INSTALLATION AND UPGRADE GUIDE

Database Performance Analyzer

Version 2024.2

SOLARWINDS

Last Updated: Monday, May 6, 2024

Table of Contents

DPA deployment overview

The following sections outline the tasks required to deploy DPA and begin monitoring database instances.

For information about upgrading DPA, see Upgrade DPA.

Options for deploying DPA

DPA offers the following deployment options:

- **Self-installed DPA server and repository database**

  You can install DPA on a server that runs either Windows or Linux. The DPA server can be on premises or in a private or public cloud. For this deployment option, complete the following tasks:

  - Complete the pre-installation checklist to plan for the installation and prepare your environment.
  - Install DPA on a server running Windows or Linux.
  - Create the repository database, which stores the performance data that DPA collects.

  When you deploy DPA by installing it yourself, you must purchase an individual license for each monitored database instance.

- **Microsoft Azure Marketplace**

  SolarWinds provides a pre-built image in the Microsoft Azure Marketplace. You can quickly deploy DPA in the Azure Marketplace without having to install it or set up the repository database. The VM contains a DPA server on Windows and a built-in Microsoft SQL Server database instance configured as the DPA repository.

  When you deploy DPA in the Azure Marketplace, you must purchase an individual license for each monitored database instance.

- **Amazon Web Services (AWS) Marketplace**

  Another option for a quick deployment is to launch an Amazon Machine Image (AMI) from the Amazon Marketplace and then create the DPA repository database.

  Individual licenses are not required for DPA deployments in the AWS Marketplace. The AWS Marketplace Metering Service is used to calculate DPA charges.

Begin monitoring database instances

When you have deployed DPA, complete the following tasks to begin monitoring database instances:

- ☐ Register each database instance you want to monitor.
- ☐ For **self-installed** or **Azure Marketplace** deployments, purchase and allocate licenses.
  1. Evaluate how many licenses of each type you need.
  2. Purchase licenses from your sales representative, and download them from the Customer Portal.

     ⓘ If you have not yet created a SolarWinds account, see Access the Customer Portal to create an account.
  3. Allocate licenses to each database instance.
- ☐ Begin monitoring database instances. See the DPA Getting Started Guide for a walk-though of performing common tasks in DPA. For example:
  - Investigate an application performance problem
  - Investigate an increase in wait time
  - Investigate a wait time anomaly
  - Create an alert to monitor SQL statement execution time
  - Create a report to track wait types for a single SQL statement

Prepare to install DPA on a self-managed server

If you are installing DPA yourself, complete the pre-installation checklists below. These checklists help you:

- Obtain the required credentials.
- Verify that system requirements are met.
- Prepare your environment.

Plan for the installation

☐	Review the Database Performance Analyzer release notes.
☐	Identify the server where DPA will be installed. Make sure the server: • Is powerful enough to handle the load of the potential number of monitored database instances that you will register. See the DPA server requirements. • Has network connectivity to the DPA repository and each of the monitored database instances that you will register. DPA can be installed on the same server as the repository, although it is not required or recommended.
☐	Identify or install the repository database. Make sure: • The repository is not installed in a critical production database instance. • The repository database and server meet the repository database requirements. • You have credentials with the required privileges.
☐	Create a Customer Portal account. To download SolarWinds products and licenses, you need a SolarWinds Customer Portal account. To create your SolarWinds account, see How do I access the Customer Portal.
☐	Obtain admin credentials for the DPA server. SolarWinds recommends using the Local Administrator Account for installation. Make sure you have local admin server credentials for the DPA server. ⓘ The Local Administrator Account is not the same as a domain account with local admin rights. A domain account is subject to your domain group policies.
☐	Schedule the installation, preferably during off-peak hours.

☐	Send a message to your company about the installation schedule and maintenance window. If you need additional help, contact and allocate staff to be available.

Prepare the environment

Before installation, prepare the SolarWinds environment:

☐	Prepare the servers based on your deployment size and system requirements.
☐	Before installation, **run all OS updates** on all servers. As you install, if an OS update runs, your system may reboot and require you to restart the installation process. These include Microsoft Windows, Linux, and others as specified in requirements.
☐	For your server ports and firewall, open the required ports. DPA uses these ports to send and receive data.

Installation gotchas

If you are installing DPA on a server with a **Linux-based** OS, be sure to:

- Set the `JAVA_HOME` variable.
- Make sure the installation path has read, write, and execute permissions.

DPA 2024.2 system requirements

See the following sections for minimum supported system requirements:

For information about what database instances DPA can monitor, see Database instances DPA can monitor.

DPA Integration Module (DPAIM) compatibility

If you are **not** monitoring PostgreSQL database instances, DPAIM 11.1 or later is fully compatible with the current version of DPA.

If you are monitoring PostgreSQL database instances, DPAIM 2020.2 or later is required to display all available data from PostgreSQL instances in the SolarWinds Platform.

Port requirements

Review and open the following ports in the firewall to support communication to and from the DPA server.

ⓘ No additional ports are required for DPA Central.

Port	Protocol	Service/Process	Direction	Description
8124 (on premises) or 443 (cloud)	TLS	Windows: Ignite PI Service Linux: Java/Tomcat	Bidirectional	Default HTTPS port for the web server.

Port	Protocol	Service/Process	Direction	Description
8127	TCP	Windows: Ignite PI Service Linux: Java/Tomcat	Internal	This port is used internally by DPA. It does not need to be opened to internal or external traffic, but it needs to be available for DPA to use.
443	TLS	Windows: Ignite PI Service Linux: Java/Tomcat	Outbound	(Optional) To participate in the SolarWinds Improvement Program (SWIP), allow access to `api.solarwinds.com` for uploads and `downloads.solarwinds.com` for downloads of XML configuration files. (Optional) To enable online license activation or deactivation, allow access to `licenseserver.solarwinds.com`. Otherwise, use offline activation or deactivation.
80	TCP/HTTP	Windows: Ignite PI Service Linux: Java/Tomcat	Outbound	(Optional) To allow product updates in self-managed deployments, allow access to `updates.solarwinds.com`.
587	SMTP	Windows: Ignite PI Service Linux: Java/Tomcat	Outbound	(Optional) To use the default SMTP server for outgoing email from DPA, allow access to `mail.authsmpt.com`. Otherwise, configure DPA to use a custom SMTP server.

If you are using the DPA Integration Module to integrate DPA with the SolarWinds Platform, see the DPAIM port requirements.

Other connections to consider include the following. The ports used for these connections depend on how your organization configures the connections:

- Monitored database instances – TCP
- Repository database – TCP
- VMware (usually 443) – TCP

- LDAP – TCP
- Custom SMTP server – based on the SMTP server
- SNMP trap – UDP

DPA server requirements

You can install SolarWinds DPA on any physical or virtual Windows or Linux server that meets the self-managed server requirements listed below.

You can also launch DPA in the cloud:

- In the Amazon Web Services (AWS) Marketplace from an Amazon Machine Image (AMI):
  - A DPA AMI with DPA installed runs on the supported **Amazon Linux 2** operating system. This image does not include a repository.
  - DPA uses the AWS Marketplace Metering Service to calculate charges.
- In the Azure Marketplace:
  - The DPA virtual machine contains a DPA server on Windows and a built-in Microsoft SQL Server database instance configured as the DPA repository.
  - Individual licenses must be purchased.

Self-managed DPA server requirements

The CPU, RAM, and disk space requirements depend on the number of database instances you plan to monitor.

⚠ If you register VMware, **increase the CPU and RAM requirements by 50%**.

ⓘ These are estimates. They are based on testing done with an average of 2-3 active sessions per monitored instance. If you are monitoring busy instances with an average of more than 2-3 active sessions, please adjust accordingly.

