PADSS Implementation Guide for Blackbaud CRM 4.0 Service Pack 5

09/30/2015 Blackbaud CRM 4.0 SP5 PADSS Implementation US

PADSS-2015

Contents

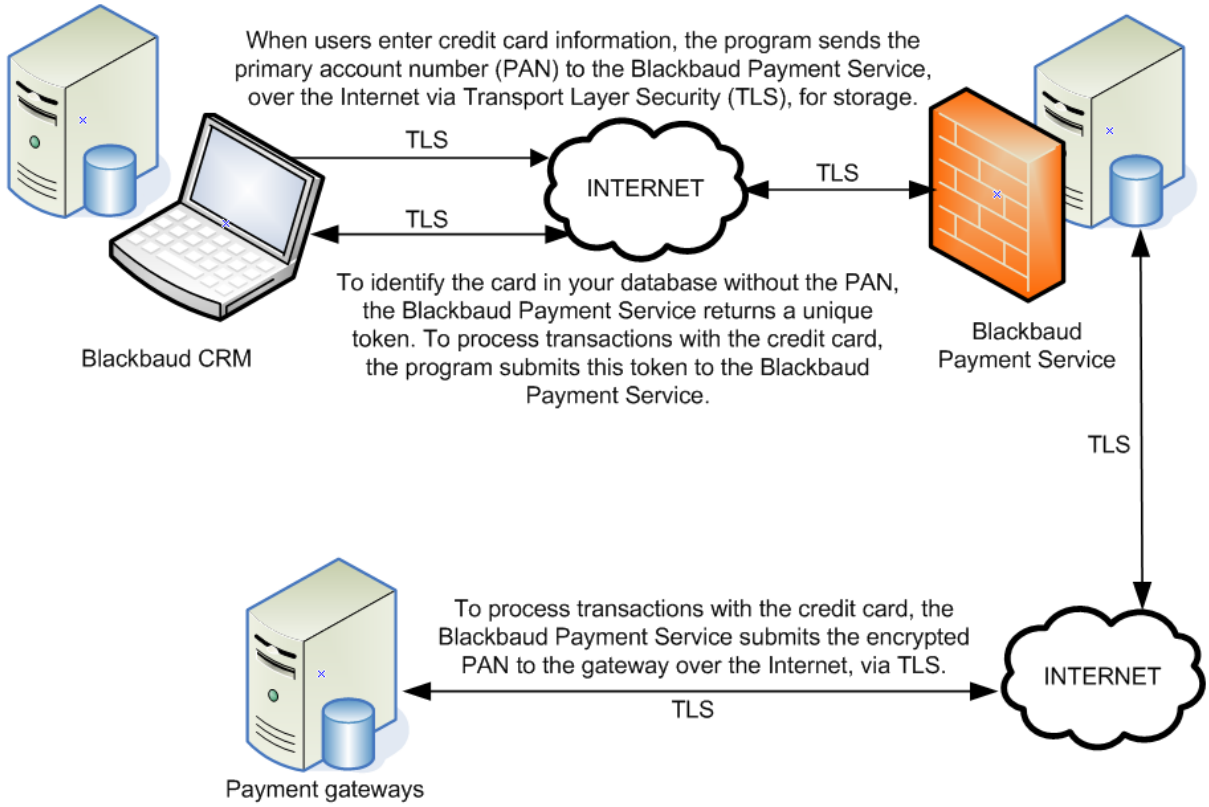
PA DSS Implementation in Blackbaud CRM 4.0 Service Pack 5

Note: This implementation guide is intended for use by Blackbaud clients only. It is not intended for use by resellers or third-party integrators.

Blackbaud CRM 2.0 or later provides enhancements to help you secure your data and comply with Payment Card Industry Data Security Standards (PCI DSS). We strongly recommend you update your software to the latest version.

Blackbaud Payment Service and Blackbaud CRM

Blackbaud CRM does not store full credit card numbers in the database. To securely store credit card and merchant account information, ***Blackbaud CRM*** uses the ***Blackbaud Payment Service***. If you process credit card payments through ***Blackbaud CRM***, the program uses the ***Blackbaud Payment Service*** to transmit credit card information and process transactions through your merchant accounts. When you first submit credit card information to the ***Blackbaud Payment Service*** for storage, it creates a unique reference number for each credit card number to securely identify and process transactions in accordance with PCI DSS.



Warning: Do not send live credit card information to the ***Blackbaud Payment Service*** from a test or staging environment. The ***Blackbaud Payment Service*** automatically purges credit card data received from these environments. To avoid the inadvertent submission of live credit card data to the web service from a test or staging environment, we recommend you delete your ***Blackbaud Payment Service*** credentials from the staging database and configure a firewall rule to prevent access to the web service.

User Account Security and Configuration

To comply with PCI DSS, you must change the supervisor login credentials from the default to a unique login name and complex password. We recommend you also change the login credentials of all default user accounts from their default settings and disable any user accounts your organization does not use. From *Administration*, you can edit the login credentials and manage application user accounts as necessary. For information about the

user account security and complex password requirements for PCI DSS, see User Account Management on page 13 and Network Maintenance on page 21.

Warning: You must create specific user accounts with limited rights to connect to the database. Do not use the default account SA or any accounts in the *SQL Server* role of sysadmin to connect the program to the database.

Warning: Do not change the default installation settings for the requirement of unique user login credentials and secure authentication. Adjustment from the default settings and requirements will result in noncompliance with PCI DSS.

The Microsoft *Windows* operating system stores the passwords for ***Blackbaud CRM*** accounts. To ensure the security of this information, you must use NT LAN Manager (NTLM) v2 authentication and the NT hash to encrypt passwords. Do not use the LM hash to secure passwords. To enable NTLMv2, set the NTLM Authentication Level to "Send NTLMv2 response only". For information about how to enable NTLMv2, see http://support.microsoft.com/kb/239869.

From *Administration*, you can enable ***Blackbaud CRM*** to automatically track the changes users make to tables in your database. To comply with PCI DSS, you must track changes made to all tables related to credit cards and security. To manage the auditing of changes to your database from *Administration*, click **Audit tables**. For information about audit tables and which ones are enabled by default, see the Audit Tables chapter of the *Security Guide* at https://www.blackbaud.com/files/support/guides/enterprise/400/security.pdf.

Warning: Do not disable or subvert the audit table functionality in ***Blackbaud CRM***. Disabling any of the default auto tables will result in noncompliance with PCI DSS.

