Blackbaud Internet Solutions

PA DSS IMPLEMENTATION GUIDE

Copyright Disclaimer

Blackbaud CRM PADSS Implementation US

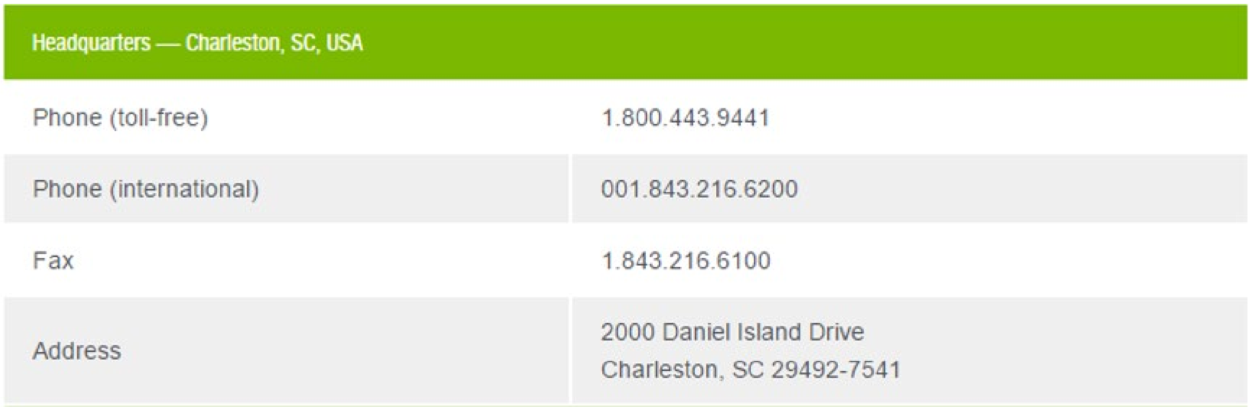
The information in this manual has been carefully checked and is believed to be accurate. Blackbaud, Inc., assumes no responsibility for any inaccuracies, errors, or omissions in this manual. In no event will Blackbaud, Inc., be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this manual, even if advised of the possibility of damages.

In the interest of continuing product development, Blackbaud, Inc., reserves the right to make improvements in this manual and the products it describes at any time, without notice or obligation.

All Blackbaud Product names appearing herein are trademark or registered trademarks of Blackbaud, Inc.

All other products and company names mentioned herein are trademark of their respective holder.

Contact



Headquarters — Charleston, SC, USA	
Phone (toll-free)	1.800.443.9441
Phone (international)	001.843.216.6200
Fax	1.843.216.6100
Address	2000 Daniel Island Drive Charleston, SC 29492-7541

Document Summary

Organization	Blackbaud
Document Name	PA - DSS Implementation guide
Version & Date	Version 2 Date: 10/10/2019
Prepared by	Esha Mishra
Reviewed by	Varun Vij
Approved by	Varun Vij

Abbreviation & Description

Abbreviation	Description
SAD	Sensitive Authentication Data
PAN	Personal Account Number
PCI-DSS	Payment Card Industry Data Security Standard
PA-DSS	Payment Application Data Security Standard
CDE	Cardholder Data Environment

TABLE OF CONTENTS

Application: - Blackbaud Internet Solutions 7.2.0.x

Brief Description of the Blackbaud Internet Solutions (7.2.0.x)

Blackbaud Internet Solutions enables organizations to build an online community where they can educate the world about their mission, add new supporters, and raise more money by personalized online experience for their constituents. It is an online communication and internet marketing platform that helps in building an expanded and loyal network of support.

You can create web pages with multiple layers of layout, template, and page design. You can generate and send an email to individuals and groups; define user roles and set security for each section; and track statistics about website usage. Website users can also make donations or register for events with online forms you create.
In addition, the program can integrate your website and your other Blackbaud products. Website users enter data into areas of your website such as profiles and donation forms, and you can download that data to another Blackbaud program.

With Blackbaud Internet Solutions You Can:
Educate the community about your mission and add new supporters
Blackbaud Internet Solutions allows you to get the word out about your **campaigns, programs, upcoming events, and volunteer opportunities**. Provide an audience-friendly website that engages visitors through a compelling design and encourages participation through intuitive navigation. Drive people to your site with emails, invite supporters to read more about the topics that interest them, broadcast your electronic to targeted audiences, and simplify your fundraising efforts with online appeals and reminders. Offer **personal pages, message boards, and blogs** to help enthusiastic supporters and busy staff members communicate within their own groups and with each other

Blackbaud CRM Integration

Complete Constituent Relationship Management for Large- to Enterprise-Level Nonprofits Blackbaud CRM helps organizations improve constituent engagement, build stronger relationships, and meet fundraising challenges by providing a complete supporter view and an organization-wide toolset for managing your constituent base.

Focus on Constituent Relationship Management Blackbaud CRM places constituents squarely in the center of your organization by bringing together information from different departments, offices, and systems and combining it into a single source. Blackbaud CRM is the one place where an organization can showcase the holistic relationship it has with a constituent and where constituent preferences are respected across channels.

System/Server requirements for Blackbaud Internet Solution application

The following pages list the minimum system requirements Blackbaud suggests for each of the **Blackbaud Internet Solutions 7.2.0.x** components. For a more in-depth technical configuration of Blackbaud Internet Solutions, read the Blackbaud Internet Solutions Configuration Overview under Support, How-to Documentation on our website.

Note: System requirements are subject to change. Blackbaud recommends the purchase of the latest software and equipment when possible and that organizations budget for continual upgrades to their system. Before you make any purchase or installation decisions, ensure you have the latest system requirements and check for third-party compatibility information in Knowledgebase. If you use multiple Blackbaud products, refer to the system requirements for each product; the total requirements may be different from what is listed below.

Minimum Requirements:

Blackbaud Internet Solutions database server

CPU	Pentium D-class 3 GHz minimum or AMD equivalent recommended.
Hard Disk	A high performance disk subsystem, such as SCSI-2 and RAID technology, is recommended.
Disk Space Required	1.2 GB minimum for Blackbaud Internet Solutions program, system, and database management console files; plus 50 MB for the workstation deployment files, which can be installed in a different location.
RAM	4 GB minimum
SQL Server	SQL Server 2012 Enterprise SP4 with compatibility level 110. SQL Server 2014 Enterprise SP1 with compatibility level 110 or SP2 with compatibility level 110. Compatibility level 120 is not supported. SQL Server 2016 Enterprise SP1 (CL 130) with version 4.0, Hotfix 61 and above.

Blackbaud Internet Solutions web server & core components

CPU	Pentium D-class 3 GHz minimum or AMD equivalent recommended.
Disk Space Required	1.2 GB minimum for Blackbaud Internet Solutions program, system, and database management console files; plus 50 MB for the workstation deployment files, which can be installed in a different location.
RAM	4 GB or more recommended.

Operating System	Windows Server 2008 R2 SP1 or higher with IIS 7.5 Windows Server 2012 R2 SP1 or higher with IIS 8.5 Windows Server 2016 Windows Server 2019 Microsoft .NET Framework 4.5.2. 64-bit supported on x64 hardware. Note: Blackbaud Internet Solutions does not support domain controllers or peer-to-peer networks.

Database Backup

Blackbaud strongly recommends the purchase and scheduled use of a tape or archival backup solution. Power blackouts and brownouts, hardware and network failures, and other unexpected circumstances can lead to an unrecoverable data loss. Blackbaud is not a vendor of backup software or hardware and cannot determine the right backup system for your organization. Consult with reputable dealers and qualified information systems professionals to implement a reliable backup system.

You should make backups daily and test them periodically to ensure their reliability. The SQL Server Enterprise Manager includes a backup utility to conduct or schedule backups while the database engine is running. These backups should then be archived to your chosen tape or archival backup solution. You should also test these backups to ensure their reliability.

Requirements Disclaimer

System requirements are based on information available on the last updated date. They are published only as a guide and relate solely to Blackbaud software.

Performance and response time are affected by many factors related to hardware (such as RAM, processor speed, and hard disk subsystem performance), network configuration (such as NIC performance, cable type, topology, operating system, parameters, and traffic), and the database (such as size, number of concurrent users, and the type of activities each user performs). In addition, network and workstation operating systems, third-party software products, and our own products are continuously updated with new features and options, which often place greater demands on hardware.
Blackbaud recommends the purchase of top-of-the-line equipment when possible and that organizations budget for continual upgrades to their system.

Blackbaud staff may provide limited informal guidance based on information made available. However, neither these system requirements nor our staff's guidance constitute a guarantee of compatibility, outcome, or performance. We encourage organizations to consult their own systems staff or outside technical experts to ensure appropriate results. Comprehensive technical consulting services are available through Blackbaud. Under a separate consulting arrangement, our consultants evaluate the installation of all Blackbaud applications and recommend optimal hardware and system configuration options. For more information, email solutions@blackbaud.com

Browser Requirements

Blackbaud Internet Solutions application is a Web based application; hence it requires the Web browser to run the application.

Application can run on the following browsers:

No.	Browser Name	Browser Version	Screen Resolution	Add-ons/ Plugins if any required
1	Internet Explorer	11.0.0	1280x1024 pixels	N/A
2	Google Chrome	76.0.3809.132	1280x1024 pixels	N/A
3	Firefox	69.0	1280x1024 pixels	N/A

Other Requirements & Recommendations

Application dependencies

i. Blackbaud CRM (4.0.181)
The Blackbaud CRM application is required to completely process the transactions that are made in the BBIS web portal. So, when a user for example: Registers, updates his profile, donates, registers for an event or joins a membership program etc. The transaction which he makes is dependent upon data created in BBCRM which is reflected on the BBIS portal. This data/transaction then flows from BBIS to BBCRM from where we completely process the transaction registering the required entries in the database through batch processing in BBCRM.

ii. BBPS **(1.0.2.0)**
The BBPS gateways are used for processing payments in BBIS.

iii. ABCpdf **(11.2.0.4)**
This is used to generate PDF.

iv. CuteEdit **(6.3.0.0)**
It enables ASP.NET Web developers to replace the Text area/Textbox in your existing content management system with a powerful, but easy to use WYSIWYG HTML editing component

v. Infragistics **(8.3.20083.1009)**
Infragistics has the UX expertise, prototyping tools, and UI controls to help you make strategic decisions about your technology landscape. You'll create memorable user experiences by default when you work with our team of consultants to integrate UX into your development process.

vi. TZ4Net (Time Zone) **(2.1.0.0)**
This is used for Time Zone Conversion.

vii. HTMLParser **(1.0.3903.24154)**
This is used to parse the HTML.

viii. Yahoo.Yui.Compressor**(1.4.2.0)**
The YUI Compressor is used to safely compress CSS files

ix. Spellserver.NET **(2.0.1513.25286)**
A lightning-fast spell checking .NET object, packaged with two complete ASP.NET applications (one in C#, one in VB.NET), SpellServer.NET has built-in customizable dictionaries for US English, UK English, French and Spanish

x. skmMenu **(3.2.2545.29944)**
It is ASP.NET DHTML Dropdown Menu Control

xi. JQuery **(3.4.1)**
JQuery offers a cleaner way to write code for querying DOM objects. The other useful feature is its event emission. It popularized the event-based paradigm in JavaScript development where you subscribe callbacks to events/topics and write reactive code in them.

xii. LumenWorks.Framework**(3.7.0.0)**
A reader that provides fast, non-cached, forward-only access to CSV data.

xiii. Microsoft.LiveFX**(0.9.3904.1)**
A set of RESTful APIs for interacting with Live Mesh and Windows Live data. A set of libraries for the .NET Framework, Silverlight and JavaScript for accessing the REST APIs.

xiv. NetSpell.SpellChecker**(2.1.7.20561)**
Spell checking engine

xv. Newtonsoft.Json**(7.0.1.18622)**

This is a popular high-performance JSON framework for .NET. The JSON serializer is a good choice when the JSON you are reading or writing maps closely to a .NET class.