Hardware or Software	1 - 20 Monitored DB Instances	21 - 50 Monitored DB Instances	51 - 100 Monitored DB Instances	101 - 250 Monitored DB Instances[1]
CPUs	2	4	4	6
RAM dedicated to DPA	2 GB	4 GB	6 GB	8 GB
Disk space for DPA	10 GB minimum 20 GB recommended			

Hardware or Software	1 - 20 Monitored DB Instances	21 - 50 Monitored DB Instances	51 - 100 Monitored DB Instances	101 - 250 Monitored DB Instances[1]
Disk space for Find SQL indexes	If the Find SQL feature is enabled, storage space for the indexes is required. By default, DPA stores the indexes on the DPA server, but you can move them. The amount of space required is determined by the number of monitored database instances. Index files for one instance can take up to 300 MB. **Example**: You are monitoring 120 instances. 120 x 0.3 GB = 36 GB Reserve at least 36 GB to provide adequate disk space for the Find SQL indexes.			
Operating system	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows 10 and 11 (evaluation only) • Linux			
Operating system architecture	64-bit			
Thread limit (Linux only)[2]	• Max user process: 4096 • Max open files: 2048	• Max user process: 4096 • Max open files: 2048	• Max user process: 6144 • Max open files: 4096	• Max user process: 8192 • Max open files: 6144
Character sets	To support a multibyte language, the DPA server, repository, and monitored instances must be configured with the same character set.			

[1] If you plan to monitor more than 250 database instances, consider using more than one DPA server and linking the servers together.

[2] To check the current max user process setting, run `ulimit -u`. To check the current max open files setting, run `ulimit -n`. To change the limits, edit the following file and restart the server:

`/etc/security/limits.conf`

Requirements for an AWS DPA server

The minimum required AWS instance type for the DPA server AMI is t2.medium. Smaller instance types are not supported.

A t2.medium size instance is typically powerful enough to monitor 20 database instances. You might need a larger instance type to reliably monitor more than 20 database instances.

Requirements for an Azure DPA server

The minimum required Azure tier is A2.

Recommendations for the DPA Central Server

SolarWinds does **not** recommend configuring DPA Central on a DPA server that is monitoring database instances. To optimize performance, configure DPA Central on a separate server.

Hardware or Software	0 - 50 Users	51 - 100 Users
CPU	4	6
RAM dedicated to DPA	4 GB	6 GB
Disk space for DPA	20 GB	20 GB

These estimates are based on the size of the cached data for each user per DPA server monitoring 250 database instances. Adjust as needed based on your deployment.

DPA repository database requirements

The repository database stores the data collected by DPA. A supported database instance must be installed on the database server.

Do not host the repository on a database instance that you plan to monitor, because this affects the performance of that instance.

Supported database versions

Database	Edition	Version
Microsoft SQL Server	• Standard • Enterprise	• 2022 (Windows or Linux) • 2019 (Windows or Linux) • 2017 (Windows or Linux) • 2016 • 2014 The latest Service Pack is supported unless otherwise noted.
Azure SQL Database	Standard Service Tier or higher	V12
MySQL	• Community • Enterprise	• 8 • 5.7.9+ • 5.6.10+ • Amazon RDS for MySQL 8.0, 5.6.34+, 5.7.16+ • Amazon Aurora for MySQL-compatible 8.0, 5.6.10a+, 5.7.12+
Oracle	• Standard • Enterprise	• 21 (single tenant and multitenant) • 19.x (single tenant and multitenant) • 18.4 (single tenant and multitenant) • 12.2 (single tenant and multitenant) • 12.1 (single tenant and multitenant)

⚠ Azure SQL Managed Instance (ASMI) is **not** supported as a DPA repository database.

ⓘ
- Although DPA will work with the Express editions of Oracle and SQL Server, SolarWinds does **not** officially support these editions for the repository because of the database size limits. If you need a free database for an evaluation, SolarWinds recommends using a MySQL database.
- You can host a self-managed Oracle, SQL Server, or MySQL database on Amazon EC2 to use as your repository.
- If you choose Azure SQL Database as your repository, SolarWinds recommends two or more database throughput units (DTU) per monitored database instance. See the Azure SQL Database DTU Calculator for more information.

Self-managed repository database server requirements

If you install DPA on the same server as the repository database, the server must meet these requirements in addition to the DPA server requirements.

⚠ If you register VMware, **increase the CPU and RAM requirements by 50%**.

ⓘ These are estimates. They are based on testing done with an average of 2-3 active sessions per monitored instance. If you are monitoring busy instances with an average of more than 2-3 active sessions, please adjust accordingly.

Hardware / Software	1 - 20 Monitored DB Instances	21 - 50 Monitored DB Instances	51 - 100 Monitored DB Instances	101 - 250 Monitored DB Instances
CPUs	2	2	4	4
Database cache available for DPA	4 GB	8 GB	8 GB	16 GB
Disk space	The amount of disk space your repository uses is determined by the number of database instances you are monitoring and the activity level of each instance: • Low: 1 GB • Medium: 3 GB • High: 5 GB **Example**: You are monitoring five low, three medium, and two high activity database instances. (5 × 1 GB) + (3 × 3 GB) + (2 × 5 GB) = 24 GB Reserve at least 24 GB to provide adequate disk space for this repository database.			

ⓘ Repository scalability depends on many things, including the database vendor and configuration, the specifications of the repository server, other activity on the repository server, and the activity levels of the monitored database instances.

Requirements for an AWS DPA repository database server

The following RDS instance types are recommended for AWS deployments.

To see the Amazon RDS database types and versions that are supported for an AWS DPA repository database, see Supported database versions.

Hardware / Software	1 - 20 Monitored DB Instances	21 - 50 Monitored DB Instances	51 - 100 Monitored DB Instances	101 - 250 Monitored DB Instances
RDS instance type	db.m5.large	db.m5.large	db.m5.xlarge	db.m5.xlarge
CPUs	2	2	4	4
Database cache available for DPA	8 GB	8 GB	16 GB	16 GB

Requirements for an Azure DPA repository database server

SolarWinds recommends two or more database throughput units (DTUs) per monitored database instance. See DTU-based purchasing model overview for more information.

Required administrator credentials

You must know the following credentials for the database instance hosting your DPA repository.

Repository database type	Credentials
SQL Server	SYSADMIN
Oracle	database administrator (DBA)
MySQL	repository administrator Alternatively, you can: • Provide the credentials of a user with privileges to create the repository user. The privileged user requires the Create, Drop, and Create User permissions and must be able to grant the following permissions: `GRANT ALL PRIVILEGES on <databaseName>` Where `<databaseName>` is the repository database you create or select when you set up the MySQL repository storage. • Run a script to create the repository user.

Repository database type	Credentials
Azure SQL Database	repository administrator Alternatively, you can: • Provide the credentials of a user with privileges to create the repository user. This user must be a member of the db_owner role. • Run a script to create the repository user.

Virtual environment requirements

In a virtual environment, DPA can remotely connect to the following to monitor the virtual environment that virtualized database instances are running on. The virtualized database instances must be registered separately from the virtual environment.

Software	Version
VMware vCenter Server	• 7.0 • 6.7 • 6.5
VMware ESX/ESXi Host	• 7.0 • 6.7 • 6.5

Supported web browsers

You can use the following browsers to access the DPA web interface:

- Chromium-based version of Microsoft Edge: the latest stable version

  Internet Explorer (IE) and legacy versions of Microsoft Edge are **not** supported. If you access DPA using these browsers, some DPA functionality is not available or does not function correctly. For example, the Find SQL and Resources tabs are not accessible, and drop-down menus in other areas do not function correctly.

- Mozilla Firefox: the latest stable version
- Google Chrome: the latest stable version

Requirements for monitoring MySQL database instances

SolarWinds recommends the following settings to optimize reporting capabilities for a MySQL database instance.

