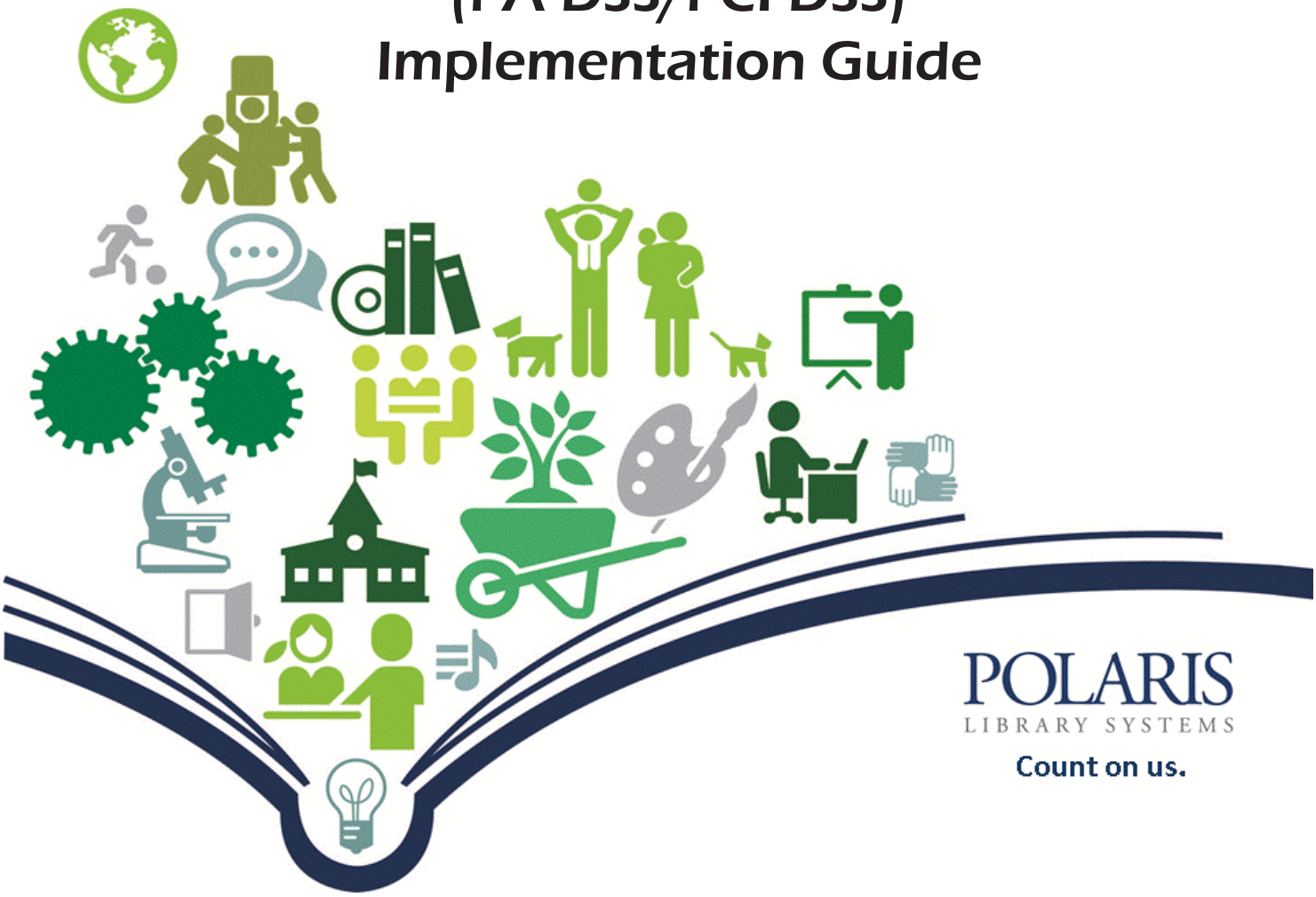
Polaris® E-Commerce Data Security Standard (PA-DSS/PCI-DSS) Implementation Guide



POLARIS
LIBRARY SYSTEMS
Count on us.

POLARIS
LIBRARY SYSTEMS

Copyright © 2013 by Polaris Library Systems

This document is copyrighted and proprietary . All rights are reserved. No part of this document may be photocopied or reproduced in any form without the prior written consent of Polaris Library Systems.

Polaris Library Systems
Box 4903
Syracuse, New York 13221-4903
www.polarislibrary.com

Send any comments or questions about this guide to your Site Manager or to the Technical Communications Group: **TechComm@polarislibrary.com**.

Trademarks Polaris® is a registered trademark of GIS Information Systems, Inc., dba Polaris Library Systems.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

PayPal® and PayflowPro® are registered trademarks of eBay, Inc. Other brands and product names are trademarks of their respective owners.

Disclaimer The information contained in this document is subject to change without notice. Polaris Library Systems shall not be liable for technical or editorial omissions or mistakes in this document nor shall it be liable for incidental or consequential damages resulting from your use of the information contained in this document.