xvi. AjaxControlToolkit **(3.5.40412.2)**

The AJAX Control Toolkit is simply a library of controls that works on top of ASP.NET AJAX, which developers can use to build client-side Web projects based on HTML5 and CSS.

xvii. AntiXssLibrary **(3.1.3524.16873)**

The Microsoft Anti Cross Site Scripting Library (AntiXSS) is an encoding library, designed and developed by CISG team at Microsoft in conjunction with the ACE Team. It is designed to help developers protect their Web-based applications from XSS attacks.

xviii. ComponentArt.Web.UI **(2006.2.1507.3)**

ComponentArt Web.UI for ASP.NET AJAX and MVC includes over 20 user interface controls for the development of sophisticated web applications. ComponentArt Web.UI for ASP.NET AJAX client-side richness is built on top of ComponentArt's innovative web user interface technology. Offering second generation web service binding through ComponentArt SOA.UI, ComponentArt Web.UI for ASP.NET AJAX delivers full server-side code reuse with Silverlight applications. ComponentArt Web.UI for ASP.NET AJAX includes Calendar, ComboBox, Editor, Grid, Menu, NavBar, SpellCheck, Splitter, TabStrip, ToolBar, Tree View and advanced data visualization components like ComponentArt Chart and ComponenArt Gauges.

xix. Google.GData**(1.6.0.0)**

GData (Google Data Protocol) provides a simple protocol for reading and writing data on the Internet, designed by Google. GData combines common XML-based syndication formats (Atom and RSS) with a feed-publishing system based on the Atom Publishing Protocol, plus some extensions for handling queries. It relies on XML or JSON as a data format.

xx. ICSharpCode.SharpZipLib **(0.85.5.452)**

#ziplib (SharpZipLib, formerly NZipLib) is a Zip, GZip, Tar and BZip2 library written entirely in C# for the .NET platform. It is implemented as an assembly (installable in the GAC), and thus can easily be incorporated into other projects (in any .NET language). The creator of #ziplib put it this way: "I've ported the zip library over to C# because I needed gzip/zip compression and I didn't want to use libzip.dll or something like this. I want all in pure C#."

xxi. ImageManipulation **(1.0.2531.23252)**

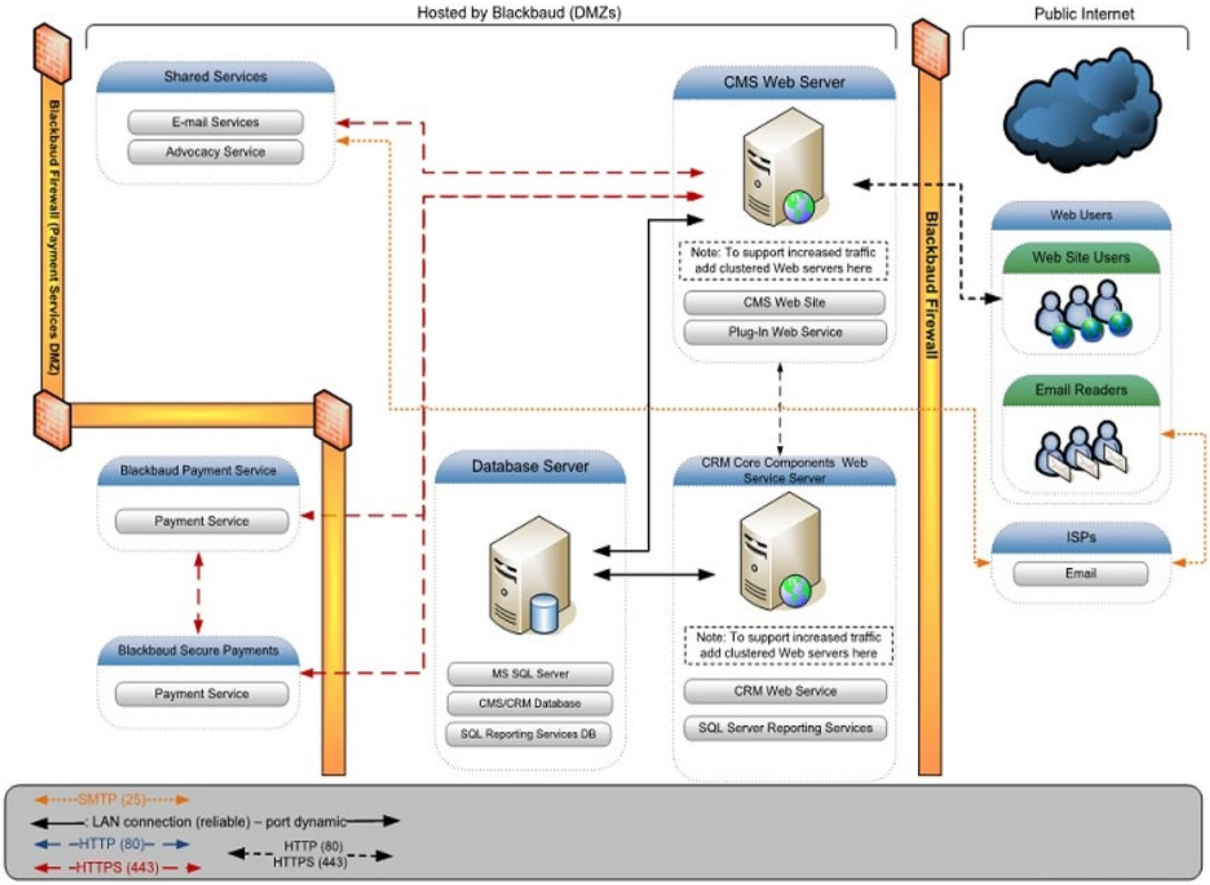
It is specifically designed to provide image manipulation for ASP.NET, while avoiding all of the GDI bugs. It provides a highly-scalable and efficient manipulation API that often only requires 1 line of code to use. It doesn't leak memory or handles, and has 0 known bugs as of this writing.

xxii. Facebook.dll **(2.0.3232.24364)**
Facebook.dll is a type of DLL file associated with Facebook C# SDK developed by Facebook C# Sdk for the Windows Operating System.

Blackbaud Implementation and Deployment Architecture

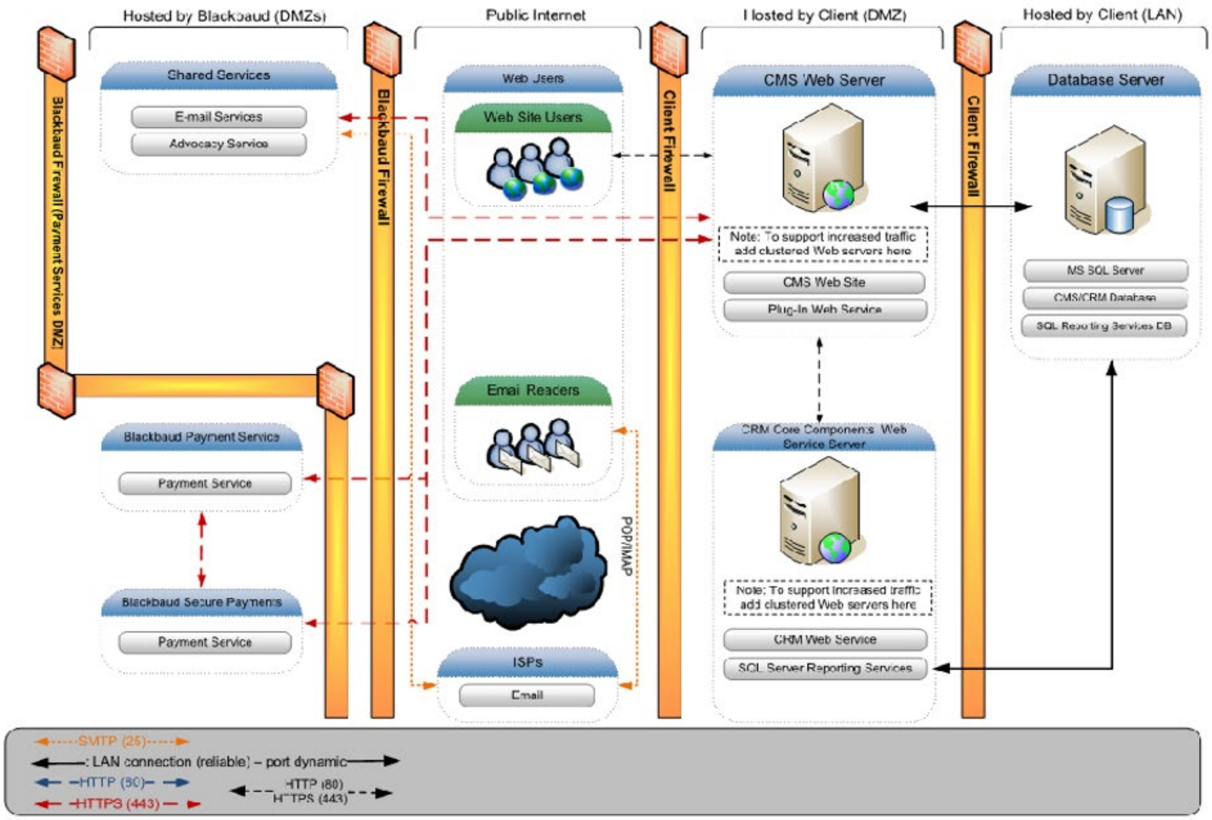
Blackbaud Enterprise CRM with Blackbaud Internet Solutions Server/Network Configuration

Hosted

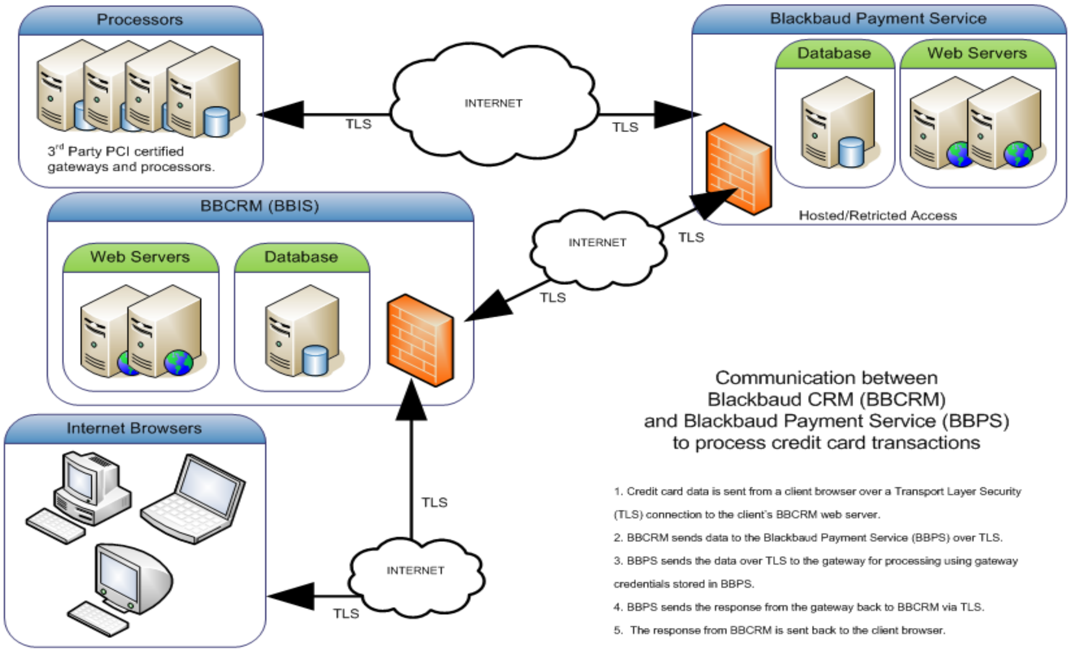

Hosted by Blackbaud (DMZs)
Public Internet
Blackbaud Firewall (Payment Services DMZ)
Shared Services
E-mail Services
Advocacy Service
CMS Web Server
Note: To support increased traffic add clustered Web servers here
CMS Web Site
Plug-In Web Service
Blackbaud Firewall
Web Users
Web Site Users
Email Readers
ISPs
Email
Blackbaud Payment Service
Payment Service
Blackbaud Secure Payments
Payment Service
Database Server
MS SQL Server
CMS/CRM Database
SQL Reporting Services DB
CRM Core Components Web Service Server
Note: To support increased traffic add clustered Web servers here
CRM Web Service
SQL Server Reporting Services
SMTP (25)
: LAN connection (reliable) – port dynamic
HTTP (80)
HTTPS (443)
HTTP (80)
HTTPS (443)