In order to be compliant with PA-DSS requirement 3.1.11, the application must log out inactive users within 15 minutes and require them to re-authenticate. To accomplish this in ***Blackbaud CRM***, Custom Basic Authentication must be used. Custom Basic Authentication can be used to adapt ***Blackbaud CRM*** to authenticate to any source. By default, Custom Basic Authentication will default to using Windows credentials. Any other sources of authentication will need to have custom code to authenticate correctly.

In order to use Custom Basic Authentication these steps must be followed:

- Disable all authentication methods for the ***Blackbaud CRM*** virtual directory on the IIS web server. This includes, but is not limited to: Anonymous Authentication, ASP .NET Authentication, Basic Authentication, Digest Authentication, Forms Authentication, and Windows Authentication.
- Ensure that the key below is present in the web.config located in the ***Blackbaud CRM*** virtual directory on the IIS web server, and the enabled value is set to “True”.

  <customBasicAuthentication enabled="True" requireSSL="True" cachingEnabled="True" cachingDuration="600" />
- If end users need to land at either or both of these URLs (<path of BBCRM IIS virtual directory>/default.htm or <path of BBCRM IIS virtual directory>/nimbus/default.aspx), then:
  - Enable Anonymous Authentication on the Default.htm file in the root of the ***Blackbaud CRM*** virtual directory on the IIS web server.
  - Enable Anonymous Authentication on the Default.aspx file in the nimbus folder in the root of the ***Blackbaud CRM*** virtual directory on the IIS web server.
- Two keys and values need to be added to the web.config in the root of the ***Blackbaud CRM*** virtual directory on the IIS web server:

  BrowserUserInactivityTimeoutInSeconds
  - This key sets the inactive time threshold where a common user would get logged out of the system and sent back to the login screen.

- The maximum value should be 900, which is 15 minutes and the maximum allowable value to be compliant.

BrowserUserInactivityTimeoutInSeconds_SystemAdmin

- This key sets the inactive time threshold where an administrative user would get logged out of the system and sent back to the login screen.
- The maximum value should be 900, which is 15 minutes and the maximum allowable value to be compliant.

Active Directory Services

To secure your database, the PCI DSS requires your organization to implement guidelines to create and manage network user accounts. ***Blackbaud CRM*** can leverage authentication based on Active Directory services (ADS). With ADS, you can configure user account lockout and enforce complex passwords and password expiration. You can also configure ADS to track users who access the database and lock users out of their workstation after 15 minutes of inactivity.

- To maintain an authentication log, enable the Audit logon events policy, located at Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy. With Audit logon events enabled, you can audit each instance when a user logs on, logs off, or makes a network connection to the database. For information about the Audit logon events policy, see http://technet.microsoft.com/en-us/library/cc787567(WS.10).aspx.
- To lock out a user after 15 minutes of inactivity, enable the Password protect the screen saver policy, located at User Configuration\Administrative Templates\Control Panel\Display. When you enable this policy, you must configure the Screen Saver executable name policy to the screen saver file to use and set the Screen Saver timeout policy to 15 minutes or less. For information about the Password protect the screen saver policy, see http://technet.microsoft.com/en-us/library/cc940428.aspx.

For information about how to configure ADS to manage user accounts, visit Microsoft TechNet at http://technet.microsoft.com.

Sensitive Authentication Data and Cardholder Data

When you enter new credit card information into ***Blackbaud CRM***, the program automatically sends the data to the ***Blackbaud Payment Service*** for storage and retains the reference number generated by the web service. For reference, only the last four digits of the credit card numbers appear in the program.

Note: Prior to version 2.0, ***Blackbaud CRM*** stored unencrypted cardholder data. After you update to ***Blackbaud CRM 2.0*** or later, the program is configured to automatically drop cardholder data from the database which would have been stored in a version prior to ***Blackbaud CRM 2.0***. This data is unrecoverable due to the fact that there are no keys to recover it with. Since ***Blackbaud CRM 2.0*** or later does not store cardholder data, there is no cardholder data to securely purge as required by PA DSS requirement 2.1. No previous versions of ***Blackbaud CRM*** used encryption; therefore, there is no cryptographic data to securely remove as required by PA DSS requirement 2.6.

Your organization can use attributes, notes, and free-text fields to store important information. However, do not use these features to store information such as sensitive authentication data or cardholder data in the program. The abuse or misuse of the program to store this information can leave you vulnerable to an attack by malicious users. If your organization used attributes, notes, or free-text fields to store sensitive authentication data or cardholder data, you must securely delete this data from your database to comply with PCI DSS.

Blackbaud CRM does not facilitate the transmission of primary account numbers (PANs) through messaging technology such as email or instant messages. For information about the transmission of cardholder data over open public networks, see Cardholder Data Encryption on page 13.

Records

Blackbaud CRM does not store or log any primary account numbers (PANs) or sensitive authentication data (SAD).

When you create a new revenue record, the program automatically sends the credit card information entered to the ***Blackbaud Payment Service*** when you click **Save**. On the saved record, only the last four digits of the primary account number (PAN) appear.

In accordance with PCI DSS, your organization must develop and maintain a data retention and disposal policy. You must keep cardholder data storage to a minimum and limit the retention time to only the duration required for business, legal, and regulatory purposes.

Batch Entry

When you enter a credit card number for a transaction in a batch and leave its row, only the last four digits of the credit card number appear in the row. When you save the revenue batch, the program sends the credit card numbers to the ***Blackbaud Payment Service*** for secure storage.

Import

In accordance with PCI DSS, you cannot import full credit card numbers into ***Blackbaud CRM***. To process credit card transactions with imported data, you must instead import the reference token generated by the ***Blackbaud Payment Service*** for the credit card numbers.

Export

In accordance with PCI DSS, you cannot export full credit card numbers from ***Blackbaud CRM***. Exported credit card numbers appear as a series of asterisks followed by the last four digits of the primary account numbers (PANs).

Merchant Accounts

Blackbaud CRM does not store unencrypted login credentials for merchant accounts in the database. The program uses the ***Blackbaud Payment Service*** to store your organization's merchant account information.

Blackbaud CRM can retrieve your merchant account information from the ***Blackbaud Payment Service***. If your organization uses additional Blackbaud programs that process payments, you can view and select merchant accounts added through that program in ***Blackbaud CRM***.

Credit Card Processing

Blackbaud CRM does not include unencrypted credit card numbers in the transmission files generated by the credit card processing process. Instead, the transmission files include the reference number received from the ***Blackbaud Payment Service*** for each credit card number. To process credit card transactions, the program sends the transmission file to the ***Blackbaud Payment Service***, which replaces the reference numbers with their corresponding credit card numbers and sends the transmission file to your payment gateway for authorization.

