Microsoft Dynamics AX

PA-DSS implementation guide

This document explains how to implement Microsoft Dynamics AX in a way that complies with the Payment Card Industry (PCI) Data Security Standard version 3.1. It is intended for customers, Microsoft Certified Partners, resellers, and integrators who are deploying Microsoft Dynamics AX in a retail organization where electronic credit card and debit card payments are accepted, and where Microsoft Dynamics AX is used as the payment application.

White paper

June 2016

Send feedback.

www.microsoft.com/dynamics/ax

Contents

PA-DSS implementation guide

The requirements in this guide **must** be followed if you want to implement Microsoft Dynamics AX in a way that is compliant with the Payment Card Industry (PCI) Data Security Standard version 3.1.

Note: Microsoft Dynamics AX includes Microsoft Dynamics AX for Retail.

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

This guide is intended for and disseminated to customers, Microsoft Certified Partners, resellers, and integrators who are deploying Microsoft Dynamics AX in a retail organization where electronic credit card and debit card payments are accepted, and where Microsoft Dynamics AX is used as the payment application. As a payment application, Microsoft Dynamics AX 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 has been validated for PCI compliance only with Payment Services for Microsoft Dynamics ERP. **If you intend to use Microsoft Dynamics AX with another payment solution or modify the out-of-box integrated payment solution, you must obtain separate compliance validation.**

Get the latest release of this guide

This guide is reviewed when a service pack or hotfix that affects payment services for Microsoft Dynamics AX is released, and when an update to one of the Data Security Standards is released. To obtain the most up-to-date copy of this guide, go to http://go.microsoft.com/fwlink/?LinkId=798763.

For more information

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

Part 1: Setup

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

Install the software

To deploy Microsoft Dynamics AX Retail components in a manner that is PCI-compliant, follow the instructions on the Microsoft Dynamics AX Help wiki: http://go.microsoft.com/fwlink/?LinkID=780591.

Important:

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

All computers: Maintain security

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

All computers: Prepare for monitoring of event logs

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

Important: The event logging should not be disabled, and doing so will result in non-compliance with PCI PA-DSS.

1. If you are running Windows 7, Windows Embedded POSReady 7, Windows 8.1, Windows 10, or Windows Server 2012 R2, click **Start**, type **Event Viewer** in the search box, and then press Enter.
2. If the **Windows Logs** folder is available, expand it, right-click **Security**, and then click **Properties**.
3. In the **Maximum log size** field, type **102400**.
4. Select **Overwrite events as needed**, and then click **OK**.

All Windows 10 computers: Disable event log Microsoft-Windows-WinINet-Capture

If you are running Windows 10, you **must** disable event log **WinINet (Microsoft-Windows-WinINet-Capture)** > **Capture/Analytic.**

1. If you are running Windows 10, click **Start**, type **Event Viewer** in the search box, and then press Enter.
2. Expand **Applications and Services Logs** > **Microsoft** > **WinINet (Microsoft-Windows-WinINet-Capture)**, right-click **Capture/Analytic**, and then click **Properties**.

3 In the **Enable logging** field, clear the check box.
4 Click **OK**.

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

All access to PCs, servers, and databases with Microsoft Dynamics AX must be controlled via unique user IDs and PCI PA-DSS–compliant secure authentication.

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

Note:

- In an implementation of Microsoft Dynamics AX, no cardholder data is stored, and users cannot change the flow or security of cardholder data. Nevertheless, you must complete the procedures in this section to comply with Requirements 10.2 and 10.3 of the PCI Data Security Standard, and to help make organizational data more secure.
- For domain computers, work with the domain administrator to ensure that local audit policies are not overwritten by less stringent domain policies.

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

1 If you are running Windows 7, Windows Embedded POSReady 7, Windows 8.1, Windows 10, or Windows Server 2012 R2, click **Start**, type **Local Security Policy** in the search box, and then press Enter.
2 Expand the **Local Policies** folder, and then click **Audit Policy**.
3 Double-click **Audit account logon events**, select both the **Success** and **Failure** check boxes, and then click **OK**.
4 Double-click **Audit account management**, select both the **Success** and **Failure** check boxes, and then click **OK**.
5 Double-click **Audit object access**, select both the **Success** and **Failure** check boxes, and then click **OK**.
6 Double-click **Audit policy change**, select both the **Success** and **Failure** check boxes, and then click **OK**.

Audit access to system folders and files

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

For Windows 7, Windows Embedded POSReady 7, Windows 8.1, Windows 10, or Windows Server 2012 R2:

- C:\Windows\System32\winevt\Logs.
- The folder where Microsoft Dynamics AX 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).

Complete this procedure for each folder in the previous list.

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

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

3. Click the **Auditing** tab. If you receive a security message, click **Continue**.
4. Click **Add**.
5. In the **Enter the object name to select** field, type **Everyone**, and then click **Check Names**.
6. If the name is valid, click **OK**.
7. In the **Apply onto** field, make sure that **This folder, subfolders and files** is selected.
8. In the **Access** list, select both the **Successful** and **Failed** check boxes for the following privileges, and then click **OK**:
   - Create files/write data
   - Create folders/append data
   - Delete subfolders and files
   - Delete
   - Read permissions
   - Change permissions

   Note: Do not enable Read permissions for the folder where Microsoft Dynamics AX for Retail Modern POS is installed (by default, C:\Program Files (x86)\Microsoft Dynamics AX\70\Retail Modern POS).

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

Required services and protocols

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

Components	Required services and protocols
AOSService web app	• Internet Information Services (HTTPS) TLS 1.2+ • Microsoft .NET 4.5 • SQL Server (Default port: 1433)
AX Batch Management Service	• Microsoft .NET 4.5 • SQL Server (Default port: 1433)
RetailServer web service	• Internet Information Services (HTTPS) TLS 1.2+ • Microsoft .NET 4.5

Components	Required services and protocols
RetailCloudPOS web app	• Internet Information Services (HTTPS) TLS 1.2+
Retail hardware station web service	• Internet Information Services (HTTPS) TLS 1.2+
Retail Modern POS (register)	• SQL Server (Default port: 1433)
Cloud POS (register)	• Internet Information Services (HTTPS) TLS 1.2+ • Web browser
Sample online storefront web app	• Internet Information Services (HTTPS) TLS 1.2+

More details can be found in the "System requirements" page on the Microsoft Dynamics AX Help wiki: http://go.microsoft.com/fwlink/?LinkId=799731.

Dependent hardware

The following PTS-terminals are used for Microsoft Dynamics AX:

- VeriFone Mx925/Mx915, PTS-approval 4-10110
- VeriFone PP1000SE, PTS-approval 4-30059
- Equinox Payment L5200, L5300, PTS-approval

Communication and database computers: Open the firewall

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

Type of computer	Open the firewall to these programs
Retail Hardware Station	Retail Hardware Station, to allow POS registers to connect to POS peripherals

Note:

- Instead of opening the firewall to Hardware Station, you might prefer to open the firewall to the TCP ports used by this program. In this case, you must know the port numbers that you specified when you deployed the services. By default, the port number is 443 for HTTPS.
- Depending on the settings of your firewall, you might also need to open the firewall to outbound traffic on client and register computers. To determine whether this is necessary, consult your network administrator.
- The instructions in the rest of this section are for Windows Firewall. If you are using another firewall, see the firewall documentation for more information.

Open Windows Firewall

To open Windows Firewall to a program on Windows 7, Windows 8, Windows 8.1, Windows 10, or Windows Server 2012 R2, use the New Rule Wizard to create a rule that manages the connections that the allowed program can receive. You can use the default settings for each rule, but you must provide the path of the program and a name for the rule.

Program	Typical program path	Suggested rule name
Retail Hardware Station (if installed)	C:\Program Files (x86)\Microsoft Dynamics AX\70\Retail Hardware Station	Retail Hardware Station
SQL Server	C:\Program Files\Microsoft SQL Server\<*instance name*>\MSSQL\Binn\Sqlservr.exe	SQL Server <*instance name*>

Note: On a 64-bit operating system, Retail Hardware Station is in the Program Files (x86) folder path instead.

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

At the head office: Set up the password policy

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

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

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

Note:

- Users of Microsoft Dynamics AX are subject to Azure Active Directory (Azure AD) security policies. Therefore, users of Microsoft Dynamics AX are subject to the same password policy as Azure AD users.
- These policies represent the minimum requirements of Requirements 8.5.9 through 8.5.14. More stringent settings can be used.
- For more information about managing password policy via group policies, see "Working with Group Policy objects" at http://technet.microsoft.com/en-us/library/cc731212.aspx.

At the head office: Set up database logging

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

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

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

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

1 To set up logging in the head office database, click **System administration** > **Setup** > **Database log setup**.
2 Create the following new entries by following the wizard.

Table name	Actual system name
POS functionality profile	RetailFunctionalityProfile
POS hardware profiles	RetailHardwareProfile
Component Item ID	RetailStaffLoginLog
Staff permission group	RetailStaffPermissionGroup
Staff	RetailStaffTable
Audit trail setup	SysDatabaseLog
POS registers	RetailTerminalTable
Payment services	CreditCardAccountSetup

Table name	Actual system name
RetailOnlineChannelPaymentConnectorLine	RetailChannelPaymentConnectorLine

3 Click **System administration** > **Setup** > **Licensing** > **Licensing configuration**.

4 Under **Administration**, select the **Electronic signature** check box, and then click **Save**.

Note:

- This procedure sets up logging on Insert, Delete, Update, and RenameKey actions. To view or modify this setup, click **System administration** > **Setup** > **Database log setup**.
- For each change to one of these tables, Microsoft Dynamics AX records the user who performed the action, the table that was modified, the action that was taken, the attribute that was changed, the time and date of the action, and the ID of the record that was modified or added. For each Update action, it also records both the previous and new settings.
- By default, any user who has database access can query a database log by using X++ or alerts, or by using direct database access. To help protect data, restrict permissions on the SysDatabaseLog table.
- For information about viewing logged actions, see Monitor Microsoft Dynamics AX activity, later in this guide.

Obtain a PCI-certified payment solution from a payment solution provider

You need to obtain a PCI-certified payment solution from a payment solution provider. A payment solution process credit card and debit card transaction at retail point-of-sale (POS) registers, in online stores, and in the **Call center** and **Accounts receivable** modules in Microsoft Dynamics AX.

A payment solution includes two components:

- A payment connector that processes "card-present" payment transactions with payment devices and "card-not-present" payment transactions. You follow the instructions provided by a payment solution provider to deploy the payment connector to your Microsoft Dynamics AX environment.
- A payment accepting page that allows you to accept credit cards for call centers or online stores PCI-free. A payment accepting page is hosted by a PCI-certified payment solution provider.

Note: For more information about payment solution providers, log on to Microsoft Dynamics Lifecycle Services to view the payment providers list: http://go.microsoft.com/fwlink/?LinkID=780625.

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

In Microsoft Dynamics AX, the only time that store employees might have access to card numbers is at the time of sale, when the cashier swipes the card. Payment card holder information is sent directly from Retail Modern POS, Retail Hardware Station, or a payment device to the processor at that time, and transactions are captured immediately.

Payment information in the Microsoft Dynamics AX database is limited to the customer's name, the payment amount, the card type, and the last four digits of the card number. The entire primary account number (PAN) is never stored.