Blackbaud Enterprise CRM with Blackbaud Internet Solutions Server/Network Configuration

Client Hosted – with Blackbaud Enterprise CRM



Application Architecture Model



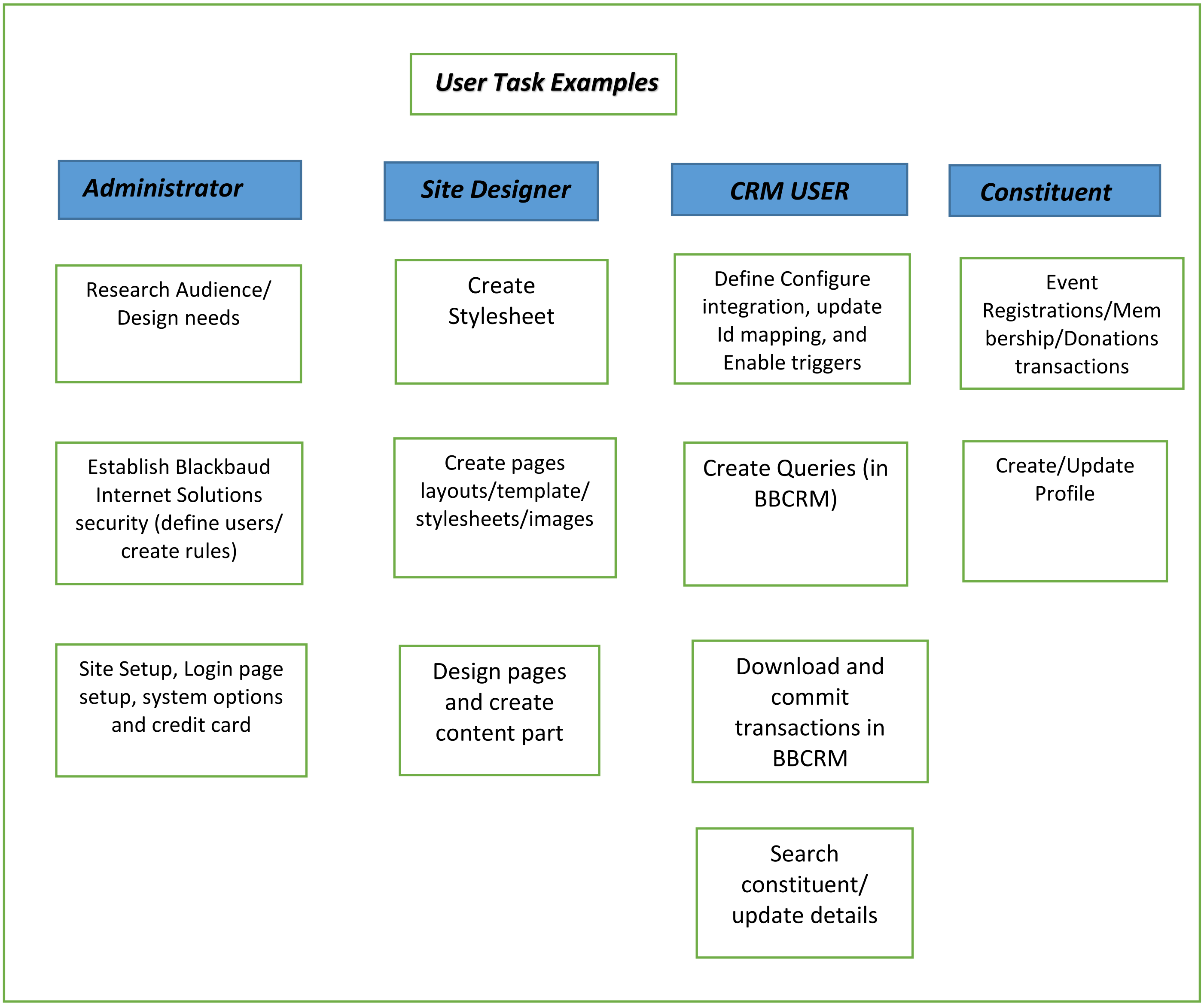
Communication between
Blackbaud CRM (BBCRM)
and Blackbaud Payment Service (BBPS)
to process credit card transactions

1. Credit card data is sent from a client browser over a Transport Layer Security (TLS) connection to the client's BBCRM web server.
2. BBCRM sends data to the Blackbaud Payment Service (BBPS) over TLS.
3. BBPS sends the data over TLS to the gateway for processing using gateway credentials stored in BBPS.
4. BBPS sends the response from the gateway back to BBCRM via TLS.
5. The response from BBCRM is sent back to the client browser.

Application Transaction Data Flow

A wide range of users perform tasks in the program. Many tasks are captured in the user roles of an Administrator, a website designer, a user from BBCM who also uses the program (most Likely someone in the Development office), and a constituent.

The following picture displays the tasks you can perform, depending on your user role

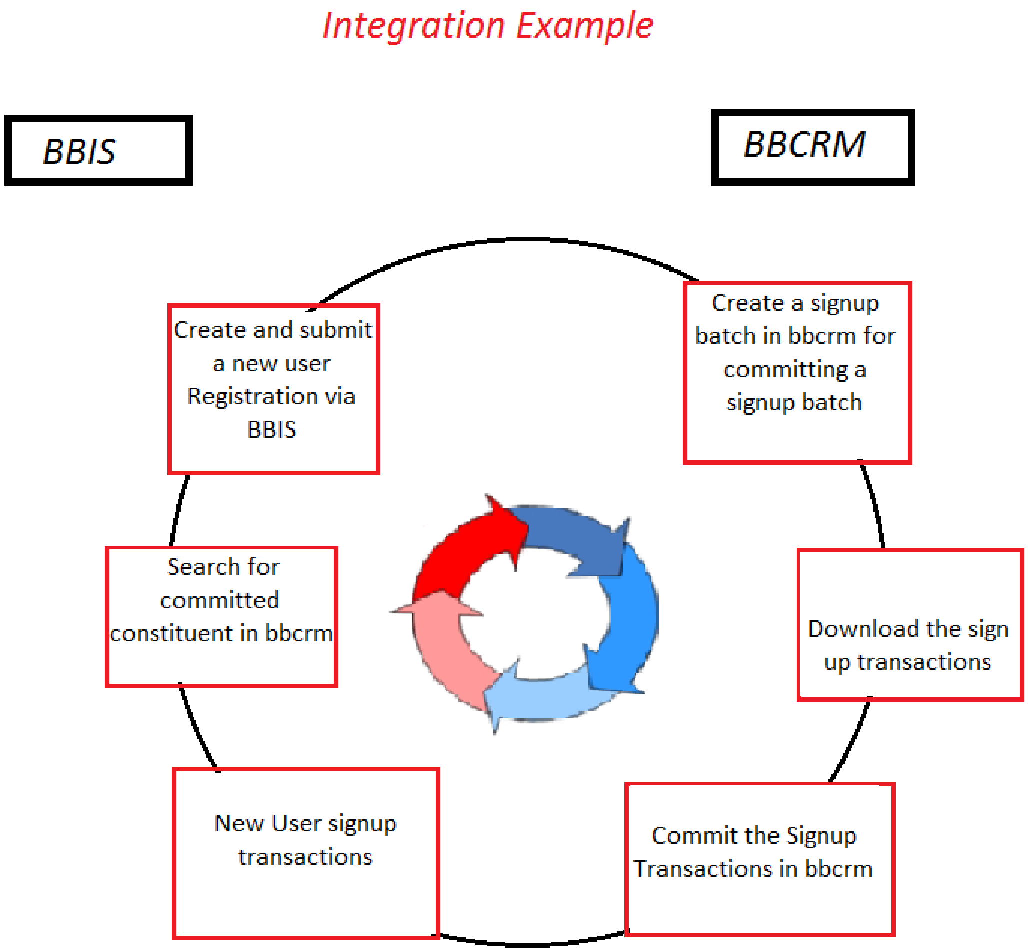


User Task Examples

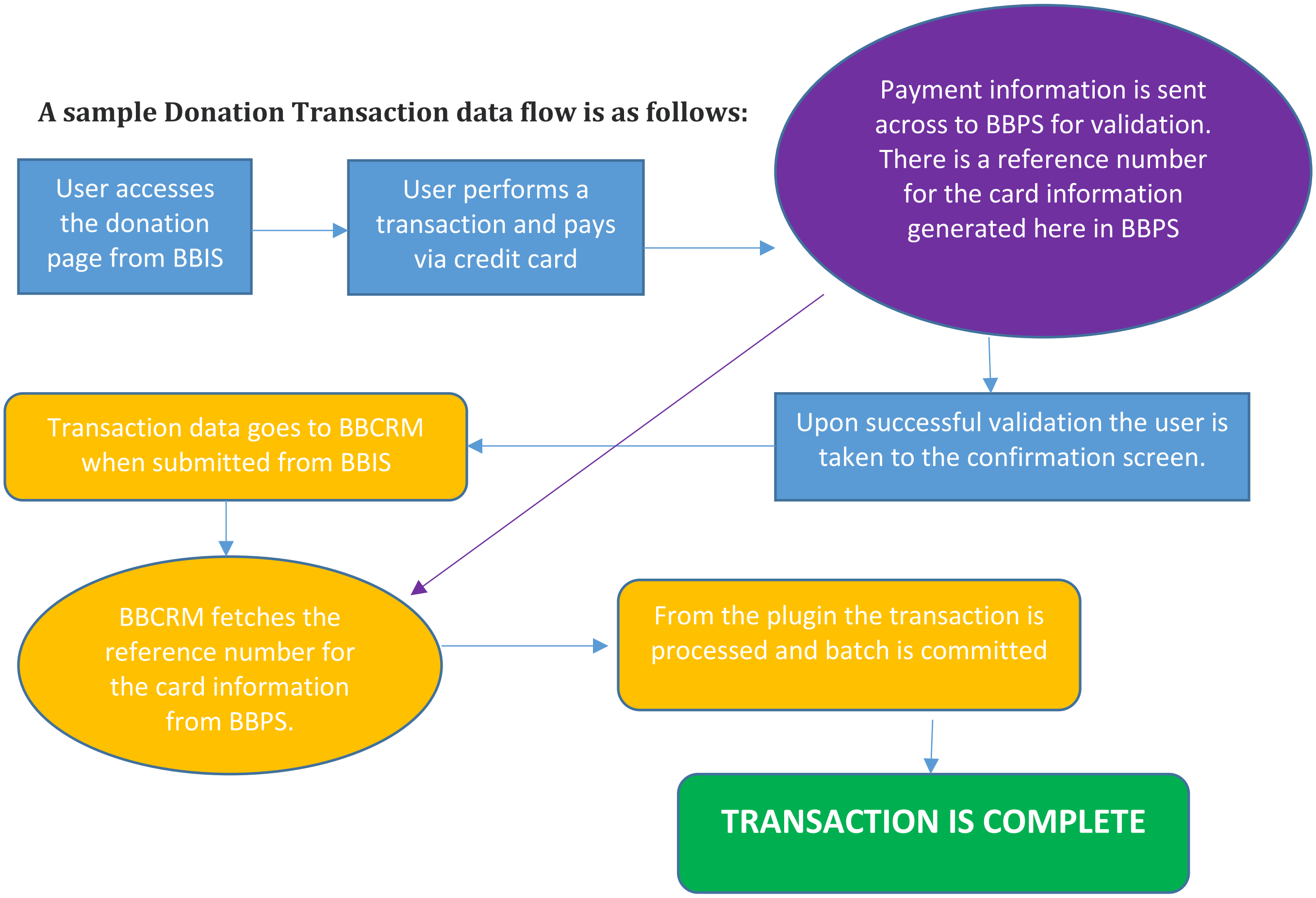
Administrator	***Site Designer***	***CRM USER***	***Constituent***
Research Audience/ Design needs	Create Stylesheet	Define Configure integration, update Id mapping, and Enable triggers	Event Registrations/Membership/Donations transactions
Establish Blackbaud Internet Solutions security (define users/ create rules)	Create pages layouts/template/ stylesheets/images	Create Queries (in BBCRM)	Create/Update Profile
Site Setup, Login page setup, system options and credit card	Design pages and create content part	Download and commit transactions in BBCRM	
		Search constituent/ update details	

Some individuals (most likely in development) at your organization may have responsibilities that are common to both the program and BBCRM. For example, your events data entry person may also be responsible for updating the events page on your website.

