

# blueprism<sup>®</sup>

## Hub und Interact 4.5 Plattformwartungshandbuch

Dokumentrevision: 1.0



## Marken- und Urheberrechtshinweise

Die in diesem Handbuch enthaltenen Informationen sind das Eigentum von Blue Prism Cloud Limited und/oder verbundenen Unternehmen, müssen vertraulich behandelt werden und dürfen ohne schriftliche Genehmigung eines autorisierten Vertreters von Blue Prism nicht an Dritte weitergegeben werden. Ohne die schriftliche Erlaubnis von Blue Prism Cloud Limited oder verbundenen Unternehmen darf kein Teil dieses Dokuments in jeglicher Form oder Weise vervielfältigt oder übertragen werden, sei es elektronisch, mechanisch oder durch Fotokopieren.

### © Blue Prism Cloud Limited, 2001 – 2022

„Blue Prism“, das „Blue Prism“ Logo und Prism Device sind Marken oder eingetragene Marken von Blue Prism Limited und seinen Tochtergesellschaften. Alle Rechte vorbehalten.

Alle anderen Warenzeichen werden hiermit anerkannt und werden zum Vorteil ihrer jeweiligen Eigentümer verwendet.

Blue Prism Cloud Limited und seine verbundenen Unternehmen sind nicht für den Inhalt externer Websites verantwortlich, auf die in diesem Handbuch Bezug genommen wird.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.

Registriert in England: Reg.- Nr. 4260035. Tel.: +44 370 879 3000. Web: [www.blueprism.com](http://www.blueprism.com)

## Inhalt

<b>Wartungsübersicht zur Blue Prism Plattform</b> .....	<b>4</b>
Zielgruppe .....	4
<b>SQL-Datenbankwartung</b> .....	<b>5</b>
Allgemeine Empfehlungen für die Datenbankwartung .....	6
Wartungsplan erstellen .....	7
Backups erstellen .....	7
Indexfragmentierung beheben .....	8
<b>Backup des Message-Broker-Servers erstellen</b> .....	<b>9</b>
<b>Logging</b> .....	<b>10</b>
Logging-Stufen .....	10
Standard-Logging-Konfiguration .....	11
Zusätzliche Logging-Konfiguration .....	11
Log-Gatherer-Service .....	12
Weitere Informationen .....	12
<b>Webserver-Wartung</b> .....	<b>13</b>
Backups .....	13
Webserver wiederherstellen .....	13

# Wartungsübersicht zur Blue Prism Plattform

Dieser Leitfaden enthält Anleitungen mit Best Practices zur Wartung für Blue Prism® Hub und Blue Prism® Interact, einschließlich:

- [Wartungsplan für SQL-Datenbank-Backups erstellen](#)
- [Backup des Message-Broker-Servers erstellen](#)
- [Backuperstellung und Wiederherstellung des Webservers](#)
- [Logging](#)

Dieser Leitfaden ist spezifisch für Blue Prism Hub und Interact. Informationen zur Wartung der Blue Prism Enterprise Datenbank finden Sie unter [Blue Prism Datenbankserver warten](#).

## Zielgruppe

Dieser Leitfaden richtet sich an erfahrene Datenbank- und Serveradministratoren.

## SQL-Datenbankwartung

Diese Informationen sollen nur als Leitfaden dienen. Es wird empfohlen, standardmäßige Best Practices der Branche zu befolgen und Empfehlungen von einem erfahrenen Datenbankadministrator einzuholen. Diese Informationen sollten unter Berücksichtigung der allgemeinen Auswirkungen auf die Gesamtumgebung verwendet werden.

Die folgenden Datenbanken müssen gewartet werden:

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



CacheDB wurde ab Hub 4.4 durch FileServiceDB ersetzt.

## Allgemeine Empfehlungen für die Datenbankwartung

Folgendes wird empfohlen:

- Legen Sie das automatische Wachstum für alle Datenbanken korrekt fest. Empfohlene Werte sind 1024 MB für die Datendatei und 2048 MB für das Transaktionslog.
- Aktualisieren Sie den Wert für das automatische Wachstum, wenn die Größe der Datenbank zunimmt, um die Häufigkeit von Ereignissen mit automatischem Wachstum zu minimieren.



Verwenden Sie kein Dateiwachstum in %, sondern legen Sie ein Wachstum um eine feste Anzahl von Megabytes fest.

