

Inside EMV

Feature Reference

Date: April 8, 2020



Verifone[®]

Inside Contact EMV

Using This Feature Reference

This Feature Reference provides detailed information on how to configure and use the Inside EMV feature on two Verifone site controllers: Commander Site Controller and Sapphire.



As of the 2020 revision, this document now discusses contactless EMV. Support for Contactless EMV begins with Commander software Base 51.

Verifone's implementation of EMV involves the VIPER EPS and the associated POPs (MX 900 Series and M400 PINpads) only. The POS platforms (Ruby, Ruby2, RubyCi, and Topaz) are not involved in EMV processing so no POS overviews or configurations are covered in this document.

This feature document contains the subsections listed below:

- **Overview** - This section contains a brief description, requirements and the supported hardware configurations for the EMV feature on the related Site Controller.
- **Configuring** - This section contains information on how to configure the EMV feature on the related Site Controller.
- **Using** - This section describes using the EMV feature.
- **Reporting** - This section contains sample reports with detailed report descriptions for the EMV feature
- **Troubleshooting** - This section provides basic troubleshooting steps if EMV transactions are not performing as expected.

Verifone, Inc.
2560 N. 1st St., Suite 220
San Jose, CA 95131
Telephone: 408-232-7800
<http://www.verifone.com>

© 2020 Verifone, Inc. All rights reserved.

No part of this publication covered by the copyrights hereon may be reproduced or copied in any form or by any means - graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems - without written permission of the publisher.

The content of this document is subject to change without notice. The information contained herein does not represent a commitment on the part of Verifone. All features and specifications are subject to change without notice.

Verifone, Ruby SuperSystem, and Secure PumpPAY are registered trademarks of Verifone, Inc. Ruby Card, iOrder, and Commander Site Controller are trademarks of Verifone. All other brand names and trademarks mentioned in this document are the properties of their respective holders.

Revision History

Date	Description
September 15, 2016	Initial Documentation Release
April 8, 2020	Added information on contactless EMV, updated address information, support information; added information on Quick Chip.

Contents

Inside EMV	1
Overview	1
Introduction	2
System Requirements	3
Supported Hardware	3
Supported Software	3
Contact Software Support	3
Contactless Software Support	4
Configuring EMV	5
Configuration Client Access	5
Commander Site Controller	5
Sapphire/Viper	5
Basic Configuration	6
Enabling EMV	6
EMV Tables	7
Updating PIN pads	9
Advanced Configuration	11
Application ID Configuration	11
AID Stand-In Configuration	12
CAPK Configuration	15
AID Rules	16
AID Selection Menu	17
Creating AID Rules	18
Using EMV	21
Performing an EMV Transaction	21
Types of EMV Transactions	22
Normal Sale - EMV Chip Read	22
Other EMV Transactions	25
Normal Inside EMV Flow	25
Exception Flow	27
Attempting to Swipe a Chip Card	27
Failed Chip Read	27
Technical Fallback Processing	28
Contact EMV: Manual Entry	28
Stand-In Processing	29
Receipts	30
Approved Transaction Receipts	30
Declined Transaction Receipts	31
Reporting	32
EMV Transaction Report	33
EMV Configuration Report	34
EMV Certificate Authority Public Key (CAPK) Report	36
EMV Transaction Statistics Report	37
EMV Failure Report	38

EMV Fallback Report	39
Troubleshooting	40
Steps of an EMV Transaction	40
EMV Menu Access Denied	41
Error Saving EMV Configuration Settings	45
EMV Initialization	45
Initialize POP	45
POP Configuration Status	46
No “Insert Card” Prompt for Contact EMV	47
No Transactions Processing as EMV transactions	47
Only Some PIN Pads Process EMV	48
Swiping an EMV Card is Allowed Without First Requiring a Chip-Read	48
Swiping Not Allowed After a Failed Chip-Read	48
An Inserted Card is Refused or Declined	48
Receipt is Slow to Print	49
Intermittent Chip Card Read Failure	49
Cleaning Process	49
System Diagnostics	51
Accessing System Diagnostic Information	51
Viewing System Diagnostic Information	51
POP Status for POP ID	52
POS Status for Workstation ID	52
Glossary of Terms	53
Supplemental Information	57
Verifone-Certified AIDs	57
Contact	57
Contactless	58
EMV Transaction Tags	58

1 INSIDE EMV

Overview

EMV is the standard for credit card processing. It describes a transaction between a chip card and an EMV-enabled terminal. EMV transactions are much more secure than magnetic-stripe-card transactions.

This feature document describes Verifone's implementation of inside EMV within the Commander Site Controller environment. It serves as an Overview, Configuration Guide, Usage Guide, Reporting Overview, and provides Troubleshooting Information for the EMV feature.

A [Glossary of Terms](#) is provided to assist with understanding content and terminology presented in this Feature Reference.

Introduction

This document covers how to enable Contact and Contactless EMV transactions. Contact EMV refers to transactions performed by inserting the chip card into the EMV slot on the device. Contactless EMV refers to transactions performed by tapping or waving a card or device by the terminal. This includes ApplePay, GooglePay, and similar services.

During Contactless EMV transactions, an RFID reader built into the screen on the MX 900 and M400 PINpads reads the chip on the card when the Consumer taps on or waves the card near the screen.



Not all Chip Cards are capable of contactless transactions. If the chip is contactless enabled it will have this symbol (a logo owned by EMVCo, LLC.) on the card.



Prior to initiating Commander Site Controller EMV configuration, contact the Front-End Processor and Merchant Service Provider to confirm the merchant account is ready for EMV processing. Refer to the appendices for processor-specific configuration details.

System Requirements

Supported Hardware



EMV implementation requires PIN pad hardware with EMV Chip Reader capability.

- MX 900 Series: MX 915 and MX 925, M400
- Commander Site Controller/RubyCi with Topaz
- Commander Site Controller/RubyCi with Ruby2
- Sapphire V910/V920 with Topaz (Contact ONLY)
- Sapphire V910/V920 with Ruby (Contact ONLY)

Supported Software

Contact Software Support

- **Commander Site Controller/RubyCi:** Production Software Base 42 and higher.
- **Sapphire:** Production Software Base 188+, and do not support Contactless EMV.
- **All MX PINpad devices:** ViperPAY 4.xx+.
- **MX 900 Series devices:** Kernel 7.00+.



POS System Software may be eligible to Upgrade through Verifone's Remote Software Delivery. For more information visit support.verifone.com and select Technical Support > Support Articles > Petro & Convenience > Products and Services > Software Updates (VRSD).

Contactless Software Support

- **Commander Site Controller/RubyCi:** Production Software Base 51+.
- **Sapphire:** Does **not** support Contactless EMV.
- **All MX PINpad devices:** ViperPAY 4.06.04.03+.
- **MX 900 Series devices:** Require a PIN pad firmware upgrade in order to support Contactless EMV: CONTACTLESS SUPPORT UPDATE VERSION 1.30.04A6 FOR MX 900 SERIES. You can find this upgrade on the Verifone Premier portal under **Manage > Petro Downloads > MX 900 > OS Software**.



The MX 900 PINpads must have the contactless firmware upgrade applied in order for contactless functionality to work. A Verifone Authorized Service Contractor (VASC) can apply the upgrade, or the Verifone Helpdesk, if the device is using the Service and Maintenance (SAM) feature.

See [Troubleshooting: System Diagnostics](#) for details on determining software versions of MX and POS devices.

Configuring EMV

By default, the Verifone site controller is installed with EMV disabled. How EMV is enabled at the site varies depending on the card processor. Some card processors require an EMV-specific download in order to activate EMV. Others, such as Buypass, may require EMV to be enabled within the site controller's payment controller configuration.

Please contact your payment network for more information on enabling EMV at the site level.



Refer to the Network-specific EMV Configuration Guide and/or contact the site's Electronic Payment Host Provider for additional details on configuring your Verifone solution for EMV.

If your payment network requires EMV to be enabled on the site controller, please proceed to the next section. All site-controller enabled EMV configurations are done through Configuration Client.

Configuration Client Access

Commander Site Controller

Access the Configuration Client for Commander Site Controller at the URL provided by your VASC, or by logging into the Configuration Manager in the CSR Functions on the register.

Login to Configuration Client using the Manager login name and current password.

- User Name: Manager
- Password: (** the current valid Manager password **)

Sapphire/Viper

Access the Configuration Client at the URL provided using the credentials provided by your VASC or other Verifone representative.

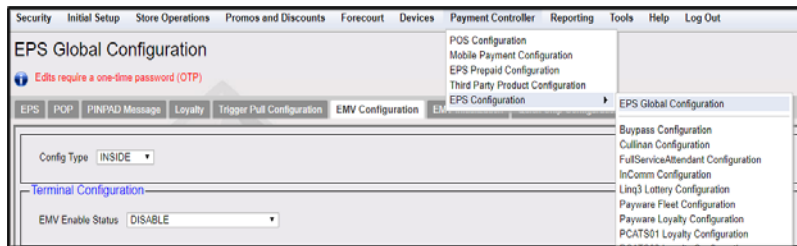
Basic Configuration

The following section provides instructions on how to enable EMV on the Commander Site Controller. Verify the Commander Site Controller is configured with the appropriate hardware and software configurations before proceeding.

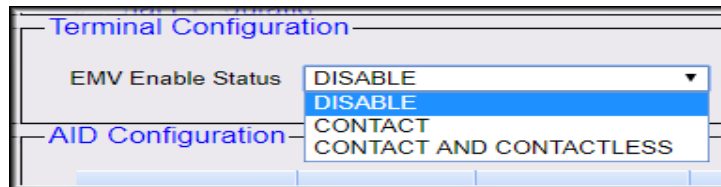
Enabling EMV

In order to process EMV transactions, EMV must be enabled on the Site Controller. Depending on your specific payment interface, EMV may be configured using Viper table downloads, a host PDL, fixed using files distributed with the payment system, or manually enabled.

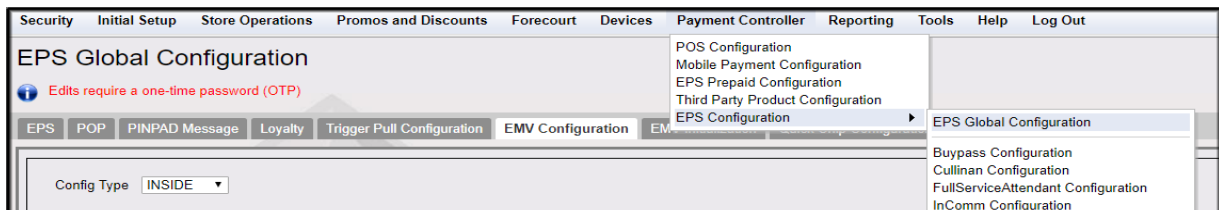
1. Navigate to Payment Controller > EPS Configuration > EPS Global Configuration > EMV Configuration.



2. To enable EMV, click on the drop-down for EMV Enable Status. You can select from CONTACT or CONTACT AND CONTACTLESS.



3. Save the configuration.



EMV Tables

EMV processing requires EMV supporting tables. The EMV tables are usually provided by the Payment Host through downloads.



Refer to the specific card processing network EMV Configuration Guide for details on how to obtain EMV tables.

After performing the EMV configuration as applicable for your network, confirm the EMV table information.

1. Navigate to Payment Controller > EPS Configuration > EPS Global Configuration > EMV Configuration.
2. Application IDs represent the card types supporting EMV processing, and will vary based on the card processing network. Confirm that Application IDs are listed in the AID Configuration section and that the **<Enable>** check box is selected for each.



Changes to this section should be considered advanced configuration.
Do not make configuration changes to this section without a complete understanding of AID parameters. See *Advanced Configuration* for additional details.



