Configuration Overview Guide

1/22/2019 Blackbaud NetCommunity 7.1 Configuration Overview UK

Config Overview-2017

Contents

Configuration Overview

The NetCommunity Server Service Oriented Architecture

Blackbaud NetCommunity Server is built on a Service Oriented Architecture (SOA).

The following table lists the services involved in the application:

Name	Type
Blackbaud NetCommunity	ASP.Net Web Application
The Raiser's Edge Database	See ***The Raiser's Edge*** documentation
Blackbaud NetCommunity Database	See ***Blackbaud NetCommunity*** system requirements document
RE7Service Web Service for ***The Raiser's Edge*** Blackbaud Core Components (includes BBAppfx service)	ASP.Net Web Service
The Raiser's Edge Client Application	Windows Application
Blackbaud Management Console	Windows Application
The Raiser's Edge deploy folder	Directory
PluginService WS	ASP.Net Web Service
Blackbaud Payment Service (BBPS)	Web Service
Mail Service WS	ASP.Net Web Service

In case of client hosted installations, most of these services are deployed at the Customer site. There are many possible configurations for the actual deployment of the various services. The exact configuration for a particular customer varies based on a number of factors:

- The existing IT/web/database infrastructure of the customer
- The number of machines available to the customer
- The customer's ability and willingness to add new hardware
- The customer's license requirements with regard to SQL Server and Windows Server
- The customer's preference for firewall, router, and domain controller topology
- The customer's preference for accessibility of various parts of the application

There is not a "one size fits all" configuration that works for every customer. To enable our customer and services team to best decide about deployment issues, this document describes the requirements for each service along with notes about any special security considerations to take into account.

Note: Although this document includes potential performance information, note that performance and response times 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).

Security Considerations

Security is a sensitive topic these days, especially related to Internet applications. The complexity of the ***Blackbaud NetCommunity*** server system, with its many interrelated services, means one must pay particular attention to security issues. For each service, there are a number of security issues to address:

- Is the service visible to the public Internet?
- On which side of a firewall should the service be located?
- If behind a firewall, which ports should be open to access the service?
- Does the service need to access other services over a public network?
- Can the service be locked down to intranet users only?
- Are secure communications required with the service?

Each service has different requirements regarding the accessibility of the service and the need for secure communication with the service. This document describes in detail the requirements for each service and suggests possible ways to secure the service.

Firewall Configuration

The concept of a firewall is an essential part of any web application deployment. Firewalls can be implemented in software or hardware, and there are many possible configurations. To isolate traffic from the public Internet, a single firewall can be used at the perimeter of the network. To add a degree of safety, one popular configuration is to employ a secondary firewall, which creates a DMZ zone to further isolate the public Internet server from the internal network. The key to the effective use

of firewalls is that they be correctly configured to allow only the minimum access required. This document has an "Accessible From" section and "Needs Access To" section for each service in the ***Blackbaud NetCommunity*** Server application. To provide guidance when configuring firewalls, these sections describe the minimum required access to and from each service.

None of the customer site web services require access from the Internet, only the ***Blackbaud NetCommunity*** application. If your firewall supports rules based on only port numbers (as opposed to specific URLs), you may want to create a second website in IIS that uses a port other than 80, such as 8001. Using the firewall policy, you can restrict access to port 8001 and only allow port 80 to be open to the Internet.

Windows Server Considerations

Worker Process Identity

The worker process model can be configured by establishing one or more application pools. You can configure each application pool to run under a different identity. The default application pool is configured to run as the user "NT Authority\Network Service". Therefore, when discussing the identity of the worker process in this document, any reference to the user account "ASPNET" should be considered the identity used by the worker process of the application pool configured for the virtual directory, which by default is "NT Authority\Network Service".

Performance Considerations

Because an unpredictable number of users with unpredictable usage patterns access the ***Blackbaud NetCommunity*** web application, this application is the major area of concern. In addition, because ***Blackbaud NetCommunity*** sometimes requests data from the RE7Service web service (***The Raiser's Edge***) or the BBAppfx web service (Blackbaud Core Components), the service is likely to be a hotspot for performance. The exact performance characteristics for the application vary, based on the number of community users, the kinds of content the customer defines, the mix of pages the customer creates, and the usage patterns of the community users.

The ***Blackbaud NetCommunity*** Server SOA scales up and scales out. This means the ***Blackbaud NetCommunity*** web application and the entire web services support is load-balanced across multiple machines. If the website becomes popular to the point of providing unacceptable response times, you can add a second or third web server to split the load. Likewise, if the RE7Service web service or BBAppfx web service becomes a bottleneck, you can add other machines in that role.