MySQL Performance Schema

The Performance Schema monitors server events and collects performance data. If the Performance Schema is not enabled, DPA provides limited data. Monitoring with the Performance Schema disabled excludes the following data:

- All instrumented wait events
- All wait operations
- All file wait time, broken out by file
- All object wait time, broken out by index and table
- SQL statistics
- Performance-schema dependent alerts

The Performance Schema must be enabled at server startup. In MySQL versions 5.6.6 and later, the Performance Schema is enabled by default.

Global Instrumentation and Thread Instrumentation

Global Instrumentation and Thread Instrumentation must be enabled in the Performance Schema configuration. Disabling these instruments has the same effect as disabling the Performance Schema.

By default, DPA enables these instruments in the configuration. However, if you select the Leave As Is option for Performance Schema setup, you must verify that Global Instrumentation and Thread Instrumentation are enabled in the existing Performance Schema configuration.

show_compatibility_56 system variable

If the monitored database instance is MySQL 5.7.6 or later, SolarWinds recommends turning on the `show_compatibility_56` system variable. If this variable is on, DPA can collect data for all metrics.

If this variable is off and the Performance Schema is enabled, DPA cannot collect data for the following metrics:

- Selects
- Inserts
- Updates
- Deletes

Java requirements

DPA ships with JDK 11.0.17 LTS for Windows and Linux and installs this version of Java on the DPA server. If you are installing DPA on a **supported** operating system, **no action** is required.

For **unsupported** operating systems, ensure that JDK 11.0.17 is installed on the DPA server. If you need to upgrade the JDK:

1. Download and install JDK 11.0.17 LTS.
2. Remove old Java information by deleting the `cat.txt` and `cat.end` files from the following directory:

   `<DPA_Home>/iwc/tomcat/ignite_config/`
3. At a command line, go to the DPA installation directory.
4. Enter the following command:

   `./startup.sh`

Install DPA

You can install DPA in any of the following environments:

- Install DPA on Windows
- Install DPA on Linux
- Install DPA on Azure Marketplace

You can also Launch DPA on Amazon Web Services. AWS deployments use the AWS Marketplace Metering Service to calculate charges.

If you want to use individual DPA licenses in the Amazon cloud, you can deploy an EC2 instance, install DPA, and apply your licenses. You cannot use both individual DPA licenses and the metering service on a single DPA server.

Install DPA on Windows

The installation process creates a Windows service called Ignite PI Server. This service is set to run automatically when the server is restarted.

To install DPA on a different platform, see Install DPA on Linux, Install DPA on Azure Marketplace, or Launch DPA on Amazon Web Services.

SolarWinds strongly recommends that you install Database Performance Analyzer on a server that is **neither** public, **nor** internet-facing. To learn about best practices for configuring your Database Performance Analyzer installation securely, see Best practices to secure SolarWinds Products.

Before you start

Before you install Database Performance Analyzer, be sure to review the pre-installation checklist and the system requirements.

Powershell execution **must** be enabled on the DPA server. Powershell execution is required to install DPA and to start or restart the DPA service.

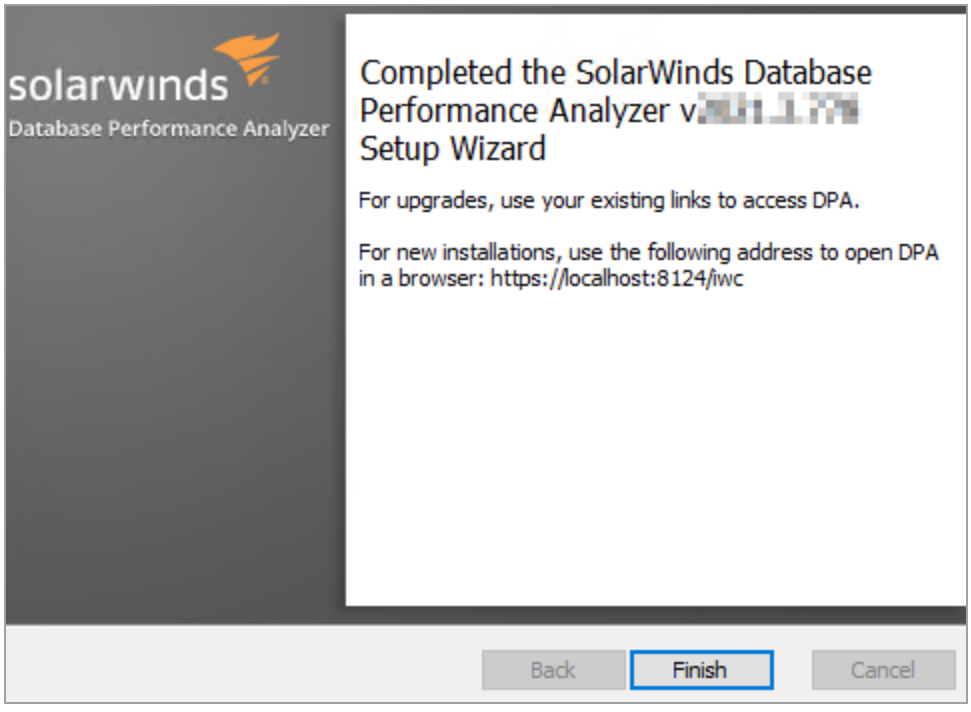
Install DPA

The log created during a Windows installation is located in `C:\Programdata\Solawinds\DPA\installer\log`.

1. Download the installation file from one of the following locations:
   - If you are installing a trial version, download it from https://www.solarwinds.com/database-performance-analyzer.
   - Otherwise, download it from the SolarWinds Customer Portal.

   If you have not yet created a SolarWinds account, see Access the Customer Portal to create an account.
2. Log in to the Windows server as an administrator.
3. Extract the contents of the downloaded installation ZIP file.
4. Run `SolarWindsDPASetup-x64.exe`. When the installer starts, click Next.
5. If you accept the terms of the license agreement, select I accept. Click Next.
6. To change the default installation directory, click Change and specify the directory.
7. Click Next, and then click Install to start the installation.

   After a successful installation, the wizard displays the default URL used to open DPA. You can use https://localhost:8124 or, instead of localhost, specify the hostname or IP address of the DPA server.



8. Click Finish to close the dialog.

Next steps

Click Open DPA, and create the repository database.

Install DPA on a Linux-based OS

To install DPA on a different platform, see Install DPA on Windows, Install DPA on Azure Marketplace, or Launch DPA on Amazon Web Services.

SolarWinds strongly recommends that you install Database Performance Analyzer on a server that is **neither** public, **nor** internet-facing. To learn about best practices for configuring your Database Performance Analyzer installation securely, see Best practices to secure SolarWinds Products.

Before you start

Before you install Database Performance Analyzer, be sure to review the pre-installation checklist.

Install the required fonts

If the required fonts are not installed, you will receive a Status 500 Internal Server Error when you attempt to start DPA. For more information, see this article.

To install the fonts that DPA requires, run one of the following commands on the DPA server:

- For Deb-based distributions (for example, Debian and Ubuntu):

  ```
  apt-get install fontconfig
  ```

- For RPM-based Linux distributions (for example, RHEL, Fedora, and CentOS):

  ```
  yum install urw-fonts
  ```

Download the installation file and verify the signature

To verify that the installation file is unmodified, use a public key to confirm that the signature of the installation file matches the signature of the corresponding `.sig` file.

1. Download the installation file and the corresponding `.sig` file from the SolarWinds Customer Portal. The file names are as follows, where *`YYYY-Q-BBBB`* is the DPA version number:
   - Installation file: `SolarWinds-DPA-`*`YYYY-Q-BBBB`*`-64bit.tar.gz`
   - Signature file: `SolarWinds-DPA-`*`YYYY-Q-BBBB`*`-64bit.tar.gz.sig`

   If you have not yet created a SolarWinds account, see Access the Customer Portal to create an account.

