Microsoft Dynamics POS 2009
Implementation Guide for PCI Compliance

February, 2009

Microsoft Dynamics

Contents

Introduction

Welcome to the Microsoft Dynamics® POS 2009 Implementation Guide for PCI Compliance. The requirements in this guide **must** be followed in order to implement Microsoft Dynamics POS 2009 in a manner that is compliant with the Payment Card Industry (PCI) Data Security Standard version 1.2.

The requirements in this guide represent best practices that should be implemented even if you are not required to comply with PCI Data Security Standard.

This guide is intended for Microsoft Certified Partners who are deploying Microsoft Dynamics POS 2009 in a retail organization where electronic credit card and debit card payments are accepted and where Microsoft Dynamics POS is used as the payment application. As a payment application, Microsoft Dynamics POS is subject to the PCI Payment Application Data Security Standard (PA-DSS); the contents of this guide reflect that standard.

IMPORTANT

Some of the steps in this guide are technical and should be completed only by a Microsoft Certified Partner. Implementation by anyone other than a Microsoft Certified Partner could be considered a red flag by PCI Security Standards Council assessors and could compromise the security of both store and cardholder information.

The requirements of the *PCI Data Security Standard* are identified in the context of the text; for example:

> "All Microsoft Dynamics POS transmissions of cardholder data, whether over a private or public network, are secured by the use of SSL. This helps to satisfy Requirement 4.1 of the PCI Data Security Standard."

The requirements of the *PCI Payment Application Data Security Standard* are identified by highlighted section numbers in headings; for example:

> "Data transmissions 12.1, 12.2"

Get the latest release of this guide

This guide is updated annually and whenever a service pack or hotfix for Microsoft Dynamics POS is released. To obtain the most up-to-date copy of this guide and view the version history (if any), visit this site:
http://go.microsoft.com/fwlink/?LinkID=134597&clcid=0x409

For more information

To read the full text of the PCI Data Security Standard or the PCI Payment Application Data Security Standard, visit http://www.pcisecuritystandards.org.

Part 1: Installing the software

To implement Microsoft Dynamics POS 2009 and Microsoft SQL Server® in a manner that is PCI compliant, follow the instructions below for the release of SQL Server that will be used by the store.

Terms used in this guide:

- The *standard installation* of Microsoft Dynamics POS includes SQL Server Express 2008. Installing SQL Server separately is not required.
- For the purposes of this guide, Standard, Enterprise, and Developer Editions of SQL Server 2005 and SQL Server 2008 are considered *full editions of SQL Server*.

IMPORTANT

- For maximum security, Microsoft Dynamics POS must be installed in the Program Files folder or a location with similar access-control protections.
- For simplicity and security reasons, Microsoft recommends using the standard installation of Microsoft Dynamics POS 2009 whenever possible, even if a full edition of SQL Server is available. That way, SQL Server Express 2008 is installed alongside any existing edition of SQL Server, and PCI-compliant security settings are implemented automatically on the default named instance, MSPOSInstance.
- If the customer is already running MSPOSInstance on a full edition of SQL Server 2005, the built-in SQL Server installation must be skipped by using the "skipsql" installation option described in "Installation using a full edition of SQL Server." Otherwise, the standard installation will fail due to the instance name conflict when Setup attempts to upgrade the instance to SQL Server 2008.
- PCI Data Security Standard Requirements 8.5.8 through 8.5.15 specify that default administrative accounts for payment application logins (for example, the "sa" account for payment application access to the database) must not be used. In addition, secure authentication must be assigned to default accounts (even if they won't be used), and then the accounts must be disabled or not used. In any event, secure authentication should be assigned to the payment application and systems whenever possible.

  The standard installation of Microsoft Dynamics POS provides these security measures by default. Any attempt to change these "out of the box" installation settings for unique user IDs and secure authentication will result in noncompliance with the PCI Data Security Standard.

  The procedures below in "Installation using a full edition of SQL Server" provide step-by-step instructions for implementing these measures in that situation.

Standard installation using the included SQL Server Express 2008

If the store does not have a full edition of SQL Server, or if the store's full edition of SQL Server will not be used with Microsoft Dynamics POS, install Microsoft Dynamics POS according to the instructions in *Getting Started*, included as a .pdf file with Microsoft Dynamics POS.

Installation using a full edition of SQL Server

To be PCI compliant when you use Microsoft Dynamics POS with a full edition of SQL Server, you must change some SQL Server settings. Once that is done, you can install Microsoft Dynamics POS and configure it to use the instance that you specify.

IMPORTANT

- You must use a new instance for Microsoft Dynamics POS. Use of an existing instance could compromise PCI compliance.
- You must complete **all** of the following procedures on the SQL Server computer. In some cases, you might discover that the desired settings are already in place, but you need to confirm this.