Set up payment processing

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

1. Obtain a PCI-certified payment connector from a payment solution provider.
2. Follow the instructions provided by your selected payment solution provider to deploy the payment connector to Microsoft Dynamics AX.
3. Start Microsoft Dynamics AX, click **Retail and commerce** > **Channel setup** > **POS setup** > **POS profiles** > **Hardware profiles**, and then, in the left pane, select the hardware profile for the store.
4. In the **EFT service** section, in the **EFT service** field, select **Payment Connector**, select your selected payment solution in the payment connector list, enter the merchant account information provided by your payment solution provider, and click **Save** to save the hardware profile configuration.
5. Associate a hardware profile with each register or Hardware Station to enable payment processing and to select devices. For more information, see Set up devices in the Retail module.
6. Set up payment methods to use payment processing. For more information, see Set up payment methods for payment processing.
7. Enable one or more payment processing tender types for each store. For more information, see Enable tender types and card types for specific stores.
8. Turn on payment processing at stores by running scheduled jobs. For more information, see Send payment processing changes to the stores.
9. Configure Accounts receivable for payment processing to support customer orders. For more information, see Set up Accounts receivable for Payment Services.

Note: These steps are not specifically required for PCI compliance. However, if these steps are skipped, the store cannot use Microsoft Dynamics AX to process the payments that are subject to the PCI Data Security Standard. The steps are described in more detail later in this section.

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

Set up devices in the Retail module

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

HKEY_LOCAL_MACHINE\SOFTWARE\OLEforRetail\ServiceOPOS

1. Start the Microsoft Dynamics AX client, and log on with Azure AD.
2. Click **Retail and commerce** > **Channel setup** > **POS setup** > **POS profiles** > **Hardware profiles**.

3 In the list, select the correct profile.
4 Configure hardware devices, such as receipt printers, MSRs (magnetic stripe readers), and PIN (personal identification number) pad devices.

   On the tab for each device, in the **Device name** field, type the appropriate device name. A description for the device is optional.

Note:

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

Configure a terminal ID for specific registers

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

1 Click **Retail and commerce** > **Channel setup** > **POS setup** > **Registers**.
2 Select the register, and click **Edit**.
3 On the **General** tab, in the **Hardware profile** field, select the appropriate profile. Then, in the **EFT POS register number** field, type one of the terminal IDs that you received from the payment provider.

   Note: Some payment providers refer to EFT POS register numbers as *terminal IDs*. In Retail Modern POS, *terminal ID* refers to the terminal number shown on the **General** tab. The terminal number and the EFT POS register number do not have to match, but both numbers must be unique for each terminal.

4 Repeat steps 2 and 3 for other registers. When you have finished associating hardware profiles with registers, close the page.

Set up payment methods for payment processing

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

1 Start the Microsoft Dynamics AX client, and log on with Azure AD.
2 Click **Retail and commerce** > **Channel setup** > **Payment methods** > **Payment methods**.
3 On the toolbar, click **New**.
4 In the new row, type a unique number and description for the new payment method. Then, in the **Default function** column, click the arrow, and select **Card**.
5 Close the page.
6 Click **Retail** > **Setup** > **Payment methods** > **Card types**.
7 On the toolbar, click **New**.

8 In the new row, type a unique ID and name for the new card type. Then, in the **Card types** column, click the arrow, and select the appropriate option.
9 While the new row is still selected, click **Card number**.
10 Create a verification mask for the card type by entering the range of digits that all cards of this type begin with. For example, Visa card numbers begin with 4, so you could verify that cards accepted as the Visa card type are really Visa cards by creating a mask of **4**.
11 Close the **Card number** page.
12 Close the **Card type** page.

Enable tender types and card types for specific stores

1 Start the Microsoft Dynamics AX client, and log on with Azure AD.
2 Click **Retail and commerce** > **Channels** > **Retail stores** > **All retail stores**.
3 Select a store, and then, on the **Setup** tab, click **Payment methods**.
4 On the toolbar, click **New**, and then, on the **General** tab, in the **Payment method** field, select a payment method. The information for the selected payment method is filled in automatically.
5 While the new payment method row is still selected, click **Card setup**.
6 On the toolbar, click **New**, and then, in the **Card ID** field, select the card type for this payment method.
7 Select the new card setup, and then, on the **General** tab, select the **Check expiration date** check box.
8 Close the **Card setup** page.
9 Close the **Payment method** page.
10 Repeat steps 3 through 8 for any other payment methods for this store.

Send payment processing changes to the stores

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

1 Start the Microsoft Dynamics AX client, and log on with Azure AD.
2 Click **Retail and commerce** > **Retail IT** > **Distribution schedule**.
3 To send the payment processing and device settings in the hardware profile, select the **1090 Registers** job, and then click **Run now**.
4 To send down the payment methods, card types, and card numbers, select the **1070 Channel configuration** job, and then click **Run now**.

At the head office: Set up Accounts receivable for payment processing

1 Start the Microsoft Dynamics AX client, and log on with Azure AD.
2 Click **Accounts receivable** > **Payment setup** > **Payment services**.
3 On the **Payment services** page, click **New**, and then, in the **Payment service** field, enter a name for the payment service.

4 In the **Payment connector** field, select **your selected payment solution** in the list, and enter the merchant account information provided by your payment solution provider.
5 Click **Validate**.

   Microsoft Dynamics AX confirms that the validation is successful.

6 Click **Credit card types**, and then add all the credit cards that you accept.
7 Click **Save** to save the configuration.

At the head office: Set up online stores for payment processing

1 Start the Microsoft Dynamics AX client, and log on with Azure AD.
2 Click **Retail and commerce** > **Channels** > **Online stores**.
3 Select an online store, and then, on the Action Pane, click **Edit**.
4 On the **Payment accounts** FastTab, in the **Connectors** field, select your selected payment solution in the payment connector list.
5 Click **Add**, and then, under **Details**, enter the merchant account information provided by your payment solution provider.

Store computers

Set up the password policy

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

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

Note: These policies represent the minimum requirements of Requirements 8.5.9 through 8.5.14. More stringent settings can be used.

1 If you are running Windows 7, Windows Embedded POSReady 7, Windows 8.1, Windows 10, or Windows Server 2012 R2 click **Start**, type **Local Security Policy** in the search box, and then press Enter.
2 Expand **Account Policies**, and then click **Password Policy**.

3 To modify a policy, right-click the policy, and then click **Properties**.
4 Click **Account Lockout Policy**.
5 To modify a policy, right-click the policy, and then click **Properties**.

Set up password-protected screen savers

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

1 In the C:\Windows\System32 folder, locate the screen saver (.scr) file to use.
2 If you are running Windows 7, Windows Embedded POSReady 7, Windows 8.1, Windows 10, or Windows Server 2012 R2, click **Start**, type **mmc** in the search box, and then press Enter.
3 On the **File** menu, click **Add/Remove Snap-in**.
4 Select **Group Policy Object Editor**, click **Add**, click **Finish**, and then click **Close** or **OK**.
5 Expand **Local Computer Policy**, expand **User Configuration**, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization** (on Windows 7) or **Display** (on other operating systems).
6 Double-click **Force specific screen saver** (on Windows 7) or **Screen Saver executable name** (on other operating systems), select **Enabled**, type the path and name of the screen saver (.scr) file that you selected in step 1, and then click **OK**.
7 Double-click **Password protect the screen saver**, select **Enabled**, and then click **OK**.
8 Double-click **Screen Saver timeout**, select **Enabled**, type **900** or a smaller value, and then click **OK**.

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

Turn off System Restore

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

Turn off Internet Explorer Automatic Crash Recovery

The Automatic Crash Recovery (ACR) feature of Internet Explorer can help prevent the loss of work and productivity in the unlikely event that the browser crashes or hangs. But data saved for crash recovery by this feature is not considered secure by the PCI Security Standards Council.

1 If you are running Windows 7, Windows Embedded POSReady 7, Windows 8.1, Windows 10, or Windows Server 2012 R2, click **Start**, type **Internet Explorer** in the search box, and then press Enter.
2 On the **Tools** menu, click **Internet options**.
3 Click **Advanced** tab, go to **Browsing** section, clear the **Enable automatic crash recovery** check box, click **OK**, and then close the browser window.

Hardening instructions for a Retail Cloud POS machine

To mitigate the security risk associated with browser-based Retail Cloud POS, the following actions must be performed on a machine that runs Retail Cloud POS.

1. Hide the Internet Explorer address bar to prevent JavaScript execution in the address bar.
2. Disable the browser's developer console.
3. Retail Cloud POS must be accessed by a low-privileged user.
4. Set up group policies to enable a kiosk session.
5. (Optional) Set up a proxy to access only whitelisted websites.

Retail Cloud POS Hardening – Hide the Internet Explorer address bar to help prevent JavaScript execution in the address bar

There is no option to disable script execution in the Internet Explorer address bar. Hiding the address bar is one alternative.

1. Create a shortcut for the Retail Cloud POS URL, and copy it to each store worker's Windows desktop.
2. Run **regedit.exe** to change the registry to disable the Internet Explorer address bar.

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\ToolBars\Restrictions]

   "NoNavBar"=dword:00000001

Retail Cloud POS Hardening – Disable the Internet Explorer developer console

- Use Group Policy Editor to enable the following group policy to disable the Internet Explorer developer console:

  \Administrative Templates\Windows Components\Internet Explorer\Toolbars\Turn off Developer Tools="Enabled"

Retail Cloud POS Hardening – Disable the Microsoft Edge developer console

- Run **regedit.exe** to change the registry to disable the developer console:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\F12]

  "AllowDeveloperTools"=dword:00000000

Retail Cloud POS Hardening – Microsoft Cloud POS must be accessed by a low-privileged user

A POS user must be a non-administrative account and must not have the privilege to change applied policies.

Retail Cloud POS Hardening – Set up group policies to enable a kiosk session

We recommend that you apply the following restrictions for Retail Cloud POS users:

- Restrict access to the file system.
- Restrict access to Control Panel.
- Restrict access to removable drives.
- Restrict access to command-executing shells.
- Restrict access to the registry.
- Restrict access to application management.

The following table shows the list of group policies to enable kiosk mode. The set of policies requires you to start your browser with a logon script. These policies can be adjusted to meet your needs, and you should always assess any security implications or talk to a specialist.