Recommended Default Configuration

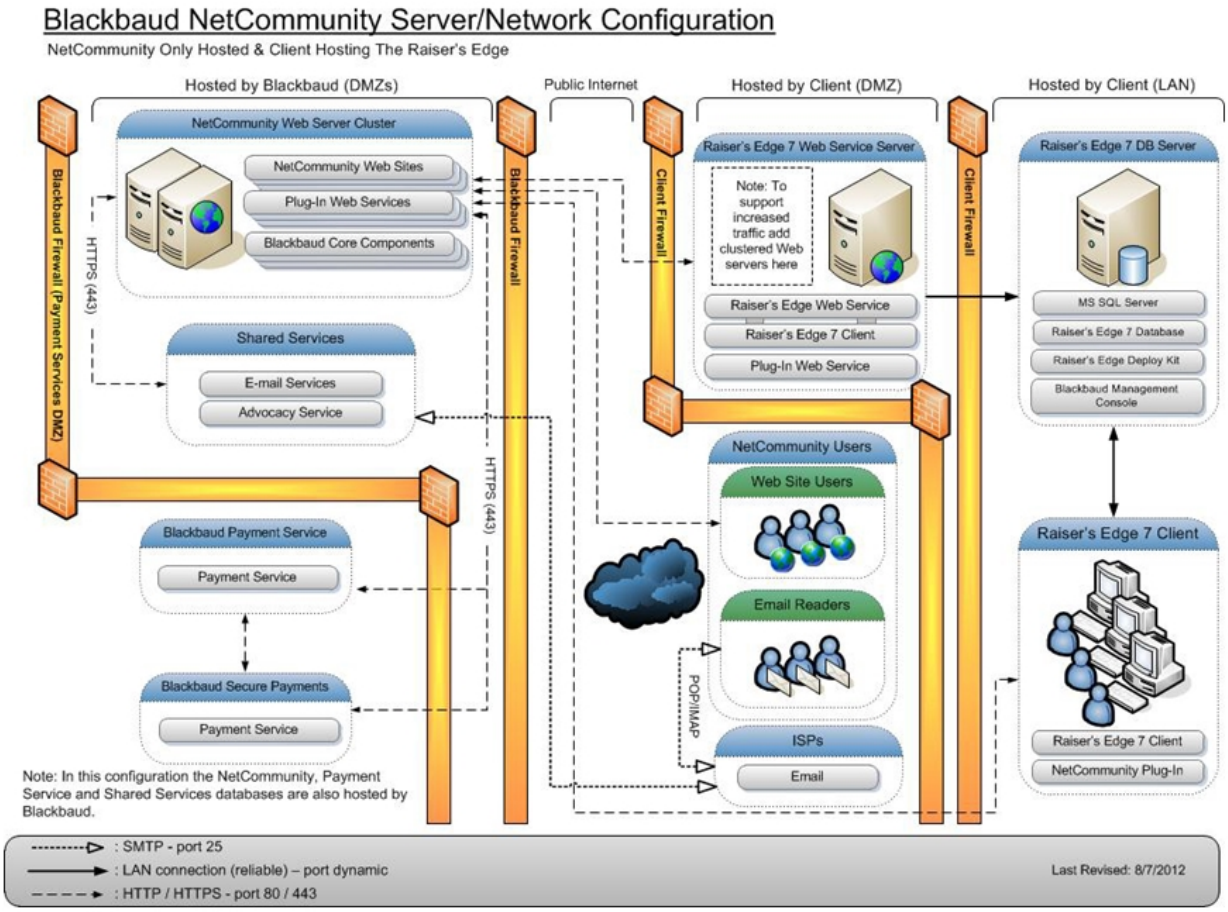
The SOA provides flexibility so you can move services between machines as required. However, the more machines involved, the greater the cost for configuration and possibly software licenses. Alternatively, a customer may want to run the Blackbaud database on an existing SQL Server instance and dedicate the web server to run the IIS/ASP.Net services. Each configuration has trade-offs with regard to complexity, security, and resources.