To select the service account

1. In SQL Server Configuration Manager, click **SQL Server Services**.
2. Right-click the correct instance, and then click **Properties**.
3. In the **Built-in account** box, select **Network Service**, and then click **OK**.

To switch to mixed-mode server authentication

1. In SQL Server Management Studio, open the Object Explorer, right-click the instance, and then click **Properties**.
2. On the Security page, under Server authentication, select SQL Server and Windows Authentication mode, and then click OK.

To manage SQL Server without using the "sa" account

Note

Completing this procedure helps to satisfy Requirement 2 of the PCI Data Security Standard.

1. Open SQL Server Management Studio Object Explorer, and then expand the folder for the correct instance.
2. Set up a new administrator account:
   a. Right-click the **Security** folder, point to **New**, and then click **Login**.
   b. On the **General** page, type a unique login name, select **SQL Server authentication**, and provide a strong password.
   c. On the **Server Roles** tab, select **sysadmin**, and then click **OK**.
3. Disable the "sa" account by expanding the **Security** folder, expanding the **Logins** folder, and then completing these steps:
   a. Right-click the account name, and then click **Properties**.
   b. Click the **Status** page, select **Disabled**, and then click **OK**.

To enable the TCP/IP network protocol and start listening to the POS port

1. In SQL Server Configuration Manager, expand SQL Server Network Configuration.
2. Click Protocols for <instance name>.
3. Right-click **Shared memory**, and then click **Enable**.
4. Right-click **TCP/IP**, and then click **Enable**.
5. Right-click **TCP/IP**, and then click **Properties**.
6. On the **IP Addresses** tab, under **IPAll**, set **TCP Port** to 1976, and then click **OK**.

Note

If you have other protocols enabled, you must disable them.

To force encryption of database communications

1. In SQL Server Configuration Manager, expand SQL Server Network Configuration.
2. Right-click the protocols for the Microsoft Dynamics POS instance, and then click **Properties**.
3. On the **Flags** tab, select **Yes** for the **Force Encryption** option, and then click **OK**.

Note

When the Force Encryption option for the database engine is set to Yes, all client/server communication is encrypted and clients that cannot support encryption are denied access.

To restart the SQL server and put your changes into effect

1. In SQL Server Configuration Manager, click SQL Server Services.
2. Right-click SQL Server (<instance name>), and then click Restart.

To install Microsoft Dynamics POS 2009 without SQL Server Express

Note

You must install Microsoft Dynamics POS 2009 on the computer where SQL Server is installed.

1. On the download page for Microsoft Dynamics POS 2009, right-click the download link, click **Save Target As**, and then save the installation package to the SQL Server computer.
2. Open the Command Prompt.
   - If you are running Windows Vista or Windows Server 2008, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
   - If you are running Windows XP or POS Ready 2009, click **Start**, click **Run**, type "cmd" without quotes, and then click **OK**.

3 Type this text to extract the contents of the installation package, replacing the question marks with the last four characters of the package file name:

```
MSDPOS2009_????.exe /x
```

4 Press ENTER, type or browse to the location where you want to extract the installation files, and then click **OK**.

5 After the files are extracted, return to the Command Prompt, and then type this text, replacing <path> with the location of the installation files:

```
<path>\setup.exe skipsql=Yes
```

6 Press ENTER, and then follow the instructions in the Installation Wizard.

7 If you are using a full edition of SQL Server 2005, install additional components by completing these steps:

   a Use Windows Explorer to view the temporary location of the installation files, and then double-click the **SMO** folder.

   b Double-click **SQLSysClrTypes.msi** and wait for the installation to complete.

   c Double-click **SharedManagementObjects.msi** and wait for the installation to complete.

8 Optionally, delete the temporary folder that contains the installation files.

Open the server firewall to Microsoft Dynamics POS communications

If the store has more than one computer that is running Microsoft Dynamics POS, the following ports must be opened in the firewall to facilitate database communication:

- The TCP port that SQL Server is listening on. For MSPOSInstance, the default port is 1976. For other SQL Server installations, the default port is 1433.
- TCP ports 139 and 445.
- UDP ports 137 and 138.

The ports need to be opened only on the database computer.

Instructions are provided below for opening these ports in Windows Firewall. If you are using a third-party firewall, consult the firewall documentation for information about opening the firewall.

Note

- When you enable File and Printer Sharing in Windows, Windows Firewall is automatically opened to ports 137, 138, 139, and 445.
- In most cases, the SQL Server listening port should be opened for the local subnet only. If machines on other subnets need access to the database, you will need to make additional change to your firewall settings. For Windows Firewall, you can change the scope of the selected exception by clicking **Edit** and then **Change scope**.

