Vault Operation and Installation Guide

Version 1.8

Revision History

Version	Date	Author	Changes
1.0	14th Aug 2012	Roger Kay	Initial version built from various existing documents.
1.1	20th Aug 2012	Roger Kay	Review changes: - Added download instructions. - Added acquirer settings. - Removed manager password - Fixed typos.
1.2	22nd Aug 2012	Roger Kay	Review changes: - Fixed typos. - Removed one section on getting the IP Address.
1.3	28th Aug 2012	Roger Kay	- Removed 6.2.4 - Updated 2.8.1
1.4	6th May 2013	Tobias Shand	Updated For 7019
1.5	27th June 2013	Andrew Gibbs	Updated for Java and the additional screen size option. Added additional configuration screen detail.
1.6	13th Aug 2014	Andrew Gibbs	Updated VeriCentre IP Address and added new EVO terminals
1.7	11th Feb 2015	Andrew Gibbs	Updated for 7019V9
1.8	4th Aug 2015	Monwa Mdwara	Added Vault-OCX and updated for 2015 software

Vault Versions Covered in this Document

Version	Hardware	Comments
PKMSNZ 7016	Vx810 / Vx510	
PKMSNZ 7018	Vx810 / Vx510	
PKMSNZ 7019 / PKMS 2015	VX820 / VX820 Duet / VX520IPP / VX680 Wi-Fi	

Contents

1 General Information

1.1 Purpose

This document explains how Vault solutions are deployed and managed.

1.2 Scope

The scope of this document is limited to payment solutions that use Vault.

1.3 Audience

This document should be read by people involved in the deployment, management, and support of Vault.

1.4 References

The following documents and/or sources are referenced by this document.

Title	Date / Version	Author / Publisher
VeriCentre Load Form	Rev 29	Verifone NZ
Evolution Downloads	Rev 1	Verifone NZ
POS Interface Configuration Guide	Rev 1	Verifone NZ

1.5 Glossary

The following specialised terms, acronyms, and abbreviations are used in this document.

Term	Definition
POS Application	The application that controls the sale process at the Point Of Sale (a checkout or store lane).
Vault Terminal	A VeriFone terminal or PIN Pad that has been configured to be integrated with a POS Application.
Operator	The person who operates the POS Application and supervises the sale process. Also known as the attendant.
Customer	A person who purchases goods or services with a card of some description.

2 About Vault

This section contains some general information about Vault.

2.1 What is Vault?

Vault is a product that enables VeriFone EFTPOS terminals to form part of an integrated EFTPOS solution. Vault consists of an application that runs on a VeriFone terminal and a library that is linked into the POS Application.

It consists of:

1. A Payment Application that runs on the EFTPOS terminal;

2. A Vault Adaptor which is linked to the POS Application by the POS application developer.

3. An interface applet that runs on the EFTPOS terminal. This applet coordinates communication between the Vault Adaptor and the Payment Application.

The main features of Vault include:

- Allows a POS Application to initiate a financial transaction. The POS Application sends the transaction amount (and optionally other sale data) to the terminal;

- Operator prompts are displayed on the POS display. The operator is not required to switch attention between the POS display and the terminal. This means the terminal (or PIN pad) may face the customer all the time;

- Receipts can be controlled by the POS Application or Vault can be configured to use any printer supported by Windows or to use a serial printer;

The features are described in more detail below.

2.2 General Features

2.2.1 Operator Console Support

Vault supports the following console (keyboard, mouse, display) configurations:

- *Touch Screen (no keyboard or mouse):* This is achieved by using oversize buttons and by providing a 'keyboard' dialog for data entry.

- *Keyboard Only:* All dialogs use the usual Windows keys for controlling navigation. Additional keyboard shortcuts are also available to speed operator interaction.

- *Mouse with No Keyboard:* This behaves similarly to the Touch Screen configuration above but the mouse is the pointing terminal instead of the screen.

- *Keyboard and Mouse:* No special support required.

No additional configuration is required to support all the configurations above. Vault supports all configurations simultaneously.

2.2.2 Deployment Features

Vault supports deployment within a variety of environments:

- Standard Thick-Client POS Applications;
- Custom server-based POS Applications;
- Windows Terminal Services hosted POS Applications;
- Citrix hosted POS Applications;

2.2.3 Standalone / Integrated Mode

Vault enabled EFTPOS terminals that have an in-built printer can be configured in standalone mode in the case of a POS failure.

2.2.4 Auto Update Feature

Vault enabled EFTPOS terminals have an Auto Update software feature built into the payment application. The Auto Update function periodically contacts VeriFone's Terminal Management System (VeriCentre) to check for new updates and downloads them. This ensures Vault terminals are using the latest software version available.

Auto Update is designed to call VeriCentre in a defined time window. By default this is between 11pm and 5am. The actual time a terminal connects during the Vault Auto Update window are randomly assigned to each lane. For merchants trading between 11pm and 5am, the start time and duration can be reconfigured to a period when the site is more likely to be quiet.

The default settings downloaded at time of install are:

- Start Time = 11pm
- Duration = 360 minutes (6 hours)
- Frequency = 7 days (7019) or 31 days (7016 / 7018)

With these default settings, auto updates will occur every 7 or 30 days, between the hours of 11pm and 5am.

2.2.5 Financial Transaction Support

The table below outlines the financial transactions supported by Vault.

Transaction	Description/Notes	Supported
Purchase	Supports EOV	**YES**
Analyse Purchase	Supports EOV for selected fuel cards	**YES**
Purchase plus Cash	-	**YES**
Refund	-	**YES**
Cash Out	-	**YES**
CSE	Currency Select Eftpos	**YES**
Cheque Authorisation	via Paymark	**YES**
Open Hospitality Account (excludes top up)	This performs a pre-authorisation transaction. It does not allow for top up or additional authorisations using the same card number.	**YES**
Close Hospitality Account	This performs a completion/advice transaction.	**YES**

2.2.6 Non-financial Transaction Support

The table below outlines the non-financial transactions supported by Vault. These functions are found under the Vault Administration menu.

Transaction	Description/Notes	Supported
Logon	Merchant Log On to the Eftpos Network	**YES**
Settlement Inquiry	Settlement Inquiry	**YES**
Settlement Cutover	Settlement Cutover	**YES**
Sub Totals (shift totals)	Shows current transaction totals for the current shift	**YES**
Stored Totals	Prints a summary of all pending transactions, EOV etc	**YES**
Card Swipe	Returns track 2 data to the POS for gift and loyalty card processing	**YES**
Reprint Receipt	Reprints last Receipt	**YES**
Upload Offline Transactions	Upload Stored EOV and Hospitality Transactions	**YES**

2.2.7 Features Supported in Standalone mode but NOT with Vault

These functions are supported within the payment application but cannot be used when integrated with Vault.

Transaction	Description/Notes	Supported
Credit Card Tipping	Allows a tip to be added to a credit card transaction that has been Pre authorised	**NO**
Instant PIN pad Tipping	Allows a tip to be added by the card holder on the PIN pad at the time of PIN entry	**NO**
Manual Log Off	Forces the terminal into a log off state	**NO**

2.2.8 Analysed Purchase

Vault supports analysed purchase transactions which are required for some fuel cards and loyalty applications. Analysed purchase software can only be installed via a VeriCentre download and must be entered into the VeriCentre record for all Vault lanes that require analysed purchase functions.

During an analysed purchase transaction the POS will send additional information with each transaction which will include product items, number of litres and transaction value. Depending of the card type presented, Vault will send this additional information to Paymark as part of the transaction message.

Account selection is not required for some analysed purchase transactions and the account selection could default to credit and bypass this step. Depending on the card type, an odometer amount may be requested.

Purchase transactions that perform Analysed Purchase are triggered by the Card BIN range (a range of card numbers) that is loaded into the Vault Analysed Purchase card table. The card table is set by various fuel companies for various fuel sites and is stored on the terminal.

It is possible for one fuel company to perform Analysed Purchase with other (fuel) company cards, yet another fuel company might only permit Analysed Purchase with their own cards.

Odometer entry can be performed either on the POS or the Eftpos Terminal (default). To change the entry location contact the VeriFone helpdesk to update the record and then complete a Utility > Download on the terminal.

2.2.9 Currency Select Eftpos (CSE)

CSE offers international customers the option to pay in their own currency. It is only available to BNZ merchants and is enabled on the terminal via a VeriCentre download and is fully supported by Vault.

While the customer is selecting the currency they wish to pay in the merchant will see the following dialog box on the POS screen.

CurrencySelect supports 12 approved foreign currencies. They are Australian, Canadian, Hong Kong, Singapore and United States dollars, Euro, British pounds, Swiss francs, Chinese yuan, Japanese yen, Korean won, and South African rand. The card presented to the terminal will determine which currency(ies) are offered to the customer.

Customers' card statements will show the price they accepted at the time of purchase. This protects customers from currency fluctuations, so for them, it's just like paying a local business.

2.3 POS Platform Requirements

The POS platform has some basic requirements which usually will already have been checked and tested by the POS vendor. Vault does not normally have platform requirements that exceed the requirements of the POS Application.

2.3.1 General Requirements

In order to run correctly Vault must be installed on a system that meets the following requirements:

- The system must have adequate RAM memory. Vault will require around an additional 8-16MB over the normal operation of the POS Application. Only systems which have barely enough memory without Vault will need to be upgraded (or have the system memory load reduced).

- The system must have at least 10MB of free HDD space for Vault to save its configuration and state information.

2.3.2 Windows Requirements

The following requirements apply to deployment with Windows based POS Applications:

- Vault requires that the Microsoft .NET Framework 2.0 (or later) is installed on the POS Platform.

- Vault is supported on Windows XP or later. Note that Vault has been tested on Windows XP through to Windows 10.

- Java API requires Java Runtime 1.5 or later.

- COM API requires the installation of the COM API install package provided with the SDK. POS vendors are responsible for its installation.

2.3.3 Linux Requirements

Vault does not yet support deployment with Linux based POS Applications.

2.4 Supported EFTPOS Terminals

Vault is supported on the following VeriFone terminals:

- VX820 PIN pad only with Ethernet dongle;
- VX820 Duet
- VX520 with Internal PIN Pad (two piece terminals are not supported)
- VX680 Wi-Fi
- Vx810 PIN pad only with Ethernet dongle;
- Vx810 Duet;
- Vx510 with Internal PIN Pad (two piece terminals are not supported);

2.5 Network Requirements

2.5.1 Connection

The connection from the POS Application to the Vault Device must be over Ethernet (TCP/IP).

2.5.2 Assigning an IP Address

Vault devices that are connected to an IP network must have an IP address assigned to them. This can be assigned manually (fixed IP address) or automatically (via DHCP).

In almost all cases, the POS application needs devices to have an IP address that does not change. This is not a problem for devices with fixed IP addresses but it will be a problem with devices that have an address assigned via DHCP. Therefore, if DHCP is the preferred choice for assigning an address to the device the DHCP server must be configured to always assign the same IP address to the device (it normally does this by reserving an IP address for a specific MAC address).
Whatever method is used for assigning IP addresses to a Vault device, there must be procedures in place to ensure that the IP address is transferred to the new device when a swap-out occurs.