WARNING: Verifone *strongly* advises against making changes in this area without a thorough knowledge of the AID parameters, because it could expose the site to chargebacks!

AID	AID Name	Enable	Bypass PIN	Account Type	Allow Standin for AAC	Standin TVR Mask	Standin TSI Mask	Standin Country Code check	Standin Floor Limit
A00000002501	Amex Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000001523010	Discover	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000041010	MC Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000043060	Maestro	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000042203	DEBIT MASTERCARD	<input checked="" type="checkbox"/>	BYPASS	DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000031010	Visa CR/DB	<input checked="" type="checkbox"/>	BYPASS	CREDIT & DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000032010	Visa Electron	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000033010	INTERLINK	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000980840	US DEBIT	<input checked="" type="checkbox"/>	BYPASS	CREDIT & DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000

- The CAPK configuration area is read-only. All configurations shown here are controlled by the card processing network. Ensure that values are listed in the CAPK Configuration. It is best practice to NOT store expiry dates. Current systems do not. The values in your system may differ from what is shown in the screenshot below.

CAPK ID	RID	CAPK Index	Expiry Date
CAPK001	A000000025	04	16-12-31
CAPK002	A000000025	0E	16-12-31
CAPK003	A000000025	0F	17-12-31
CAPK004	A000000025	10	18-12-31
CAPK005	A000000025	97	18-12-31
CAPK006	A000000025	98	18-12-31
CAPK007	A000000025	99	18-12-31
CAPK008	A000000025	C1	20-12-31
CAPK009	A000000025	C2	20-12-31
CAPK010	A000000025	C3	20-12-31

1-10 of 37

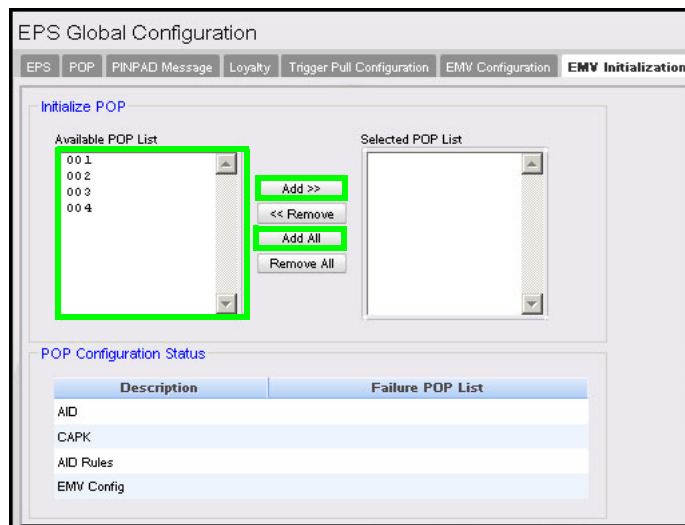
Updating PIN pads

1. Log out of Sales mode and back in to Sales mode on the POS.
The PIN pad will download the new EMV tables when you do so.
2. Verify that the EMV card slip is lit up on the PIN pad.
PIN pad prompts will also change and update to say, "SWIPE, INSERT, OR TAP CARD".



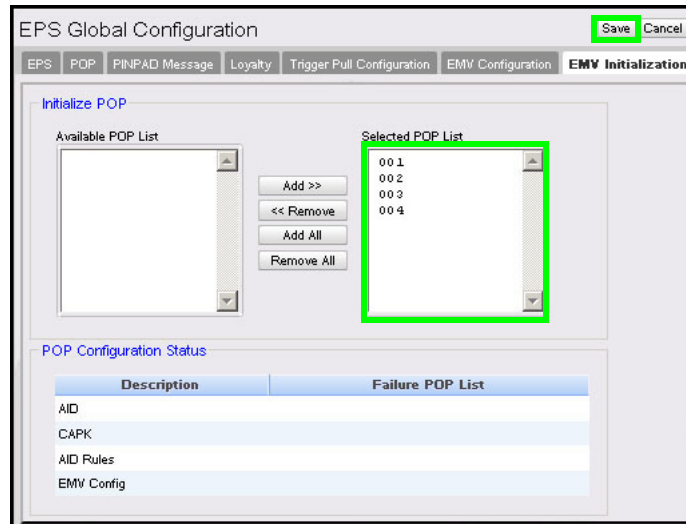
If the PIN pad was not initialized by logging into Sales mode, you can also use the process below to manually initialize individual PIN pads.

3. Navigate to Payment Controller > EPS Configuration > EPS Global Configuration > EMV Initialization.



4. The list of PIN pads that did not update will appear in the *Available POP List*. Select all PIN pads from the *Available POP List*, and move them to the *Selected POP List* using the **[Add>>]** or **[Add All]** buttons. This will instruct the system to update the PIN pads.

5. Click **[Save]** to force an initialization through to the selected PIN pads.



In the event PIN pads are not listed in the POP Configuration Status panel on the EMV Initialization screen, see the Troubleshooting section for more information. PIN pads listed here may not be receiving the proper configurations to run EMV transactions.

Advanced Configuration



WARNING: Verifone strongly recommends that clients do not attempt advanced configuration unless they are experts in EMV AIDs. For most customers, this section is included for reference only.

Application ID Configuration

Application IDs represent the card types supporting EMV processing, and systems that process EMV transactions must specify which AIDs the system can process.



Merchants cannot add additional AIDs, and disabling an AID is not recommended. Disabling an existing AID could leave the merchant liable for transactions that should otherwise use that AID.

In order to process a card transaction as an EMV transaction, there must be an AID match between the system's AIDs and the card's (i.e. the same AID must be present on both). The AIDs available on the system are specified by the Acquiring Hosts and placed in the EMV processing terminal by VIPER. The Acquiring Host can only accept the AIDs they have communicated to the system.

Ensure that when EMV is being enabled, AIDs are listed in the system and are enabled.

AID	AID Name	Enable	Bypass PIN	Account Type	Allow Standin for AAC	Standin TWR Mask	Standin TSI Mask	Standin Country Code check	Standin Floor Limit
A00000002501	Amex: Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000001523010	Discover	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000041010	MC Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000043060	Maestro	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000042203	DEBIT MASTERCARD	<input checked="" type="checkbox"/>	BYPASS	DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000031010	Visa CR/DB	<input checked="" type="checkbox"/>	BYPASS	CREDIT & DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000032010	Visa Electron	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000033010	INTERLINK	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A00000000980840	US DEBIT	<input checked="" type="checkbox"/>	BYPASS	CREDIT & DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000

The AID Configuration panel consists of the following:

1. The **AID** alpha-numeric string is supplied by the acquiring host and may be a full or partial AID. Merchant level configuration is not available for this field.
2. The **AID Name** is associated with a card type supporting EMV processing and is provided by the acquiring host. The AID Name displays on the PIN pad if an AID selection menu is presented. Merchant configuration is not available for this field.
3. The **AID <Enable>** checkbox allows selecting to enable the AID. The AID may be disabled if the merchant should desire. Verifone discourages disabling an AID as this could lead to Merchant liability for transactions that should have been processed through EMV using the AID.
4. **<Bypass PIN>** Entry is an optional EMV function that if enabled may be invoked when the following occurs:
 - The Card Verification Method (CVM) list of the selected AID has PIN as the preferred CVM for the given transaction and the terminal has a Terminal Capability indicator supporting "PIN".
 - The terminal prompts the cardholder for a PIN.
 - The cardholder opts to not enter the PIN and invokes this function

For these transactions, the approving host is notified with a transaction indicator that the PIN was manually bypassed on a PIN-preferring card.

5. **<Account Type>** configuration allows selection for the transaction type associated with the AID: Credit Only, Debit Only, Credit & Debit. This configuration option can lead to additional Credit/Debit prompting in the transaction flow. In most cases this value will come from the VIPER table owner.

AID Stand-In Configuration



Verifone recommends the Stand-In TVR Mask field remain unchanged unless the person editing the configuration is an EMV Expert, and fully understands the ramifications of updates to this field.

As with traditional MSR processing, EMV based transactions may allow stand-in processing to approve transactions even if the online payment host is offline and not available.

EMV data in a transaction allows the system to consider many conditions when making a decision to stand in for a transaction. The system still uses the traditional Magnetic

Swipe Read (MSR) data points, but additional EMV data allow for much finer decision points for consideration.

AID	AID Name	Enable	Bypass PIN	Account Type	Allow Standin for AAC	StandIn TVR Mask	StandIn TSI Mask	StandIn Country Code check	StandIn Floor Limit
A00000002501	Amex Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000001523010	Discover	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000041010	MC Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000043060	Maestro	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000042203	DEBIT MASTERCARD	<input checked="" type="checkbox"/>	BYPASS	DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000031010	Visa CR/DB	<input checked="" type="checkbox"/>	BYPASS	CREDIT & DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000032010	Visa Electron	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000033010	INTERLINK	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000
A0000000980840	US DEBIT	<input checked="" type="checkbox"/>	BYPASS	CREDIT & DEBIT	<input checked="" type="checkbox"/>	FD7FFB270F	E800	<input checked="" type="checkbox"/>	0000

The AID Configuration panel provides the following:

1. The **<Allow Stand-In for AAC>** setting tells the system whether to allow offline processing for the AID. If this box is left unchecked, stand-in processing is disabled for the card types associated with the AID.

When Stand-In Processing is turned off for an AID, no offline authorizations will be allowed for any transaction, regardless of what other criteria are present.

2. The **<Stand-In TVR Mask>** field allows editing mask definitions that will be logically *ANDed* with the Terminal Verification Results. If this logic results in a non-zero result, the system will not stand-in for the transaction.

In the example image shown below, the Stand-In TVR Mask value is 80008000. If Offline Data Authentication is not performed, or Cardholder Verification is not performed, the transaction will be declined.

AID	AID Name	Enable	Bypass PIN	Account Type	Allow Standin for AAC	StandIn TVR Mask	StandIn TSI Mask	StandIn Country Code check	StandIn Floor Limit
A00000002501	Amex Credit	<input checked="" type="checkbox"/>	BYPASS	UNKNOWN	<input checked="" type="checkbox"/>	80008000		<input type="checkbox"/>	0000

See EMV 4.3 Specification Book 3, at www.emvco.com/specifications.aspx?id=223 for details of the five-byte binary bitmap TVR.

3. The **<Stand-In TSI Mask>** field operates like the TVR mask but is logically *ANDed* with the Transaction Status Information.
4. The **<Stand-In Country Code Check>** controls the acceptance of foreign cards. When enabled, the terminal's country code is compared with the card's AID country code. If the codes match, the transaction will be approved in stand-in

mode; if not, the transaction will be declined. This allows a merchant to decline foreign cards in stand-in.

5. The **<Stand-In Floor Limit>** allows setting a dollar amount, such that no transactions over the set Floor Limit will be approved. If the Floor Limit is set to zero (0), that essentially turns off any stand-in option for that AID.

This value is separate from the floor limit present on the card.

CAPK Configuration



The CAPK configuration area is read-only. There is no action required at the site level to create or maintain these keys.

CAPKs are specific to each card brand and are used by the EMV cryptographic functions during EMV processing. Keys are set to expire, however each FEP has a mechanism to ensure keys are kept current.

Ensure that when EMV is being enabled, CAPKs are listed in the CAPK Configuration Table.



Please contact the Helpdesk or your VASC if no CAPKs are listed. CAPK errors will compromise system functionality.

CAPK ID	RUD	CAPK Index	Expiry Date
AmericanExpress1152a	A000000025	C1	
AmericanExpress1152b	A000000025	C8	
AmericanExpress1400a	A000000025	C2	
AmericanExpress1400b	A000000025	C9	
AmericanExpress1984a	A000000025	C3	
AmericanExpress1984b	A000000025	CA	
Discover1152	A000000152	5B	
Discover1408	A000000152	5C	
Discover1984	A000000152	5D	
JCB1152	A000000065	11	

AID Rules



Implementing AID Rules should be considered advanced configuration and only undertaken by individuals with a complete understanding of AID selection.

