Microsoft Dynamics™

Implementation Guide for PCI Compliance

Microsoft Dynamics® RMS

November 2013

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 website 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

Important

This guide applies to Microsoft Dynamics RMS 2.0 Cumulative Update 5.

If you accept credit card payments in your store, you are required to comply with the Payment Card Industry (PCI) Data Security Standard. This standard was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International. It sets out twelve requirements that merchants must meet in order to protect cardholder information.

In October 2013, Microsoft Dynamics RMS was validated by a Payment Application Qualified Security Assessor. To view the list of validated applications, see https://www.pcisecuritystandards.org/security_standards/vpa/.

Important

Integration with TSYS, Microsoft Dynamics Online, and the Microsoft Dynamics Online Payment Connector are the only payment solutions that have been validated for PCI DSS compliance. Other payment processors have not been validated.

In this guide, we'll discuss ways that Microsoft Dynamics Retail Management System (RMS) can help stores comply with the standard, and we'll set out some specific responsibilities that store owners must meet in order to make a Microsoft Dynamics RMS system compliant with the standard.

Note

This guide is not intended to replace or stand in place of the PCI Data Security Standard and must not be exclusively relied upon to comply with the standard or with other requirements set out by your bank. Microsoft strongly recommends reviewing the full text of the PCI Data Security Standard, available at https://www.pcisecuritystandards.org/.

Microsoft also strongly recommends implementing Microsoft Dynamics RMS into a secure environment and according to the recommendations in this guide. Keep in mind that the use of Microsoft Dynamics RMS alone is not enough to comply with the PCI Data Security Standard.

Updates to this guide

This guide is reviewed annually, whenever a service pack, cumulative update, or hotfix for Microsoft Dynamics RMS is released, and whenever an update to one of the Data Security Standards is released. Make sure you have the most up-to-date copy of this guide, available at http://go.microsoft.com/fwlink/?LinkID=111473&clcid=0x409.

For more information

Microsoft provides training materials to our partners, resellers, and integrators to help ensure that they can implement Microsoft Dynamics RMS 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=207811 (PartnerSource login required).

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

About Microsoft Dynamics RMS

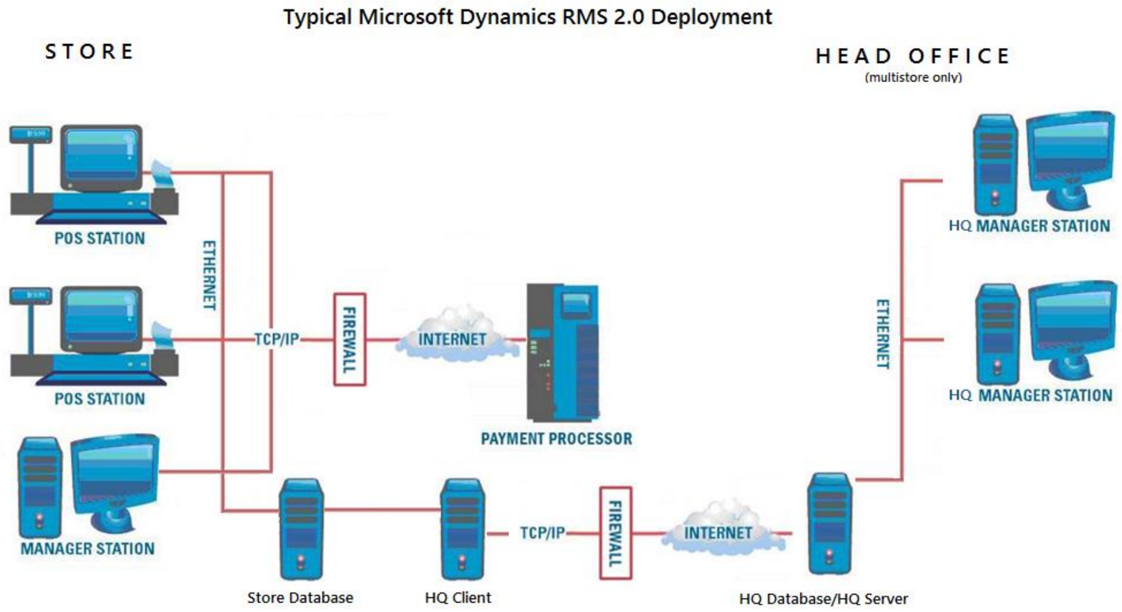
With integrated payment processing, Microsoft Dynamics RMS is considered a payment application. Credit card industry guidelines for the development of payment applications—such as the guidelines set out in the PCI Payment Application Data Security Standard (PCI PA-DSS)—are intended to promote more secure payment applications and, in turn, facilitate merchant compliance with the PCI Data Security Standard (PCI DSS). Payment applications that have been validated against these development standards minimize the potential for security breaches that lead to fraudulent card use.