2.5.3 Dynamic DNS

VeriFone terminals do not support Dynamic DNS at the present time.

2.5.4 Internal Firewall Requirements

Default configuration
When using Ethernet connections any firewalls must allow the POS Application to connect to the device over TCP port 20001. Firewalls must also allow connections from the device back to the POS Application using any of the dynamically assigned TCP ports. On Windows Vista and later this range is 49152 to 65535. Earlier versions of Windows will use the range 1025 to 5000.

Custom configuration
Vault terminals create two TCP/IP connections during operation. One connection originates from the Vault library to the terminal using a well-known port number (20001). The other connection, called the device channel connection, originates from the terminal to the Vault library. This second connection uses a dynamically allocated port on the POS machine.
Using a dynamically allocated port for the device channel connection can cause difficulties when it comes to firewall configuration. To address this issue Vault allows the device channel port to be statically configured during deployment. This feature is enabled by creating a file called '*DeviceChannelPorts.xml.txt*' in the Vault configuration directory. This directory is located in:

- *C:\ProgramData\Vault* on Windows 7 or later **OR**;
- *C:\Documents and Settings\All Users\Application Data\Vault* on Windows XP and Windows 2000.

The file content should be a properly formed XML document with the following structure:

```
<ports>
    <lanes>
        <LANE1>
            <device-channel-port>30001</device-channel-port>
        </LANE1>
        <LANE2>
            <device-channel-port>30002</device-channel-port>
        </LANE2>
    </lanes>
    <default>
        <device-channel-port>31000</device-channel-port>
    </default>
</ports>
```

The example file above says that “LANE1” and “LANE2” should use port 30001 and 30002 respectively and that all other lanes should use port 31000. The <lanes> node is optional and can be removed if not required.
If only one POS lane will be controlled from the POS PC then the simplest configuration will have only the <default> node present.
If multiple POS lanes will be controlled from the PC (e.g. on a server-based POS) then the <lanes> node should be present and a separate node should exist for each named lane. The lane names must match the name sent to create the Vault Session object.

NOTE: Device channel port is only supported with Vault Adaptor 292.0 or later

2.5.5 External Firewall Requirements

In order for the solution to operate correctly the firewall that controls access to the internet will need to be configured to permit the following outbound connections.

Host	Port	Description
117.120.34.110	33876	Paymark Primary
117.120.32.110	33876	Paymark Secondary
117.120.34.103	7540	Paymark RKI Server
203.79.66.113	8013	VeriCentre
vericentre.co.nz	FTP (21)	FTP Host required for CSE

2.5.6 Terminal Communication Options

The following terminal options for communication to the switch are supported:

- *Direct IP Only*: With this option the terminal has two IP addresses that the terminal can use to connect to the switch.

- *Direct IP with Dialup Concentrator*: This option is like the first option except that one of the IP addresses points to a dialup concentrator (VEAC) on the network.

2.5.7 Wireless Networks

External
Wireless networks are supported for external network access.

Internal
Wireless networks can be used with Vault but particular care needs to be taken to ensure that the link is very reliable. Even a 0.5% connection loss rate will likely cause every tenth financial transaction to fail and resort to potentially lengthy link failure processing.

2.6 Printer Support

Vault solutions support the following print methods:

- Any printer controlled by the POS Application;
- Any printer that is installed as a Windows printer. This includes network printers;
- Any ASCII serial printer (e.g. EPSON TM-T88 or similar);

The print options available to Vault are determined by the POS developers. Where POS controlled printing (Option 1 above) has not been developed the raw print data is delivered to Vault to direct to a printer (Options 2 and 3 above). Often these last two options result in a poorly laid out eftpos receipt. See section 9.3 for instructions on printer setup in these scenarios.

2.7 Approvals

2.7.1 Paymark

The following software combinations are certified for use in a Vault solution. Each line in the table below represents a certified combination. Any other combinations are not certified and must not be deployed.

Payment Application Version	**Vault Applet Versions** (On Terminal)	**Vault Adapter Version** (on POS)
PKMSNZ 7016	WIN32 VAULT 0205 WIN32 VAULT 0207	Version 2.3 and later
PKMSNZ 7018	WIN32 VAULT 0207	Version 2.8 and later
PKMSNZ 7019 V3 / V4 / V5 /V6	WIN32 VAULT 1.0.0	Version 292.0 and later
PKMSNZ 7019 V7 / V8	WIN32 VAULT 1.0.6	Version 292.0 and later
PKMSNZ 7019 V9	WIN32 VAULT 2.0.0	Version 294.0 and later
PKMS 2015 V1	WIN32 VAULT 2.0.0	Version 295.0 and later

See section 4.7.1 on the process to check version numbers.

2.8 Read-only VDI Considerations

VDI is a software technology that separates the desktop environment and associated application software from the physical client device that is used to access it. It has significant benefits in terms of management, security, and costs. Read-only VDI systems are used to ensure that desktop images never change over time. Any changes applied to the file system of the desktop image are discarded after the image is shutdown. This reduces the likelihood of viruses and other malware infecting the system and other systems.

Vault will not work correctly on read-only VDI systems since it must be able to keep records of transactions and configuration between user sessions. Getting Vault to work on VDI systems requires one of the following changes:

1. The VDI system must exclude *C:\ProgramData\Vault* from the read-only portion of the file system;

2. The Vault data and log files must be stored on a separate file-system that is not rolled back at the end of a VDI session.

It is difficult to achieve option 1 above but option 2 can be implemented by adding a *redirect.xml* file to the *C:\ProgramData\Vault* directory. The *redirect.xml* file is used to tell Vault where the Vault data and log files can be found and updated. An example of the file is shown below:

```
<redirect>P:/Vault</redirect>
```

The content in the *<redirect>* tag should contain the path of the directory where the files can be found and updated. The system administrator will need to grant sufficient privileges to allow authenticated users to create, delete, and update files and sub-directories within this directory.

3 Vault Installation and Configuration

3.1 Installation Overview

Installation of one or more Vault lanes follows the process below:

1. The reseller submits a VeriCentre load form (or forms) to VeriFone with the Vault terminals configuration. VeriFone will confirm that the lane(s) has been loaded;

2. The installer ensures that all items on the pre-installation checklist have been completed;

3. The installer delivers and connects up the Vault terminal;

4. The installer downloads the terminal settings from VeriCentre;

5. The installer initiates Remote Key Injection (RKI);

6. (Optional) The installer configures the POS Application to activate the Vault interface to communicate with the Vault terminal;

7. The installer verifies that the installation is operating correctly by performing an EFTPos Logon from the POS;

The following sections cover the steps above in more detail:

3.2 (Step 1) Loading Lanes on VeriCentre

This step is normally handled by the reseller. It involves the completion of either the VeriCentre load form or direct record creation via the web console for individual lanes or the VeriCentre Excel template for mass record creation. Refer to Paypedia for the latest version of the VeriCentre Load Form.

3.3 (Step 2) Pre-Installation Checklist

The items on the checklist below should be completed before going out to the Merchant site and installing the Vault hardware. Failure to do so may mean lengthy delays and additional trips to the site.

1. Confirm that the Vault lane has been set up on VeriCentre.

2. Confirm that the POS Application has been approved to interface with Vault enabled terminals.

3. Confirm that the correct POS software version been installed and set up on the merchant's POS system. You may need to check with the POS vendor.

4. *[Reserved DHCP Solutions Only]* If the terminals will use DHCP to get their IP address then ensure that the site has reserved IP addresses for each terminal. In order to do this the merchant will need to be supplied with the MAC addresses of the terminals to be installed. *Note:* If non-reserved DHCP addresses are used then Vault lanes may fail to work if the terminal's IP address changes (i.e. during a hardware swap out or reboot).

5. *[Static IP Solutions Only]* Collect all the network parameters for the terminals being installed. The parameters that are required are:

   - *Terminal IP Address*.
   - *The Network Mask*.
   - *The Gateway Address*.
   - *(Optional) Primary and Secondary DNS addresses.*

6. Make sure the IP addresses for all the terminals are recorded for later use.

7. Ensure that either:
   - All POS machines have been pre-configured to use Vault as the preferred method of integrated payment;
   - The information or expertise required to configure the POS machines to use Vault terminals is available;

8. Ensure that instructions for getting a POS machine to perform a logon via the Vault interface are available.

9. Ensure that the required hardware is available. For example, Ethernet cables, Ethernet switch, etc.

10. Ensure that the site has the appropriate services available at each POS lane. These will include power sockets, Ethernet ports, etc.

11. Ensure that the network firewalls been setup to allow the required communication paths. See above sections for details on the required firewall configurations.

Please contact the POS Vendor or site administrator if you are unsure or require assistance with POS and firewall set ups

3.4 (Step 3) Install Hardware

Once at site the terminal should be installed, connected, and then powered up. If the EFTPOS terminal is intended to operate in standalone mode then ensure that a paper roll is loaded in the terminal's in-built receipt printer. At the end of the step the terminal must be connected to the local area network and have access to the internet.

3.5 (Step 4) Download Terminal Configuration

In this step, the installer gets the terminal to download its settings from the VeriCentre TMS. The settings will have already been loaded into VeriCentre in step 1 above.

Download Parameters

Host IP :	203.79.66.113
Host Port:	8013
*ZA:	*MA
*ZT:	VeriCentre Record ID, (Usually the Terminal ID). If unsure check with the VeriFone NZ Helpdesk.

Paymark software version 7019V8 and below

On the terminal:

1. If the administration menu is not active, activate it by pressing ENTER followed by 7 and then enter the manager password (default 999).
2. Scroll to Utility.
3. Press Utility.
4. Scroll to Download.
5. Press Download.
6. Press IP (If requested)
7. Press Yes when asked to EDIT ALL PARAMETERS?
8. The terminal will display Host IP VALUE. This should be: 203.79.66.113
9. If correct press the green enter button. If not type in and then press Enter.
10. The terminal will display Host Port VALUE. This needs a value of: 8013
11. If correct press the green enter button. If not type in and then press Enter.
12. Select Fixed and continue to step 13 or DHCP and skip to step 18.
13. Type in Terminal IP VALUE and press Enter.
14. Type in Gateway VALUE and press Enter.
15. Type in Subnet Mask VALUE and press Enter.
16. Type in Primary DNS VALUE and press Enter or press Enter to accept the default 0.0.0.0.
17. Type in Secondary DNS VALUE and press Enter or press Enter to accept the default 0.0.0.0.
18. The terminal will display *ZA VALUE. This needs a value of: *MA
19. If correct press the green enter button. If not type in and then press enter.
20. The terminal will display *ZT VALUE. This is the VeriCentre record number (usually this is set to the Terminal ID of the lane being installed). If correct press enter or type in the correct details and press enter.
21. Press Yes to initiate the download.

