Implementation Guide for PCI Compliance
Microsoft Dynamics® AX for Retail
April 2011
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.

Copyright © 2011 Microsoft. All rights reserved.

Microsoft, Microsoft Dynamics, SQL Server, Windows, Windows Server, Windows Vista, and the Microsoft Dynamics Logo are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Get the latest release of this guide</td>
<td>1</td>
</tr>
<tr>
<td>For more information</td>
<td>1</td>
</tr>
<tr>
<td><strong>Part 1: Setup</strong></td>
<td></td>
</tr>
<tr>
<td>Install the software</td>
<td>2</td>
</tr>
<tr>
<td>All computers: Maintain security</td>
<td>2</td>
</tr>
<tr>
<td>All computers: Prepare for monitoring the event logs</td>
<td>2</td>
</tr>
<tr>
<td>All computers: Set up auditing of file access, object access, and audit-policy changes</td>
<td>3</td>
</tr>
<tr>
<td>Audit access to system folders and files</td>
<td>3</td>
</tr>
<tr>
<td>Communication and database computers: Open the firewall</td>
<td>4</td>
</tr>
<tr>
<td>Open Windows Firewall on Windows 7, Windows Vista, or Windows Server 2008</td>
<td>5</td>
</tr>
<tr>
<td>Open Windows Firewall on Windows XP or POSReady 2009</td>
<td>6</td>
</tr>
<tr>
<td>At the head office: Set up the password policy</td>
<td>6</td>
</tr>
<tr>
<td>At the head office: Set up database logging</td>
<td>7</td>
</tr>
<tr>
<td>At the head office: Enable SQL Server trace logging</td>
<td>8</td>
</tr>
<tr>
<td>At the head office: Set up payment processing and hardware devices</td>
<td>9</td>
</tr>
<tr>
<td>Configure payment processing and set up devices in Retail Headquarters</td>
<td>10</td>
</tr>
<tr>
<td>Enable payment processing and select devices for specific registers</td>
<td>10</td>
</tr>
<tr>
<td>Set up tender types for payment processing</td>
<td>10</td>
</tr>
<tr>
<td>Enable tender types and card types for specific stores</td>
<td>11</td>
</tr>
<tr>
<td>Turn on payment processing at the stores</td>
<td>11</td>
</tr>
<tr>
<td>Test payment processing</td>
<td>12</td>
</tr>
<tr>
<td>Store computers: Set up the password policy</td>
<td>12</td>
</tr>
<tr>
<td>Store computers: Set up password-protected screensavers</td>
<td>13</td>
</tr>
<tr>
<td>Store computers: Turn off System Restore</td>
<td>13</td>
</tr>
<tr>
<td>Turn off System Restore on Windows 7</td>
<td>13</td>
</tr>
<tr>
<td>Turn off System Restore on Windows Vista</td>
<td>14</td>
</tr>
<tr>
<td>Turn off System Restore on Windows XP or POSReady 2009</td>
<td>14</td>
</tr>
<tr>
<td><strong>Part 2: Features that facilitate PCI compliance</strong></td>
<td></td>
</tr>
<tr>
<td>Audit logging</td>
<td>15</td>
</tr>
<tr>
<td>User names, passwords, and authentication</td>
<td>15</td>
</tr>
<tr>
<td>Set up a new cashier in Microsoft Dynamics AX</td>
<td>15</td>
</tr>
<tr>
<td>Data storage and deletion</td>
<td>16</td>
</tr>
<tr>
<td>Data transmissions</td>
<td>17</td>
</tr>
<tr>
<td>Flow of payment data</td>
<td>17</td>
</tr>
<tr>
<td><strong>Part 3: Connection limitations</strong></td>
<td></td>
</tr>
<tr>
<td>Internet connections</td>
<td>18</td>
</tr>
<tr>
<td>Wireless connections</td>
<td>18</td>
</tr>
<tr>
<td>Remote access</td>
<td>18</td>
</tr>
<tr>
<td>Non-console administrative access</td>
<td>19</td>
</tr>
<tr>
<td>Part 4: Audit logging</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------</td>
</tr>
<tr>
<td>Monitor Retail Headquarters activity</td>
<td>20</td>
</tr>
<tr>
<td>View information about user logon and user logoff</td>
<td>20</td>
</tr>
<tr>
<td>View the audit trail</td>
<td>20</td>
</tr>
<tr>
<td>View the SQL Server trace log files</td>
<td>21</td>
</tr>
<tr>
<td>Monitor Retail POS activity</td>
<td>21</td>
</tr>
<tr>
<td>Monitor event logs</td>
<td>22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 5: Software updates and support</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software updates</td>
<td>24</td>
</tr>
<tr>
<td>Troubleshooting and support</td>
<td>24</td>
</tr>
<tr>
<td>Support personnel access the customer's desktop</td>
<td>25</td>
</tr>
<tr>
<td>Support personnel obtain a copy of the store database</td>
<td>25</td>
</tr>
<tr>
<td>Support personnel travel to the customer's place of business</td>
<td>26</td>
</tr>
<tr>
<td>Distribution of hotfixes</td>
<td>26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix A: Version history</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A: Version history</td>
<td>27</td>
</tr>
</tbody>
</table>
Introduction