If the roles for your job are similar to this, review the following diagram for an example of integration between the program and BBCRM. If you have rights to create and edit parts or pages of your website, this diagram helps you get started in the program and understand how the integration process works.


Integration Example
BBIS
BBCRM
Create and submit a new user Registration via BBIS
Create a signup batch in bbcrm for committing a signup batch
Download the sign up transactions
Commit the Signup Transactions in bbcrm
New User signup transactions
Search for committed constituent in bbcrm

A sample Donation Transaction data flow is as follows:


User accesses the donation page from BBIS
User performs a transaction and pays via credit card
Payment information is sent across to BBPS for validation. There is a reference number for the card information generated here in BBPS
Upon successful validation the user is taken to the confirmation screen.
Transaction data goes to BBCRM when submitted from BBIS
BBCRM fetches the reference number for the card information from BBPS.
From the plugin the transaction is processed and batch is committed
TRANSACTION IS COMPLETE

PA - DSS Overview & Conformance Instructions

The Payment Application Data Security Standard (PA-DSS) is based largely on VISA's Payment Application Best Practices (PABP) program, which was introduced in 2005 to help software vendors create secure payment applications.

The PA-DSS, which is endorsed by the five major payment card brands (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc.), will ensure payment applications don't store sensitive card data and aren't rife with flaws that can lead to cross-site scripting and SQL injection attacks.

Requirement – 1 (Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data)

PA-DSS 1.1.4 (Aligns with PCI DSS Requirement 3.2)

Securely delete any track data (from the magnetic stripe or equivalent data contained on a chip), card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application

Software Vendor Conformance:

Blackbaud Internet Solutions application never stores any SAD values in any current or prior versions of application and also there is no previous PA-DSS certified version of Blackbaud Internet Solutions application exists. Hence this requirement is not applicable.

Guidance to Customers/Integrators:

Not Applicable as previous or current version of application did not store SAD.

PA-DSS 1.1.5 - Aligns with PCI-DSS Requirement 3.2

Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.

Software Vendor Conformance:

Blackbaud, Inc does not need any Sensitive Data for any troubleshooting purpose. Blackbaud Internet Solutions does not store Sensitive Data in its database.

Instruct customer to not send any of the sensitive authentication data to vendor for troubleshooting purposes. This requirement is not applicable since application doesn't collect sensitive data for troubleshooting.

Guidance to Customers:

Customers are advised not to send any of the SAD to Blackbaud, Inc. for troubleshooting purposes of any transactions or disputes.

Requirement 2 – Protect Stored Cardholder Data

PA-DSS 2.1 (Aligns with PCI DSS Requirement 3.1)

Securely delete cardholder data after customer-defined retention period.

Software Vendor Conformance:

BBIS application stores the cardholder's PAN data in the identified few locations mentioned in the Cardholder's data storage matrix table (see below). The card holder data storage matrix clearly depicts the list of locations where the card data is stored with the protection. It helps the customer to identify the location where the payment application stores cardholder data so that customer knows the locations of the data that needs to be deleted securely.

Database Name	Table Name	Column Name	SAD Stored	Protection Mechanism
BBIS	DonationTransactions	XMLObjectData	PAN	Truncation(only last 4 digits)
BBIS	Transactions	Data	PAN	Truncation(only last 4 digits)

Guidance to Customers:

If you use Microsoft Windows OS , 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.

When required, PAN data stored in database can also be securely deleted using the DELETE SQL command which permanently deletes the information without impacting the data integrity of the table.

Steps to configure Heidi Eraser –

1. Download Eraser application from http://eraser.heidi.ie/download.php:
2. Double click at installation file.
3. Accept GNU License terms.
4. Select "Typical" installation.
5. Select "Install".
6. Eraser application will be installed on your internal HD and shortcut will be available at desktop.
7. Select "Finish".
8. From your desktop shortcut open Eraser application.
9. Drag and drop file or folder you selected for permanent disposal. A message will pop-up to confirm you want to permanently delete selected file or folder

PA-DSS 2.2 (Aligns with PCI DSS Requirement 3.3)

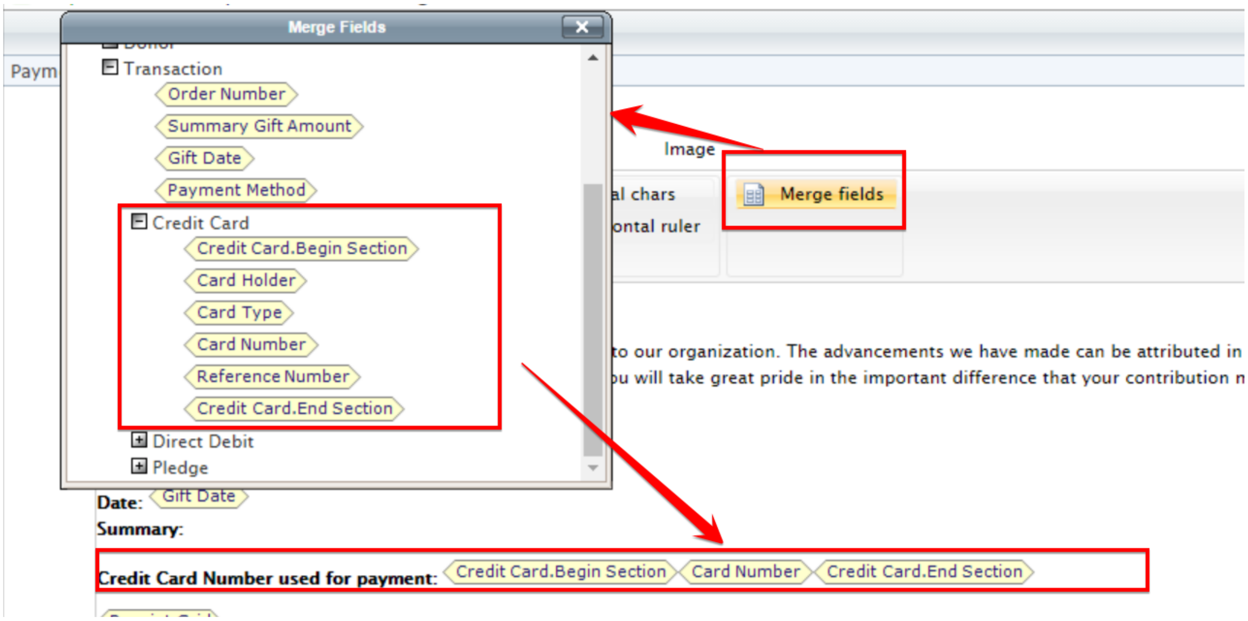
Mask PAN when displayed so only personnel with a business need can see more than the first six/last four digits of the PAN.

Details of all instances where PAN is displayed:

The 16-digit credit card number/PAN is always masked in the application. This masked PAN is managed by <merge fields> on all instances where it might need to be displayed. Only the person with Administrative privilege has the ability to choose to implement these <merge field> which can display the masked PAN.

No one (including admin) can see the full PAN number or can't see even first six digits. Only the last four digits will be visible.

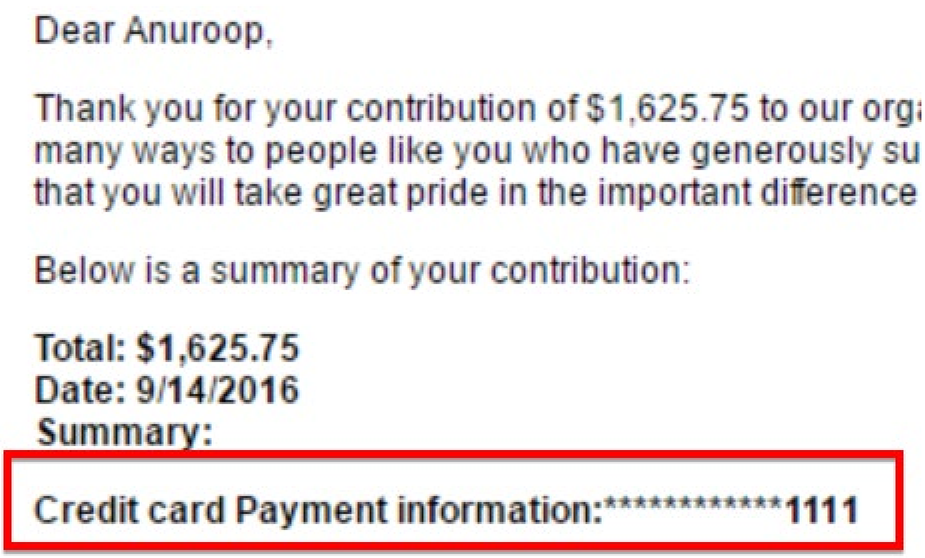
The following is an example of designing a message template on the **confirmation screen** of a part which will be used to perform a payment.



to our organization. The advancements we have made can be attributed in
ou will take great pride in the important difference that your contribution n

Date: Gift Date
Summary:
Credit Card Number used for payment: Credit Card.Begin Section Card Number Credit Card.End Section

This implementation would display the credit card details after a successful transaction as follows:


Dear Anuroop,

Thank you for your contribution of $1,625.75 to our org
many ways to people like you who have generously su
that you will take great pride in the important difference

Below is a summary of your contribution:

Total: $1,625.75
Date: 9/14/2016
Summary:

Credit card Payment information:**********1111**

Areas where the Credit card number/PAN can be displayed*(masked)*:

Confirmation Screen:

This screen is visible to the user after successful transaction on the webpage itself.