Versioning Scheme

Blackbaud CRM follows a numeric versioning scheme to identify the latest software release and the type of update. The versioning scheme structure is the major release number, minor release number, build number, and patch, with each number separated by a period:

major.minor.build.patch

The major release number increases when significant changes to the product's functionality or user interface are added. The minor release number increases when smaller changes to the product's behavior or user interface, such as adding, removing, or changing specific behavior, are made. A build number change indicates the latest build of the application and could indicate a security-impacting change to the system. The patch segment is a wildcard character and will be incremented with each patch to a build. The patch segment indicates cosmetic changes or minor functionality changes and will never indicate a security-impacting change. The build segment is the only segment which, when changed, could imply a security-impacting change. When a security-impacting change is made, the Release Notes for that version will communicate the security impact. When no security-impacting change is made, the Release Notes will indicate as such.

For example, the third patch released for version 1.1 of and addressed in build 7 appears as Patch 1.1.7.3.

Rollback and Uninstall

Before you install any updates, we strongly recommend you back up your database. For information about the update process, see the *Installation and Upgrade Guide*.

If you encounter problems during the installation process, you can cancel the installation before it finishes. After you cancel, the install utility returns your machine to its state before the installation. If you complete the installation process but feel the program may have installed improperly, you can sue the **Add or Remove Programs** utility, available from the Control Panel in *Windows*-based operating systems, to safely uninstall the application.

All installation and update guides are available from the user guides area of our website at https://www.blackbaud.com/support/guides/guides.aspx.

Blackbaud may deliver an installation or update through remote access, such as to help resolve a Support issue. If your organization receives an installation or update through remote access, you must secure the use of remote access technology only as needed and ensure the immediate deactivation of the remote access upon completion. For a computer connected through VPN or another high-speed connection, use a personal firewall to secure the "always-on" connections. For information about how to use remote access in compliance with PCI DSS, see Remote Access on page 19.

Transport Layer Security (TLS) Configuration

To configure ***Blackbaud CRM*** for secure communications, you must implement and install a certificate from a trustworthy Certificate Authority (CA) source and implement industry standard network security protocols. Transport Layer Security (TLS) is a protocol that provides communications privacy and security between two applications communicating over a network. Microsoft Internet Explorer, as well as many other modern browsers, supports TLS. ***Blackbaud CRM*** version 4.0 Service Pack 5 (or higher) supports the use of TLS 1.2 to safely transmit confidential information over networks.

It is essential to employ secure server settings to support TLS 1.2. Environments using Microsoft Windows Server 2008 R2 require specific configuration changes to enable TLS 1.2, which later versions of Windows Server do not.

Note: If you use Windows Server 2008 R2, you must review http://support.microsoft.com/en-us/kb/245030 to ensure your server is configured correctly.

Blackbaud recommends putting in place controls that will help reduce the risk of using older protocols until your organization updates to ***Blackbaud CRM*** version 4.0 Service Pack 5 (or higher) which supports the use of TLS 1.2. For information about risk-mitigation controls, see the PCI Security Council Information Supplement Migrating from SSL and Early TLS at https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information Supplement_v1.pdf.

Warning: Versions of Microsoft Windows Server prior to 2008 R2 do not support TLS 1.2. Using an unsupported version will result in noncompliance with PCI DSS.

To ensure the security of data from ***Blackbaud CRM***, you must configure your TLS settings to enforce strong encryption. To prevent weak encryption of credit card information, follow the guidance of OWASP on the use of strong protocols and ciphers. For more information, see https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet.

In order to ensure the most secure cryptography configuration settings and that only trusted keys and/or certificates are accepted the following steps are recommended:

- Inspect that the certificate has a valid signature
- Renew certificates every year, always with new private keys

Additional guidance on the installation of trusted certificates is available through many third party sources including the following:

https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf

Warning: If you modify the registry file incorrectly, serious problems may occur. Before you edit the registry, we strongly recommend you create a backup so you can restore the file if necessary. For information about how to back up and restore the registry file, see http://support.microsoft.com/kb/322756.

Protected Configuration and IIS Registration

To ensure the security of data, do not store highly sensitive information—such as user names, passwords, connection strings, and encryption keys—in a format that is easily read or decoded. To help secure sensitive information, ASP.NET provides a feature called Protected Configuration. To use Protected Configuration to encrypt the contents of the web.config file that contains the credentials used for services integration, run the ASP.NET IIS Registration tool on the web server that hosts ***Blackbaud CRM*** or ***Blackbaud Internet Solutions (BBIS)***.

Tip: To verify encryption, view the contents of the web.config file before and after you run the IIS Registration tool. The web.config file appears in the BBNCSvc folder in the root deployment directory of Blackbaud CRM, such as <deployment folder>\bbappfx\vroot\BBNCSvc. In the <configuration> section of an encrypted web.config file, keys are encrypted and the application settings display attributes for the configProtectionProvider and CipherData.

To encrypt the web.config file with the ASP.NET IIS Registration tool, run as a user with administrative rights, open a command-line window, and execute the Aspnet_regiis.exe tool located in the %windows%/Microsoft.NET/Framework/<version number> folder.

```
cd C:\WINDOWS\microsoft.net\Framework\v2.0.50727

aspnet_regiis -pe "appSettings" -app "/bbAppFx/BBNCSvc"
```

Note: These commands include the default arguments for standard deployments. If necessary, replace the arguments below to match your specific deployment. For example, replace the argument for the -app parameter to match the virtual directory for your deployment such as -app "<BlackbaudCRMVirtualDirectory>/BBNCSvc".

After you run the command, Encrypting configuration section... Succeeded! should appear in the command-line window.

For information about the IIS Registration tool and Protected Configuration, refer to the Microsoft Development Network (MSDN) at http://msdn.microsoft.com/en-us/library/zhhddkxy.aspx and http://msdn.microsoft.com/en-us/library/53tyfkaw.apsx.

Download File Verification

To ensure the integrity of files downloaded from Blackbaud, each product download page contains cryptographic Secure Hash Algorithms (SHA) that produce unique message digests, or checksums, of each file. To confirm that a file downloaded from Blackbaud is unaltered from its original source, you can use a SHA-1 utility to calculate your own checksum for the file to verify it matches the checksum provided by Blackbaud. You can obtain a SHA-1 utility for most operating systems.

- For *Windows*, you can use the File Checksum Integrity Verifier (FCIV) utility package, available for download at http://support.microsoft.com/kb/841290.
- For *Mac OS X*, you can enter the prompt openssl sha1 [full path to file] through the Terminal. For information about Mac and SHA-1, see http://support.apple.com/kb/HT1652.
- For *Linux*, most installations provide a sha1sum command for SHA-1 checksums.