Welcome to the Microsoft Dynamics® AX for Retail Implementation Guide for PCI Compliance. The requirements in this guide must be followed in order to implement Microsoft Dynamics AX for Retail and Payment Services for Microsoft Dynamics® AX (the integrated payment solution from Microsoft Dynamics Online) in a manner that is compliant with the Payment Card Industry (PCI) Data Security Standard version 2.0.

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 for Retail in a retail organization where electronic credit card and debit card payments are accepted and where Microsoft Dynamics AX for Retail is used as the payment application. As a payment application, Microsoft Dynamics AX for Retail 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 for Retail has been validated for PCI compliance only with Payment Services for Microsoft Dynamics AX, the integrated payment solution from Microsoft Dynamics Online. If you intend to use Microsoft Dynamics AX for Retail 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 for Retail 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. To obtain the most up-to-date copy of this guide, visit 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 for Retail and related systems and networks according to this guide and in a manner that is compliant with the PCI Data Security Standard. For more information, visit 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, visit http://www.pcisecuritystandards.org.
Part 1: Setup

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

Install the software

To deploy Microsoft Dynamics AX for Retail in a manner that is PCI-compliant, follow the instructions in the Deployment and Installation Guide, included as a .pdf file with Microsoft Dynamics AX for Retail.

Important

- For maximum security, Microsoft Dynamics AX for Retail must be installed in the Program Files folder or a location with similar access-control protections.
- PCI Data Security Standard Requirement 8.5.8 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 the event logs

The event logging capabilities built into 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 XP, Windows Vista®, or 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 or Windows Server® 2008, click Start, type Event Viewer into the search box, and then press ENTER.

2. If available, expand the Windows Logs folder, 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 as well as access to log files and system objects, complete both of the following procedures on all computers.

**Note**
- In an implementation of Microsoft Dynamics AX for Retail that uses the integrated payment solution from Microsoft Dynamics Online, no cardholder data is stored and users cannot change the flow or security of cardholder data. Even so, the procedures in this section must be completed in order 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 XP or 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 Vista, or Windows Server 2008, click Start, type Local Security Policy into 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 Vista, and Windows Server 2008:

- C:\Windows\System32\winevt\Logs
- The folder where Microsoft Dynamics AX for Retail 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 XP and POSReady 2009:

- C:\Windows\System32\config
- The folder where Microsoft Dynamics AX for Retail is installed (by default, C:\Program Files\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>\MSSQL\Log)

Complete this procedure for each of the above folders.

1. In Windows Explorer, right-click the folder name, and then click Properties.
   
   ![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 a security message appears, 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 Retail POS is installed (by default, C:\Program Files\Microsoft Dynamics AX\50\Retail POS).

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

**Communication and database computers: Open the firewall**

In order 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.
On this type of computer | Open the firewall to these programs
---|---
Head-office communications server | Retail Store Connect  
Store communications server | Microsoft SQL Server (to allow connections to the message database)  
Store database server | Microsoft SQL Server  
Store register with its own local database | Microsoft SQL Server only if Retail Store Connect is on a different computer

**Note**
- If you prefer to open the firewall to the TCP ports used by Retail Store Connect and Retail Transaction Service instead of the programs themselves, you must know the port numbers that you specified when you deployed the services. By default, these 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 opening 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, refer to 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 to the program and a name for the rule.