Verifone is not responsible for AID Rule configurations. Contact the Front-End Processor and Merchant Service Provider to assist with determining AID order for rules.

The EMV Application ID selection occurs immediately after the Consumer inserts their card. When the card is inserted, the terminal must determine what AIDs are mutually supported between the card chip and the terminal, then select an AID to process the transaction.

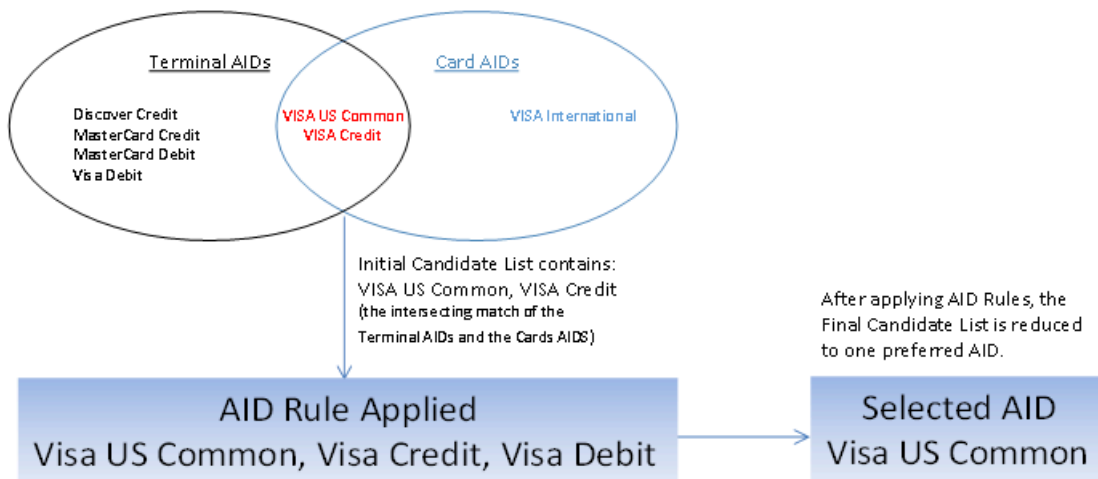
For Debit Cards, or when there is more than one AID that is mutually supported between the chip card and the terminal, a choice must be made regarding which AID to select to process the transaction.

AID Rules allow setting preferences for a selected AID over others by configuring a *Rules List*.

The AID Rules section allows creating the *Rules List* to define a set of preferred AIDs for use during the AID selection phase.

The functionality is specifically designed to support the U.S. Common Debit AID, allowing the Common AID to be selected by default when multiple AIDs are present.

Multiple AIDs can be included when creating an AID Rule. When viewing a Rule Exclusion List, selection preference is given to the included AIDs from left to right.



AID Selection Menu



Verifone systems are designed so that the user should never see this menu. If this menu does appear, it is possible the system is not working correctly. If this menu appears, the EMV settings, particularly the AID Rules, should be confirmed with Verifone or the network processor.

AID Menu Selections are derived from the AID name and may be confusing to the Consumer. Use of AID rules reduces or eliminates prompt occurrence.

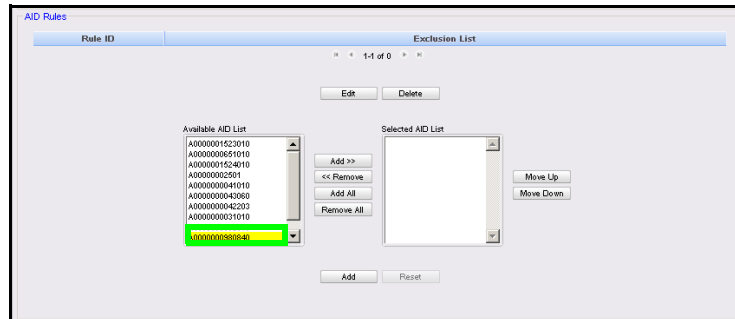
In most instances, the system uses only the selected AID, but it is possible that there could be more than one AID match. If multiple AIDs are available, and AID Rules have not been established, the system will generate a prompt for the Consumer to select the AID to use.

Once the AID is selected, the system will generate prompts to guide the Consumer through the steps in the chip-based transaction.

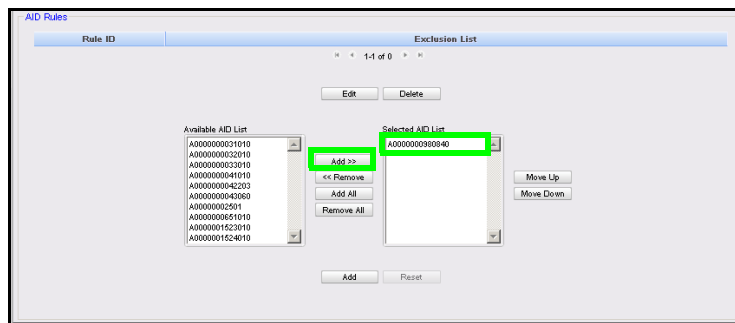


Creating AID Rules

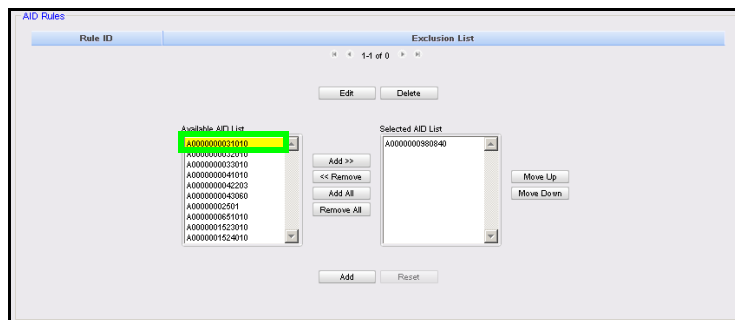
1. Click to select and highlight the first AID to be included in the rule from the Available AID List. AID 980840 is the Visa U.S. Common Debit AID.



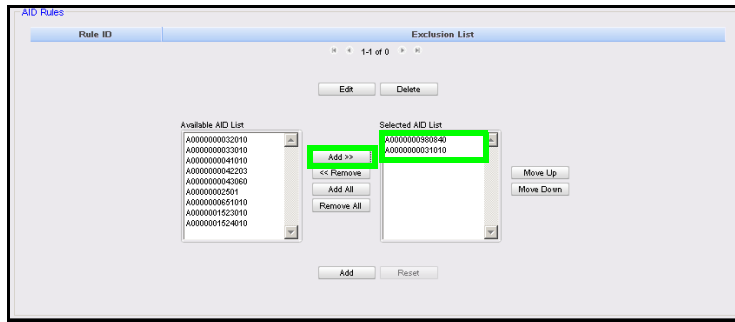
2. Click **[Add>>]** to move the AID to the Selected AID List.



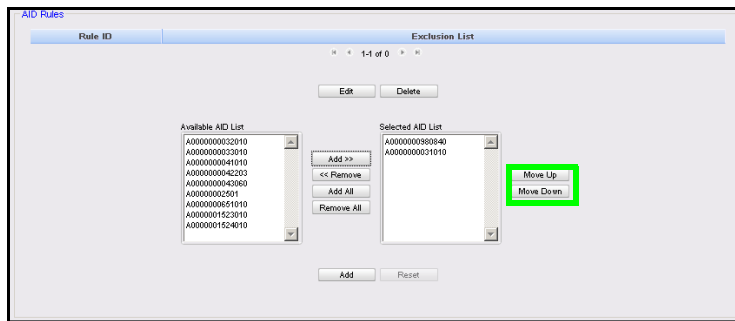
3. Click to select and highlight the next AID to be included in the rule from the Available AID List. AID 31010 is the Visa Global Debit/Credit AID.



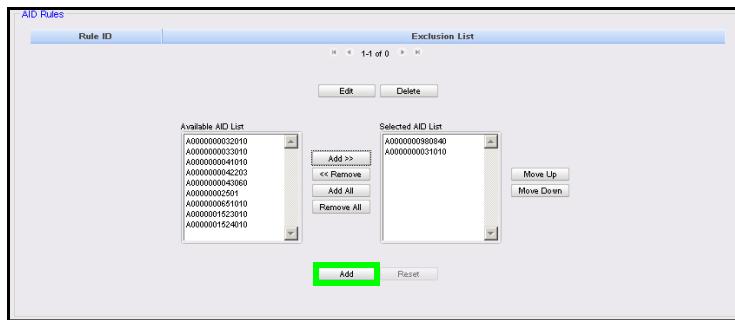
- Click **[Add>>]** to move the AID to the Selected AID List.



- Continue adding AIDs from the Available AID List to the Selected AID List as necessary. Click **[Move Up]** and **[Move Down]** to re-order the AIDs as needed, with the AIDs in descending order of preference.



- Click **[Add]**.



The new AID Rule is created, assigned a Rule ID number and added to the AID Rules List.



In the example *Rule 001* shown above, if after the terminal and card have determined that mutually present AIDs exist, and both AID 31010 and 980840 are present in the candidate list, the rule will be applied. The order the AIDs appear in the list is the order the AIDs will be prioritized, so *Rule 001* will prioritize the Visa U.S. Common Debit AID over the Visa Global AID, and the system will select the Visa U.S. Common Debit AID with no menu selection required.

Without the defined rule, this example scenario with two mutually matching AIDs, would generate a menu prompt.



After creating AID Rules, log out and log back in to all POS to update the PIN pad to use the new rules.

Using EMV

Performing an EMV Transaction

EMV transactions progress in the following manner:

Card detection and reset: In this phase,

Contact EMV: The Consumer inserts the card into the PIN pad. The terminal reads the data from the card and sends a message specifying how it will deal with the card. The Consumer does not remove the card at this stage.

Contactless EMV: When the Consumer taps or waves the card over the reader sensor, the terminal detects the chip in the card (using NFC), and sends a message specifying how the terminal must interface with the card.



Even though with Contactless EMV, and Visa's Quick Chip standard, the Consumer does not keep their card with the PIN pad (as they do when the card is inserted), the PIN pad may still display prompts for the Consumer to take action, such as selecting Credit or Debit, or requesting a Cashback. See "Types of EMV Transactions" below for more information.

7. AID List Creation: The card and terminal have lists of AIDs that they compare to find a match, which is also determined by any business rules that are in place. (Please see "Application ID Configuration" and "AID Rules" above for more information.)
8. AID Selection: The terminal and card determine which AID they are going to use for the transaction.
9. Authentication and Risk Management: The terminal uses the read chip data to verify that the card is genuine and not modified. and determines actions accordingly.
10. Online Processing: The terminal sends the information to the card issuer, which checks the card status and determines whether to accept or reject the transaction.
11. Transaction completed: After the card has been analyzed and the transaction accepted or rejected, the transaction finishes. For Contact EMV, the Consumer removes the card from the PIN pad at this stage.

Types of EMV Transactions

Normal Sale - EMV Chip Read

When the Cashier begins the transaction, the PIN pad becomes active.



Initial Prompt Instructing Consumer to Insert, Tap, or Swipe the card.

The Cashier may monitor the instructions shown on the PIN pad by referring to the *PIN pad Prompts To Cashier* section of the POS. Verifone recommends enabling these prompts when EMV is initially enabled to aid in the Cashier's understanding of what the Consumer sees on the PIN pad device.