To open Windows Firewall on Windows Vista or Windows Server 2008

1. Log on to the main computer as a Windows Administrator.
2. Click **Start**, and then click **Control Panel**.
3. If needed, switch to Classic View, and then double-click **Network and Sharing Center**.
4. Turn on **Network discovery**, **File sharing**, and **Printer sharing**. For each, click the down-arrow at right, select the **Turn on...** option, and then click **Apply**.
5. Click the **Back** button to return to **Control Panel**, and then double-click **Windows Firewall**.
6. Click Allow a program through Windows Firewall.
7. On the **Exceptions** tab, click **Add port**.
8. In the **Name** box, type a name for the port that SQL Server is listening on, such as "POS listening port".
9. In the **Port** box, type the port number.
10. Make sure **TCP** is selected, and then click **OK**.
11. Verify that the **File and Printer Sharing** check box is selected, and then click **OK**.

To open Windows Firewall on Windows XP or POS Ready 2009

1. Log on to the main computer as a Windows Administrator.
2. On the **Start** menu, click **Control Panel**.
3. If needed, switch to Classic View, and then double-click **Windows Firewall**.
4. On the **Exceptions** tab, click **Add Port**.
5. In the **Name** box, type a name for the port that SQL Server is listening on, such as "POS listening port".
6. In the **Port** box, type the port number.
7. Make sure **TCP** is selected, and then click **OK**.
8. Select the **File and Printer Sharing** check box, and then click **OK**.

To configure Microsoft Dynamics POS to use the correct instance

1. In Windows Explorer, navigate to the folder where Microsoft Dynamics POS is installed.
2. Use Notepad or another text editor to open the **RMSSecured.config** file.
3. Change the <instancename> values for both the production and offline databases to the correct instance name.
4. Save and close the file.
5. Start Microsoft Dynamics POS to create the store database and set up the store.

Note

When you set up register computers, you will have the opportunity during installation of Microsoft Dynamics POS to specify the server and instance where the database is located.

Maintain the security of the SQL Server

You must install security hotfixes and service packs as soon as they become available. For best results, turn on Automatic Updates.

Part 2: Other setup requirements

You must complete **all** of the procedures in this section.

Run the script to enable SQL trace logging

To monitor access to payment-related information in the store database, you must enable SQL trace logging by using the POSTrace.sql file, which is included in the Microsoft Dynamics POS installation files in the installation folder (C:\Program Files\Microsoft Dynamics – Point of Sale by default). This helps to satisfy requirements 10.2 and 10.3 of the PCI Data Security Standard. Failing to enable logging will result in noncompliance with the PCI Data Security Standard.

To enable SQL trace logging

1. Copy POSTrace.sql to the computer where the store database is located.
2. Open Command Prompt as an Administrator.
   - If you are running Windows XP or POS Ready 2009, you must log on as an Administrator. Next, click **Start**, click **Run**, type "cmd" without quotes, and then click **OK**.
   - If you are running Windows Vista or Windows Server 2008, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
3. Type this command, replacing "C:\<path>" with the actual location of the .sql file and <instance> with the name of the correct instance:

   ```
   sqlcmd -S .\<instance> -i "C:\<path>\POSTrace.sql"
   ```

   For example, using the default SQL Server instance, the command would be:

   ```
   sqlcmd -S . -i "C:\Program Files\Microsoft Dynamics - Point
   of Sale\POSTrace.sql"
   ```

   Or, using the msposinstance, the command would be:

   ```
   sqlcmd -S .\msposinstance -i "C:\Program Files\Microsoft
   Dynamics - Point of Sale\POSTrace.sql"
   ```

4. Press ENTER.

   When the operation is complete, you should see lines of text on the screen similar to these:

   ```
   INFO: Successfully created the trace with ID 3
   ```

   ```
   INFO: Trace file 2 path is C:\Program Files\Microsoft SQL
   Server\MSSQL.1\MSSQL\LOG\pos_trace_pmt_2008-08-05T131824373
   ```

To verify that SQL trace logging is enabled

1. Look at the size of the log file.
2. Process some credit card transactions in Microsoft Dynamics POS 2009.

3 Confirm that the size of the log file increased. It might take a number of transactions to cause a change in the file size.

Note

- As shown on the previous page, the log files will be in the Log directory for the instance.
- SQL trace log files have a maximum file size of 100MB. When the size of a log file exceeds this limit, a new log file is created using a date-based numbering scheme.
- For information about viewing and managing log files, see Part 5, "Audit logging," later in this guide.

Set up auditing of file access, object access, and audit-policy changes

To audit changes made to the computer's audit policy as well as access to log files and system objects, complete both of the following procedures *on all computers where Microsoft Dynamics POS is installed*. This helps to satisfy requirements 10.2 and 10.3 of the PCI Data Security Standard. Failing to enable logging will result in noncompliance with the PCI Data Security Standard.

For information about viewing and managing log files, see Part 5, "Audit logging," later in this guide.

