

***Bravura Security Fabric* Implementation:**

Pre-Installation

This document contains:

- [Network components](#)
- [Platform](#)
- [Primary server requirements](#)
- [Installing Python](#)
- [Support for virtual machines](#)
- [Domain requirements](#)
- [Database server](#)
- [Replicated server requirements](#)
- [Proxy servers](#)
- [Cryptographic certificates](#)
- [Browser support](#)

1 Network components

This section provides an overview of software components, on various servers throughout the network, of a *Hitachi ID Bravura Security Fabric* installation. This includes:

- [Core server components](#)
- [Optional local agents and services](#)

This section also shows you how to [calculate the number of servers required \(p3\)](#).



1.1 Core server components

Table 1: Core server components

Component	Description
Database server	<p>Stores and manages <i>Hitachi ID Bravura Security Fabric</i> data.</p> <p>The location of the software depends on the third-party database management system (DBMS) that you are using. You will also need to install database client software on the <i>Bravura Security Fabric</i> server. For Microsoft SQL Server, it is recommended that you install the database on Windows Server 2012 R2, 2016 or 2019.</p>
<i>Bravura Security Fabric</i> server	<p>Provides web access (the GUI), core functionality, and essential services.</p> <p>The software is installed on a Windows-based server. It is recommended that you install on three or more replicated servers.</p>
<i>Hitachi ID Connector Pack</i>	<p>Facilitates communication between the <i>Bravura Security Fabric</i> server and the target systems.</p> <p>The connectors are installed on the <i>Bravura Security Fabric</i> server, as well as all replicated servers. They must also be installed on any proxy servers that are utilized by the <i>Bravura Security Fabric</i> server. For installation details see the Connector Pack Integration Guide.</p>
Optional	
<i>Bravura Security Fabric</i> proxy server	<p>Fulfills requests on behalf of the <i>Bravura Security Fabric</i> server. The proxy service is useful for securing connections or accessing client software.</p> <p>This optional software is installed on a Windows-based server.</p>
Mobile Proxy Service (mobproxy)	<p>This server runs on the Hitachi ID Bravura One proxy server and communicates with the Mobile Worker Service (mobworker) to allow the Hitachi ID Bravura One App on mobile devices to access <i>Bravura Security Fabric</i> servers.</p> <p>This optional software is installed on a Linux-based server. For installation details see the Hitachi ID Bravura One Configuration Guide.</p>

1.2 Optional local agents and services

Table 2: Optional local agents and services

Component	Description
 Hitachi ID Password Change Notification Module	<p>When <i>Bravura Pass</i> is licensed, intercepts native password changes and propagates them to the <i>Hitachi ID Bravura Security Fabric</i> server for policy validation and to initiate transparent password synchronization.</p> <p>The Interceptor DLL can be installed on a Windows 201x domain controller.</p>
 Privileged Access Manager Local Workstation Service (hipamlws)	<p>Manages local password resets for <i>Hitachi ID Bravura Privilege</i>, secures communication between <i>Bravura Privilege</i> server and the managed resource, and provides load balancing.</p> <p>The software is installed on Windows resources.</p>

... continued on next page

Table 2: Optional local agents and services (Continued)

Component	Description
IBM OS/400 exit program	Intercepts password changes on OS/400 and propagates them to the <i>Hitachi ID Bravura Pass</i> server for policy validation and to initiate transparent synchronization.
Unix listener	Secures communication between the <i>Bravura Security Fabric</i> server and a Unix server when a secure protocol, such as SSH, is not available. The software is installed on supported flavors of Unix. For details see the Unix / Linux Integration Guide (unix-linux.pdf).
Mainframe Connector	Secures communication between the <i>Bravura Security Fabric</i> server and OS/390 mainframes. The software is installed on the OS/390. This component is sold separately from <i>Bravura Security Fabric</i> and is available as a separate download. Contact support@Hitachi-ID.com for details.

1.3 Calculating the number of servers required

Hitachi ID Systems *strongly* recommends that you create at least two or three replicated *Hitachi ID Bravura Security Fabric* database nodes for fault tolerance and backup, depending on which products are licensed and which features are implemented. When *Hitachi ID Bravura Privilege* is installed, or when close to 100% uptime is required from the instance, the recommended minimum is three. This is because when backend database replication is performed, at least two database nodes have to go down at the same time.

On the other hand, avoid setting up too many replicated database nodes. It is likely that the additional overhead of any more than six fully replicated nodes would outweigh the advantage of having multiple nodes to do work. If you implement transparent password synchronization, it is recommended that you avoid having more than five concurrently active database nodes.