Acknowledgement email:

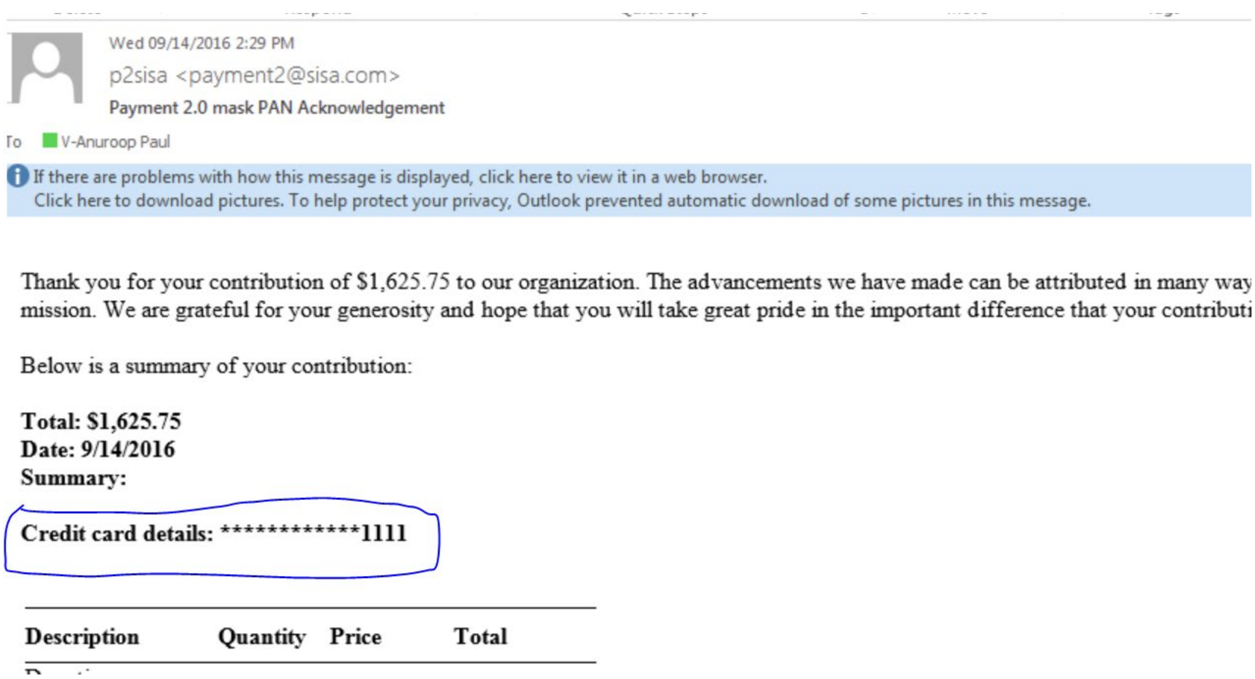
This email message is sent across to the intended recipient after a successful transaction on the webpage on the email address provided while completing the transaction. The message content here is again designed the same way as above. The PAN/credit card is always masked.

Areas where a credit card transaction can be processed:

- Donation
- Event registration classic
- Event registration New
- Membership form registration
- Using payment part 1
- Using payment part 2
- Donation through eCards
- Sponsorship
- Mini Donation Form

All the above parts have the confirmation screen and acknowledgement email which can be designed as described above.

The screen shot below refers to an **Acknowledgement email** received after successful completing a donation transaction.



Wed 09/14/2016 2:29 PM

p2sisa <payment2@sisa.com>

Payment 2.0 mask PAN Acknowledgement

To 🟩 V-Anuroop Paul

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Thank you for your contribution of $1,625.75 to our organization. The advancements we have made can be attributed in many way mission. We are grateful for your generosity and hope that you will take great pride in the important difference that your contributi

Below is a summary of your contribution:

Total: $1,625.75
Date: 9/14/2016
Summary:

Credit card details: ************1111

Description	Quantity	Price	Total

Blackbaud Internet Solutions does not facilitate the transmission of primary account numbers (PANs) through messaging technology such as email or instant messages.

Guidance: The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently.

The masking approach should always ensure that only the minimum number of digits are displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits.

PA-DSS 2.3 (Aligns with PCI DSS Requirement 3.4)

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).

Software Vendor Conformance:

Blackbaud Internet Solutions uses Truncation to ensure that the PAN is unreadable wherever it is stored. PAN is always truncated and that only last 4 digits of PAN is stored. By default, only last 4 digits of PAN are stored.

Guidance to Customers:

Ensure that PAN is rendered unreadable anywhere it is stored. Debugging logs are never enabled in the application, such feature is not provided in application. But still if any kind of logs include the PAN, they must be protected in accordance with PCI DSS and should be disabled as soon as any troubleshooting is completed. These should be securely deleted when they are no longer needed.

PA-DSS 2.4 (Aligns with PCI DSS Requirement 3.4)

Protect keys used to secure cardholder data against disclosure and misuse.

Software Vendor Conformance:

Blackbaud Internet Solutions does not store complete credit card numbers in its database. Application stores only truncated PAN number.

Guidance to Customers:

NA

PA-DSS 2.5 (Aligns with PCI DSS Requirement 3.6)

Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

Blackbaud Internet Solutions does not store or use any keys for encryption. Application stores only truncated PAN in database.

PA-DSS 2.6 (Aligns with PCI DSS Requirement 3.6)

Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.

Blackbaud Internet Solutions does not use keys for encryption. Application stores only truncated PAN in database.

USER ACCOUNT SECURITY

Requirement – 3 (Provide secure authentication features)

PA-DSS 3.1 (Aligns with PCI DSS Requirement 8.1 and 8.2)

Use unique user IDs and secure authentication for administrative access and access to cardholder data.

The payment application supports and enforces the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication is enforced to all accounts generated or managed by the application by the completion of installation and for subsequent changes after installation.

Guidance to Customers:

By ensuring each user is uniquely identified—instead of using one ID for several employees—an application supports the PCI DSS requirements to maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.

Secure authentication, when used in addition to unique IDs, helps protect users' IDs from being compromised, since anyone attempting to compromise an account would need to know both the unique ID and the password (or other authentication used).

PA-DSS Requirement 3.1.1(aligns with PCI DSS requirement 2.1)

Blackbaud Internet Solutions does not use any default administrative account which is used to log in to other Software which is necessary.

PA-DSS Requirement 3.1.2 (aligns with PCI DSS requirement 2.1)

There is no default supervisor login credential in clean Database which is provided to clients in case of a split hosted system. It is up to the client to set up the supervisor account with administrative rights with a complex password left up to the client's discretion.

In *Administration*, you can edit the login credentials and manage user accounts as necessary.

Guidance: If the application doesn't enforce changing of default passwords, the application could be left exposed to unauthorized access by anyone knowledgeable of the default settings

PA-DSS Requirement 3.1.3 (aligns with PCI DSS requirement 8.1.1)

Blackbaud Internet Solutions assigns unique user ids to every individual who registers with it.

Guidance: When each user is assigned a unique user ID, their access to and activities within the payment application can be traced back to the individual who performed them**.**

PA-DSS Requirement 3.1.4 (aligns with PCI DSS requirement 8.2)

Blackbaud Internet Solutions uses unique user ID and password for authentication.

Guidance: These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used).

By ensuring each user is uniquely identified—instead of using one ID for several employees—an application supports the PCI DSS requirements to maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.

When each user is assigned a unique user ID, their access to and activities within the payment application can be traced back to the individual who performed them.

PA-DSS Requirement 3.1.5 (aligns with PCI DSS requirement 8.5)

Blackbaud Internet Solutions does not use any group login such that a group of users share the same password.

Guidance: If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to assign accountability for, or to have effective logging of, an individual's actions, since a given action could have been performed by anyone that has knowledge of the authentication credentials.

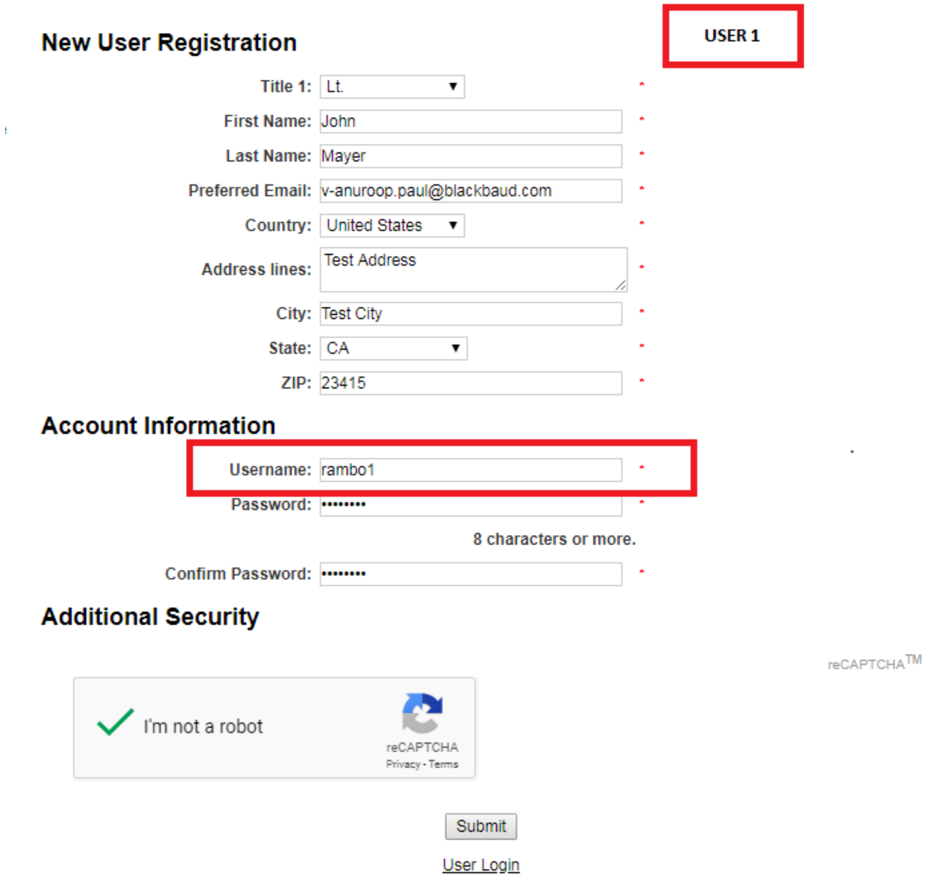
Warning: Do not change the default installation settings for the requirement of unique user login credentials and secure authentication. Adjustment from the default settings and requirements will result in noncompliance with PCI DSS.

The Blackbaud Internet Solutions employs a password to authenticate all users.

- **Authentication Mechanism:** Used id and Password
- **Method for protecting password (Hashing/Encryption):** Hashing and Salting
- **Algorithm used:** BCrypt
- **Location where credentials and salt are stored:** Database tables (Hashed value is stored in separate table in encrypted form in database.
- **Location database connection string is stored:** Web.config

The authentication method, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication if used).