<PIN pad Prompts To Cashier> may be turned on or off using Configuration Client. (In Configuration Client, navigate to **Payment Controller > EPS Configuration > EPS Global Configuration > EPS tab > Misc.**

The prompts show in the status window on the Topaz or Ruby2 POS.



PIN pad Messages are Visible to Cashier

When the Consumer uses a chip card, it must be inserted in the PIN pad EMV card slot.

When the card is inserted, the system will perform AID selection to choose the application from the card that will control the rest of the transaction.

The first instructions advise the Consumer to leave their card in the chip reader.



Instructioning Consumer to Leave Card Inserted

Depending on the Card Type and configuration settings, a Credit/Debit prompt may be presented to the Consumer.



System Prompting for Credit or Debit

When the Consumer confirms the amount, the Cardholder Verification stage of EMV processing begins. There are four CVMs processing can take, depending on the selected AID and terminal configuration.

The four possible options include:

1. Offline PIN: Card validates the PIN
2. Online PIN: PIN is validated at the issuing bank
3. Signature: Cashier validates the cardholder signature
4. NO CVM: no CVM is performed

The Consumer should follow prompts during the Cardholder Verification stage.

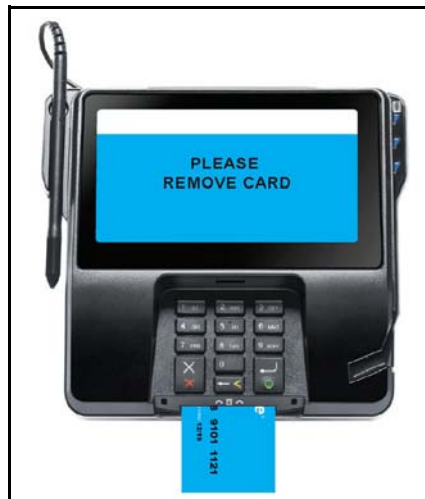
Prompting at this stage comes directly from the AID, so during this phase the Cashier will not be able to follow what is displayed on the PIN pad. When the CVM phase is complete the transaction will continue processing.

Following the Credit/Debit Selection, the system will prompt for a confirmed amount. If the Consumer has requested cash back, the amount will include the Cashback. The Consumer then OKs the amount and the next EMV stage begins.



Consumer Prompt to Confirm Amount

When the transaction completes, if the Consumer has inserted their card into the POS, the system will instruct the Consumer to remove the card from the slot. The terminal also provides an audible reminder to remove the card.



Prompt to Remove EMV Card

The final receipt will not print and the transaction will not clear from the POS register until the card is removed. Once the card is removed the receipt prints and the register

will clear the sale. The Cashier should provide guidance to the Consumer at this phase if the transaction does not clear from the register after network approval.

Other EMV Transactions

Other transactions are run with EMV cards in very similar fashion. Refunds and Prepay transactions are run just as they are in a magnetic stripe environment with the exception of leaving the card in the slot during the transaction.

Normal Inside EMV Flow

1. Consumer brings goods or service requests to the Cashier.
2. The Cashier rings up the goods and services. This can include both prepay and post-pay fuel sales and non-fuel items.
3. **Contact EMV:** The Consumer inserts the EMV card into the PIN pad's EMV card reader. The card remains in the chip reader for the duration of the transaction while the chip is read and while any customer verification prompting is performed. When the EMV card processing is finished, the consumer will be notified to remove the card. In Verifone's Quick Chip flow, the card does not need to remain in the reader for the duration of the transaction. Card insertion, like the MSD swipe ahead, can be done at any time.

Contactless EMV: After being prompted to tap or wave, the Consumer waves or taps the EMV card against the PIN pad's wave/tap card reader. The card only needs to be in proximity to the sensor long enough for the reader to obtain the required data.

Reading the card chip is the first interaction between the PIN pad and the chip on the card.



4. The Cashier tenders the transaction for network payment the same as would be done for MSD tendering.

5. The "Network tender" triggers a request for payment to VIPER, which in turn communicates with the PIN pad to process the EMV payment request. This step in EMV processing is referred to as the *First Generate AC*.
 - The 1st Gen AC is the second communication, after the read, with the card. The 1st Gen AC performs the CVM processing and results in either an offline approval, a request to go online, or a decline. The results of the CVM processing are also returned.
6. VIPER uses card data from the Contact or Contactless EMV card and transaction information from the POS to obtain payment authorization from the payment host.
7. If the transaction is approved, the Approval is indicated to the Consumer and the Cashier.
8. **Contact EMV only:** Note that the receipt will not print and the transaction will not clear from the POS until the Consumer removes their card. The Cashier should prompt the Consumer to remove the card if they do not do so in a timely manner following the transaction approval.
9. The receipt prints and the transaction is cleared from the POS.

Exception Flow

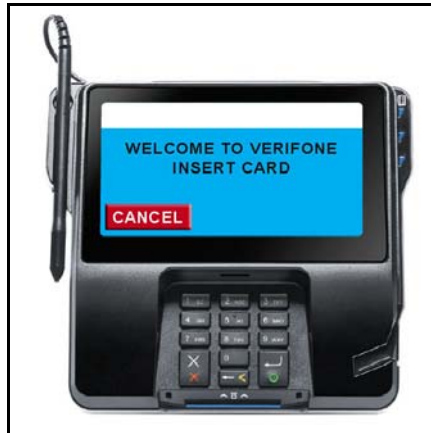
Attempting to Swipe a Chip Card

If an EMV enabled card is swiped instead of inserted into the card reader, the proper response as defined by EMVCo is to prompt the Consumer to insert the card.

For Verifone systems, the expected behavior when attempting to swipe an EMV card is to prompt the Consumer to insert the card.

Verifone systems manage this based on specific Card Table configurations. The Card Table is not site configurable but is either downloaded, distributed, or built from a PDL.

If the system does not behave in the expected manner, the site should confirm with the FEP table owner that the Card Table is configured properly.



Failed Chip Read

When an EMV card read fails, the system will indicate the failure with a prompt on the PIN pad for the Consumer.

Depending on the table configuration, the system may allow a magnetic swipe after a contact EMV chip-read failure, or card insertion after a contactless EMV chip-read failure. This process is called a *Technical Fallback*.

This behavior is defined by the VIPER tables. If the system is not behaving as desired, the merchant will need to contact and work with the table owner.

Technical Fallback Processing

Technical Fallback is the exception process whereby in contact EMV, the magnetic stripe, rather than the chip data, is read by an EMV-capable device.



A Contactless EMV Read error does not result in a technical fallback, i.e. the consumer cannot immediately swipe the card. Instead a "Switch Interface" message is generated. If the resulting Contact EMV chip read then fails, a Technical Fallback can occur following the chip read error.

Contact EMV: Two common scenarios exist for this process:

1. Consumer Attempts to Swipe Card First
 - a. Consumer swipes the EMV card instead of inserting the card into the EMV card slot.
 - b. The system detects a swiped EMV card and instructs the Consumer to insert the card.
 - c. Consumer inserts the card and the read fails.
 - d. System then uses the swiped data to process the transaction. The MSR data is now approved since a chip-read has been attempted.
2. Consumer Attempts to Insert a Card and the Chip-Read Fails
 - a. Consumer can now swipe the card and MSR swipe data is used. Swiping an EMV card always requires a chip-read be attempted first.
 - b. System will use the swiped data to process the transaction.

The ability to perform technical fallback processing is controlled by the VIPER tables. There is no site configuration allowing modification of the Technical Fallback.

If the system is not processing Technical Fallback in a manner acceptable to the merchant, the site manager must coordinate any changes in functionality with the VIPER table owner.

Contact EMV: Manual Entry

If all contact entry modes for EMV cards fail, the system may allow manual entry of the card data. Manual entry is controlled by the VIPER tables.

At this time, there is no way to modify site configuration to enable or disable manual entry for cards. Please contact your card processor to determine if they can modify this setting.

If the system is not processing EMV manual entry in a manner acceptable to the merchant, the site manager must coordinate any changes in functionality with the VIPER table owner.

Stand-In Processing

As with traditional MSR processing, EMV-based transactions may allow stand-in processing, that is approvals for transactions even if the Online payment host is offline and not available.

Verifone systems retain all of the logic traditional MSR transactions used to control offline processing. In addition, EMV transactions provide even more data for merchants to use in order to make informed decisions when allowing offline approvals.

Some of the additional data includes the following:

- Stand-in based on the AID, or allowing stand-in at all for a specific AID.
- Base approvals on certain EMV tags, e.g. don't approve offline transactions where the PIN was bypassed.
- Approvals based on a floor limit by AID. This is in addition to traditional MSR floor limits.

Each of these mechanisms may be configured using the Configuration Client.

Receipts

EMV receipts can vary based on the data required by either the major oil customer or the Acquiring Host specifications. Common fields required on an EMV receipt often include the AID (tag 4F), the TC (tag 9F26), the TSI (tag 9B), and the authorization code (tag 8A). Each of these tags is included on the receipt by the VIPER Receipt table. The receipt table is controlled by the VIPER table owner, so if there are additional fields desired on a site receipt, the site will need to work with the table owner to provide the receipt data.

Approved Transaction Receipts

The Network portion of the receipt is controlled by the VIPER Receipt Table. There is no configuration available locally to change the network portion of the receipt. Only the table owner can update the data contained on the receipt. Any EMV tag data may be included on a receipt, but the table owner must define the receipts in the VIPER Receipt Table.

```
WELCOME TO
OUR STORE
VP13007411001
VeriFone Gold Disk

FL

Description      Qty      Amount
-----
T ITEM F          1          9.99
Subtotal          9.99
Tax                2.50
TOTAL 12.49
CREDIT $ 12.49

VISA $12.49
Acct/Card #: XXXXXXXXXX8473
Auth #:
Resp Code: 1
4F AID:A0000000031010
9F26 TC:C3223FAGD479805E
95 TVR:080008000
9B TSI:E800
RA Auth:00
STAN: 000212169
Invoice #: 12189
SITE ID: VP13007411001
CUSTOMER COPY

ST# AB123 TILL XXX DR# 1 TRAN# 1010066
CSH: 1 03/09/16 07:59:05
```

Tag IDs are shown for example purposes only.

Actual receipts will vary and may contain other Tag IDs.

The STAN identifies the EMV transaction.

The system prompts for the STAN when running the EMV Transaction Report.

Sample Receipt showing EMV Data

Declined Transaction Receipts

Some FEPs require a receipt to print for declined EMV transactions. Verifone systems will generate a declined receipt if required by each FEP. Usually, the receipt contains all of the EMV tags that are available to the system.

If a site experiences higher than expected EMV transaction failures, these *failure* receipts may be useful in working with the Acquiring Host or the Verifone helpdesk to determine the root cause for EMV transaction failures.