Both the PCI PA-DSS and the PCI DSS were used as guidelines during the development and testing of Microsoft Dynamics RMS. A qualified security assessor validated the software prior to its release.

Note

Download the PCI DSS from this website: https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml.

The following diagram shows a typical implementation of Microsoft Dynamics RMS.



How Microsoft Dynamics RMS helps with compliance

To help our customers comply with the PCI Data Security Standard, and to pass the PCI payment application audit, Microsoft implemented the following features and security measures in Microsoft Dynamics RMS:

- Full magnetic stripe or CVV2 data is not retained. Microsoft Dynamics RMS does not store sensitive authentication data subsequent to authorization, PIN numbers and card validation codes are never stored, and account numbers are either masked, encrypted, or both. Beyond the time they have the customer's actual card in hand, store employees do not ever have access to customer card numbers. Cardholder data is securely purged from the database as each batch is settled (typically, daily).
- Historical cardholder data (including magnetic stripe data, card validation codes, PINs, and PIN blocks) that was stored by previous releases of Microsoft Dynamics RMS is securely deleted when the database is upgraded to the latest release. This removal is absolutely necessary for PCI DSS compliance.
- Encryption keys can be replaced regularly, and old keys are not retained. For more information about encryption, see “Reset the encryption key” later in this guide.
- You must create a unique user account (employee ID and password) for each employee of the store. An employee cannot use Microsoft Dynamics RMS without a user account, and these user accounts are subject to the password policy you have established in Microsoft Dynamics RMS. For more information, see "Set up a password policy" later in this guide.
- Microsoft Dynamics RMS maintains event logs that record each time an employee logs on to Microsoft Dynamics; cashier creation, deletion, and security rights changes; and transaction access, settlement, printing, and deletion from the store database. For more information about event logging, see “Monitoring employee activities using logs and reports” in "Monitoring" later in this guide.
- Microsoft Dynamics RMS was developed using industry best practices, with emphasis on information security throughout the development lifecycle, and according to Microsoft's rigorous internal security guidelines. Thorough testing of all security and configuration features was performed.
- Microsoft does not support the use of wireless connections for Microsoft Dynamics RMS database communication. If you choose to use a wireless connection in spite of this restriction, see the information about increasing the security of wireless connections in "General requirements" later in this guide.
- Microsoft Dynamics RMS and its component software were thoroughly tested for known security vulnerabilities. As new vulnerabilities are discovered, Microsoft is committed to responding promptly with security patches, upgrades, or other solutions.
- Any security patches or other updates that become available for Microsoft Dynamics RMS will be offered for download rather than being provided via remote access to the store network. Updates will only be downloaded and installed at your request. Additionally, updates are available only via a password-protected website.
- You can implement Microsoft Dynamics RMS into a secure network environment. The program will not interfere with network address translation (NAT), port address translation (PAT), traffic filtering network devices, antivirus protection, patch or update installation, or the use of encryption.

- Microsoft Dynamics RMS does not provide Internet access to stored cardholder data, and it does not require placement of the store database either on a Web server or in the "demilitarized zone" (DMZ) with the Web server.
- Microsoft Dynamics RMS does not enable remote access.
- In accordance with PCI DSS Requirement 4.1, transmissions of cardholder data over public networks and the Internet are encrypted using Secure Sockets Layer (SSL) 128-bit safeguards.
- Microsoft Dynamics RMS does not allow users to view card numbers or to send cardholder information or PANs via e-mail messages or other end-user messaging technologies.
- Web-based or remote administration, including non-console administration, is not supported by Microsoft Dynamics RMS. If you choose to use remote access or non-console administration in spite of this restriction, see the information about increasing authentication and other security requirements in "General requirements" later in this guide.
- You can set up security—employee by employee—for many of the features in Microsoft Dynamics RMS. For more information, see "Setting up security structure" in Store Operations Online Help.