USER 1:



USER 1

New User Registration

Title 1:	Lt. ▾ *
First Name:	John *
Last Name:	Mayer *
Preferred Email:	v-anuroop.paul@blackbaud.com *
Country:	United States ▾ *
Address lines:	Test Address *
City:	Test City *
State:	CA ▾ *
ZIP:	23415 *

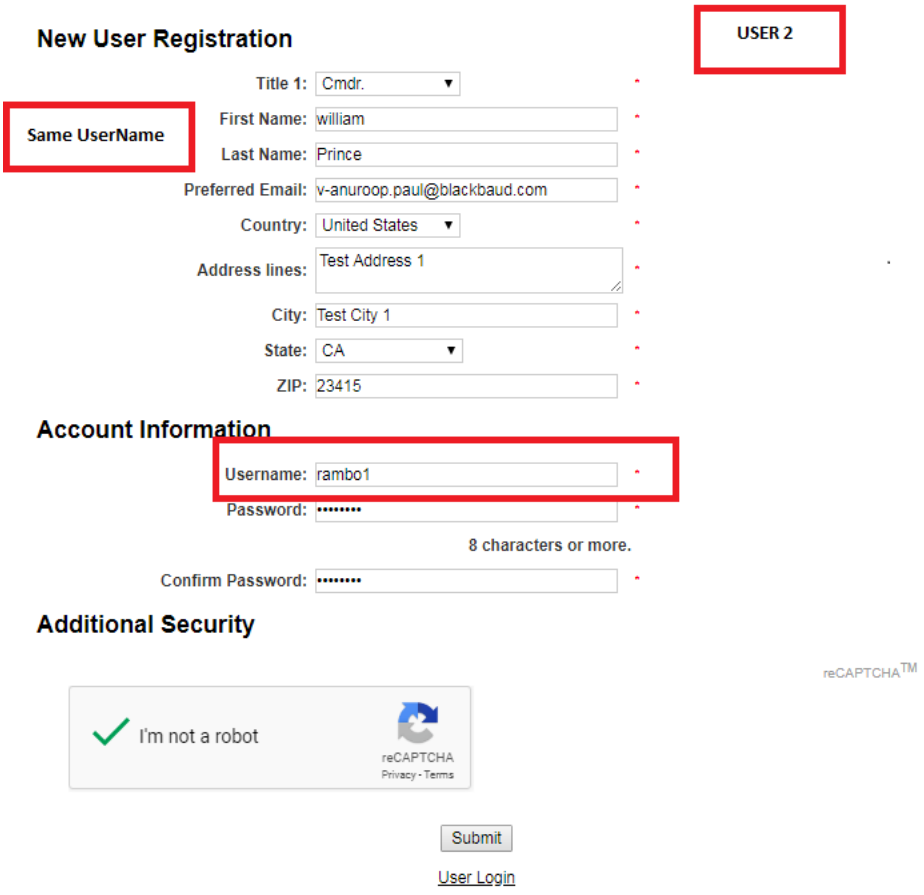
Account Information

Username:	rambo1 *
Password:	•••••••• *
	8 characters or more.
Confirm Password:	•••••••• *

Additional Security

reCAPTCHA™

USER 2



USER 2

Same UserName

New User Registration

Title 1:	Cmdr. ▼ *
First Name:	william *
Last Name:	Prince *
Preferred Email:	v-anuroop.paul@blackbaud.com *
Country:	United States ▼ *
Address lines:	Test Address 1 *
City:	Test City 1 *
State:	CA ▼ *
ZIP:	23415 *

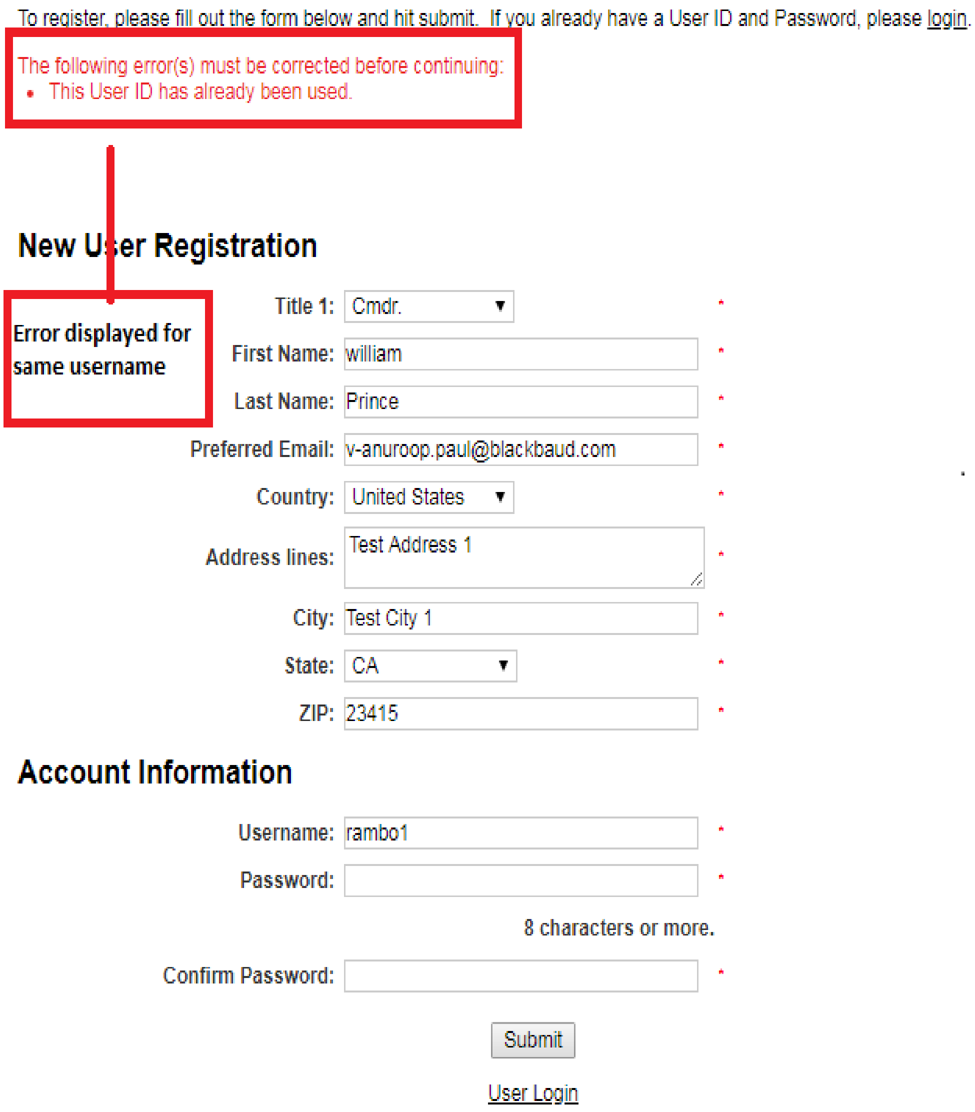
Account Information

Username:	rambo1 *
Password:	•••••••• *
	8 characters or more.
Confirm Password:	•••••••• *

Additional Security

reCAPTCHA™

ERROR ENCOUNTERED:



To register, please fill out the form below and hit submit. If you already have a User ID and Password, please login.

The following error(s) must be corrected before continuing:

- This User ID has already been used.

Error displayed for same username

New User Registration

Title 1:	Cmdr. ▼	*
First Name:	william	*
Last Name:	Prince	*
Preferred Email:	v-anuroop.paul@blackbaud.com	*
Country:	United States ▼	*
Address lines:	Test Address 1	*
City:	Test City 1	*
State:	CA ▼	*
ZIP:	23415	*

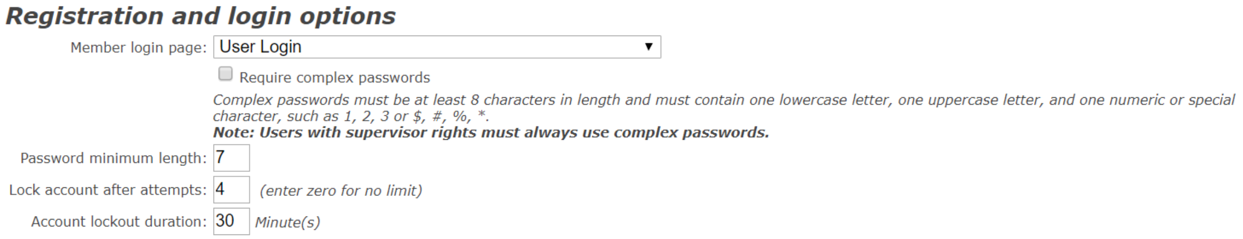
Account Information

Username:	rambo1	*
Password:		*
	8 characters or more.	
Confirm Password:		*

PA-DSS Requirement 3.1.6 (aligns with PCI DSS requirement 8.5)

In *Administration*, you can select to require users to use complex passwords from the System Options page. Complex passwords require at least eight characters, including one upper-case and one lower-case letter and either a special character or number. If you do not select **Require complex passwords**, you must configure the minimum number of characters required and select whether passwords are case-sensitive.

Guidance: Malicious individuals will often try to find accounts with weak or non-existent passwords in order to gain access to an application or system. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts, and compromise an application or system under the guise of a valid user ID. This requirement specifies passwords be a minimum of seven characters in length and that both numeric and alphabetic characters should be used. For cases where this minimum cannot be met due to technical limitations, entities can use "equivalent strength" to evaluate their alternative. NIST SP 800-63-1 defines "entropy" as "a measure of the difficulty of guessing or determining a password or key." This document and others that discuss "password entropy" can be referenced for more information on entropy value and equivalent password strength for passwords of different minimum formats.



Registration and login options

Member login page: User Login ▾

□ Require complex passwords

*Complex passwords must be at least 8 characters in length and must contain one lowercase letter, one uppercase letter, and one numeric or special character, such as 1, 2, 3 or $, #, %, *.*
Note: Users with supervisor rights must always use complex passwords.

Password minimum length: 7

Lock account after attempts: 4 *(enter zero for no limit)*

Account lockout duration: 30 *Minute(s)*

PA-DSS Requirement 3.1.7 (aligns with PCI DSS requirement 8.2.4)

Blackbaud Internet Solutions requires changes to user passwords at least once every 90 days.

PA-DSS Requirement 3.1.8 (aligns with PCI DSS requirement 8.2.5)

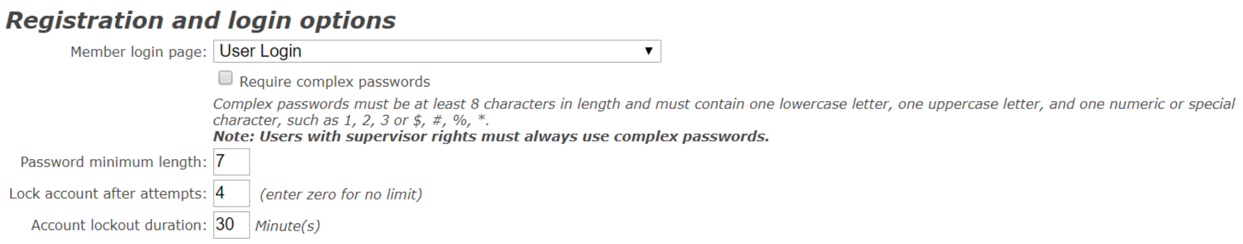
Blackbaud Internet Solutions keeps password history and requires that a new password is different than any of the last four passwords used.

PA-DSS Requirement 3.1.9 (aligns with PCI DSS requirement 8.1.6)

To secure your database, ***Blackbaud Internet Solutions*** can automatically lock out a user account after a specified number of failed login attempts. To prevent further attempts, a locked user account remains locked for a specified time period. On the System Options page, you can configure business rules to specify the number of failed attempts to allow before the program locks the user account and the duration of the lockout.

Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account

Invalid attempt configuration screen:



Registration and login options

Member login page: User Login ▾

□ Require complex passwords

*Complex passwords must be at least 8 characters in length and must contain one lowercase letter, one uppercase letter, and one numeric or special character, such as 1, 2, 3 or $, #, %, *.*

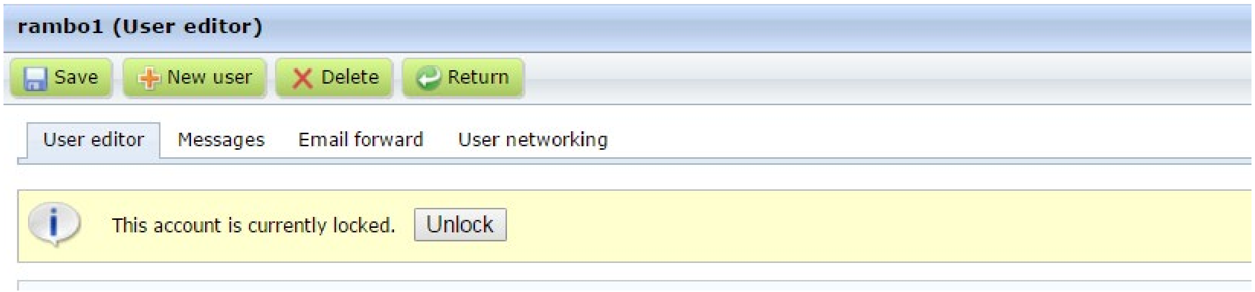
Note: Users with supervisor rights must always use complex passwords.