Calculate the number of database nodes you require with the following formula:

$$N = \text{ceil}(1 + [U/P * 7/5/Z * A]/[60 * 60 * C/T])$$

Where:

U = # of users

P = days between password expiry

Z = time zones

A = accounts/user

C = # of concurrently running connectors

T = seconds on average to change a password

For example, when:

U = 10000 people

P = 45 days

Z = 1 time zone

A = 10 accounts/user

C = 30 connectors at a time

T = 2 seconds

then:

$$N = \text{ceil}(1 + [10000/45 * 7/5/1 * 10]/[60 * 60 * 30/2])$$

$$N = \text{ceil}(1 + [3111]/[54000])$$

$$N = \text{ceil}(1.0576)$$

$$N = 2$$

See also:

- [Installing with a shared schema](#)
- [Configuring Replicated Servers](#)

2 Platform

The *Hitachi ID Bravura Security Fabric* server and any replicated servers must be installed on a Windows Server operating system. Windows 2016 is recommended at the current release level of *Bravura Security Fabric*, and will be mandatory in the next major release.

Installing on Windows Server enables *Bravura Security Fabric* to leverage client software that is available only on the “Wintel” platform. In turn, this makes it possible for *Bravura Security Fabric* to manage passwords and accounts on target systems without installing a server-side agent.

Bravura Security Fabric stores all of its data in an *external database*. The database and its corresponding client software must be installed and configured before the *Bravura Security Fabric* server software can be installed.

If you are installing the *Bravura Security Fabric* on the same server as the database, ensure you take into consideration the server requirements for the database software when calculating the requirements for the *Bravura Security Fabric* server.

Each *Bravura Security Fabric* application server must also be configured with a web server. The *Bravura Security Fabric* installer is aware of and can automatically configure IIS web servers for use with *Bravura Security Fabric*.

The *Bravura Security Fabric* server is a security server, and should be locked down accordingly. See Locking Down a *Bravura Security Fabric* Server ([**server-hardening.pdf**](#)) for more information.

Bravura Security Fabric servers to learn how to do this. In short, most of the native Windows services can and should be removed, leaving a very small attack surface, with exactly one inbound TCP/IP port (443):

1. No ASP, JSP or PHP are used, so such code interpreters should be disabled.
2. Web-facing .NET is not used and should be disabled (some connectors require it, due to .NET API bindings).
3. No ODBC or DCOM are required inbound, so these services should be filtered or disabled at the web server. As with .NET, ODBC is sometimes needed to connect to target systems.
4. Inbound file sharing should be disabled.
5. Remote registry services should be disabled.
6. Inbound TCP/IP connections should be firewalled, allowing only port 443, remote desktop services (to configure the software) and a handful of ports between *Bravura Security Fabric* servers, mainly for data replication.

Each *Bravura Security Fabric* server requires a database instance. Microsoft SQL 2016 is the recommended choice. Microsoft SQL 2014 and 2012 are also supported. Oracle database was supported on versions up to 9.0.x and is *not* supported on 10.0 or later releases.

Bravura Security Fabric is compatible with 64-bit Windows Servers:

1. The core software is compiled as 64-bit binaries.
2. Components that execute in the context of the core OS, such as password synchronization triggers, event hooks, etc. are available in both 64- and 32-bit versions for compatibility.

3 Primary server requirements

Each *Hitachi ID Bravura Security Fabric* server is configured as follows:

☐ **Hardware requirements:**

- ☐ Intel Xeon or similar CPU. Multi-core CPUs are supported and leveraged. Dual core is a minimum.
- ☐ At least 16GB RAM – 32GB or more is leveraged and is typical for a server.
- ☐ At least 600GB of HD storage, preferably in an enterprise RAID configuration for reliability and preferably larger for retention of more historical and log data.
More space is always better, to increase log retention.
- ☐ At least one Gigabit Ethernet NIC.

Ensure you take into consideration the hardware requirements of any other software that may share the *Bravura Security Fabric* server; for example, database storage requirements.

See [Support for virtual machines](#) for more information about support for virtual machines.

☐ **Operating system:**

- ☐ Windows Server 2012 R2.
- ☐ Windows Server 2016.
- ☐ Windows Server 2019.

It is recommended that the server is not a domain controller.

In addition to the above editions, core mode on Server 2012 R2 and Server 2016 is also supported.

☐ **Networking:**

- ☐ TCP/IP networking, with a static IP address and DNS name entry
- ☐ Cryptographic certificate
- ☐ Microsoft .NET Framework 3.5 and 4.5+
- ☐ Web Service Enhancements (WSE) 2.0 SP3 for Microsoft .NET
- ☐ Web server (IIS) with the following:

- * HTTP redirection
- * The IIS URL Rewrite module from:
<http://www.iis.net/downloads/microsoft/url-rewrite>
- * CGI
- * Dynamic Compression
- * Static Compression

Modified in
version 10.1.0

☐ **Database / connectivity software:**

- A Microsoft SQL Server 2016 (recommended), 2014 or 2012 instance is required to host the *Bravura Security Fabric* schema:
 - Normally one database instance per application server.
 - The SQL Server database software can be deployed on the same server as the *Bravura Security Fabric* application, as this reduces hardware cost and allows application administrators full DBA access for troubleshooting and performance tuning purposes. See [Where to install the software](#) for more information.
 - If the database software is deployed on a separate server, it is recommended that you install the client software that corresponds to the database backend.

See the “Installing Database Software” ([sql-server.pdf](#)) task doc or the [Bravura Security Fabric Documentation](#) for details.