To enable auditing of file access, object access, and audit-policy changes

1 Click **Start**, and then click **Control Panel**.

2 If needed, switch to Classic View.

3 Double-click **Administrative Tools**, and then double-click **Local Security Policy**.

4 Expand the **Local Policies** folder, and then click **Audit Policy**.

5 Double-click **Audit account logon events**, select both the **Success** and **Failure** check boxes, and then click **OK**.

6 Double-click **Audit account management**, select both the **Success** and **Failure** check boxes, and then click **OK**.

7 Double-click **Audit object access**, select both the **Success** and **Failure** check boxes, and then click **OK**.

8 Double-click **Audit policy change**, select both the **Success** and **Failure** check boxes, and then click **OK**.

Note

If you are implementing Microsoft Dynamics POS into a domain environment, these policies must be implemented via a group policy. For assistance, contact the network administrator.

To start auditing access to system folders and files

The steps for turning on folder and file auditing are provided below. The folders you must audit vary by operating system.

For Windows Vista or Windows Server 2008:

- C:\Windows\System32\winevt\Logs
- The folder where Microsoft Dynamics POS is installed (C:\Program Files\Microsoft Dynamics – Point of Sale by default) . See note in step 8, below.
- The SQL data directory (C:\Program Files\Microsoft SQL Server\MSSQL10.MSPOSINSTANCE\Log by default)
- C:\ProgramData\Microsoft\Microsoft Dynamics POS\Logs

For Windows XP and POS Ready 2009:

- C:\Windows\System32\config
- The folder where Microsoft Dynamics POS is installed (C:\Program Files\Microsoft Dynamics – Point of Sale by default). See note in step 8, below.
- The SQL data directory (C:\Program Files\Microsoft SQL Server\MSSQL10.MSPOSINSTANCE\Log by default)
- C:\Documents and Settings\All Users\Application Data\Microsoft\Microsoft Dynamics POS\Logs

1. In Windows Explorer, right-click the folder name, and then click **Properties**.
2. On the **Security** tab, select the **Everyone** group, and then click **Advanced**.
3. On the **Auditing** tab, if a security message appears, click **Continue**.
4. Click **Add**.
5. In the **Enter the object name to select** box, type "Everyone" without quotes, and then click **Check Names**.
6. If the name is valid, click **OK**.
7. In the **Apply onto** box, make sure that **This folder, subfolders and files** is selected.
8. In the **Access** list, select both the **Successful** and **Failed** check boxes for the following privileges, and then click **OK.**
    - Create files/write data
    - Create folders/append data
    - Delete subfolders and files
    - Delete
    - Change permissions
    - Read permissions

Note

Do not enable Read permissions for the folder where Microsoft Dynamics POS is installed (C:\Program Files\Microsoft Dynamics – Point of Sale by default)

9 Select the **Replace all existing inheritable auditing entries...** check box, and then click **OK**.

Prepare for monitoring the event logs

The event logging capabilities built into Windows will help you achieve compliance with Requirements 10.2 and 10.3 of the PCI Data Security Standard. Complete the following procedure on all computers where Microsoft Dynamics POS is installed.

To configure the retention period for event logs

1 Click **Start**, and then click **Control Panel**.

2 If needed, switch to Classic View.

3 Double-click **Administrative Tools**, and then double-click **Event Viewer**.

4 If available, expand the **Windows Logs** folder, right-click **Security**, and then click **Properties**.

5 In the **Maximum log size** box, type "102400" without quotes.

6 Select **Overwrite events as needed**, and then click **OK**.

Set up the password policy for the store

Requirement 8 of the PCI Data Security Standard sets out specific password and user account regulations. To comply with these requirements, complete the following procedures on all computers where Microsoft Dynamics POS is installed.

Note

See the IMPORTANT notes on page 3 about installation and administrative accounts.

To set local password and other account security policies

1 Click **Start**, and then click **Control Panel**.

2 If needed, switch to Classic View.

3 Double-click **Administrative Tools**, and then double-click **Local Security Policy**.

4 Expand the **Account Policies** folder, and then change the settings under **Password Policy** and **Account Lockout Policy** to meet the following PCI Data Security Standard minimum requirements:

Policy	Security Setting
Enforce password history	4 passwords remembered
Maximum password age	90 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Account lockout duration	30 minutes
Account lockout threshold	6 invalid logon attempts

Note

- To satisfy PCI requirement 8.5.8, do not use group, shared, or generic accounts and passwords.

  8.5.8.a – For a sample of system components, critical servers, and wireless access points, examine user ID lists to verify the following:

  - Generic user IDs and accounts are disabled or removed
  - Shared user IDs for system administration activities and other critical functions do not exist
  - Shared and generic user IDs are not used to administer wireless LANs and devices

  8.5.8.b – Examine password policies and procedures to verify that group and shared passwords are explicitly prohibited.

- These policies represent the minimum requirements of Requirements 8.5.9 through 8.5.14 of the PCI Data Security Standard. More stringent settings can be used.
- If you are implementing Microsoft Dynamics POS into a domain environment, these policies must be implemented via a group policy. For assistance, contact the network administrator.