2. Copy one of the following public keys into a file, name the file `public.pem`, and save it in the same directory as the `tar.gz` and `tar.gz.sig` files:

   - If you are installing **DPA 2023.2 or later**, copy the following public key:

     ```
     -----BEGIN PUBLIC KEY-----
     MIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBwzDldHd3s548ogwcCVTRF2WXcfJj
     BIfElvDzX+5zjDghxCJzFO4pXSMtUFoB2fD2BGjVgdcZRDRacrv/9GS52fcBV9sY
     qRjkQVVzsodD02QokDTnTLOAig4LMvnEJWO1F8UGM5gbiaXtuUNMFNEFElCN3FH6
     a8eT4QRV5XoKNZz3mo4=
     -----END PUBLIC KEY-----
     ```

   - If you are installing **DPA 2023.1 or earlier**, copy the following public key:

     ```
     -----BEGIN PUBLIC KEY-----
     MIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQAOmd4V9OCdJF2cZ73G2IqrW9G/3Ny
     Qeh2jOwg0VJaCecsNxXmpsjvJ2YMQJHMBddB++c81ys3NLwUGsJswxm/rCMA7bN1
     q/zOV3oCoDfvXN2B6o1kTMJNebF6VDBc+c2phlrkJDjctSSVigTxYpZ33bgX9IxZ
     NImi0LvVvOSNaQi1jR4=
     -----END PUBLIC KEY-----
     ```

3. Run one of the following commands to verify the signature:

   ```
   openssl dgst -sha512 -keyform PEM -verify public.pem -signature
   <signature_file_name> <dpa_installer_file_name>

   Expect: Verified OK
   ```

   or

   ```
   openssl dgst -binary -sha512 <dpa_installer_file_name> > digest.bin
   openssl pkeyutl -verify -pubin -keyform PEM -inkey public.pem -in
   digest.bin -sigfile <signature_file_name>

   Expect: Signature Verified Successfully
   ```

Install DPA

1. Create a directory to hold this version of DPA. For example: `/home/dpa`.
2. Extract the downloaded TAR installation file into the new directory.

3. Use either of the following methods to run the `dpa_version_installer.sh` script from the command line:
   - Make it executable and run it directly:

     ```
     chmod +x dpa_version_installer.sh
     ```

     ```
     ./dpa_version_installer.sh
     ```
   - Run it in the shell:

     ```
     sh dpa_version_installer.sh
     ```
4. When prompted, create a directory on the server for installation. This becomes the DPA Home directory.
5. Start DPA by running the following command from the Home directory:

   ```
   ./startup.sh
   ```

Next steps

Go to `https://yourServer:8124` in a web browser and create the repository database.

Deploy DPA in the Azure Marketplace

You can deploy DPA on a virtual machine in the Microsoft Azure Marketplace. The VM contains a DPA server on Windows and a built-in Microsoft SQL Server database instance configured as the DPA repository.

You can access the DPA user interface on the standard HTTP port 80 and HTTPS port 443. The Windows Firewall settings have been set to allow inbound HTTP and HTTPS traffic.

> To install DPA on a different platform, see Install DPA on Windows, Install DPA on Linux or Unix, or Launch DPA on Amazon Web Services.

Create a DPA instance in the Azure Marketplace

1. Log in to the Azure Marketplace.
2. In the left column, click New.
3. In the Search the marketplace bar, enter `SolarWinds`.
4. Click Database Performance Analyzer, and then click Create in the right pane.

Create the virtual machine

Follow the five-step wizard to create the virtual machine that will host DPA.

Basics: Configure basic settings	1. Enter the basics such as VM name, VM credentials, and your location. 2. Click OK.
Size: Choose virtual machine size	1. Click a size based on your needs. 2. Click Select.
Settings: Configure optional features	1. Customize the additional settings if necessary. 2. Click OK.
Summary: Database Performance Analyzer	1. Review the summary. 2. If everything looks good, click OK.
Buy	1. Review the offer details. 2. If everything looks good, click Purchase.

Log in to the Azure DPA server

1. In the left column, click Virtual machines.
2. Click the name of the VM you just created for DPA.
3. In Overview > Essentials, copy the value in the Public IP address field.
4. Paste the IP address in a new browser tab.
5. If you agree, accept the DPA end-user license agreement.
6. Create a DPA password, select a time zone, and click Set up DPA.
7. Log in using your DPA password.
8. Start using DPA by registering a database instance for monitoring.

Create the DPA repository database

After you install DPA and open it for the first time, you must create a repository database. The repository database stores monitoring user credentials and the performance data that DPA collects from monitored database instances.

Create the repository using a wizard (password authentication)

You can use a wizard to create the repository database on any of the following database types:

- Create a SQL Server repository database
- Create an Oracle repository database
- Create a MySQL repository database
- Create an Azure SQL Database repository database

⚠ Azure SQL Managed Instance (ASMI) is **not** supported as a DPA repository database. See the system requirements for more information.

Create a repository that uses CyberArk for authentication

If you plan to configure DPA to use CyberArk, see Create a DPA repository that uses CyberArk for authentication.

Automate repository creation

If you want to automate repository creation (for example, as part of a silent installation), see Automate repository creation.

Create a SQL Server repository database

After you install DPA, you must create the repository database, which holds the performance data that DPA collects. Use this procedure to create a SQL Server repository database.

💡 If one or more monitored database instances is created with multi-byte support, the repository database should also be created with multi-byte support.

Before you start

Before you run the Repository wizard:

☐	Make sure the repository database server meets the system requirements.
☐	Install a supported version of SQL Server on the database server.
☐	If you run the wizard from a different computer (**not** the server where DPA was installed), make sure the required firewall port is open. By default, port 8124 must be open.
☐	The DPA server connects to the repository through a TCP/IP connection. Make sure that connection is not blocked by a firewall.
☐	Make sure you have credentials to a login with SYSADMIN privileges for the SQL Server database instance.

Run the wizard

1. To open DPA, enter the following URL in a web browser, where *yourServer* is the hostname or IP address of the DPA server:

   `https://yourServer:8124`

   If the repository database has not been created, the Repository wizard opens automatically.
2. Click Create New Repository.
3. Complete the remaining wizard panels as described in the following table.

Panel	Instructions
Select Repository Database Instance Type	Select Microsoft SQL Server as the database type.

Panel	Instructions
Enter Repository Connection Information	1. Enter connection information for the SQL Server instance: • If the SQL Server browser service is running, enter the server name or IP address and the instance name in this format: `Server\Instance`. • Otherwise, enter the server name or IP address and the port number. 2. Select the type of authentication you want to use. If Mixed Mode was selected during the SQL Server installation, you can choose either option. 3. Enter a SYSADMIN login that DPA can use to create the repository. ⓘ DPA does not use or store these credentials after you complete the Repository Wizard. • For Windows authentication, enter `<DOMAIN>\<username>` in the SYSADMIN User field. • For SQL Server authentication, enter the credentials that you enter on the Connect to Server dialog in SQL Server Management Studio (with Database Engine as the Server type). 4. If you are installing DPA **2021.3.7388** or **2021.3.7438** and you chose Windows Authentication and entered a domain user, add the following connection properties: a. Click Advanced Connection Properties. b. Under JDBC URL Properties, enter: `authenticationScheme=NTLM;integratedSecurity=true` ⓘ Adding these connection properties is not necessary for DPA 2021.3.7445 and later.