Printed in the
United States of America
August 06, 2013

This guide is written for Polaris 4.1R2.1110 or later.
Rev. 6

Revision History		
Version	**Date**	**Description**
Polaris 4.0.564 - 1	7/6/11	Initial publication
Polaris 4.0.564 - 2	7/12/11	IIS7.5/SSL 2.0; wireless policy; software updates; compulsory audit logs
Polaris 4.0.564 - 3	8/06/11	Content organization improved
Polaris 4.0.564 - 4	8/31/11	Network diagram and software updates practice clarified
Polaris 4.1.520 - 5	2/22/13	Windows Server 2008 R2 and TLS 1.1/1.2
4.1R2	8/2/13	Web servers using SSL/TLS for HTTPs must use 2048-bit certificates by January 1,2014

Contents

© 2013 Polaris Library Systems

Introduction

This document is a reference guide for Polaris Library Systems customers located in the United States who are using or intend to use Polaris e-commerce as part of their Polaris Integrated Library System (ILS). While it is Polaris Library Systems' responsibility to ensure that the Polaris ILS application meets the standards of the PCI Security Standards Council, it is the library's responsibility to make sure its network structure, network maintenance, policies and procedures meet these standards. PCI standards numbers (version 1.2) are included in the margins of the document where applicable.

This document applies specifically to the Polaris version number noted on the title page and is updated and published whenever a Polaris software update requires changes in the security configuration.

About the PCI Security Standards Council

The PCI Security Standards Council is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements. The Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. All five payment brands share equally in the council's governance; have equal input to the PCI Security Standards Council and share responsibility for carrying out the work of the organization. All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs.

To learn more, see the following site link:

https://www.pcisecuritystandards.org/about/index.shtml

PCI Security Standards

The PCI Security Standards were developed by the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures. They include requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. They are intended to help organizations protect customer account data, and are periodically enhanced to include any new or modified requirements necessary to mitigate emerging payment security risks.

© 2013 Polaris Library Systems

PA-DSS

The PCI Payment Application Data Security Standard (PA-DSS) applies to the payment application itself. It is the responsibility of Polaris Library Systems to obtain and maintain PA-DSS certification; that is, to make sure that Polaris is designed to meet the standards for payment applications as set by the PCI Security Standards Council. Polaris Library Systems has worked with a certified security consultant (PA-QSA) to be sure that Polaris 4.1 complies with the provisions of PA-DSS version 1.2.

Important:
Compliance with the provisions of PA-DSS has been achieved for the Polaris application software and the Polaris development environment, but each individual operating environment, including Hosted Polaris, must meet PCI-DSS compliance. See "PCI-DSS" below.

PCI-DSS

The PCI Data Security Standard (PCI-DSS) applies to merchants and e-commerce Web site owners. *It is the library's responsibility to obtain and maintain PCI-DSS certification.* To learn more about PCI-DSS standards, see the following site link:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

You can use the information from that document and the information in this manual to ensure that your library system is PCI-DSS compliant. The table summarizes the general requirements.

Security Practice	*Requirements*	*Responsible Party*		*More Information*
		Polaris	*Library*	
Build and Maintain a Secure Network	Requirement 1: Install and maintain a firewall configuration to protect cardholder data.		X	"Network Firewall Configuration" on page 7 "Remote Access Practices" on page 14 "Wireless Networks" on page 15
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.		X	"Unique User Accounts and E-Commerce Permissions" on page 15 "Wireless Networks" on page 15

© 2013 Polaris Library Systems

Security Practice	*Requirements*	*Responsible Party*		*More Information*
		Polaris	*Library*	
Protect Cardholder Data	Requirement 3: Protect stored cardholder data	X	X	"Data Storage" on page 5
	Requirement 4: Encrypt transmission of cardholder data across open, public networks	X	X	"Data Transmission - Secure Socket Layer (SSL)" on page 5 "Remote Access - Terminal Services" on page 14 "Wireless Networks" on page 15
Maintain a Vulnerability Management Program	Requirement 5: Use and regularly update anti-virus software		X	"Anti-Virus Software" on page 9
	Requirement 6: Develop and maintain secure systems and applications	X	X	"Protecting Cardholder Data" on page 5
Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need-to-know.		X	"Unique User Accounts and E-Commerce Permissions" on page 15
	Requirement 8: Assign a unique ID to each person with computer access.		X	"Unique User Accounts and E-Commerce Permissions" on page 15
	Requirement 9: Restrict physical access to cardholder data.		X	"Unique User Accounts and E-Commerce Permissions" on page 15
Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data.		X	"Auditing Logon/Logoff Events" on page 11 "Best Practices" on page 17
	Requirement 11: Regularly test security systems and processes.		X	"Best Practices" on page 17
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security.		X	"Best Practices" on page 17

PCI-DSS Compliance and Transaction Volume

Note that the library's PCI-DSS compliance requirements may be more stringent if your transaction volume is high. Transaction volume is based on the number of transactions (payments, credits, and voids) in a 12-month period. Merchants are classified at one of four merchant levels based on transaction volume:

- **Level 1** - Any merchant, regardless of acceptance channel, processing over 6,000,000 transactions per year.
- **Level 2** - Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 transactions per year.
- **Level 3** - Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.

© 2013 Polaris Library Systems

- **Level 4** - Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants, regardless of acceptance channel, processing up to 1,000,000 transactions per year.

  Source, Visa USA:
  http://usa.visa.com/merchants/risk_management/cisp_merchants.html?it=c|/merchants/risk_management/cisp.html|Defining%20Your%20Merchant%20Level#anchor_2

As an example, a library with 190,000 patrons, 1.25M items and 5M annual circ may see an average of 12,000 to 14,000 e-commerce transactions per year. This volume falls well within Level 4, a relatively low volume of transactions, and the library's certification requirements may be less stringent.