Setting	State	Comment	Path
Enable screen saver	Disabled	No	\Control Panel\Personalization
Allow DFS roots to be published	Disabled	No	\Shared Folders
Allow shared folders to be published	Disabled	No	\Shared Folders
Add Search Internet link to Start Menu	Disabled	No	\Start Menu and Taskbar
Show Quick Launch on Taskbar	Disabled	No	\Start Menu and Taskbar
Show the Apps view automatically when the user goes to Start	Disabled	No	\Start Menu and Taskbar
Show "Run as different user" command on Start	Disabled	No	\Start Menu and Taskbar
Add the Run command to the Start Menu	Disabled	No	\Start Menu and Taskbar
Show Start on the display the user is using when they press the Windows logo key	Disabled	No	\Start Menu and Taskbar
Show Windows Store apps on the taskbar	Disabled	No	\Start Menu and Taskbar
Turn off shell protocol protected mode	Disabled	No	\Windows Components\File Explorer
Turn on menu bar by default	Disabled	No	\Windows Components\Internet Explorer
Turn on Script Execution	Disabled	No	\Windows Components\Windows PowerShell
Hide the "Add a program from CD-ROM or floppy disk" option	Enabled	No	\Control Panel\Add or Remove Programs

Setting	State	Comment	Path
Hide the "Add programs from Microsoft" option	Enabled	No	\Control Panel\Add or Remove Programs
Hide the "Add programs from your network" option	Enabled	No	\Control Panel\Add or Remove Programs
Hide Add New Programs page	Enabled	No	\Control Panel\Add or Remove Programs
Remove Add or Remove Programs	Enabled	No	\Control Panel\Add or Remove Programs
Hide the Set Program Access and Defaults page	Enabled	No	\Control Panel\Add or Remove Programs
Hide Change or Remove Programs page	Enabled	No	\Control Panel\Add or Remove Programs
Go directly to Components Wizard	Enabled	No	\Control Panel\Add or Remove Programs
Remove Support Information	Enabled	No	\Control Panel\Add or Remove Programs
Hide Add/Remove Windows Components page	Enabled	No	\Control Panel\Add or Remove Programs
Disable the Display Control Panel	Enabled	No	\Control Panel\Display
Hide Settings tab	Enabled	No	\Control Panel\Display
Prevent changing color scheme	Enabled	No	\Control Panel\Personalization
Prevent changing theme	Enabled	No	\Control Panel\Personalization
Prevent changing visual style for windows and buttons	Enabled	No	\Control Panel\Personalization
Prohibit selection of visual style font size	Enabled	No	\Control Panel\Personalization
Prevent changing color and appearance	Enabled	No	\Control Panel\Personalization
Prevent changing desktop background	Enabled	No	\Control Panel\Personalization
Prevent changing desktop icons	Enabled	No	\Control Panel\Personalization
Prevent changing mouse pointers	Enabled	No	\Control Panel\Personalization
Prevent changing screen saver	Enabled	No	\Control Panel\Personalization
Prevent changing sounds	Enabled	No	\Control Panel\Personalization
Prevent addition of printers	Enabled	No	\Control Panel\Printers
Prevent deletion of printers	Enabled	No	\Control Panel\Printers
Hide "Set Program Access and Computer Defaults" page	Enabled	No	\Control Panel\Programs

Setting	State	Comment	Path
Hide “Get Programs” page	Enabled	No	\Control Panel\Programs
Hide “Installed Updates” page	Enabled	No	\Control Panel\Programs
Hide “Programs and Features” page	Enabled	No	\Control Panel\Programs
Hide the Programs Control Panel	Enabled	No	\Control Panel\Programs
Hide “Windows Features”	Enabled	No	\Control Panel\Programs
Hide “Windows Marketplace”	Enabled	No	\Control Panel\Programs
Turn off automatic learning	Enabled	No	\Control Panel\Regional and Language Options\Handwriting personalization
Hide Regional and Language Options administrative options	Enabled	No	\Control Panel\Regional and Language Options
Hide and disable all items on the desktop	Enabled	No	\Desktop
Remove the Desktop Cleanup Wizard	Enabled	No	\Desktop
Hide Internet Explorer icon on desktop	Enabled	No	\Desktop
Remove Computer icon on the desktop	Enabled	No	\Desktop
Remove My Documents icon on the desktop	Enabled	No	\Desktop
Hide Network Locations icon on desktop	Enabled	No	\Desktop
Remove Properties from the Computer icon context menu	Enabled	No	\Desktop
Remove Properties from the Documents icon context menu	Enabled	No	\Desktop
Do not add shares of recently opened documents to Network Locations	Enabled	No	\Desktop
Remove Recycle Bin icon from desktop	Enabled	No	\Desktop
Remove Properties from the Recycle Bin context menu	Enabled	No	\Desktop
Don’t save settings at exit	Enabled	No	\Desktop
Turn off Aero Shake window minimizing mouse gesture	Enabled	No	\Desktop
Prevent adding dragging dropping and closing the Taskbar’s toolbars			Enabled

Setting	State	Comment	Path
Prohibit adjusting desktop toolbars	Enabled	No	\Desktop
Force Start to be either full screen size or menu size	Enabled	No	\Start Menu and Taskbar
Go to the desktop instead of Start when signing in	Enabled	No	\Start Menu and Taskbar
Turn off personalized menus	Enabled	No	\Start Menu and Taskbar
Lock the Taskbar	Enabled	No	\Start Menu and Taskbar
Turn off notification area cleanup	Enabled	No	\Start Menu and Taskbar
Remove Balloon Tips on Start Menu items	Enabled	No	\Start Menu and Taskbar
Prevent users from customizing their Start Screen	Enabled	No	\Start Menu and Taskbar
Remove common program groups from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Favorites menu from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Search link from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove frequent programs list from the Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Games link from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Help menu from Start Menu	Enabled	No	\Start Menu and Taskbar
Turn off user tracking	Enabled	No	\Start Menu and Taskbar
Remove All Programs list from the Start menu	Enabled	No	\Start Menu and Taskbar
Remove Network Connections from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove pinned programs list from the Start Menu	Enabled	No	\Start Menu and Taskbar
Do not keep history of recently opened documents	Enabled	No	\Start Menu and Taskbar
Remove Recent Items menu from Start Menu	Enabled	No	\Start Menu and Taskbar

Setting	State	Comment	Path
Do not use the search-based method when resolving shell shortcuts	Enabled	No	\Start Menu and Taskbar
Do not use the tracking-based method when resolving shell shortcuts	Enabled	No	\Start Menu and Taskbar
Remove Run menu from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Default Programs link from the Start menu.	Enabled	No	\Start Menu and Taskbar
Remove Documents icon from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Music icon from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Network icon from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Pictures icon from Start Menu	Enabled	No	\Start Menu and Taskbar
Do not search communications	Enabled	No	\Start Menu and Taskbar
Remove Search Computer link	Enabled	No	\Start Menu and Taskbar
Remove See More Results / Search Everywhere link	Enabled	No	\Start Menu and Taskbar
Do not search for files	Enabled	No	\Start Menu and Taskbar
Do not search Internet	Enabled	No	\Start Menu and Taskbar
Do not search programs and Control Panel items	Enabled	No	\Start Menu and Taskbar
Remove programs on Settings menu	Enabled	No	\Start Menu and Taskbar
Prevent changes to Taskbar and Start Menu Settings	Enabled	No	\Start Menu and Taskbar
Remove Downloads link from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Homegroup link from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Recorded TV link from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove user's folders from the Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Videos link from Start Menu	Enabled	No	\Start Menu and Taskbar
Force classic Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Clock from the system notification area	Enabled	No	\Start Menu and Taskbar

Setting	State	Comment	Path
Prevent grouping of taskbar items	Enabled	No	\Start Menu and Taskbar
Do not display any custom toolbars in the taskbar	Enabled	No	\Start Menu and Taskbar
Remove access to the context menus for the taskbar	Enabled	No	\Start Menu and Taskbar
Hide the notification area	Enabled	No	\Start Menu and Taskbar
Prevent users from uninstalling applications from Start	Enabled	No	\Start Menu and Taskbar
Remove user folder link from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove user name from Start Menu	Enabled	No	\Start Menu and Taskbar
Remove links and access to Windows Update	Enabled	No	\Start Menu and Taskbar
Remove the "Undock PC" button from the Start Menu	Enabled	No	\Start Menu and Taskbar
Remove Notifications and Action Center	Enabled	No	\Start Menu and Taskbar
Disable showing balloon notifications as toasts.	Enabled	No	\Start Menu and Taskbar
Remove the Security and Maintenance icon	Enabled	No	\Start Menu and Taskbar
Remove the networking icon	Enabled	No	\Start Menu and Taskbar
Remove the battery meter	Enabled	No	\Start Menu and Taskbar
Remove the volume control icon	Enabled	No	\Start Menu and Taskbar
Turn off feature advertisement balloon notifications	Enabled	No	\Start Menu and Taskbar
Do not allow pinning Store app to the Taskbar	Enabled	No	\Start Menu and Taskbar
Do not allow pinning items in Jump Lists	Enabled	No	\Start Menu and Taskbar
Do not allow pinning programs to the Taskbar	Enabled	No	\Start Menu and Taskbar
Do not display or track items in Jump Lists from remote locations	Enabled	No	\Start Menu and Taskbar

Setting	State	Comment	Path
Turn off automatic promotion of notification icons to the taskbar	Enabled	No	\Start Menu and Taskbar
Lock all taskbar settings	Enabled	No	\Start Menu and Taskbar
Prevent users from adding or removing toolbars	Enabled	No	\Start Menu and Taskbar
Prevent users from rearranging toolbars	Enabled	No	\Start Menu and Taskbar
Do not allow taskbars on more than one display	Enabled	No	\Start Menu and Taskbar
Turn off all balloon notifications	Enabled	No	\Start Menu and Taskbar
Remove pinned programs from the Taskbar	Enabled	No	\Start Menu and Taskbar
Prevent users from moving taskbar to another screen dock location	Enabled	No	\Start Menu and Taskbar
Prevent users from resizing the taskbar	Enabled	No	\Start Menu and Taskbar
Turn off taskbar thumbnails	Enabled	No	\Start Menu and Taskbar
Remove Task Manager	Enabled	No	\System\Ctrl+Alt+Del Options
Code signing for device drivers	Enabled	No	\System\Driver Installation
Turn off Windows Update device driver search prompt	Enabled	No	\System\Driver Installation
Disallow selection of Custom Locales	Enabled	No	\System\Locale Services
Disallow changing of geographic location	Enabled	No	\System\Locale Services
Disallow user override of locale settings	Enabled	No	\System\Locale Services
CD and DVD: Deny read access	Enabled	No	\System\Removable Storage Access
CD and DVD: Deny write access	Enabled	No	\System\Removable Storage Access
Floppy Drives: Deny read access	Enabled	No	\System\Removable Storage Access
Floppy Drives: Deny write access	Enabled	No	\System\Removable Storage Access
Removable Disks: Deny read access	Enabled	No	\System\Removable Storage Access
Removable Disks: Deny write access	Enabled	No	\System\Removable Storage Access
All Removable Storage classes: Deny all access	Enabled	No	\System\Removable Storage Access
Tape Drives: Deny read access	Enabled	No	\System\Removable Storage Access

Setting	State	Comment	Path
Tape Drives: Deny write access	Enabled	No	\System\Removable Storage Access
WPD Devices: Deny read access	Enabled	No	\System\Removable Storage Access
WPD Devices: Deny write access	Enabled	No	\System\Removable Storage Access
Prevent access to the command prompt	Enabled	No	\System
Prevent access to registry editing tools	Enabled	No	\System
Prevent the wizard from running.	Enabled	No	\Windows Components\Add features to Windows 10
Turn off Program Compatibility Assistant	Enabled	No	\Windows Components\Application Compatibility
Search, Share, Start, Devices and Settings don't appear when the mouse is pointing to the upper-right corner of the screen	Enabled	No	\Windows Components\Edge UI
Disable help tips	Enabled	No	\Windows Components\Edge UI
Turn off tracking of app usage	Enabled	No	\Windows Components\Edge UI
Do not show recent apps when the mouse is pointing to the upper-left corner of the screen	Enabled	No	\Windows Components\Edge UI
Prevent users from replacing the Command Prompt with Windows PowerShell in the menu they see when they right-click the lower-left corner or press the Windows logo key+X	Enabled	No	\Windows Components\Edge UI
Turn off switching between recent apps	Enabled	No	\Windows Components\Edge UI
Turn on or off details pane	Enabled	No	\Windows Components\File Explorer\Explorer Frame Pane
Turn off Preview Pane	Enabled	No	\Windows Components\File Explorer\Explorer Frame Pane
Do not display the Welcome Center at user logon	Enabled	No	\Windows Components\File Explorer
Turn on Classic Shell	Enabled	No	\Windows Components\File Explorer
Remove CD Burning features	Enabled	No	\Windows Components\File Explorer
Remove DFS tab	Enabled	No	\Windows Components\File Explorer