The terminal will then perform the download. On completion of the download, the downloaded files will be decompressed and installed. The terminal will then reboot into Integrated Mode.

Paymark software version 7109V9 / 2015

7019V9 terminals are provided in DHCP mode. If the network does not have DHCP available then a static IP address will need to be programmed prior to the download being initiated.

To change IP settings on the terminal:

1. If the administration menu is not active, activate it by pressing ENTER (7019) or # (2015) followed by 7 and then enter the manager password (default 999).
2. Scroll down if necessary and Press UTILITY
3. Press COMMS SETTINGS
4. SELECT HOST ADDRESS TYPE is displayed
5. Press IP
6. ENTER HOST IP 117.120.34.110 is displayed
7. Press the Green Enter Key if correct, otherwise type in a new HOST IP address and press green Enter key
8. ENTER SECONDARY IP 117.120.32.110 is displayed
9. Press the green Enter key if correct, otherwise type in a new SECONDARY IP address and press green Enter key
10. ENTER IP PORT 33876 is displayed
11. Press the green Enter key if correct, otherwise type in a new IP PORT number and press green Enter key
12. USE SSL? Is displayed
13. Press NO
14. SELECT IP ADDRESS SETUP is displayed
15. Press DHCP (the terminal will restart and will be using DHCP addressing) or FIXED to continue with static configuration
16. ENTER TERMINAL IP ADDRESS is displayed
17. Type in the new TERMINAL IP ADDRESS and press green Enter key, or press green Enter key if correct
18. ENTER GATEWAY IP ADDRESS is displayed
19. Type in the new GATEWAY ADDRESS and press green Enter key, or press green Enter key if correct
20. ENTER SUBNET MASK is displayed
21. Type in the new SUBNET MASK and press green Enter key, or press green Enter key if correct
22. ENTER PRIMARY DNS is displayed
23. Type in the new PRIMARY DNS and press green Enter key, or press green Enter key if correct
24. ENTER SECONDARY DNS is displayed
25. Type in the new SECONDARY DNS and press green Enter key, or press green Enter key if correct
26. The terminal will restart and return to the idle screen

To initiate the download on the terminal:

1. If the administration menu is not active, activate it by pressing ENTER (7019) or # (2015) followed by 7 and then enter the manager password (default 999).
2. Scroll to Utility.
3. Press Utility.
4. Scroll to Download.
5. Press Download.
6. Press IP (If requested)
7. Press Yes when asked to EDIT ALL PARAMETERS?
8. The terminal will display Host IP VALUE. This needs a value of: 203.79.66.113
9. If correct press the green enter button. If not type in and then press enter.
10. The terminal will display Host Port VALUE. This needs a value of: 8013
11. If correct press the green enter button. If not type in and then press enter.
12. The terminal will display *ZA VALUE. This needs a value of: *MA
13. If correct press the green enter button. If not type in and then press enter.
14. The terminal will display *ZT VALUE. This is the VeriCentre record number (usually this is set to the Terminal ID of the lane being installed). If correct press enter or type in the correct details and press enter.
15. Press Yes to initiate the download.

The terminal will then perform the download. On completion of the download, the downloaded files will be decompressed and installed. The terminal will then reboot

3.6 (Step 5) Initiate Remote Key Injection (RKI)

At this point a new terminal will not have any security keys from Paymark installed. To install the keys, Remote Key Injection (RKI) is required. To initiate RKI the installer must follow the instructions below:

SOFTWARE VERSION 7016 / 7018

With software version 7018 this needs to be performed on the terminal and not via the POS (Administration Menu). This is due to the lengthy key exchanges which results in the terminal taking too long to respond to the POS, which will cause the Vault Adaptor to display a “Power / Link Failure” and the final result of the RKI (Accepted or Please Try Again) will be missed. The solution with this software version is to perform the Init RKI on the terminal.

1. On the terminal press ENTER followed by the 7 key.
2. Enter the manager password (default 999).
3. Select **Utility**.
4. Scroll down and select **Init RKI**.
5. Enter the password 6987 and press ENTER.
6. Wait while RKI completes.

7. Once Accepted call Paymark's Keyset Express system to complete the RKI process.

SOFTWARE VERSION 7019 / 2015

With software versions 7019 and 2015 the Init RKI should be performed from the POS via the Vault Eftpos Admin menu prior to logging on for the first time. Init RKI will be completed after the configuration of the POS application outlined below.

3.7 (Step 6) Configure POS Application

This step involves the installer configuring the POS Application(s) to use Vault as the preferred method of integrated payment. This step may not be required if the POS Application has already been configured by the merchant or POS Vendor.

If the POS Application has not been configured then the installer will need to either:

1. Request the POS Vendor to make the necessary changes;

2. Use documentation provided by the POS Vendor to make the necessary changes;

3. Use POS Interface Configuration Guide to make the necessary changes.

3.8 (Step 7) Complete and Verify Installation

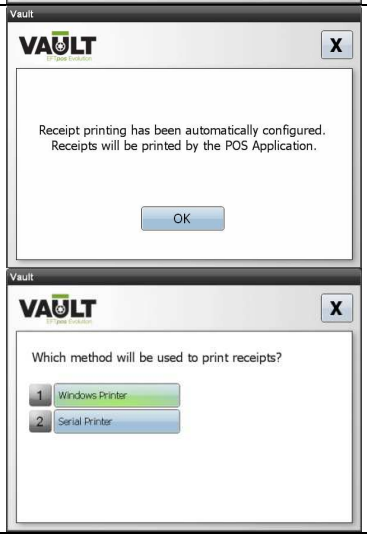
In this step, the installer verifies that the installation has been completed successfully. To do this the installer attempts to successfully complete a logon transaction.

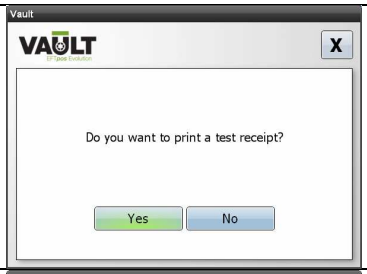
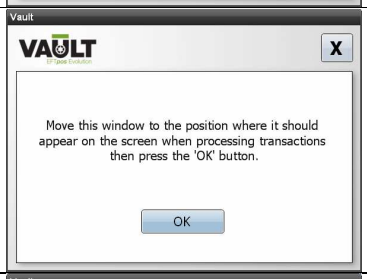
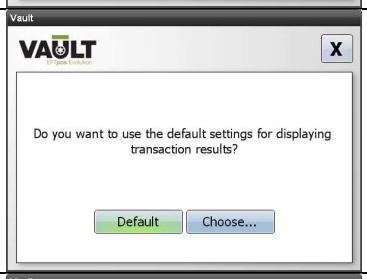
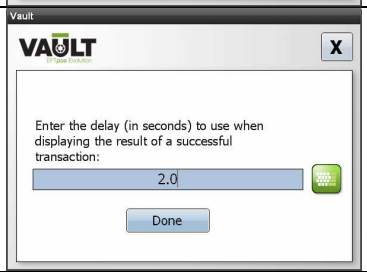
Start the POS Application and locate the EFTPOS administration menu. This may be listed under a different name depending on the POS Application. If in doubt, consult the POS Vendor's documentation. Once the administration menu is activated you will see the following window appear to configure the Vault interface.

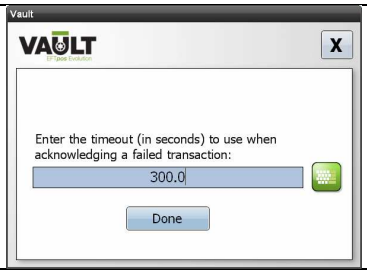
Note: The Vault wizard window shown below will only appear if the POS is not using a Dynamic Configuration to automatically configure the Vault POS parameters. Otherwise go straight to 3.8.1 Log On.

VAULT CONFIGURATION WIZARD

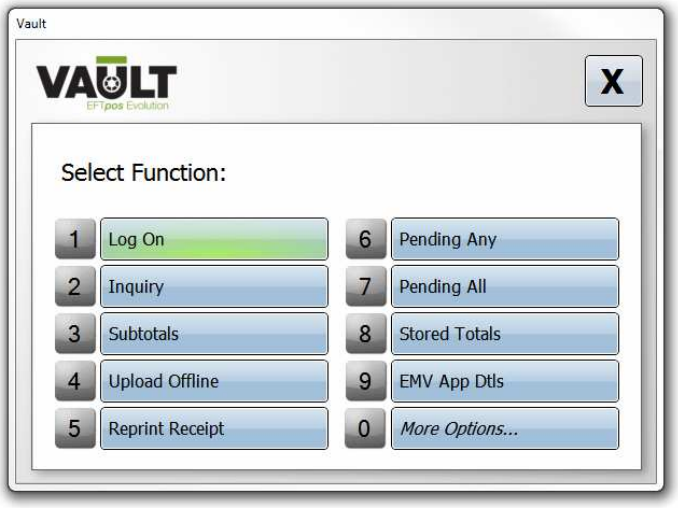
If unsure about any settings choose the 'default' option – these can be changed at a later stage if they are incorrect.

Configuration Step 1		Initiating an Eftpos transaction or bringing up the Vault Admin menu will bring up the configuration wizard. Select Yes to continue.
Configuration Step 2		Enter in the Vault terminals IP address and select Done.
Configuration Step 3		The Vault Adapter will attempt to communicate with the terminal.
Configuration Step 4		If there is a newer Vault Adapter installed on the terminal it will install now.
Configuration Step 5		The receipt printing method will now be requested. If the POS Application is controlling the receipt it will automatically advise this with an OK prompt else the option to Choose a Windows or Serial printer will appear. Choose the appropriate option. See Appendix D for Windows and Serial Printer screens.

Configuration Step 6		Select No to print a test receipt.
Configuration Step 7		Since the 293.0 Adapter release the addition of two Vault window sizes have been possible. Choose either Default or Small as required.
Configuration Step 8		Move the window to the best location for the Vault messages to appear and select OK.
Configuration Step 9		Select Default to accept the default settings or Choose for custom settings. If Default is selected the configuration will have been completed.
Configuration Step 10		Select No unless Operators are required to acknowledge the completion of every successful transaction.
Configuration Step 11		This controls the length of time the Accepted message must be displayed for. The minimum allowed is 2.0 seconds. If this is desired to be longer enter the time in seconds that the accepted message will remain before the transaction continues.

Configuration Step 12		A failed transaction will require the operator to acknowledge the failure before continuing for this length of time. After this length of time the Declined transaction will timeout and return to the idle screen.