To force users to log on again when the computer has been idle

1. On the **Start** menu, click **Run**, type "mmc" without quotes, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then, if you are running Windows XP, click **Add**.
3. Select **Group Policy Object Editor**, click **Add**, click **Finish**, and then click **Close** or **OK**.
4. Expand Local Computer Policy, expand User Configuration, expand Administrative Templates, expand Control Panel, and then click Display.
5. Double-click **Screen Saver executable name**, select **Enabled**, type the name of a screen saver (.scr) file, and then click **OK**. These files are located in the C:\Windows\System32 folder.

6 Double-click **Password protect the screen saver**, select **Enabled**, and then click **OK**.

7 Double-click **Screen Saver timeout**, select **Enabled**, type "900" or less, and then click **OK**.

Note

Completing this procedure on each computer in the store helps to satisfy Requirement 8.5.15 of the PCI Data Security Standard.

Turn off System Restore

System Restore is a Windows feature designed to help you restore your computer's system files to an earlier point in time. The restore points saved by this feature are not considered secure by the PCI Security Standards Council.

To turn off System Restore on Windows Vista or Windows Server 2008

1 On the **Start** menu, right-click **Computer**, and then click **Properties**.

2 Click System protection.

3 Clear the check box for the C: drive, click **Turn System Restore Off**, and then click **OK**.

To turn off System Restore on Windows XP or POS Ready 2009

1 On the **Start** menu, right-click **My Computer**, and then click **Properties**.

2 On the **System Restore** tab, select the **Turn off System Restore** check box, and then click **OK**.

Set up payment processing and payment methods

Once the auditing and other security measures are in place, the store can begin accepting card payments. To do so, the following steps must be completed:

- The store must contract with a bank for a merchant account.
- The payment processing feature in Microsoft Dynamics POS must be turned on.
- One or more payment methods in Microsoft Dynamics POS must be set up to use payment processing.

Note

These steps are not specifically required for PCI compliance. However, if these steps are skipped, the store will not be able to use Microsoft Dynamics POS to process payments that are subject to the PCI Data Security Standard.

To obtain a merchant account

- The store owner should contact an acquiring bank to obtain a merchant account and inform the bank that Microsoft Dynamics POS is the payment application being used.

  The bank will provide merchant account and payment processor information.

To turn on payment processing in Microsoft Dynamics POS

1 If the store will be using an add-in from a third-party provider, install the add-in according to the provider.

IMPORTANT

If a third-party add-in is being used for payment processing, confirm with the add-in provider that the add-in has been certified PCI compliant.

2 In Microsoft Dynamics POS, switch to Manager View.

3 On the **Settings** menu, point to **Store Settings**, and then click **Options**.

4 On the **Payment** tab, in the **Available Services** box, select the appropriate payment processor, and then click **Setup**.

5 Using the information provided by the bank, type in the merchant account information, and then click **OK**.

6 Repeat Steps 4 and 5 for any other payment processors.

To set up payment methods in Microsoft Dynamics POS to use payment processing

1 On the **Settings** menu, point to **Store Settings**, and then click **Payment Methods**.

2 Click **New** to create a new credit card or debit card payment method, or double-click an existing credit card payment method.

3 In the **Format** box, select **Credit card**.

4 Enter or change basic settings for the payment method as desired, and then click **Advanced**.

5 Select the **Verify using this payment processing service** check box, select the appropriate payment processor from the list, enter other settings as desired, and then click **OK**.

6 Click **Save and Close**.

7 Repeat this procedure for any other payment methods that will be used to process payments.

For more information about payment processing and payment methods in Microsoft Dynamics POS, see “About payment processing” and “About payment methods” in Manager View Help.

For more information about the settings in the Options dialog box, the Payment Method window, or the Advanced Options dialog boxes, click the Help button in the dialog box or window.

Part 3: Features that facilitate PCI compliance

In this part, we'll discuss some of the features in Microsoft Dynamics POS that facilitate merchant compliance with the PCI Data Security Standard.

User names, passwords, and authentication 3.1, 3.2

Microsoft Dynamics POS does not provide any default accounts or passwords. Instead, a unique user name and password is required for each user, including the user who sets up the software. Microsoft Dynamics POS user accounts are securely authenticated through Windows and are subject to the same security policies as other Windows users. These features help to satisfy Requirements 2 and 8 of the PCI Data Security Standard.

Note

Do not allow employees to share employee IDs or passwords. Doing so will result in non-compliance with the PCI Data Security Standard.

To set up a new employee account

1. Open Microsoft Dynamics POS, and then switch to Manager View.
2. On the **People** menu, click **Employees**, and then click **New**.
3. Type in the employee's name, unique employee ID, and password.
4. Click **OK**.

For more information about the settings in this window, click the Help button. 