Software updates and support

Software updates

You must install security hotfixes and service packs as soon as they become available. We also recommend upgrading Internet Explorer and other browsers to the latest versions. For best results, turn on Automatic Updates.

Updates to Microsoft Dynamics RMS 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 RMS 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 RMS 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 RMS; 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 LogMeIn Rescue to access the customer's desktop and investigate the issue directly. LogMeIn Rescue is a remote support solution that gives support engineers access to the merchant’s system, only when authorized by the merchant, in an encrypted session.

The LogMeIn Rescue process looks like this:

1. The support engineer logs into LogMeIn Rescue via secure link, using a unique user name and password, and sets up a new session with a unique personal identification number (PIN) that is provided to the customer.
2. The customer visits the Receive Remote Assistance Support from Microsoft page at http://support.microsoft.com/help, accepts the license terms, and then enters the PIN for their session.
3. If needed, the customer downloads and installs the LogMeIn Rescue applet, and then waits for the support engineer to start the remote control session. The support engineer does not have access to the customer’s computer until the customer specifically accepts the connection. If the customer does not reply within 30 seconds, or if the customer clicks Cancel in the request to connect, the connection is denied. If the customer accepts the connection, a chat window appears on the customer’s computer screen.
4. At the conclusion of the session, or at any time the customer chooses, the customer can stop sharing and terminate the session by closing the chat window by clicking the X close button. After the session is terminated, the support engineer cannot send or receive chat messages and has no access to the customer’s computer. There is no way for the engineer to reestablish the session except by sending a new request.

Support engineers have no ability to obtain unattended access to the customer’s computer; the customer must be present, enter the PIN, and approve the connection. At no point does the support engineer have access to the cards or card data. Likewise, support engineers cannot request or receive files, and screen recording is disabled and cannot be turned on.

Support personnel obtain a copy of the store database

In the rare event when support personnel need to obtain a copy of the store database, the database is transmitted to Microsoft 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

In the event a support engineer travels to the customer’s place of business in order to investigate an issue on-site, 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.

General requirements

In this section, we'll provide some general requirements for complying with the PCI Data Security Standard (PCI DSS).

Important

To ensure that you are fully compliant, read and implement the entire list of requirements in the PCI DSS. The standard includes very detailed and specific rules for merchants. It is available at https://www.pcisecuritystandards.org.

You must:

- Prohibit the use of default administrative accounts.
- Prevent the use of group, shared, and generic accounts. PCI DSS Requirement 8.5.8 provides test procedures for verifying this.
- Require cashiers to log on to Windows using an account that does not have administrator access. For more information about setting up standard user accounts for your employees, search for "user accounts" in Windows Help.
- Control access to any PCs, servers, and databases that house payment applications and cardholder data by using unique user IDs and PCI DSS-compliant secure authentication. Assign secure authentication for payment applications and systems whenever possible.
- Control access to Microsoft Dynamics RMS and your store data by assigning a unique employee ID and password to each employee. Do not allow employees to share IDs or passwords. For more information, see "Managing cashier information" and "Changing an employee password" in Store Operations Online Help. Changing “out of the box” installation settings for unique user IDs and secure authentication will result in noncompliance with the PCI DSS.
- Use the preferred-acquirer solution for payment processing.

  Important

  Integration with TSYS and Microsoft Dynamics Online are the only payment solutions that have been validated for PCI DSS compliance. Other payment processors—including ICVerify for Windows, PC-Charge, Atomic Authorizer, and WinTI/European EFT—have not been validated.
- Install Internet Explorer 8.0 or later.

  Note

  In order to use the payment processing features in Microsoft Dynamics RMS, you must have Internet Explorer installed on your computer. In order to be compliant with the PCI DSS, you must have at least Internet Explorer 7.0.
- Perform regular audits and spot-checks of employee activities and program access, as described in “Monitoring” later in this guide.
- If you choose to use remote access despite the fact that remote access is not supported by Microsoft Dynamics RMS, you must use two-factor authentication (user ID and password and an additional authentication item such as a smart card, token, or PIN). You must also adhere to the following remote access security requirements:
  - Change default settings in the remote access software (for example, change default passwords and use unique passwords for each merchant).
  - Allow connections only from specific (known) IP/MAC addresses.