Services and Protocols

Blackbaud CRM does not require the use of any insecure services or protocols. The services and protocols that ***Blackbaud CRM*** requires are Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS), which require port 443.

Ports to Open on the Windows Firewall

Only the following ports must be open in for the application server to communicate with the database server: TCP 1433 and TCP 1036.

Only the following ports must be open for AD integration: TCP 88, TCP 445, UDP 88, and UDP 389.

Note: Opening additional ports other than those noted above to accomplish may result in a non-secure network configuration.

For payment services to function correctly, you must configure your firewall to allow inbound and outbound traffic to and from https://payments.blackbaud.com and https://payment.service.blackbaudhost.com over port 443.

For the SQL Server installations, enable Named Pipes and TCP/IP Connections. For basic instructions from Blackbaud, see Enable Named Pipes and TCP/IP Connections at https://www.blackbaud.com/files/support/infinityinstaller/content/installermaster/tkenablenamedpipesandtcpipconnections.htm. For Microsoft's guidance about network protocols, see Choosing a Network Protocol at http://technet.microsoft.com/en-us/library/ms187892.aspx.

For detailed information on environment configuration of both web and database servers, including instructions and documentation on Windows services required for ***Blackbaud CRM***, please see the Blackbaud Infinity Installation Guide at https://www.blackbaud.com/files/support/infinityinstaller/infinity-installation.htm.

PCI DSS Implementation

When you accept payment cards for donations or revenue, the security of the credit card information is very important. Used properly, Blackbaud programs can help you maintain this information in accordance with the Payment Card Industry Data Security Standard (PCI DSS). To help promote this awareness of the security requirements for credit card and cardholder data, this chapter provides information about PCI DSS and how it impacts your organization. With the proper security of credit card information, you can protect your constituents and clients from inconvenience and financial and personal loss, and help protect your organization from additional expense.

Note: This guide provides only an overview of PCI DSS requirements and recommended best practices to ensure compliance. For additional detail, visit https://www.pcisecuritystandards.org to download the PCI DSS specification.

Payment Card Industry and Payment Application Data Security Standards

Developed by Visa, the Payment Application Data Security Standard (PA DSS) requires software companies such as Blackbaud to develop secure programs that enable users to comply with the PCI DSS. To learn more about PA DSS and download the specification, visit http://usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc.

Note: The Payment Card Industry (PCI) Security Standards Council includes American Express, Discover Financial Services, JCB International, Mastercard Worldwide, and Visa Inc. and was formed to help implement consistent data security measures on a global basis.

Developed by the PCI Security Standards Council, the PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other proactive measures. As an organization that collects payment card information, such as to process payments or donations, you must adhere to the PCI DSS and proactively protect this data. To learn more about PCI DSS and download the specification and its supporting documents, visit https://www.pcisecuritystandards.org.

Note: Depending on your organization and the number of payment card transactions you process, you may need to engage an external security assessment company to determine your level of compliance with PCI DSS

and other security compliance programs. If you use an external assessor, we recommend you select one that is qualified and familiar with the latest requirements from the PCI Security Standards Council. To validate whether your organization is compliant with PCI DSS, we recommend you also visit https://www.pcisecuritystandards.org and complete the PCI Security Standards Council Self-Assessment Questionnaire.

Data Management

Encryption is necessary to protect cardholder data. If a user circumvents security controls and gains access to encrypted data, without the proper cryptographic keys, the user cannot read or use the data. To reduce the risk of malicious abuse, you must consider other effective methods to protect stored data. For example, store cardholder data only when it is absolutely necessary, and do not send the cardholder data in unencrypted email messages.

Sensitive Authentication Data and Cardholder Data Retention

You should keep the storage of cardholder data to a minimum. To comply with PCI DSS, your organization must develop and maintain a data retention and disposal policy.

- Limit the cardholder data stored and the retention time to only that which is required for business, legal, and regulatory purposes.
- Purge all cardholder data that exceeds the retention period.

Do not retain sensitive authentication data, such as the full magnetic stripe, card validation code, or personal identification number (PIN) information, in your database. If you must retain sensitive authentication data, such as for troubleshooting purposes, you must follow these guidelines:

- Collect sensitive authentication data only when necessary to solve a specific problem.
- Store sensitive authentication data only in specific, known locations with limited access.
- Collect only the limited amount of data necessary to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete sensitive authentication data after use.

Warning: To comply with PCI DSS, you must remove historical sensitive authentication data and cardholder data from your database. If you upgrade from a non-compliant version, or if your organization used attributes, notes, or text-free fields to store sensitive authentication information or cardholder data, you must search for and securely delete this data from your database to comply with PCI DSS.

To ensure the complete and secure removal of cardholder data, you must securely erase temporary files that may contain sensitive authentication information and cardholder data.

- If you use Microsoft *Windows XP* or *Windows Vista*, turn off System Restore on the System Properties screen. To track changes in *Windows*, System Restore creates and uses restore points, which may retain cardholder data. When you turn off System Restore, the operating system automatically removes existing restore points and stops the creation of new restore points.
- To ensure the complete removal of data, install and run a secure delete tool such as Heidi *Eraser*. With a secure delete tool, you can safely erase temporary files that may contain sensitive information or

cardholder data. For information about how to install and run the secure delete tool, refer to the manufacturer's documentation.

Cardholder Data Encryption

To comply with PCI DSS, your organization must encrypt cardholder information during transmission over open public networks that malicious users could abuse to intercept, modify, and divert data during transit. These open public networks include the Internet, WiFi (IEEE 802.11x), the global system for mobile communication (GSM), and general packet radio service (GPRS). To safeguard sensitive authentication information and cardholder data during transmission, use strong cryptography and security protocols such as Transport Layer Security (TLS) version 1.2 (or above) and Internet Protocol Security (IPSEC). Never send unencrypted cardholder data in an email message.

Network Security

With a secure network, you can protect your system and credit card information from internal and external malicious users. To secure your network, we recommend you utilize a firewall and configure wireless devices and remote access software.

User Account Management

To comply with PCI DSS, you must assign unique identification to each person who accesses networks, workstations, or servers that contain the program or cardholder data. Unique login credentials ensure that only authorized users can access and work with the critical data and systems included in your network. With unique login credentials, you can also trace actions on your network to specific users. These credentials must include a unique user name and a way to authenticate the user's identity, such as a complex password, a token key, or biometrics.

At a minimum, your organization must implement these guidelines to create network user accounts and manage user authentication and passwords. You must communicate password procedures and policies to all users who can access cardholder data.

