Microsoft Dynamics™

Implementation Guide for PCI Compliance

Microsoft Dynamics® AX 2012

February 2012

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989

Worldwide +1-701-281-6500

www.microsoft.com/dynamics

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Table of contents

Introduction

The requirements in this guide **must** be followed if you want to implement Microsoft Dynamics® AX 2012 and Payment Services for Microsoft Dynamics ERP (the integrated payment solution from Microsoft) in a manner that is compliant with the Payment Card Industry (PCI) Data Security Standard version 2.0.

Note

Microsoft Dynamics AX 2012 includes Microsoft Dynamics AX for Retail.

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

This guide is intended for and disseminated to customers, Microsoft® Certified Partners, resellers, and integrators who are deploying Microsoft Dynamics AX 2012 in a retail organization where electronic credit card and debit card payments are accepted, and where Microsoft Dynamics AX 2012 is used as the payment application. As a payment application, Microsoft Dynamics AX 2012 is subject to the PCI Payment Application Data Security Standard (PA-DSS). The contents of this guide reflect that standard.

Important

- Although this guide is made available to Microsoft customers, some of the steps in the 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 cause for concern by PCI Security Standards Council assessors, and could compromise the security of both cardholder and proprietary information.
- Microsoft Dynamics AX 2012 has been validated for PCI compliance only with Payment Services for Microsoft Dynamics ERP, the integrated payment solution from Microsoft. If you intend to use Microsoft Dynamics AX 2012 with another payment solution, you must obtain separate compliance validation.

Get the latest release of this guide

This guide is reviewed annually, whenever a service pack or hotfix for Microsoft Dynamics AX 2012 is released, and whenever an update to one of the Data Security Standards is released. For information about what has changed, see Appendix A: Version history, later in this guide. To obtain the most up-to-date copy of this guide, go to http://go.microsoft.com/fwlink/?LinkID=188804.

For more information

Microsoft provides training materials to our partners, resellers, and integrators to help ensure that they can implement Microsoft Dynamics AX 2012 and related systems and networks in accordance with this guide, and in a manner that is compliant with the PCI Data Security Standard. For more information, go to http://go.microsoft.com/fwlink/?LinkID=188800.

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

Part 1: Setup

For PCI compliance, you must complete **all** the procedures in this part of the guide.

Install the software

To deploy Microsoft Dynamics AX 2012 in a manner that is PCI-compliant, follow the instructions in the *Retail Deployment Guide: Microsoft Dynamics AX 2012*, which is available as a download at http://go.microsoft.com/fwlink/?LinkId=231846.

Important

- For maximum security, Microsoft Dynamics AX 2012 must be installed in the Program Files folder or a location with similar access control protections.
- Requirement 8.5.8 of the PCI Data Security Standard specifies that group, shared, and generic accounts (for example, the sa account for access to the database) must be disabled or removed.

All computers: Maintain security

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

All computers: Prepare for monitoring of event logs

The event logging capabilities built in to Microsoft Windows® help you comply with Requirements 10.2 and 10.3 of the PCI Data Security Standard. Complete the following procedure on all computers to configure the retention period for event logs.

1. If you are running Windows Embedded POSReady 2009, click **Start**, click **Control Panel**, switch to Classic View, double-click **Administrative Tools**, and then double-click **Event Viewer**.

   If you are running Windows 7, Windows Embedded POSReady 7, or Windows Server® 2008, click **Start**, type **Event Viewer** in the search box, and then press ENTER.
2. If the **Windows Logs** folder is available, expand it, right-click **Security**, and then click **Properties**.
3. In the **Maximum log size** box, type **102400**.
4. Select **Overwrite events as needed**, and then click **OK**.

All computers: Set up auditing of file access, object access, and audit policy changes

To audit changes made to the computer's audit policy, and access to log files and system objects, complete both the following procedures on all computers.

Note

- In an implementation of Microsoft Dynamics AX 2012 that uses Payment Services for Microsoft Dynamics ERP, no cardholder data is stored, and users cannot change the flow or security of cardholder data. Nevertheless, you must complete the procedures in this section to comply with Requirements 10.2 and 10.3 of the PCI Data Security Standard, and to help make organizational data more secure.
- For domain computers, work with the domain administrator to ensure that local audit policies are not overwritten by less stringent domain policies.
- For information about viewing and managing log files, see Part 4: Audit logging, later in this guide.

Enable auditing of file access, object access, and audit-policy changes

1. If you are running Windows Embedded POSReady 2009, click **Start**, click **Control Panel**, switch to Classic View, double-click **Administrative Tools**, and then double-click **Local Security Policy**.

   If you are running Windows 7, Windows Embedded POSReady 7, or Windows Server 2008, click **Start**, type **Local Security Policy** in the search box, and then press ENTER.
2. Expand the **Local Policies** folder, and then click **Audit Policy**.
3. Double-click **Audit account logon events**, select both the **Success** and **Failure** check boxes, and then click **OK**.
4. Double-click **Audit account management**, select both the **Success** and **Failure** check boxes, and then click **OK**.
5. Double-click **Audit object access**, select both the **Success** and **Failure** check boxes, and then click **OK**.
6. Double-click **Audit policy change**, select both the **Success** and **Failure** check boxes, and then click **OK**.