Setting	State	Comment	Path
Hide these specified drives in My Computer	Enabled	No	\Windows Components\File Explorer
No Entire Network in Network Locations	Enabled	No	\Windows Components\File Explorer
Remove File menu from File Explorer	Enabled	No	\Windows Components\File Explorer
Do not allow Folder Options to be opened from the Options button on the View tab of the ribbon	Enabled	No	\Windows Components\File Explorer
Remove Hardware tab	Enabled	No	\Windows Components\File Explorer
Hides the Manage item on the File Explorer context menu	Enabled	No	\Windows Components\File Explorer
Remove Shared Documents from My Computer	Enabled	No	\Windows Components\File Explorer
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled	No	\Windows Components\File Explorer
Remove the Search the Internet "Search again" link	Enabled	No	\Windows Components\File Explorer
Remove Security tab	Enabled	No	\Windows Components\File Explorer
Remove Search button from File Explorer	Enabled	No	\Windows Components\File Explorer
Remove File Explorer's default context menu	Enabled	No	\Windows Components\File Explorer
Prevent access to drives from My Computer	Enabled	No	\Windows Components\File Explorer
Turn off Windows+X hotkeys	Enabled	No	\Windows Components\File Explorer
No Computers Near Me in Network Locations	Enabled	No	\Windows Components\File Explorer
Request credentials for network installations	Enabled	No	\Windows Components\File Explorer
Prevent users from adding files to the root of their Users Files folder.	Enabled	No	\Windows Components\File Explorer
Turn off Accelerators	Enabled	No	\Windows Components\Internet Explorer\Accelerators

Setting	State	Comment	Path
File menu: Disable closing the browser and Explorer windows	Enabled	No	\Windows Components\Internet Explorer\Browser menus
File menu: Disable Save As... menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
File menu: Disable Save As Web Page Complete	Enabled	No	\Windows Components\Internet Explorer\Browser menus
File menu: Disable New menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
File menu: Disable Open menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'Send Feedback' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'For Netscape Users' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'Tip of the Day' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'Tour' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Turn off Shortcut Menu	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Hide Favorites menu	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Disable Open in New Window menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Turn off Print Menu	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Turn off the ability to launch report site problems using a menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Disable Save this program to disk option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Tools menu: Disable Internet Options... menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus

Setting	State	Comment	Path
View menu: Disable Full Screen menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
View menu: Disable Source menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Turn off Developer Tools	Enabled	No	\Windows Components\Internet Explorer\Toolbars
Turn off toolbar upgrade tool	Enabled	No	\Windows Components\Internet Explorer\Toolbars
Hide the Command bar	Enabled	No	\Windows Components\Internet Explorer\Toolbars
Hide the status bar	Enabled	No	\Windows Components\Internet Explorer\Toolbars
Disable customizing browser toolbars	Enabled	No	\Windows Components\Internet Explorer\Toolbars
Disable customizing browser toolbar buttons	Enabled	No	\Windows Components\Internet Explorer\Toolbars
Turn off add-on performance notifications	Enabled	No	\Windows Components\Internet Explorer
Do not allow users to enable or disable add-ons	Enabled	No	\Windows Components\Internet Explorer
Disable changing Advanced page settings	Enabled	No	\Windows Components\Internet Explorer
Turn off Favorites bar	Enabled	No	\Windows Components\Internet Explorer
Prevent per-user installation of ActiveX controls	Enabled	No	\Windows Components\Internet Explorer
Turn off Reopen Last Browsing Session	Enabled	No	\Windows Components\Internet Explorer
Turn off Tab Grouping	Enabled	No	\Windows Components\Internet Explorer
Prevent managing the phishing filter	Enabled	No	\Windows Components\Internet Explorer
Turn off Managing SmartScreen Filter for Internet Explorer 8	Enabled	No	\Windows Components\Internet Explorer
Prevent managing SmartScreen Filter	Enabled	No	\Windows Components\Internet Explorer
Turn off the Security Settings Check feature	Enabled	No	\Windows Components\Internet Explorer
Enforce full-screen mode	Enabled	No	\Windows Components\Internet Explorer

Setting	State	Comment	Path
Disable Import/Export Settings wizard	Enabled	No	\Windows Components\Internet Explorer
Prevent Internet Explorer Search box from appearing	Enabled	No	\Windows Components\Internet Explorer
Turn off Quick Tabs functionality	Enabled	No	\Windows Components\Internet Explorer
Turn off tabbed browsing	Enabled	No	\Windows Components\Internet Explorer
Disable changing Automatic Configuration settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing Temporary Internet files settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing Calendar and Contact settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing certificate settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing default browser check	Enabled	No	\Windows Components\Internet Explorer
Disable changing color settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing connection settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing font settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing language settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing link color settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing Messaging settings	Enabled	No	\Windows Components\Internet Explorer
Prevent managing pop-up exception list	Enabled	No	\Windows Components\Internet Explorer
Turn off pop-up management	Enabled	No	\Windows Components\Internet Explorer
Disable changing Profile Assistant settings	Enabled	No	\Windows Components\Internet Explorer
Prevent changing proxy settings	Enabled	No	\Windows Components\Internet Explorer
Disable changing ratings settings	Enabled	No	\Windows Components\Internet Explorer
Turn off the auto-complete feature for web addresses	Enabled	No	\Windows Components\Internet Explorer
Turn off suggestions for all user-installed providers	Enabled	No	\Windows Components\Internet Explorer
Turn off the quick pick menu	Enabled	No	\Windows Components\Internet Explorer

Setting	State	Comment	Path
Search: Disable Find Files via F3 within the browser	Enabled	No	\Windows Components\Internet Explorer
Search: Disable Search Customization	Enabled	No	\Windows Components\Internet Explorer
Turn off ability to pin sites in Internet Explorer on the desktop	Enabled	No	\Windows Components\Internet Explorer
Turn off the offer to update to the latest version of Windows	Enabled	No	\Windows Components\Store
Turn off the Store application	Enabled	No	\Windows Components\Store
Prohibit New Task Creation	Enabled	No	\Windows Components\Task Scheduler

Retail Cloud POS Hardening – Set up a proxy to access only whitelisted websites

Define a list of websites that a store worker (cashier) needs for normal operations, and set up an admin-controlled proxy to have access only to these websites. Retail Cloud POS requires access to the following websites:

- Cloud POS website
- Retail Server website
- Credit Card Payment acceptance page (optional)
- Bing Maps resources
- Media resources
- Azure AD logon page

Part 2: Features that facilitate PCI compliance

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

Protect stored cardholder data

Microsoft Dynamics AX provides the following capability to protect cardholder data:

- For storing cardholder data:
  - Microsoft Dynamics AX does not store sensitive authentication data.
  - Microsoft Dynamics AX does not store the primary account number (PAN).
  - Microsoft Dynamics AX stores truncated a PAN (last four digits) and the cardholder name.
- For displaying cardholder data:
  - Microsoft Dynamics AX Retail Modern POS and Retail Cloud POS display a masked PAN (first six and last four digits of the PAN) on the following pages:
    - Payment screen
    - Sales receipt
  - The Microsoft Dynamics AX client displays the cardholder name, last four digits of the PAN, and expiration date on the following page:
    - Accounts receivable – **Customer credit cards** page
    - Call center – **Enter customer payment information** page

Provide secure authentication features

Microsoft Dynamics AX provides the following secure authentication features

Store user names, passwords, and authentication

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

Microsoft Dynamics AX does not provide any default accounts or passwords. Instead, a unique user name and password are required for each user, including the user who sets up the software.

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

When cashiers log onto Retail Modern POS or Retail Cloud POS at the store, their employee user names and passwords are securely authenticated by Microsoft Dynamics Retail Server or Microsoft Dynamics Commerce Runtime. Cashier passwords are always one-way hashed with salt.

Store managers and cashiers have no administrative access.

Head office user names, passwords, and authentication

Users of Microsoft Dynamics AX are using Azure AD to manage user names and passwords, and are subject to Azure AD security policies. Therefore, users of Microsoft Dynamics AX are subject to the same password policy as Azure AD users. For more information about Azure AD password policy and restrictions, go to https://azure.microsoft.com/en-us/documentation/articles/active-directory-passwords-policy/.

Customers and integrators/resellers must comply with PA-DSS Requirements 3.1.1 through 3.1.11 when managing authentication credentials and creating strong authentication for all application-level and user accounts with administrative access, and for all accounts with access to cardholder data, as follows:

- PA-DSS Requirement 3.1.1: You shall not use any default administrative accounts for Microsoft Dynamics AX.
- PA-DSS Requirement 3.1.2: You shall enforce the changing of all default application passwords for all accounts that are generated or managed. This applies to all accounts, including user accounts, application and service accounts, and accounts used by the vendor for support purposes.
- PA-DSS Requirement 3.1.3: You shall assign unique IDs for user accounts.
- PA-DSS Requirement 3.1.4: You shall use a user name and password to authenticate all users.
- PA-DSS Requirement 3.1.5: You shall not require or use any group, shared, or generic accounts and passwords.
- PA-DSS Requirement 3.1.6: You shall require that passwords meet the following parameters:
  - They have a minimum length of seven characters.
  - They contain both numeric and alphabetic characters.
  - Alternatively, the password/phrase must have complexity and strength at least equivalent to the previous parameters.
- PA-DSS requirement 3.1.7: You shall require changes to user passwords at least once every 90 days.
- PA-DSS requirement 3.1.8: You shall require that a new password be different from any of the last four passwords used.
- PA-DSS requirement 3.1.9: You shall limit repeated access attempts by locking out the user account after no more than six logon attempts.
- PA-DSS requirement 3.1.10: You shall set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
- PA-DSS requirement 3.1.11: If a payment application session has been idle for more than 15 minutes, Microsoft Dynamics AX shall require the user to re-authenticate to re-activate the session.

Set up a new store user (manager or cashier) in Microsoft Dynamics AX

1. Start the Microsoft Dynamics AX client, and log on with Azure AD.
2. Click **Retail and commerce** > **Employees** > **All workers**.
3. Click **New**, type the new cashier's name, and then click **Hire new worker**.
4. Enter information about the employee on the tabs as needed.
5. On the **Worker** page, click the **Retail** link, and then select a layout ID and a language for the employee.
6. In the **Employment type** field, select **Cashier**, and then type a name in the **Name on receipt** field.

7 In the **Password** field, type the employee's password.
8 Click **POS permissions**, and then select a position for the cashier.

Important:

- When setting up Azure AD accounts for employees, and when setting up employee accounts in Microsoft Dynamics AX, you must use a "least privilege" approach, granting employees only those privileges that they require to perform their duties. For example, although trusted management personnel might require Administrator privileges on store computers, employee logon accounts must belong to a group that does not have these privileges.
- Each employee must have his or her own logon account. Do not allow employees to share employee IDs or passwords.

Log payment application activity

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

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

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

Monitor Microsoft Dynamics AX activity

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

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

View information about user logon and user logoff

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

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

View the audit trail

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

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

Monitor Retail Modern POS and Retail Cloud POS activity

Logging of PCI-relevant activity at the register needs to be configured. Activity in Retail Modern POS and Retail Cloud POS is logged in the AX.RetailTransactionTable, AX.RetailAuthenticationLog, and AX.RetailLog tables in the store or register offline database. It provides logging of the events that must be monitored for PCI compliance. These events are as follows:

- Employee logon and logoff
- Failed logon attempts

Note: The logging can be modified only at the head office, via changes to the functionality profile for each channel/store. Confirm that **Audit** logging is still assigned to each functionality profile on the **Functionality profile** page (**Retail and commerce** > **Channel setup** > **POS setup** > **POS profiles** > **Functionality profiles**).

