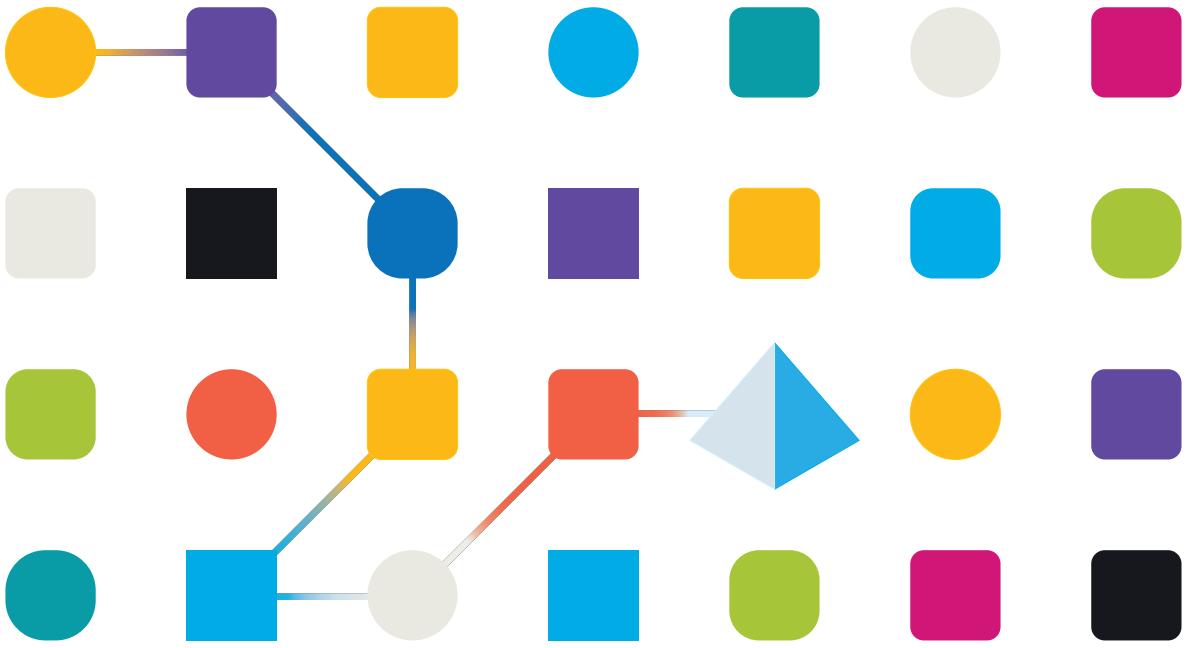
Hub and Interact 4.5

Platform Maintenance Guide

Document Revision: 1.0



Trademarks and Copyright

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: www.blueprism.com

Contents

Blue Prism Platform maintenance overview

This guide provides guidance on maintenance best practices for Blue Prism® Hub and Blue Prism® Interact, including:

- Creating a maintenance plan for SQL database backups
- Backing up the Message Broker Server
- Backing up and restoring the web servers
- Logging

This guide is specific to Blue Prism Hub and Interact. For information about maintaining the Blue Prism Enterprise database, see Maintain a Blue Prism database server.

Intended audience

This guide is intended for experienced database and server administrators.

SQL database maintenance

This information is provided as a guide only. It is recommended that you follow industry standard best practice and seek recommendations from an experienced database administrator. This information should be used with consideration of the wider impact on the overall environment.

The following databases need to be maintained:

- InteractDB
- InteractCacheDB
- IadaDB
- AuthenticationServerDB
- HubDB
- AuditDB
- NotificationCenterDB
- LicenceManagerDB
- EmailServiceDB
- BluePrismDecisionDB
- ImsDB
- FileServiceDB

> CacheDB was replaced with FileServiceDB from Hub 4.4.

General recommendations for database maintenance

It is recommended that you:

- Set auto-growth correctly for all databases. Recommended values are 1024 MB for the data file and 2048 MB for the transaction log.
- Re-establish value for auto-growth as database size increases to minimize the frequency of auto-growth events.

  Do not use % file growth, grow by a fixed amount of megabytes instead.
- Remove any excessive transaction log file fragmentation. For more information, see the Microsoft online help.
- Turn on instant file initialization. For more information, see the Microsoft online help.
- Turn off auto-shrink operations, set the page verification for all databases to checksum, and turn on AUTO_CREATE_STATISTICS and AUTO_UPDATE_STATISTICS. Have a regular process in place to update statistics.