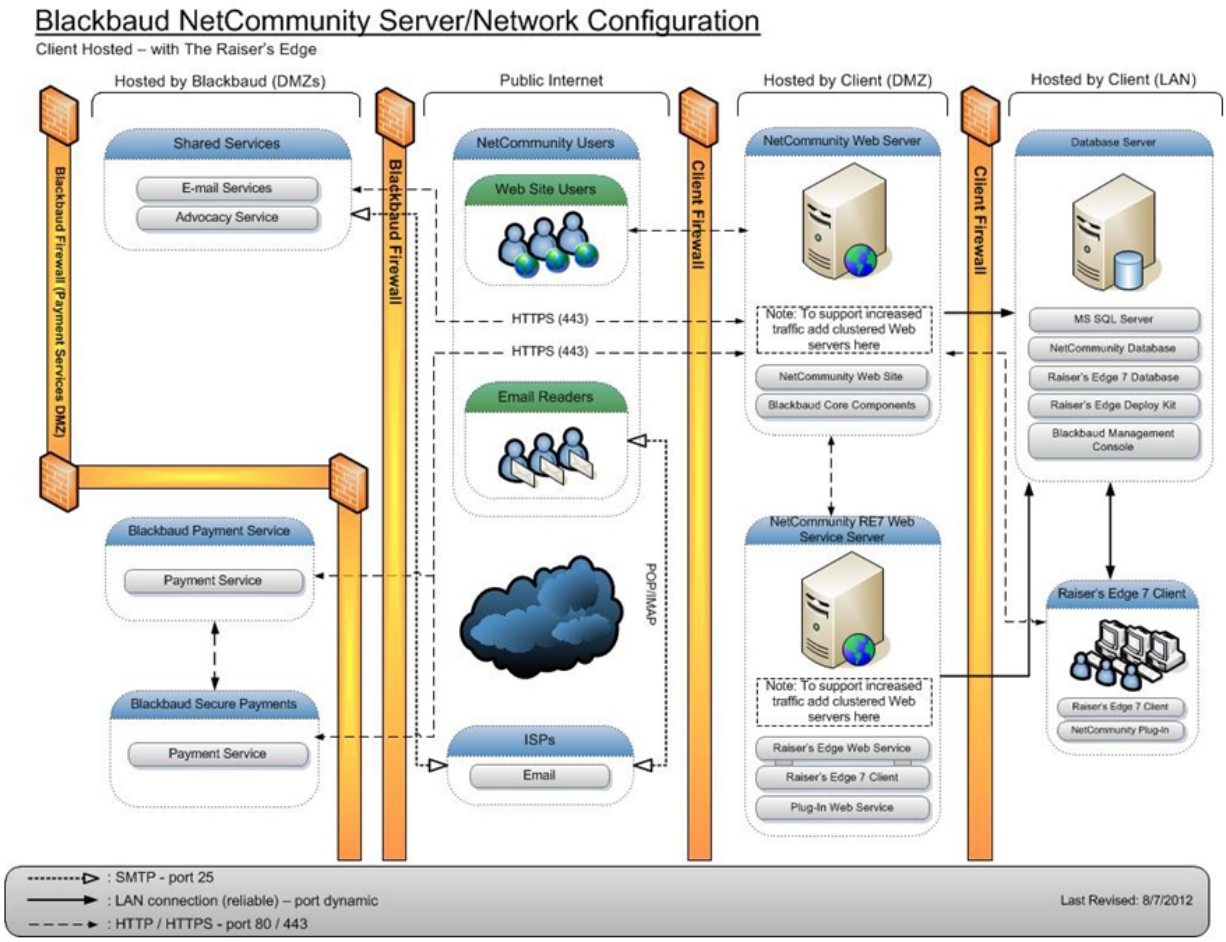
The recommended default configuration should be considered just that — a recommendation to establish a baseline configuration. Each customer may choose to customise this configuration based on specific requirements.

The minimum recommended baseline consists of the following machines:

— Fire Wall from Internet to DMZ —
Open Ports: 80, 443, 8001 (Intranet Addresses ONLY!)
DMZ
Server 1
Blackbaud NetCommunity web application (port 80, 443) Blackbaud Core Components (install on Server 1 for ***The Raiser's Edge*** 7.x solutions)
— Fire Wall from DMZ to Intranet —
Open Ports: 80
Intranet
Server 2
RE7Service Web Service for ***The Raiser's Edge*** (port 80), or Blackbaud Core Components (install on Server 2 for non-***Raiser's Edge*** 7.x solutions) Plugin Service WS (port 8001)
Server 3
The Raiser's Edge SQL Server database or Blackbaud database

For visual assistance in deciding the configuration for your organisation, see the following diagram s of ***Blackbaud NetCommunity***'s architecture for ***The Raiser's Edge***. For installation information, see the *Infinity Platform Installation and Upgrade Guide*.