Polaris and E-Commerce

Polaris supports credit card payments using the credit card processing service PayPal® Payflow Pro®. The library can accept credit card payments from the staff client, Polaris ExpressCheck client, and Web-based public access catalog (PAC) for charges on the patron account and donations to the library (PAC only).

- **Staff client** - The permissioned library staff member selects Credit Card as the payment method in those workflows that involve accepting payments from patrons. The staff member then manually enters or swipes the patron's credit card into the Polaris credit card processing window. Cardholder data is transmitted from the Polaris workstation software to the PayPal Payflow Pro gateway via the PayPal Payflow Pro API. This transmission occurs using an SSL/TLS channel over the Internet.
- **Polaris ExpressCheck (self-check client)** - The Polaris ExpressCheck workstation is equipped with a credit card reader. A logged-in patron can pay fines from the Fines and Fees page of the patron account. The patron selects some or all charges to pay and selects **Pay fines now** to display the payment form, then "swipes" the credit card. Cardholder data is transmitted from the Polaris ExpressCheck workstation software to the PayPal Payflow Pro gateway via the PayPal Payflow Pro API. This transmission occurs using an SSL/TLS channel over the Internet.
- **Polaris PowerPAC (via Internet)** - A logged-in library patron can pay fines from the Fines and Fees page of the patron account. The patron selects the charges to pay and clicks **Pay fines now** to display the payment form. Cardholder data is transmitted from the library's Polaris Web server software to the PayPal Payflow Pro gateway via the PayPal Payflow Pro API. This transmission occurs using an SSL/TLS channel over the Internet. When the transaction is complete, the patron can receive an e-mail receipt that lists the charges paid. PAC users do not have to log in to make a donation.

© 2013 Polaris Library Systems

Protecting Cardholder Data

Data Storage

PCI DSS 1.3.4, PA-DSS 9.1
PCI DSS 3.2, PA-DSS 1.1.4
PCI DSS 3.5, PA-DSS 2.5
PCI DSS 3.6, PA-DSS 2.6, 2.7

Sensitive Authentication Data (SAD) is security-related information (such as card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. Polaris does not store sensitive authentication data. *Absolutely no credit card numbers (PANs), full magnetic-stripe data, or CVV2s are stored in the Polaris patron record or with the Polaris patron account, and they do not appear on printed fine receipts*. The patron account retains only the charge and payment data (amount, dates, reason for charge and payment method), as it does for any other transaction. Polaris stores only a series of Xs and the last 4 digits of the card number in the ILSStoreTransactions database table that is used to track credit card transactions. (Polaris does not support debit card transactions, so no PINs are collected or stored.)

Encryption Key Management

PCI-DSS 4.2, PA-DSS 2.7

Because Polaris does not store cardholder data, cryptographic keys are not necessary to encrypt cardholder data, and there is no cardholder data to be removed during the upgrade process.

Data Transmission - Secure Socket Layer (SSL)

PCI-DSS 4, PA-DSS 12.1

Secure Socket Layer (SSL) provides a secure environment for Web-based credit card transactions that follows industry standards. All communications use https:// by an SSL connection. This standard protocol uses site certificates to encrypt and securely exchange payment data. Payments via Internet from PAC cannot be made unless you have installed an SSL server certificate and an SSL connection has been established. A binding is made between port 443 and the PowerPAC Web site certificate, and SSL encrypts the data transferred from the patron's Web browser to the library's PowerPAC Web site (IIS) server.

To enable SSL in IIS, you must first obtain a certificate that is used to encrypt and decrypt the information that is transferred over the network. The certificate must support 128-bit encryption.

In compliance with Certificate Authority/Browser forum requirements based on NIST Special Publication 800-131A, at the end of 2013 all web browsers and Certificate Authorities (CAs) will no longer sell or support

© 2013 Polaris Library Systems

1024-bit RSA certificates. Certificates issued after January 1, 2014 must be at least 2048-bit key length.

IIS includes its own certificate request tool that you can use to send a certificate request to a certification authority. This tool simplifies the process of obtaining a certificate. For instructions on enabling SSL in IIS, go to:

http://technet.microsoft.com/en-us/library/bb727098.aspx

You must also enable SSL in Polaris Administration. Set the **SSL: Enable** parameter for the Web server to **Yes**. For instructions, see "Setting Web Server Parameters" in the *Polaris Administration Guide* or the equivalent topic in Polaris staff client online help.

For Polaris PowerPAC, patrons must have SSL protocol (https://) enabled for their Web browser and may have to accept the certificate the first time they log on from outside the library.

After receiving payment information from the PAC over an SSL connection, Polaris software uses the PayPal Payflow Pro API to establish a second secure SSL connection to the PayPal payment gateway. The credit information is then passed to the PayPal payment gateway. PayPal securely routes the transaction through the financial network to the appropriate bank, ensuring that your patrons are authorized to make their purchases. The whole transaction is accomplished in a matter of seconds and is immediately settled (approved or declined). If the payment is approved, the patron's library account is credited immediately. No overnight batch processing is required in Polaris.

The library does not have to install its own SSL server certificate for credit card transactions through the staff client and Polaris ExpressCheck. The PayPal Payflow Pro controls are installed on each staff client and ExpressCheck workstation. The credit card transaction data is automatically encrypted via the Payflow Pro controls and is sent directly to the PayPal gateway. SSL is used in the communication between the staff client or Polaris ExpressCheck and the Payflow Pro gateway, but the certificate is installed at the Payflow Pro gateway.