- Use authorization forms to control the addition, deletion, and modification of user IDs.
- Verify the identity of users before you reset passwords.
- Immediately revoke account access for terminated users.
- Remove or disable inactive user accounts at least every 90 days.
- Enable user accounts for use by vendors for remote maintenance only when needed, and immediately deactivate them after use.
- Do not use group, shared, or generic user accounts and passwords.
- Require users to change their initial passwords immediately after the first use and subsequent passwords at least every 90 days.
- Require passwords with a minimum length of seven numeric and alphabetic characters.
- Require that new passwords not match one of the last four passwords used by the user.
- Lock out the user account after no more than six failed login attempts. Set the lockout duration to 30

minutes or until a system administrator enables the user account.

- Log out idle sessions after 15 minutes so users must enter the password to activate the workstation.
- To log user authentication and requests, turn on database logging in Microsoft *SQL Server*.

Audit Trails and Centralized Logging

PA-DSS 4.1 states that Payment Applications must set PCI DSS-compliant log settings, per PCI DSS Requirement 10. In addition, logs must be enabled, and disabling the logs will result in noncompliance with PCI DSS. ***Blackbaud CRM*** has PA-DSS-compliant logging enabled by default. Assurance that logging is in place is contingent on operating system and web server logging remaining enabled.

Enable database logging in SQL Server

1. In Microsoft *SQL Server Management Studio*, connect to the instance of the database engine.
2. Under **Object Explorer**, right-click on the server name and select **Properties**. The Server Properties page appears.
3. On the Security page, select **Both failed and successful logins** under **Login auditing** and click **OK**.
4. Stop and restart the SQL Server service for the database.
5. To view the log of failed and successful logins, access the Security log in the Event Viewer.

   For information about how to enable *SQL Server* to write to the Security log, see http://msdn.microsoft.com/en-us/library/cc645889.aspx.

IIS on Web Servers

Ensure logging is configured in IIS. ***Blackbaud CRM*** functions on web requests and the requests are an integral part of the audit trail. Since the web requests are a part of the IIS web server logging, you can centralize your logs through this common log file format.

For information about how to configure logging in IIS, see http://www.iis.net/learn/manage/provisioning-and-managing-iis/configure-logging-in-iis or contact your Technical Account Manager at Blackbaud Support at https://www.blackbaud.com/support.

The web requests that get sent to ***Blackbaud CRM*** and logged into the IIS web server log can be tracked back to an action taken within ***Blackbaud CRM***. To find specific requests within the IIS server log, the action type and system record ID of the artifact is needed.

Administrators can search and filter their IIS logs using a text editor tool, or IIS log parsing tool, to find all instances of a specific action ID. Below is an example of a web request logged to the ***Blackbaud CRM*** web server, with the key pieces of action and system record ID highlighted.

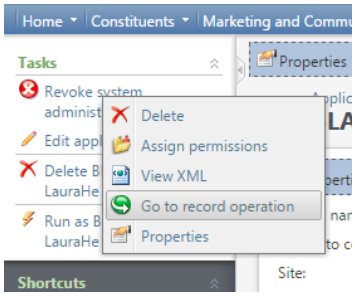
```
2014-11-30 14:41:35 W3SVC1 10.41.1.22 POST /bbappfx/webui/WebShellService.ashx
databaseName=BBInfinity&action=recordOperationPerform&recordOperationId=0ba30310-a816-4037-a039-
b074b27681f6&recordId=f994e7f8-f940-46bf-b80f-005ed1ea0422&_ts=1440686495656 80 DOMAIN\UserName 10.41.1.22
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/44.0.2403.157+Safari/537.36 200 0
0 6
```

To identify web requests related to relevant changes to user authorization, the following actions and IDs can be used to search the web request logs.

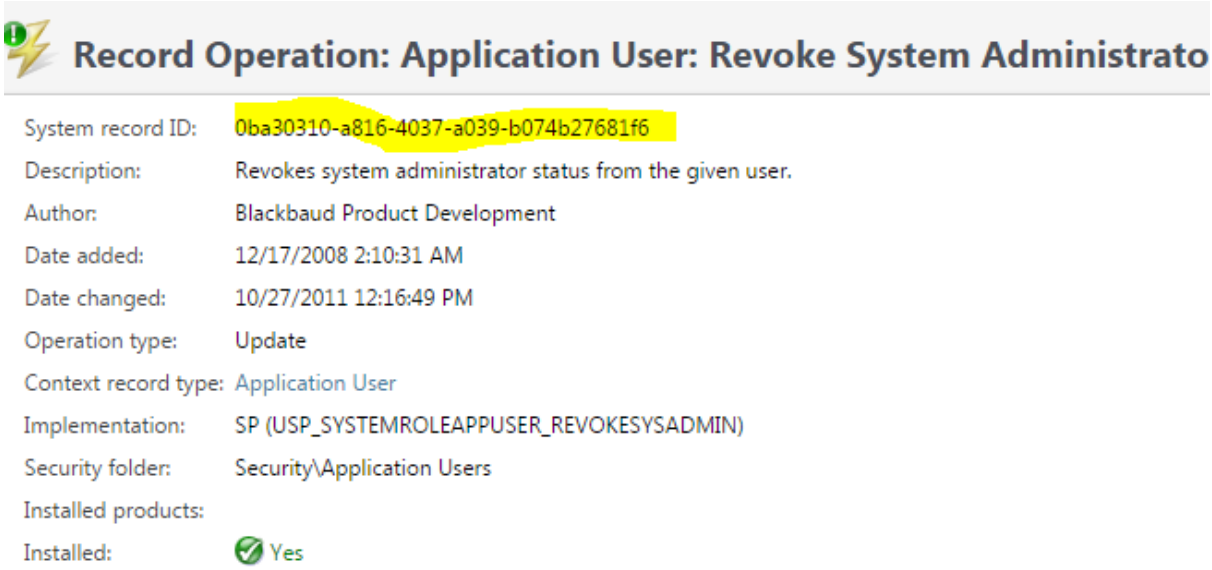
Action Type	ID	Name
DataForm	fc5e2987-3936-4679-8984-c85fc3e7570f	App User Send Reset Password Email
Record Operation	50e1455b-90c0-475f-8b0d-86fd683de61f	Application User : Delete
DataForm	6dab0be8-5b26-4336-8c1c-441bdbef0354	Application User Add Form
DataForm	e9eb9af1-c947-4e86-bb0a-9bb1245726fc	Application User Edit Form
DataForm	F2B751BF-8ED3-48E4-9EC2-4D7FB5E46B01	Application User System Role Add Form
DataForm	75D3C427-3DD7-4618-8CB4-9FCA0F55E492	Application User System Role Edit Form
DataForm	c946fe31-2f9b-473d-b4b7-d351eb2e200d	Application User System Roles Edit Form
Record Operation	da395bb1-82a7-400b-8573-8733af74f76f	Application User: Make System Administrator
Record Operation	0ba30310-a816-4037-a039-b074b27681f6	Application User: Revoke System Administrator
DataForm	91B43924-717B-4863-BC32-0B38D0539393	System Role Add Custom Users By Name Edit Form
DataForm	52E9EF22-CEDA-4F6C-8A8E-9FCE9B21A249	System Role Add Custom Users Edit Form
DataForm	47B7DA87-ACAB-48D5-B428-4EFEAE700B8F	System Role Add Form
DataForm	5EC62F04-733F-4606-B4E7-C9EE7D0DCC3F	System Role Add Groups Edit Form
DataForm	43019C20-8134-4EA1-990E-EB9EEA1F20BF	System Role Add Users By Name Edit Form
DataForm	FB8C569F-D353-4A06-A52E-57F84F68EA15	System Role Add Users Edit Form
DataForm	1163130A-7A4E-4C4C-B0A3-20B6A593A01E	System Role Assign Groups Edit Form
DataForm	14E7E0E3-3A95-4C3F-83FB-610C53BE89AF	System Role Assign Tasks Edit Form
DataForm	E4F589FE-344A-4D74-9432-BA19870AE620	System Role Assign Users Edit Form
DataForm	2E0A73FA-CBE0-4611-871A-EB56CCAB0D10	System Role Code Table Permissions Edit Form
DataForm	b9c5ae3e-1e40-4e33-9682-18fb0bb40ff2	System Role Copy Add Form
DataForm	c55dd36b-a34f-4dd5-982e-c267f0fb8d93	System Role Edit Form
DataForm	DBF7A15D-900A-418D-8C61-9D1F43F9B164	System Role Existing User Add Form
DataForm	7835089F-AF32-405B-B75C-C5A13C8D4694	System Role Feature Permissions Edit Form
DataForm	2D01BF70-222A-44E6-96CD-6D8401C60FC2	System Role Group Add Form
Record Operation	3ABB9E3A-BFD7-4A33-843E-2EDFC760BD08	System Role Group: Delete
DataForm	9D604AAC-129A-4357-ADED-47D3E3E1FA17	System Role User Add Form
DataForm	C41517D7-D81C-4075-869F-912DA19AAD34	System Role User Edit Form
DataForm	47b7da87-acab-48d5-b428-4efeae700b8f	System Role: Add
Record Operation	5699cbe7-d29b-4356-8514-cbb7ca2eb579	System Role: Delete