□ **Hitachi ID Connector Pack:**

- The *Connector Pack* contains connectors which integrate *Bravura Security Fabric* with target systems.
 - It is recommended, but not required, that you install the *Connector Pack* after the *Bravura Security Fabric*. This allows you to select instance-specific or global installation.
- See the Connector Pack Integration Guide for details.

□ **Installed and tested software:**

- Native clients for the systems that *Bravura Security Fabric* will interface with
Refer to the Connector Pack Integration Guide for information specific to each type of target system.
- Python 3.7.3+

Note: Python 3.7.3+ *must* be installed before installing *Bravura Security Fabric* or *Connector Pack*. It is required for certain *Bravura Security Fabric* components, including the Python IDMLib library used to help create plugin programs, Health check monitor, and reference builds.

Ensure that Python is installed for all users to allow the *Bravura Security Fabric* service user (psadmin) account to have appropriate access to the Python installation.

Note: It is recommended to add Python to the system PATH. This may also be added by selecting the option for “Add Python 3.7 to PATH” during the Python installation.

Note: Python 3.8.x or later is *not* currently supported.

See [Installing Python](#) to learn how to install Python to meet these requirements.

- Microsoft Visual C++ 2015 Redistributable (x64)
Microsoft Visual C++ 2015 Redistributable Package (x64) is required for *Bravura Security Fabric* 10.0 and higher. It is required for certain *Bravura Security Fabric* run-time components that use Visual C++ libraries. This is automatically installed during **setup**, if prerequisites are met.

Note: The installer checks prerequisites for C++ runtime and universal CRT. Before these two can be installed, the system requires the KB2919355 update (this is a set of patches, which has to be installed in order by clearcompressionflag.exe, KB2932046, KB2959977, KB2937592, KB2938439, KB2934018). KB2938439 must be patched before KB2919355 can be patched. During the installation of patches, if a Windows dialog box displays the message: "The update is not applicable to your computer" and you are sure that you installed the patch that matches your operating system, it is likely that there are other prerequisites that need to be installed before the current patch.

- ☐ At least one web browser (such as Chrome), and PDF viewer (to read the documentation)
- ☐ A Git client (for revision control)

4 Installing Python

Python 3.7.3+ *must* be installed before installing *Hitachi ID Bravura Security Fabric* or *Hitachi ID Connector Pack*. It is required for certain *Bravura Security Fabric* components, including the Python IDMLib library used to help create plugin programs, Health check monitor, and reference builds.

Ensure that you install the 64-bit version of Python.

Ensure that Python is installed for all users to allow the *Bravura Security Fabric* service user (psadmin) account to have appropriate access to the Python installation.

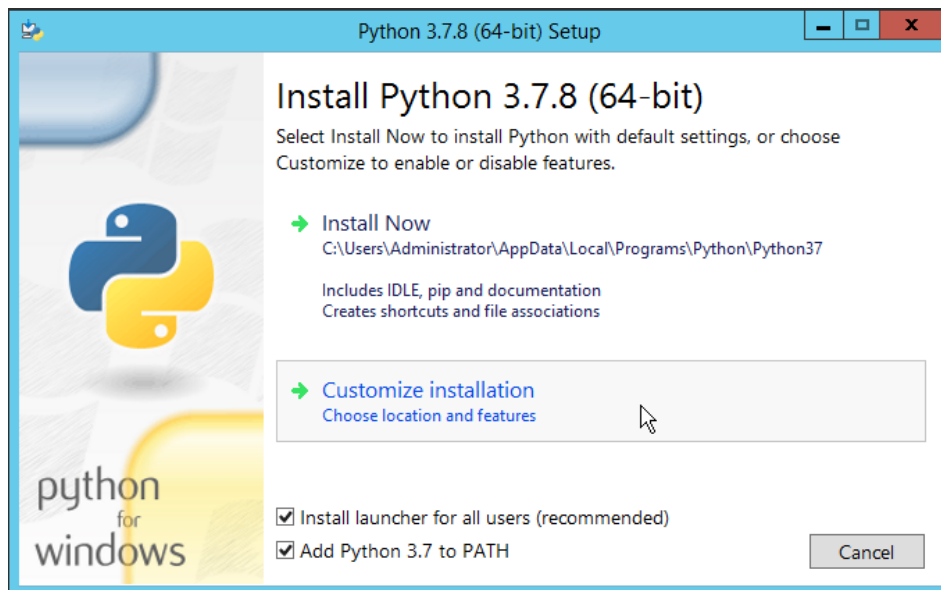
Note: Python 3.8.x or later is *not* currently supported.