Audit access to system folders and files

The following procedure provides steps for turning on folder and file auditing. The folders that you must audit vary by operating system.

For Windows 7, Windows Embedded POSReady 7, and Windows Server 2008:

- C:\Windows\System32\winevt\Logs.
- The folder where Microsoft Dynamics AX 2012 is installed (by default, C:\Program Files\Microsoft Dynamics AX or, on a 64-bit computer, C:\Program Files (x86)\Microsoft Dynamics AX). See the note in step 8 of the following procedure.
- The Microsoft SQL Server® data directory (by default, C:\Program Files\Microsoft SQL Server\<*instance name*>\MSSQL\Log).

For Windows Embedded POSReady 2009:

- C:\Windows\System32\config.
- The folder where Microsoft Dynamics AX 2012 is installed (by default, C:\Program Files\Microsoft Dynamics AX). See the note in step 8 of the following procedure.
- The SQL Server data directory (by default, C:\Program Files\Microsoft SQL Server\<*instance*>\MSSQL\Log).

Complete this procedure for each folder in the previous lists.

1. In Windows Explorer, right-click the folder name, and then click **Properties**.
2. On the **Security** tab, click **Advanced**.

   Note

   If the **Security** tab is not available, click **Folder Options** on the **Tools** menu, click the **View** tab, and then clear the **Use simple file sharing** check box.

3. Click the **Auditing** tab. If you receive a security message, click **Continue**.
4. Click **Add**.
5. In the **Enter the object name to select** box, type **Everyone**, 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
   - Read permissions
   - Change permissions

   Note

   Do not enable Read permissions for the folder where Microsoft Dynamics AX for Retail POS is installed (by default, C:\Program Files\Microsoft Dynamics AX\50\Retail POS).

9. If the previous settings provide more auditing than is otherwise set up for the folder, select the **Replace all existing inheritable auditing entries** check box, and then click **OK**.
10. Click **OK** in the remaining dialog boxes.

Required services and protocols

The following table lists the services and protocols that are required by Microsoft Dynamics AX for Retail and its components.

Retail components	Required services and protocols
Microsoft Dynamics AX for Retail	Microsoft Dynamics AX
Microsoft Dynamics AX for Retail Store Connect	• Windows Sockets • Internet Protocol security (IPsec) (Default port: 16750) • SQL Server (Default port: 1433) • Microsoft Dynamics AX .NET Business Connector (BC.NET)

Retail components	Required services and protocols
Microsoft Dynamics AX for Retail Transaction Service	• Microsoft .NET Remoting (Default port: 1239) • .NET Business Connector (BC.NET)
Retail POS	SQL Server (Default port: 1433)
Microsoft Dynamics AX for Retail POS Offline Sync Service	Microsoft Sync Framework 2.1
Microsoft Dynamics AX for Retail POS Database Utility	SQL Server (Default port: 1433)

Communication and database computers: Open the firewall

To establish communications between computers in the organization, open the firewall on any communications server and on store database computers, as described in the following table.

Type of computer	Open the firewall to these programs
Head office communications server	• Retail Store Connect • Retail Transaction Service
Store communications server	• SQL Server, to enable connections to the message database • Retail Store Connect
Store database server	SQL Server
Store register with its own local database	SQL Server, but only if Retail Store Connect is on a different computer

Note

- Instead of opening the firewall to Retail Store Connect and Retail Transaction Service, you might prefer to open the firewall to the TCP ports used by these programs. In this case, you must know the port numbers that you specified when you deployed the services. By default, the port numbers are 1433 for SQL Server, 16750 for Retail Store Connect, and 1239 for Retail Transaction Service.

  If you are using multiple instances of Retail Store Connect on a single computer, we recommend that you open the firewall to specific port numbers instead.
- Depending on the settings of your firewall, you might also need to open the firewall to outbound traffic on client and register computers. To determine whether this is necessary, consult your network administrator.
- The instructions in the rest of this section are for Windows Firewall. If you are using another firewall, see the firewall documentation for more information.

Open Windows Firewall on Windows 7, Windows Vista, or Windows Server 2008

To open Windows Firewall to a program on Windows 7, Windows Vista®, or Windows Server 2008, use the New Rule Wizard to create a rule that manages the connections that the allowed program can receive. You can use the default settings for each rule, but you must provide the path of the program and a name for the rule.

Program	Typical program path	Suggested rule name
SQL Server	C:\Program Files\Microsoft SQL Server\<*instance name*>\MSSQL\Binn\Sqlservr.exe	SQL Server <*instance name*>
Retail Store Connect (if installed)	C:\Program Files\Microsoft Dynamics AX\50\Retail Store Connect\bin\Dbserver.exe	Retail Store Connect
Retail Transaction Service (if installed)	C:\Program Files\Microsoft Dynamics AX\50\Retail Transaction Service\RetailTransactionService.exe	Retail Transaction Service

Note

On a 64-bit operating system, Retail Store Connect and Retail Transaction Service are in the Program Files (x86) folder path instead.

