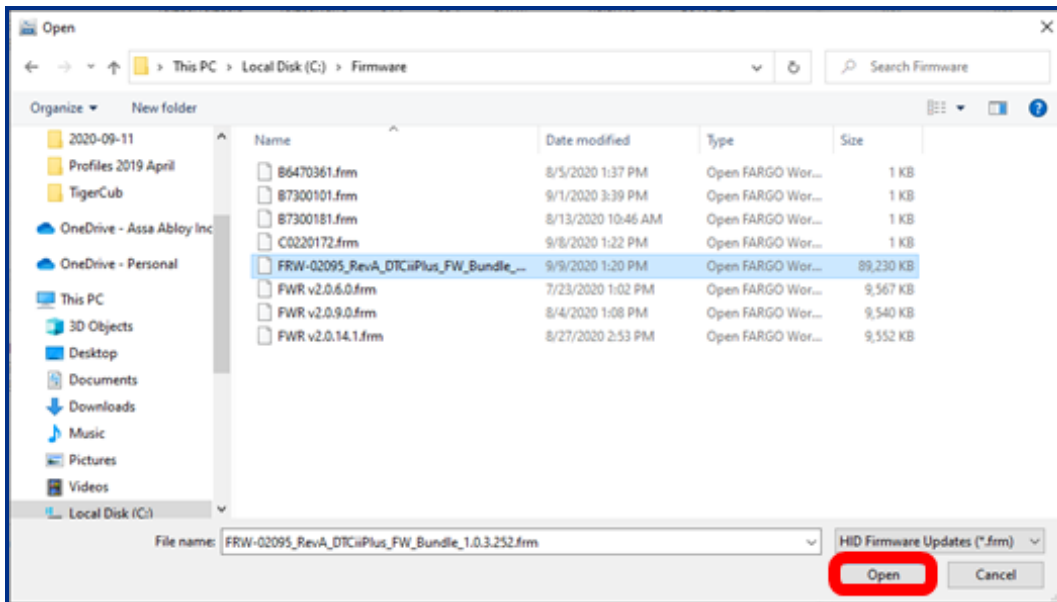
Device Name	Device IP	Service IP	Film	Ribbon	Firmware Version	Service Build	Serial Number
HDP600i Branch 1	10.236.16.200:0	10.236.16.73	94%	85%	8.1.1.7	1.0.0.110	B9151242
HDP600i Branch 2	10.236.16.201:0	10.236.16.73	67%	47%	8.1.1.7	1.0.0.110	C0020423
HDP600i Branch 3	10.236.16.202:0	10.236.16.73	35%	94%	8.1.1.7	1.0.0.113	C0020638
DTCi Plus Branch 4	10.236.16.203:0	10.236.16.73	82%	86%	2.0.18.1	1.0.3.252	C0020538
DTCi Plus Branch 5	10.236.16.204:0	10.236.16.73			2.0.18.1	1.0.3.252	C0018568

Device Name	Device IP	Update Status
DTCi Plus Branch 4	10.236.16.203:0	
DTCi Plus Branch 5	10.236.16.204:0	

Location of Firmware File:

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**.



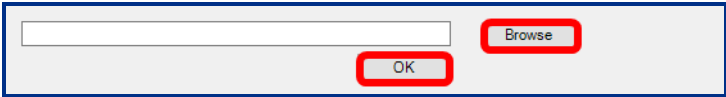
4. Once the printers and firmware are selected, click **Upgrade** to begin the upgrade process.

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

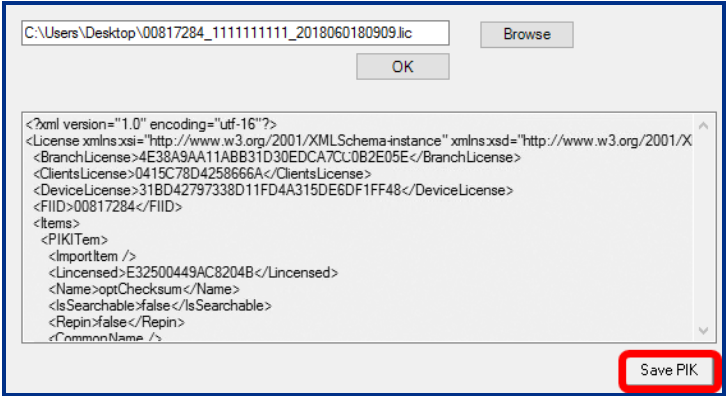
8.7 License

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

- On the main menu, click **Help > License**.
- Click **Browse** to navigate to the license file.
- Click **OK**.



- 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 **Help > System Status**.

Service	Version	Start Time	Last Update Time	Last Status
DSI Calculation Service	5.0.0.0	13/02/2018 09:31:34	20/02/2018 12:01:43	Running
Portico	6.0.0.0	26/06/2018 08:32:49	26/06/2018 15:32:59	Ready
PPC Collector	6.0.10.0	13/06/2018 14:19:43	13/06/2018 14:19:44	Starting
Passport Import	6.0.0.0	15/06/2018 08:43:34	15/06/2018 09:12:08	Stopped
Core1	6.0.5.0	01/11/2017 16:56:26	25/05/2018 09:54:45	Ready
Core2	6.0.5.0	01/11/2017 16:56:29	25/05/2018 09:54:45	Ready
Card Printer Service	6.0.6.64	26/06/2018 08:32:44	27/06/2018 06:36:39	Ready

- Green:** status table in database is running.
- Red:** status table has not been updated for the number of minutes specified by the **Configure > General > Minutes before Red Icon (Down) on HealthBar** option (see page [7.1 General](#)).