To identify web requests associated with additional features within ***Blackbaud CRM***, an administrator can use the "Design Mode" feature within ***Blackbaud CRM*** to easily the find the artifact system record ID and action type. The administrator will need to click the "Design Mode" button in the upper right corner of the ***Blackbaud CRM*** application.

Once in design mode, the administrator will be able to right-click buttons (tasks, actions, etc.) within ***Blackbaud CRM*** and receive a context menu. On that context menu, there will be a "Go to <action type>" option.



Once clicked, the administrator will be met with a page that contains the needed information.



The administrator can search web request logs to find the specified action type and system record ID.

Windows Application Event Logs

Blackbaud CRM is an ASP.NET web application, therefore exception and error information is captured in the Windows Application Event logs on the web server under the ASP.NET source. ***Blackbaud CRM*** does not interfere with other applications or server components logging to the Windows Server logs.

Because ***Blackbaud CRM*** can write event logs to the Windows event logs, you can centralize your logs through this common log file format.

For information on viewing and managing Windows Application Event logs, please refer to Microsoft Windows Server documentation, such as https://technet.microsoft.com/en-us/library/cc749021.aspx.

Audit Tables in Blackbaud CRM

From *Administration*, you can enable ***Blackbaud CRM*** to automatically track the changes users make to tables in your database. To comply with PCI DSS, you must track changes made to all tables related to credit cards and security. To manage the auditing of changes to your database from *Administration*, click **Audit tables**.

The audit tables track changes and deletions made to your data at the database level. From the Audit Tables page, you can quickly produce reports that list exactly which fields were changed, along with who made the change, and when it was made. These reports can be used to track changes made to user accounts and application system privileges.

Because audit trails are supported at the database level, all changes made are subject to the audit process, even those made outside the program. So not only are changes made through the program interface included but changes made via direct database access by database administrators are also included. This ensures that the audit trail content is always completely accurate and up to date.

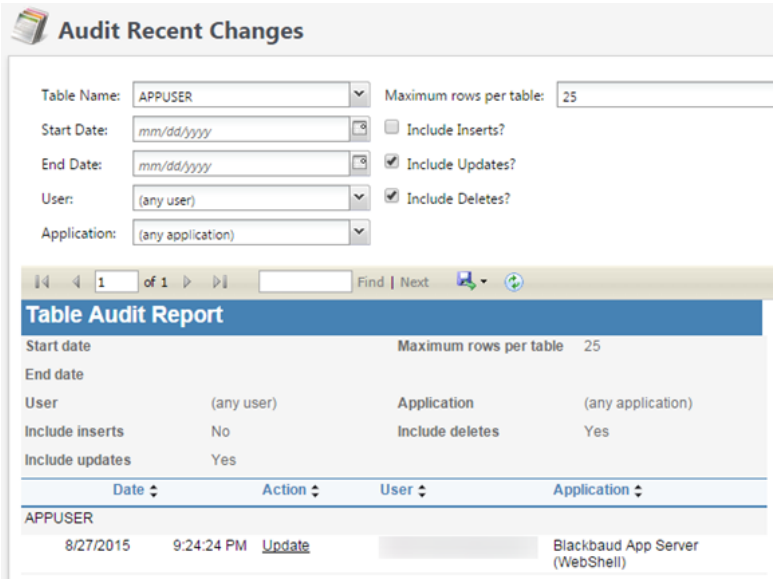
To audit changes related to user accounts and application system privileges, create audit reports for tables that begin with APPUSER and SYSTEMROLE. Any changes reported represent changes to access or authorization.