1. Log on to the computer as a Windows Administrator.
2. Click **Start**, type **wf.msc** in the search box, and then press ENTER.
3. Click **Inbound Rules**.
4. To create a new rule, click **New Rule**, select **Program**, and then complete the New Inbound Rule Wizard.
5. Repeat step 4 for the other programs that should be allowed through the firewall.

Open Windows Firewall on Windows Embedded POSReady 2009

1. Log on to the computer as a Windows Administrator.
2. Click **Start**, and then click **Control Panel**.
3. If necessary, switch to Classic View, and then double-click **Windows Firewall**.
4. On the **Exceptions** tab, click **Add Program**.
5. In the **Programs** list, select the program, and then click **OK**.
6. Repeat steps 4 and 5 other the other programs that should be allowed through the firewall, and then click **OK**.

At the head office: Set up the password policy

Requirement 8.5.8 of the PCI Data Security Standard specifies that group, shared, and generic accounts must not be used, and provides test procedures for verifying this.

Requirements 8.5.9 through 8.5.14 specify password and account security regulations for people with administrative access to the payment application. To comply with these requirements, contact the domain administrator to establish group policies for the domain that meet the **minimum** requirements described in the following table.

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

- Users of Microsoft Dynamics AX 2012 are subject to Active Directory Domain Services security policies. Therefore, users of Microsoft Dynamics AX are subject to the same password policy as domain users.
- Installing Microsoft Dynamics AX 2012 on a computer that is not part of the domain is not supported.
- These policies represent the minimum requirements of Requirements 8.5.9 through 8.5.14. More stringent settings can be used.
- For more information about managing password policy via group policies, see "Working with Group Policy objects" at http://technet.microsoft.com/en-us/library/cc731212.aspx.

At the head office: Set up database logging

By modifying the audit trail in Microsoft Dynamics AX 2012, you can enable logging of the following events in the head office database:

- **Changes to the audit trail settings.** These settings are stored in the DATABASELOG table for the head office and in the RetailFunctionalityProfile table for Retail POS.
- **Changes to the payment processing configuration.** These settings are stored in the RetailHardwareProfile table for both the head office and Retail POS.
- **The creation, deletion, or modification of cashier user accounts and permissions.** These settings are stored in the RetailStaffPermissionGroup table for the head office and in the RetailStaffTable table for Retail POS.

Note

Although the logging of activity in the head-office database is related to Requirements 10.2 and 10.3 of the PCI Data Security Standard, it is beyond the scope of the PCI requirements because, in an implementation of Microsoft Dynamics AX 2012 that uses Payment Services for Microsoft Dynamics ERP, no cardholder data is stored, and users cannot change the cardholder data flow or the security of cardholder data.

Therefore, the following procedure is included in this guide as an optional best practice that helps make organizational data more secure.

1. To set up logging in the head office database, click **System administration** > **Setup** > **Database** > **Database log setup**.

2. Create the following new entries by following the wizard.

Table name	Actual system name
POS functionality profile	RetailFunctionalityProfile
POS hardware profiles	RetailHardwareProfile
Component Item ID	RetailStaffLoginLog
Staff permission group	RetailStaffPermissionGroup
Staff	RetailStaffTable
Audit trail setup	SysDatabaseLogTableSetup

3. Click **System administration** > **Setup** > **Licensing** > **Licensing configuration**.
4. Under **Administration**, select the **Electronic signature** check box, and then click **OK**. If you are prompted to synchronize tables, click **Yes**.

Note

- This procedure sets up logging on Insert, Delete, Update, and RenameKey actions. To view or modify this setup, click **System administration** > **Setup** > **Database** > **Database log setup**.
- For each change to one of these tables, Microsoft Dynamics AX records the user who performed the action, the table that was modified, the action that was taken, the attribute that was changed, the time and date of the action, and the ID of the record that was modified or added. For each Update action, it also records both the previous and new settings.
- By default, any user who has database access can query a database log by using .NET Business Connector, X++, or alerts, or by using direct database access. To protect data, restrict permissions on the SysDatabaseLog table. For more information, see "Manage table and field access" at http://technet.microsoft.com/en-us/library/aa834466.aspx and "Table Properties" at http://msdn.microsoft.com/en-us/library/aa871620.aspx.
- For information about viewing logged actions, see Monitor Microsoft Dynamics AX activity, later in this guide.

At the head office: Enable SQL Server trace logging

To monitor access to the audit log, enable SQL Server trace logging by using the AxRetailTrace.sql file.

Note

- AxRetailTrace.sql is included in the Microsoft Dynamics AX 2012 download package and can be found in the RetailSecurityGroups subfolder of the folder where you extracted the installation files.
- Although this procedure is related to Requirements 10.2 and 10.3 of the PCI Data Security Standard, it is beyond the scope of the PCI requirements because, in an implementation of Microsoft Dynamics AX 2012 that uses Payment Services for Microsoft Dynamics ERP, no cardholder data is stored, and users cannot change the cardholder data flow or the security of cardholder data. Therefore, the following procedure is included in this guide as an optional best practice that helps make organizational data more secure.