To install Python 3.7.3+:

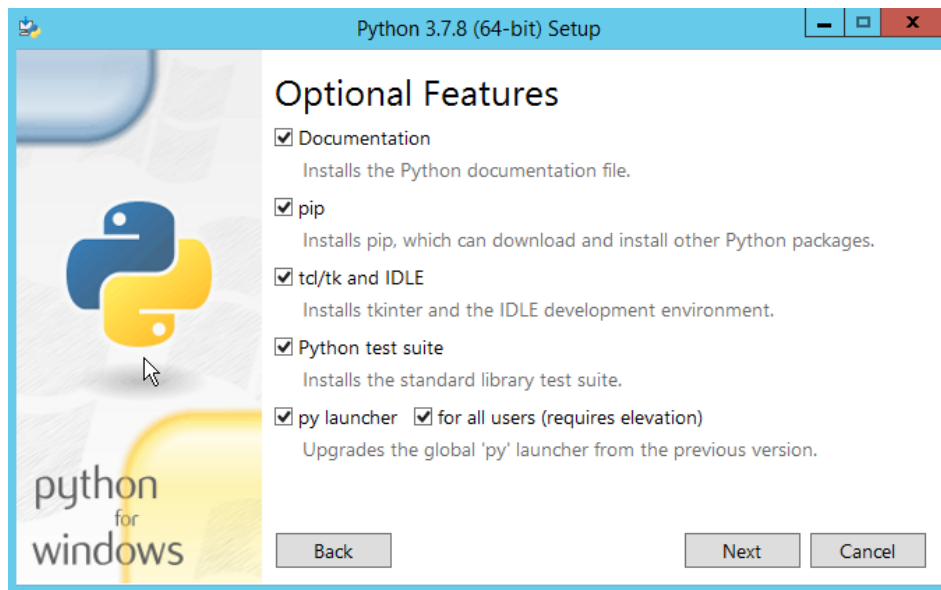
1. Download and run the 64-bit installer from python.org.
2. On the first screen, check the **Add Python 3.7 to PATH** option.



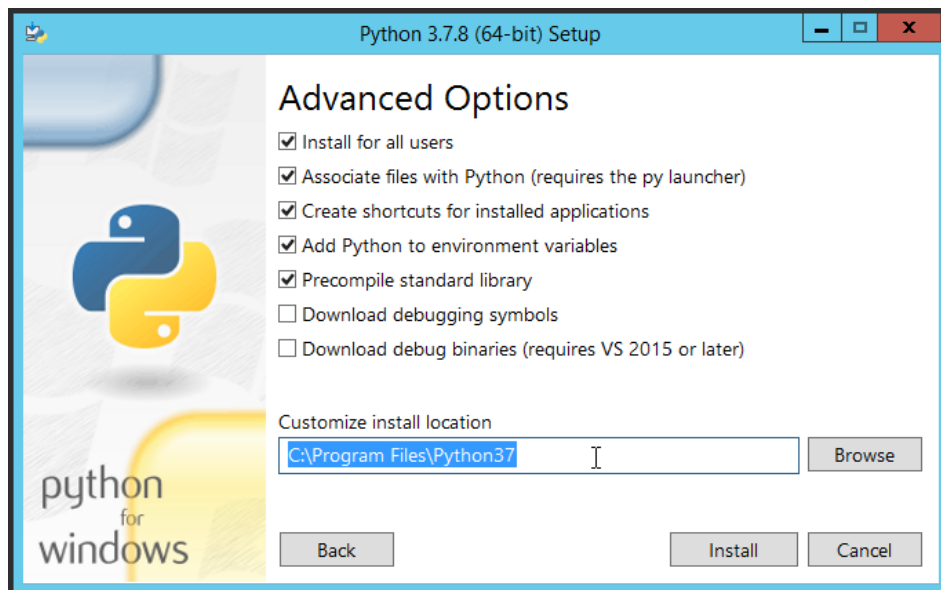
3. Click **Custom** installation.



4. Use all **Optional Features**.



5. On the **Advanced Options** screen, select **Install for all users**, and ensure that the path is correct in the **Custom install location**.



6. Click **Install**.

5 Support for virtual machines

Hitachi ID Bravura Security Fabric is compatible with VMware, Xen Project, Microsoft Hyper-V and Oracle VirtualBox virtual machine platforms. It can also be deployed on IaaS, including AWS. It generally works well with other virtualization platforms, but Hitachi ID Systems primarily tests with these. Hitachi ID Systems officially supports running *Bravura Security Fabric* on these virtual servers and will make a best effort to support customers who run on other hypervisors.

So long as the database server that hosts the *Bravura Security Fabric* back-end has access to reasonably fast I/O (e.g., NAS or similar) and so long as connectivity between the *Bravura Security Fabric* application sever and the database is fast and low latency (e.g., 1Gbps/1ms) there should be no adverse performance impact when comparing *Bravura Security Fabric* installed on hardware vs. *Bravura Security Fabric* installed on a similarly-equipped virtual server.

The key point above is to ensure sufficient I/O capacity for the database (MSSQL). If the database server is virtualized, using network attached storage (NAS) is recommended, as virtualized I/O (files such as VMDK's emulating an HDD image) is often substantially slower than physical I/O.

Even where customers choose to deploy the main *Bravura Security Fabric* servers on raw hardware, virtual machines are an excellent platform for proxy servers, test servers, development servers and model PCs.