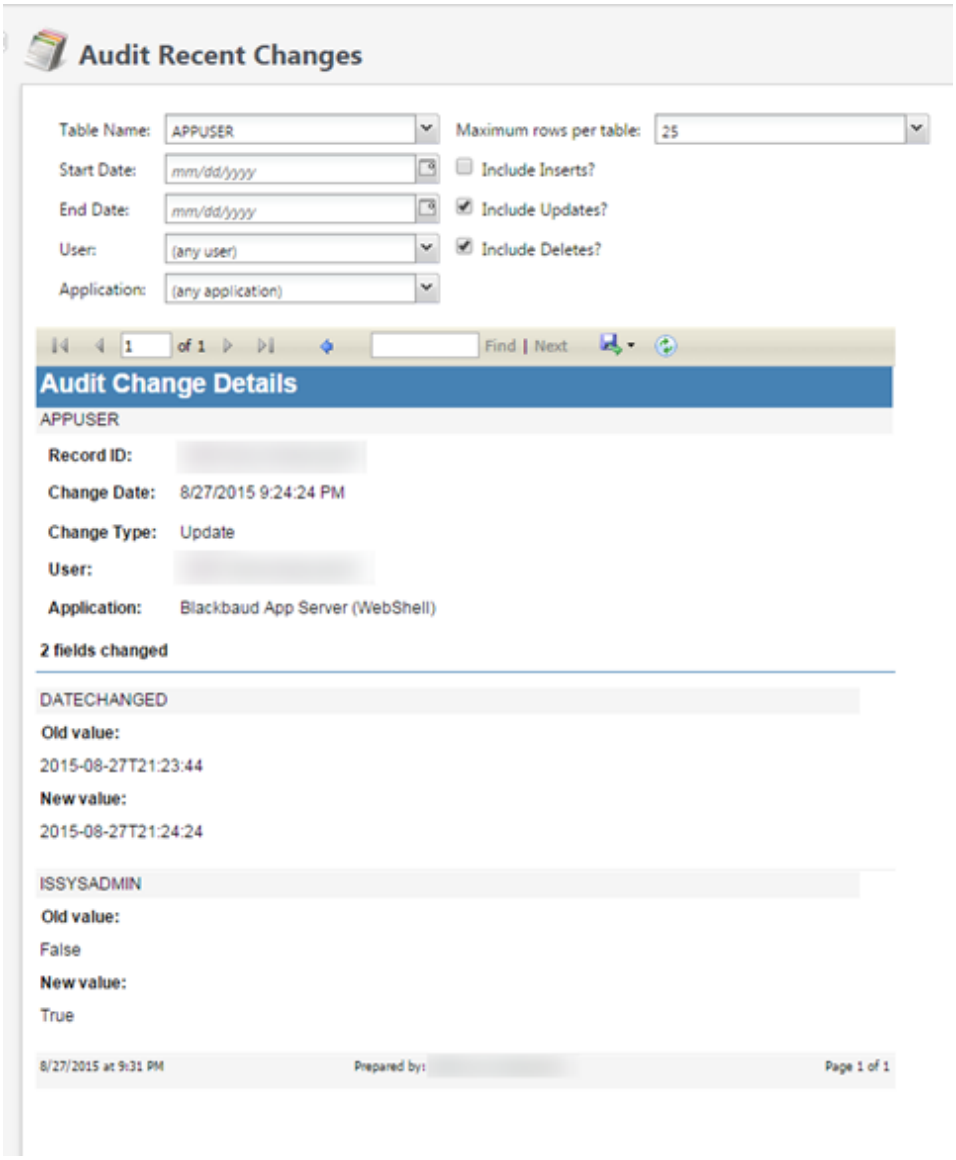
For information about audit tables, see the Audit Tables chapter of the *Security Guide* at https://www.blackbaud.com/files/support/guides/enterprise/400/security.pdf.

Warning: Do not disable or subvert the audit table functionality in ***Blackbaud CRM***. An adjustment from the default settings and requirements will result in noncompliance with PCI DSS.

Using audit table reports

1. From *Administration*, click **Audit tables**. The Audit Tables screen appears.
2. Select the table for which you want to view an audit report and click Audit report. The Table Audit Report appears. Below is a sample of an audit table report of the APPUSER table.





Firewall Management

If you use software to process payments, we recommend you verify that the workstation's link to the Internet is secure. If you transfer transactions online, ensure your Internet hardware, such as the modem or DSL router, provides a built-in firewall. You must restrict connections between publicly accessible servers and any system component that stores cardholder data, including connections from wireless networks. To comply with PCI DSS, the firewall configuration must:

- Restrict inbound Internet traffic to Internet Protocol (IP) addresses within the DMZ.
- Not allow internal addresses to pass from the Internet into the DMZ.
- Implement inspection or dynamic packet filtering to allow only established connections into the network.
- Place the payment processing program and the database that contains the cardholder data in an internal

network zone segregated from the DMZ.

- Restrict inbound and outbound traffic to only that which is necessary for the cardholder data environment, and deny all other traffic that is not specifically allowed.
- Secure and synchronize router configuration files such as running and start-up configuration files.

Your organization must also 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. To comply with PCI DSS, your organization must configure all mobile and employee-owned computers with direct connectivity to the Internet, such as laptop computers, used to access the network with an installation of personal firewall software.

Wireless Devices

If you use wireless devices to store or transmit payment transaction information, you must configure these devices to ensure network security in compliance with PCI DSS.

- Install perimeter firewalls between any wireless networks and systems that store cardholder data. These firewalls must deny or control any traffic necessary for business purposes from the wireless environment to the cardholder data environment.
- Implement strong encryption, such as Advanced Encryption Standard (AES), on all wireless networks.
- At installation, change wireless encryption keys, passwords, and SNMP community strings from the default. After installation, change wireless encryption keys, passwords, and SNMP community strings when anyone with knowledge of these items leaves the organization or changes positions with the organization.
- Do not use the vendor-supplied defaults for the wireless environment. Change the default passwords or pass phrases on access points and single network management protocol (SNMP) community strings on wireless devices.
- Change the default service set identifier (SSID) and disable SSID broadcasts when applicable.
- Update the firmware on wireless devices to support strong encryption—such as WiFi-protected access (WPA or WPA2) technology, Internet Protocol security virtual private network (IPSec VPN), or Transport Layer Security (TLS)—for authentication and transmission over wireless networks.
- Use industry best practices (for example, IEEE 802.11i) to implement strong encryption for the transmission of cardholder data and sensitive authentication data over the wireless network in the cardholder data environment.

Warning: As of June 30, 2010, it is prohibited to use Wired Equivalent Privacy (WEP) for payment applications. We strongly recommend you use WPA2 technology to secure wireless implementations.

To comply with PCI DSS, your organization must configure all mobile and employee-owned computers with direct connectivity to the Internet, such as laptop computers, used to access the network with an installation of personal firewall software. The firewalls must be active and configured to a specific standard that users cannot alter.

Remote Access

Blackbaud CRM payment functionality is accessible only to users with access to your organization's network. The application is configured to only be accessible with network access by default. Blackbaud does not have nor

require access to customer networks in order to install ***Blackbaud CRM***. ***Blackbaud CRM*** updates are not delivered via remote access from Blackbaud.