Data Transmission - End-User Messaging Technologies

PCI-DSS 4.2, PA-DSS 12.2

Polaris does not support e-commerce with end-user messaging technologies such as e-mail, instant messaging, or chat, so no cardholder data can be transmitted by these means.

© 2013 Polaris Library Systems

Securing the Network

Polaris customers are responsible for maintaining the security of their networks, servers, and clients. You must maintain a firewall, and keep antivirus software and software patches current on servers and clients.

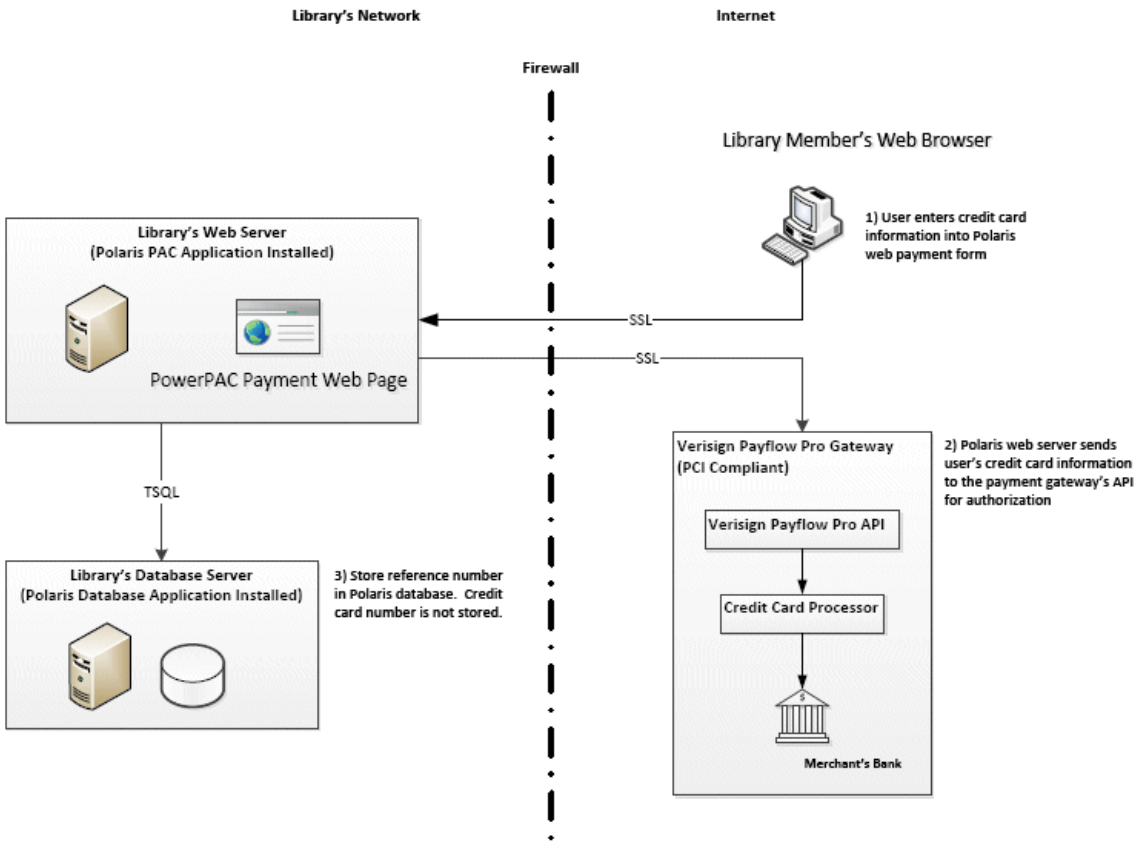
Network Firewall Configuration

PCI-DSS 1.3.4, PA-DSS 9.1

PCI-DSS section 1 requires the installation and ongoing maintenance of firewalls to control computer traffic between your internal "trusted" network and external networks. Your Web server and database server must not be on the same server.