Password minimum length: 7

Lock account after attempts: 4 *(enter zero for no limit)*

Account lockout duration: 30 *Minute(s)*

In the Admin screen, see that the respective account is locked:



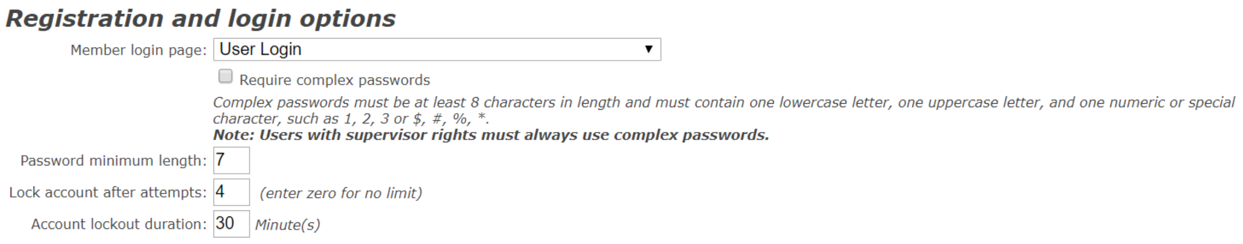
rambo1 (User editor)

This account is currently locked.

PA-DSS Requirement 3.1.10 (aligns with PCI DSS requirement 8.1.7)

Blackbaud Internet Solutions has the facility to configure the lockout duration on the Admin screen as below. The Site Admin needs to ensure that this is set to a minimum of 30 minutes.

Guidance: If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the administrator can validate that it is the actual account owner requesting reactivation.



Registration and login options

Member login page: User Login ▾

□ Require complex passwords

*Complex passwords must be at least 8 characters in length and must contain one lowercase letter, one uppercase letter, and one numeric or special character, such as 1, 2, 3 or $, #, %, *.*

Note: Users with supervisor rights must always use complex passwords.

Password minimum length: 7

Lock account after attempts: 4 *(enter zero for no limit)*

Account lockout duration: 30 *Minute(s)*

PA-DSS Requirement 3.1.11(aligns with PCI DSS requirement 8.1.8)

If a Blackbaud Internet Solutions session has been idle for more than 15 minutes, the application requires the user to re-authenticate to re-activate the session.

PA-DSS 3.2 (Aligns with PCI DSS Requirement 8.1 and 8.2)

Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.

Software Vendor Conformance:

Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication.

Blackbaud Internet Solutions supports customer use of unique ID's and secure authentication for user accounts and password used to access PCs, servers, and databases. It doesn't require the default administrator password for regular usage of the features and functionalities of the product.

Guidance to Customers:

Ensure that unique user IDs and secure authentication are followed

LOGGING APPLICATION ACTIVITY

Requirement – 4 (Log payment application activity)

PA-DSS 4.1 (Aligns with PCI DSS Requirement 10.1)

Implement automated audit trails.

Software Vendor Conformance:

Blackbaud Internet Solutions logs all the activities to the application by default. Whenever we have a new user /applicant to the system we have audit trails /logs which are maintained in the database which are unique for all individual users.

Guidance to Customers: It is critical that the application has a process or mechanism that links users to the application resources accessed, generates audit logs, and provides the ability to trace back suspicious activity to a specific user. Post-incident forensic teams heavily depend on these logs to initiate the investigation.

In BBIS Application, all the errors are logged in the error table in BBIS database and for user audit trials they are saved in Audit Table.

Enable database logging 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.

Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise. Including payment application logs in a centralized logging system allows the customer to integrate and correlate their logs and secure the logs consistently in their environment.

It is essential that logs are enabled by default and that disabling of logs are not compliant as per PCI DSS

PA-DSS 4.4 (Aligns with PCI DSS Requirement 10.5.3)

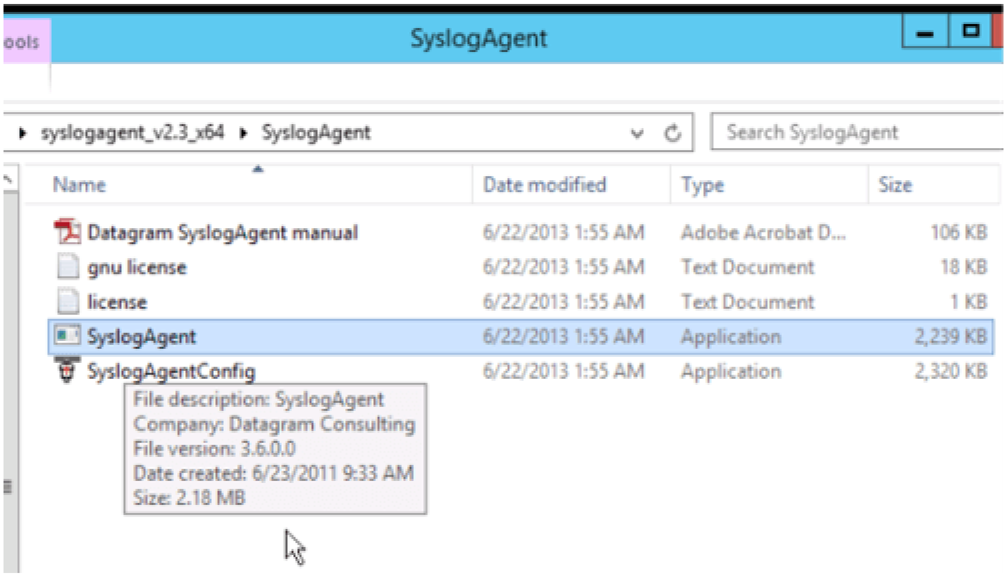
Facilitate centralized logging.

Software Vendor Conformance:

In Blackbaud Internet Solutions, all the logs are stored in database. All the errors are logged in the error table in BBNC database and for user audit trials they are saved in Audit Table. This can be achieved by using any of the tools like Rsyslog, syslog and log4net etc.

Steps to configure syslog: -

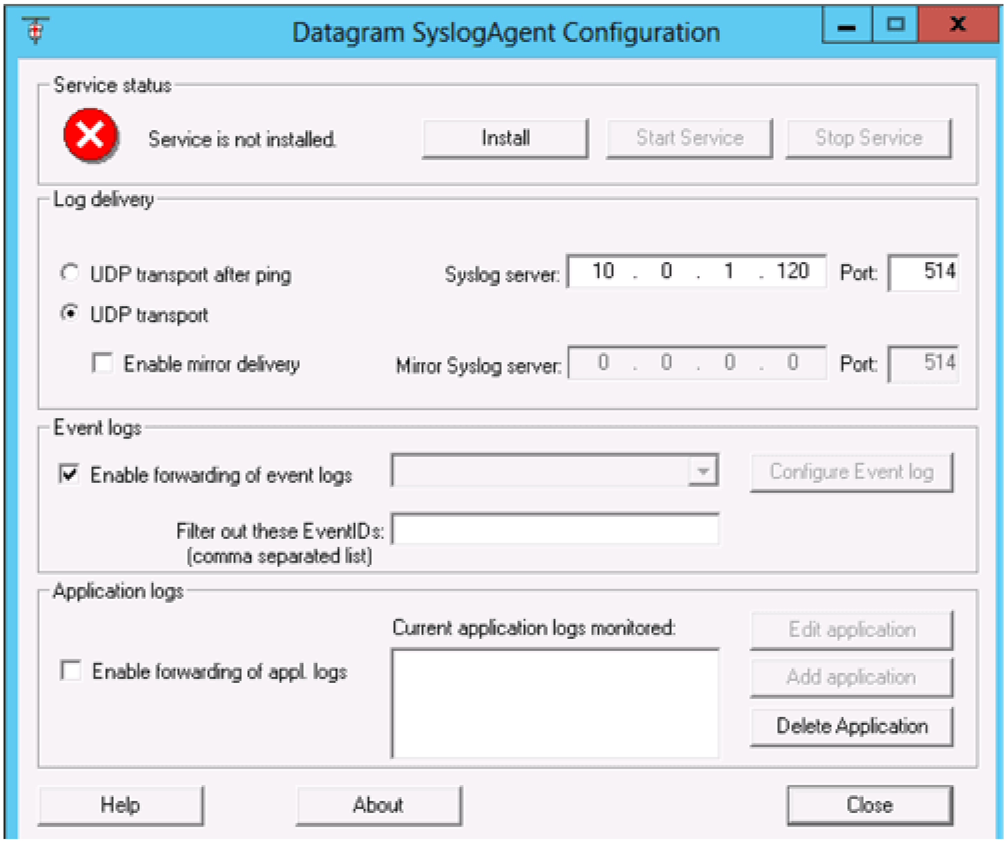
1. Download the tool and extract the 2MB Syslog file that you downloaded. Below are Syslog Agent Installation Files –



Name	Date modified	Type	Size
Datagram SyslogAgent manual	6/22/2013 1:55 AM	Adobe Acrobat D...	106 KB
gnu license	6/22/2013 1:55 AM	Text Document	18 KB
license	6/22/2013 1:55 AM	Text Document	1 KB
SyslogAgent	6/22/2013 1:55 AM	Application	2,239 KB
SyslogAgentConfig	6/22/2013 1:55 AM	Application	2,320 KB

File description: SyslogAgent
Company: Datagram Consulting
File version: 3.6.0.0
Date created: 6/23/2011 9:33 AM
Size: 2.18 MB

2. Installing the SyslogAgent Service



Datagram SyslogAgent Configuration

Service status

Service is not installed.

Log delivery

○ UDP transport after ping

● UDP transport

□ Enable mirror delivery

Syslog server: 10 . 0 . 1 . 120 Port: 514

Mirror Syslog server: 0 . 0 . 0 . 0 Port: 514

Event logs

☑ Enable forwarding of event logs

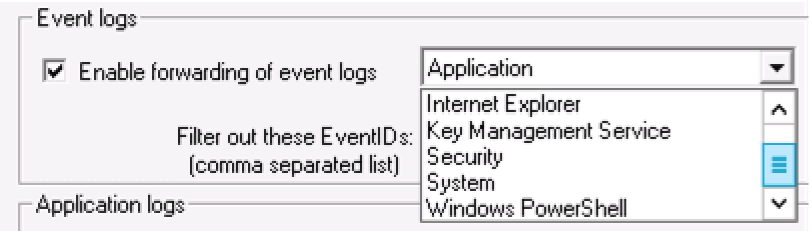
Filter out these EventIDs: (comma separated list)

Application logs

□ Enable forwarding of appl. logs

Current application logs monitored:

3. Selecting the Event Logs to Send to the Syslog Host



Event logs

☑ Enable forwarding of event logs

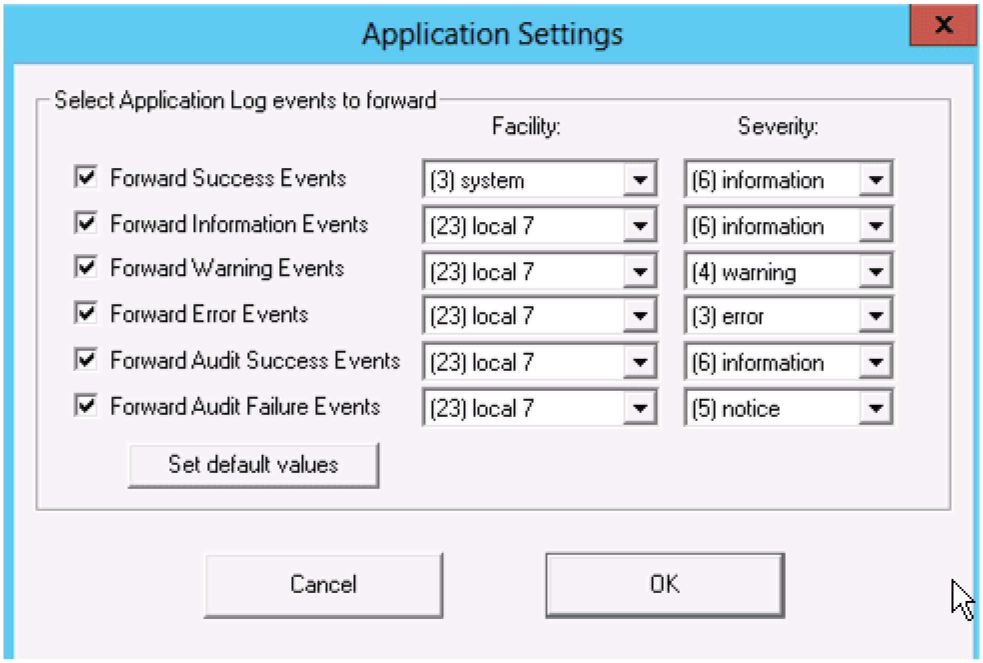
Application

- Internet Explorer
- Key Management Service
- Security
- System
- Windows PowerShell