- Beseitigen Sie übermäßige Transaktionslog-Dateifragmentierung. Weitere Informationen finden Sie in der [Microsoft-Onlinehilfe](#).
- Aktivieren Sie die sofortige Dateiiinitialisierung. Weitere Informationen finden Sie in der [Microsoft-Onlinehilfe](#).
- Deaktivieren Sie die automatische Verkleinerung, legen Sie die Seitenüberprüfung für alle Datenbanken auf Prüfsumme fest und aktivieren Sie AUTO\_CREATE\_STATISTICS und AUTO\_UPDATE\_STATISTICS. Richten Sie einen regelmäßigen Prozess zur Aktualisierung der Statistiken ein.

Zu diesem Zweck können Sie für jede der von Hub und Interact installierten Datenbanken die folgende T-SQL festlegen:

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

- Richten Sie einen regelmäßigen Prozess zum Ausführen von DBCC CHECKDB ein – Es wird empfohlen, dass ein SQL-Agentenauftrag mindestens einmal pro Tag ausgeführt wird, wenn eine geringe oder keine Systemauslastung vorliegt. Die Ergebnisse sollten auf eine Beschädigung hin überprüft werden. Es könnte nützlich sein, SQL-Agentenalarme zu erstellen, um eine Operatorgruppe über die folgenden Fehler zu benachrichtigen:
  - 823 – Hard I/O Corruption (Schwere I/O-Beschädigung)
  - 824 – Soft I/O Corruption (Leichte I/O-Beschädigung)
  - 825 – Read/Retry Corruption (Lese-/Wiederholungsbeschädigung)
  - 9100 – Index Corruption (Indexbeschädigung)
  - Severity 19-25 Errors (Fehler mit Schweregrad 19–25)
- Optimize for ad-hoc workloads = ON (Optimierung für Ad-hoc-Workloads = EIN)
- Backup compression default = ON (Standardmäßige Backup-Komprimierung = EIN)
- Backup checksum default = ON (Standardmäßige Backup-Prüfsumme = EIN)
- Cost threshold for parallelism (Kostenschwelle für Parallelität) – 50 ist ein guter Ausgangspunkt.
- Max degree of parallelism (Max. Grad der Parallelität) – Hängt von der NUMA-Konfiguration vom SQL Server ab, aber nicht mehr als die Anzahl der Kerne für einen einzigen NUMA-Knoten.

- Set auto close = ON (Automatisch schließen = EIN)
- Min Server Memory (Min. Serverspeicher) – Unterschiedlich pro SQL Server, sollte aber festgelegt werden.
- Max Server Memory (Max. Serverspeicher) – Unterschiedlich pro SQL Server, sollte aber festgelegt werden.

## Empfehlungen zur Datenträgerverwendung

Es wird empfohlen, separate Laufwerke für Daten- und Transaktionslogdateien, temporäre Datenbanken und Backups zu verwenden.

## Wartungsplan erstellen

Stellen Sie sicher, dass ein Wartungsplan besteht, um regelmäßige Backups durchzuführen. Verwenden Sie den bevorzugten Wartungsplan Ihres Unternehmens zum Sichern von SQL-Datenbanken. Wenn Ihr Unternehmen keinen Wartungsplan hat, wird empfohlen, dass Sie sich über die Best Practices der Branche informieren und einen Wartungsplan auswählen, der die Anforderungen Ihres Unternehmens erfüllt.

## Backups erstellen


Backups sollten basierend auf den Recovery Point (RPO) und Recovery Time Objectives (RTO) Ihres Unternehmens geplant werden.

- RPO – Der Zeitpunkt, für den Sie Ihre Daten nach einem Ausfall wiederherstellen können. Dies entscheidet darüber, wie viele Daten verloren gehen.
- RTO – Die Dauer der Wiederherstellung Ihrer Daten nach einem Ausfall. Dies entscheidet über den Zeitraum, während dem die Plattform nicht verfügbar ist.

Beim Erstellen eines Backup- und Wiederherstellungsplans für Blue Prism Datenbanken ist es wichtig, die folgenden Punkte zu berücksichtigen und zu implementieren:

- Definieren Sie RPO und RTO.
- Verwenden Sie das Wiederherstellungsmodell FULL (Vollständig), um vollständige, differenzielle und Transaktionslog-Backups gemäß Ihrer RPO- und RTO-Konfiguration zu ermöglichen.
- Verwenden Sie die Optionen WITH CHECKSUM (Mit Prüfsumme) und VERIFYONLY (Nur prüfen) bei allen Backups, um zu überprüfen, ob die Backups in Ordnung sind und bei Bedarf wiederhergestellt werden können.
- Verwenden Sie die Option WITH COMPRESSION (Mit Komprimierung), um Speicherplatz zu sparen und die Zeit zu reduzieren, die zum Sichern der Datenbanken und optional zum Wiederherstellen benötigt wird.
- Dokumentieren Sie den Backup- und Wiederherstellungsprozess.
- Überprüfen Sie, ob Ihre Backups zuverlässig sind, indem Sie regelmäßig testen, ob sie eine Wiederherstellung ermöglichen.