  - Use strong authentication and complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15.
  - Enable encrypted data transmission according to PCI DSS Requirement 4.1.
  - Enable account lockout after a certain number of failed login attempts according to PCI DSS 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 the logging function.
  - Restrict access to merchant passwords to authorized reseller/integrator personnel.
  - Establish merchant passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

  If you fail to use two-factor authentication or to adhere to the security features described above, your system is noncompliant.

- If you choose to use wireless connections despite the fact that these connections are not supported for Microsoft Dynamics RMS database communications, make sure you are doing so in accordance with PCI requirements. You must:
  - Install a firewall between any wireless networks and systems that store cardholder data, and configure the firewall to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
  - Ensure that all wireless networks implement strong encryption mechanisms (for example, AES).
  - Use WPA/WPA2. Do not use WEP. (WEP has been prohibited for new wireless implementations since March 31, 2009, and for current wireless implementations since June 30, 2010.)
  - Update firmware on wireless devices to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2).
  - Change the defaults on your wireless modem or router. These defaults might include (but are not limited to) the encryption keys, default service set identifier (SSID), passwords or passphrases on access points, SNMP community strings, or other settings. The encryption keys must also be changed whenever anyone with knowledge of the keys leaves the company or changes positions.
- If you choose to use non-console administration despite the fact that this is not supported by Microsoft Dynamics RMS, you must use SSH, VPN, or SSL/TLS for encryption of non-console administrative access. If you do not, your system is noncompliant.
- If you download orders from the web to Microsoft Dynamics RMS, causing orders (XML files) to be directly imported into the Exchange Table in the Microsoft Dynamics RMS database that contain unencrypted cardholder data, you must securely delete these credit card numbers after the transactions have been settled. To be compliant with the PCI DSS, unencrypted credit card numbers cannot be stored.
- Refrain from storing cardholder data on servers or computers that are connected to the Internet.

  Note

  The PCI DSS recommends the use of a dedicated database computer. Microsoft facilitates this by allowing you to install an extra copy of Microsoft Dynamics RMS—at no additional charge—on a back-office computer that will not be used to process sales transactions.
- Complete all setup requirements detailed in the remainder of this guide.

Headquarters Client setup requirements

In a multistore environment, the instance of Headquarters Client deployed at each store must be in the DMZ. It cannot be installed on the same computer where a Microsoft Dynamics RMS database is hosted.

SQL Server setup requirements

This section provides the SQL Server 2008 and SQL Server 2005 setup steps that are required for PCI compliance.

Important

You must use a new instance for Microsoft Dynamics RMS. Use of an existing instance could compromise PCI compliance.

You must complete **all** of the following procedures on the SQL Server computer. In some cases, you might discover that the desired settings are already in place, but you need to confirm this.

Switch to mixed-mode server authentication

1. In SQL Server Management Studio, right-click the instance being used by Microsoft Dynamics RMS, and then click **Properties**.
2. On the **Security** page, under **Server authentication**, select **SQL Server and Windows Authentication** mode, and then click **OK**.

Manage SQL Server without using the “sa” account

Note

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

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

Enable C2 auditing

1. In SQL Server Management Studio, right-click the correct instance, and then click **Properties**.
2. In the **Server Properties** window, click **Security**.
3. Under **Login auditing**, select **Both failed and successful logins**.
4. Under **Options**, select **Enable C2 audit tracing**.
5. Click **OK**.
6. Right-click the instance and click **Stop**, and then right-click the instance and click **Start**.

Select the service account

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

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

1. In SQL Server Configuration Manager, expand SQL Server Network Configuration.
2. Click Protocols for <instance name>.
3. Right-click **Shared memory**, and then click **Enable**.
4. Right-click **TCP/IP**, and then click **Enable**.
5. Right-click **TCP/IP**, and then click **Properties**.
6. On the **IP Addresses** tab, under **IPAll**, set **TCP Port** to 1433, and then click **OK**.