Filter out these EventIDs: (comma separated list)

Application logs

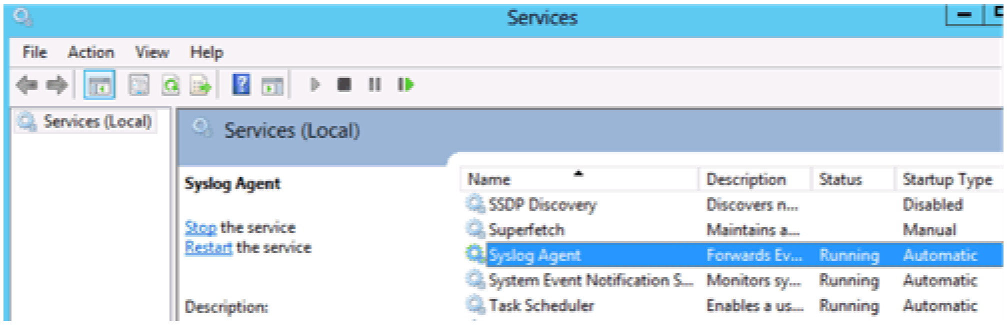
4. Customizing Facility and Severity



Select Application Log events to forward

	Facility:	Severity:
☑ Forward Success Events	(3) system	(6) information
☑ Forward Information Events	(23) local 7	(6) information
☑ Forward Warning Events	(23) local 7	(4) warning
☑ Forward Error Events	(23) local 7	(3) error
☑ Forward Audit Success Events	(23) local 7	(6) information
☑ Forward Audit Failure Events	(23) local 7	(5) notice

5. Once configured, Click Start Service. SyslogAgent Running in Services



Syslog Agent

Stop the service
Restart the service

Description:

Name	Description	Status	Startup Type
SSDP Discovery	Discovers n...		Disabled
Superfetch	Maintains a...		Manual
Syslog Agent	Forwards Ev...	Running	Automatic
System Event Notification S...	Monitors sy...	Running	Automatic
Task Scheduler	Enables a us...	Running	Automatic

Requirement – 5 (Develop Secure Payment Applications)

PA-DSS 5.4.4

Implement and communicate application versioning methodology

VERSIONING SCHEME

Blackbaud software products follow a numeric versioning scheme to identify the latest software release and the type of update:

- ➔ Major release,
- ➔ Minor release,
- ➔ Security
- ➔ Build

Major. Minor. Security. Build

Major - Denotes the major feature change

Minor - Denotes minor feature change

Security - Denotes PA-DSS or Security impacting change

Build – Wildcard element which denotes the build number or version

WIRELESS TRANSMISSIONS

Requirement – 6 (Protect Wireless Transmissions)

PA-DSS 6.1 (Aligns with PCI DSS Requirements 1.2.3 & 2.1.1)

Securely implement wireless technology.

Software Vendor Conformance:

Blackbaud Internet Solutions is **not developed** to be operated as a wireless payment application. Hence this requirement is not applicable.

Guidance to Customers:

Blackbaud Internet Solutions application is not developed and doesn't support for use with wireless technology. If wireless technology is used only to access the Blackbaud Internet Solutions application, ensure that the below controls are in place.

PA-DSS 6.2 (Aligns with PCI DSS Requirement 4.1.1)

Secure transmissions of cardholder data over wireless networks.

Software Vendor Conformance:

Blackbaud Internet Solutions is not designed to be operated as a wireless payment application. However, PCI DSS-compliant wireless settings should be configured if the wireless communication is used in the internal network.

Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks.
Strong cryptography for authentication and transmission of cardholder data is required to prevent malicious users from gaining access to data on a wireless network or utilizing wireless networks to access other systems or data.

Guidance to Customers:

For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

PA-DSS 6.3 (Aligns with PCI DSS Requirement 1.2.3, 2.1.1, & 4.1.1)

Provide instructions for secure use of wireless technology.

Software Vendor Conformance:

Blackbaud Internet Solutions application is not developed for use with wireless technology. However, PCI DSS-compliant wireless settings should be configured if the wireless communication is used in the internal network.

Guidance to Customers:

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 encryption keys from the default. After installation, change encryption keys when anyone with knowledge of the keys 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 Wi-Fi 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 to implement strong encryption for the transmission of cardholder data and sensitive authentication data over the wireless network in the cardholder data environment

Requirement – 7

PA-DSS 7.2.3

Provide instructions for customers about secure installation of patches and updates.

Software Vendor Conformance:

Patches and updates are communicated through E-Mail. To ensure the chain of trust, the installer will be digitally signed along with MD5 checksum to ensure the integrity

Notifications on New Patches and updates are done via the following URL as well:

https://community.blackbaud.com/blogs/54

Guidance to Customers:

Before you install any updates, we strongly recommend you back up your database. For information about the update process, see the Update and New Features 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

SERVICES AND PROTOCOLS

Requirement – 8 (Facilitate secure network implementation)

PA-DSS 8.2 (Aligns with PCI DSS Requirement 2.2.2)

Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

Software Vendor Conformance:

Application uses SMTP(25) - Used for communicating with email services, HTTP(80) - Used for internal communication with other backend services, HTTPS(443) - Used for interfacing with end customer and SQL Traffic – Used for communicating with DB Server. This is Customizable in site and settings. Apart from these application makes use of TLS v1.2.

Payment application by default uses and enables only the services, protocols, ports, daemons, component, dependent software and hardware which are required for the proper functioning of payment application. All the services, ports, protocols which are not required for the payment application to be disabled by the system administrators.

Note: *SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that uses or supports TLS must not allow fallback to SSL*

Guidance to Customers:

Customer should harden the servers and applications as per the vendor security guidelines and run only the services, ports and protocols which are required for the application mentioned above. All the unwanted services to be disabled.

Requirement 9: Cardholder data must never be stored on a server connected to the internet

PA-DSS 9.1 (Aligns with PCI DSS Requirement 1.3.7)

Store cardholder data only on servers not connected to the Internet.

Software Vendor Conformance:

The payment application must be developed such that any web server and any cardholder data storage component (for example, a database server) are not required to be on the same server, nor is the data storage component required to be on the same network zone (such as a DMZ) with the web server

Guidance to Customers:

Customer sensitive information such as cardholder data should not be stored on any system that can be accessed from the Internet.

In an Internet-based application configuration, the role of the web server and the database server containing customer sensitive information must not be performed by the same physical machine, and the database server must not be exposed directly to the Internet.

Requirement – 10 (Facilitate secure remote access to payment application)

PA-DSS 10.1 (Aligns with PCI DSS Requirement 8.3)

Implement multi-factor authentication for all remote access to payment application that originates from outside the customer environment.

Software Vendor Conformance:

Application does not support the remote access to payment application.

Multi-factor authentication requires at least two methods of authentication for access originating from outside the network.

The requirement for multi-factor authentication applies to all personnel with remote access that originates from outside the customer environment.

Guidance to Customers:

Customers should ensure to follow multi factor authentication for any remote access originating from outside the customer environment

PA-DSS 10.2 (Aligns with PCI DSS Requirement 1 and 12.3.9)

Securely deliver remote payment application updates.

Software Vendor Conformance:

If Application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes.

Alternatively, if delivered via virtual private network (VPN) or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections.

Guidance to Customers:

Any remote-access mechanism employed by the payment application vendor and/or integrators/resellers—for example, to support services being delivered by those providers—should support all applicable PCI DSS requirements.

PA-DSS 10.2.3

Securely implement remote-access software

Software Vendor Conformance:

Blackbaud Internet Solutions application doesn't provide the functionality for remote access. Hence this requirement is not applicable. Any remote access to the server at the operating system layer must require the organization implementing multi-factor authentication mechanism if access to the payment application server is originating from outside the customer environment to access the server.

Guidance to Customers:

The default settings in the remote-access software such as default passwords should be changed. Unique passwords should be used for each customer. The connections from specific (known) IP/MAC address only should be allowed. For logins, strong authentication and complex passwords should be used (for reference, see PA-DSS requirements 3.1.1 through 3.1.11).

The data transmission should be encrypted as per PA-DSS requirement 12.1. The account lockout should be enabled after failed login attempts (for reference see PA-DSS requirement 3.1.9 through 3.1.10).

The virtual Private Network ("VPN") connection should be established via a firewall before the access is allowed. The logging functionality should be enabled. The authorized integrator/reseller personnel should be restricted access to customer environments.

If access to CCA is provided to remote users, customer must implement remote authentication mechanisms and security controls in adherence to PCI DSS requirements.

NETWORK SECURITY

Requirement – 11 (Encrypt sensitive traffic over public networks)

PA-DSS 11.1 (Aligns with PCI DSS Requirement 4.1)

Secure transmissions of cardholder data over public networks.

Software Vendor Conformance:

Payment application uses secure HTTPS protocol for the communication across all open and public networks.

Guidance to Customers:

Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data.

Note that some protocol implementations (such as SSL, SSH version 1.0, and early TLS) have documented vulnerabilities, such as buffer overflows, that an attacker can use to gain control of the affected system. Regardless of which security protocols are used by the payment application, ensure they are configured by default to use only secure configurations and versions to prevent an insecure connection being used.

Ensure that policies and processes are in-place to ensure that any cardholder information are transmitted

PA-DSS 11.2 (Aligns with PCI DSS Requirement 4.2)

Encrypt cardholder data sent over end-user messaging technologies.

Software Vendor Conformance:

Blackbaud Internet Solutions does not support sending of PANs by end-user messaging technologies.

Guidance to Customers:

Customers are instructed not to use any end-user messaging technologies for sending the PAN numbers in the internal or external network. Payment application administrator at the customer environment is responsible for providing access on the role based for the users of payment application and enables the view of PAN number on need to know basis

NON-CONSOLE ADMINISTRATIVE ACCESS

Requirement – 12 (Encrypt all non-console administrative access)

PA-DSS 12.1 (Aligns with PCI DSS Requirement 2.3)

Encrypt non-console administrative access.

Software Vendor Conformance:

Blackbaud, Inc. does not allow non-console access to the application.

Guidance to Customers:

If non-console access is required, use of strong cryptography for encryption should be used.

PA-DSS 12.2: Use multi-factor authentication for all personnel with non-console administrative access.

Use multi-factor authentication for all personnel with non-console administrative access.

Software Vendor Conformance:

Administrative access requires a higher level of assurance that the individual attempting to gain access is who they claim to be.

When accessing machines installed with Blackbaud Internet Solutions make sure to follow these guidelines for non-console administrative access below.

Guidance to Customers:

Blackbaud, Inc. recommends customer to adhere to the following:

* Use multi-factor authentication for all personnel with non-console administrative access.

* All non-console administrative access should be secured using technologies such as SSH, VPN, or TLS, for web-based management and other non-console administrative access

* Use Secure Terminal emulator such as putty and select SSH for securely accessing Unix based environment

* **Note:** Clear-text protocols such as Telnet or rlogin must never be used for administrative access. SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.