Once the configuration wizard is complete you will see the following window:



3.9 *Log On*

SOFTWARE VERSION 7016 and 7018

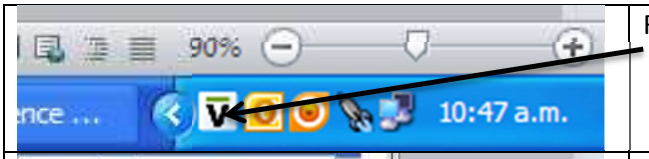
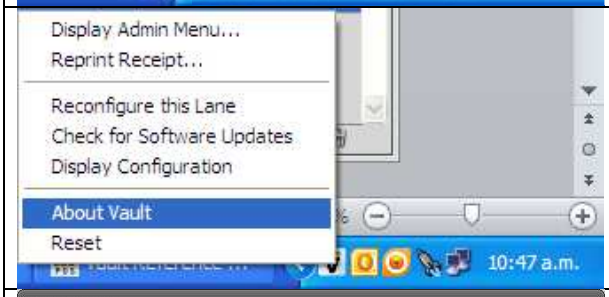
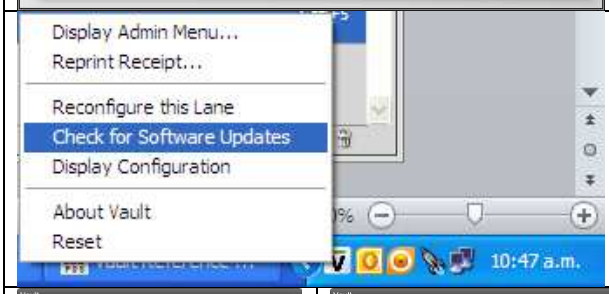
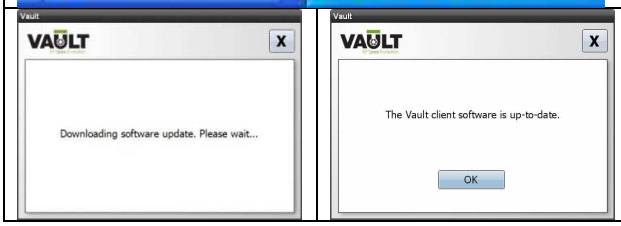
Select the 'Log on' option. If everything has been set up correctly then a Logon transaction will complete successfully and a receipt will be printed.

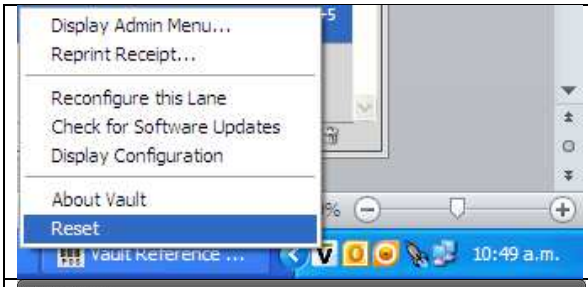
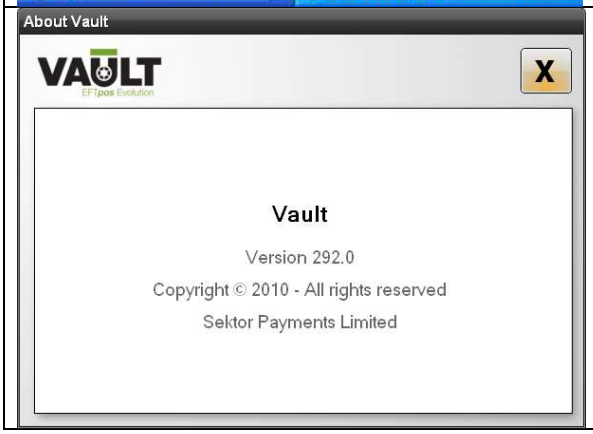
SOFTWARE VERSION 7019 and 2015 - Initiate Remote Key Injection (RKI) and Log On

From the POS application select the Vault administration Menu. Select *More Options…* and then Init RKI. Once Accepted call Paymark's Keyset Express system to complete the RKI process. Once complete, from the POS application select the Vault administration Menu. Select the 'Log on' option. If everything has been set up correctly then a Logon transaction will complete successfully and a receipt will be printed.

3.10 Check for a new Vault Adapter

During the installation process a new Vault Adapter may have been downloaded into the terminal. It is recommend to check for a later version at this point.

	RIGHT CLICK on the Vault icon
	Select ABOUT VAULT
	This will display the current Vault Adapter version. Use this to double check the upgrade was successful when finished
	RIGHT CLICK on the Vault icon again and select CHECK FOR SOFTWARE UPDATES
	If there is a newer adapter it will begin to download from the terminal. Else it will advise there is no update required.

	Once complete RIGHT CLICK the Vault icon and select RESET
	Once the Vault icon returns RIGHT CLICK it again and select ABOUT VAULT. The version number should have changed since first checked.

If the update fails see Appendix C for additional information.

3.11 First Auto Update

Once installed, Vault will automatically connect to VeriCentre at a predefined date and time to check for new software updates or configuration changes. With 7016 and 7018 software, the first Auto Update will occur within 24 hours of installing the terminal. With 7019 and 2015 software the first Auto Update will occur within the Auto Update window set in the terminal (by default, in 7days time). Thereafter all terminals will check for updates according to their defined Auto Update parameters.

3.12 Manual PAN Entry

While Vault supports Manual PAN entry this feature can be disabled by changing a setting on VeriCentre and completing a Utility > Download on the terminal. By disabling this feature it will override the Paymark configuration where it might be turned on.
To make the change you can either modify the setting via the web console or by contacting the Verifone NZ Helpdesk on 0800 837 436 prior to downloading. By default, Manual PAN entry is enabled.

4 Vault-OCX Adapter

The Vault OCX Adapter opens up POS Applications that have been certified for use with PCEFTPOS to be recertified as a Vault payment solution. For an up-to-date list of certified solutions check the verifone.co.nz website.

4.1 Requirements

The Vault OCX adapter is available from Paypedia and must be installed on the same machine as the POS Application. It can be deployed on machines running Windows XP or later and that have the Microsoft .NET Framework v2.0 or later installed.

4.2 Limitations

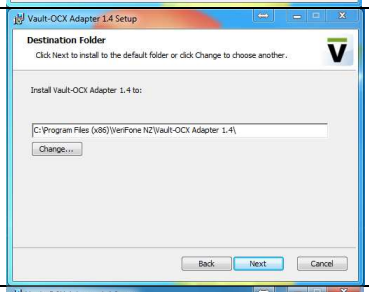
Due to differences between PCEFTPOS and Vault not all features of Vault or PCEFTPOS are supported. These limitations are outlined below:

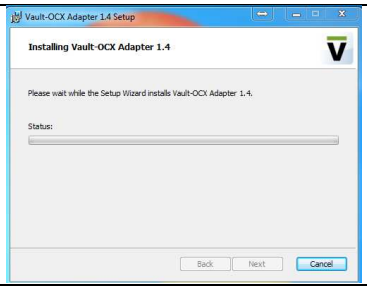
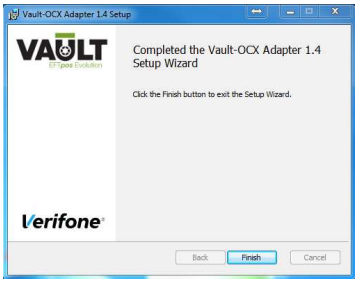
Limitation	Description/Notes	Supported
Logon	The logon function will not directly cause the PIN pad to logon to Paymark. It will open the administration menu and the operator will need to select the 'Logon' menu item.	**YES**
Settlement Inquiry	The settlement enquiry function will not directly cause the PIN pad to perform a settlement enquiry (or inquiry). It will open the administration menu and the operator will need to select the 'Settlement Inquiry' menu item.	**YES**
Multi Merchant	The adapter will, by default, support only one merchant. Supporting multiple merchants can be implemented by creating a special configuration file in the Vault directory (Requires extra certification). (See 4.4 Multi-Merchant Configuration below).	**YES**
Analysed Purchase	Support for Analysed Purchase transactions.	**NO**
Manual PAN	Manual PAN entry from the POS Application.	**NO**
Disabling Credit Account	Disabling the Credit account selection option.	**NO**
CAID	Attempts to get the terminal CAID will always return "000000000000000".	**NO**

Card Types	The transaction card types will be different to those returned by PCEFTPOS. This is because the card logo is now being returned by Paymark. It could affect merchants reporting.	**YES**
Track 1	Track1 cannot be retrieved when using the query card functionality. (e.g Cardholder name etc).	**NO**
Instances	Only one instance of a PCEFTPOS POS Application can be run at a time on the machine.	**NO**

4.3 Installation

Prior to installation please shutdown all POS Applications. If PCEFTPOS is installed please uninstall it (see Appendix for instructions).

Configuration Step 1		Run the *Setup_VaultOCX_nnnn.msi* installer (This can be downloaded from Paypedia) Select Next to continue.
Configuration Step 2		Enter in the destination folder and Select Next to continue.
Configuration Step 3		Select Install to initiate install. Windows will often ask you for permission before performing install, you'll just have to say yes or no.

Configuration Step 4		You will be presented with a progress bar screen.
Configuration Step 5		When finished installing you will be presented with a completed screen. Select Finish to complete

Note: After the adapter has been installed you will then be able to run the POS Application and test it. The POS needs to have its integration type set to PC EFTPOS.

Running the POS Application the first time should cause the Vault configuration wizard to appear. You should follow 3.8 (step7) (found in the Vault operations guide) to configure Vault.

4.4 Multi-Merchant Configuration

By default, single merchant operation is supported. However, adding an XML configuration file named '*PCE.merchants.xml*' into the drectory '*C:/ProgramData/Vault/{machine-name}/Configuration'* will cause the adapter to support up to 8 merchants. In Windows XP the directory will be called *'C:/Documents and Settings/All Users/AppData/ Vault/{machine-name}/Configuration'*.

An example of the file content is shown below.

```
<?xml version="1.0" encoding="utf-8" ?>
<merchants>
  <merchant index="1" name="MERCHANT ONE"/>
  <merchant index="5" name="FIVE"/>
  <merchant index="6" name="SIX SIX SIX SIX SIX SIX"/>
</merchants>
```

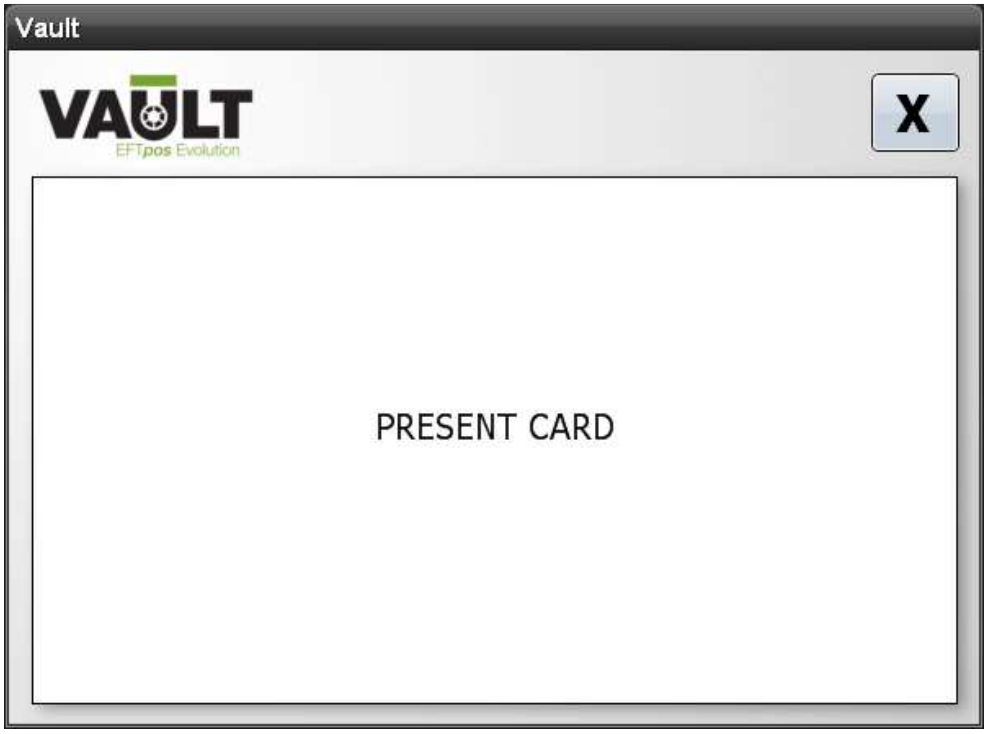
5 Vault Operation

This section describes how to use Vault after it has been installed and configured.