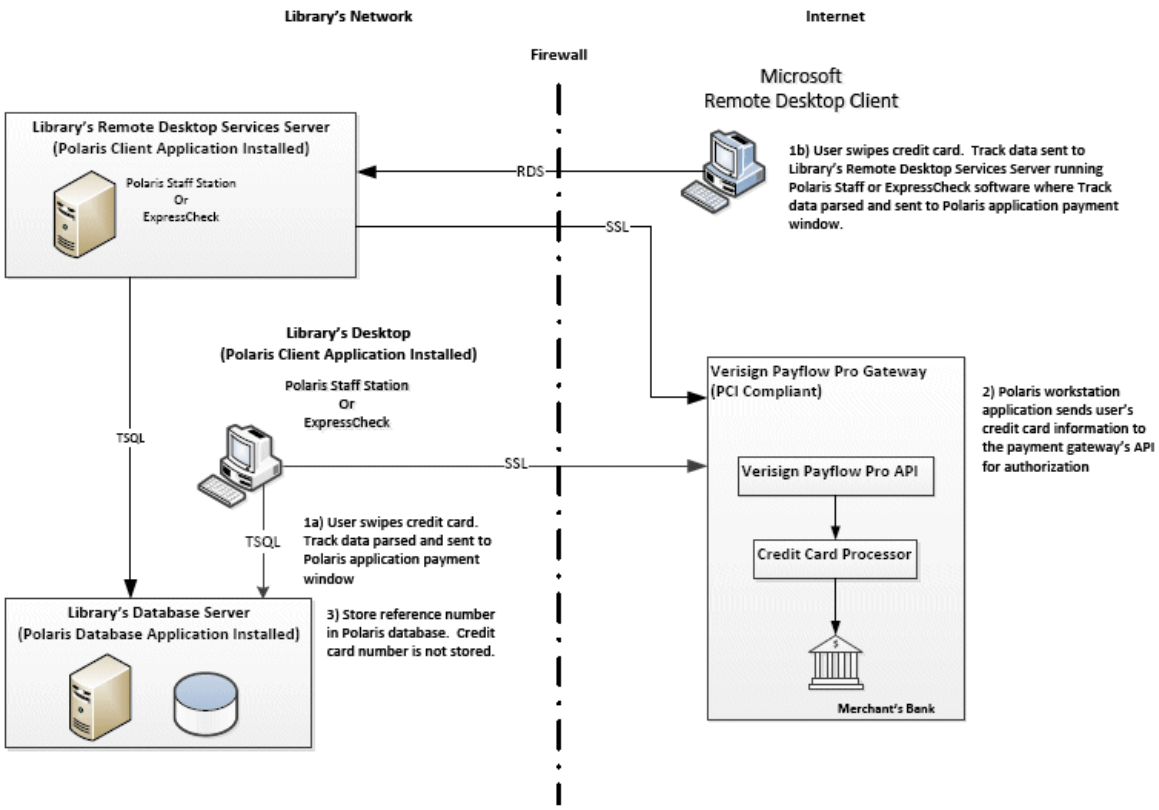
These diagrams show basic network structure with Polaris e-commerce.

Polaris Credit Card Payment – Website – Card Not Present



© 2013 Polaris Library Systems

Polaris Credit Card Payment – Windows Application – Retail



© 2013 Polaris Library Systems

Ports

Ports should be open as follows:

Communication	*Port*	*Purpose*
Client/Server, Server/Server	1	DCOM requires this port to be open if PING is off
	1433	Required for SQL communication
	1434	Required for multiple SQL instances only
	210	Allows Z39.50 searches in remote catalogs
	135	DCOM
	137	Name Resolution
	445	Required for Server Messaging Block
	499	Inter-Library Loan
	5000-5100	Customizable range for DCOM
	13088	Electronic Resource Management System
	443	Secure Socket Layer
Polaris PowerPAC Users	80	HTTP
	443	HTTPS
	210	Z39.50
Remote Desktop Client	3389	Remote Desktop Client Access

Anti-Virus Software

PCI-DSS 5.1

Anti-virus software must be installed and must be configured to automatically receive and install updates in accordance with the manufacturer's recommendations. The anti-virus software must be current, actively running and set to generate audit logs. It should also be capable of detecting, removing and protecting against other malicious software such as adware and spyware. It is the library's responsibility to make sure the anti-virus database is kept up to date and the software license is renewed as needed.

Polaris Software Updates

Updates to the current version of Polaris are initiated by Polaris Library Systems and cannot be started remotely by the customer. Polaris updates are stored on a private server in a secure location. All updates are verified for integrity before installation. Only approved updates are available to Polaris customers.

© 2013 Polaris Library Systems

Security Vulnerability Updates

Polaris Library Systems will notify customers if a security vulnerability is discovered in Polaris software. In addition, Polaris customers should subscribe to services that provide timely security notices and alerts for other system software. For example:

- **US-CERT** (United States Computer Emergency Readiness Team), a part of the Department of Homeland Security, offers mailing lists and feeds for a variety of products including the National Cyber Alert System and Current Activity updates. The National Cyber Alert System was created to ensure that you have access to timely information about security topics and threats. Subscribe to these services at:
  http://www.us-cert.gov/cas/signup.html
- **Microsoft** provides Technical Security Notifications, Alerts and Advisories. Subscribe to these services at:
  http://technet.microsoft.com/en-us/security/dd252948.aspx
- **Most anti-virus software vendors** offer free security alerts and notices. A subscription to the service provided by your anti-virus provider is highly recommended. For example, McAfee Labs Security Advisories is a free notification service that maps high-profile threats to the McAfee technologies. These advisories are intended for McAfee customers. Subscribe to these services at:
  http://www.mcafee.com/apps/mcafee-labs/signup.aspx

IIS 7.5 and Secure Socket Layer (SSL)

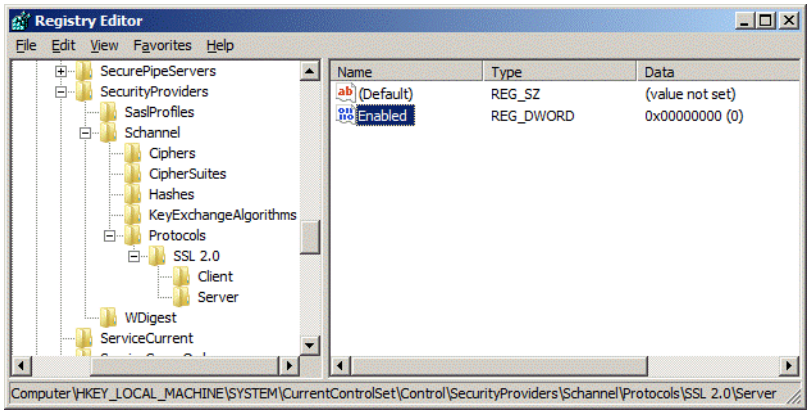
Note:
For more information about SSL, see "Data Transmission - Secure Socket Layer (SSL)" on page 5.