Wie oft Sie diese Backups durchführen sollten, hängt von der Größe Ihres Unternehmens und der Menge und dem Wert der gefährdeten Daten ab.

 Es wird empfohlen, dass vollständige Backups während absoluter Ausfallzeiten durchgeführt werden. Inkrementelle Backups können durchgeführt werden, ohne Dienste zu unterbrechen, mit dem Risiko, dass einige Daten verloren gehen.

## Indexfragmentierung beheben

Die Datenbank-Indexfragmentierung verschlechtert mit der Zeit die Abfrage-Performance. Um dies zu verhindern, sollten Indizes so häufig neu erstellt werden, wie es die Datenbankausfallzeit zulässt. Auch die Neuerstellung von Indizes nach Backups und/oder Löschungen von großen Datenmengen wird empfohlen. Es wird auch empfohlen, dass Sie Indizes neu erstellen, bevor Sie ein vollständiges Datenbankbackup erstellen, um die Indexfragmentierung im Falle der Wiederherstellung eines vollständigen Backups zu minimieren.

Empfohlene Schwellenwerte für die Neuerstellung/Reorganisation der Indexwartung sind: < 30 % Reorganisation und > 30 % Neuerstellung.

Die Neuerstellung von Datenbankindizes kann so geplant werden, dass sie als Auftrag im Datenbankserver ausgeführt und/oder dem Datenbankwartungsplan hinzugefügt wird. Es wird empfohlen, dass Sie diese Prozesse während Zeiten niedriger Systemaktivität ausführen und dass sie so geplant werden, dass eine Überschneidung mit Backups und der DBCC CHECKDB-Wartung vermieden wird.



## Backup des Message-Broker-Servers erstellen

Der Message-Broker-Server führt RabbitMQ™ aus. Informationen zum Erstellen von Backups des Message-Broker-Servers finden Sie in der [RabbitMQ-Onlinehilfe](#).

## Logging

Der Zweck diagnostischen Loggings besteht darin, während der Ausführung der Anwendung mehr Informationen zur Verfügung zu stellen. Geloggte Fehler und Warnungen können helfen, Fehler innerhalb des Systems, die für einen Endbenutzer womöglich nicht sofort offensichtlich sind, genau zu ermitteln. Temporär kann ausführlicheres Logging aktiviert werden, um bei der Behebung eines Fehlers einen hilfreichen Einblick in das Verhalten der Anwendung zu gewinnen.

Zum Ausgeben und Aufzeichnen von Loginformationen verwendet Blue Prism eine bewährte und zuverlässige Bibliothek namens NLog. Ein Administrator kann die Menge der protokollierten Informationen entweder global oder in bestimmten Bereichen der Anwendung anpassen.

## Logging-Stufen

Logeinträge werden in Stufen kategorisiert. Einträge mit der Stufe *Information* oder höher werden in der Regel standardmäßig aufgezeichnet. Niedrigere, detailliertere Stufen, wie *Debug* und *Trace*, liefern ausführlichere Informationen, müssen jedoch aktiviert werden.

NLog definiert die folgenden Stufen:

- **Trace** – Sehr detaillierte Logs, die große Informationsmengen wie Protokollnutzlasten, enthalten können. Diese Logstufe wird typischerweise nur während der Entwicklung aktiviert.
- **Debuggen**– Debugging-Informationen mit weniger Details als Trace, normalerweise in Produktionsumgebungen aufgrund möglicher Auswirkungen auf die Leistung nicht aktiviert.
- **Information** – Informationsmeldungen, die normalerweise in Produktionsumgebungen aktiviert sind.
- **Warning** – Warnhinweise, typischerweise für nicht kritische Probleme, die gelöst werden können, oder für vorübergehende Fehler.
- **Error** – Fehlermeldungen – meist sind dies Ausnahmen.
- **Fatal** – Sehr schwerwiegende Fehler.

## Standard-Logging-Konfiguration

Die Logging-Stufen werden in der „appsettings.json“-Datei im Installationsordner für jede Website und jeden Dienst definiert. Bei Standardinstallationen finden Sie diese Ordner unter C:\Programme (x86)\Blue Prism\.