5.1 User Interface

5.1.1 Vault Dialogs

When a transaction is taking place Vault will normally open dialogs on the desktop to tell the operator what is happening and in some cases to request the operator to perform some data entry. An example of a Vault dialog is shown below:



The example above is normally the first dialog an operator will see when a financial card transaction is started from the POS Application.

5.1.2 Cancel Button

The button with the 'X' is the cancel button. It can be used to cancel the current transaction or function. If the transaction or function is in a state that cannot be cancelled then clicking on the button will have no effect and the transaction will proceed as normal.

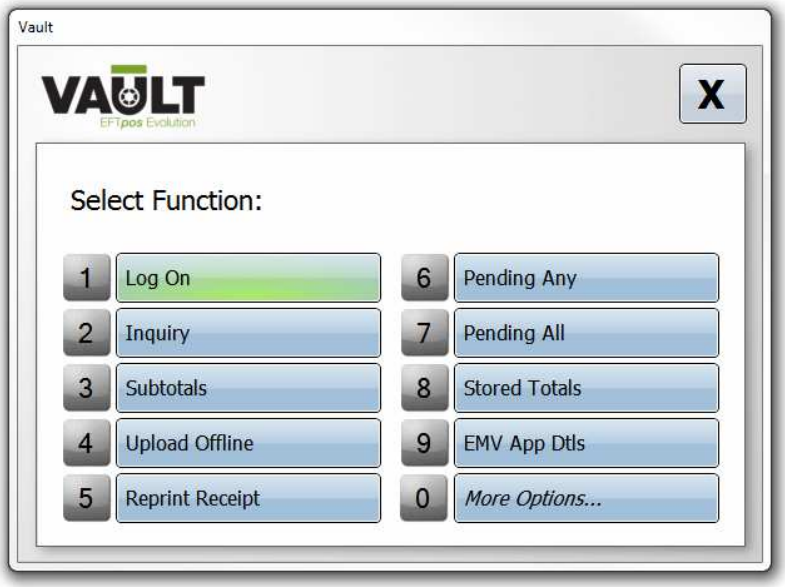
5.1.3 The Keypad

The button with the keypad icon allows data entry to be performed without a keyboard. It opens the keypad dialog that allows the user to use the mouse or the touchscreen to enter data. The screen shot below shows how the keypad dialog looks.

5.1.4 Keyboard Shortcuts

Vault uses the standards Windows key assignments for navigating the dialogs without a mouse or touchscreen.

- The <TAB> key moves between the buttons and data entry controls. <Shift><TAB> moves in the reverse direction.
- The <SPACE> key will activate (press) the current selected button.
- The <ENTER> key will activate (press) the current selected button.
- The <ENTER> key will accept the current data entry and complete the current data entry operation.
- The arrow keys can be used to navigate data entry controls.
- The arrow keys can also be used to navigate between buttons.
- On dialogs which allow selection between multiple options (these dialogs have numbers next to each selection) the associated number key can be pressed to select the desired option. In the example below pressing 1 will select ‘Logon’.



5.2 The Vault Tray Icon

When the POS Application opens a session to the Vault Terminal the Vault icon will appear in the system tray. The Vault Icon has the following appearance:

If the Vault Icon is right clicked on then a menu appears with various administration functions. Each of the functions is described in the sections following.

5.2.1 Display Administration Menu

This function will display the administration menu of the Vault Terminal. This menu will allow the user to select from various financial administration functions available on the terminal. These functions include 'Logon', 'Settlement Enquiry', 'Print Stored Totals' etc.

5.2.2 Reprint Receipt

This function will allow the user to select and print the receipt from a recent transaction.

5.2.3 Reconfigure this Lane

This function will restart the configuration wizard and allow the user to re-configure the integration settings for the lane (i.e. checkout, counter, etc). If the wizard is cancelled at any point then the current configuration remains unchanged.

5.2.4 Check for Software Updates

This function will ensure that the PC based part of the Vault software is up to date. If a newer version is available then it will be downloaded from the Vault terminal and installed immediately.

5.2.5 Display Configuration

This function displays the current configuration of the lane.

5.2.6 About Vault

This function displays the current version of the Vault software.

5.2.7 Reset

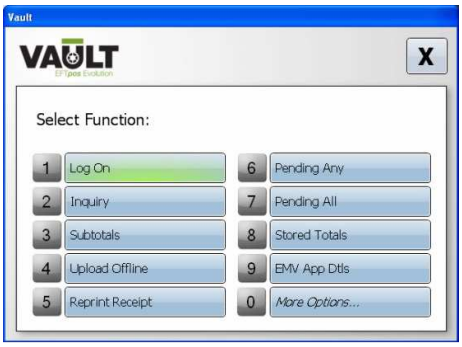
This function resets the connection between the POS Application and the Vault terminal.

5.3 Accessing Administration Functions

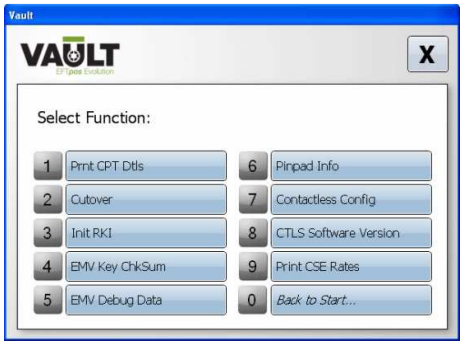
Initiating administration functions can be done one of two ways:

1. Right-click on the Vault tray icon and select Display Administration Menu;

2. Select the Vault Administration function from the POS Application. The method for doing this will be specific to each POS Application;



Admin Menu 1



Admin Menu 2

ADMINISTRATION MENU	
1 Log On	Does a Merchant Log On to the Eftpos Network
2 Inquiry	Settlement Inquiry
3 Subtotals	Shows the transaction totals for the current shift and offers to reset them
4 Upload Offline	Upload Stored EOV and Hospitality Transactions

5 Reprint Receipt	Reprints last Receipt
6 Pending Any	Reprint a specific pending stored transaction
7 Pending All	Prints all pending Transactions, EOV transactions Etc. . .
8 Stored Totals	Prints a summary of all pending transactions, EOV etc. . .
9 EMV App Dtls	EMV application identifiers.
0 *More Options...*	Shows second Admin Screen
1 Prnt CPT Dtls	Prints Card Prefix table
2 Cutover	Performs a settlement cutover
3 Init RKI	Perform an Init RKI. (7019/2015 software only)
4 EMV Key ChkSum	EMV Checksum of all EMV data pages.
5 EMV Debug Data	EMV debug data for previous EMV transaction
6 Pinpad Info	Displays current KVC Value
7 Contactless Config	Prints out the Application ID's and transaction limits
8 CTLS Software Version	Displays the current firmware version of the contactless reader
9 Print CSE Rates	Prints out the current CSE rates. Will offer to update if rates have expired
0 *Back to Start...*	Returns to the first Admin screen.

5.4 Switching Between Integrated and Standalone Mode

For terminals that have a built-in printer the terminal can be placed in standalone mode either temporarily or permanently.

- **To enter Non Integrated Mode Temporarily**: press ENTER (7018/7019) or # (2015) followed by 7 and enter the manager password (Default 999). The

terminal can then be used to process transactions manually. The terminal reverts to integrated mode after 30 seconds of inactivity.

- **To enter Non Integrated Mode Permanently**: Use the instructions in Appendix B below.

Temporary mode is recommended unless the POS system is likely to be down for a long period of time.

5.5 Settlement Cutover

Settlement cutover is activated from the POS. When performing a Settlement Cutover, Vault will also perform an additional function – it will print any declined Electronic Offline Vouchers (EOV). These may be required for accurate reconciliation of the bank transactions with the sales information from the POS.

Note: If the EFTPOS terminal is going to be relocated, decommissioned, repaired or replaced, please perform a settlement cutover prior to disconnecting to ensure any declined EOV receipts are printed.

5.6 Electronic Offline Voucher mode

The EFTPOS terminal may go into offline mode for various reasons. When in Offline mode, all transactions performed are defined as EOV (Electronic Offline Voucher) transactions, where the terminal will perform a series of risk management routines to determine the outcome of the transaction. If the terminal accepts the transaction, it will print the necessary EFTPOS receipt and store the transaction until such time as the transaction can be uploaded to Paymark.

Once back online the operator has the ability to manually upload the stored EOV transactions, but most likely, the terminal will automatically upload the transactions without the operator realising. When the terminal performs an automatic EOV upload, it cannot instruct the POS to print any declined EOV transactions as the POS will be performing other functions and will be not ready to receive any EFTPOS receipts. Therefore, the terminal will store the declined EOV receipts and print these when the POS operator / supervisor performs a settlement cutover.

5.7 Diagnostics

This section contains information about extracting diagnostic information from Vault solutions.

5.7.1 Obtain Vault Version Numbers

To determine the software versions of each component in a Vault solution use the instructions below:

Payment Application

On the terminal:

1. If in integrated mode, activate menus by pressing *ENTER* (7018/7019) or # (2015) then *7*; *Managers password (default 999)*
2. Scroll to and select **Utility**;
3. Scroll to **Terminal SWV**;
4. Select **Terminal SWV**;

Vault Applet

On the terminal:

1. If in integrated mode, activate menus by pressing *ENTER* (7018/7019) or # (2015) then *7*; *Managers password (default 999)*
2. Scroll to and select **Utility**;
3. Scroll to **Interface Config**;
4. Press **Interface Config**;
5. Scroll to **About**;
6. Press **About**;

Vault Adapter

On the POS:

1. Right click on the Vault Icon in the system tray;
2. Click **About Vault**;

5.7.2 Get Terminal IP Address

To get the IP Address of the terminal:

1. If in integrated mode, activate menus by pressing *ENTER* (7018/7019) or # (2015) then *7;*
2. Enter the manager password (default 999);
3. Select **Setup**;
4. Enter the manager password again (default 999);
5. Scroll and select **Comm Utils**;
6. Select **Terminal IP**;
7. Read IP Address from screen;

5.7.3 Vault Logs

If the help desk asks for the Vault logs you will find them in:

- **C:/ProgramData/Vault** (Windows Vista and Windows 7)
- **C:/Documents and Settings/All Users/Application Data/Vault** (Windows XP)

Just ZIP up the entire contents of the directory and send to VeriFone.