Declined receipts are defined in the Receipt Table by the table owner according to the requirements of the FEP. There is no local configuration for declined receipts.

```

WELCOME TO
OUR STORE
8529
VeriFone Gold Disk

FL
Description      Qty      Amount
-----
T ITEM F          1          9.99
Subtotal          9.99
Tax                2.58
TOTAL          12.49
CREDIT $          12.49

SALE Receipt
VISA CREDIT   USD$12.49
Acct/Card #: XXXXXXXXXXXX5993
Entry Method: Chip Read
Stan: 0001127
Invoice #: 17
SITE ID: 8529
TERMINAL ID: 00000001
Declined
Mode: Card
AID: A000000031010
TVR: 0030000000
IAD: 0000003000002
TS1: 0000
ARC: I1

EMV Offline Data
Tag 50: Visa Credit or Debit
Tag 5F2A: 0040
Tag 5F34: 01
Tag 82: 5400
Tag 95: 0030000000
Tag 9A: 150413
Tag 9C: 00
Tag 9F02: 000000001200
Tag 9F03: 000000000000
Tag 9F07: FF00
Tag 9F08: F040000000
Tag 9F0E: 0000000000
Tag 9F0F: F040000000
Tag 9F10: 00010003000000
Tag 9F12: VISA CREDIT
Tag 9F1A: 040
Tag 9F26: 7214685270500418
Tag 9F27: 00
Tag 9F34: 000000
Tag 9F36: 0002
Tag 9F37: 20FC00E2
TAC Default: DC40000000
TAC Online: 0030000000
TAC Online: DC4004F000

MERCHANT COPY
ST# AB123 TILL XXXX DR# 1 TRN# 3030015
CSH:1 04/13/15 07:03:34
  
```

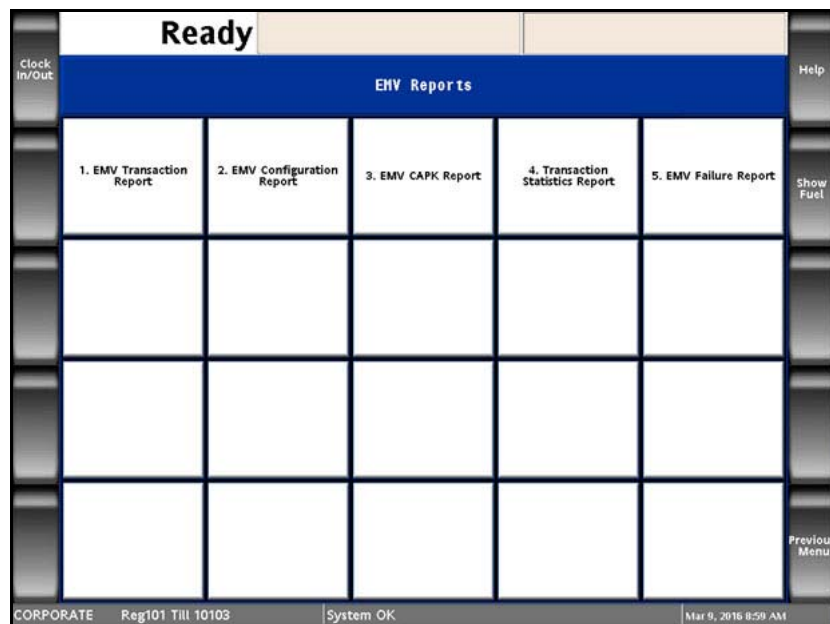
Sample Declined Transaction Receipt

Reporting

Verifone provides the following EMV reports:

- Individual EMV transactions
- EMV configuration
- EMV CAPK
- Transaction Statistics
- EMV Failures

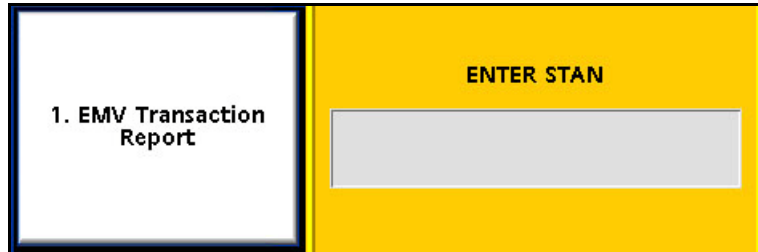
EMV reports are available on the POS from the CSR Functions menu by selecting **Network Menu > EPS Network Reports > EMV Reports**.



Menu of EMV Reports

EMV Transaction Report

The EMV Transaction Report provides all the EMV data (tags) that the system tracked during execution of a particular transaction. When the report is requested, the system prompts for the System Trace Audit Number (STAN), which is available from the receipt.



A sample report is provided. Actual printed reports may vary.

```

EPS NETWORK REPORT
-----
DATE: 10/16/15          TIME: 13:28:28
      Verifone Gold Disk
      Address
      City
      FL
      12345
      Merchant ID

      EMV TRANSACTION REPORT

Transaction #: 3180
Terminal Batch : 1

TAG  FIELD          VALUE
9A   TRANS DATE    2015-10-16
9F21 TRANS TIME      11:37:02.900
4F   AID           A0000000031010
9C   EMV TRANS TYPE 00
82   AIP           3C00
5A   APP PAN       414720****9424
5F2A CURRENCY CODE  0840
84   DEDICATED FNAME A0000000031010
5F34 APP PAN SEQ NUM **
50   APP LABEL     VISA CREDIT

**FIRST AC**
95   TVR          95
9F1A TERM COUNTRY CD 8400
9F26 CRYPTOGRAM     0C0524760F283BFF
9F27 CID            80
9F02 PRIMARY AMOUNT 2.96
9F36 ATC            0260
9F34 CYM            1E0002
96   TSI          EB00
9F10 ISSUER APP DATA 08040A032C8918
9F0F IAC ONLINE      F470C49800
9FDE IAC DENIAL      0000000000
9F00 IAC DEFAULT     F470C49800

**SECOND AC**
95   TVR          95
9F26 CRYPTOGRAM     0C0524760F283BFF
9F27 CID            80

**FINAL RESULT**
98   TSI          7800
8A   AUTH REP CODE 00
-----
    
```

Sample EMV Transaction Report

EMV Configuration Report

The EMV Configuration Report contains general EMV configuration data for each Terminal ID including the following:

- EMV Kernel information
- Last PIN pad Configuration Time
- Terminal Type
- Terminal Capabilities
- Country Code
- Currency Code
- Currency Exponent
- Transaction Category Code
- Merchant Category Code

This data is set for each installation instance (FEP) and is not site configurable. The information is provided as informational only.

```
DATE : 03/08/2016 TIME : 22:37:12
VeriFone Gold Disk
FL
VP13007411001

EMV CONFIGURATION REPORT

TERMINAL ID : 01

*** EMV KERNEL VERSION ***
POP ID EMV KERNEL VERSION
001 L2 7.00001

*** EMV POP LAST UPDATE TIME ***
POP ID DATE TIME
POP001 03/08/2016 17:29:06

*** EMV CONTACT PROPERTIES ***
TERM TYPE : 22
ADDITIONAL TERMINAL : 6000F0F001
CAPABILITY
TERMINAL COUNTRY : 840
TERMINAL CURRENCY : 840
TRANSACTION CURRENCY : 2
EXPONENT
TRANSACTION CATEGORY : R
CODE
MERCHANT CATEGORY : 5541
CODE
```

Sample EMV Configuration Report

The EMV Configuration Report also contains each Application Identifier's specific configuration.

Information provided for each AID includes the following:

- AID Label (will be used if an AID menu is required)
- AID code
- AID floor limit (important for offline processing)
- other configurations unique to each AID.

The report will contain a section for each AID configured in the system.

A sample report is provided. Actual printed reports may vary.

```
AIDLABEL : American Express  
  
APPLICATION ID (AID) : A000000025010  
TERMINAL FLOOR LIMIT : 00000000  
RANDOM SEL THRESHOLD : 00000000  
RANDOM SEL TARGET % : 00  
RANDOM SEL TARGET MAX : 00  
TAC DEFAULT : C800000000  
TAC DENIAL : 0000000000  
TAC ONLINE : C800000000  
DEFAULT DDOL : 9F3704  
DEFAULT TDOL :  
TERMINAL CAPABILITY : E0B8C8  
ALLOW PIN BYPASS : FALSE  
APP VERSION(PRIMARY) : 0001
```

Sample EMV Configuration Report, AID Specification

EMV Certificate Authority Public Key (CAPK) Report

The system provides reporting to confirm CAPKs for each PIN pad and each Registered Application Provider Identifier, and is primarily used in troubleshooting with Verifone Helpdesk personnel.

The report provides visibility to the PIN pads that have received the CAPKs, the RID, the CAPK Index, the key itself, and the CAPK Exponent.

There is no site level configuration that can be done for CAPK data.

A sample report is provided. Actual printed reports may vary.

```
DATE : 03/08/2016 TIME : 22:55:39
VeriFone Gold Disk
FL
VP13007411001

EMV CAPK REPORT

TERMINAL ID : 01

*** EMV POP LAST UPDATE TIME ***
POP ID DATE TIME
POP001 03/08/2016 17:29:06

RID : A000000003

CAPK INDEX : 94
CAPK MODULUS : ACD2B12302EE644F3F83
5ABD1FC7A6F62CCE48FF
EC622AA8EF062BEF6FB8
BA8BC68BBF6AB5870EED
579BC3973E121303D348
41A796D6DCBC41DBF9E5
2C4609795C0CCF7EE86F
A1D5CB041071ED2C51D2
202F63F1156C58A92D38
BC60BDF424E1776E2BC9
648078A03B36FB554375
FC53D57C73F5160EA59F
3AFC5398EC7B67758D65
C9BFF7828B6B82D4BE12
4A416AB7301914311EA4
62C19F771F31B3B57336
000DF732D3B83DE0705
2D730354D297BEC72871
DCCF0E193F171ABA27EE
464C6A97690943D59BDA
BB2A27EB71CEEBDFA11
76046478FD62FEC452D5
CA393296530AA3F41927
ADFE434A2DF2AE3054F8
840657A26E0FC617
CAPK EXPONENT : 03
```

Sample EMV CAPK Report

EMV Transaction Statistics Report

The EMV Transaction Statistics Report shows all EMV transaction data by Terminal Batch Number for each PIN pad, designated by the Terminal ID.

Grand totals for all PIN pads are also included.

The report allows the site to track the following transaction data:

- Total EMV Transactions, shown as ICC (Integrated Card Chip)
- EMV Magstripe Fallback, shown as ICC Fallback Swipe
- Swiped (normal MSR)
- Manual Keyed
- RFID Contactless (non-EMV)

A sample report is provided. Actual printed reports may vary.

```
EPS Network Report
-----
DATE:10/16/15          TIME:16:48:27
VeriFone Gold Disk

FL

VP13007411001

TRANSACTION STATISTICS REPORT

Terminal Batch: 1
Terminal Batch Open : 10/06/15 10:33:45
Terminal Batch Close : OPEN

Terminal ID : 01

*** TERMINAL BATCH STATISTICS ***

TOTAL TRANSACTIONS: 18

ENTRY MODE          TRANS  TRANS%
-----
ICC                 11     61.11
ICC FALLBACK SWIPE  0       0
SWIPE)              7     38.89
KEYED                0       0
RFID CONTACTLESS    0       0

*** ACQUIRER BATCH STATISTICS ***

Acquirer Batch: 1
TOTAL TRANSACTIONS: 18

ENTRY MODE          TRANS  TRANS%
-----
ICC                 11     61.11
ICC FALLBACK SWIPE  0       0
SWIPE)              7     38.89
KEYED                0       0
RFID CONTACTLESS    0       0
-----
```

Sample EMV Transaction Statistics Report

EMV Failure Report

The EMV Failure Report details the EMV transactions that experience the following:

- Chip read failures
- PIN entry errors
- Offline declines
- Transactions processed in technical fallback using the ICC magstripe fallback.

The EMV Failure Report shows the transaction data by Terminal Batch Number for each PIN pad, designated by the Terminal ID.

A sample report is provided. Actual printed reports may vary.

EPS Network Report		
DATE:10/16/15	TIME:17:00:22	
VeriFone Gold Disk		
FL		
VP13007411001		
EMV FAILURE REPORT		
Terminal Batch: 1		
Terminal Batch Open : 10/06/15 10:33:45		
Terminal Batch Close : OPEN		
Terminal ID : 01		
TOTAL EMV/CHIP CARD TRANSACTIONS: 25		
FAILURE TYPE	TRANS	TRANS%


POP ID : 001		
CHIP READ FAILURES	14	56.00
PIN ENTRY ERRORS	0	0.00
EMV OFFLINE DECLINED	1	4.00
TOTAL FAILURES	15	60.00
*** EMV FALLBACK SWIPE TRANSACTIONS ***		
ICC FALLBACK SWIPE	0	0.00

Sample EMV Failure Report

EMV Fallback Report

The EMV Fallback Report shows the total number of EMV transactions, and the number and percentage of transactions processed as Fallback for each PIN pad, designated by the POP ID.