Blackbaud NetCommunity Server/Network Configuration
NetCommunity Only Hosted & Client Hosting The Raiser's Edge
Hosted by Blackbaud (DMZs)
Public Internet
Hosted by Client (DMZ)
Hosted by Client (LAN)
Blackbaud Firewall (Payment Services DMZ)
NetCommunity Web Server Cluster
NetCommunity Web Sites
Plug-In Web Services
Blackbaud Core Components
HTTPS (443)
Shared Services
E-mail Services
Advocacy Service
Blackbaud Payment Service
Payment Service
Blackbaud Secure Payments
Payment Service
Note: In this configuration the NetCommunity, Payment Service and Shared Services databases are also hosted by Blackbaud.
Blackbaud Firewall
HTTPS (443)
Client Firewall
Raiser's Edge 7 Web Service Server
Note: To support increased traffic add clustered Web servers here
Raiser's Edge Web Service
Raiser's Edge 7 Client
Plug-In Web Service
NetCommunity Users
Web Site Users
Email Readers
POP/IMAP
ISPs
Email
Client Firewall
Raiser's Edge 7 DB Server
MS SQL Server
Raiser's Edge 7 Database
Raiser's Edge Deploy Kit
Blackbaud Management Console
Raiser's Edge 7 Client
Raiser's Edge 7 Client
NetCommunity Plug-In
: SMTP - port 25
: LAN connection (reliable) – port dynamic
: HTTP / HTTPS - port 80 / 443
Last Revised: 8/7/2012



Service Security Requirements

NetCommunity Web Server

Service Type

- ASP.Net web application

Accessible From

- Public Internet (for donor facing pages) (HTTP + HTTPS)
- Intranet (for administrative pages)

Note: Administrative pages may be optionally made available over the public Internet. If you plan to have the administrative site available over the Internet, we recommend you enable SSL for your administrative pages. For information about how to enable SSL, see the *Infinity Platform Installation and Upgrade Guide*.

Needs Access To

- Blackbaud Database
- RE7Service Web Service (***The Raiser's Edge***)/Blackbaud Core Components
- Blackbaud Hosted Web Services

Secured Communications Required

We recommend you secure all administrative pages and certain client site pages in the application — such as pages that accept credit card information for donations — with Transport Layer Security (TLS). TLS is the current standard technology, which replaces Secure Sockets Layer (SSL), for establishing encrypted links between web servers and browsers. From the ***Blackbaud NetCommunity*** web application administrative interface, users can decide which pages to secure. The SSLPage.aspx resource serves any page that contains content that should be secured. Users should assign a TLS certificate to the ***Blackbaud NetCommunity*** web server with the IIS Administration tool and set SSLPage.aspx to require TLS.

Blackbaud TLS provides communication to the Blackbaud-hosted web services. No action is needed by clients to enable this.

If any other services are accessed over a public network, we recommend you employ IPSec or TLS to secure communications between the ***Blackbaud NetCommunity*** web application and those services. Normally, this will not be the case because all the other services are located inside the DMZ behind the firewall.

Deployment Considerations

Depending on the graphics and web design, a first time ***Blackbaud NetCommunity*** web page request without client-caching (for example, when you press CTRL F5 to refresh) can be 500 to 600 KB in size. However, because the browser caches images and other objects, a typical request may generate 10KB of HTML traffic from server to browser.

For best results, we recommend you use a dedicated circuit, such as full T1 to a tier 1 ISP, scaled to aggregate the concurrent applications users (100 - 200 Kbps per typical web user). The necessary connection speed depends on the ***Blackbaud NetCommunity*** activity based on your website's usage by visiting users and should be reviewed with your consultant during implementation.

The following table shows the potential pages per second a user can download based on the connection speed to the IIS server.

***In these examples, we assume a 10KB request includes protocol overhead.**

Connection Type	Connection Speed	10KB Pages per Second
DSL (ADSL or SDSL)	640 Kbps (common upstream speed)	8
T1	1.544 Mbps	19
10 Mb Ethernet	8 Mbps (best case)	100
DS3/T3	44.736 Mbps	560
OC1	51.844 Mbps	648

***In these examples, we assume a 10KB request includes protocol overhead.**

Connection Type	Connection Speed	10KB Pages per Second
100 Mb Ethernet	80 Mbps (best case)	1,000
OC3	155.532 Mbps	1,944
1 Gb Ethernet	800 Mbps (best case)	10,000

Database Access

The ***Blackbaud NetCommunity*** application must be able to access the Blackbaud database. For security purposes, the database should be maintained behind the firewall; however, other custom configurations are possible.

Blackbaud NetCommunity uses the connection string specified in the web.config file to connect to the database.