Windows Server 2008 R2 with IIS 7.5 allows SSL 2.0 by default. However, SSL 2.0 is not adequate for PCI-DSS compliance. To properly secure your server and meet PCI-DSS compliance requirements, you will need to disable SSL 2.0 and disable weak ciphers. To disable SSL 2.0 in IIS 7.5 and make sure that the stronger SSL 3.0 or TLS 1.1/1.2 is used, follow these steps:

1. Click **Start**, click **Run**, type **regedit**, and click **OK**.
2. In Registry Editor, locate the following registry key/folder:
   HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0
3. Right-click on the SSL 2.0 folder, select **New** and click **Key**.
4. Name the new folder **Server**.
5. In the new **Server** folder, click the **Edit** menu, select **New**, and click **DWORD (32-bit) Value**.
6. Enter **Enabled** as the name, and press **ENTER**.

© 2013 Polaris Library Systems

7. Confirm that the Data column displays **0x00000000 (0)** (the default value). If a different value is displayed, right-click, select **Modify** and enter **0** as the **Value** data.



8. Restart the computer.

SQL Server Secure Connection

The transaction reference number is supplied to the Polaris database from the staff client or server. You must use a secure connection for SQL Server.

The Polaris database is secured by both indirect and direct methods. Indirectly, that is, via external access from the server, the data is secured by limiting access to the Polaris database with two accounts. The application services account is typically a domain user account that has no administrative rights on the domain, nor on the local server for which the service account runs. The Polaris ILS client connects to the database by first requiring the end-user to authenticate via the Polaris business object, which is running under this service account. In turn, the service account retrieves from the database the connectivity information that is passed back to the client using packet encryption. The connection information contains the SQL account and password that the application will then use to connect to the database. This connectivity information is never exposed to the end-user.

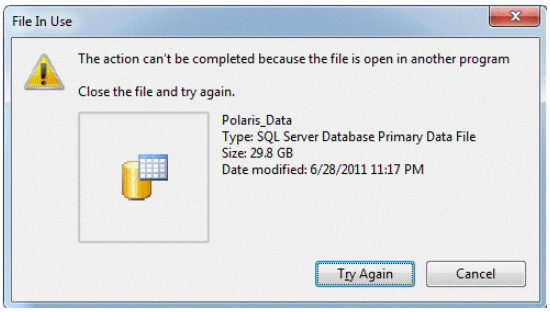
Auditing Logon/Logoff Events

PCI-DSS 10, PA-DSS 4.2

Since the Polaris database resides on a server, the database files cannot be physically accessed without actually logging into the server. Furthermore, administrative credentials are required to access the folders in which the SQL data files reside. Finally, the database files cannot be copied or accessed by any other process while the SQL Server service process to which the database belongs is running, since the process maintains an

© 2013 Polaris Library Systems

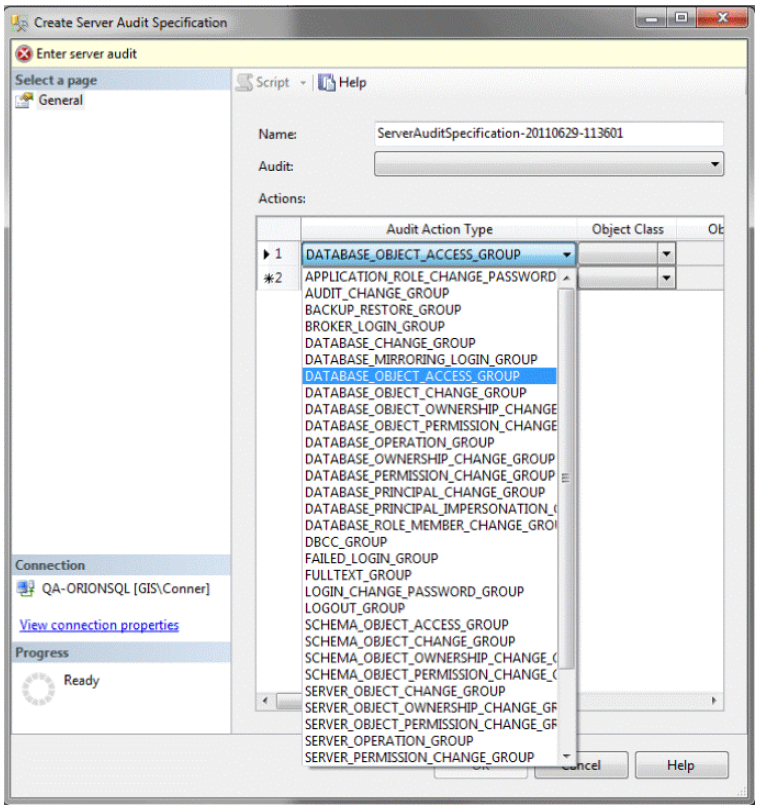
exclusive lock on those files. If server security is compromised and the file system is accessed to copy the database files remotely, the following error dialog is presented when an attempt is made to copy the file:



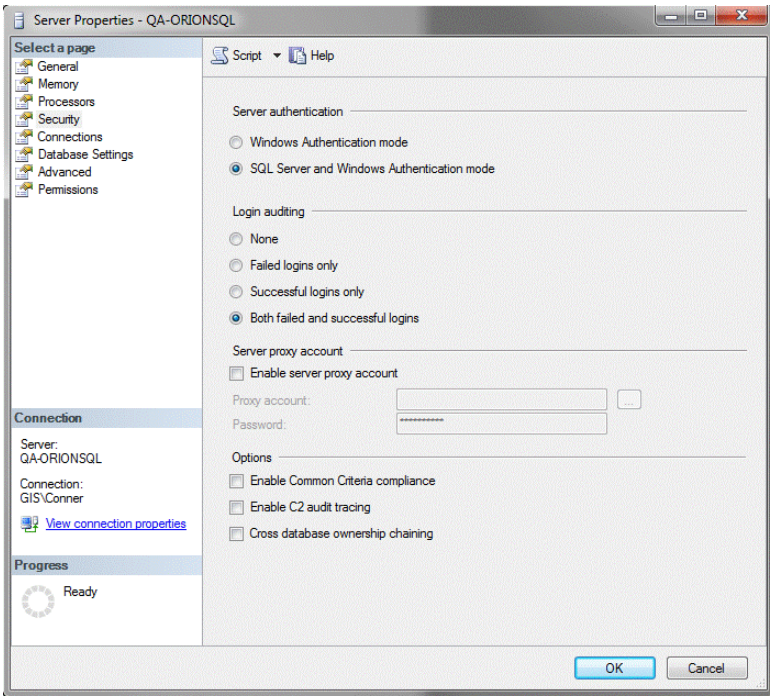
Windows provides the ability to audit logon and logoff events to the server itself, whether they are remote access or physical access attempts. These events are recorded in the event log. SQL Server also provides auditing mechanisms that record database logon and logoff events.

Important:
Audit logs must be enabled for PCI-DSS compliance.

The audit specification in SQL Server can be set to audit events at a very granular level:



For basic auditing purposes, such as failed and successful logons, simpler auditing can also be used:



Server and Client Software Patches

Immediately after you install operating system software on any computer, check for and apply all security updates and security patches from the software manufacturer. On an ongoing basis, security updates and patches, including but not limited to all Critical and Important Microsoft Updates, must be applied regularly according to the software manufacturer's recommendations.

Non-Console Administrative Access

PCI-DSS 2.3, PA-DSS 13.1

You must encrypt all non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. For example, Telnet or rlogin must never be used for administrative access.

© 2013 Polaris Library Systems

Remote Access Practices

PCI-DSS 1, 12.3.9, PA-DSS 10.1, 11.3.b

PCI-DSS compliance requires secure use of remote-access technologies. Use a firewall if the computer is connected via VPN or another "always on" high-speed connection. Examples of remote access security practices include:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8-8.5.15.
- Enable encrypted data transmission according to PCI DSS Requirement 4.1.
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.
- Enable the logging function.
- Restrict access to passwords to authorized personnel only.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Use two-factor authentication (user ID and password and an additional authentication item, such as a smart card, token, or PIN) if you allow any remote access via the Internet or from outside your local/private network to your Polaris system.

Remote Access - Terminal Services

PA-DSS 11.3

You may use Windows Server 2008R2 Remote Desktop Services remote access software. However, to be compliant, every such session must be encrypted with at least 128-bit encryption. For RDP/Terminal Services this means using the high encryption setting. When encryption is set at this level, clients that do not support this level of encryption will not be able to connect. For more information, see

http://technet.microsoft.com/en-us/magazine/ff458357.aspx

© 2013 Polaris Library Systems

Wireless Networks

PCI-DSS 1.2.3, 2.1.1, 4.1.1, PA-DSS 6.1, 6.2

If you will use e-commerce capabilities in a wireless network, the wireless technology must be implemented securely. You must install a perimeter firewall between the wireless network and the cardholder data environment, and configure the firewall to deny or control traffic from the wireless environment into the cardholder data environment. Additionally, you must meet the following PCI-DSS requirements for wireless environments connected to the cardholder data environment or transmitting cardholder data:

- Do not use default encryption keys.
- Encryption keys should be changed when someone who knows the keys leaves the library; also change SNMP community strings on wireless devices.
- Change default settings and passwords on wireless devices.
- The wireless devices firmware must support strong encryption for authentication and transmission; for example, WPA (WiFi Protected Access) or WPA2. Do not use WEP (Wired Equivalent Privacy) security.
- Follow industry standard best practices, such as IEEE 802.11i, when transmitting cardholder data over wireless networks.
- Maintain a wireless access policy for library employees and guest users.
- Maintain an updated network diagram including all wireless network access.
- Document credit card data flows over any wireless network.

Unique User Accounts and E-Commerce Permissions

PCI-DSS 8.5.8-8.5.15

PCI DSS compliance requires that you follow these practices:

- Do not use default administrative accounts for Polaris application logins. For example, do not use the administrator account for staff client access to the Polaris database.
- Assign secure authentication to these default accounts (even if they will not be used), and then disable or do not use the accounts.
- Assign secure authentication for Polaris applications and related systems whenever possible.
- Create PCI DSS-compliant secure authentication to access Polaris by using Microsoft Active Directory best practices as follows:
  - Do not use group, shared, or generic accounts and passwords.
  - Change user passwords at least every 90 days.
  - Require a minimum password length of at least seven characters.
  - Use passwords containing both numeric and alphabetic characters.