1. Copy AxRetailTrace.sql to the computer where the head office database is located.
2. Open SQL Server Management Studio, and connect to the instance of SQL Server that is used in the Microsoft Dynamics AX deployment.
3. On the **File** menu, point to **Open**, click **File**, browse to and select the .sql file, and then click **OK**.
4. Click **Execute**.

Note

- The trace log files are located in the Log directory for the instance. SQL Server trace log files have a maximum size of 100 MB. When the size of a log file exceeds this limit, a new log file is created by using a date-based numbering scheme.
- For information about viewing and managing log files, see Part 4: Audit logging, later in this guide.
- A commented section at the end of the AxRetailTrace.sql script file contains the code for performing several operations related to trace logging. These include manually starting and stopping the trace, viewing the contents of the Microsoft Dynamics AX log tables, viewing the trace detail, and disabling the automatic start of tracing. To complete one of these operations, copy the code for the operation into a new query file, modify the script as described in the comments, and then click **Execute**.

At the head office: Set up payment processing and hardware devices

In Microsoft Dynamics AX 2012, the only time that store employees have access to card numbers is at the time of sale, when the cashier swipes the card. Payment information is sent directly from Retail POS to the processor at that time, and transactions are settled immediately.

Payment information in the Microsoft Dynamics AX 2012 database is limited to the customer's name, the payment amount, the card type, and the last four digits of the card number. The entire primary account number (PAN) is never stored. All processed transactions can be reviewed by using the built-in payment report in Microsoft Dynamics AX.

After auditing and other security measures are in place, the store can begin accepting card payments. To do this, complete the following steps:

1. Obtain a Payment Services for Microsoft Dynamics ERP subscription from Microsoft online services, and associate it with the retail organization's merchant account. For more information and instructions, go to http://go.microsoft.com/fwlink/?LinkID=188806.
2. Modify hardware profiles to configure payment processing and support for hardware devices, such as receipt printers, magnetic stripe readers (MSRs), and personal identification number (PIN) pad devices.
3. Associate a hardware profile with each register to enable payment processing and to select devices.
4. Set up one or more tender types to use payment processing.
5. Enable one or more payment processing tender types for each store.
6. Turn on payment processing at stores by running scheduled jobs.

Note

- These steps are not specifically required for PCI compliance. However, if these steps are skipped, the store cannot use Microsoft Dynamics AX 2012 to process the payments that are subject to the PCI Data Security Standard. The steps are described in more detail later in this section.
- By using Payment Services for Microsoft Dynamics ERP, you can easily and securely accept and process credit and debit card payments in your applications, online, from the head office, and in your stores. The PCI-certified service lets you choose from a number of payment providers, and seamlessly incorporates multiple payment options without the need for additional software or integration.
- As Microsoft Dynamics AX 2012 is shipped in the United States and Canada, the only processor that it communicates with is Payment Services for Microsoft Dynamics ERP. This communication is configured in the **Retail** module, and then the settings are sent down to the stores. During authorization and settlement, these settings are used to identify the organization's subscription and its associated merchant account. No cardholder data is included.

Important

Microsoft Dynamics AX 2012 has been validated for PCI compliance only with Payment Services for Microsoft Dynamics ERP. If you intend to use Microsoft Dynamics AX 2012 with another payment solution, you must obtain separate compliance validation.

Configure payment processing and set up devices in the Retail module

You must obtain the actual device names from the store to complete this procedure. Device names can be viewed on the register by viewing the appropriate device class (MSR, PINPad, or POSPrinter) in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\OLEforRetail\ServiceOPOS

1. Click **Retail** > **Setup** > **POS** > **Profiles** > **Hardware profiles**.
2. In the list, select the correct profile.
3. On the **EFT service** tab, enter the information provided by Payment Services for Microsoft Dynamics ERP.
4. On the tab for each device, in the **Device name** box, type the appropriate device name. A description for the device is optional.

Note

- You must use the same device names in the hardware profile that you use when you configure the actual devices on each terminal.
- If you have registers where payment processing will not take place, consider using a hardware profile that does not have payment processing configured.
- You must create a separate hardware profile for each combination of devices used at the stores. Similarly, if like devices are named differently on different registers or at different stores, you must create additional hardware profiles.

Enable payment processing and select devices for specific registers

To enable payment processing and select devices, associate the hardware profile with each register.

1. Click **Retail** > **Setup** > **POS** > **POS terminals**.

2. Double-click the register to modify.
3. On the **General** tab, in the **Hardware profile** box, select the appropriate profile. Then, in the **EFT POS register number** box, type one of the register numbers that you received from the payment provider.

   Note

   Some payment providers refer to EFT POS register numbers as *terminal IDs*. In Retail POS, *terminal ID* refers to the terminal number shown on the **General** tab. The terminal number and the EFT POS register number do not have to match, but both numbers must be unique for each terminal.
4. Repeat steps 2 and 3 for other registers. When you have finished associating hardware profiles with registers, close the form.