Important: Logging should not be disabled, and doing so will result in non-compliance with PCI DSS.

At the store, events are logged in the AX.RetailTransactionTable, AX.RetailAuthenticationLog, and AX.RetailLog tables. For each event in the tables, the following information is logged:

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

Logged events in stores are transmitted to the central back office and stored in the RetailTransactionTable, RetailAuthenticationLog, and RetailLog tables.

Important: Microsoft Dynamics AX facilitates centralized logging by sending all audit logs to the central Microsoft Dynamics AX. You must configure a P-Job to include the RetailAuthenticationLog and RetailLog tables.

Monitor event logs

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

1. If you are running Windows 7, Windows Embedded POSReady 7, Windows 8, Windows 8.1, Windows 10, or Windows Server 2012 R2, click **Start**, type **Event Viewer** in the search box, and then press Enter.
2. If the **Windows Logs** folder is available, expand it, and then click **Security**.

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

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

- The Windows user account that was involved in the operation
- The type of event
- The date and time that the event occurred
- The success or failure of the operation
- The origination of the event
- The identity or name of any affected data, component, or resource
- If appropriate, the user group for which a user was added or removed

Operation	Event ID
Windows Embedded POSReady 7, Windows 7, Windows 8, Windows 8.1, Windows 10, and Windows Server 2012 R2	
Logon attempt	4776
Logon success	4624
Logon failure	529, 535, 539
Logoff	4634
User password reset	4724
User account created	4720
User account disabled	4725
User account deleted	4726
User account added	4728
User account changed	4738
User account locked out	4740
Member added to user group	4732
Member removed from user group	4733
Object access (update or deletion of monitored files)	None
File modified and saved	4663
Audit policy changed	None
Domain policy changed	4739
Event Viewer Security log cleared	1102

Data storage and deletion

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

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

- Primary account numbers (PANs) are not retained, so no periodic purging is necessary. This helps satisfy Requirement 3.1 of the PCI Data Security Standard.
- Sensitive authentication data is never retained, cannot be reproduced from within the program, and is not available in log files or debug files.
- Credit card numbers are tokenized and secured by your selected payment solution provider, and only card tokens are sent to Microsoft Dynamics AX.
- Card numbers are truncated after authorization, so that only the last four digits remain. Card numbers on both printed and journaled receipts are always truncated.
- Like this release of Microsoft Dynamics AX, the previous release (Microsoft Dynamics AX 2012 R3) did not retain any sensitive authentication data. Compliance with Requirement 3.2 of the PCI Data Security Standard does not require the removal of historical data.
- Because cardholder data is not retained, no encryption is required. Therefore, there is no need to periodically delete the encryption key. This helps satisfy Requirement 3.6 of the PCI Data Security Standard.

Versioning methodology

The Microsoft Dynamics AX versioning methodology is Major.Minor.Build.Minor Build. For example, 7.0.1232.0 means:

- 7 is the major version.
- 0 is the minor version.
- 1232 is the build number.
- 0 is the minor build number.

For the current version of Microsoft Dynamics AX, the major version number is 7. It will change if there is a major release in the future, which will require a new PA-DSS audit.

The minor version number is used to track a new minor release or a cumulative update of Microsoft Dynamics AX.

A hotfix will be indicated by either a build number or minor build number change.

Security-affecting changes will be indicated by either a build number or minor build number change.

Protect wireless transmissions

The Microsoft Dynamics AX point-of-sale system does not require or support wireless connections.

If wireless connections are part of the store's local area network (LAN)—even if they are not used with Microsoft Dynamics AX—you must install a firewall and use compliant wireless settings, as described in Requirements 1.2.3, 2.1.1, and 4.1.1 of the PCI Data Security Standard. Specific requirements include:

- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.
- Change wireless vendor default values, including but not limited to default wireless encryption keys, passwords, and Simple Network Management Protocol (SNMP) community strings.
- Ensure that wireless device security settings are enabled for strong encryption technology for authentication and transmission.
- Use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
- Ensure that procedures are in place for changing wireless encryption keys and passwords, including SNMP strings, any time anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Ensure that you configure firewalls to deny or—if such traffic is necessary for business purposes—permit only authorized traffic between the wireless environment and the cardholder data environment.

Note: For new wireless implementations, implementing Wired Equivalent Privacy (WEP) has been prohibited.

Important:

- Encryption keys shall be changed from the default values at installation, and shall be changed any time anyone with knowledge of the keys leaves the company or changes positions.
- Default SNMP community strings on wireless devices shall be changed.
- Default passwords/passphrases on access points shall be changed.
- Firmware on wireless devices shall be updated to support strong encryption for authentication and transmission over wireless networks.
- Other security-related wireless vendor defaults shall be changed, if applicable.

Internet connections

The Microsoft Dynamics AX point-of-sale system includes Retail Modern POS, Retail Cloud POS, and Retail Hardware Station. A perimeter network, which is also known as a DMZ and a screened subnet, can be used to separate the Internet from point-of-sale systems that transmit cardholder data. Cardholder data is never stored, including on the internal network and the perimeter network. The point-of-sale database server is in Microsoft Azure and behind a firewall. This helps satisfy Requirement 1.3 of the PCI Data Security Standard.

Remote access

The Microsoft Dynamics AX point-of-sale system does not provide features that allow or facilitate remote connections into the payment environment. If you choose to use a remote connection, you must use two-factor

authentication (user name and password, plus an additional authentication item, such as a token), as required by Requirement 8.3 of the PCI Data Security Standard.

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

- Change default settings in the remote access software (for example, change default passwords, and use unique passwords for each user).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication, and establish user password policies, according to Requirement 8 of the PCI Data Security Standard.
- Enable encrypted data transmission, according to Requirement 4.1 of the PCI Data Security Standard.
- Enable account lockout after a certain number of failed logon attempts, according to Requirement 8.5.13 of the PCI Data Security Standard.
- Configure the system so that a remote user must establish a virtual private network (VPN) connection via a firewall before access is allowed.
- Enable logging.
- Restrict access to user passwords to authorized reseller/integrator personnel.

Data transmissions

All Microsoft Dynamics AX transmissions of cardholder data, whether over a private network or a public network, are secured by the use of TLS 1.2+. This helps satisfy Requirement 4.1 of the PCI Data Security Standard.

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

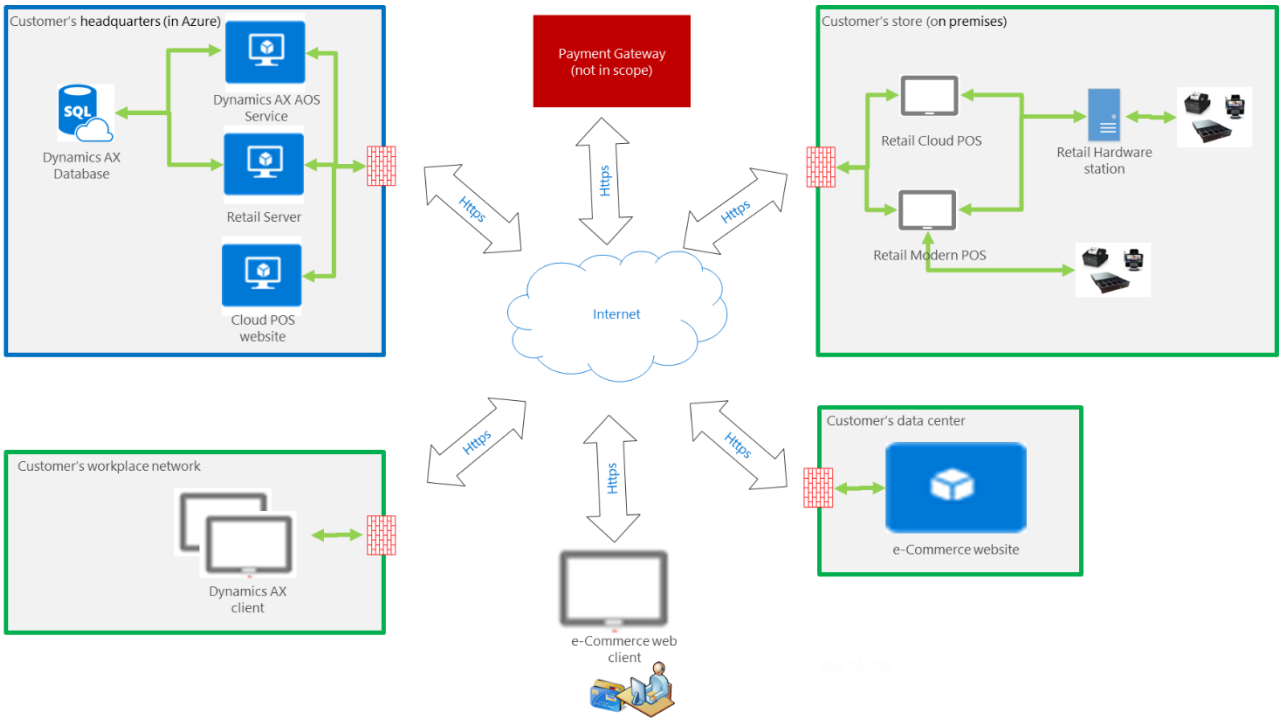
Important:

- Strong cryptography and security protocols must be used for data transmission over public networks.
- Only trusted keys and/or certificates can be accepted.
- You must use only secure versions and secure implementations of security protocols.
- Prevent fallback to an insecure version or configuration (for example, if TLS is used, the application must not allow fallback to SSL).
- You must use proper encryption strength for the encryption methodology.