Panel	Instructions
Enter Repository Login	DPA can create the repository administrator account, or you can specify an existing account. To ensure that the account has the required permissions, SolarWinds recommends creating a new account. To create a new account: 1. Click Yes. 2. Select SQL Server as the authentication method. (DPA cannot create a new Windows account.) 3. Enter a user name and password for the new account. To specify an existing account: 1. Click No. 2. Select either authentication method. 3. Enter the user name and password of an existing account. For Windows authentication, enter *DOMAIN\username* in the Repository Login field. You can also authenticate using a Windows Computer Account. For SQL Server authentication, only the user name is required. Do not specify a domain.
Specify Database for the Repository	Create a new database, or select an existing, empty database if one is available: • To create a new database, enter the database name. The name is automatically prefixed by `dpa_` for identification. • The Existing empty database option is shown only if the repository contains an empty database. If your database administrator created a database for DPA, select it from the list.
Contact Information	Enter your name and email. DPA sends database performance reports to this address.
Summary	Review the information and click Create Repository.
Finished Repository Creation	After the repository has been created, click Register Database Instance to start registering instances, or close the wizard and register instances later.

Create an Oracle repository database

After you install DPA, you must create the repository database, which holds the performance data that DPA collects. Use this procedure to create an Oracle repository database.

If one or more monitored database instances is created with multi-byte support, the repository database should also be created with multi-byte support.

Oracle multitenant databases

You can create the DPA repository database on an Oracle pluggable database (PDB), but not a container database (CDB). If you create the repository on a PDB, the PDB can be moved:

- If the PDB is moved to another CDB on the same server, the connection string does not change. No action is required.
- If the PDB is moved to a CDB on a **different** server, the connection string changes. You must update the connection string in the `repo.properties` file in the following location:

  DPA-Install-Dir`\iwc\tomcat\ignite_config\iwc\repo.properties`

Before you start

Before you run the Repository Creation wizard, complete the following tasks:

- Make sure the repository database server meets the system requirements.
- Install a supported version of Oracle on the database server.
- If you run the wizard from a different computer (**not** the server where DPA was installed), make sure the required firewall port is open. By default, port 8124 must be open.
- The DPA server connects to the repository through a TCP/IP connection. Make sure that connection is not blocked by a firewall.
- Have the credentials of a **privileged user**. The privileged user is used to create the DPA repository user. DPA does **not** use or store the privileged user's credentials after the repository has been created.

Choose one of the following as the privileged user:

- Choose a user with the `DBA` role (but not `SYS`).
- Choose a user with the following privileges:

Privilege	Description	Grant level
CREATE_SESSION	Required to create a connection to the database.	User or role level
SELECT_ANY_DICTIONARY	Required to access views in the SYS schema for performance tuning.	User or role level
CREATE_TABLE	Required to create repository tables.	User or role level
CREATE_SEQUENCE	Required to create sequences in repository tables.	User or role level
DPA **2023.2.1 and earlier**: UNLIMITED_TABLESPACE DPA **2023.2.100 and later**: QUOTA UNLIMITED on the tablespace where DPA will store performance data	Required to create repository tables. In DPA 2023.2.1 and earlier, UNLIMITED_TABLESPACE is not needed if the repository user has privileges to use the tablespace provided in a request.	User level

Run the wizard

1. To open DPA, enter the following URL in a web browser, where *yourServer* is the hostname or IP address of the DPA server:

   `https://yourServer:8124`

   If the repository database has not been created, the Repository wizard opens automatically.
2. Click Create New DPA Repository.
3. As the database type, select Oracle, and click Next.

4. On the Enter Repository Connection Information pane:

   a. Select the option for connecting to the Oracle database, and enter the associated connection values:

Direct Connect	Enter the Service Name or System Identifier (SID), host name or IP address, and port. The default port is 1521. ⚠ Do not use a critical production database.
TNS Connect Descriptor	Enter the Connect Descriptor value, which contains everything after `NAME=` in the `tnsnames.ora` file. The beginning `(DESCRIPTION=` is necessary. For example: `(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = demo.myserver.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME = demo)))`
LDAP or TNS Name	Enter the LDAP or TNS name. To use this option, Oracle Name Resolution must be configured. For instructions, see Connect to Oracle using name resolution. After you configure Oracle Name Resolution, you can use the LDAP/TNS Name when registering additional monitored database instances.

   b. Enter the credentials of the privileged user that DPA will use to create the DPA repository user.

   c. Click Next.

      If your repository database server does **not** meet the minimum requirements, the Repository Database Server Warnings page is displayed.

5. If the Repository Database Server Warnings page is displayed, it shows a report of the current Oracle parameters with values below the recommended minimum. SolarWinds recommends correcting these parameters before continuing. You can continue without fixing these parameters, but parameter values below the recommend minimums may affect the performance of the repository.

Minimum Oracle Parameters	
`db_block_buffers` (or `db_cache_size`) ⚠ This is a critical parameter.	> 100 MB per monitored database

Minimum Oracle Parameters	
`shared_pool_size`	> 50 MB
`sort_area_size`	> 4 MB
`log_buffer`	> 1 MB
`session_cached_cursors`	> 10
`Redo Log Size (select min(bytes) from v$log)`	> 10 MB

When you are ready to continue, click Next.

6. On the Enter Repository Login page:
   a. Next to Create New User, click Yes if you want DPA to create the repository administrator account. Or click No if you want to specify an existing account.

      To ensure that the account has the required permissions, recommends creating a new account.

   b. Enter the user name and password.
   c. Click Next.
7. On the Specify Tablespaces for the Repository page, specify what tablespaces will store repository data:
   a. Select a tablespace where DPA will store performance data.
   b. Select a temporary tablespace for the DPA repository user.
   c. Click Next.
8. On the Contact Information page, enter the name and email address to receive database performance reports from DPA. Then click Next.
9. On the Summary page, review the information and click Create Repository.

   DPA creates a new Oracle schema and populates it with tables, indexes, and initial data.

   After the repository has been created, click Register Database Instance to start registering instances, or close the wizard and register instances later.

Create a MySQL repository database

After you install DPA, you must create the repository database, which holds the performance data that DPA collects. Use this procedure to create a MySQL repository database.

If one or more monitored database instances is created with multi-byte support, the repository database should also be created with multi-byte support.

Before you start

Before you run the Repository wizard:

- ☐ Make sure the repository database server meets the system requirements.
- ☐ Install a supported version of MySQL on the database server.
- ☐ If you run the wizard from a different computer (**not** the server where DPA was installed), make sure the required firewall port is open. By default, port 8124 must be open.
- ☐ The DPA server connects to the repository through a TCP/IP connection. Make sure that connection is not blocked by a firewall.

Run the wizard

1. To open DPA, enter the following URL in a web browser, where *yourServer* is the hostname or IP address of the DPA server:

   `https://yourServer:8124`

   If the repository database has not been created, the Repository wizard opens automatically.
2. Click Create New Repository.
3. Complete the remaining wizard panels as described in the following table.

Panel	Instructions
Select Repository Database Instance Type	Select MySQL as the database type.

Panel	Instructions

Enter Repository Connection Information	DPA creates a new database and populates it with tables, indexes, and initial data.
	1. Enter the server name or IP address and port.
	2. Select a method for creating or configuring the MySQL repository user.
	If you are using MySQL 8.0 as the repository database, you must create the repository user manually, and you must include the following in the `CREATE USER` command:
	`IDENTIFIED WITH mysql_native_password BY 'yourPassword';`
	To create a new account:
	1. Click Provide a privileged user.
	2. Enter the credentials of an existing user with privileges to create the repository user and grant the required permissions. The credentials for the privileged user are not used or stored after the registration.
	The privileged user requires the Create, Drop, and Create User permissions and must be able to grant the following permissions:
	`GRANT ALL PRIVILEGES on databaseName`
	Where *`databaseName`* is the repository database you create or select when you set up the MySQL repository storage.
	To specify and existing account:
	1. Click Provide the repository user.
	2. Enter credentials. DPA encrypts the password.
	Alternatively, you can use the script that DPA provides to create a repository user.
	1. Click Repository DB and User Creation Script, and follow the on-screen instructions.
	2. Copy the edited script to the MySQL console, and run it.
	3. Provide this user as your repository user.