If your organization allows for remote network access by employees, administration, and vendors, you must implement two-factor authentication (T-FA) for logins in order to meet PCI-DSS requirements. T-FA requires unique login credentials (username and password) and an additional authentication item such as a token or individual certificate. Use of technology such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens or VPN (based on TLS or IPSec) with individual certificates are acceptable methods of T-FA.

To comply with PCI DSS, your organization must configure the remote access software to ensure network security.

- Do not use the vendor-supplied defaults, such as passwords, for the remote access software.
- Establish unique login credentials and complex passwords for remote access users in accordance with PCI DSS requirements 8.1.5 and 8.3. For information, see User Account Management on page 13.
- Allow connections from only specific known IP and MAC addresses.
- Enable encrypted data transmission in accordance with PCI DSS 4.1.
- Lock out the remote access user account after no more than six failed login attempts.
- Require remote access users to establish a VPN connection through a firewall before they connect to the network.
- Enable the logging function.
- Establish complex passwords for customers in accordance with PCI DSS requirements 8.2.3.
- Restrict access to customer passwords to authorized third-party personnel.
- To verify the identities of remote access users, require T-FA such as both a user login and a password.

If your organization enables remote access for use by vendors, it should be only when needed and immediately deactivated after use.

Non-console Administrative Access

To comply with PCI DSS, your organization must encrypt all non-console administrative access. For web-based management and other non-console administrative access, use technologies such as Secure Shell (SSH), VPN, or TLS.

If you use Remote Desktop (RDP) for non-console administrative access, it is advised that you follow best practices for RDP security such as digitally signing RDP files with a custom certificate, tightening connection security through a TLS security layer and raising the encryption level to high, and using network level authentication.

For information on configuring RDP security, see Microsoft documentation at https://technet.microsoft.com/en-us/library/cc753488.aspx.

Internet-Accessible Systems

Do not store cardholder data on Internet-accessible systems. For example, do not house the database server within the same server as the web server.

System Maintenance

Once you secure your system, you must keep your equipment current. Malicious users can use security vulnerabilities to access your system. Both hardware and software manufacturers occasionally issue updates to products, such as to remedy these vulnerabilities and help prevent such attacks. We recommend you ensure you have the most recently released patches installed. For example, you can frequently review the manufacturer's websites, newsletters, and online forums to check for the current patches.

Occasionally, a manufacturer may stop support of a product. In this case, we recommend you determine whether your organization should continue to use an unsupported product. Also, a manufacturer may inform you of a flaw or defect in a product that may make your organization vulnerable to attack. We recommend you pay attention to these alerts and update your system accordingly.

To further reduce vulnerability, we recommend you also deploy anti-virus software on your systems and ensure they are current, actively running, and can generate assessment logs.

Network Maintenance

Once you secure your system, you must monitor and track access to the network and your credit card information, such as with logging mechanisms. The lack of activity logs can make the determination of the cause of an attack very difficult. Logs help you track and analyze network activity when something goes wrong. To further reduce vulnerability, we recommend you also frequently test your network to verify its security continues to be maintained, regardless of age or changes in software.

To comply with PCI DSS, you must implement automated audit trails for all system components to track these events:

- All individual users who access cardholder data.
- All actions performed by users with root or administrative privileges.
- All access of the audit trails.
- All invalid logical access attempts.
- All use of identification and authentication mechanisms.
- The initialization of the audit logs.
- The creation and deletion of system-level objects.

For each event, your organization must also record these audit trail entries for all system components:

- The user who initiates the event.
- The type of event.
- The date and time of the event.
- Whether the event succeeds or fails.
- The origination of the event.
- The data, system component, or resource the event affects.

Revision Information

This guide is reviewed and updated as necessary on a yearly basis and based on changes to ***Blackbaud CRM 4.0*** or the PCI DSS and PA DSS specifications. Blackbaud distributes this guide through the How-to user guides page on our website at https://www.blackbaud.com/howto/.

Author	Revision date	Summary of changes
Steve Stegelin (Technical Writer III)	March 2009	
Steve Stegelin (Technical Writer III)	January 2010	Add Transport Layer Security (TLS) Configuration on page 7.
Steve Stegelin (Senior Technical Writer)	June 2010	Add Transport Layer Security (TLS) Configuration on page 7
Steve Stegelin (Senior Technical Writer)	January 2011	Update document template.
Steve Stegelin (Senior Technical Writer)	July 2011	Add Protected Configuration and IIS Registration on page 7 for PA DSS requirement 3.3.
Steve Stegelin (Senior Technical Writer)	September 2011	Add Download File Verification on page 8.
Steve Stegelin (Senior Technical Writer)	October 2011	Update link URLs.
Steve Stegelin (Information Archi- tect)	May 2012	Rebrand to ***Blackbaud CRM***.
Steve Stegelin (Information Archi-	June 2012	Update document template; minor edit to remove recent-speaking terms such as "now" and "new".

Author	Revision date	Summary of changes
tect)		
Steve Stegelin (Information Architect)	October 2012	Reverse order of chapters; add Services and Protocols on page 8.
Tina Fei (Technical Writer)	April 2015	Update SSL information to TLS; add hyperlinks to included Microsoft KB tips; update diagram with TLS and change product name to "Blackbaud CRM"; remove information about the "Credit card conversion process" global change; add Blackbaud product version scheme information; add clarification that we do not store or log any authentication data or PANs; add clarification that only partial card numbers are stored.
Tina Fei (Technical Writer)	August 2015	Update information about complete removal of cardholder data from the program; add section on "Audit Trails and Centralized Logging" with a new subsection for how to enable IIS logging on web servers with additional information about how to interpret information in the logs, as well as Windows application event logs; update "Remote Access" section with more specific requirements; update "Versioning Scheme" section to clarify the versioning, particularly with regard to security-impacting changes; remove "Encryption Key Management" section; update "Services and Protocols" section to more explicitly state required port, in addition to information about services; update section "Non-console Administrative Access" with encryption, security, and best-practice guidance; update "Transport Layer Security (TLS) Configuration" section with more specific information; update "User Account Security and Configuration" section to include information about audit tables, including a link the Security Guide PDF with more information, in addition to some clarification about authentication requirements; include versioning information specific calling out CRM 4.0 Service Pack 2; add section "Audit Tables in Blackbaud CRM" which includes information about audit tables and audit table reports to monitor application user and system role security changes.

Author	Revision date	Summary of changes
Tina Fei (Technical Writer)	September 2015	Update content to reflect changes in TLS version 1.0 to 1.2, in addition to the updated Blackbaud CRM version number to 4.0 Service Pack 5.

Index

R

S

T

U

V

W