A related question is often “how large can the deployment get before we have to move from a VM to hardware?” Unfortunately, there is no simple, universal answer:

1. Virtual servers vary in capabilities – they may have a 32-bit or a 64-bit CPU, may have 1, 2, 4 or 8 CPU cores allocated, may have different amounts of memory and may link to different types of storage infrastructure.
2. The load created by the application also varies – is there complex business logic? Do users access the application at random times or all at once? Are there just a few or thousands of integrations?

This variability means that the safest bet is to use benchmark results, using a configuration as similar as possible to the production setup, to gauge the performance of *Bravura Security Fabric* on representative physical and virtual servers.

As a general standard, the ratio of vCPU to CPU (core) is 3:1. Therefore the actual vCPU performance will be 33% of the actual CPU. If the *Bravura Security Fabric* is deployed in a virtualized environment, and the general ratio on the hypervisor is 3:1, then a virtualized setup would require 6vCPU to match the minimal 2 CPU physical CPU requirement.

6 Domain requirements

While *Hitachi ID Bravura Security Fabric* servers are capable of operating as domain members, we suggest you take the following into consideration:

- Security / limited accessibility:

If the *Bravura Security Fabric* server is part of the domain, then other administrative users from the domain (who may not be *Bravura Security Fabric* administrators) can gain administrative logon access to the server and can then access (encrypted) credentials for target systems other than the domain.

A policy of segregation of duties suggests that it is preferable to eliminate the ability of administrators of one system to access privileged accounts for another system and since *Bravura Security Fabric* houses such credentials, it makes sense to avoid domain membership.

- Secure service account:

Bravura Security Fabric requires a service account which *Bravura Security Fabric* services will run as. It is recommended to restrict the service account's abilities to interactively log on to networks when a domain account is used. This is a recognized industry best-practice and it can be configured by using group policy.

See [Creating a secure service account](#) for more details.

- Windows credential conflicts:

To change/verify passwords on an Active Directory domain, *Bravura Security Fabric* uses ADSI, which may connect a named pipe to a share on a domain controller, such as the NETLOGON share.

If an administrative user logs into the *Bravura Security Fabric* server console and makes a similar connection but using his personal credentials (not those encoded into *Bravura Security Fabric*), then the Windows network provider may produce a credential conflict error. This can interrupt *Bravura Security Fabric*'s ability to manage user objects on the domain, for the duration of the interactive login session.

If *Bravura Security Fabric* is not a domain member, then the set of administrators who are able to inadvertently cause this error condition is significantly reduced and so *Bravura Security Fabric* operation is more reliable (less prone to human-induced errors).

- Password randomization

Credential problems can also occur if the *Hitachi ID Bravura Privilege* server is also a Domain Controller, and *Bravura Privilege* is used to manage the administrator account used to target the system. When the administrator account has its password randomized, the target system administrator credentials may not be updated.

6.1 Creating a secure service account

The following steps for creating a secure service account are demonstrated on Windows 2019 server:

1. Launch **Active Directory Users and Computers**.
2. Create an OU.

3. In the OU, create an account as the service account as well as a security group.
4. Add the service account as a member of the security group.
5. Launch **Group Policy Management Console (GPMC)**.
6. Create a new group policy.
7. Right click on the group policy, then click on **Edit...** to launch **Group Policy Management Editor**, configure the group policy with following settings:
 - Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **User Rights Assignments**
 - Select **Deny log on locally** and enter the security group created previously.
 - Select **Deny log on through remote desktop services** and enter the security group created previously.
 - Exit from **Group Policy Management Editor**.
8. Back to **Group Policy Management Console (GPMC)**, click on **Scope** tab to ensure the GPO is set to authenticated users.
9. Link the GPO to any OUs containing machines which you want to stop the service account from being able to log on to interactively, or the domain level for all machines.
10. If you have more than one domain, you can put groups from the trusted domain in the GPO. However, you might want to make a GPO like this on both sides (in case of two-way trusts).
11. Reboot or run command "gpupdate.exe /force" on the machines to apply the GPO.
12. Test to ensure the service account is not allowed to log on the machines where the GPO is applied.

7 Database server

Hitachi ID Bravura Security Fabric requires MS SQL Server 2019 or 2016, typically with one database instance per application server. In most environments, the Microsoft SQL Server software is installed on the same hardware or VM as the *Bravura Security Fabric* software, on each *Bravura Security Fabric* server node. This reduces hardware cost, eliminates network latency and reduces the security surface of the combined solution.

Be sure to install the following components that come with Microsoft SQL Server 2019 and 2016:

- Database Engine Services
- Client Tools Connectivity
- Management Tools - Basic
- Management Tools - Complete

Database I/O performance on a virtualized filesystem (e.g., VMDK or equivalent) is slow. If the database server software runs on a VM, please use a fast, nearby NAS or SAN to store the actual data files.

Bravura Security Fabric can leverage an existing database server cluster, but Hitachi ID Systems recommends a dedicated database server instance, preferably one per *Bravura Security Fabric* application server, installed on the same OS image as the core application.