Set up payment methods for payment processing

Payment methods are the types of tender accepted by the store—in this case, credit cards and debit cards. Card types are the specific credit cards accepted for a card tender type. For more information about the steps in this procedure, see Microsoft Dynamics AX 2012 Help.

1. Click **Retail** > **Setup** > **Payment methods** > **Payment methods**.
2. On the toolbar, click **New**.
3. In the new row, type a unique number and description for the new payment method. Then, in the **Default function** column, click the arrow, and select **Card**.
4. Close the form.
5. Click **Retail** > **Setup** > **Payment methods** > **Card types**.
6. On the toolbar, click **New**.
7. In the new row, type a unique ID and name for the new card type. Then, in the **Card types** column, click the arrow, and select the appropriate option.
8. While the new row is still selected, click **Card number**.
9. Create a verification mask for the card type by entering the range of digits that all cards of this type begin with. For example, Visa card numbers begin with 4, so you could verify that cards accepted as the Visa card type are really Visa cards by creating a mask of **4**.
10. Close the **Card number** form.
11. Close the **Card type** form.

Enable tender types and card types for specific stores

1. Click **Retail** > **Common** > **Retail channels** > **Retail stores**.
2. Select a store, and then, on the **Setup** tab, click **Payment methods**.
3. On the toolbar, click **New**, and then, on the **General** tab, in the **Payment method** field, select a payment method. The information for the selected payment method is filled in automatically.
4. While the new payment method row is still selected, click **Card setup**.
5. On the toolbar, click **New**, and then, in the **Card ID** field, select the card type for this payment method.

6. Select the new card setup, and then, on the **General** tab, select the **Check expiration date** check box.
7. Close the **Card setup** form.
8. Close the **Payment method** form.
9. Repeat steps 3 through 8 for any other payment methods for this store.

Send payment processing changes to the stores

Payment processing changes do not take effect until the associated scheduled jobs are run and the information included in the jobs is sent down to the stores. This procedure describes how to run the jobs manually.

1. Click **Retail** > **Periodic** > **Retail scheduler** > **Create actions**. The preactions that were generated when you changed the payment processing settings are converted into actions, or jobs.
2. Click **Retail** > **Periodic** > **Retail scheduler** > **Distribution schedule**.
3. To send down the payment processing and device settings in the hardware profile, select the **A-1090 Registers** job, and then click **Run directly**.
4. To send down the payment methods, card types, and card numbers, select the **A-1070 Stores and tenders** job, and then click **Run scheduler job directly**.

Test payment processing

You can test payment processing by processing card transactions in test mode.

1. In a register or store database, in the POSHARDWAREPROFILE table, change the value in the EFTTESTMODE column to **1**.
2. Process a card transaction.
3. Verify that the transaction went through by visiting the Payment Services payment portal at https://payments.dynamicsonline.com/Home/Dashboard.aspx.

Note

You can test payment processing only if Retail POS is running in production mode.

Store computers: Set up the password policy

Requirements 8.5.9 through 8.5.14 of the PCI Data Security Standard specify password and account security regulations for people with access to the payment application. To comply with these requirements, the password policy on each store computer where Retail POS is installed must meet the minimum requirements described in the following table.

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

- These policies represent the minimum requirements of Requirements 8.5.9 through 8.5.14. More stringent settings can be used.
- For more information about setting up a Windows account for each store user, see the *Retail Deployment Guide: Microsoft Dynamics AX 2012*, which is available as a download at http://go.microsoft.com/fwlink/?LinkId=231846.

1. If you are running Windows Embedded POSReady 2009, click **Start**, click **Control Panel**, switch to Classic View, double-click **Administrative Tools**, and then double-click **Local Security Policy**.

   If you are running Windows 7, click **Start**, type **Local Security Policy** in the search box, and then press ENTER.
2. Expand **Account Policies**, and then click **Password Policy**.
3. To modify a policy, right-click the policy, and then click **Properties**.
4. Click **Account Lockout Policy**.
5. To modify a policy, right-click the policy, and then click **Properties**.

Store computers: Set up password-protected screen savers

At each register, set up a screen saver that appears when the register is idle, and that requires the password for the cashier's Windows user account to be entered before access to Retail POS is regained.

1. In the C:\Windows\System32 folder, locate the screen saver (.scr) file to use.
2. If you are running Windows Embedded POSReady 2009, click **Start**, click **Run**, type **mmc**, and then click **OK**.

   If you are running Windows 7 or Windows Embedded POSReady 7, click **Start**, type **mmc** in the search box, and then press ENTER.
3. On the **File** menu, click **Add/Remove Snap-in**, and then, if you are running Windows Embedded POSReady 2009, click **Add**.
4. Select **Group Policy Object Editor**, click **Add**, click **Finish**, and then click **Close** or **OK**.
5. Expand **Local Computer Policy**, expand **User Configuration**, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization** (on Windows 7) or **Display** (on other operating systems).
6. Double-click **Force specific screen saver** (on Windows 7) or **Screen Saver executable name** (on other operating systems), select **Enabled**, type the path and name of the screen saver (.scr) file that you selected in step 1, and then click **OK**.
7. Double-click **Password protect the screen saver**, select **Enabled**, and then click **OK**.
8. Double-click **Screen Saver timeout**, select **Enabled**, type **900** or a smaller value, and then click **OK**.