Tip

In order to comply with PCI Data Security Standard Requirements 8.5.8 through 8.5.15, you must set up password and account lockout policies in Windows, as described in "Set up the password policy for the organization" in Part 2, "Other setup requirements," earlier in this guide.

IMPORTANT

You must also use a "least privilege" approach for the user accounts that store employees use to log on to Windows itself. According to Requirement 8.1 of the PCI Data Security Standard, each employee must have his or her own logon account. While the store owner or trusted management personnel will need to have Administrator privileges on each computer in the store, employee logon accounts must belong to the Standard User group or another group that does not have Administrator privileges.

On Windows Vista, Microsoft Dynamics POS should never be run as an Administrator. On Windows XP, Microsoft Dynamics POS should be run as an Administrator only in those limited circumstances when it is required, such as when creating a new employee or performing certain database operations.

Data storage and deletion

Several of the requirements in the PCI Data Security Standard relate to protecting sensitive cardholder data. These requirements call for the safe storage, encryption, and removal of cardholder information, such as magnetic stripe data, card validation codes and values, PINs, and PIN blocks. In particular, Requirements 1.3 and 1.3.4 of the standard prohibit storing cardholder data on servers that are connected to the Internet; the database server cannot also be a Web server. **9.1**

Microsoft Dynamics POS helps merchants comply with the PCI Data Security Standard regarding data storage and retention in the following ways:

- Prior to settlement, cardholder information is encrypted in the store database and cannot be viewed. After settlement, except as noted below, cardholder data is securely deleted from the database tables where it was stored[1], so no periodic purging is necessary. This helps to satisfy Requirement 3.1 of the PCI Data Security Standard. **2.1**
- Encrypted card numbers in the database are truncated after settlement so that only the last four digits remain. Card numbers on receipts (both printed and journaled) are always truncated.
- The previous release of the software did not retain sensitive authentication data, so removal of that historical data is not necessary. This helps to satisfy Requirement 3.2 of the PCI Data Security Standard. **1.1.4**
- After upgrading to Microsoft Dynamics POS from Microsoft Dynamics – Point of Sale, the program's Query Tool can be used to delete the old private key from the database. This helps to satisfy Requirement 3.6 of the PCI Data Security Standard. **2.7**
- A tool for resetting the encryption key is built into the software. The previous encryption key is removed and replaced by the new key. A reset of the encryption key must be performed annually and whenever a security breach is suspected. This also helps to satisfy Requirement 3.6 of the PCI Data Security Standard.

To delete the old private key

Note

You must log on to Microsoft Dynamics POS as an employee whose role allows performing SQL queries. This employee role setting is: **Perform other database operations**.

1 Start Microsoft Dynamics POS, and then switch to Manager View.

2 On the **Tools** menu, point to **Database**, and then click **Query Tool**.

[1] The PaymentAuthorization (PAN), PaymentAuthorizationConfig (public key), and PaymentSettlementConfig (private key) tables

3 On the **Query** tab, type this query:

```
delete from databasemetadata where propertyname =
'StoreDataRetrieveConfigInfo'
```

4 On the Query Tool toolbar, click **Run**.

To reset the encryption key

1 Start Microsoft Dynamics POS, and then switch to Manager View.

2 Settle any outstanding transactions by clicking **Settle Transactions** on the **Transactions** menu.

3 On the **Tools** menu, click **Reset Payment Encryption**, and then click **Yes**.

Data transmissions 12.1, 12.2

All Microsoft Dynamics POS transmissions of cardholder data, whether over a private or public network, are secured by the use of SSL. This helps to satisfy Requirement 4.1 of the PCI Data Security Standard.

Microsoft Dynamics POS does not allow or facilitate transmission of Primary Account Numbers (PANs) via e-mail or other end-user messaging technologies. If any such transmission takes place, encryption is required in order to meet Requirement 4.2 of the Data Security Standard.

Part 4: Connection limitations

Internet connections

Microsoft Dynamics POS does not require a Web server. A DMZ can be used to separate the Internet from systems that store cardholder data. Cardholder data must be stored in the internal network and never in the DMZ. The database server should never be on a Web server, or in the DMZ with the Web server, and Microsoft Dynamics POS does not require this.

Wireless connections 6.1, 6.2

Microsoft Dynamics POS does not require or support wireless connections. Microsoft does not recommend using wireless connections with Microsoft Dynamics POS. Using wireless connections could cause the software to stop working and could prevent PCI compliance. Even if wireless connections are part of the store's LAN and not used with Microsoft Dynamics POS, you must install a firewall and use compliant wireless settings as described in Requirements 1.2.3, 2.1.1, and 4.1.1 of the PCI Data Security Standard, respectively. Specific requirements include:

- Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.
- Changing wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
- Ensuring wireless device security settings are enabled for strong encryption technology for authentication and transmission.
- Using industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

Note

For new wireless implementations, implementing WEP is prohibited after March 31, 2009. For current wireless implementations, it is prohibited after June 30, 2010

Remote access 11.2, 11.3

Microsoft Dynamics POS does not provide features that allow or facilitate remote connection into the payment environment, and Microsoft does not provide support for such connections. If you choose to use a remote connection, you must use two-factor authentication (username and password plus an additional authentication item, such as a token), as required by Requirement 8.3 of the PCI Data Security Standard.