1. The data managed by *Bravura Security Fabric* is extremely sensitive, so it is desirable to minimize the number of DBAs who can access it (despite use of encryption).
2. SQL Server has limited features to isolate workloads between database instances on the same server. This means that a burst of activity from *Bravura Security Fabric* (as happens during auto-discovery) would cause slow responses in other applications. Conversely, other applications experiencing high DB load would slow down *Bravura Security Fabric*.
3. *Bravura Security Fabric* already includes real-time, fault-tolerant, WAN-friendly, encrypted database replication between application nodes, each with its own back-end database. Use of an expensive DB server cluster is neither required nor beneficial.
4. Deploying the database to localhost has performance advantages (minimal packet latency from the application to its storage).
5. Allowing *Bravura Security Fabric* administrators full control over the database simplifies performance and related diagnostics and troubleshooting, especially when we consider that database administrators in most organizations are few in number and very busy.
6. Eliminating reliance on shared database infrastructure also eliminates the need to coordinate events such as database version upgrades, which involve reboots. Some Hitachi ID Systems customers who leverage a shared database infrastructure have experienced application disruption due to unscheduled and un-communicated database outages and restarts.

See the “Installing Database Software” ([sql-server.pdf](#)) task doc or the [Bravura Security Fabric Documentation](#) for details.

8 Replicated server requirements

Requirements for replicated servers are the same as for a primary server. Hitachi ID Systems *strongly* recommends that you install at least three replicated *Hitachi ID Bravura Security Fabric* servers for fault tolerance and back up. Configuration of replicated servers is detailed in [Configuring Replicated Servers](#).

All replicated servers must be created with the same instance name. It is recommended that all replicated servers be created with the same *Bravura Security Fabric* license, and use the same type of *Hitachi ID Connector Pack*. All server clocks must be synchronized.

9 Proxy servers

In some cases, the connection to a target system may be slow, insecure or blocked. This may be because the connection spans multiple data centers or uses an insecure network protocol.

To address such connectivity problems, *Hitachi ID Bravura Security Fabric* includes a connector proxy server. When a proxy server is deployed, the main *Bravura Security Fabric* server ceases to make direct connections to some target systems and instead forwards all communication to those systems through one or more connector proxies, which are co-located with the target systems in question.

Communication from the main *Bravura Security Fabric* server to the connector proxy is encrypted and works well even when there is low bandwidth or high packet latency. It uses a single, arbitrarily-numbered TCP port number. Connections are established from the main *Bravura Security Fabric* application server to the proxy server. A single TCP port supports an arbitrarily large number of target systems at the connector proxy's location.

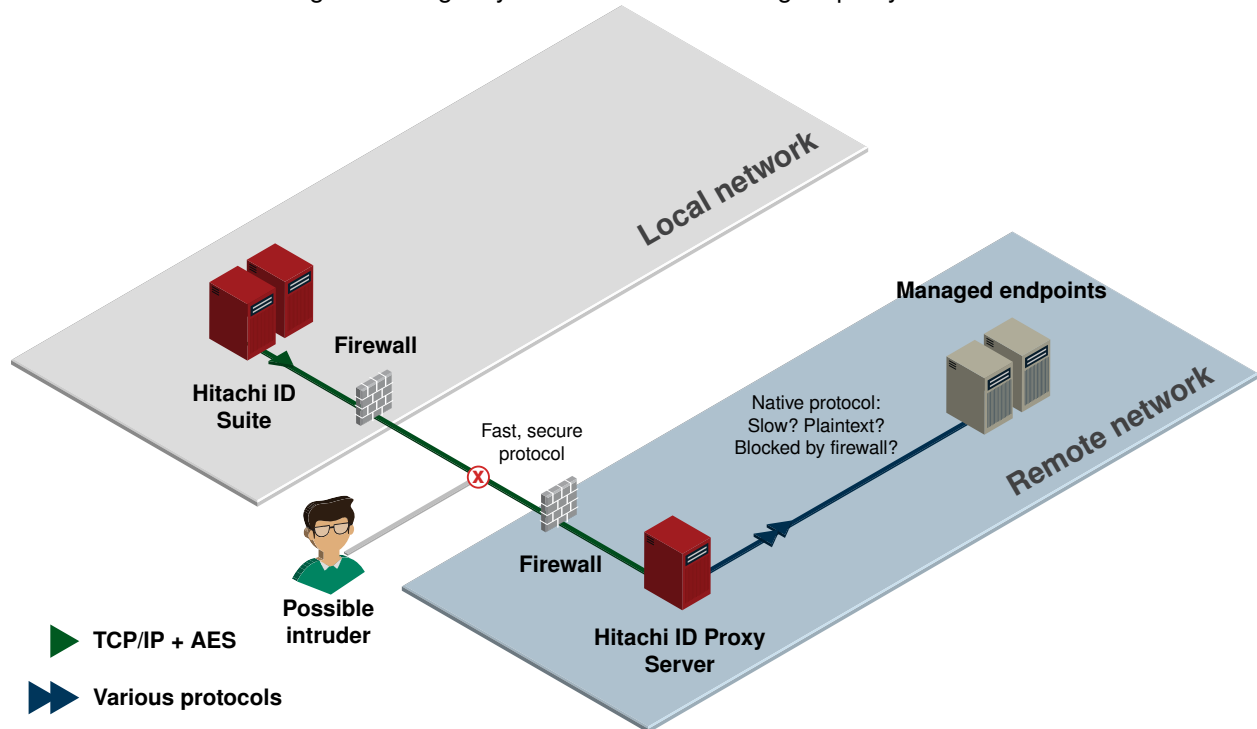
It is simple for firewall administrators to open a single TCP port per proxy server. Since connections are efficient and encrypted, there are usually no objections to doing so.