Note

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

Force encryption of database communications

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

Note

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

Restart the SQL server and put your changes into effect

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

Set access policies

Set policies to manage access to store computers and to the Microsoft Dynamics RMS Store Operations software. Complete the following tasks on each computer where Store Operations is installed:

- Disable the local Administrator account
- Set up a password policy for Windows users
- Set up a password policy for employees
- Modify the manifest file for Store Operations POS

Disable the local Administrator account

To run Store Operations Administrator, the person who is logged on to Windows must be a member of the Administrators users group on the local computer. The built-in Administrator account must never be used for this purpose.

Note

Before completing this procedure, confirm that at least one user is a member of the Administrators group.

1. In Control Panel, click or double-click **Administrative Tools**, and then double-click **Local Security Policy**.
2. In the **Users** folder, double-click the **Administrator** account.

Note

If the **Users** folder is not present, you need to open **Local Users and Groups** instead. Click **Start**, click **Settings**, and type “local users”, and then click **Edit local users and groups**.

3. If it is not already selected, select the **Account is disabled** check box, and then click **OK**.

Set up a password policy for Windows users

Requirements 8.5.9 through 8.5.14 specify password and account security regulations for people with administrative access to the payment application. You can meet these requirements by establishing a password policy for Windows users. Policy settings that meet the requirements are set out 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.
- Periodically check the PCI Data Security Standard for the latest password requirements.

Set up a domain password policy

If you are running Store Operations on a domain, contact the domain administrator to establish group policies for the domain. 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.

Set up a local password policy

If you are running Store Operations in a workgroup, you must complete the following procedure on each computer in the network.

1. In Control Panel, click or double-click **Administrative Tools**, and then double-click **Local Security Policy**.
2. Expand the **Account Policies** folder, and then change the settings under **Password Policy** and **Account Lockout Policy** as needed to meet the requirements in the table above.

Set up a password policy for employees

Store employees using Microsoft Dynamics RMS have access to credit card data only when they are swiping credit cards. For that reason, the employee passwords within Microsoft Dynamics RMS are out of scope for PCI DSS compliance. As a best practice, however, you can use Store Operations Administrator to set up a password policy for your registers, similar to the Windows password policy that you are required to set up (as described in the previous section).

1. Open Store Operations Administrator.
2. On the **Database** menu, click **Password Policy Settings**.
3. In the **Password Policy Settings** dialog box, select all six of the check boxes.
4. Enter the values shown in the following table, or specify more stringent requirements.

Setting name	Recommended value
Maximum age of passwords (days)	90
Number of passwords to save	4
Failed logon attempts allowed	5

Lockout period (minutes)	30
Minimum password length	7

5. Click **OK**.

   For more information about the settings in the **Password Policy Settings** dialog box, click the **Help** button in the dialog box.

Note

Except for password expiration and account lockout, the password policy takes effect the next time an employee changes his or her password. To force employees to change their passwords soon and become compliant with the policy, select the **Passwords expire periodically** check box and set a low maximum password age. Password age is calculated from the date when the password was last changed.

Modify the manifest file for Store Operations POS

The manifest file controls the user context that Store Operations POS runs under. To comply with the PCI DSS, you must modify the default setting in this file. The file is named SOPOSUser.exe.manifest, and it is located in the installation folder (by default, C:\Program Files\Microsoft Retail Management System\Store Operations).

1. Activate and register Store Operations POS, and then close Store Operations POS.
2. In the folder where Store operations is installed, locate the SOPOSUser.exe.manifest file, and then open it in Notepad or another text editor.
3. Change the **requestedExecutionLevel** parameter to **AsInvoker**, so that it looks like this:

   ```
   <requestedExecutionLevel level="AsInvoker"></requestedExecutionLevel>
   ```

4. Save and close the manifest file. You might need to save it to another location and then copy it back into the install folder, overwriting the copy that is there.

Turn off System Restore

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

Note

System Restore is not available in Windows Server operating systems.

Turn off System Restore on Windows 8

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

Turn off System Restore on Windows 7 or POSReady 7

4. On the **Start** menu, right-click **Computer**, and then click **Properties**.
5. Click **System protection**.
6. Select the C: drive, click **Configure**, select **Turn off system protection**, 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**.

Disable the Volume Shadow Copy service

Volume Shadow Copy service is a Windows service that can be used to create backup files on a server that is used as a file server. To avoid capturing backup images that contain card data, this service should be disabled on all machines where Microsoft Dynamics RMS is installed. The service is disabled by default on most operating systems.