  You can set the following T-SQL for each of the databases installed by Hub and Interact for this purpose:

```
ALTER DATABASE [DatabaseNameHere] SET AUTO_CLOSE OFF;
ALTER DATABASE [DatabaseNameHere] SET AUTO_SHRINK OFF;
ALTER DATABASE [DatabaseNameHere] SET AUTO_UPDATE_STATISTICS ON;
ALTER DATABASE [DatabaseNameHere] SET AUTO_CREATE_STATISTICS ON;
ALTER DATABASE [DatabaseNameHere] SET PAGE_VERIFY CHECKSUM;
```

- Have a regular process to run DBCC CHECKDB – It is recommended that an SQL Agent job is run at a minimum of once per day during periods of little to no system utilization. Results should be checked for corruption. It may be beneficial to create SQL Agent alerts to notify an operator group of the below errors;
  - 823 - Hard I/O Corruption
  - 824 - Soft I/O Corruption
  - 825 - Read/Retry Corruption
  - 9100 - Index Corruption
  - Severity 19-25 Errors
- Optimize for ad-hoc workloads = ON
- Backup compression default = ON
- Backup checksum default = ON
- Cost threshold for parallelism – 50 is a good starting point.
- Max degree of parallelism - Depends on the NUMA configuration of the SQL Server but no more than the number of cores for a single NUMA node.
- Set auto close = ON
- Min Server Memory - Different per SQL Server but should be set.
- Max Server Memory - Different per SQL Server but should be set.

Disk layout recommendations

It is recommended that separate drives are used for data and transaction log files, temporary databases, and backups.

Create a maintenance plan

Ensure you have a maintenance plan in place to take regular backups. Use your organization's preferred maintenance plan for backing up SQL databases. If your organization does not have a maintenance plan, it is recommended that you research industry best practices and select a maintenance plan that suits your organization's needs.

Take backups

Backups should be designed based on your organization's recovery point (RPO) and recovery time (RTO) objectives.

- RPO – The point in time you can recover your data following a failure. This determines how much data is lost.
- RTO – The amount of time you have to recover your data following a failure. This determines the length of time that the platform is unavailable.

When creating a backup and recovery plan for Blue Prism databases it is important to consider and implement the points below:

- Define both RPO and RTO.
- Use the FULL recovery model to allow for full, differential, and transaction log backups in-line with your RPO and RTO.
- Use WITH CHECKSUM and VERIFYONLY options on all backups to verify backups are valid and can be restored if required.
- Use WITH COMPRESSION option to save disk space and reduce the time taken to back up the databases and optionally restore them.
- Document the backup and recovery process.
- Check your backups are reliable by regularly trying to restore them.

How often you perform these backups depends on the size of your organization, and the amount and value of data risk.

It is recommended that full backups are performed during absolute downtime. Incremental backups can be performed without stopping any services with the risk that some data may be lost.

Resolve index fragmentation

Database index fragmentation lowers query performance over time. To prevent this, rebuild indexes as frequently as database downtime will allow. Rebuilding indexes after taking backups and/or deleting large amounts of data is also advised. It is also recommended that you rebuild indexes before taking a full database backup to minimize index fragmentation in the event of having to restore a full backup.

Recommended thresholds for rebuilding/reorganizing index maintenance are: < 30% reorg and > 30% rebuild.

Rebuilding database indexes can be scheduled to run as a job inside the database server and/or added to the database maintenance plan. It is recommended that you run them during periods of low system activity and that they are scheduled to avoid overlapping with the backup and DBCC CHECKDB maintenance.

Back up the Message Broker Server

The Message Broker Server runs RabbitMQ™. See the RabbitMQ online help for creating backups of the Message Broker Server.

Logging

The purpose of diagnostic logging is to make more information available as the application executes. Logged errors and warnings can help pinpoint failures within the system that might not be immediately obvious to an end user. More verbose logging can be enabled temporarily to provide a useful picture of how an application is behaving when troubleshooting a problem.

Blue Prism uses a proven and reliable library called NLog to output and record log information. An administrator can fine-tune the amount of information logged, either globally or in specific areas of the application.

Logging levels

Log entries are categorized by level. Entries with a level of *Information* or upwards are usually recorded as standard. Lower, more detailed levels, such as *Debug* and *Trace*, provide more verbose information but need to be enabled.

NLog defines the following levels:

- **Trace** – Very detailed logs, which may include high-volume information such as protocol payloads. This log level is typically only enabled during development.
- **Debug** – Debugging information, less detailed than Trace, typically not enabled in production environments due to a possible impact on performance.
- **Information** – Information messages, which are normally enabled in production environments.
- **Warning** – Warning messages, typically for non-critical issues, which can be recovered or which are temporary failures.
- **Error** – Error messages – most of the time these are exceptions.
- **Fatal** – Very serious errors.

Standard logging configuration

The logging levels are defined within the appsettings.json file in the installation folder for each web site and service. For default installations, these folders are located under C:\Program Files (x86)\Blue Prism\.

You should not need to amend the log configuration settings in the appsettings.json file yourself during normal usage. Blue Prism Customer Support will provide alternative log configuration settings when investigating a problem with the product. If the logging settings are changed in the appsettings.json file, the site will need restarting within IIS.

Amending the logging configuration can affect the performance of the application and special care should be taken if amending in a production environment.

The default configuration writes log entries at information level and upwards (including warnings, errors and fatal errors) to a log file. Log files are written to the directory specified in the LogsFolder setting in the appsettings.json file, typically this is set to ./Logs_{Application}, for example ./Logs_Hub or ./Logs_Interact.