Note

Completing this procedure on each computer in the store helps satisfy Requirement 8.5.15 of the PCI Data Security Standard. According to this requirement, 900 seconds (15 minutes) is the maximum time that the register can be idle without locking. You can specify a shorter time if you prefer.

Store computers: Turn off System Restore

System Restore is a Windows feature that restores your computer's system files to the state they were in at an earlier time. The restore points saved by this feature are not considered secure by the PCI Security Standards Council.

Note

System Restore is not available on Windows Server 2008.

Turn off System Restore on Windows 7

1. On the **Start** menu, right-click **Computer**, and then click **Properties**.
2. Click **System protection**.
3. Select the C: drive, click **Configure**, select **Turn off system protection**, and then click **OK**.

Turn off System Restore on Windows Embedded POSReady 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**.

Part 2: Features that facilitate PCI compliance

This part of the guide discusses some of the features in Microsoft Dynamics AX 2012 that facilitate merchant compliance with the PCI Data Security Standard.

Audit logging

Logging of PCI-relevant activity at the register is automatic. For more information, see Monitor Retail POS activity, later in this guide.

User names, passwords, and authentication

Stores and cashiers have no administrative access, and no access to reports. They have access to card numbers only when a card is swiped.

Users of Microsoft Dynamics AX are subject to Active Directory Domain Services security policies. Therefore, users of Microsoft Dynamics AX are subject to the same password policy as domain users.

Employee user names and passwords are set up in the **Retail** module of Microsoft Dynamics AX 2012. Only approved Microsoft Dynamics AX users have access to these features.

Microsoft Dynamics AX 2012 does not provide any default accounts or passwords. Instead, a unique user name and password are required for each user, including the user who sets up the software. These features help satisfy Requirements 2.1 and 8 of the PCI Data Security Standard.

Activities related to setting up new employees, deleting employees, and changing employee user names or passwords are logged. For more information, see Monitor Microsoft Dynamics AX activity, later in this guide.

When cashiers log on to Retail POS at the store, their employee user names and passwords are securely authenticated by either Retail Transaction Service or Retail Store Connect, depending on employee settings. Cashier passwords are always hashed (obscured).

Set up a new cashier in Microsoft Dynamics AX

1. Click **Retail** > **Common** > **Workers**.
2. Click **Hire new worker**, and then type the new cashier's name.
3. Enter information about the employee on the tabs as needed.
4. In the **Worker** form, click the **Retail** link, and then select a layout ID and a language for the employee.
5. In the **Employment type** box, select **Cashier**, and then type a name in the **Name on receipt** box.
6. In the **Password** box, type the employee's password.
7. Click **POS permissions**, and then select a position for the cashier.

Important

When setting up Windows user accounts for employees, and when setting up employee accounts in Microsoft Dynamics AX, you must use a "least privilege" approach, granting employees only those privileges that they require to perform their duties. For example, although trusted management personnel might require Administrator privileges on store computers, employee logon accounts must belong to a group that does not have these privileges. This helps you comply with Requirement 7 of the PCI Data Security Standard.

According to Requirement 8.1 of the PCI Data Security Standard, each employee must have his or her own logon account. Do not allow employees to share employee IDs or passwords.

For more information about user accounts for employees, see the *Retail Deployment Guide: Microsoft Dynamics AX 2012*, which is available as a download at http://go.microsoft.com/fwlink/?LinkId=231846.

Data storage and deletion

Several 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 prohibit storing cardholder data on servers that are connected to the Internet. The database server cannot also be a web server.

Microsoft Dynamics AX 2012 helps merchants comply with the PCI Data Security Standard regarding data storage and retention in the following ways:

- Primary account numbers (PANs) are not retained, so no periodic purging is necessary. This helps satisfy Requirement 3.1 of the PCI Data Security Standard.
- Sensitive authentication data is never retained, cannot be reproduced from within the program, and is not available in log files or debug files.
- Card numbers are truncated after authorization, so that only the last four digits remain. Card numbers on both printed and journaled receipts are always truncated.
- Like this release of Microsoft Dynamics AX 2012, the previous release (Microsoft Dynamics AX for Retail) did not retain any sensitive authentication data.Compliance with Requirement 3.2 of the PCI Data Security Standard does not require the removal of historical data.
- Because cardholder data is not retained, no encryption is required. Therefore, there is no need to periodically delete the encryption key. This helps satisfy Requirement 3.6 of the PCI Data Security Standard.

Data transmissions

All Microsoft Dynamics AX 2012 transmissions of cardholder data, whether over a private network or a public network, are secured by the use of Secure Sockets Layer (SSL). This helps satisfy Requirement 4.1 of the PCI Data Security Standard.

Microsoft Dynamics AX 2012 does not allow or facilitate the transmission of PANs via email or other end-user messaging technologies. Any such transmission that takes place must be encrypted to satisfy Requirement 4.2 of the PCI Data Security Standard.