If remote access software is used by partners or resellers, security features must be implemented and used. Examples of remote access security features include:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each user).
- Allow connections only from specific (known) IP/MAC addresses.

- Use strong authentication and complex passwords for logins, according to PCI Data Security Standard Requirements 8.1, 8.3, and 8.5.8–8.5.15.
- Enable encrypted data transmission according to PCI Data Security Standard Requirement 4.1.
- Enable account lockout after a certain number of failed login attempts according to PCI Data Security Standard Requirement 8.5.13.
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Enable logging.
- Restrict access to user passwords to authorized reseller/integrator personnel.
- Establish user passwords according to PCI Data Security Standard Requirements 8.1, 8.2, 8.4, and 8.5.

Non-console administrative access 13.1

Non-console administrative access to Microsoft Dynamics POS is not supported and could prevent PCI compliance. If you choose to use non-console administrative access, you must implement and use SSH, VPN, or SSL/TLS for encryption, as required by Requirement 2.3 of the Data Security Standard.

Part 5: Audit logging 4.2

In order to comply with Requirement 10 of the PCI Data Security Standard, logging must be enabled as described in Part 2, "Other setup requirements," earlier in this guide, and you must monitor and manage the log files that are produced.

Monitoring event logs

Microsoft Dynamics POS 2009 uses a unique Windows user account for every POS user, so POS user logon and logoff or other user management events can be viewed from the Windows Event Log. With file and system object access being audited, you can also use the Event Log to monitor access to the auditing files themselves.

To view an event log

1 Click **Start**, and then click **Control Panel**.

2 If needed, switch to Classic View.

3 Double-click **Administrative Tools**, and then double-click **Event Viewer**.

4 If available, expand the **Windows Logs** folder, and then click **Security**.

Each event has a unique Event ID, and the Windows Event Viewer provides a filter tool to make it easier to view occurrences of specific events. The following table identifies the Windows Event IDs that are logged based on corresponding operations in Windows or Microsoft Dynamics POS 2009.

	Event ID	
Operation	**Vista**	**Windows XP**
Logon attempt	4776	680
Logon success	4624	528
Logon failure	529, 535, 539	529, 535, 539
Logoff	538	538
User password reset	4724	628
User account created	4720	624
User account disabled	4725	629
User account deleted	4726	630
User account added	4728	632
User account changed	4738	642
User account locked out	4740	644

Member added to user group (permission granted to POS user)	4732	636
Member removed from user group (permission revoked from POS user)	4733	637
Object access (update or deletion of monitored files)	---	560
File modified and saved	4663	567
Audit policy changed	---	612
Domain policy changed	4739	643
Event Viewer Security log cleared	1102	517

For each event, the following information is logged and can be viewed in the Event Viewer:

- The Windows user account that was involved in the operation (sometimes corresponding to the Microsoft Dynamics POS employee ID, such as R#_1 for an the employee ID "1")
- The type of event
- The date and time the event occurred
- The success or failure of the operation
- The origination of the event
- The identity or name of any affected data, component, or resource
- If appropriate, the user group for which a user was added or removed

Note

The Microsoft Dynamics POS user group identifies the specific permissions that were granted to or revoked from the user.

Monitoring access to payment-related information

The SQL trace logs facilitate monitoring of all access to payment-related information in the store database. Whenever any payment-related information is accessed, either through Microsoft Dynamics POS 2009 or by using any other tool or application, an audit log entry is generated.

The following information is captured for audit purposes:

- The user that is logging in to access data
- The type of event
- The specific database query that was used to access data, which indicates whether data was read or modified
- The date and time of access

- The success or failure of the operation
- The origination of the event (client application)
- The identity or name of the resource (database table) that was accessed

To view a SQL trace log

1 In SQL Server Management Studio[2], on the **File** menu, point to **New**, and then click **Query with Current Connection**.

2 In the right pane, type this text, replacing "C:\<path>" with the actual location of the trace file and <date> with the date string of the correct trace file:

```
select * FROM
::fn_trace_gettable('C:\<path>\pos_trace_pmt_<date>.trc',
default)
```

3 On the **Query** menu, click **Execute**.

The results of the query provide the audit log.

Note

The SQL trace log files are saved in a secure location that only Administrators can access.