If you run the database on a separate machine, use a connection string like the following to use SQL Server authentication:

<add key="ConnectionString"

value ="server = {SERVER NAME}; database={DATABASENAME}; user id={BBPortalWebUser};

pwd={PASSWORD}" />

*where {SERVER NAME}, {DATABASENAME}, {BBPortalWebUser}, and {PASSWORD} are determined by the customer

Note: Windows authentication is also supported. Please see https://msdn.microsoft.com/en-us/library/ms178371(v=vs.100).aspx for more details. This is configured with information requested during the standard ***Blackbaud NetCommunity*** installation.

Web Service Access

The web application connects to the RE7Service web service (***The Raiser's Edge***) or BBAppfx web service (Blackbaud Core Components) as specified in the configuration.aspx. In the web application, the user can specify these settings on the Configuration page in *Administration*. The relevant settings are:

- **Database Number** – The RE_iniX number, as specified in the RE7Service or BBAppfx web service machine registry.
- **URL** – The URL that points to the web server where the RE7Service or BBAppfx web service runs.
- **User** and **Password** – The specific user name and password unique to the customer site. This pair is mirrored in the web.config of the RE7Service or BBAppfx web service to protect the credentials from unauthorised use. If properly configured, the RE7Service or BBAppfx web service is not visible to anything except the web server; this serves as an additional gatekeeper.

Blackbaud Hosted Service Access

Blackbaud hosts several web services, including those responsible for sending email, making credit card transactions, and processing advocacy transactions. You can access these services using a

Blackbaud supplied user name and password. In the web application, the user can specify these settings on the Configuration page in *Administration*. In the Blackbaud Services frame, the relevant settings are:

- **Host Name** – The host name that points to the Blackbaud hosted web server responsible for the services.
- **Connect to Blackbaud Services using https** – Mark this checkbox to connect to the Blackbaud services via https. Unless otherwise instructed by Blackbaud Support, leave this checkbox marked.
- **User** and **Password** – The user name and password, provided by Blackbaud, that are unique to the customer site. The user name and password are requested during the ***Blackbaud NetCommunity*** installation.

Blackbaud NetCommunity Application Configuration Checklist

[ ] Isolate the web server from the Internet by a firewall (hardware or software). Only port 80 (HTTP) and 443 (HTTPS) should be open.

[ ] Secure SSLPage.aspx with an SSL certificate.

[ ] (Recommended) When building client page URLs that contain secure content, such as login screens or credit card forms, require Windows authentication. On the Configuration page in *Administration*, mark **Require for secure content**.

[ ] (Recommended) For Administrative tools, require Windows authentication. On the Configuration page in *Administration*, mark **Require administration pages**.

The installation updates the following settings.

- ConnectionString

- REDBNumber

- RE7ServiceURL

- RE7ServiceUser (CUSTOMER SPECIFIC)

- RE7ServicePassword (CUSTOMER SPECIFIC)

- BlackbaudServices (provided by Blackbaud)

- BlackbaudServiceUser (provided by Blackbaud)

- BlackbaudServicePassword (provided by Blackbaud)

Blackbaud Database

Service Type

- SQL Server is required, See system requirements document

Accessible From

- ***Blackbaud NetCommunity*** application web server
- ***Blackbaud CRM*** Client Application

- PluginService web service
- BBAppfx Web Service

Needs Access To

- N/A

Secured Communications Required

Normally, this server is behind a firewall and communication is not over a public network. Therefore, there is no requirement to secure communication with this server. If the user desires a secure communication between the web servers and the database server, IPSec can be used.

Deployment Considerations

SQL Server is required, See system requirements document

The ***Blackbaud NetCommunity*** application, BBAppfx web service, and PluginService must be able to access the Blackbaud database.

Role Based Security

The database contains a role named BBWebPortalRole, which has been assigned a minimum set of permissions. The applications that access the database must be configured to connect as a user that is a member of this role.

Authentication

The ***Blackbaud NetCommunity*** server default installation creates a SQL Server authentication login named "BBPortalWebUser" and requests a password for this user on your SQL Server instance. The installation updates all the appropriate web.configs of all services that access the Blackbaud database with the new password.

Blackbaud Database Configuration Checklist
[ ] SQL Server is required, See system requirements document
[ ] Verify the database is isolated from the Internet by a firewall and, optionally, from a DMZ by a secondary firewall.
If you are not using the ***Blackbaud NetCommunity*** installation:
[ ] Change BBWebPortalUser password (and update web.config in dependent services).