Flow of payment data

Figure 1 shows the flow of payment data in the Retail POS system.

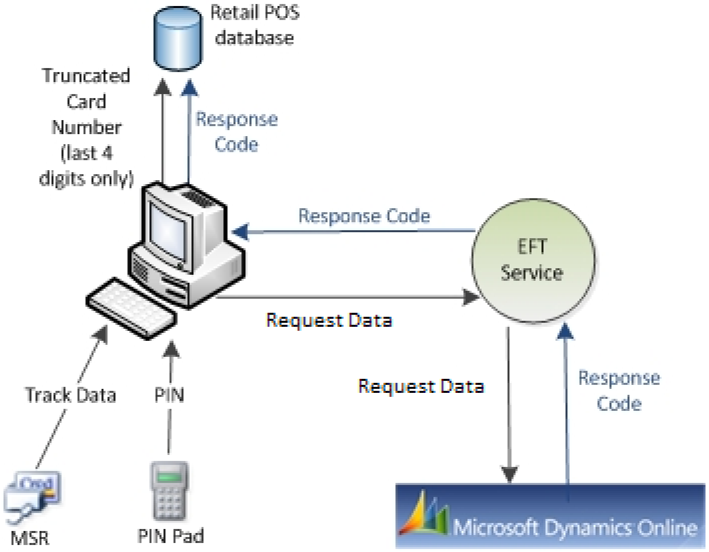

Figure 1 Payment data flow

Part 3: Connection limitations

Internet connections

Microsoft Dynamics AX 2012 does not require a web server. A perimeter network, which is also known as a DMZ (demilitarized zone) and a screened subnet, can be used to separate the Internet from systems that transmit cardholder data. Cardholder data is never stored, including on the internal network and the perimeter network. The database server should never be on a web server or in a DMZ that contains a web server, and Microsoft Dynamics AX 2012 does not require these configurations. This helps satisfy Requirement 1.3 of the PCI Data Security Standard.

Wireless connections

Microsoft Dynamics AX 2012 does not require or support wireless connections, and we do not recommend using wireless connections with Microsoft Dynamics AX 2012. Using wireless connections could cause the software to stop working and could prevent PCI compliance.

If wireless connections are part of the store's local area network (LAN)—even if they are not used with Microsoft Dynamics AX 2012—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. Specific requirements include:

- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.
- Change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and Simple Network Management Protocol (SNMP) community strings.
- Ensure that wireless device security settings are enabled for strong encryption technology for authentication and transmission.
- Use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

Note

For new wireless implementations, implementing Wired Equivalent Privacy (WEP) has been prohibited since March 31, 2009. For current wireless implementations, WEP is prohibited after June 30, 2010.

Remote access

Microsoft Dynamics AX 2012 does not provide features that allow or facilitate remote connections 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 (user name 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 establish user password policies, according to Requirement 8 of the PCI Data Security Standard.
- Enable encrypted data transmission, according to Requirement 4.1 of the PCI Data Security Standard.
- Enable account lockout after a certain number of failed logon attempts, according to Requirement 8.5.13 of the PCI Data Security Standard.
- Configure the system so that 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.

Non-console administrative access

Non-console administrative access to Microsoft Dynamics AX 2012 is not supported and could prevent PCI compliance. If you choose to use non-console administrative access, you must implement and use Secure Shell (SSH), VPN, or Secure Sockets Layer/Transport Layer Security (SSL/TLS) for encryption, as required by Requirement 2.3 of the PCI Data Security Standard.

Part 4: Audit logging

To comply with Requirement 10 of the PCI Data Security Standard, you must enable logging as described in the following sections in this guide:

- All computers: Prepare for monitoring the event logs
- All computers: Set up auditing of file access, object access, and audit-policy changes
- At the head office: Set up database logging

You must monitor and manage the log files that are produced.

Monitor Microsoft Dynamics AX activity

At the head office, audit logged information according to the schedule described in Requirement 10 of the PCI Data Security Standard.

Note

Although the procedures in this section are related to Requirement 10 of the PCI Data Security Standard, they are beyond the scope of the PCI requirement because, in an implementation of Microsoft Dynamics AX 2012 that uses Payment Services for Microsoft Dynamics ERP, no cardholder data is stored, and users cannot change the cardholder data flow or the security of cardholder data. Therefore, the following procedures are included in this guide as optional best practices that help make organizational data more secure.

View information about user logon and user logoff

View the user log in Microsoft Dynamics AX to see logon information for each authorized user.

1. Click **System administration** > **Inquiries** > **Users** > **User log**. The logon dates and times shown are also the dates and times that the log was initialized.
2. To view the date and time that a particular user logged off, select the logon event that you are interested in, and then click the **General** tab.

View the audit trail

Use the database log in Microsoft Dynamics AX to view changes to the tables that you selected for auditing as described in At the head office: Set up database logging, earlier in this guide.

1. Click **System administration** > **Inquiries** > **Database** > **Database log**.
2. Select the record to view, and then click the **History** tab.