Non-console administrative access

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

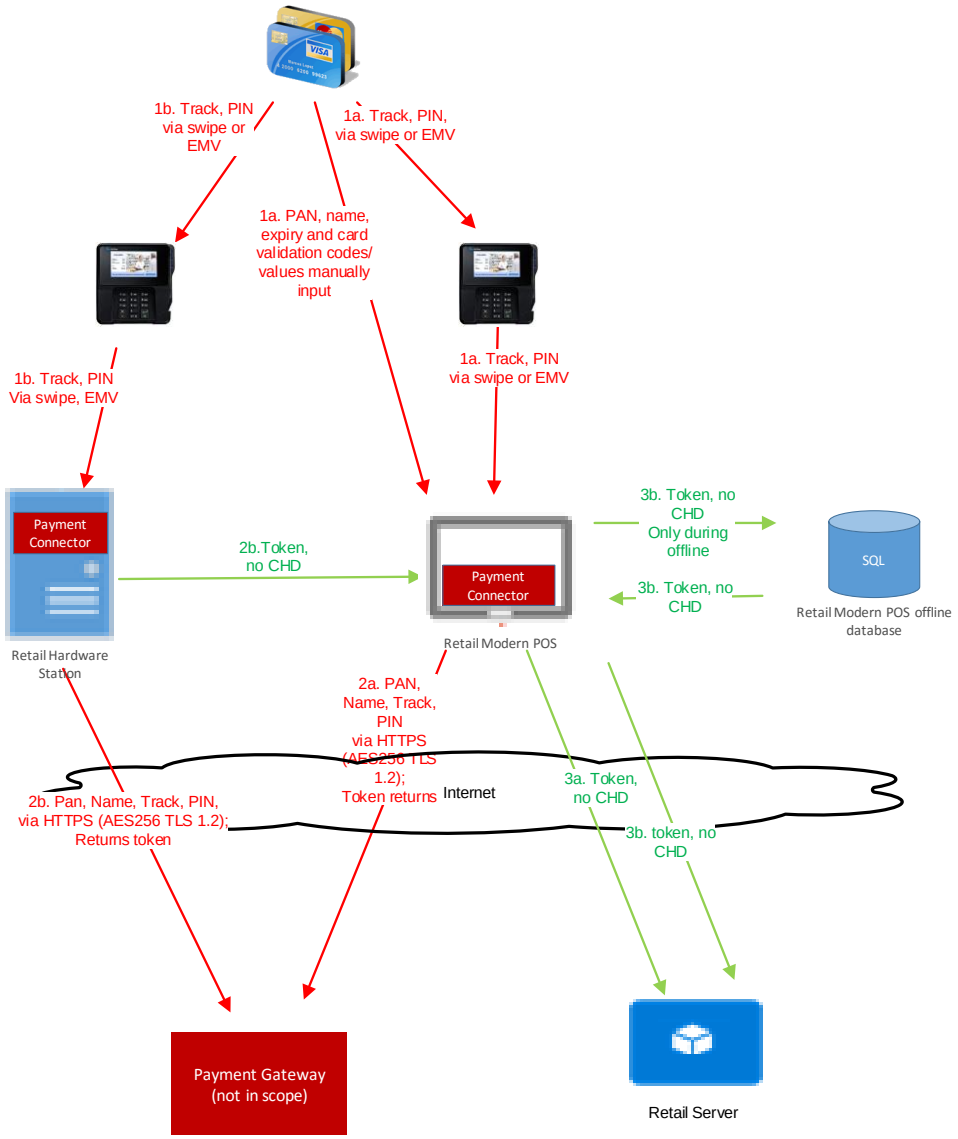
Overall implementation diagram



Payment data flow diagrams

Flow of payment data in Retail Modern POS with full integration model

The following figure shows payment data in Retail Modern POS with full integration model.



Details:

1 Retail Modern POS including Retail Hardware Station receives cardholder data through the following channels:

- **a** For Retail Modern POS:
  - **1** Track or track-equivalent data via PINpad for card-present credit transactions
  - **2** PIN-based transactions via PINpad for debit transactions
  - **3** PAN, expiry, and card validation codes/values manually entered via POS user interface

b Or, for Retail Hardware Station:

1 Track or track-equivalent data via PINpad for card-present credit transactions

2 PIN-based transactions via PINpad for debit transactions

2 Retail Modern POS including Retail Hardware Station processes a payment transaction:

a Retail Modern POS creates authorization requests and sends them out to a Payment Gateway (AES256 TLS 1.2) via a payment connector. The payment connector is provided by a third-party payment solution provider and installed on the same machine. Authorization requests include track or track-equivalent data, PIN block, PAN, expiry, and card validation codes/values. Retail Modern POS receives an authorization reply, including a card token and a transaction approval message.

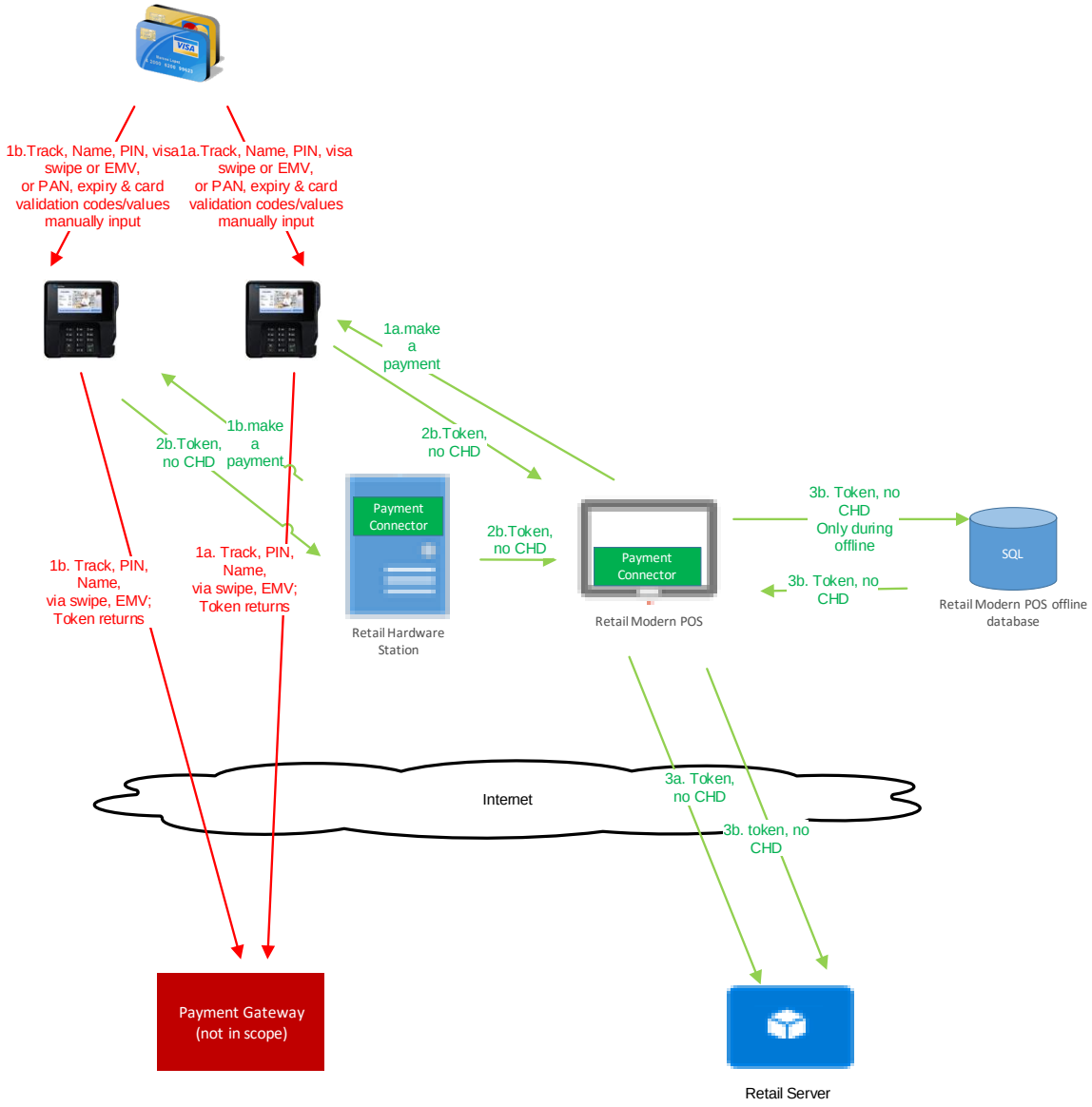
b Retail Hardware Station creates authorization requests and sends them out to a Payment Gateway (AES256 TLS 1.2) via a payment connector. The payment connector is provided by a third-party payment solution provider and installed on the same machine. Authorization requests includes track or track-equivalent data, PIN block, PAN, expiry, and card validation codes/values. Retail Hardware Station receives an authorization reply, including a card token and a transaction approval message. Retail Hardware Station then forwards the truncated PAN (first six and last four digits), card token, and transaction approval message to Retail Modern POS.

3 **a** From Retail Modern POS, only the card token and truncated PAN (first six and last four digits) are sent back to Retail Server on the Azure cloud platform. For the truncated PAN, only the last four digits are stored by Retail Server.

b If Retail Server on the Azure cloud platform is not reachable, the truncated PAN (last four digits) and card token are stored in the Retail Modern POS offline database. After the connection is restored, the truncated PAN (last four digits) and card token are sent back to Retail Server on the Azure cloud platform and stored in a database on the Azure cloud platform, and such data is deleted from the Retail Modern POS offline database.

Flow of payment data in Retail Modern POS with semi-integrated model

The following figure shows the flow of payment data in the Retail Modern POS with semi-integrated model.



Details:

1 Retail Modern POS (1a) or Retail Hardware Station (1b) sends out the payment request to the PINpad asking for a payment. No cardholder data is involved at this point. The PINpad is asking for the payment through the following channels:

- Track or track-equivalent data for card-present credit transactions, including EMV
- PIN-based transactions for debit
- PAN, expiry, and card validation codes/values manually entered via PINpad

The PINpad sends out the authorization request to a Payment Gateway (AES256 TLS 1.2) and receives the authorization reply. Authorization requests include track or track-equivalent data, PIN block, PAN, expiry, and card validation codes/values.

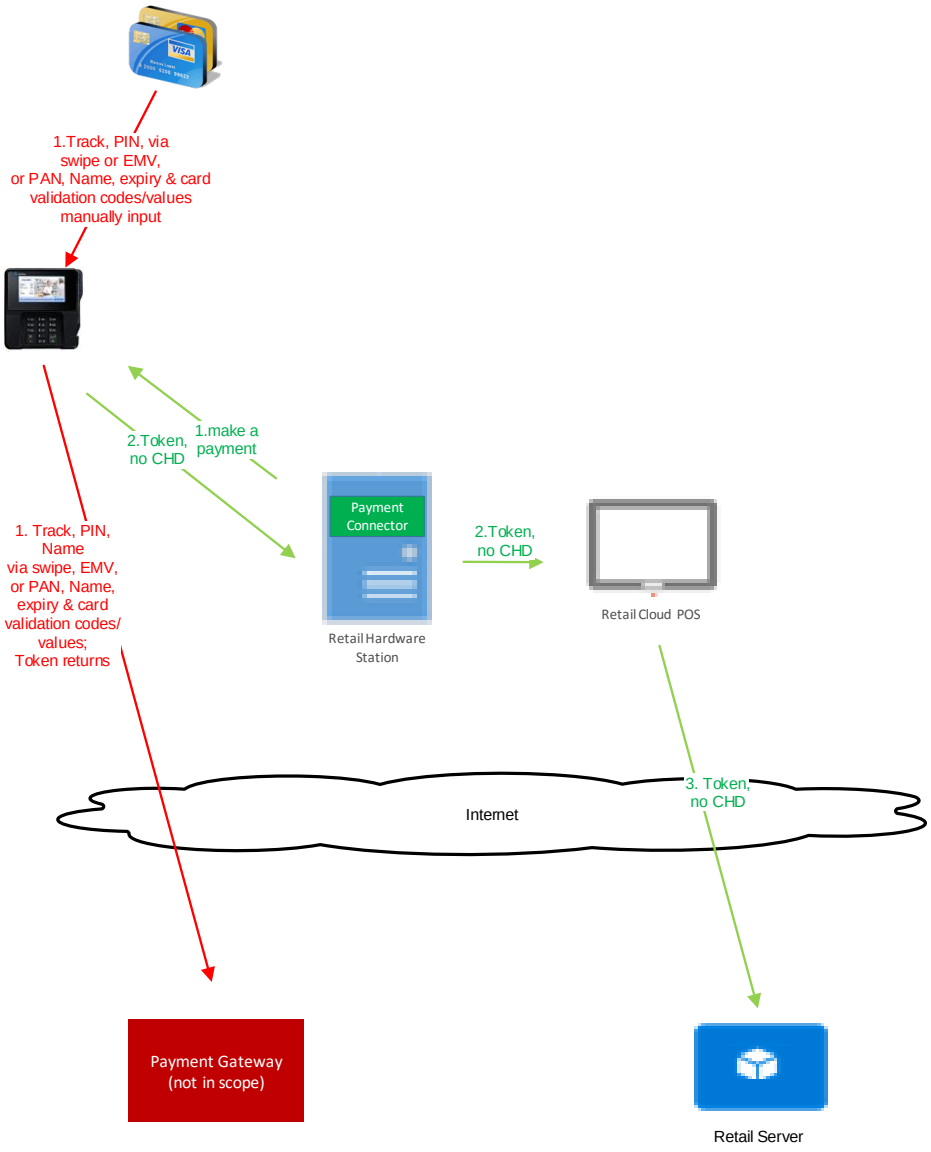
2 The PINpad sends the truncated PAN (first six and last four digits), card token, and transaction approval message directly to Retail Modern POS (2a); or it sends this data to Retail Hardware Station, and Retail Hardware Station forwards the data to Retail Modern POS (2b).