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 Server 2012 R2, 2016, 2019, 2022	Windows 8/8.1, 10, 11
Database software	SQL Server 2016 (SP2), 2017, 2019, Standard, Express, or Enterprise Edition	N/A

Note:

- A dedicated server and SQL instance is strongly recommended on the server. High volumes of printers, mixed printer environments or embossers may require a separate printer server.
- It is recommended to use the Standard or Enterprise edition of SQL Server in a system 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" x 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 x 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 x 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 x 640

A.3 Custom image guidelines

Your financial institution reserves the right to determine, in its sole discretion, whether a submitted image will be 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.
Log into Thost	Allows you to log in to the T-Host server.
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.

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 tool bar and to access the Order Card button on the quick launch tool bar.
View Actions	Allows you to access the Request menu on the main tool bar.
Edit Permissions	Allows you to access the Request > Edit Permissions option on the main tool bar.
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 login.
PIN Mailer Only	Allows you to access the Request > PIN Mailer option on the main tool bar.
Print Transactional 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 Transactional Report	Allows you to access the Print Transactional Report option to mask the customer data on the report. This is for security.
Force Masked Card Number on Trans Report	Allows you to access the Print Transactional Report option to mask the card number on the report.
Read a Card	Allows you to access the Request > Read a Card option on the main tool bar.
CVV2 Calculator	Allows you to access the Request > CVV2 Calculator option on the main tool bar.
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 tool bar and to access the Queue button on the quick launch tool bar.
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 tool bar 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 tool bar and the Reports button on the quick launch tool bar.

Permission	Description
View Local Reports	Allows you to see the predefined reports as well as custom reports that have been saved.
Run End of Day Reports	Allows you to access the End of Day option in the Reports menu of the main tool bar and the End of Day button on the quick launch tool bar.
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 tool bar.
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 tool bar.
Print Reports	Allows you to print reports.
Data Log	Allows you to access the Data Log option in the Help menu of the main tool bar.
Error Log	Allows you to access the Error Log option in the Help menu of the main tool bar.
Client Information	Allows you to access the Client Information option in the Help menu of the main tool bar.
Device Access	Allows you to access the Device Access report in the Reports menu of the main tool bar.
Vault Supply	Allows you to access the Vault Supply Tracking report in the Reports menu of the main tool bar.
Device Error	Allows you to access the Device Error report in the Reports menu of the main tool bar.
Spoiled Card	Allows you to access the Spoiled Card report in the Reports menu of the main tool bar.
Spoiled Card For all Branches	Allows you to access the Spoiled Card report with all branches available in the Reports menu of the main tool bar.
Branch Activity	Allows you to access the Branch Activity report in the Reports menu of the main tool bar.
Device Access Report (CardStock)	Allows you to access the Device Access report in the Reports menu of the main tool bar.
Background	Allows you to have access to the Background report in the Reports menu of the main tool bar.
Same PINS	Allows you to have access to the Same PINS report in the Reports menu of the main tool bar.
Different PINS	Allows you to have access to the Different PINS report in the Reports menu of the main tool bar.
Historical Transfers	Allows you to have access to the Historical Transfers report in the Reports menu of the main tool bar.
Historical Vault	Allows you to have access to the Historical Vault report in the Reports menu of the main tool bar.
Historical Central Vault	Allows you to have access to the Historical Central Vault report in the Reports menu of the main tool bar.
Customer Removal	Allows you to have access to the Customer Removal tool in the Reports menu of the main tool bar.

A.4.5 Inventory

Permission	Description
View Inventory	Allows you to access the Inventory menu of the main tool bar.
Device Unlock	Allows you to access the Device Unlock function (card add and removal) in the Inventory menu of the main tool bar.
View Card Stock	No longer used.
View Vault Inventory	Allows you to access the Inventory > Vault Inventory option in the main tool bar. 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/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.

A.4.6 Configure

Permission	Description
View Settings	Allows the user to access the Configure option on the main tool bar
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.
MSR Editing	Allows you access to the MSR 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.

Permission	Description
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/green status lights in the main tool bar.
Show System Status Table	Allows you to access the Help > System Status option of the main tool bar.

A.5 Troubleshooting

A.5.1 EMV

Issue	Possible Causes/Resolutions
Job stuck in Ready Photo	- Card Printer Service is not running - Printer name in Windows Devices & Printers is not identical to the device name in TRISM client¹ - Printer device type not correct in TRISM Devices¹ - Incorrect Card Printer Service IP in TRISM Devices¹ - Card Printer Service not running as local admin - Card Printer Service domain login is incorrect ¹Any changes to devices in the configuration menu will 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 device hopper and loaded correctly - Verify all fonts are loaded on server by pulling in .xml via 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 6 and they should still work correctly.
No settings for Card Printer Service in Interface Settings	EMV is not PIK'd - load new PIK



Issue	Possible Causes/Resolutions
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 6.x.	C.2
June 2024	Reverts this document to cover TRISM 6.x. For TRISM 7.x, see <i>HID TRISM Financial Instant Issuance Administrator Manual</i> (PLT-07643).	C.1
May 2023	Updated for version 7.0	C.0
July 2022	Updated system requirements.	B.8
September 2021	Added subsection in Section 2 for the HSM XT installation-Mastercard CVC3 fix.	B.7
December 2020	Added subsections in Section 7 for job settings.	B.6
October 2020	Added subsections in Section 7 for Regions and Section 9 for Device information. Updated system requirements.	B.5
May 2020	Updated note in Section 3 to specify Verifone and P200 pin pad functionality.	B.4
March 2020	Removed support for Windows Server 2019.	B.3
January 2020	Updated card type format for EMV and system requirements.	B.2



hidglobal.com

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

© 2025 HID Global Corporation/ASSA ABLOY AB.

All rights reserved.

PLT-03654, Rev. C.2

Part of ASSA ABLOY