6 Appendix A – Manual Configuration

The following sections describe how to manually configure a VeriFone terminal to use Vault. This documentation applies only to terminals that have Vault enabled software loaded. This process should **only** be followed if downloading the configuration via VeriCentre has failed and the VeriFone help desk is not available.

6.1 One-piece Terminals and Administration

Vault can only be deployed on a single piece terminal. The terminal will normally be mounted in front of the customer and display the idle screen at all times. Once Vault has been enabled, access to the administration functions of the terminal is not possible without a password and the knowledge as to how to activate the administration menu.

6.1.1 The Manager Password

In order to access the administration menu when the idle screen is visible, you must press the green ENTER (7018/7019 software) or # (2015 software) button followed by the number 7 button (do not press the two buttons together). The terminal will then ask for the manager password (default 999);. You can then select the administration / configuration functions required. If you do not interact with the terminal for 30 seconds then the terminal will go back to the idle screen once again.

6.2 Recommended Configuration Process

The following steps should be followed when configuring a Vault terminal.

1. Change the acquirer (Paymark Merchant) settings.
2. Review / change the Communications Channel(s).
3. Set the IP address of the terminal.
4. Enable Vault.

Each of the steps above is described in detail below:

6.2.1 Entering the Acquirer Settings

In order to get the terminal to log on to Paymark's switch you must enter a merchant and terminal ID into the terminal. Instructions on how to do this follow:

1. If the administration menu is not active, activate it by pressing Enter (7018/7019) or # (2015) followed by 7 and then enter the manager password (default 999);.
2. Select SETUP.
3. Enter the manager password again (default 999); and then press the Green Enter Key.
4. Press the scroll button until EDIT ACQUIRER is shown.
5. Select EDIT ACQUIRER.
6. Select the appropriate Record, Record 1 unless multi merchant.

7. Select Terminal ID.
8. Type the Terminal ID and press the Green Enter Key. NOTE: The usual format for the Terminal ID is the last 6 digits of the Paymark Merchant Number followed by 01 for terminal 1, 02 for terminal 2, etc.
9. Select Merchant ID.
10. Type the Merchant ID and press the Green Enter Key. NOTE: The usual format for the Merchant ID is the 8 digit Paymark Merchant Number followed by 001 for terminal 1, 002 for terminal 2, etc.
11. Press the Red X Key.
12. Select Yes to Save Changes save changes.
13. Press the RED X Key a couple of times to return to the idle screen.

Special Notes
For Paymark 9 digit merchant numbers:

- The Merchant ID is usually set to 111 followed by the first 8 digits of the 9 digit Paymark merchant number. Example: 11112345678.

For any other formats, especially fuel merchants, contact Paymark for information.

6.2.2 Selecting the Communication Channels

There are only two Communication Channels that can be selected for use with Vault. These are IP-IP or IP. The default setting is IP-IP which allows both the primary and secondary Paymark IP addresses to be loaded. IP-IP is also used when a VEAC is installed.

- **IP-IP**: The primary IP address is used to transmit the transaction. If the primary IP channel suffers a failure, the terminal will use the secondary IP address. The terminal will remain on the secondary IP address until the configurable switching time has expired, after which it will return to the primary IP address. Use this setting if a VEAC is installed on the merchant's IP network, or an alternative IP address is available to communicate with Paymark
- **IP**: Only the primary IP address is used to transmit the transaction. If this channel suffers a failure, the transaction will fail. Use this setting if only one IP address is used.

To change the communication channel:

1. If the administration menu is not active, activate it by pressing ENTER (7018/7019) or # (2015) followed by 7 and then enter the manager password (default 999);.
2. Press the scroll button until **UTILITY** is shown.
3. Select **UTILITY.**
4. Press the scroll button until **COMM CHANNEL** is shown.
5. Select **COMM CHANNEL.**

6. Choose one of the options mentioned above. *If IP-IP is selected, please type in the switch time (in minutes) and press enter.*
7. The terminal will restart.

Notes:

- Vault is only able to communicate to Paymark with either IP or IP-IP options. Choosing the other options which are applicable only to standalone terminal installs will result in a loss of communication with the POS
- The default setting when deployed or downloaded is IP -IP.

6.2.3 Setting the IP Address of the Terminal

It is recommended a Vault terminal be assigned a fixed or static IP address. In order for the POS to communicate with the Vault terminal, the Vault Adaptor requires the IP address of the terminal. If DHCP is utilised, then there is an issue where if the terminal is restarted, it could be assigned a new IP address, thus the link between the POS and terminal will be lost. Therefore, the following parameters need to be configured:

1. The IP address assigned to the Vault EFTPOS terminal.
2. The subnet mask of the assigned terminal IP address.
3. The Gateway address.

Additionally, the following may be entered into the terminal:

1. The Primary DNS address.
2. The Secondary DNS address.

Note that the function used to change the IP address of the terminal is also used to change the addresses the payment application uses in order to communicate with Paymark. Both groups of settings must be configured at the same time. Follow the instructions below when configuring a terminal to use Vault.

ALL VAULT TERMINALS (excluding Wi-Fi)

1. If the administration menu is not active, activate it by pressing ENTER (7018/7019) or # (2015) followed by 7 and then enter the manager password (default 999);.
2. Press the scroll button until **UTILITY** is shown.
3. Press **UTILITY**.
4. Press the scroll button until **COMMS SETTINGS** is shown.
5. Press **COMMS SETTINGS.**
6. COMMS SETTINGS SELECT HOST ADDRESS TYPE is displayed.
7. Press **IP.**
8. ENTER HOST IP **117.120.34.110** is displayed.
9. This is the IP address of Paymark. Press the Green Enter Key if correct, otherwise type in new HOST IP address and press Green Enter Key.

10. ENTER SECONDARY IP **117.120.32.110** is displayed.
11. Press the Green Enter Key if correct, otherwise type in new SECONDARY IP address and press Green Enter Key. (Note: This will be the IP address of the VEAC if installed, or an alternative IP address to communicate with Paymark).
12. ENTER IP PORT **33876** is displayed.
13. Press the Green Enter Key if correct, otherwise type in new IP PORT number and press Green Enter Key.
14. USE SSL? Is displayed.
15. Press **NO.**
16. SELECT IP ADDRESS SETUP is displayed.
17. Press **FIXED** (unless using DHCP, then press DHCP. If DHCP is pressed, the terminal will restart).
18. ENTER TERMINAL IP ADDRESS is displayed.
19. Type in the new TERMINAL IP ADDRESS and press Green Enter Key, or press Green Enter Key if correct.
20. ENTER GATEWAY IP ADDRESS is displayed.
21. Type in the new GATEWAY ADDRESS (optional) and press Green Enter Key, or press Green Enter Key if correct.
22. ENTER SUBNET MASK is displayed.
23. Type in the new SUBNET MASK and press Green Enter Key, or press Green Enter Key if correct.
24. ENTER PRIMARY DNS is displayed.
25. Type in the new PRIMARY DNS (optional) and press Green Enter Key, or press Green Enter Key if correct.
26. ENTER SECONDARY DNS is displayed.
27. Type in the new SECONDARY DNS (optional) and press Green Enter Key, or press Green Enter Key if correct.
28. The terminal will restart and return to the idle screen.

Wi-Fi TERMINALS

1. If the administration menu is not active, activate it by pressing ENTER (7018/7019) or # (2015) followed by 7 and then enter the manager password (default 999);.
2. When the terminal is at the idle screen, press the scroll button until **UTILITY** is shown on the screen.
3. Select **UTILITY.**
4. Select **WI-FI SETTINGS.**
5. SELECT HOST ADDRESS TYPE is displayed.
6. Select IP.
7. ENTER HOST IP **117.120.34.110** is displayed.
8. Press the Green Enter Key if correct, otherwise type in a new HOST IP address and press green Enter key.
9. ENTER SECONDARY IP **117.120.32.110** is displayed.
10. Press the green Enter key if correct, otherwise type in a new SECONDARY IP address and press green Enter key.

11. ENTER IP PORT **33876** is displayed.
12. Press the green Enter key if correct, otherwise type in a new IP PORT number and press green Enter key.
13. USE SSL? Is displayed.
14. Select **NO.**
15. SELECT IP ADDRESS SETUP is displayed. Select **DHCP** or **FIXED**. If DHCP is selected go to step 21. If FIXED is selected go to Step 16.
16. ENTER TERMINAL IP ADDRESS is displayed. Type in the IP ADDRESS and press the green Enter key.
17. ENTER GATEWAY IP ADDRESS is displayed. Type in the GATEWAY IP ADDRESS and press the green Enter key.
18. ENTER SUBNET MASK is displayed. Type in the SUBNET MASK and press the green Enter key.
19. ENTER PRIMARY DNS will be displayed. If applicable type in the PRIMARY DNS and press the green Enter key.
20. ENTER SECONDARY DNS will be displayed. If applicable type in the SECONDARY DNS and press the green Enter key.
21. Enter SSID will be displayed. Type in the SSID and press the green Enter key.
22. Enter CHANNEL will be displayed. Type in the CHANNEL and press the green Enter key; Note: type in -1 to enable automatic selection of the channel.
23. Select ENCRYPTION will be displayed. Select the relevant encryption mode; None, WEP, WEP2, WPA, or WPA2. The encryption method will be determined by the merchant's Wireless Access Point configuration. If NONE is selected the terminal will reboot. If WEP or WEP2 were selected go to Step 23. If WPA or WPA2 were selected go to step 27.
24. Select NETWORK AUTHENTICATION is displayed. Select the relevant NETWORK AUTHENTICATION; Open or Shared. This will be determined by the merchant's Wireless Access Point configuration.
25. Enter INDEX KEY is displayed. Type in the relevant INDEX KEY. This will be determined by the merchant's Wireless Access Point configuration.
26. Enter WEP will be displayed. Enter the Access point's password into this field.
27. The terminal will reboot to apply the changes.
28. PLEASE SELECT ENCRYPTION is displayed with two choices. Select either TKIP (WPA) or AES-CCMP (WPA2).
29. ENTER PRE SHARED KEY is displayed. Type in the key as configured on the merchants Wireless Access Point.
30. The terminal will reboot to apply the changes.