By default, the logging configuration settings in the appsettings.json file are:

```
"Logging": {
      "LogsFolder": "./Logs_{Application}",
      "LogLevel": {
        "Default": "Information",
        "System": "Warning",
        "Microsoft": "Warning"
      }
    },
```

Separate log files are generated based on the log level and the date, and these are reflected in the log filename, such as warns.2021-05-07 or infos.2021-05-07.

Below is an example of a line from an information log file:

```
[08:58:11.4549] Connect.Core.Actions.UpdateCacheAction - Cache for widgets was updated
```

The format of this text contains the following elements:

- Time (using the time zone set on the server) – The date is reflected in the filename.
- Logger name – This usually identifies the class and namespace from which the log entry originates.
- The log message.
- Error information – Only available if exception information is logged. Full details are logged on a separate line below the log message.

Additional logging configuration

Blue Prism has developed additional logging configuration settings that can be added to the appropriate appsettings.json file to capture activity by certain components.

Debugging LDAP

You can configure logging to help debug any issues that may arise when synchronizing Hub with LDAP. You will need to set the logging up in the Authentication Server appsettings.json file before you synchronize the users in the Hub UI.

1. On the server, navigate to the Authentication Server folder. By default, this is located in C:\Program Files (x86)\Blue Prism\.
2. Open the appsettings.json file in a text editor.

3. Locate the Logging section and add `"ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"` to the LogLevel section and insert a comma at the end of the line above, for example:

```
"Logging": {
      "LogsFolder": "./Logs_AuthenticationServer",
      "LogLevel": {
        "Default": "Information",
        "System": "Warning",
        "Microsoft": "Warning",
        "ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"
      }
    },
```

4. Save the file.
5. Recycle the Authentication Server pool in the IIS Application Pools.

   If you have upgraded from a version prior to 4.3, you will need to recycle the IMS pool.

6. Restart the Authentication Server site in the IIS Sites.

This creates a file with the prefix "debug" and the appropriate date in the Logs_AuthenticationServer directory.

After successfully solving any issues using the debugging information, you must remove the added line and the comma, save the file and repeat steps 5 and 6. Otherwise, the log file will significantly increase in size and potentially fill the memory.

Log gatherer service

This Windows service removes old product logs from each web server component (Hub, Interact, Authentication Server , Audit Service, Audit Service Listener, Email Service, Log Gatherer Service, IADA, Interact Remote API, SignalR, Submit Form Manager). This service is scheduled to do so on the 7th of every month and the logs are moved to C:\Program Files (x86)\Blue Prism\ArchivedLogs.

You can change the archived log folder path and scheduler date within apppsettings.json – “ArchivedFolder” in C:\Program Files (x86)\Blue Prism\Log Service (default), will allow you to change the archive path and “DayOfMonth” will allow you to change the scheduler date.

Further information

The following links may provide useful further information:

- NLog Github Repository – Basic Tutorial
- NLog Official Website – Configuration Options

Web server maintenance

If your Hub or Interact web servers fail, you will need to recreate them. To be able to do this, you must ensure you have the required backups available.

Backups

Files

You should regularly back up the Files folder located in C:\Program Files (x86)\Blue Prism. This folder contains application data, and any files and attachments that have been submitted through Interact (unless the files and attachments were specified to be in another location in the File Service appsettings.json file).

> This is the default install location. If you entered a different location during the initial install, the Files folder will be located there.

If you have Interact 4.4 installed or you are upgrading from Interact 4.4, any new files are located in the database. These will be backed up as part of your database schedule. However, if you have upgraded from an earlier version of Interact, you should still back up the Files folder.

Certificates

Optionally you can back up certificates used by your web server. For a complete list of certificates, see the Hub Maintenance Guide, as well as the following additional certificates:

- BluePrismCloud_IMS_JWT
- BluePrismCloud_Data_Protection
- BPC_SQL_CERTIFICATE

Restore a web server

If your existing Hub or Interact web servers fail, you will need to rebuild them.

Hub web server

> Prior to uninstalling Hub, it is recommended that you stop all Application Pools and remove the BPC certificates created by the installer.

1. If you are rebuilding an existing web server, uninstall Hub.
2. Install Hub.

   Enter the same settings as you did for the original installation, including:

   - On any Server SQL connection pages in the Blue Prism Hub Setup Wizard, enter the same **Username** and **Password** that you used for the previous installation.
   - On any Server IIS setup pages in the Blue Prism Hub Setup Wizard, enter the same **Host name** and **Certificate** that you used for the previous installation.
3. Paste the backup copy of the Files folder back into your installation location, for example: C:\Program Files (x86)\Blue Prism.

Interact web server

1. If you are rebuilding an existing web server, Uninstall Interact.
2. Install Interact:

   Enter the same settings as you did for the original install, including:

   - On any **Server SQL connection** pages in the Blue Prism Interact Setup Wizard, enter the same **Username** and **Password** that you used for the previous installation.
   - On any **Server IIS setup** pages in the Blue Prism Interact Setup Wizard, enter the same **Host name** and **Certificate** that you used for the previous installation.
3. Paste the backup copy of the Files folder back into your installation location, for example: C:\Program Files (x86)\Blue Prism.