Sie sollten die Logkonfigurationseinstellungen in der „appsettings.json“-Datei bei normaler Verwendung nicht eigenständig ändern müssen. Der Blue Prism Kundensupport stellt bei der Untersuchung eines Problems mit dem Produkt alternative Logkonfigurationseinstellungen bereit. Wenn die Logging-Einstellungen in der „appsettings.json“-Datei geändert werden, muss die Site in IIS neu gestartet werden.

Das Ändern der Logging-Konfiguration kann sich auf die Performance der Anwendung auswirken und bei Änderungen in einer Produktionsumgebung ist besondere Vorsicht geboten.

Die Standardkonfiguration schreibt Logeinträge der Stufe „Information“ und höher (einschließlich „Warning“, „Error“ und „Fatal“) in eine Logdatei. Logdateien werden in das Verzeichnis geschrieben, das für die „LogsFolder“-Einstellung in der „appsettings.json“-Datei angegeben ist. Typischerweise ist dies festgelegt auf „./Logs\_{Anwendung}“, beispielsweise „./Logs\_Hub“ oder „./Logs\_Interact“.

Die standardmäßigen Logging-Konfigurationseinstellungen in der Datei appsettings.json sind:

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

Separate Logdateien werden basierend auf der Logstufe und dem Datum generiert und diese werden in die Logdateinamen aufgenommen, zum Beispiel „warns.2021-05-07“ oder „infos.2021-05-07“.

Es folgt ein Beispiel für eine Zeile in einer Information-Logdatei:

```
[08:58:11.4549] Connect.Core.Actions.UpdateCacheAction - Cache für Widgets wurde aktualisiert
```

Das Format dieses Texts enthält die folgenden Elemente:

- Zeit in UTC – Dateiname beinhaltet das Datum.
- Logger-Name – Identifiziert normalerweise die Klasse und den Namespace, aus dem der Logeintrag stammt.
- Die Lognachricht.
- Fehlerinformationen – nur verfügbar, wenn Ausnahmeanforderungen protokolliert werden. Die vollständigen Details werden in einer separaten Zeile unter der Lognachricht protokolliert.

## Zusätzliche Logging-Konfiguration

Blue Prism hat zusätzliche Logging-Konfigurationseinstellungen entwickelt, die der jeweiligen „appsettings.json“-Datei hinzugefügt werden können, um Aktivitäten bestimmter Komponenten zu erfassen.

## Debugging von LDAP

Sie können das Logging so konfigurieren, dass es beim Debugging von Problemen hilft, die bei der Synchronisierung von Hub mit LDAP auftreten können. Sie müssen das Logging in der Datei appsettings.json von Authentication Server einrichten, bevor Sie die Benutzer in der Hub

Benutzeroberfläche synchronisieren.

1. Navigieren Sie auf dem Server zum Ordner „Authentication Server“. Standardmäßig befindet er sich in C:\Programme (x86)\Blue Prism\.
2. Öffnen Sie die Datei „appsettings.json“ in einem Texteditor.
3. Suchen Sie den Logging-Abschnitt, fügen Sie `"ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"` zum „LogLevel“-Abschnitt hinzu und setzen Sie ein Komma an das Ende der obigen Zeile. Zum Beispiel:

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

4. Speichern Sie die Datei.
5. Recyceln Sie den Authentication Server Pool in den IIS-Anwendungspools.



Wenn Sie ein Upgrade von einer Version vor 4.3 durchgeführt haben, müssen Sie den IMS-Pool recyceln.

6. Starten Sie die Authentication Server Site in den IIS-Sites neu.

Dadurch wird eine Datei mit dem Präfix „debug“ und dem entsprechenden Datum im Verzeichnis „Logs\_AuthenticationServer“ erstellt.



Nachdem Sie mit den Debugging-Informationen die Probleme erfolgreich gelöst haben, müssen Sie die hinzugefügte Zeile und das Komma entfernen, die Datei speichern und die Schritte 5 und 6 wiederholen. Andernfalls wird die Größe der Logdatei deutlich zunehmen und möglicherweise den Speicher füllen.

## Log-Gatherer-Service

Dieser Windows-Dienst entfernt alte Produktlogs von der jeweiligen Webserver-Komponente (Hub, Interact, Authentication Server, Audit Service, Audit Service Listener, Email Service, Log-Gatherer-Service, IADA, Interact Remote API, SignalR, Manager für die Formularübermittlung). Dies geschieht jeweils am 7. des Monats und die Logs werden in C:\Programme (x86)\Blue Prism\ArchivedLogs verschoben.