Panel	Instructions
Enter Repository Login	If you provided the repository user in the previous step, the wizard skips this step. DPA can create the repository administrator account, or you can specify an existing account. To ensure that the account has the required permissions, SolarWinds recommends creating a new account. To create a new account: 1. Next to Create New User, click Yes. 2. Enter the user name and password. To specify an existing account: 1. Next to Create New User, click No. 2. Enter the user name and password.
Specify Database for the Repository	To store the repository in a new database, enter a database name. DPA prefixes the name with `dpa_` for identification. To store the repository in an existing database, select a database from the list. ⓘ This option is available only if the repository instance contains an empty database. • If your MySQL Administrator created a database for DPA, select the database from the list. • If you provided a privileged user, DPA only displays tables with Select permissions granted to the privileged user. • If you provided the repository user, DPA only displays tables with Select permissions granted to the repository user. • No database permissions are required while using the privileged user. DPA grants the required permissions to the specified user when creating the repository. • The All privilege is required to use the database.
Contact Information	Enter your name and email. DPA sends database performance reports to this address.
Summary	Review the information and click Create Repository.
Finished Repository Creation	After the repository has been created, click Register Database Instance to start registering instances, or close the wizard and register instances later.

Create an Azure SQL Database repository database

After you install DPA, you must create the repository database, which holds the performance data that DPA collects. Use this procedure to create an Azure SQL Database repository database.

⚠ Azure SQL Managed Instance (ASMI) is **not** supported as a DPA repository database. See the system requirements for more information.

If one or more monitored database instances is created with multi-byte support, the repository database should also be created with multi-byte support.

Before you start

Before you run the Repository wizard:

☐	Create a database in Azure SQL Database.
☐	The DPA server connects to the repository through a TCP/IP connection. Make sure that connection is not blocked by a firewall.

Run the wizard

1. To open DPA, enter the following URL in a web browser, where `yourServer` is the hostname or IP address of the DPA server:

   `https://yourServer:8124`

   If the repository database has not been created, the Repository wizard opens automatically.
2. Click Create New Repository.
3. Complete the remaining wizard panels as described in the following table.

Panel	Instructions
Select Repository Database Instance Type	Select Azure SQL as the database type.

Panel	Instructions
Enter Repository Connection Information	Before connecting, the database must exist in Azure and be empty. 1. Enter the server name, port, and database name. You cannot use an IP address in the Server Name field. 2. Select a method for creating or configuring the repository administrator. To create a new account: 1. Click Let DPA create and configure the user for me. 2. Enter the credentials of an existing user with privileges to create the repository user and to grant the required permissions. This user must be a member of the db_owner role. To specify an existing account, enter the user name and password of an existing account that DPA will use the interact with the repository. Alternatively, you can use the provided script to create the repository user. 1. Click Repository User Creation Script, and follow the on-screen instructions. 2. Copy and run the edited script on your Azure SQL database. 3. Provide this user as your repository administrator.
Enter Repository Login	DPA can create the repository administrator account, or you can specify an existing account. To ensure that the account has the required permissions, SolarWinds recommends creating a new account. To create a new account: 1. Click Let DPA create a new user. 2. Enter a user name and password for the new account. To specify an existing account: 1. Click Let DPA configure an existing user. 2. Enter the user name and password of an existing account.
Contact Information	Enter your name and email. DPA sends database performance reports to this address.
Summary	Review the information and click Create Repository.

Panel	Instructions
Finished Repository Creation	After the repository has been created, click Register Database Instance to start registering instances, or close the wizard and register instances later.

Create a DPA repository that uses CyberArk for authentication

If you plan to configure DPA to use CyberArk, you can use credentials stored in CyberArk to authenticate the repository administrator account. To create a repository that uses CyberArk credentials, you must run a script to create the required database structures, and then use the DPA REST API to create the repository.

If you created the DPA repository before integrating DPA with CyberArk, you can update the existing repository to use CyberArk credentials.

1. Make sure the following prerequisites are met:
   - Make sure a supported database version is installed on the database server and that it meets all other system requirements.
   - If you create the repository on a different computer (**not** the server where DPA was installed), make sure the required firewall port is open. By default, port 8124 must be open.
   - The DPA server connects to the repository through a TCP/IP connection. Make sure that connection is not blocked by a firewall.
2. Run a script to create the required database structures:
   a. Depending on your repository database type, copy one of the scripts under Scripts to create the required database structures.
   b. Edit the script to replace the placeholders in angle brackets (for example, `<DATABASE NAME>`) with the actual values.
   c. Connect to the database as a user with the necessary privileges:
      - SQL Server: SYSADMIN
      - Oracle: database administrator (DBA)
      - MySQL: repository administrator
      - Azure SQL DB: repository administrator
   d. Run the script.

3. Send an API request to create the DPA repository. See API request to create the repository for information about the information the request must include, and examples of the request sent using the curl command line tool.

   For more information about working with the DPA REST API, see Automate tasks with the DPA REST API.

Scripts to create the required database structures

Before you send an API request to create the repository, edit and run one of the following scripts to prepare the database server and create structures needed by the DPA repository. The scripts create an empty database (or tablespace) and a repository user with the required permissions.

SQL Server

```
create database <DATABASE NAME>;
create login <REPOSITORY USER NAME> with password=N'<REPOSITORY USER
PASSWORD>', default_database=<DATABASE NAME>, check_expiration=off, check_
policy=off;
use [<DATABASE NAME>];
create schema ignite;
create user <REPOSITORY USER NAME> for login <REPOSITORY USER NAME> with
default_schema = ignite;
sp_addrolemember "db_owner", <REPOSITORY USER NAME>;
```

Oracle

```
CREATE TABLESPACE <TABLESPACE NAME>
DATAFILE '<TABLESPACE FILE NAME>.dat' SIZE 500M AUTOEXTEND ON ONLINE;
CREATE USER <REPOSITORY USER NAME> IDENTIFIED BY <REPOSITORY USER PASSWORD>;
GRANT CREATE TABLE TO <REPOSITORY USER NAME>;
GRANT CREATE SEQUENCE TO <REPOSITORY USER NAME>;
GRANT CREATE SESSION TO <REPOSITORY USER NAME>;
GRANT SELECT ANY DICTIONARY TO <REPOSITORY USER NAME>;
```

MySQL 5.7 and earlier

```
CREATE DATABASE <DATABASE NAME> CHARACTER SET utf8 COLLATE utf8_unicode_ci;
CREATE USER '<REPOSITORY USER NAME>'@'%' IDENTIFIED BY '<REPOSITORY USER
PASSWORD>';
GRANT ALL PRIVILEGES ON <DATABASE NAME>.* TO '<REPOSITORY USER NAME>'@'%';
```

MySQL 8

For MySQL 8, the authentication plugin must be specified for the user.

```
CREATE DATABASE <DATABASE NAME> CHARACTER SET utf8 COLLATE utf8_unicode_ci;
CREATE USER '<REPOSITORY USER NAME>'@'%' IDENTIFIED WITH mysql_native_
password BY '<REPOSITORY USER PASSWORD>';
GRANT ALL PRIVILEGES ON <DATABASE NAME>.* TO '<REPOSITORY USER NAME>'@'%';
```

Azure SQL DB

```
create database <DATABASE NAME>;
use[<DATABASE NAME>];
create user [<REPOSITORY USER NAME>] with password=N'<REPOSITORY USER
PASSWORD>', default_schema = [ignite];
alter role db_owner add member <REPOSITORY USER NAME>;
go
create schema [ignite] authorization [<REPOSITORY USER NAME>];
```

API request to create the repository

The API request to create the repository must include the following information. You can use the curl command line tool or any other REST client capable of sending requests. Examples are provided in the following section.