The Raiser's Edge Database

Service Type

- SQL Server or Oracle Database; See systems requirements document for ***The Raiser's Edge***

Accessible From

- RE7Service Web Service
- ***The Raiser's Edge*** Client Application

Needs Access To

- N/A

Deployment Considerations

The RE7Service web service is the only service that needs a direct connection to the database. The database does not need to be visible to the ***Blackbaud NetCommunity*** web application or any of the other web services.

RE7Service Web Service/BBAppfx Web Service

Service Type

- ASP.Net Web Service

Accessible From

- Portal Web Application
- NetCommunity WS
- Plugin Service WS

Needs Access To

- RE7 Database (***The Raiser's Edge***)
- Blackbaud Database (***Blackbaud CRM*** and ***Blackbaud NetCommunity***)

Deployment Considerations for The Raiser's Edge

The RE7Service acts as a web service facade to ***The Raiser's Edge*** API and is accessible over HTTP. You must install the RE7Service web service on a machine that has ***The Raiser's Edge*** client installed and properly configured to connect to the database in ***The Raiser's Edge***. Because this service must access ***The Raiser's Edge*** database, we recommend you install it on a distinct machine on the intranet side of a DMZ.

To secure this service from Internet users, you can install the RE7Service web service on a web server that is not visible to the public Internet. If that is not possible, you can configure the site to use a port other than port 80, then configure the firewall accordingly. The site can also be configured to disallow anonymous access. To further enforce this, configure the IIS virtual directory to allow access from only the necessary IP addresses (***Blackbaud NetCommunity*** web servers, services servers, and ***The Raiser's Edge*** workstations).

Even if RE7Service web service is installed on a machine on the intranet side of the DMZ, access to this service should still be limited. This can be done either with firewall policy or via IIS IP Address security or IPSec.

As a final gatekeeper to this service, there is a web.config setting that lists valid username/password pairs for the service. Any consumer of this service has to supply a username and password that match an entry in this list. For example, the following setting:

<add key="RE7ServiceUsers"

value="UserName1\UserPassword1,UserName2\UserPassword2" />

This means users UserName1 and UserName2 can access this service if they supply the appropriate password. Note that these user names have no relationship to any Windows or Community server identities. They are simply customer-defined strings.

Connectivity Requirements Between The Raiser's Edge Web Service Server and The Raiser's Edge SQL Database Server

To ensure maximum performance when ***Blackbaud NetCommunity*** connects to ***The Raiser's Edge*** with ***The Raiser's Edge*** Web Service, Blackbaud requires that ***The Raiser's Edge*** Web Service server and ***The Raiser's Edge*** SQL database server are located on the same network. When ping response times between the two systems exceed double digits in milliseconds, performance degrades for most operations.

Deployment Considerations for Blackbaud CRM

BBAppfx service, which is part of the Blackbaud Core Components, acts as a web service facade to ***Blackbaud CRM*** API and is accessible over HTTP. You must install this service on the same server as ***Blackbaud CRM***.

To secure this service from Internet users, you can install the service on a web server that is not visible to the public Internet. If that is not possible, you can configure the site to use a port other than port 80, then configure the firewall accordingly. The site can also be configured to disallow anonymous access. To further enforce this, configure the IIS virtual directory to allow access from only the necessary IP addresses (***Blackbaud NetCommunity*** web servers, services servers, and ***Blackbaud CRM*** workstations).

If BBAppfx is installed on a server on the intranet side of the DMZ, access to this service should still be limited. This can be done either with firewall policy or via IIS IP Address security or IPSec.

As a final gatekeeper to this service, there is a web.config setting that lists valid username/password pairs for the service. Any consumer of this service has to supply a username and password that match an entry in this list. For example, the following setting:

<add key="RE7ServiceUsers"

value="UserName1\UserPassword1,UserName2\UserPassword2" />

This means users UserName1 and UserName2 can access this service if they supply the appropriate password. Note that these user names have no relationship to any Windows or Community server identities. They are simply customer-defined strings.

Windows Server Considerations

To ease security configuration and enhance stability when deploying the RE7Service web service (***The Raiser's Edge***) or BBAppfx web service (Blackbaud Core Components) on Windows Server OS, you may want to take advantage of the application pool feature.

You can establish a separate application pool and configure it to run as a specific identity. For example, to simplify giving all the permissions required to create COM objects in ***The Raiser's Edge*** or ***Blackbaud CRM***, you can give the application pool the identity of "Local System". You receive a warning, but since the RE7Service or BBAppfx web service is secured from the public Internet, this should not be a problem.