6.2.4 Enabling Vault

To enable the Vault interface, the following steps should be followed:

1. If the administration menu is not active, activate it by pressing ENTER (7018/7019) or # (2015) followed by 7 and then enter the manager password (default 999);.
2. Press the scroll button until **UTILITY** is shown.
3. Select **UTILITY.**
4. Press the scroll button until **INTERFACE CONFIG** is shown.
5. Select **INTERFACE CONFIG.**
6. Select **INTERFACE.**
7. Point of Sale Present is prompted. Press **YES.**

   Note: This option may not be displayed depending on the hardware configuration. If this option is not present, the terminal will immediately display “Select Link Comms” (step 8) after pressing the Interface button (step 6).
8. At the Select Link Comms prompt choose **IP**.
9. Enter the ECP TCP port is displayed. This is the port number the terminal will listen for commands from the Vault Adaptor (default is **20001**). Type in the port number and press ENTER (or press enter if correct).
10. Enter POS IP address is displayed. This is the IP address of the POS (Default is **AUTO**). Type in the POS IP address or AUTO and press ENTER (or press enter if correct).
11. Enter the POS TCP port is displayed. This is the port number the Vault Adaptor will listen for data from the EFTPOS terminal. The default value displayed is **20005** but the Vault Adaptor will update this value automatically. There is no need to configure this value.
12. Select **POS** for the Display Mode.
13. The terminal will restart and be ready to accept transactions from the POS.

After restarting, the terminal will only display the Idle logo with the application locked down.

7 Appendix B – Standalone Mode

7.1 Switching to Standalone Mode

To disable the Vault interface and return the terminal to standalone mode, the following steps should be followed:

1. Press **ENTER** (7018/7019) or **#** (2015) followed by **7** and then enter the manager password (default 999);.
2. Press the scroll button until **UTILITY** is shown.
3. Select **UTILITY.**
4. Press the scroll button until **INTERFACE CONFIG** is shown.
5. Select **INTERFACE CONFIG.**
6. Select **INTERFACE.**
7. Point of Sale Present is prompted. Press **NO.** The terminal will return to the idle screen.

Note: If the "Point of Sale Present" prompt is not displayed, then continue with the following

- At the *Select Link Comms* prompt choose **IP**.
- Press the **enter** button 3 times to bypass the ECP TCP, POS IP, and POS TCP prompts.
- Select **TERMINAL** for the Display Mode.

If the terminal does not have a built in printer e.g a VX820 or Vx810 PIN PAD, the terminal will only display the Utility and Setup buttons.

7.2 Switching back to Integrated Mode

To enable the Vault interface, the following steps should be followed:

1. If the administration menu is not active, activate it by pressing ENTER (7018/7019) or # (2015) followed by 7 and then enter the manager password (default 999);.
2. Press the scroll button until **UTILITY** is shown.
3. Press **UTILITY.**
4. Press the scroll button until **INTERFACE CONFIG** is shown.
5. Press **INTERFACE CONFIG.**
6. Press **INTERFACE.**
7. Point of Sale Present is prompted. Press **YES**

   Note: This option may not be displayed depending on the hardware configuration. If this option is not present, the terminal will immediately display "Select Link Comms" (step 8) after pressing the Interface button (step 6).
8. At the Select Link Comms prompt choose **IP**.

9. “Enter the ECP TCP port” is displayed. This is the port number the terminal will listen for commands from the Vault Adaptor (default is **20001**). Type in the port number and press ENTER (or press enter if correct).
10. Enter POS IP address is displayed. This is the IP address of the POS (Default is **AUTO**). Type in the POS IP address or AUTO and press ENTER (or press enter if correct).
11. Enter the POS TCP port is displayed. This is the port number the Vault Adaptor will listen for data from the EFTPOS terminal. The default value displayed is **20005** but the Vault Adaptor will update this value automatically. There is no need to configure this value.
12. Select **POS** for the Display Mode.
13. The terminal will restart and be ready to accept transactions from the POS.

After restarting, the terminal will only display the default idle screen.

8 Appendix C - Operational Issues and Error Messages

This section covers the operation of Vault solutions from an administration and troubleshooting perspective. For the operation of Vault with respect to financial transactions the reader should consult the operation manual of the POS Application.

8.1 Error Messages

If a serious error condition occurs during operation, the Vault solution will display a notification in the system tray area. The possible error conditions are explained below:

- **Unable to Connect:** The POS Application was unable to connect to the terminal (terminal or PIN Pad). This may occur because the terminal is not connected or powered on. This may also occur if the terminal configuration has been changed. You can use the reconfigure function to redo the configuration if necessary.

- **Connection Interrupted:** The connection to the terminal was interrupted during operation. The most likely cause for this is the terminal was disconnected or powered down.

- **Terminal Unresponsive:** The terminal is not responding to the POS Application. It may occur if the terminal is faulty or if the network is not operational. To resolve this issue double-check the terminal connections, check the network, and then reboot the terminal.

- **Sign-On Failed:** The terminal is not allowing the POS Application to sign on. This may occur if the POS Application is not configured properly.

- **System Error:** This indicates an unexpected error condition that is not resolvable by the operator. Contact technical support to resolve the issue.

- **Printer Not Ready:** The configured printer is not ready to print. This message will normally suggest the reason as well as the solution for the problem.

8.2 Installation Trouble Shooting

- **The Vericentre Download Process Fails:** If the download process continually fails then the recommended course of action is to call the VeriFone help desk (0800 VERIFONE) and explain the issue. If it is outside of business hours then you can try to manually configure the terminal using the instructions in Appendix A above. Note that manual configuration still requires the installer to contact the VeriFone help desk as soon as possible since the configuration stored in VeriCentre will overwrite the manually supplied configuration in less

than 24 hours for Verix terminals and 7 days for Evolution terminals. The help desk will need to ensure that the current terminal configuration is reflected in the VeriCentre record for that terminal. Once the record is updated it is recommended that the download steps above in section 3.5 are performed again so that the terminal updates all settings needed to operate correctly.

- **No Vault Dialog Appears After activating Administration Menu Function:** If no dialog appears then it is likely that the POS Application has not been configured to use Vault as the preferred integrated payment provider. Please contact the POS Vendor to resolve the issue.

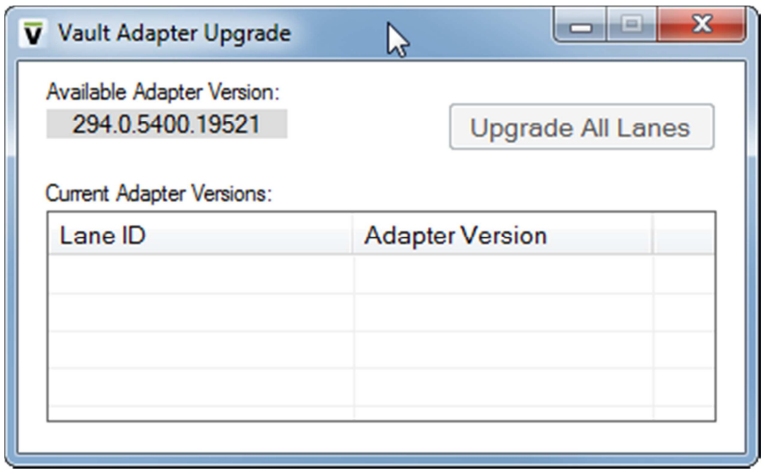
- **The Configuration Wizard is Unable to Find the Terminal:** If this happens then double check the following:
  - Is the terminal connected to the LAN and powered on?
  - Is the POS machine connected to the LAN?
  - Is the LAN operational? (switches powered on etc).
  - Is the terminal's IP address correct? (see diagnostics section below for information on getting the terminal's IP address).
  - Has the Windows firewall blocked connections to or from the terminal?
  - Has any other firewall blocked connections to or from the terminal?

- **All Vault options greyed out, POS 'Waiting on Terminal'**
  The POS may have been configured with the wrong IP address of the terminal, if unable to reconfigure lane close the POS and then go to:
  C:/ProgramData/Vault (Windows Vista and Windows 7);
  C:/Documents and Settings/All Users/Application Data/Vault (Win XP).
  There will be a folder named after your Vault session, delete this and then restart the POS, this will then prompt the configuration wizard.

- **The Logon Starts but the Transaction Times Out:** If this happens then one or more of the following may be true:
  - The site does not have access to the internet (try pinging google.com to see if internet is available);
  - The external firewall is not set up correctly;
  - The terminal has been set up with an incorrect terminal/merchant ID in VeriCentre;
  - The terminal has not been set up at Paymark;
  - The Paymark host is down (very unlikely).

- **The Configuration Wizard starts and indicates Downloading:** The terminal can deliver an updated adapter to the default version packaged with the POS. On a new install this can occur while running the wizard. Issues can occur if a local firewall blocks this update or after updating, the wizard fails to continue to the next step. See Section 2.5.4 for Internal Firewall options. If the wizard fails to continue restart the POS or call a Vault function and the wizard should continue. If the adapter update via the terminal fails, Paypedia contains an executable to manually update the adapter. Download the exe to the POS and

run. Once running select UPGRADE ALL LANES. The update will take seconds and can be confirmed by viewing an updated Adapter version against the Lane ID.



8.3 Known Operational Issues

Below are some known operational issues.

8.3.1 Vault Window is not in the foreground

This sometimes occurs because Windows Xp, 7 and 8.x have a feature that stops background applications from popping up windows and taking the input focus. Vault includes code that prevents this from happening but this can be defeated by POS solutions that open Vault sessions in a process that is not the POS Application itself. The anti-popup feature in Windows can be disabled by setting the HKCU\Control Panel\Desktop\ForegroundLockTimeout registry key to 0 instead of the default value of 200000.

Note: This will only change the setting for the current logged on user. If you log on as another user you will need to repeat the above for that user.

8.3.2 Init RKI

To complete a terminals installation it requires an INIT RKI to be performed before a logon or transaction can be initiated. With software version 7018 this needs to be performed on the terminal and not via the POS (Administration Menu). This is due to the lengthy key exchanges which results in the terminal taking too long to respond to the POS, which will cause the Vault Adaptor to display a “Power / Link Failure” and the final result of the RKI (Accepted or Please Try Again) will be missed. The solution with this software version is to perform the Init RKI on the terminal.

With software version 7019 this is resolved and the Init RKI should be performed via the Eftpos Admin menu prior to logging on for the first time.

8.3.3 Sometimes 'port-in-use' Errors Occur in Operation

This can happen because static port configuration has been enabled to make firewall configuration easier (see Firewall Considerations above). The workaround is to retry the operation or to modify the POS Application to make sure it waits briefly before opening a session.

8.3.4 Minor Issues

There are a few known issues with Vault which may be observed. These are all minor and in no way affect the financial integrity or operation of the EFTPOS terminal.

1. The (Paymark) Logo is blinking continuously when idle.

2. During a power failure recovery, the terminal may have a blank screen for some time before it displays "please wait".

3. If the cancel key is pressed while displaying the transaction result on the terminal, the application refreshes the screen but the top line has remains of the transaction type for few moments until the date / time is refreshed.

4. If the terminal has been disconnected from the IP network or not configured, the Vault Adaptor may take some time before it reports a connection problem.