© 2013 Polaris Library Systems

- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.

Important:
PCI DSS compliance *requires* that you use unique user IDS and secure authentication best practices. Changing these settings results in noncompliance with PCI DSS.

Polaris Library Systems also recommends that you change the standard PolarisExec user account default password to a complex password.

Each Polaris staff member must have a unique user name and password to access the Polaris staff client. In the Polaris staff client, staff members need the system-level Circulation permissions **Fines: Allow credit card payments** and **Fines: Allow refunds** to accept credit card payments and issue refunds on credit card accounts.

Reports and Error Logs

Payment and refund transactions are recorded in the Polaris Transactions log, where they are available for viewing and reporting. (Cardholder data is not stored in Polaris. See "Data Storage" on page 5.)

Polaris also provides separate credit card error logs for the staff client, Polaris PowerPAC, and Polaris ExpressCheck. These track errors, warnings, and other information about credit card transactions. They do not include cardholder data.

Note:
You should also audit logon/logoff events to the database server itself and to SQL Server. See "Auditing Logon/Logoff Events" on page 11.

© 2013 Polaris Library Systems

Best Practices

In order to sustain PCI DSS compliance, libraries are advised to implement the following recurring security activities for their Polaris ILS environments.

PCI-DSS 1.2 Requirement	*Activity*	*Frequency*
1.1.6	Review firewall and router rule sets at least every six months	Semi-annually
1.1.2	Keep network diagram current	As required
3.6.4	Change cryptographic key(s), at least annually	Annually
5.1	Update anti-virus definitions	Daily/Automatically per manufacturer recommendations
6.1	Ensure that all system components and software have the latest Windows security patches installed	Daily/Automatically per manufacturer recommendations
8.5.5	Remove/disable inactive user accounts at least every 90 days	Quarterly
10.6	Review logs for all system components at least daily	Daily
11.1	Test for the presence of wireless access points by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS to identify all wireless devices in use	Quarterly
11.2	Run internal and external network vulnerability scans at least quarterly	Quarterly
11.3	Perform external and internal penetration testing at least once a year and after any significant infrastructure of application upgrade or modification	Annually or as needed
12.1.2	Conduct risk assessment	Annually
12.1.3	Review and update security policy and procedures	Annually
12.6.1	Deliver security training to employees upon hire and at least annually.	Annually

© 2013 Polaris Library Systems

Appendix: Installation Checklist

Use this section as a guide to installing operating system and Polaris software to meet PCI-DSS security standards.

> **Note:**
> For detailed instructions on installing Polaris software, see the *Polaris 4.1 Installation Guide*, available on the Customer Extranet.

For best results, use the Administrator account rather than an account with administrator privileges to do these procedures.

- ☐ Install the following Microsoft server software on the appropriate servers. Review all licensing issues and requirements whenever you install any Microsoft products.
  - **All servers** - Microsoft Windows Server 2008 R2. After you install the operating system software, go to Windows Updates to check for updates and security patches. Install all Microsoft Windows updates that are critical or recommended.
  - **Application server** - All Polaris servers require MSMQ to be installed if the Polaris Application Server feature is installed as part of the Polaris server-side installation. Message Queuing can be installed under the Features section of the server features list in Server Manager.
  - **Web server, Polaris Fusion provider** - Microsoft Internet Information Services (IIS) and Microsoft Internet Explorer. Mobile PAC also requires ASP.NET MVC 2.0. SMTP is installed as a feature in Server Manager. If selected, its pre-requisite IIS 6.0 Manager will also be installed. The full IIS role (with Web and other features) is not necessary for SMTP to be installed.
- ☐ Create a PolarisServices account on the domain and give the account appropriate rights. The PolarisServices account must be a domain account. If this is a workgroup Polaris application server, then create the PolarisServices account locally in computer management. See "Create a PolarisServices account" and "Give appropriate local security policy rights" in the *Polaris 4.1 Installation Guide*.
- ☐ Open Disk Management and set up the data and tempDB drives. The tempDB drive is used by SQL processes and improves performance. Set the drives to 64K cluster size. Within the drives, create the folder structure **\mssql\data**.
- ☐ Move the databases from the old server to the new location.
- ☐ Install SQL Server 2008 R2 64-bit. If you plan to have both a production and training server, SQL Server will need to be installed individually on each server. You cannot mix a training database and a production database on one server.
- ☐ Create a PolarisExec account for support purposes. See "Create a PolarisExec account" in the *Polaris 4.1 Installation Guide.*

© 2013 Polaris Library Systems

- ☐ Configure DCOM on all servers that will have the Polaris Application Server feature installed.
- ☐ Install the Polaris prerequisite server software on all servers. See "Installing Polaris Windows Components Updates" in the *Polaris 4.1 Installation Guide.*
- ☐ Install Polaris 4.1 server software. See "Installing Polaris Server Software" in the *Polaris 4.1 Installation Guide*. Reboot the server after installing Polaris 4.1 server software. Do not install any Polaris 4.1 server software on the domain controller.
- ☐ Set up the client computers. See "Client Installation" in the *Polaris 4.1 Installation Guide*.

© 2013 Polaris Library Systems