Element	Value
Endpoint URL	`http://<DPA Server>:<DPA port>/iwc/rest/repository/create`
Method	`POST`
Headers	`Content-Type: application/json`

Element	Value

Body for a SQL Server repository	{
	"databaseType": "SQLSERVER",
	"hostName": "<DATABASE HOSTNAME>",
	"port": "<DATABASE PORT>",
	"database": "<DATABASE NAME>",
	"cyberArkQuery": "<CYBERARK QUERY>",
	"contactEmail": "<EMAIL>",
	"contactName": "<NAME>"
	}

Body for an Oracle repository	{
	"databaseType": "ORACLE",
	"hostName": "<DATABASE HOSTNAME>",
	"port": "<DATABASE PORT>",
	"sid": "<SID>",
	"tablespace": "<TABLESPACE>",
	"cyberArkQuery": "<CYBERARK QUERY>",
	"contactEmail": "<EMAIL>",
	"contactName": "<NAME>"
	}

Body for a MySQL repository	{
	"databaseType": "MYSQL",
	"hostName": "<DATABASE HOSTNAME>",
	"port": "<DATABASE PORT>",
	"database": "<DATABASE NAME>",
	"cyberArkQuery": "<CYBERARK QUERY>",
	"contactEmail": "<EMAIL>",
	"contactName": "<NAME>"
	}

Element	Value
Body for an Azure SQL DB repository	`{ "databaseType": "AZURESQLDB", "hostName": "<DATABASE HOSTNAME>", "port": "<DATABASE PORT>", "database": "<DATABASE NAME>", "cyberArkQuery": "<CYBERARK QUERY>", "contactEmail": "<EMAIL>", "contactName": "<NAME>" }`

Examples of repository creation requests

The following examples use the curl command line tool to send a repository creation request to the DPA API. The placeholders enclosed in angle brackets (for example `<DATABASE HOSTNAME>`) must be replaced with actual values.

SQL Server example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"SQLSERVER\", \"hostName\": \"<DATABASE HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"database\": \"<DATABASE NAME>\",
\"cyberArkQuery\": \"<CYBERARK QUERY>\", \"contactEmail\": \"<EMAIL>\",
\"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

Oracle example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"ORACLE\", \"hostName\": \"<DATABASE HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"sid\": \"<SID>\", \"tablespace\":
\"<TABLESPACE>\",
\"cyberArkQuery\": \"<CYBERARK QUERY>\", \"contactEmail\": \"<EMAIL>\",
\"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

MySQL example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"MYSQL\", \"hostName\": \"<DATABASE HOSTNAME>\",
```

```
\"port\": \"<DATABASE PORT>\", \"database\": \"<DATABASE NAME>\",
\"cyberArkQuery\": \"<CYBERARK QUERY>\", \"contactEmail\": \"<EMAIL>\",
\"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

Azure SQL DB example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"AZURESQLDB\", \"hostName\": \"<DATABASE
HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"database\": \"<DATABASE NAME>\",
\"cyberArkQuery\": \"<CYBERARK QUERY>\", \"contactEmail\": \"<EMAIL>\",
\"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

The scripts are not supported under any SolarWinds support program or service. The scripts are provided AS IS without warranty of any kind. SolarWinds further disclaims all warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The risk arising out of the use or performance of the scripts and documentation stays with you. In no event shall SolarWinds or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the scripts or documentation.

Automate repository creation

To automate the creation of the DPA repository (sometimes called silent creation), you can run a script to create the required database structures, and then use the DPA REST API to create the repository.

ⓘ The repository created with this procedure does **not** use CyberArk for authentication. If your organization plans to integrate DPA with CyberArk, see Create a DPA repository that uses CyberArk for authentication.

1. Make sure the following prerequisites are met:
   - Make sure a supported database version is installed on the database server and that it meets all other system requirements.
   - If you create the repository on a different computer (**not** the server where DPA was installed), make sure the required firewall port is open. By default, port 8124 must be open.
   - The DPA server connects to the repository through a TCP/IP connection. Make sure that connection is not blocked by a firewall.
2. Run a script to create the required database structures:
   a. Depending on your repository database type, copy one of the scripts under Scripts to create the required database structures.
   b. Edit the script to replace the placeholders in angle brackets (for example, `<DATABASE NAME>`) with the actual values.
   c. Connect to the database as a user with the necessary privileges:
      - SQL Server: SYSADMIN
      - Oracle: database administrator (DBA)
      - MySQL: repository administrator
      - Azure SQL DB: repository administrator
   d. Run the script.
3. Send an API request to create the DPA repository. See API request to create the repository for information about the information the request must include, and examples of the request sent using the curl command line tool.

   For more information about working with the DPA REST API, see Automate tasks with the DPA REST API.

Scripts to create the required database structures

Before you send an API request to create the repository, edit and run one of the following scripts to prepare the database server and create structures needed by the DPA repository. The scripts create an empty database (or tablespace) and a repository user with the required permissions.

SQL Server

```
create database <DATABASE NAME>;
create login <REPOSITORY USER NAME> with password=N'<REPOSITORY USER
PASSWORD>', default_database=<DATABASE NAME>, check_expiration=off, check_
policy=off;
```

```
use [<DATABASE NAME>];
create schema ignite;
create user <REPOSITORY USER NAME> for login <REPOSITORY USER NAME> with
default_schema = ignite;
sp_addrolemember "db_owner", <REPOSITORY USER NAME>;
```

Oracle

```
CREATE TABLESPACE <TABLESPACE NAME>
DATAFILE '<TABLESPACE FILE NAME>.dat' SIZE 500M AUTOEXTEND ON ONLINE;
CREATE USER <REPOSITORY USER NAME> IDENTIFIED BY <REPOSITORY USER PASSWORD>;
GRANT CREATE TABLE TO <REPOSITORY USER NAME>;
GRANT CREATE SEQUENCE TO <REPOSITORY USER NAME>;
GRANT CREATE SESSION TO <REPOSITORY USER NAME>;
GRANT SELECT ANY DICTIONARY TO <REPOSITORY USER NAME>;
```

MySQL 5.7 and earlier

```
CREATE DATABASE <DATABASE NAME> CHARACTER SET utf8 COLLATE utf8_unicode_ci;
CREATE USER '<REPOSITORY USER NAME>'@'%' IDENTIFIED BY '<REPOSITORY USER
PASSWORD>';
GRANT ALL PRIVILEGES ON <DATABASE NAME>.* TO '<REPOSITORY USER NAME>'@'%';
```

MySQL 8

For MySQL 8, the authentication plugin must be specified for the user.

```
CREATE DATABASE <DATABASE NAME> CHARACTER SET utf8 COLLATE utf8_unicode_ci;
CREATE USER '<REPOSITORY USER NAME>'@'%' IDENTIFIED WITH mysql_native_
password BY '<REPOSITORY USER PASSWORD>';
GRANT ALL PRIVILEGES ON <DATABASE NAME>.* TO '<REPOSITORY USER NAME>'@'%';
```

Azure SQL DB

```
create database <DATABASE NAME>;
use[<DATABASE NAME>];
create user [<REPOSITORY USER NAME>] with password=N'<REPOSITORY USER
PASSWORD>', default_schema = [ignite];
alter role db_owner add member <REPOSITORY USER NAME>;
```

```
go
create schema [ignite] authorization [<REPOSITORY USER NAME>];
```

API request to create the repository

The API request to create the repository must include the following information. You can use the curl command line tool or any other REST client capable of sending requests. Examples are provided in the following section.