<table>
<thead>
<tr>
<th>Program</th>
<th>Typical program path</th>
<th>Suggested rule name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>C:\Program Files\Microsoft SQL Server&lt;instance name&gt;\MSSQL\Bin\Sqlservr.exe</td>
<td>SQL Server &lt;instance name&gt;</td>
</tr>
<tr>
<td>Retail Store Connect (if installed)</td>
<td>C:\Program Files\Microsoft Dynamics AX\50\Retail Store Connect\bin\Dbserver.exe</td>
<td>Retail Store Connect</td>
</tr>
<tr>
<td>Retail Transaction Service (if installed)</td>
<td>C:\Program Files\Microsoft Dynamics AX\50\Retail Transaction Service\RetailTransactionService.exe</td>
<td>Retail Transaction Service</td>
</tr>
</tbody>
</table>

**Note**

On a 64-bit operating system, Retail Store Connect and Retail Transaction Service will be in the Program Files (x86) folder path instead.
1. Log on to the computer as a Windows Administrator.
2. Click **Start**, and then, in the search box, type `wf.msc` 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 XP or POSReady 2009**
1. Log on to the computer as a Windows Administrator.
2. Click **Start**, and then click **Control Panel**.
3. If needed, 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 for other the other programs that should be allowed through the firewall, and then click **OK**.

**At the head office: Set up the password policy**

PCI Data Security Standard Requirement 8.5.8 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 set out in the following table.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Security setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>4 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>90 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>7 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Account lockout duration</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Account lockout threshold</td>
<td>6 invalid logon attempts</td>
</tr>
</tbody>
</table>

**Note**
- Users of Microsoft Dynamics AX for Retail Headquarters, as users of Microsoft Dynamics AX, are subject to Active Directory security policies. This means that Retail Headquarters users are subject to the same password policy as domain users.
- Installing Retail Headquarters 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.
At the head office: Set up database logging

By modifying the audit trail in Microsoft Dynamics AX 2009, 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 SysDatabaseLogTableSetup table for the head office and in the POSFunctionalityProfile table for Retail POS.
- **Changes to the payment processing configuration.** These settings are stored in the POSHardwareProfile table.
- **Creation, deletion, or modification of cashier user accounts and permissions.** These settings are stored in the RBOStaffPermissionGroup and RBOStaffTable tables.

**Note**

While logging of activity on the head-office database is related to requirements 10.2 and 10.3 of the PCI Data Security Standard, doing so is beyond the scope of the PCI requirements because, in an implementation of Microsoft Dynamics AX for Retail that uses the integrated payment solution from Microsoft Dynamics Online, no cardholder data is stored and users cannot change the cardholder data flow or the security of cardholder data. The following procedure is therefore included in this document as an optional best practice that will help to make organizational data more secure.

1. To set up logging in the head-office database, click Administration > Setup > Life science electronic signature audit trail.
2. Create the following new entries.

<table>
<thead>
<tr>
<th>Domain ID</th>
<th>System name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>POSFunctionalityProfile</td>
</tr>
<tr>
<td>Admin</td>
<td>POSHardwareProfile</td>
</tr>
<tr>
<td>Admin</td>
<td>RBOStaffLoginLog</td>
</tr>
<tr>
<td>Admin</td>
<td>RBOStaffPermissionGroup</td>
</tr>
<tr>
<td>Admin</td>
<td>RBOStaffTable</td>
</tr>
<tr>
<td>Admin</td>
<td>SysDatabaseLogTableSetup</td>
</tr>
</tbody>
</table>

When you select the system name, the name of each table is automatically filled in to the Name of table column.

3. Click Administration > Setup > System > Configuration.
4. 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 Administration > Setup > Database log.
- 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 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 Retail Headquarters activity later in this guide.

At the head office: Enable SQL Server trace logging

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

Note

- AxRetailTrace.sql is included in the Retail Headquarters download package and can be located in the RetailSecurityGroups subfolder of the folder where you extracted the installation files.
- While 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 for Retail that uses the integrated payment solution from Microsoft Dynamics Online, no cardholder data is stored and users cannot change the cardholder data flow or the security of cardholder data. The following procedure is therefore included in this document as an optional best practice that will help to 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 being 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 will be located in the Log directory for the instance. SQL Server 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 4: Audit logging later in this guide.
- In a commented section at the end of the script file, AxRetailTrace.sql 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

With Microsoft Dynamics AX for Retail, 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 Microsoft Dynamics AX for Retail POS to the processor at that time, and transactions are settled immediately.