In addition, to enhance stability, you may want to enable process recycling or run the pool as a "web garden." The RE7Service web service uses API components in ***The Raiser's Edge*** and certain Microsoft components such as the Jet/DAO components, while the BBAppfx web service uses the ***Blackbaud CRM*** API as well as certain Microsoft components. The application pool feature allows robust availability of the service used by your configuration, even in the face of bugs or memory leaks in the code or dependencies of the application.

Lastly, configure ***The Raiser's Edge*** or ***Blackbaud CRM*** to check for a deployment package locally. If either program checks for the deployment package on a network location that is not accessible

without authentication, performance for the ***Blackbaud NetCommunity*** application is degraded when connecting to the program.

RE7Service Web Service Configuration Checklist

[ ] Verify ***The Raiser's Edge*** client application is installed on the same machine and can connect to ***The Raiser's Edge*** (run the RE7.exe client and login).

The following settings are configured by the ***Blackbaud NetCommunity*** installation.

Edit the following <appsettings> in web.config.

- RE7ServiceUsers (USE SOMETHING CUSTOMER SPECIFIC!)

[ ] Secure access to the service via a firewall and/or IIS IP address security. Only the ***Blackbaud NetCommunity*** web application and PluginService WS need to access this service.

[ ] (Optional Windows Server 2003/2008) Configure a specific application pool for use by the service.

[ ] Verify ***The Raiser's Edge*** is searching for a local deployment package.

BBAppfx Web Service Configuration Checklist

[ ] Log into ***Blackbaud CRM***.

The following settings are configured by the ***Blackbaud NetCommunity*** installation.

Edit the following <appsettings> in web.config.

- RE7ServiceUsers (USE SOMETHING CUSTOMER SPECIFIC!)

[ ] Secure access to the service via a firewall and/or IIS IP address security. Only the ***Blackbaud NetCommunity*** web application and PluginService WS need to access this service.

[ ] (Optional Windows Server 2003/2008) Configure a specific application pool for use by the service.

[ ] Verify ***Blackbaud CRM*** is searching for a local deployment package.

Plugin Service WS

Service Type

- ASP.Net Web Service

Accessible From

- ***The Raiser's Edge*** Client Application or ***Blackbaud CRM***

Needs Access To

- Blackbaud Database, or
- ***The Raiser's Edge*** Database

Deployment Considerations

The PluginService web service provides access to data contained in the database, for example, donations and event registrations that have been processed on the web in ***Blackbaud NetCommunity*** but have not yet been imported into ***The Raiser's Edge*** or Blackbaud database.

The Plugin Service WS does not need to be accessed from the Internet. It only needs to be accessed from ***The Raiser's Edge*** client application or ***Blackbaud CRM***. Therefore, this service should not be visible to the Internet. It can be secured by firewall policy or IIS IP security. In addition, if the server it runs on can communicate with a domain controller, the virtual directory can be configured to disallow anonymous access and allow only Windows Authentication. In this case, the web.config can be edited to allow only specific users to access the service. For example, the following limits the users to those that are a member of the group "paulgi\PluginUsers":

(in the system.web section)

<authentication mode="Windows"/>

<identity impersonate="true"/>

<authorization>

<allow roles="paulgi\PluginUsers"/>

<deny users="*" />

</authorization>

The PluginService accesses the Blackbaud database and the RE7Service web service (***The Raiser's Edge***) or BBAppfx web service (Blackbaud Core Components).

Plugin Service WS Configuration Checklist
[ ] Secure the virtual directory from the Internet via firewall.
[ ] Configure the virtual directory to disallow anonymous access and edit web.config to restrict access to members of a specific NT security group.
During the installation, the ConnectionString <appsettings> in web.config is updated.

Performance and Custom Configuration Related Settings

Blackbaud NetCommunity Web Server

Cache Settings

To minimise calls to the database and web services (WS), cache settings on the Configuration page in *Administration* place objects in memory. These settings leverage the .NET cache by setting a sliding expiration. If an object, such as a constituent in ***The Raiser's Edge*** or ***Blackbaud CRM***, is placed in cache and not accessed for the set value of minutes, the object is removed unless the application code, such as Fundraiser Synchronize, is executed beforehand. The following is the list of currently supported key/value pairs.

Note: If these settings are not present in the configuration file, the .NET default for the application cache (20 minutes) is used.

To meet the needs of the customer site(s), these fields in the Cache frame on the Configuration page can be configured.