A sample report is provided. Actual printed reports may vary



The image shows a sample printout of an EMV Fallback Report. The report is titled "EPS Network Report" and includes the following information:

- DATE: 07/23/15
- TIME: 10:08:58
- VeriFone Gold Disk
- Address
- CL
- City
- 12345
- Merchant ID
- ICC FALLBACK REPORT
- TOTAL EMV/CHIP CARD TRANSACTIONS: 28
- A table with 3 columns: POP ID, TRANS, and % OF TRANS.

POP ID	TRANS	% OF TRANS
001	4	14
TOTAL	4	14

Sample EMV Fallback Report

Troubleshooting

The following section presents possible problem scenarios and discusses how to troubleshoot possible issues with EMV. It does not cover hardware or PIN pad communication issues that are not directly related to EMV.

Steps of an EMV Transaction

A fundamental starting point in troubleshooting is to understand the major steps included in an EMV transaction. If issues do arise, then the source of the problem can be more quickly identified.

An EMV transaction progresses through the following steps:

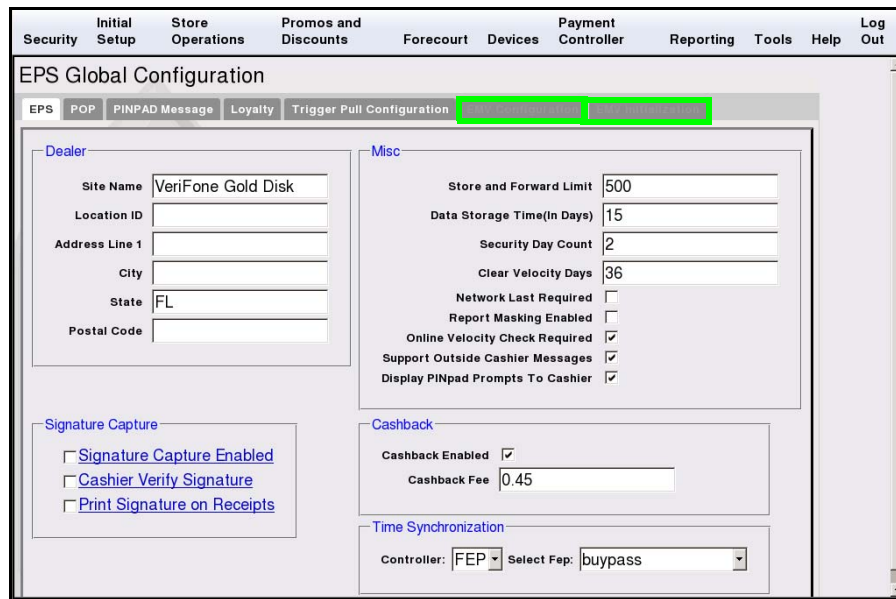
1. Prompt at the PIN pad to Read or Insert Card
2. Insert/Tap/Wave EMV Card and Read the Chip
3. EMV AID selection
4. VIPER BIN Match
5. Perform CVM processing and 1st GEN AC
6. Amount Verification
7. Host Authorization According to EMV Quick Chip Rules
8. EMV Completion
9. Card Removal
10. Receipt Printing

EMV Menu Access Denied

Whenever an existing system is upgraded, and new features requiring configurations are added, administrators *must* update existing user roles to grant access to the new feature. This is not an issue for a new installation, as the default user roles for a fresh install contain the updated configuration settings.

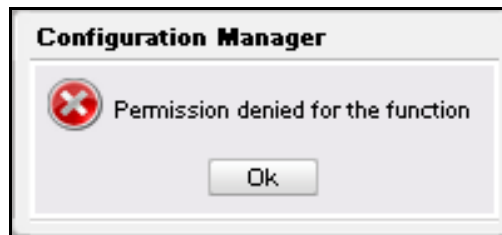
In the event the Controller software was updated through an Auto Upgrade, the EMV menus will be inaccessible.

If accessing the Configuration Client from the POS, and the EMV Configuration and Initialization tabs are grayed out, then this indicates the logged in user account does not have the correct functions added to the associated role.



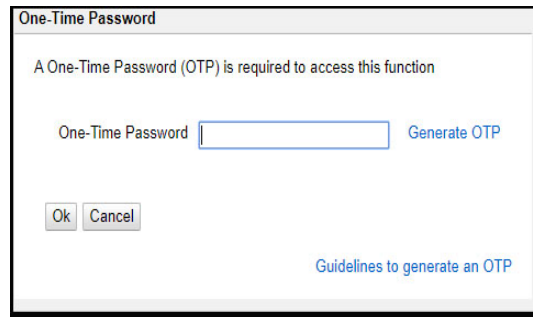
The screenshot displays the 'EPS Global Configuration' window. At the top, there is a navigation menu with tabs: Security, Initial Setup, Store Operations, Promos and Discounts, Forecourt, Devices, Payment Controller, Reporting, Tools, Help, and Log Out. Below this, a sub-menu contains tabs for EPS, POP, PINPAD Message, Loyalty, Trigger Pull Configuration, and two EMV-related tabs that are highlighted with a green box. The main content area is divided into several sections: 'Dealer' (Site Name: VeriFone Gold Disk, Location ID, Address Line 1, City, State: FL, Postal Code), 'Misc' (Store and Forward Limit: 500, Data Storage Time: 15, Security Day Count: 2, Clear Velocity Days: 36, Network Last Required, Report Masking Enabled, Online Velocity Check Required, Support Outside Cashier Messages, Display PINpad Prompts To Cashier), 'Signature Capture' (Signature Capture Enabled, Cashier Verify Signature, Print Signature on Receipts), 'Cashback' (Cashback Enabled, Cashback Fee: 0.45), and 'Time Synchronization' (Controller: FEP, Select Fep: buypass).

If accessing the Configuration Client from a PC, and the logged in user account does not have EMV role permissions, then attempting to access the EMV tabs returns a Permissions Denied message.



You can update user roles through Configuration Client. (For more information on Configuration Client user roles, please see the full Configuration Client documentation.)

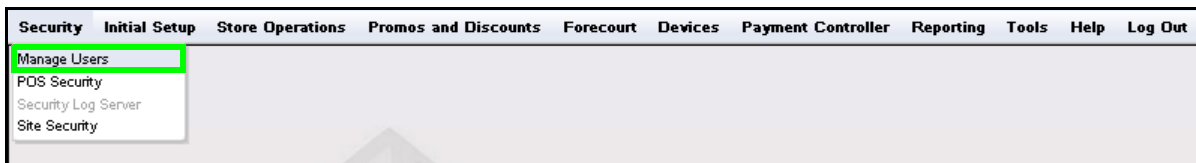
1. Navigate to Security > Manage Users. You will be prompted to enter a One-Time Password. Read it from the status display on the POS, or the Event notification, and enter it in the field provided.



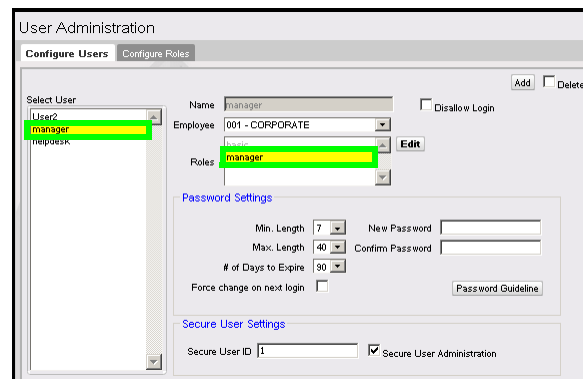
A One-Time Password (OTP) is required to access this function

One-Time Password [Generate OTP](#)

[Guidelines to generate an OTP](#)



2. Click OK.
3. The *Configure Users* tab will be displayed.
4. Click to select the User ID and confirm the assigned role.



User Administration

Configure Users Configure Roles Add Delete

Select User: User2 manager manager

Name: manager Disallow Login

Employee: 001 - CORPORATE Edit

Roles: manager

Password Settings

Min. Length: 7 New Password:

Max. Length: 40 Confirm Password:

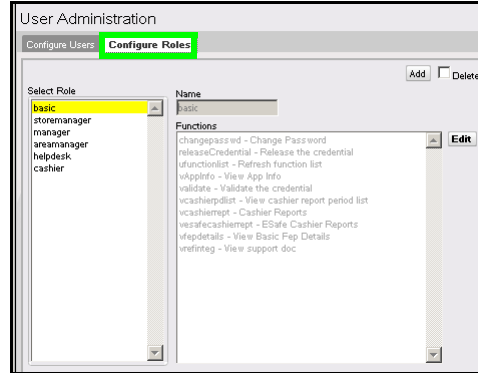
of Days to Expire: 90 Password Guideline

Force change on next login

Secure User Settings

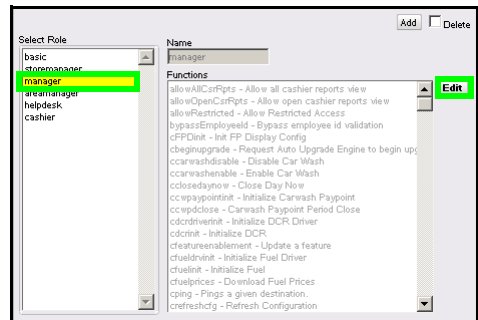
Secure User ID: 1 Secure User Administration

- Click to select the *Configure Roles* tab



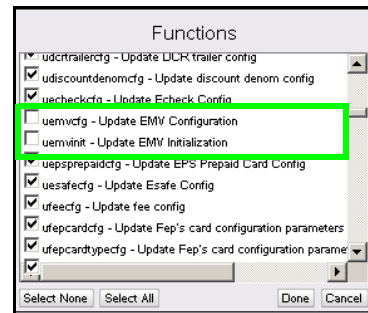
- Click to select the Role to update.

- Click **[Edit]**.

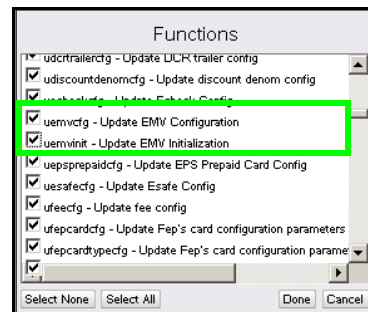


The Functions list is displayed with items listed alphabetically.

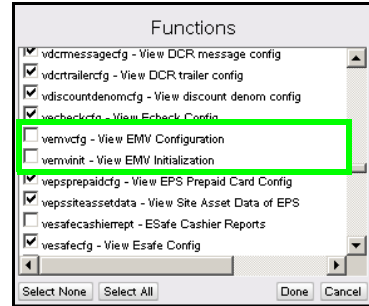
- Scroll down the Functions list and locate *uemvcfg* - Update EMV Configuration and *uemvinit* - Update EMV Initialization.



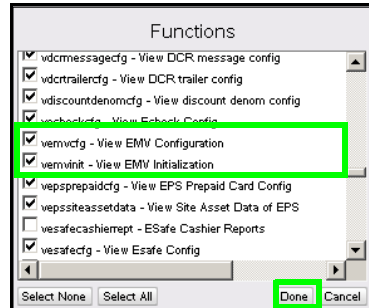
- Click the checkboxes to activate the **uemvcfg** and **uemvinit** functions.