5. Vault cannot be used with any value added applications (Epay, Ezi-Pay) unless these applications are supported via the POS application which will request Vault to perform a card read on behalf of the POS and to pass the track 2 data from the card to the POS application for processing to epay or Ezi-Pay host

6. After downloading software from the VeriCentre, the terminal's screen will be blank for up to one minute before decompressing the files.

7. If the VEAC Reg applet has been installed, it can only be executed from the VEAC menu when first powered up and before the payment application automatically executes.

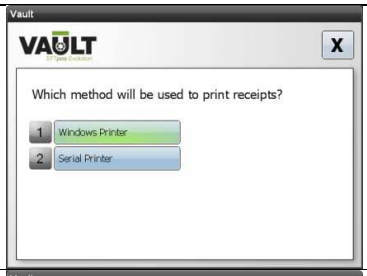
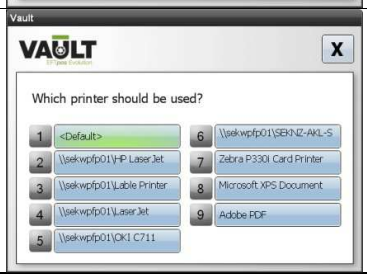
8. REMOVE CARD with an OK button. An intermittent issue may occur where Vault will display "Remove Card" with an OK button at the end of a transaction instead of the result of the transaction.

9. PROCESSING NOW with an OK button. This issue occurs with an Analysed Purchase transaction where the cardholder has entered their PIN incorrectly. Vault will allow the cardholder to re-enter their PIN but if the card holder (or operator) presses cancel on either the terminal or Vault window, Vault will display "Processing Now" with an OK button instead of "Trans. Cancelled".

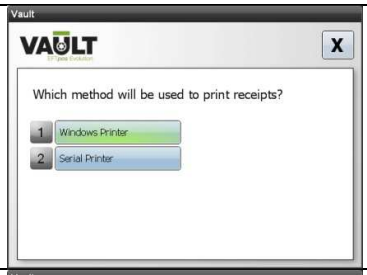
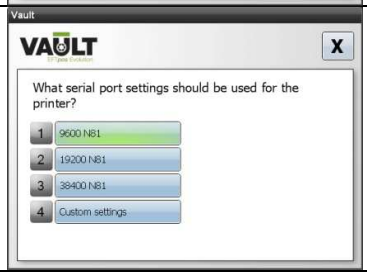
9 Appendix D – Printer Configuration

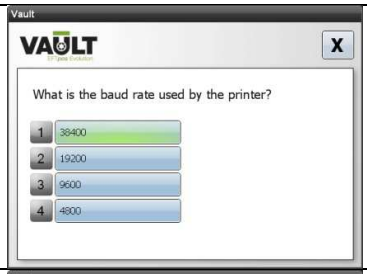
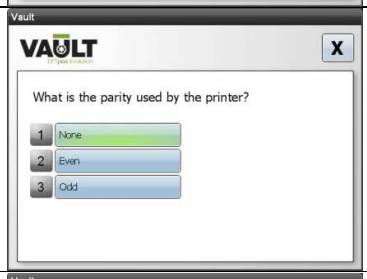
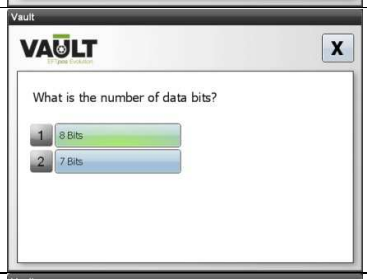
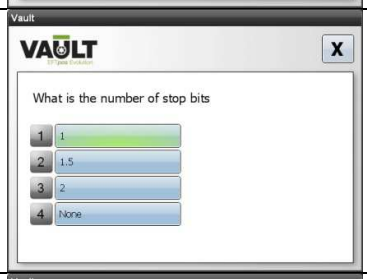
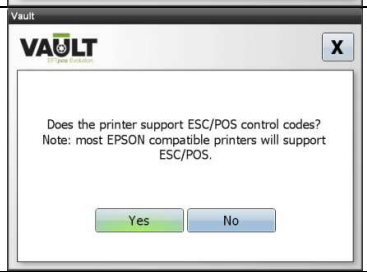
This section covers the necessary steps to manually configure a printer where POS printing is not the default.

9.1 Windows Printing Setup

Configure Windows Printer		Select Windows Printer
		Choose Printer

9.2 Serial Printing Setup

Configure Serial Printer		Select Serial Printer
		Choose required setting

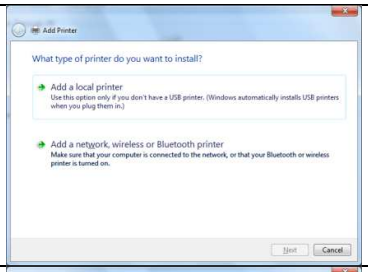
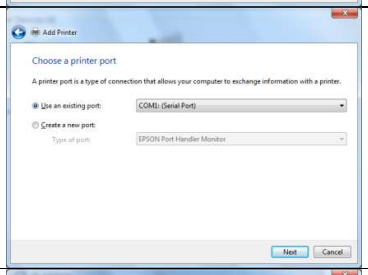
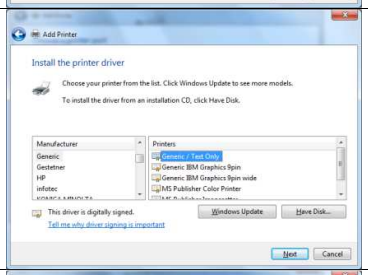
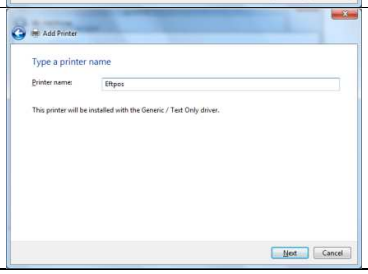
		Choose required setting
		Choose required setting
		Choose required setting
		Choose required setting
		Choose required setting
		Choose required setting

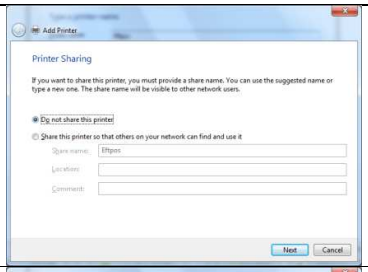
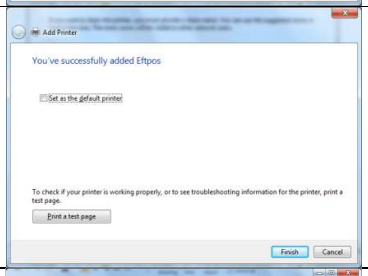
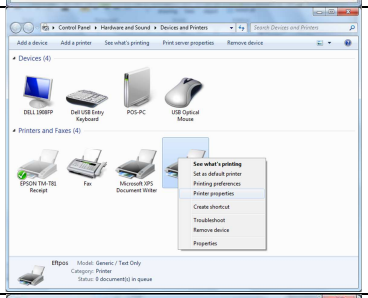
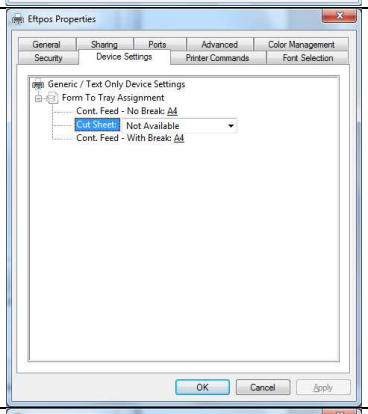
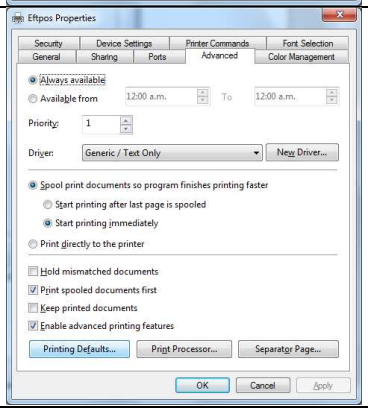
9.3 Windows Settings for Vault controlled printing

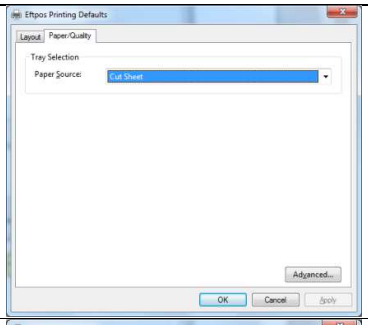
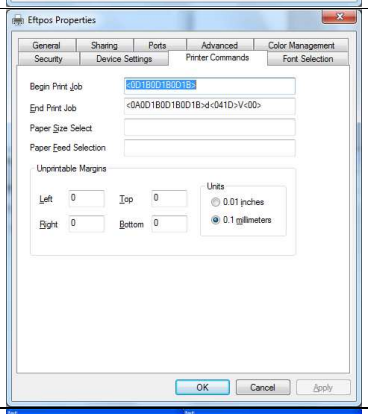
Often when using Vault controlled printing the initial receipts that print out are not aligned, fed sufficiently, or cut off after printing. If the POS is printing its receipts on the same printer then adding the necessary commands into the printer setup to sort these issues out is often not possible as they will be in conflict with each other.

Where possible we recommend setting up a Generic Text printer with the below settings applied. This has proved successful in the scenarios we have encountered.

On the POS open PRINTERS and select ADD PRINTER

Configure Vault Printer		Select ADD A LOCAL PRINTER
		Select the desired port under USE AN EXISTING PORT
		Scroll down to GENERIC and select GENERIC / TEXT ONLY and select NEXT
		Give the printer a name. E.G EFTPOS and select NEXT

		Select DO NOT SHARE THIS PRINTER and then NEXT unless you are looking to print the eftpos receipts from multiple lanes on this printer
		Untick SET AS THE DEFAULT PRINTER and select FINISH
		Right click the new printer and select PRINTER PROPERTIES
		Select the DEVICE SETTINGS tab and change CUT SHEET to NOT AVAILABLE and select APPLY
		Select the ADVANCED tab and select PRINTING DEFAULTS

		Select the PAPER/QUALITY tab and select CUT SHEET and then APPLY. Click OK to close
		Select the PRINTER COMMANDS tab and enter in the below commands: BEGIN PRINT JOB: <0D1B0D1B0D1B> END PRINT JOB: <0A0D1B0D1B0D1B>d<041D>V<00> Click APPLY and then OK
		Reconfigure the Vault lane and select WINDOWS PRINTER and the EFTPOS printer you just created. If requested for MARGIN settings set these to 0mm

10 Appendix E – Uninstall Previous POS

Please make sure that you have removed/uninstalled all other integration software (e.g PCEFTPOS or DPS) from the computer you are planning to install on. In order to learn how to uninstall an application from your PC please organise with the software provider.

NB: We recommend that you only remove/uninstall once Vault is working. It is good practice to keep the previous system as a backup just in case there are complications with the Vault install.