Disable the service in Windows Small Business Server 2011

1. In Control Panel, click or double-click **Administrative Tools**, click **Computer Management**, and then click **Disk Management**.
2. Right-click the hard disk, and then click **Properties**.
3. On the **Shadow Copies** tab, select the drive, click **Disable**, and then click **Yes** to confirm the change.

Confirm that the service is disabled in other operating systems

1. Click **Start**, and then type **services.msc**.
2. In the list of services, locate the Volume Shadow Copy service.
3. If the service is running, right-click the service, and then click **Stop**.
4. If the **Startup Type** is not already set to **Manual**, right-click the service, click **Properties**, and then specify **Manual** in the **Startup type** box.

Disable browser recovery features

Some Internet browsers offer features for recovering loaded web pages in the event of an application crash. To avoid capturing card requests sent over the Internet, disable these features on every computer where Microsoft Dynamics RMS is installed.

1. In Internet Explorer, click the **Tools** ⚙ button, and then click **Internet Options**.
2. On the **Advanced** tab, scroll down to the **Browsing** settings.
3. Clear the **Enable automatic crash recovery** check box, and then click **OK**.

Note

If you are using another browser, your steps will vary.

Reset the encryption key

Encryption keys from previous releases of Microsoft Dynamics RMS are securely deleted when the database is upgraded to the most recent release. The current encryption key is not visible to employees, is itself stored in encrypted format, and cannot be distributed.

You must periodically reset the encryption key for the store database. Reset the encryption key at least once a year, any time a key is known or suspected to be compromised, or any time an employee with knowledge of the key leaves the company or changes positions. When you reset the key by using the New Encryption Key feature in Store Operations Administrator, the old encryption key is securely deleted and replaced by a new key. Only database administrators can reset the encryption key.

Removal of old encryption keys is absolutely necessary for PCI compliance but happens automatically with Microsoft Dynamics RMS.

To set a new encryption key, complete the following procedure.

1. Bring all registers out of offline mode.
2. Settle all transactions.
3. Open Store Operations Administrator and connect to the database server.
4. On the **Database** menu, click **New Encryption Key**.
5. If you are ready to proceed, click **Yes**.
6. Run a Z report on every register to synchronize the offline databases with the new encryption key.

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 user account to be entered in order to regain access to Store Operations POS.

1. In the C:\Windows\System32 folder, locate the name of the screen saver (.scr) file that you want to use.
2. 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** or **Screen Saver executable name** (depending on your operating system), 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.

Verify digital signatures

Confirm that the binary files for Microsoft Dynamics RMS Store Operations have been digitally signed by Microsoft. The binary files for Store Operations are:

- SOADMIN.exe
- SOMANAGER.exe
- SOPOSUSER.exe
- QSRules.dll

Complete the following procedure for each of the files listed above.

1. In Windows Explorer, open the Store Operations installation folder. The default path to the installation folder is C:\Program Files\Microsoft Dynamics RMS or, on a 64-bit computer, C:\Program Files (x86)\Microsoft Retail Management System.
2. Right-click the file name, and then click **Properties**.
3. On the **Digital Signatures** tab, verify that **Microsoft Corporation** appears in the **Name of signer** column.

Monitoring

Important

Disabling or failing to enable the monitoring, auditing, and logging mechanisms described in this section will result in noncompliance with the PCI DSS.

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. Click **Start**, type **Event Viewer** into the search box, and then press ENTER.
2. If available, expand the **Windows Logs** folder
3. Right-click **Security**, and then click **Properties**.
4. In the **Maximum log size** box, type 102400.
5. Select **Overwrite events as needed**, and then click **OK**.

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

- For domain computers, work with the domain administrator to ensure that local audit policies are not overwritten by domain policies.
- For information about viewing and managing log files, see "Monitor event logs" later in this section.

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

1. In Control Panel, click or double-click **Administrative Tools**, and then double-click **Local Security Policy**.
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 newer operating systems:

- C:\Windows\System32\winevt\Logs
- The folder where Microsoft Dynamics RMS is installed (by default, C:\Program Files\Microsoft Dynamics RMS or, on a 64-bit computer, C:\Program Files (x86)\Microsoft Dynamics Retail Management System)
- The Microsoft® SQL Server® data directory (by default, C:\Program Files\Microsoft SQL Server\<*version*>\<*instance name*>\MSSQL\Log)

For Windows XP and POSReady 2009:

- C:\Windows\System32\config
- The folder where Microsoft Dynamics RMS is installed (by default, C:\Program Files\Microsoft Dynamics RMS)
- 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**.
2. On the **Security** tab, click **Advanced**.