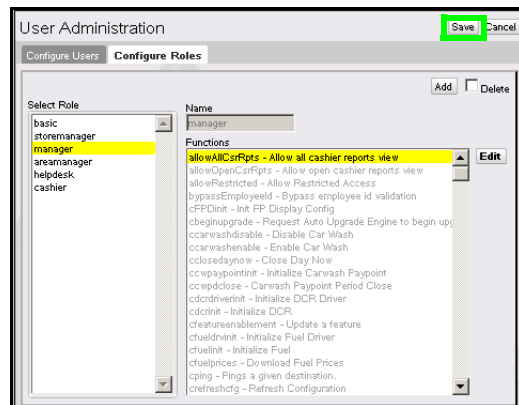
10. Scroll down the Functions list and locate *vemvcfg* - View EMV Configuration and *vemvinit* - View EMV Initialization.



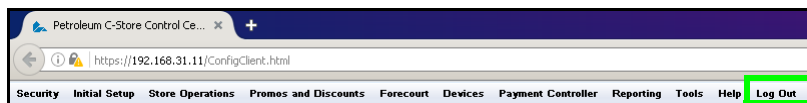
11. Click the checkboxes to activate the **vemvcfg** and **vemvinit** functions.
12. Click **[Done]**



13. Click **[Save]**.



14. Log out of the Configuration Client.



15. Log back into the Configuration Client to apply the permission updates.

Error Saving EMV Configuration Settings

Using an unsupported browser application can cause errors when attempting to save or update configuration settings. If these errors occur, try making changes using Configuration Manager on the POS, or use a supported browser (Firefox or Internet Explorer).

EMV Initialization

The EMV Initialization tab allows forced initialization on selected POP devices, and provides confirmation of any PIN pad updates that have failed.

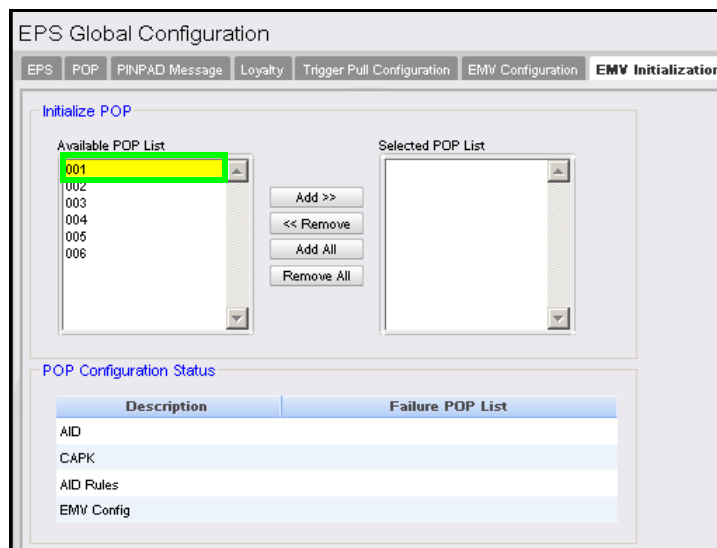
The Initialize POP process is performed automatically for each PIN pad in the system during initial EMV implementation, which is initiated through a PDL or table download.

The POP Configuration Status Panel keeps track of what data has been sent and any error messages that may have occurred.

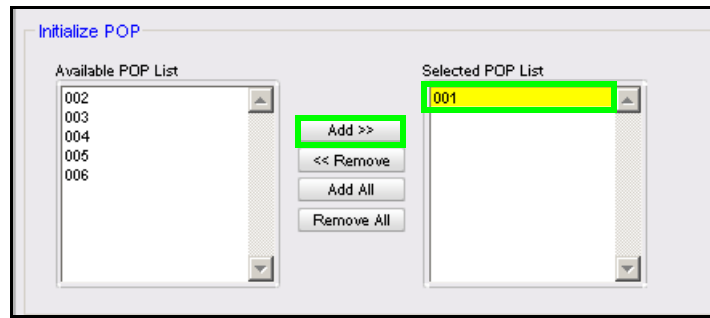
Utilizing the Initialize POP function is only required for new PIN pad terminals that are introduced to a running system, or if errors are detected and shown in the *POP Configuration Status* panel.

Initialize POP

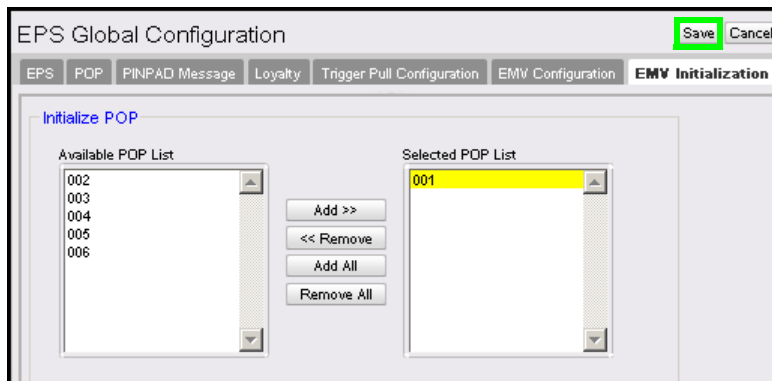
1. Navigate to Payment Controller > EPS Global Configuration > EMV Initialization
2. Click to select and highlight the POP ID(s) to be initialized from the Available POP List.



3. Click **[Add>>]** or **[Add All]** to move the AID(s) to the Selected AID List.



4. Click **[Save]** to initialize the selected POP devices for EMV use.



Do not navigate away from the EMV Initialization tab before saving, unless you wish to cancel the initialization. Once the user navigates away from the EMV Initialization tab, the page is reset.

Without saving, all POP devices will be displayed in the Available POP List again.

Initialization of selected PIN pad(s) occurs with the corresponding SAVE.

POP Configuration Status

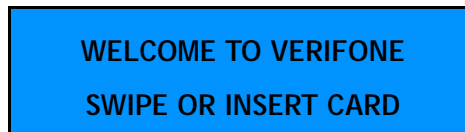
You can use the PIN pad Configuration Status section to monitor the PIN pad configuration status, which allows site operators to confirm that all PIN pads in the system have received the proper configuration for AIDs, AID Rules, CAPKs, and EMV.

Any PIN pad that has not received specific configuration data will be listed in the applicable *Failure POP List* section. A PIN pad that appears in the *Failure POP List* may not operate properly in an EMV environment.

POP Configuration Status	
Description	Failure POP List
AID	Any POP IDs showing here indicates that EMV may not function properly on those listed terminals.
CAPK	
AID Rules	
EMV Config	

No “Insert Card” Prompt for Contact EMV

1. The card prompt should contain text that includes verbiage about inserting a card.



If the displayed prompt does not include instructions to “Insert the Card”, see the section for Enabling EMV, and verify EMV is enabled.

2. Use the EMV Configuration Report or check Configuration Client EMV Initialization tab to verify the EMV configuration has been pushed to the PIN pads.

No Transactions Processing as EMV transactions

1. See the section for Enabling EMV, and verify EMV is enabled.
2. Use the EMV Configuration Report or check the Configuration Client EMV Initialization tab to verify that the EMV configuration has been pushed to the PIN pads.
3. Confirm that AIDs exist in the AID list.
If there are no AIDs, EMV cannot process cards. AIDs cannot be site configured and must be either part of the distribution or downloaded by the table owner. If there are no AIDs present in the system, make sure the system has performed a PDL or Table Download, whichever is appropriate for the FEP.
4. Confirm that CAPKs exist in the CAPK list and are not expired.
If there are no CAPKs, or if CAPKs are expired, EMV cannot process cards correctly. CAPKs cannot be site configured and must be either part of the distribution or downloaded by the table owner. If there are no CAPKs present in the system, make sure the system has performed a PDL or Table Download, whichever is appropriate for the FEP. If there are expired CAPKs present in the system, perform a PDL or Table Download, as appropriate for the FEP.

5. Confirm network connectivity as network communications issues could also cause problems.

Only Some PIN Pads Process EMV

Although not recommended, the system allows split processing between EMV and MSR transactions where some PIN pads are configured to allow EMV, and some are not.

1. Verify the PIN pad terminal is EMV capable and has a chip reader.
2. Use the EMV Configuration Report or check Configuration Client EMV Initialization tab to verify the EMV configuration has been pushed to the PIN pads.

Swiping an EMV Card is Allowed Without First Requiring a Chip-Read

1. See the section for Enabling EMV, and verify EMV is enabled. If EMV is not enabled, card swipes may be allowed.
2. The VIPER Card Table may be explicitly allowing this behavior. Table analysis is possible using the VIPER Diagnostics page to display the Card Table. Verify with the table owner the intended operation.

Swiping Not Allowed After a Failed Chip-Read

The VIPER Card Table may be explicitly preventing this behavior. Table analysis is possible using the VIPER Diagnostics page to display the Card Table. Verify with the table owner the intended operation.

This behavior depends on explicit table entries as documented in the Card Table Specifications available from the table owner.

An Inserted Card is Refused or Declined

1. If an inserted card is refused or declined before the amount confirmation, see Using EMV: Transaction Steps.
 - a. The chip-read itself could have failed.
This can be tested by inserting a card with the "chip side out". This guarantees a chip-read error. If the response is the same, the issue may be a chip-read failure. Attempt a chip-read with the card on another PIN pad to isolate and determine if the PIN pad or the card is bad.
 - b. The issue may be that no matching AIDs were found between the card and the terminal.
Is this a foreign card?

- c. The Card table may not contain an entry for this card. Confirm with the Table Owner that they accept the card.
2. If an inserted card is refused or declined after the amount confirmation,
 - a. The Host authentication could have failed. Check for a response code indication.
 - b. The Host is unavailable and no stand-in was done. Verify AID Stand-In configuration logic.
 - c. The card may have been removed prior to completing the transaction. EMV processing will decline a transaction, even after host approval, if the terminal and the card cannot communicate after host approval. This is the Complete EMV 2nd Gen AC in the transaction steps. Confirm that the card remains firmly in the reader slot until instructed to remove it.
 - d. Confirm there are no expired CAPKs present in the system. If there are expired CAPKs present in the system, perform a PDL or Table Download, as appropriate for the FEP.
 - e. There is a possibility that the chip has failed.

Receipt is Slow to Print

A receipt will not print, and the transaction will not clear from the POS, until the EMV card is removed from the PIN pad.

Ensure the Consumer removes the card when prompted to do so.

Intermittent Chip Card Read Failure

The PIN pad sometimes fails to read the chip on the card.

The chip card reader may need to be cleaned. Verifone recommends that you purchase a Verifone chip card reader cleaning kit (part number 02746-02).

Cleaning Process

3. **Inspect** – First, visually inspect the terminal's Smart Card Reader before attempting to clean the unit. All debris, "foreign objects," and other material must be removed from the Smart Card Reader before using the cleaning cards.



If at any time during the inspection, testing diagnostics or cleaning process, "foreign objects" are found in the Smart Card Reader, stop the cleaning process and send the terminal to a Verifone authorized repair center. Customers' removal of foreign objects from Smart Card Readers may void terminal warranty.

4. **Pre-Test** — If no debris is found in the Smart Card Reader, run the internal Smart Card test using the following steps.
 - a. If an application is already loaded and running, put the terminal into System Mode by pressing keys 1, 5, 9 at the same time. If there is no application loaded, the terminal will boot up to the System Mode Login Screen.
 - b. Navigate to Diagnostics > Card > Smart Card. Insert a card before selecting the tab.
 - c. If the terminal passes the diagnostic test, proceed to the next step.
 - d. If the terminal fails the diagnostic test, make a note of the failure and proceed to the next step.
5. **Cleaning** — Use the Smart Card Reader Cleaning Kit (Verifone PN 02746-02).



New cleaning cards must be used per terminal each time during the cleaning process. Used or old cleaning cards must not be reused. Reuse of old cleaning cards may result in more debris becoming trapped inside the reader.