3 **a** From Retail Modern POS, only the card token and truncated PAN (first six and last four digits) are sent back to Retail Server on the Azure cloud platform, and only the card token and truncated PAN (last four digits) are stored by Retail Server in databases.

b If Retail Server on the Azure cloud platform is not reachable, the truncated PAN (last four digits) and card token are stored in the Retail Modern POS offline database. After the connection is restored, the truncated PAN (last four digits) and card token are sent back to Retail Server on the Azure cloud platform and stored in a database on the Azure cloud platform, and such data is deleted from the Retail Modern POS offline database.

Flow of payment data in Retail Cloud POS with Hardware Station semi-integrated model

The following figure shows the flow of payment data in the Retail Cloud POS with Hardware Station semi-integrated model.



Details:

1 Retail Hardware Station sends out the payment request to the PINpad asking a payment. No cardholder data is involved at this point. The PINpad is asking for the payment through the following channels:

- Track or track-equivalent data for card-present credit transactions, including EMV
- PIN-based transactions for debit
- PAN, expiry, and card validation codes/values manually entered via PINpad

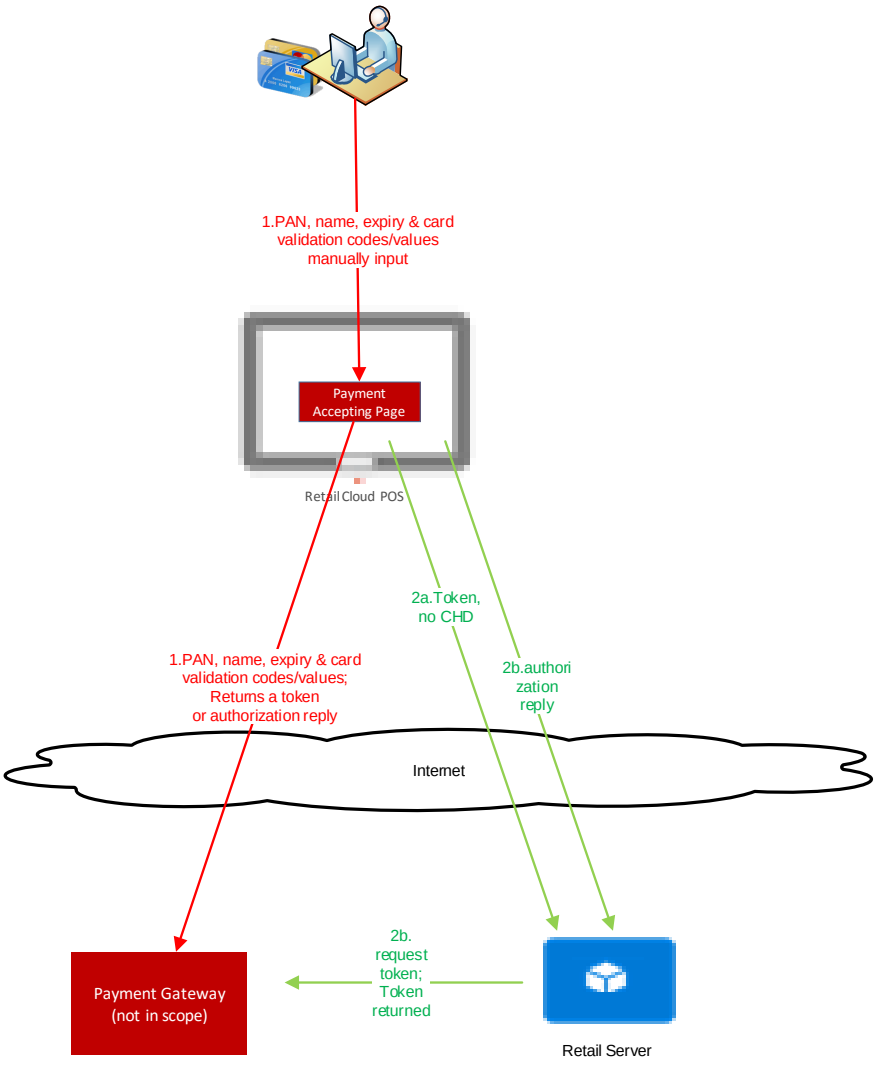
The PINpad sends out the authorization request to a Payment Gateway (AES256 TLS 1.2) and receives the authorization reply. Authorization requests include track or track-equivalent data, PIN block, PAN, expiry, and card validation codes/values.

2 The PINpad sends the truncated PAN (first six and last four digits), card token, and transaction approval message to Retail Hardware Station, and Retail Hardware Station sends the truncated PAN (first six and last four digits), card token, and transaction approval message to Retail Cloud POS.

3 From Retail Cloud POS, only the card token and truncated PAN (first six and last four digits) are sent back to Retail Server on the Azure cloud platform, and the card token and truncated PAN (last four digits) are stored in a database on the Azure cloud platform.

Flow of payment data in Retail Cloud POS with a payment provider payment accepting page

The following figure shows the flow of payment data in the Retail Cloud POS with a payment provider payment accepting page.

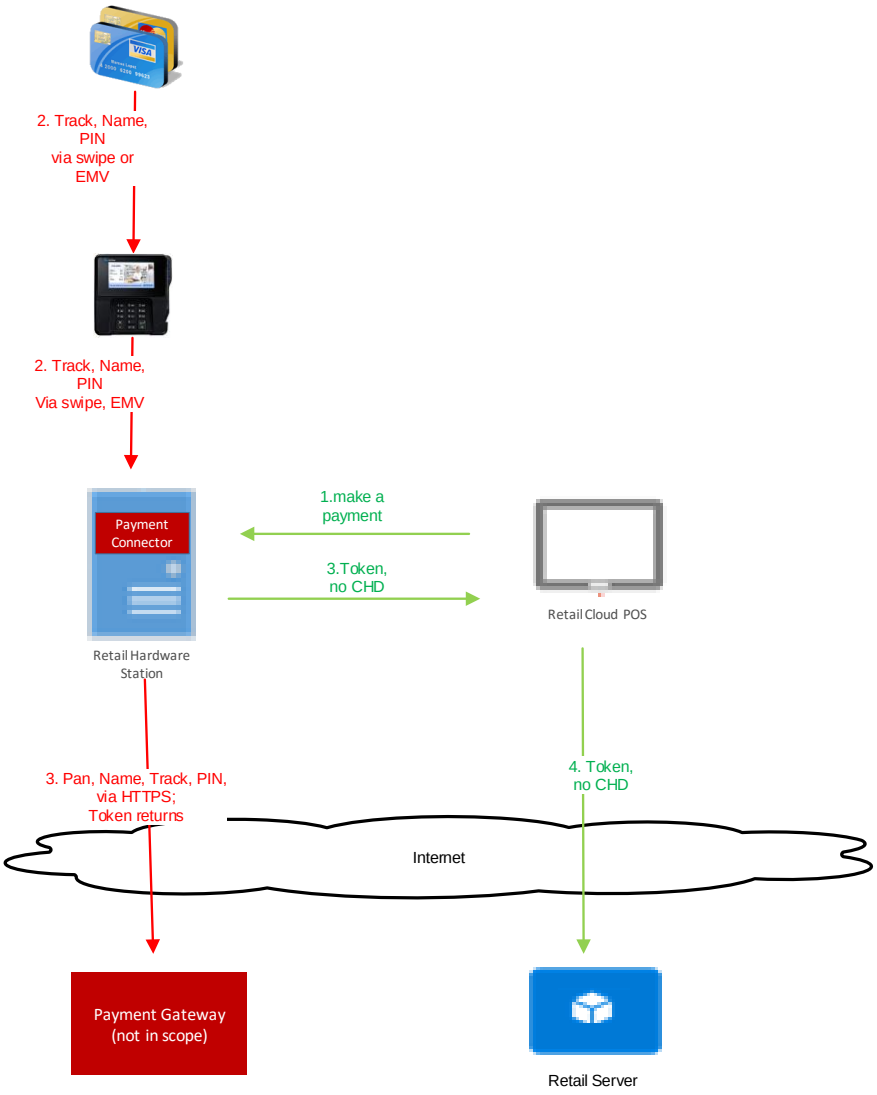


Details:

1. The Retail Cloud POS client renders a web payment accepting page from a third-party payment provider in an Iframe. Cardholder data, including the PAN, name, expiration date, and CVV2, is entered manually into the Iframe-based third-party payment provider's web payment accepting page. The CVV2 is optional. The Iframe-based third-party payment provider's web payment accepting page sends cardholder data, including the PAN, name, expiration date, and CVV2, to the payment provider's payment accepting website for payment authorization and/or tokenization (AES256 TLS 1.2).
2. The Retail Cloud POS client has two ways to receive authorization and a card token:
   a. The Retail Cloud POS client receives a card token and authorization reply from the Payment Gateway and sends the card token and truncated PAN (first six and last four digits) to Retail Server on the Azure cloud platform, and the card token and truncated PAN (last four digits) are stored in database on the Azure cloud platform.
   b. The Retail Cloud POS client receives an authorization reply only. The Retail Cloud POS client forwards the authorization reply to Retail Server on the Azure cloud platform. Retail Server sends the authorization reply to the Payment Gateway to retrieve the card token. Retail Server stores the card token and truncated PAN (last four digits) in a database on the Azure cloud platform.

Flow of payment data in Retail Cloud POS with Hardware Station full integrated model

The following figure shows the flow of payment data in the Retail Cloud POS with Hardware Station full integrated model.