View the SQL Server trace log files

Monitor the SQL Server trace log files to see which users accessed the log files. Each entry in the trace log file includes the user who logged on 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), and the identity or name of the resource (database table) that was accessed.

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

2. In the right pane, type the following 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 Server trace log files are saved in a secure location that only administrators can access. Typically, the path of the files is C:\Program Files\Microsoft SQL Server\<*instance name*>\MSSQL\Log.

Monitor Retail POS activity

Activity in Retail POS is logged in the POSIsLog table in the store or register database. The default logging level, **Debug**, provides logging of the events that must be monitored for PCI compliance. These events are as follows:

- Program startup (the initialization of the log file)
- Employee logon and logoff
- Failed logon attempts

Note

The logging level can be modified only at the head office, via changes to the functionality profile for each terminal. Confirm that the **Debug** logging level is still assigned to each functionality profile in the **Functionality profile** form (**Retail** > **Setup** > **POS** > **Profiles** > **Functionality profiles**). The **Trace** logging level is also PCI-compliant but can substantially increase the size of the database.

At the store, use a query in SQL Server Management Studio to view the POSIsLog table. For each event in the table, the following information is logged:

- The type of event
- The date and time that the event occurred
- The origination of the event (store and terminal)
- For logon events, the ID of the cashier who logged on. This cashier is associated with all events after the logon event, until a logoff event occurs.

Monitor event logs

You must monitor the event logs on every computer in the Microsoft Dynamics AX 2012 system. Windows user logon and logoff events, and other user management events, can be viewed from the Windows event log. When file and system object access is audited, you can also use the event log to monitor access to the auditing files themselves.

The event log also shows initialization of the log file in Microsoft Dynamics AX. This is indicated by the event for Application Object Server (AOS) startup, because when the AOS service is running, logging is turned on. The event is Event ID 149, "Object Server <*server name*>: Ready for operation."

1. If you are running Windows Embedded POSReady 2009, click **Start**, click **Control Panel**, switch to Classic View, double-click **Administrative Tools**, and then double-click **Event Viewer**.

   If you are running Windows 7, Windows Embedded POSReady 7, or Windows Server 2008, click **Start**, type **Event Viewer** in the search box, and then press ENTER.

2. If the **Windows Logs** folder is available, expand it, 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 Event IDs that are logged, based on corresponding operations in Windows.

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

- The Windows user account that was involved in the operation
- The type of event
- The date and time that 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

Operation	**Event ID**	
	Windows Embedded POSReady 7, Windows 7, Windows Server 2008	**Windows Embedded POSReady 2009**
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	4732	636
Member removed from user group	4733	637
Object access (update or deletion of monitored files)	None	560
File modified and saved	4663	567
Audit policy changed	None	612
Domain policy changed	4739	643
Event Viewer Security log cleared	1102	517

Part 5: Software updates and support

Software updates

Updates to Microsoft Dynamics AX 2012 are not delivered via remote connection. Instead, updates are either downloaded from a secure website, at the merchant's specific request, or installed from a CD. Software updates must not be downloaded via remote connection.

Troubleshooting and support

This section outlines the process that Microsoft and its Certified Partners are required to follow when a Microsoft Dynamics AX 2012 customer requires troubleshooting of a specific problem. This process is designed to ensure the security of sensitive information in the database, including employee passwords and payment-related data, and helps satisfy Requirement 3.2 of the PCI Data Security Standard. 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 AX 2012 product team. Microsoft Certified Partners are required to implement support processes and tools with equivalent security measures in place. These measures include but are not limited to the following:

- Collect sensitive authentication data only when it is needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Securely delete such data immediately after use.
- Encrypt sensitive authentication data while it is stored. (No sensitive data is stored by Microsoft Dynamics AX 2012. This refers to any data that might be stored via third-party add-ins or other sources.)

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 necessary, 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 (which contains no sensitive cardholder data).
- 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*, which is available for download at http://www.microsoft.com/downloads.

The Easy Assist process is as follows:

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, 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. 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 the customer a request for sharing, which the customer can explicitly approve or deny.
4. At the conclusion of the session, or at any time that 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. After 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.

At no point in this process does the support engineer have access to the customer's card number or card data.

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 the secure Microsoft HTTPS file transfer services. After 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. There is no sensitive authentication data in the database, and the database is attached to a SQL Server only during active troubleshooting.

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

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 website at the customer's specific request.

Appendix A: Version history

The following changes have been made to this guide since it was originally published in June 2010:

- Dates and version numbers have been updated.
- The note at the beginning of "All computers: Set up auditing of file access, object access, and audit-policy changes" has been modified to indicate that completing the procedures in that section is required, and the words "less stringent" have been added to the second bulleted item.
- An error in step 2 of "Audit access to system folders and files" has been corrected.
- A note has been added to "Store computers: Turn off System Restore" to point out that System Restore is not available on Windows Server 2008.
- The figure in "Flow of payment data" has been updated to include the flow of the response code from Payment Services to the Retail POS database.
- Minor editorial changes have been made.
- The information has been updated for the release of Microsoft Dynamics AX 2012.