6. **Test After Cleaning** — Retest the Smart Card reader in Diagnostic mode using the instructions in step 2.
 - a. If the terminal fails the Smart Card Reader Test, send the terminal in for repair.
 - b. If the terminal passes the Smart Card Reader Test, reboot the terminal's application for regular use.

System Diagnostics

System Diagnostics provide useful information that may be helpful in troubleshooting.

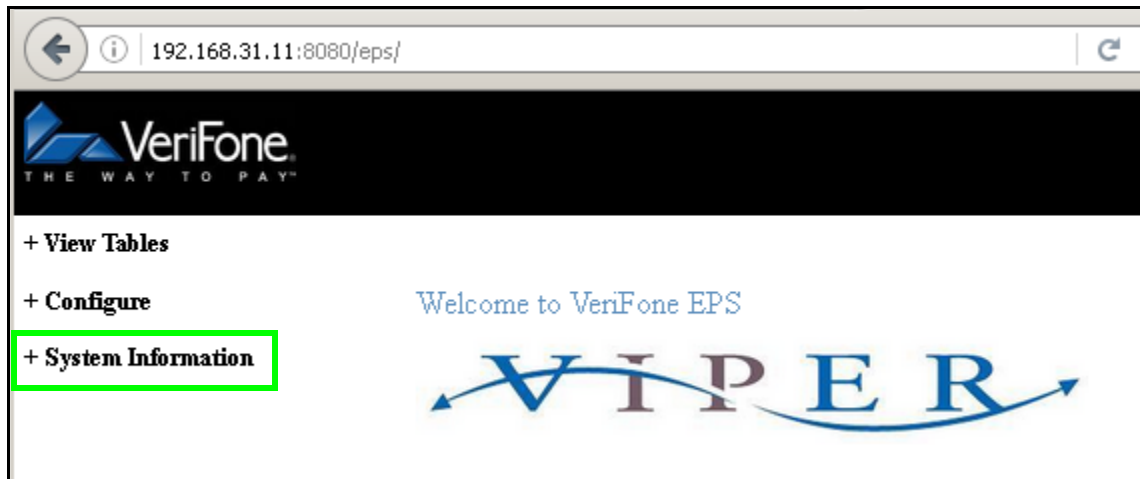
Accessing System Diagnostic Information

For Commander Site Controller and RubyCi systems, in a browser window, open the following address: <http://192.168.31.11:8080/eps/>.

For Sapphire systems, in a browser window, open the following address: <http://192.168.31.13:8080/eps/>.

Viewing System Diagnostic Information

1. Click [+ System Information] to expand the menu item list.



2. Click [Diagnostics] to display the system diagnostic details.



3. Scroll down the list to view the POP and POS diagnostic information and details.

POP Status for POP ID

POP Status									
POP ID	IP Address	Status	POP Model	Software Version	OS Version	Kernel Version	RFID Version	Touchscreen	Ping
001	192.168.31.126	Online	Mx870	ViperPay 4.00.02	release-30140200	2.6.31.14-vf 1.2.7.1404	140200	Present	<input type="button" value="Ping 001"/>

The POP Status panel shows the following:

- POP ID - PIN pad identifier.
- Status - Online/Offline.
- POP Model - EMV functions require PIN pad hardware with an EMV Chip Reader.
- Software Version - MX devices require ViperPAY 4.xx.xx.
- Kernel Version - MX 900 Series devices require Kernel 7.00+.
MX 800 Series devices require Kernel 4.00+.

POS Status for Workstation ID

POS Status							
Workstation ID	Status	POP ID	POS Name	Software Version	Clerk ID	Clerk Level	Loyalty
POS101	Logged In	101	DCR	Base 042.00.00	0	0	Enabled
POS001	Logged In	001	Topaz	Base 042.00.00	1	9	Enabled
POS000	Logged In	000	coresvcs	Base 042.00.00	0	5	Enabled

The POS Status panel shows the following:

- Workstation ID- POS Terminal Identifier.
- Status- Logged In/ Logged Off.
- POP ID- ID of associated PIN pad.
- POS Name- Device name.
- Software Version- Commander Site Controllers require Base 042.00.00 or higher.

2 GLOSSARY OF TERMS

The following terms and definitions will assist with understanding the contents of the Feature Reference.

Term	Definition
AAC	Application Authentication Cryptogram. Generated whenever a card declines a transaction. This may be generated at the 1st or 2nd GenAC step.
AID	Application Identifier, specified by the acquiring host and used to identify the EMV applications that a system can support. Cards and terminals use AIDs to determine which applications are mutually supported, as both the card and the terminal must support the same AID to initiate a transaction. Both cards and terminals may support multiple AIDs.
ARC	Authorization Response Code indicates the transaction disposition of the transaction received from the issuer for online authorisations.
ARQC	Authorization Request Cryptogram. Generated by the card when it instructs the system to go online for an approval. An ARQC is generated at the 1st Gen AC step.
CAPK	Certificate Authority Public Key. The list of keys created by the card issuers used to support EMV cryptographic functions. Each card brand has CAPKs. These keys are loaded into the PIN Pad's during system startup and kept up to date by the system based on data exchanges from the acquiring host.
Contact EMV	An EMV transaction where the EMV card data is read by inserting a chipped card into the card reader slot on the PINpad. The card remains inserted in the PINpad for the duration of the transaction. The PINpad and the card communicate several times during the course of a transaction.
Contactless EMV	See NFC, Near Field Communications.

Term	Definition
CVM	Cardholder Verification Method. The method that the card instructs the terminal to use in order to validate the cardholder. Consists of online PIN, offline PIN, Signature, and No CVM.
EMV	<p>Europay, MasterCard, and Visa.</p> <p>The implementation-oriented global specifications regarding the use of chip card technology for the payments industry; established to ensure interoperability and acceptance of payment system Integrated Circuit Cards on a worldwide basis; the acronym refers to the three organizations that initially collaborated on the specification, now maintained by EMVCo.</p> <p>EMV is now analogous with payment cards with embedded security microchips.</p> <p>Within this document EMV is assumed to mean "Inside Contact EMV" .</p>
EMV Kernel	A layer of software, specific to the hardware it is running on that handles the actual communication with the EMV chip on the card. It is versioned, it has an expiration date, and is certified by EMVCo.
EMV Tag	An EMV identifier. EMV data is maintained in tags - for example 8A and 9F12 are tags representing Authorization Response Code and Application Preferred Name respectively.
EPS	Electronic Payment Server
Fallback	Fallback in EMV terms means allowing a magnetic stripe swipe if the chip read fails. See Technical Fallback.
FEP	Front-End Processor
First Generate AC or 1st Gen AC	At a high level this is the stage in an EMV transaction where an approval is first requested from the card. Responses can be a TC (approved by the card), ARQC (request to go online for approval) or an AAC (decline).
Global AID	An AID that is owned by the global/international payment network whose logo is on the card. Global Payment Networks include American Express, Discover, MasterCard and Visa.
IAD	The Issuer Application Data (IAD) contains proprietary application data for transmission to the issuer in an online transaction.
ICC	Integrated Chip Card, or Integrated Circuit Card.

Term	Definition
Magnetic Stripe Fallback	See Technical Fallback.
MSA	Merchant Services Account.
MSD	Magnetic Stripe Data - The term is used to describe the legacy card entry method requiring a swipe of the card to read the magnetic stripe.
MSP	A merchant services provider (MSP) is an umbrella term that covers banks, third-party processors or any other entity that provides businesses and individuals with the products and services necessary to accept credit cards, debit cards and other forms of electronic payment.
MSR	Magnetic Swipe Read.
NFC	Near Field Communications is used to describe an EMV transaction where the EMV card data is read by tapping or waving the card above the PINpad within the zone, allowing the card and the PINpad to interact. The card is then removed from the zone and the transaction proceeds with no further Card to PINpad interaction.
PDL	Parameter Download. Some acquiring hosts supply configuration and other processing data via a PDL.
PIN	Personal Identification Number.
POP	Point of Purchase hardware, referring to MX 900 Series PINpads used to read EMV cards.
POS System	Includes the POS (Point of Sale) terminal(s), site controller and the electronic payment system (EPS).
Quick Chip	Quick Chip is a specification enhancement for EMV from Visa that enables chip reads in two seconds or less.
Rapid Connect	Rapid Connect is a payment interface that provides single point integration to all First Data payment platforms including Buypass.
RCI	Remote Configuration Interface.
RID	Registered Application Provider Identifier. The RID is a fixed length unique identifier allocated to each card scheme to identify EMV applications provided by that scheme. The schemes may then suffix this with an optional PIX to further differentiate between multiple products supported by the scheme, and together they form the AID.

Term	Definition
STAN	The System Trace Audit Number which identifies the transaction number processed through the merchant account.
Stand-in	A process whereby a transaction may be approved locally according to specific transaction criteria even if the system cannot approve a transaction online.
Table Owner	The entity responsible for maintaining the VIPER tables. Depending on the FEP and the brand, this may be the major oil brand, the processor, Verifone, or a combination of Verifone and brand/processor.
TC	Transaction Certificate. Generated at the 2nd Gen AC step for approved transactions.
Technical Fallback	This is the exception process whereby an EMV-capable device either reads the chip from an inserted card, or reads the magnetic stripe rather than the chip data. (This latter method is deprecated.)
Terminal ID	The PINpad terminal identifier.
TPP ID	Third Party Processor ID. This is an ID that uniquely identifies a particular version of a payment application and which also functions as the Project ID during the certification process. It is assigned when the project is created and follows the application through to the production environment.
TSI	Transaction Status Information.
TVR	Terminal Verification Results.
UMF	Universal Message Format. This is the XML-based message format specification for the Rapid Connect application.
U.S. Common Debit AID	An AID that is owned by a global card brand, but can be licensed by a debit network. Discover, MasterCard, and Visa all provide a U.S. Common Debit AID.
VAP	Value Added Platform.
VIPER	Verifone's EPS payment processing application.

3

SUPPLEMENTAL INFORMATION

Verifone-Certified AIDs

The following is a list of EMV Application Identifiers that Verifone certifies. Names may vary in downloaded EMV tables and on cards, as the processor and issuer can choose their preferred naming conventions to associate with the AID.

Contact

AID	AID Name	Vendor
A00000002501	Amex Credit	American Express
A0000001523010	Discover	Discover
A0000001524010	Discover Common	Discover
A0000000041010	MC Credit	Mastercard
A0000000043060	Maestro	Mastercard
A0000000042203	Debit Mastercard	Mastercard
A0000000031010	Visa CR/DB	Visa
A0000000032010	Visa Electron	Visa
A0000000033010	INTERLINK	Visa
A0000000980840	US DEBIT	U.S. Common Debit AID
A0000000049999C00016	Voyager	U.S. Bank (fleet card)
A0000007681010	WEX	WEX
A0000000033010	INTERLINK	Interlink

Contactless

AID	AID Name	Vendor
A0000000033010	INTERLINK	Interlink
A0000000032010	Visa Electron	Visa
A0000000031010	Visa CR/DB	Visa
A0000000980840	US Debit	U.S. Common Debit AID
A0000000041010	MC Credit	Mastercard
A0000000043060	Maestro	Mastercard
A0000000042203	Debit Mastercard	Mastercard
A00000002501	Amex Credit	
A0000001524010	Discover Common	
A0000001523010	Discover D-PA	

EMV Transaction Tags

For a list of EMV Transaction Tags, Verifone recommends referring to EMV Book 3, which can be found here:

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_3_Application_Specification_20120607062110791.pdf

You can also find a complete list of EMV Transaction tags at:

<https://www.eftlab.com/knowledge-base/145-emv-nfc-tags/>