Details:

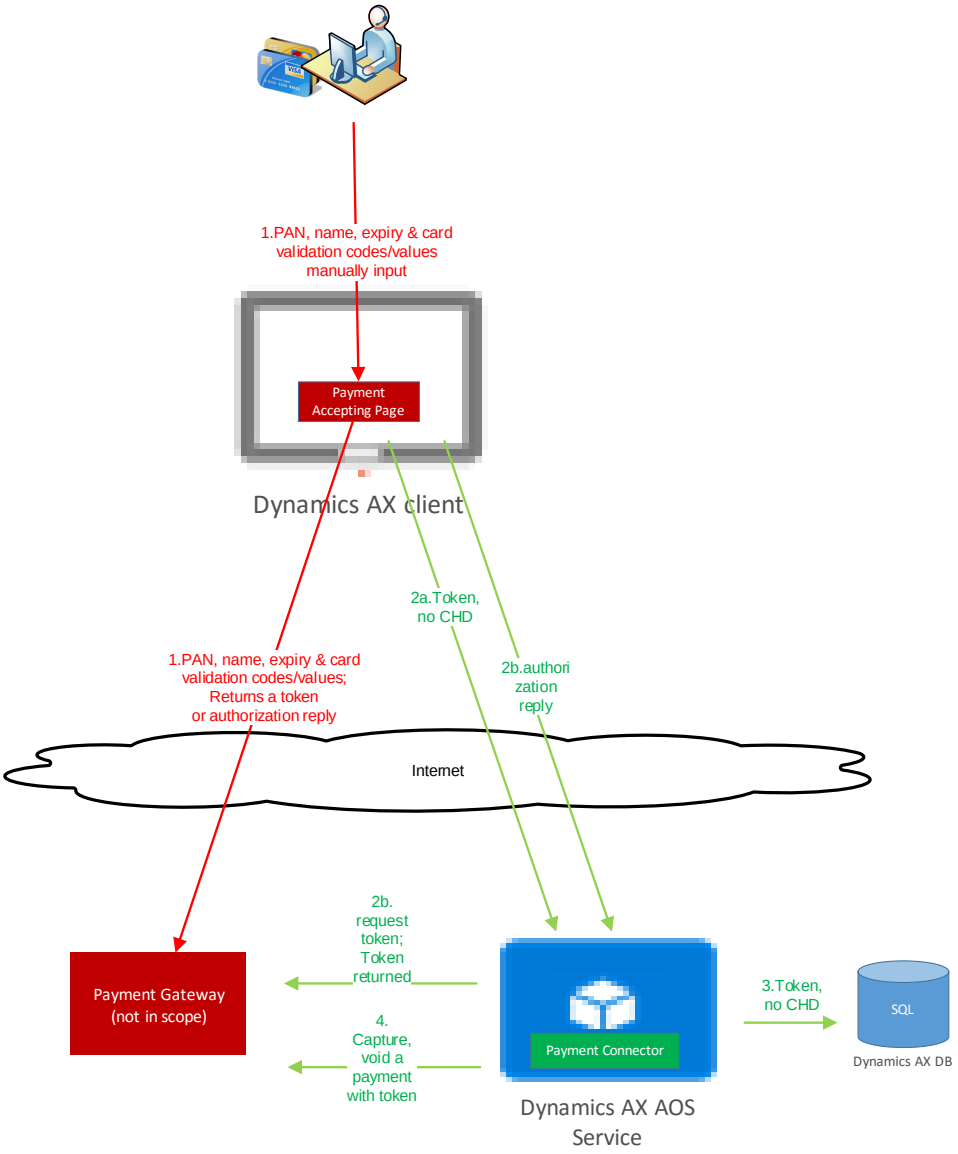
1. Retail Cloud POS requests Retail Hardware Station to make a payment.
2. The customer performs a card-present credit or debit transaction on a payment device connected to Retail Hardware Station.
   a. Track or track-equivalent data for card-present credit transactions, including EMV
   b. PIN-based transactions for debit

3 Retail Hardware Station sends cardholder data (track or track-equivalent data, and PIN block) to the Payment Gateway (AES256 TLS 1.2) for authorization. Retail Hardware Station returns the authorization response, card token, and truncated PAN (first six and last four digits) to Retail Cloud POS.

4 Retail Cloud POS sends the card token and truncated PAN (first six and last four digits) to Retail Server on the Azure cloud platform, and the card token and truncated PAN (last four digits) are stored in a database on the Azure cloud platform.

Flow of payment data in Microsoft Dynamics AX Accounts receivable and Call center

The following figure shows the flow of payment data in Accounts receivable with a payment provider payment accepting page.

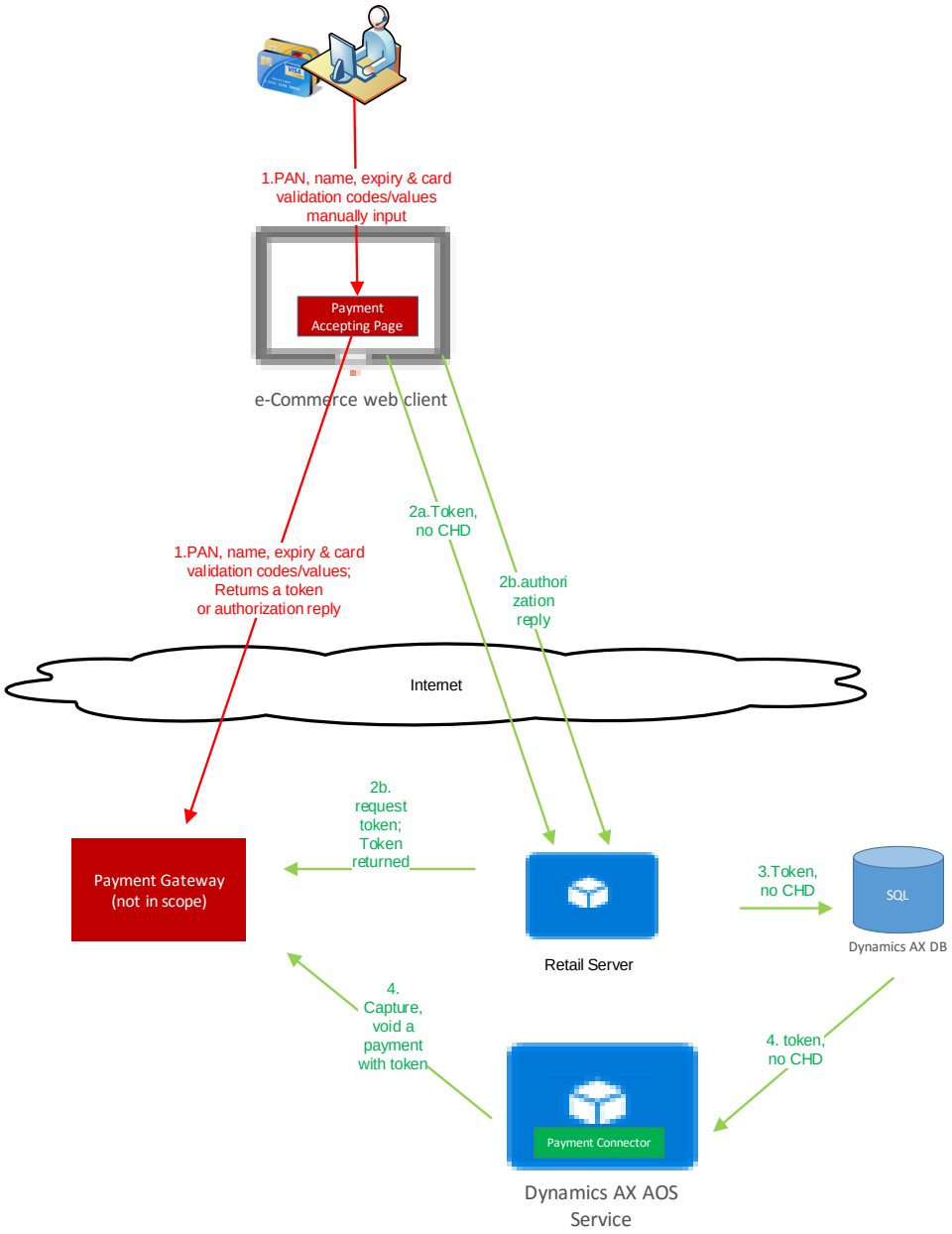


Details:

1. The Microsoft Dynamics AX client renders a web payment accepting page from a third-party payment provider in an Iframe. Cardholder data, including the PAN, name, expiration date, and CVV2, is entered manually into the Iframe-based third-party payment provider's web payment accepting page. The CVV2 is optional. The Iframe-based third-party payment provider's web payment accepting page sends cardholder data, including the PAN, name, expiration date, and CVV2, to the payment gateway's payment accepting website for payment authorization and/or tokenization.
2. The Microsoft Dynamics AX client has two ways to receive authorization and a card token:
   a. The Microsoft Dynamics AX client receives a card token and authorization reply from the Payment Gateway and sends the card token and truncated PAN (last four digits) to the Microsoft Dynamics AX AOS service on the Azure cloud platform.
   b. The Microsoft Dynamics AX client receives an authorization reply only. The Microsoft Dynamics AX client forwards the authorization reply to the Microsoft Dynamics AX AOS service on the Azure cloud platform. The Microsoft Dynamics AX AOS service sends the authorization reply to the Payment Gateway to retrieve the card token.
3. The card token and truncated PAN (last four digits) are stored in the Microsoft Dynamics AX database on the Azure cloud platform.
4. The card token and truncated PAN (last four digits) are used to perform other payment operations by payment connector, such as void or capture.

Flow of payment data in an e-Commerce Sample Web Storefront

The following figure shows the flow of payment data in an E-Commerce Sample Web Storefront with a payment provider payment accepting page.



Details:

1 An e-Commerce web client renders a web payment accepting page from a third-party payment provider in an Iframe. Cardholder data, including the PAN, name, expiration date, and card validation codes/values, are entered manually into the Iframe-based third-party Payment Gateway's web payment accepting page. Card validation codes/values are optional. The Iframe based third-party Payment Gateway's web payment accepting page sends

cardholder data, including the PAN, name, expiration date, and card validation codes/values, to the Payment Gateway for payment authorization and/or tokenization.

2 The e-Commerce web client has two ways to receive authorization and a card token:
   - **a** The e-Commerce web client receives a card token and authorization reply, and sends the card token and truncated PAN (first six and last four digits) back to Retail Server on the Azure cloud platform.
   - **b** The e-Commerce web client receives an authorization reply only. The e-Commerce web client forwards the authorization reply to Retail Server on the Azure cloud platform. Retail Server sends the authorization reply to the Payment Gateway's Payment Gateway to retrieve the card token.
3 The card token and truncated PAN (last four digits) are stored in the Microsoft Dynamics AX database on the Azure cloud platform.
4 The card token and truncated PAN (last four digits) are used to perform other payment operations by the payment connector, such as void or capture.

Part 3: Software updates and support

Software updates

Updates to Microsoft Dynamics AX are either directly applied to the merchant's head office environment in Microsoft Azure by merchant-initiated request or applied to the merchant's point-of-sale system on-premises by merchant-initiated request.

Troubleshooting and support

Microsoft Dynamics AX does not provide the ability to collect or store sensitive authentication data for troubleshooting purposes.

This section outlines the process that Microsoft and its Certified Partners are required to follow when a Microsoft Dynamics AX customer requires troubleshooting of a specific problem. This process is designed to help ensure the security of sensitive information in the database, including employee passwords and payment-related data, and helps satisfy Requirement 3.2 of the PCI Data Security Standard. Support personnel are required to collect only the limited amount of data needed to solve the specific problem being reported.

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

- Collect sensitive authentication data only when it is needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.

- Securely delete such data immediately after use.
- Encrypt sensitive authentication data while it is stored. (No sensitive data is stored by Microsoft Dynamics AX. This refers to any data that might be stored via third-party add-ins or other sources.)

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

- Support personnel access the customer's desktop.
- Support personnel obtain a copy of the store database (which contains no sensitive cardholder data).
- Support personnel travel to the customer's place of business.

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

Support personnel access the customer's desktop

With the customer's specific approval, a support engineer can use Microsoft Skype for Business to access the customer's desktop and investigate the issue directly. Support engineer does not have access to the customer's card number or card data.

Support personnel travel to the customer's place of business

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

Distribution of hotfixes

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

Send feedback.

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.

United States and Canada toll-free: (888) 477-7989

Worldwide: (1) (701) 281-6500

www.microsoft.com/dynamics