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

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

1. Obtain a Payment Services for Microsoft Dynamics AX subscription from Microsoft Dynamics Online and associate it with the retail organization's merchant account. For more information and instructions, refer to this Web site: http://go.microsoft.com/fwlink/?LinkId=188806
2. Modify hardware profiles to configure payment processing and support hardware devices, such as receipt printers, magnetic stripe readers (MSR), and personal identification number (PIN) pad devices.
3. Associate a hardware profile with each register to enable payment processing and 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 for Retail to process the payments that are subject to the PCI Data Security Standard. The steps are described in more detail later in this section.

• With Payment Services for Microsoft Dynamics AX, 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 shipped in the United States and Canada, the only processor that Microsoft Dynamics AX for Retail communicates with is Payment Services for Microsoft Dynamics AX. This communication is configured in Retail Headquarters, 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 for Retail has been validated for PCI compliance only with Payment Services for Microsoft Dynamics AX. If you intend to use Microsoft Dynamics AX for Retail with another payment solution, you must obtain separate compliance validation.
Configure payment processing and set up devices in Retail Headquarters

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 Headquarters > Setup > POS > Hardware Profiles.
2. On the Overview tab, select the correct profile.
3. On the EFT Service tab, enter the information provided by Dynamics Online.
4. On the tab for each device, select OPOS, and then, in the Device name box, type the appropriate device name. Typing a description for the device is optional.
5. On the toolbar, click Save.

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 in use at the stores. Similarly, if like devices are named differently on different registers or at different stores, you must have additional hardware profiles.

Enable payment processing and select devices for specific registers

This is done by associating the hardware profile with each register.

1. Click Retail Headquarters > Setup > Store > POS Terminals.
2. On the Overview tab, select the register that you want to modify.
3. On the General tab, select the appropriate profile in the Hardware profile box, and 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. On the toolbar, click Save, and then repeat for other registers. When you have finished associating hardware profiles with registers, close the window.

Set up tender types for payment processing

Tender types 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 under a card tender type. For more information about the steps in this topic, see "Tender types" in the Retail Headquarters User's Guide.

1. Click Retail Headquarters > Setup > Tender types > Tender types.
2. On the toolbar, click the New button.
3. In the new row, type a unique number and description for the new tender type, and then, in the Default function column, click the arrow and select Card.

4. On the toolbar, click Save, and then close the window.

5. Click Retail Headquarters > Setup > Tender types > Card types.

6. On the toolbar, click the New button.

7. In the new row, type a unique ID and name for the new card type, and then, in the Card types column, click the arrow and select the appropriate option.

8. With the new row still selected, click the Card number button.

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 being accepted under the Visa card type are in fact Visa cards by creating a mask of 4.

10. On the toolbar of the Card number window, click Save, and then close the window.

11. On the toolbar of the Card type window, click Save, and then close the window.

Enable tender types and card types for specific stores
1. Click Retail Headquarters > Setup > Store > Stores.

2. Select the store you want, click Setup, and then click Tender types.

3. On the toolbar, click New, and then, in the new row, click the arrow in the Tender type column and select the tender type that you want. The information for the selected tender type fills in automatically.

4. With the new tender type row still selected, click Setup, and then click Card setup.

5. On the toolbar, click New, and then, in the new row, click the arrow in the Card ID column and select the card type for this tender type.

6. With the new card setup selected, click the General tab, and then select the Check expiration date check box.

7. On the toolbar of the Card setup window, click Save, and then close the window.

8. On the toolbar of the Tender type window, click Save, and then close the window.

9. Repeat steps 3 through 8 for any other tender types for this store.

10. On the toolbar of the Store window, click Save, and then close the window.

Turn on payment processing at 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 scheduler > Periodic > Actions > Preactions > Functions > Create actions. This converts the preactions (generated when you changed the payment processing settings) into actions, or jobs.

2. Click Retail scheduler > Common Forms > Scheduler job.

3. To send down the payment processing and device settings in the hardware profile, select the A-1090 Terminals job, click Functions, and then click Run scheduler job directly.