   Note

   If the **Security** tab is not available, click **Cancel**, 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**, and then, if available, click **Select a principal**.
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** or **Applies to** box, make sure that **This folder, subfolders and files** is selected.
8. If available, click **Show advanced**.
9. In the list of permissions, select the checkboxes for the following privileges. If available, select both the **Successful** and **Failed** check boxes.
   - Create files/write data
   - Create folders/append data
   - Delete subfolders and files
   - Delete
   - Read permissions
   - Change permissions
10. Click **OK**.
11. If the above settings provide more auditing than is otherwise set up for this folder, select the **Replace all existing inheritable auditing entries…** or **Replace all child object auditing entries…** check box, and then click **OK**.
12. Click **OK** in the remaining dialog boxes.
13. Repeat this procedure for the next folder in the list at the start of this topic.

Monitor event logs

You must monitor the event logs on every computer in the Microsoft Dynamics RMS 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.

1. In Control Panel, click or double-click **Administrative Tools**, and then double-click **Event Viewer**.
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

Operation	**Event ID**	
	Most operating systems	**Windows XP**
Logon attempt	4776	680
Logon success	4624	528
Logon failure	529, 535, 539	529, 535, 539
Logoff	538	538
User password reset	4724	628
User account created	4720	624
User account disabled	4725	629
User account deleted	4726	630
User account added	4728	632
User account changed	4738	642
User account locked out	4740	644
Member added to user group	4732	636
Member removed from user group	4733	637
Object access (update or deletion of monitored files)	---	560
File modified and saved	4663	567
Audit policy changed	---	612
Domain policy changed	4739	643
Event Viewer Security log cleared	1102	517

Monitor employee activities using logs and reports

There are a number of tools that will help you monitor employee access to Microsoft Dynamics RMS and your store information.

Tool	Information provided
Cashier Log report	Times and dates of each cashier's access to Store Operations POS.
Manager Login query	Times and dates of each employee's access to Store Operations Manager
Operations Log query	Failed login attempts Cashier creation and deletion Changes to cashier user ID, rights, or security level Batch settlement and outcome Transaction or journal view from Store Operations Manager Journal printing from Store Operations Manager Transaction deletion by database administrator
Credit Card Transaction Detail query	Credit card transactions processed by each employee, with card expiration date and last four digits of card number
Debit Card Transaction Detail query	Debit card transactions processed by each employee, with card expiration date and last four digits of card number

View the Cashier Log

1. On the **Reports** menu in Store Operations Manager, point to **Miscellaneous**, and then click **Cashier Log**.
2. In the **From** and **To** boxes, type the start and end dates for the date range you are interested in, and then click **Change**.
3. Click **OK** to generate the report.

View audit-log information using a database query

1. Click here to download the auditing queries. Save the .zip file to a computer where Store Operations is installed.
2. Open the .zip file and extract the queries to a folder on the computer.
3. On the **File** menu in Store Operations Administrator, click **Connect**, specify database administrator credentials, select the store database, and then click **OK**.

4. On the **File** menu, click **Open**, browse to the folder where you extracted the query files, and then double-click the query that you want to run.

   MgrLogin.sql – Manager Login query

   OpsLog.sql – Operations Log query

   CreditCardDetail.sql – Credit Card Transaction Detail query

   DebitCardDetail.sql – Debit Card Transaction Detail query

5. On the **Query** menu, click **Run**.

About the query results

Descriptions of the results of the four audit-log queries are provided in the following table.

Query	**Description of results**
Manager Login view sample	*Cashier Number*: The login ID of the employee who logged in. *Name*: The employee who logged in. *Register ID*: The register where the login occurred. *Logged In*: The date and time the employee logged in. *Logged Out*: The date and time the employee logged out. *Hours*: The amount of time the employee was logged in. *Rights*: Whether the employee was logged in with manager rights or administrator rights.
Operations Log view sample	*Cashier ID*: The internal database ID of the employee who performed the operation. *Cashier Number*: The login ID of the employee who performed the operation. *Cashier Name*: The employee who performed the operation. *Operation ID*: An internal number associated with the type of operation that was performed. *Operation Performed*: A description of the operation that was performed. *Record ID*: The code or ID of the database record associated with the operation, such as the number of the cashier whose record was modified. *Additional Information*: More details about the operation. Date and Time of Operation: The date and time at which the operation occurred.