Communication between the proxy server and target systems continues to use whatever protocol each system supports natively. This communication is confined to a physically secure data center with a high-bandwidth, low-latency local network.

Deployment of the secure *Bravura Security Fabric* proxy server is illustrated in [Figure 1](#).

See the "Proxy Server Management" ([manage-proxy.pdf](#)) task doc or the [Bravura Security Fabric Documentation](#) for more information.

Figure 1: Target systems connected through a proxy server



10 Cryptographic certificates

Hitachi ID Systems strongly recommends that users access *Hitachi ID Bravura Security Fabric* using SSL (HTTPS). To do this:

1. Assign a fixed IP address to each *Bravura Security Fabric* server.
2. Assign a single DNS host name to all *Bravura Security Fabric* servers.
3. Install the web server (IIS)
4. Create a certificate signing request (CSR) file.
5. Submit the CSR file to a certificate authority such as Verisign.
6. Receive and install a signed certificate.

Alternatively, if you have the appropriate software, you can generate a self-signed certificate.

11 Browser support

The following browsers are supported:

- Internet Explorer 11 or later (*recommended*).
- Microsoft Edge.
- Edge Chromium.
- Latest versions of Mozilla Firefox and Google Chrome.

Font downloads must be enabled in the browser to allow *Hitachi ID Bravura Security Fabric* to use Font Awesome.

Some plugins require that you configure ActiveX security.

11.1 HTTPS settings

As of version 12.1.1 *Bravura Security Fabric* adds the "Strict-Transport-Security" header to IIS for all resources. What this means is that if you have configured your site to use SSL and if you have accessed your site using HTTPS protocol, the browser will cache that the site supports HTTPS and prevents the browser from using HTTP. This keeps your site secure but occasionally in testing there will be a need to downgrade the browser security to allow accessing your site via HTTP. In order to do this you must clear the HSTS settings in the browsers.

These links show how to clear the HSTS settings in the browsers:

- <https://www.thesslstore.com/blog/clear-hsts-settings-chrome-firefox/>
- <https://tinsley.net.co.uk/2017/hsts/>

11.2 Configuring ActiveX security

For an ActiveX control to be downloaded and executed by a Internet Explorer or Edge Legacy, the browser must identify and authenticate the ActiveX control, or be configured with a lower security setting to accept unsigned controls (not recommended).

Note: These settings are not required for Edge Chromium, Google Chrome or Firefox.

To allow *Bravura Security Fabric* users' web browsers to safely accept trusted ActiveX controls, your company can obtain and implement a Certificate that enables web servers and users to establish your identity before making a sensitive transaction. Alternatively, you may choose to have the ActiveX control "signed"

by a trusted third-party organization. For more information on Certificates and ActiveX registration, consult your web server documentation, web browser documentation, or on-line authority.

It is recommended that the website for the *Hitachi ID Bravura Security Fabric* server be added to the Trusted Site or Local Intranet zone in Internet Explorer.

11.2.1 Configuring internet options on a workstation

To configure internet options on a workstation:

1. Open Internet Explorer.
2. From the **Tools** → **Internet Options** → **Security** tab, choose the **Trusted sites** or **Local intranet** zone.
3. Click **Custom level**.
4. Ensure that the following ActiveX controls are *enabled*:
 - **Download signed ActiveX controls**
 - **Automatic prompting for ActiveX controls**
 - **Run ActiveX controls and plugins**
 - **Script ActiveX controls marked safe for scripting**
5. Click **Sites** to add the web site for the *Bravura Security Fabric* web server as a trusted site or local intranet site.

Troubleshooting

- If you are prompted with a message to allow/disallow an add-on, try resetting your Internet Explorer security options to default before re-configuring your internet options. Alternatively, selecting allow will refresh the page and require you to login again, but this is only required once for each add-on/plugin.

11.2.2 Using GPOs to globally configure Internet Explorer/ActiveX security settings

You can use Group Policy Objects (GPOs) to globally configure Internet Explorer/ActiveX security settings. To do this:

1. Put the *Hitachi ID Bravura Security Fabric* server in the approved installation sites list, and allow sites to run ActiveX controls.
See [Allowing approved installation sites to run ActiveX controls](#).
2. Put the *Bravura Security Fabric* server in the trusted security zone, and allow trusted sites to run ActiveX controls.
See [Allowing trusted sites to run ActiveX controls](#).

3. Enable automatic download and installation of ActiveX controls provided by trusted sites.
See [Enabling automatic download and installation](#).