Sie können den Pfad für archivierte Logdaten und das Zeitplanerdatum in appsettings.json ändern – unter „ArchivedFolder“ in C:\Programme (x86)\Blue Prism\Log Service (Standard) können Sie den Archivpfad und unter „DayOfMonth“ das Zeitplanerdatum ändern.

## Weitere Informationen

Die folgenden Links können weitere nützliche Informationen liefern:

- [NLog GitHub Repository – Basis-Tutorial](#)
- [Offizielle Website von NLog – Konfigurationsoptionen](#)


## Webserver-Wartung

Wenn Ihre Hub oder Interact Webserver ausfallen, müssen Sie sie neu erstellen. Damit dies möglich ist, müssen Sie sicherstellen, dass die erforderlichen Backups verfügbar sind.

### Backups

#### Dateien

Sie sollten regelmäßig ein Backup des Ordners „Files“ erstellen, der sich in „C:\Programme (x86)\Blue Prism“ befindet. Dieser Ordner enthält Anwendungsdaten und alle Dateien und Anhänge, die per Interact übermittelt wurden (außer in der „appsettings.json“-Datei von File Service wurde ein anderer Speicherort für die Dateien und Anhänge angegeben).

 Dies ist der standardmäßige Installationsort. Wenn Sie während der Erstinstallation einen anderen Speicherort eingegeben haben, befindet sich der Ordner „Files“ an diesem.

Wenn Sie Interact 4.4 installiert haben oder ein Upgrade von Interact 4.4 durchführen, befinden sich alle neuen Dateien in der Datenbank. Diese werden im Rahmen Ihres [Datenbankzeitplans](#) in Backups gesichert. Wenn Sie jedoch ein Upgrade von einer früheren Version von Interact durchgeführt haben, sollten Sie dennoch ein Backup des Ordners „Files“ erstellen.

#### Zertifikate


Optional können Sie Backups von Zertifikaten erstellen, die von Ihrem Webserver verwendet werden. Eine vollständige Liste der Zertifikate finden Sie im [Hub Wartungshandbuch](#) sowie in den folgenden zusätzlichen Zertifikaten:

- BluePrismCloud\_IMS\_JWT
- BluePrismCloud\_Data\_Protection
- BPC\_SQL\_CERTIFICATE

## Webserver wiederherstellen

Wenn Ihre bestehenden Hub oder Interact Webserver ausfallen, müssen Sie sie neu erstellen.

### Hub Webserver

 Es wird empfohlen, vor der Deinstallation von Hub alle Anwendungspools zu stoppen und die vom Installationsprogramm erstellten BPC-Zertifikate zu entfernen.

1. Wenn Sie einen vorhandenen Webserver neu erstellen, müssen Sie [Hub deinstallieren](#).
2. [Hub installieren](#):

Geben Sie die gleichen Einstellungen wie bei der ursprünglichen Installation ein, einschließlich:

- Geben Sie auf allen Server-SQL-Verbindungsseiten im Blue Prism Hub Setup-Assistenten den gleichen **Benutzernamen** und das gleiche **Passwort** ein, die Sie für die vorherige Installation verwendet haben.
- Geben Sie auf allen Seiten vom Server-IIS-Setup im Blue Prism Hub Setup-Assistenten den gleichen **Hostnamen** und das gleiche **Zertifikat** ein, die Sie für die vorherige Installation verwendet haben.

3. Fügen Sie die Backup-Kopie des Ordners „Files“ wieder am Installationsort ein, zum Beispiel: „C:\Programme (x86)\Blue Prism“.

## Interact Webserver

1. Wenn Sie einen vorhandenen Webserver neu erstellen, müssen Sie [Interact deinstallieren](#).

2. [Interact deinstallieren](#):

Geben Sie die gleichen Einstellungen wie bei der ursprünglichen Installation ein, einschließlich:

- Geben Sie auf allen **Server-SQL-Verbindungsseiten** im Blue Prism Interact Setup-Assistenten den gleichen **Benutzernamen** und das gleiche **Passwort** ein, die Sie für die vorherige Installation verwendet haben.
  - Geben Sie auf allen Seiten vom **Server-IIS-Setup** im Blue Prism Interact Setup-Assistenten den gleichen **Hostnamen** und das gleiche **Zertifikat** ein, die Sie für die vorherige Installation verwendet haben.
3. Fügen Sie die Backup-Kopie des Ordners „Files“ wieder am Installationsort ein, zum Beispiel: „C:\Programme (x86)\Blue Prism“.