[2] SQL Server® Management Studio Express is available free. Visit the Microsoft Download Center at http://www.microsoft.com/downloads to download Microsoft SQL Server 2008 Express with Tools. On the **Installation Type** page of the setup wizard, select **Perform a new installation of SQL Server 2008**, and then continue with the wizard. On the **Feature Selection** page, clear the check box for **Database Engine Services** and select the check box for **Management Tools – Basic**, and the complete the wizard.

Part 6: Software updates and support

Software updates 10.1

Updates to Microsoft Dynamics POS are not delivered via remote connection. Instead, updates are either downloaded from a secure Web site, at the merchant's specific request, or installed from a CD. In the unlikely event that a software update is downloaded via remote connection, this must be done through a firewall and via secure modem, as described in Requirements 1 and 12.3, respectively.

Troubleshooting and support 1.1.5

This section outlines the process that Microsoft and its Certified Partners are required to follow when a Microsoft Dynamics POS customer requires troubleshooting of a specific problem. This process is designed to ensure the security of sensitive information in the customer's store database, including employee passwords and payment-related data such as credit card numbers, and helps to satisfy Requirement 3.2 of the PCI Data Security Standard. The store database is the only place that contains sensitive cardholder information, and support personnel are required to collect only the limited amount of data needed to solve the specific problem being reported.

The remaining paragraphs in this section describe the process followed by Microsoft support personnel and the Microsoft Dynamics POS product team. Microsoft Certified Partners are required to implement support processes and tools with equivalent security measures in place, including but not limited to:

- Collection of sensitive authentication data only when needed to solve a specific problem.
- Storage of such data only in specific, known locations with limited access.
- Collection of only the limited amount of data needed to solve a specific problem.
- Encryption of sensitive authentication data while stored (provided automatically by Microsoft Dynamics POS).
- Secure deletion of such data immediately after use.

When a customer contacts Microsoft Technical Support, the support engineer creates a record of the issue and initiates an investigation. The product team then attempts to reproduce the issue on test databases and, if needed, with test credit-card accounts. If the issue cannot be reproduced on test databases, support personnel follow one of the following processes, depending on the situation:

- Support personnel access the customer's desktop
- Support personnel obtain a copy of the store database
- Support personnel travel to the customer's place of business

In all scenarios, access to the database is restricted to these support personnel: Escalation Engineers, Support Escalation Engineers, Tech Leads, and Team or Service Delivery Managers.

Support personnel access the customer's desktop

With the customer's specific approval, a support engineer can use Microsoft Easy Assist to access the customer's desktop and investigate the issue directly. Easy Assist is a remote support solution based on the Microsoft Office Live Meeting 2007 service and subject to all Live Meeting security measures. These include a full suite of access, content storage, hosting infrastructure, and data transmission security features and measures. For details, see the Microsoft Office Live Meeting Service Security Guide.

The Easy Assist process looks like this:

1. The support engineer sets up the session, and then sends a session invitation to the customer. This invitation contains a link that connects the customer to a specific Easy Assist session. Alternatively, the engineer can provide the Session ID to the customer, which the customer can use to log on at http://support.microsoft.com/ea.
2. The customer accepts the Easy Assist Terms of Use and, if necessary, installs the Easy Assist software.
3. Once in the Easy Assist session, the customer specifically allows the support engineer to share the customer's desktop by pointing to **Share My Desktop** on the **Tools** menu and then clicking **Start**. Alternatively, the support engineer can send a request for sharing to the customer, which the customer can explicitly approve or deny.
4. At the conclusion of the session, or at any time the customer chooses, the customer stops sharing the desktop by pointing to **Share My Desktop** on the **Tools** menu and then clicking **Stop**. At this point, the support engineer can still exchange chat messages with the customer and accept files specifically transferred by the customer, but the engineer has no direct access to the customer's computer.
5. The customer terminates the Easy Assist session (at any time) by clicking **Exit** on the **File** menu. Once the session is terminated, the support engineer cannot send or receive chat messages, cannot receive files, and has no access to the customer's computer. There is no way for the engineer to reestablish the session.

Support personnel obtain a copy of the store database

The database is transmitted to Microsoft either by means of the File Transfer utility in Easy Assist or by using Microsoft's secure https file transfer services. Once the database reaches Microsoft, it is stored on a specific Support file server that is secured according to Microsoft corporate and Support guidelines and to which only support personnel have access. Sensitive authentication data in the database remains encrypted at all times, and the database is not attached to a SQL Server except during active troubleshooting.

When troubleshooting is complete, the store database is immediately, securely deleted from the Microsoft server. Any associated .bak, .mdf, and .ldf files are also destroyed.

Note

If the issue does not involve payments, Microsoft directs the customer to settle all transactions prior to transmitting the database, thereby removing all sensitive authentication data.

Support personnel travel to the customer's place of business

The support engineer investigates the issue on-site, and the customer's data never leaves the store.

Distribution of hotfixes

When a resolution becomes available for a reported issue, a hotfix is released. Hotfixes are distributed via secure download from the Microsoft Web site, at the customer's specific request.