Allowing approved installation sites to run ActiveX controls

The following are instructions for Windows 8:

1. Open *Microsoft Management Console* by running `mmc.exe`.
2. Select **File** → **Add/Remove Snap-in...**
3. Select **Group Policy Object...**
4. Click **Add**.
5. In the **Select Group Policy Object** window, browse for a **Group Policy Object** or click **Finish** to accept the default.
6. Click **OK**.
7. In the tree, navigate to **Console Root** → **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **ActiveX Installer Service**.
8. In the right panel, right-click on **Approved Installation Sites for ActiveX Controls** and select **Edit**.
9. Select **Enabled**.
10. Under **Options**, click **Show...**
11. Under **Value name**, enter the server IP address.
12. Under **Value**, enter custom settings or leave blank for default.
13. Click **OK**.
14. Click **OK**.
15. Close *Microsoft Management Console*.

Allowing trusted sites to run ActiveX controls

The following are instructions for Active Directory 2008:

1. Open *Microsoft Management Console* by running `mmc.exe`.
2. Select **File** → **Add/Remove Snap-in...**
3. Select **Group Policy Management Editor** for AD 2008.
4. Click **Add**.
5. In the **Select Group Policy Object** window, browse for a **Group Policy Object** or click **Finish** to accept the default.

6. Click **OK**.
7. In the tree, navigate to **Console Root** → **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Internet Explorer** → **Internet Control Panel** → **Security Page**.
8. In the right panel, double-click to view **Site to Zone Assignment List** properties.
9. Select **Enabled**.
10. Under **Options**, click **Show...**
11. Click **Add ...**
12. Enter a name of the item to be added that matches what was specified as the server address for the *Hitachi ID Bravura Security Fabric* server when the add-on software was installed on workstations; for example, an IP address or DNS name for the server.
13. Enter a value of the item to be added.

This can vary depending on your organization. There are four zones that may be specified:

 - 1 – Intranet zone – sites on your local network
 - 2 – Trusted Sites zone – sites that have been added to your trusted sites
 - 3 – Internet zone – sites that are on the Internet
 - 4 – Restricted Sites zone – sites that have been specifically added to your restricted sites.

The recommended zone to specify is 2 for the Trusted Sites zone.
14. Click **OK**.
15. Click **Apply**.
16. In the tree, navigate to **Security Page** → **Trusted Sites Zone**.
17. Enable the following, by double-clicking in the right panel to open their respective properties page:
 - **Download signed ActiveX controls**
 - **Automatic prompting for ActiveX controls**
 - **Run ActiveX controls and plugins**
 - **Script ActiveX controls marked safe for scripting**

Enabling automatic download and installation

Windows Server 2008

When using a Windows Server 2008 Active Directory, you can use the ActiveX Installer Service to enable automatic download and installation of ActiveX controls for workstations running Windows Vista and newer.

To enable automatic download and installation of ActiveX controls from Windows Server 2008:

1. In the Group Policy Management Editor expand the domain policy → **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **ActiveX Installer Service**

2. Double-click to view Approved Installation Sites for ActiveX Controls

- (a) Select the **Enable** radio button
- (b) Click **Show** to enter the approved sites.
- (c) Click **Add...**
- (d) Enter the DNS or IP address of the *Hitachi ID Bravura Pass* server exactly as it will be entered into the address bar of Internet Explorer by users, or the Credential Provider (including the http:// or https:// prefix in this case).
- (e) Enter the value of the item to be added, in the format N,N,N,N where N is 0, 1 or 2 as defined below.

The value for each Host URL is four settings in CSV format. For maximum security, we recommend a value of 1,1,0,0 (prompt user for initial installation) or 2,2,0,0 (silently install), which represents:

"TPSSignedControl,SignedControl,UnsignedControl,ServerCertificatePolicy".

The three left most values in the policy control the installation of ActiveX controls based on their signature, and can be one of the following values:

- 0 – ActiveX control will not be installed
- 1 – Prompt the user to install ActiveX control
- 2 – ActiveX control will be silently installed Controls signed by certificates in trusted publisher store will be silently installed Silent installation for unsigned controls is not supported

The right most value in the policy is a bitmasked flag The flags are used for ignoring https certificate errors. The default value is 0, which means that the https connections must pass all security checks.

Use the combination of the following values to ignore invalid certificate errors

- 0x00000100 Ignore Unknown CA
- 0x00001000 Ignore invalid CN
- 0x00002000 Ignore invalid certificate date
- 0x00000200 Ignore wrong certificate usage

- (f) Click **OK** when setup finished

3. Double-click to view ActiveX installation policy for sites in Trusted zones

- (a) Select the **Enable** radio button
- (b) The following values are the recommended settings for maximum security:

Setting	Recommended value
Installation Policy for ActiveX control signed by trusted publisher	Prompt the user or Silently install
Installation Policy for signed ActiveX control	Prompt the user or Silently install
Installation Policy for unsigned ActiveX control	Don't install
Unknown certification authority (CA)	Disabled
Invalid certificate name (CN)	Disabled
Expired certificate validation date	Disabled
Wrong certificate usage	Disabled