- **Application (minutes)** – This is used for any object that is placed in the cache while the application is running and for which there is no overriding value below.
- **Event Items (minutes)** – ***The Raiser's Edge*** Event Management module fetched via the RE7Service web service or ***Blackbaud CRM*** Events data fetched via the BBAppfx web service.
- **Code Tables (minutes)** – ***The Raiser's Edge*** code tables and table entries fetched via the RE7Service web service or ***Blackbaud CRM*** code tables and table entries data fetched via the BBAppfx web service.
- **NewsReader (minutes)** – RSS or Atom content retrieved for the News Reader part.
- **NewsFeed (minutes)** – RSS content created by the Weblog part in the ***Blackbaud NetCommunity*** web application.
- **Enable database cache monitoring** – If the client site uses multiple web servers, mark this checkbox to enable the database cache monitor to ensure each server's cache is properly maintained.

Role Refresh Settings

For information about the role refresh functionality and behavior, see the "Role Refresh" section of the ***Blackbaud NetCommunity*** help file. To meet the needs of the customer site(s), these fields in the Role Refresh frame on the Configuration page can be configured.

- **Frequency** – the interval to lapse between the role refresh processes. You can select to never run a role refresh process, enter an interval to lapse between the end of one role refresh process and the beginning of the next, or schedule the process to run once at a specific time each day.
- **Log Directory** – the location of the log that records role refresh data
- **Log Level** – the level of detail recorded in the log

Custom Error Code Settings

By default, ***Blackbaud NetCommunity*** is installed with CustomErrors=RemoteOnly. Therefore, website users see a simple error message. Only users running locally see the rich error information that provides a stack trace.

NetCommunity web.config key:

<customErrors mode="On"/>

Setting optons:

- **RemoteOnly** – Custom error pages are shown for all remote users. ASP.NET error pages with rich error information are displayed only for local users.
- **On** – Custom error pages are always shown, unless one is not specified. When a custom error page is not defined, an ASP.NET error page will be displayed which describes how to enable remote viewing of errors.
- **Off** – Custom error pages are not shown. Instead, ASP.NET error pages will be displayed always, which will have rich error information.

Maximum File Upload Size and Website Timeout Settings

By default, the maximum file upload size setting is 4 MB (4096 KB). This is applicable for an HTTP Runtime request, such as a Fundraiser Synchronize or Directory search, or an uploaded document, such as for the Document part or an imported email list. To increase this setting, you can adjust the web.config file.

In the system.web section, add or adjust the maxRequestLength key in the <httpRuntime> element. To increase the maximum number of seconds a request can execute, such as for very large files, you can also adjust the executionTimeout key. If you receive an HTTP Runtime error in the event log, increase these settings until you no longer receive the error. For example, the following increases the maximum file upload size to 16384 KB and the timeout setting to 1 hour (3600 seconds).

(in the system.web section)

<httpRuntime useFullyQualifiedRedirectUrl="true" executionTimeout="3600" maxRequestLength="16384" />

Before you maximise the file size or website timeout settings, review the Microsoft Knowledgebase article at http://support.microsoft.com/?id=295626.

Certificate Domain Setting for Multiple Web Addresses

If you use multiple URLs for your website but purchase an SSL certificate for only one, your website users can experience errors when they access secured pages through the web addresses not associated with the certificate. To prevent these errors, you can add the CertificateDomain key in the appSettings section to redirect website users to the URL associated with the SSL certificate regardless of the web address they use to access your website. For example, the following directs website users to www.mydomain.org when they use another URL associated with the website.

(in the appSettings section)

<add key="CertificateDomain" value="www.mydomain.org">

Note: If the user accesses your website through an IP address, the redirect does not occur.

Timeout Settings

By default, the timeout settings for calls to the RE7Service web service (***The Raiser's Edge***) or BBAppfx web service (Blackbaud Core Components) are 15 seconds. To increase these settings, you can pass along a querystring parameter to the testconfig.

The RE7Timeout querystring parameter indicates the timeout setting, in milliseconds, for the call to the RE7Service or BBAppfx web service. For example, this querystring parameter increases the timeout setting to 45000 milliseconds (45 seconds): https://www.yourdomain.com/NETCOMMUNITY/testconfig.aspx?RE7Timeout=45000.

You can also specify the timeout setting for the call to the Blackbaud Services, such as to process email. The BBSvcTimeout querystring parameter indicates this timeout setting in milliseconds. For example, this querystring parameter increases both the timeout settings for the RE7Service or BBAppfx web service and the Blackbaud Services to 45000 milliseconds (45 seconds) each:

https://www.yourdomain.com/NETCOMMUNITY/testconfig.aspx?RE7Timeout=45000&BBSvcTimeout=45000.