Credit Card Transaction Detail view sample	*Cashier Name*: The employee who rang up the sale. *Cashier Number*: The login ID of the employee who rang up the sale. *Description*: The name of the tender type that was used. *Transaction Number*: The number of the transaction within the batch. *Credit Card Number*: The masked number of the credit card used in the transaction. *Expiration Date*: The expiration date of the credit card used in the transaction. *Date and Time of Transaction*: The date and time at which the transaction took place.
Debit Card Transaction Detail view sample	*Cashier Name*: The employee who rang up the sale. *Cashier Number*: The login ID of the employee who rang up the sale. *Description*: The name of the tender type that was used. *Transaction Number*: The number of the transaction within the batch. *Debit Card Number*: The masked number of the debit card used in the transaction. *Expiration Date*: The expiration date of the credit card used in the transaction. *Date and Time of Transaction*: The date and time at which the transaction took place.

Delete audit logs

The PCI Data Security Standard recommends saving audit logs for at least one year. Older logs can be securely deleted periodically to save space in the store database and on the hard drive. For more information, see “Deleting audit logs” in Store Operations Administrator Online Help.

Review C2 audit trace files

The reports and tools described earlier in this section provide most of the assessment trail specified by Requirement 10 of the PCI Data Security Standard. To monitor activities by database administrators, such as the times when an administrator has logged in or viewed the audit log table in the Microsoft Dynamics RMS database, enable SQL Server C2 auditing, as described in “Enable C2 auditing” in “SQL Server setup requirements” earlier in this guide. With C2 auditing turned on, you can monitor actions taken by individuals who have administrative privileges on the database.

Notes

- *C2* refers to a security rating for computer software that was established by the U.S. National Computer Security Center (NCSC). It specifies that individuals must log on with a password, that an audit mechanism must be in place, and that access to audit data must be limited to authorized administrators. C2 auditing does not prevent system attacks, but it is a vital aid in identifying intruders and attacks in progress and diagnosing attack footprints.
- C2 Audit Mode data is saved in a log file in the Data directory for your database. If the audit log file reaches its size limit of 200 megabytes, SQL Server will create a new file, close the old file, and write all new audit records to the new file. This process will continue until the Data directory fills up or auditing is turned off.
- C2 Audit Mode saves a large amount of event information, so the database log file can grow quickly. If the Data directory runs out of space, SQL Server will shut itself down. If auditing is set to start up automatically, you must free up disk space for the audit log before you can restart the instance of SQL Server. When deleting audit logs, keep in mind that the PCI Data Security Standard requires records to be maintained for at least one year.

What to look for in the audit trace file

The C2 auditing in SQL Server captures a lot of information for each audited event, including an account of all grant/revoke/deny access checks and a record of all points where the database owner decided to grant access. View this information by reviewing the audit trace files.

If you are using the other audit tools described earlier in this guide to satisfy most PCI audit requirements, the events you will need to view in the C2 audit trace files are logins by database-administrator logins and views of the Microsoft Dynamics RMS audit log table. Both of these events will show up in the audit trace file as events in the Store Operations Administrator application. The following table shows the statement text to look for to locate these events.

To locate this type of event	Look for statements (TextData) that begin with this text
Logins by administrators	if (object_id('master.dbo.sp_MSSQLDM090_version') is not null)…
Views of the audit log table	select * from AuditLog

Each event will show the SQL user who performed the action.

Review a trace audit file using SQL Server Management Studio

1. In SQL Server Management Studio, connect to the SQL server and database instance.
2. Right-click the instance, and then click **Stop**.
3. On the **File** menu, point to **Open**, and then click **File**.
4. Navigate to the folder where the Microsoft Dynamics RMS data and trace files are located.
5. Use the dates within the file names to locate the trace (.trc) file you want, select it, and then click **Open**.

   The trace file will open in SQL Profiler where you can view event details.
6. When you are done reviewing the trace file, close it, and then right-click the instance and click **Start**.