4. To send down the tender types, card types, and card numbers, select the A-1070 Stores and tenders job, click Functions, 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.

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

Store computers: Set up the password policy
Requirements 8.5.9 through 8.5.14 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 be set up to meet the minimum requirements set out in the following table.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Security setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>4 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>90 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>7 characters</td>
</tr>
<tr>
<td>Password must meet complexity require</td>
<td>Enabled</td>
</tr>
<tr>
<td>Account lockout duration</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Account lockout threshold</td>
<td>6 invalid logon attempts</td>
</tr>
</tbody>
</table>

Note
- These policies represent the minimum requirements of Requirements 8.5.9 through 8.5.14. More stringent settings can be used.
- For additional information about setting up a Windows account for each store user, see the Deployment and Installation Guide.

1. If you are running Windows XP, Windows Vista, or 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 into 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 screensavers

At each register, set up a screensaver that (1) comes on when the register has been idle, and (2) requires the password for the cashier's Windows user account to be entered in order to regain access to Retail POS.

1. In the C:\Windows\System32 folder, locate the name of the screen saver (.scr) file that you want to use.
2. If you are running Windows XP, Windows Vista, or POSReady 2009, click Start, click Run, type mmc, and then click OK.
   If you are running Windows 7, click Start, type mmc into the search box, and then press ENTER.
3. On the File menu, click Add/Remove Snap-in, and then, if you are running Windows XP, 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 (in Windows 7) or Display (in other operating systems).
6. Double-click Force specific screen saver (in Windows 7) or Screen Saver executable name (in other operating systems), select Enabled, type the path and name for 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 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. 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 period if you prefer.

Store computers: Turn off System Restore

System Restore is a Windows feature that restores your computer’s system files to 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 in 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 Vista
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.

Turn off System Restore on Windows XP or 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 discusses some of the features in Microsoft Dynamics AX for Retail 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, no access to reports, and no access to card numbers except when they swipe a card.

Users of Retail Headquarters, as users of Microsoft Dynamics AX, are subject to Active Directory security policies. This means that Retail Headquarters users are subject to the same password policy as domain users.

Employee user names and passwords are set up in Microsoft Dynamics AX for Retail Headquarters. Only approved Microsoft Dynamics AX users have access to these features.

Microsoft Dynamics AX for Retail 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. These features help to 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 Retail Headquarters 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 Retail Headquarters by means of 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 Basic > Common Forms > Employee Details.
2. Click New.
3. In the new row, type a unique identifier and name for the employee, and then select Sales in the User Profile column.
4. With the new employee still selected, switch to the General tab and select the Retail check box.
5. Enter other information about this employee on other tabs as needed, and then click the Retail button.
6. On the **General** tab of the **Staff** window, type a name in the **Name on receipt** box.

7. On the **Personal** tab, type the employee's password.

8. On the **Privileges** tab, select the appropriate **Staff permission group**.

9. On the toolbar, click **Save**, and then close the **Staff** window.

---

**Important**

When setting up Windows user accounts for employees and when setting up employee accounts in Retail Headquarters, you must use a "least privilege" approach, granting to employees only those privileges required for them to perform their duties. For example, while trusted management personnel might need to have Administrator privileges on store computers, employee logon accounts must belong to a group that does not. This helps you to 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 *Deployment and Installation Guide*.

---

**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.

Microsoft Dynamics AX for Retail helps merchants to 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 to 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 receipts (both printed and journaled) are always truncated.
- As with this release of Microsoft Dynamics AX for Retail, the previous release did not retain any sensitive authentication data; removal of historical data to comply with Requirement 3.2 of the PCI Data Security Standard is not necessary.
- Because cardholder data is not retained, no encryption is required. This means that there is no need to periodically delete the encryption key. This helps to satisfy Requirement 3.6 of the PCI Data Security Standard.
Data transmissions

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

Microsoft Dynamics AX for Retail 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.

Flow of payment data

The flow of payment data in the Retail POS system is shown in Figure 1.
Part 3: Connection limitations

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

Wireless connections
Microsoft Dynamics AX for Retail does not require or support wireless connections, and we do not recommend using wireless connections with Microsoft Dynamics AX for Retail. 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 for Retail, 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 Simple Network Management Protocol (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 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 for Retail 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 (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 PCI Data Security Standard Requirement 8.
- Enable encrypted data transmission according to PCI Data Security Standard Requirement 4.1.
- Enable account lockout after a certain number of failed logon 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.

Non-console administrative access

Non-console administrative access to Microsoft Dynamics AX for Retail 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 Data Security Standard.
Part 4: Audit logging

In order to comply with Requirement 10 of the PCI Data Security Standard, logging must be enabled as described in the following topics 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 Retail Headquarters activity

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

Note

While the procedures in this topic 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 for Retail that uses the integrated payment solution from Microsoft Dynamics Online, no cardholder data is stored and users cannot change the cardholder data flow or the security of cardholder data. The following procedures are therefore included in this document as optional best practices that will help to make organizational data more secure.

View information about user logon and user logoff

View the user log in Microsoft Dynamics AX 2009 to see logon information for each authorized user.

1. Click Administration > Inquiries > 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 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 2009 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 Administration > Inquiries > Database log.

2. Select the record that you want to view, and then click the History tab.
View the SQL Server trace log files

Monitor the SQL Server trace log files to see what users accessed the log files. Each entry in the trace log file includes the user that logged 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), 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.

   ```sql
   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. The typical path to 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:

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

   √ Note
   The logging level can only be modified 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 Headquarters > Setup > POS > 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 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 for Retail system. Windows user logon and logoff events and 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.

The event log also shows initialization of the log file in Microsoft Dynamics AX 2009. This is indicated by the event for 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 XP or 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 Vista, or Windows Server 2008, click Start, type Event Viewer into the search box, and then press ENTER.

2. 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 table on the next page 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 the Event Viewer:

- The Windows user account that was involved in the operation
- 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
<table>
<thead>
<tr>
<th>Operation</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon attempt</td>
<td>4776</td>
</tr>
<tr>
<td>Logon success</td>
<td>4624</td>
</tr>
<tr>
<td>Logon failure</td>
<td>529, 535, 539</td>
</tr>
<tr>
<td>Logoff</td>
<td>538</td>
</tr>
<tr>
<td>User password reset</td>
<td>4724</td>
</tr>
<tr>
<td>User account created</td>
<td>4720</td>
</tr>
<tr>
<td>User account disabled</td>
<td>4725</td>
</tr>
<tr>
<td>User account deleted</td>
<td>4726</td>
</tr>
<tr>
<td>User account added</td>
<td>4728</td>
</tr>
<tr>
<td>User account changed</td>
<td>4738</td>
</tr>
<tr>
<td>User account locked out</td>
<td>4740</td>
</tr>
<tr>
<td>Member added to user group</td>
<td>4732</td>
</tr>
<tr>
<td>Member removed from user group</td>
<td>4733</td>
</tr>
<tr>
<td>Object access (update or deletion of monitored files)</td>
<td>---</td>
</tr>
<tr>
<td>File modified and saved</td>
<td>4663</td>
</tr>
<tr>
<td>Audit policy changed</td>
<td>---</td>
</tr>
<tr>
<td>Domain policy changed</td>
<td>4739</td>
</tr>
<tr>
<td>Event Viewer Security log cleared</td>
<td>1102</td>
</tr>
</tbody>
</table>

Windows Vista
Windows 7, Windows Server 2008
Windows XP
---
560
567
612
643
517
Part 5: Software updates and support

Software updates

Updates to Microsoft Dynamics AX for Retail 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. 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 for Retail 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 to 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 for Retail 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.
- Secure deletion of such data immediately after use.
- Encryption of sensitive authentication data while stored. (No sensitive data is stored by Microsoft Dynamics AX for Retail; 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 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 (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, available for download at http://www.microsoft.com/downloads.

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. 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. 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 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 Microsoft’s secure 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 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.
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.
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.
- In "All computers: Set up auditing of file access, object access, and audit-policy changes", the note at the beginning of has been modified to show that completing the procedures in that section is required, and the words "less stringent" have been added to the second bullet 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" that points out that System Restore is not available in Windows Server 2008.
- The diagram in the "Flow of payment data" has been updated to include the flow of the response code from Microsoft Dynamics Online to the Retail POS database.
- Minor editorial changes have been made.