Element	Value
Endpoint URL	`http://<DPA Server>:<DPA port>/iwc/rest/repository/create`
Method	`POST`
Headers	`Content-Type: application/json`

Body for a classic SQL Server repository	<pre>{
	  "databaseType": "SQLSERVER",
	  "serverName": "<DATABASE HOSTNAME>",
	  "port": "<DATABASE PORT>",
	  "database": "<DATABASE NAME>",
	  "repositoryUser": "<USER NAME>",
	  "repositoryPassword": "<PASSWORD>",
	  "authenticationSchema": "PASSWORD",
	  "contactEmail": "<EMAIL>",
	  "contactName": "<NAME>"
	}</pre>

Element	Value

Body for a SQL Server named instance repository	{
	"databaseType": "SQLSERVER",
	"serverName": "<IP ADDRESS>\<INSTANCE NAME>",
	"port": "<DATABASE PORT>",
	"database": "<DATABASE NAME>",
	"repositoryUser": "<USER NAME>",
	"repositoryPassword": "<PASSWORD>",
	"authenticationSchema": "PASSWORD",
	"contactEmail": "<EMAIL>",
	"contactName": "<NAME>"
	}

Body for a SQL Server classic repository using Windows authentication	{
	"databaseType": "SQLSERVER",
	"serverName": "<DATABASE HOSTNAME>",
	"port": "<DATABASE PORT>",
	"database": "<DATABASE NAME>",
	"repositoryUser": "<USER NAME>",
	"repositoryPassword": "<PASSWORD>",
	"authenticationSchema": "PASSWORD",
	"jdbcUrlProperties": "useNTLMv2=true",
	"contactEmail": "<EMAIL>",
	"contactName": "<NAME>"
	}

Body for an Oracle repository	{
	"databaseType": "ORACLE",
	"hostName": "<DATABASE HOSTNAME>",
	"port": "<DATABASE PORT>",
	"serviceName": "<SERVICE NAME>",
	"repositoryUser": "<USER NAME>",
	"repositoryPassword": "<PASSWORD>",
	"authenticationSchema": "PASSWORD",
	"tablespace": "<TABLESPACE>",
	"contactEmail": "<EMAIL>",
	"contactName": "<NAME>"
	}

Element	Value

Body for a MySQL repository	<pre>{
	  "databaseType": "MYSQL",
	  "hostName": "<DATABASE HOSTNAME>",
	  "port": "<DATABASE PORT>",
	  "database": "<DATABASE NAME>",
	  "repositoryUser": "<USER NAME>",
	  "repositoryPassword": "<PASSWORD>",
	  "authenticationSchema": "PASSWORD",
	  "contactEmail": "<EMAIL>",
	  "contactName": "<NAME>"
	}</pre>

Body for an Azure SQL DB repository	<pre>{
	  "databaseType": "AZURESQLDB",
	  "hostName": "<DATABASE HOSTNAME>",
	  "port": "<DATABASE PORT>",
	  "database": "<DATABASE NAME>",
	  "repositoryUser": "<USER NAME>",
	  "repositoryPassword": "<PASSWORD>",
	  "contactEmail": "<EMAIL>",
	  "contactName": "<NAME>"
	}</pre>

Examples of repository creation requests

The following examples use the curl command line tool to send a repository creation request to the DPA API. The placeholders enclosed in angle brackets (for example `<DATABASE HOSTNAME>`) must be replaced with actual values.

SQL Server example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"SQLSERVER\", \"hostName\": \"<DATABASE HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"database\": \"<DATABASE NAME>\",
\"repositoryUser\": \"<USER NAME>\", \"repositoryPassword\": \"<PASSWORD>\",
\"authenticationSchema\": \"PASSWORD\", \"contactEmail\": \"<EMAIL>\",
\"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

Oracle example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"ORACLE\", \"hostName\": \"<DATABASE HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"serviceName\": \"<SERVICE NAME>\",
\"repositoryUser\": \"<USER NAME>\", \"repositoryPassword\": \"<PASSWORD>\",
\"authenticationSchema\": \"PASSWORD\", \"tablespace\": \"<TABLESPACE>\",
\"contactEmail\": \"<EMAIL>\", \"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

MySQL example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"MYSQL\", \"hostName\": \"<DATABASE HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"database\": \"<DATABASE NAME>\",
\"repositoryUser\": \"<USER NAME>\", \"repositoryPassword\": \"<PASSWORD>\",
\"authenticationSchema\": \"PASSWORD\", \"contactEmail\": \"<EMAIL>\",
\"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

Azure SQL DB example using curl

```
curl -X POST -H 'Content-Type: application/json'
-d '{ \"databaseType\": \"AZURESQLDB\", \"hostName\": \"<DATABASE
HOSTNAME>\",
\"port\": \"<DATABASE PORT>\", \"database\": \"<DATABASE NAME>\",
\"repositoryUser\": \"<USER NAME>\", \"repositoryPassword\": \"<PASSWORD>\",
\"contactEmail\": \"<EMAIL>\", \"contactName\": \"<NAME>\" }'
http://localhost:8124/iwc/rest/repository/create
```

The scripts are not supported under any SolarWinds support program or service. The scripts are provided AS IS without warranty of any kind. SolarWinds further disclaims all warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The risk arising out of the use or performance of the scripts and documentation stays with you. In no event shall SolarWinds or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the scripts or documentation.

Uninstall DPA

You might need to uninstall and then reinstall DPA to resolve an issue or to move to a new server during a migration. To uninstall DPA from a self-managed server, see the following sections:

- Before you uninstall
- Uninstall DPA on a Windows server
- Uninstall DPA on a Unix or Linux server

Before you uninstall

Before you uninstall DPA, SolarWinds recommends the following preparation:

☐	Back up the existing database	To preserve your data, back up your DPA repository database. If you need help with backups, check your vendor's site for documentation and instructions. If your database is on a VM, create a snapshot or copy of your VM.
☐	Back up the DPA directory	Create a copy of the DPA home directory. You could have customizations in this directory specific to your installation.

Uninstall DPA on a Windows server

To remove DPA from a Windows server, complete the following steps.

1. Deactivate all monitored instance licenses.
2. Stop the Ignite PI Server service.
3. Uninstall DPA.
    a. From the Windows Control Panel, open Uninstall or change a program.
    b. Right-click SolarWinds Database Performance Analyzer, and choose Uninstall.
    c. Click Yes at the confirmation prompt.
4. Delete the DPA home directory. The default home directory is:

    ```
    C:\Program Files\SolarWinds\DPA\
    ```

5. Restart the server.

    You can now reinstall DPA.

Uninstall DPA on a Linux server

1. Deactivate all monitored instance licenses.
2. Stop DPA by running the `shutdown.sh` command from the DPA directory.
3. Remove all cron jobs that start DPA.
4. Delete the DPA home directory.
5. Restart the server.

   You can now reinstall DPA.

Upgrade DPA

Use the following information to prepare for your upgrade.

Supported upgrade paths

The supported upgrade paths are:

- DPA 2022.3 → 2024.2
- DPA 2022.4 → 2024.2
- DPA 2023.1 → 2024.2
- DPA 2023.2.1 → 2024.2
- DPA 2023.2.100 → 2024.2
- DPA 2023.4.300 → 2024.2

ⓘ If you are upgrading from a version of DPA that is no longer supported, contact SolarWinds Support for assistance with your upgrade.

DPAIM compatibility

If you are **not** monitoring PostgreSQL database instances, DPAIM 11.1 or later is fully compatible with the current version of DPA.

If you are monitoring PostgreSQL database instances, DPAIM 2020.2 or later is required to display all available data from PostgreSQL instances in the SolarWinds Platform.

My upgrade plan checklist

Use this checklist to help plan and prepare for your upgrade.

☐	Review the **release notes** for information about new features, fixed issues, and known issues.
☐	Review the **system requirements** to make sure your environment meets all hardware and software requirements.

☐	Review your current **product licenses** and determine if you need to make any changes. You can download any updated license keys for your upgrade through your Customer Portal. Verify any license upgrades and needs with your SolarWinds account manager or contact SolarWinds.
☐	Gather **credentials**. Make sure you have your SolarWinds account and local administrator credentials for the DPA server.
☐	Check for and run all Windows or Linux **operating system updates**.
☐	**Schedule** the upgrade. Set up the maintenance window, preferably during off-peak hours. The duration depends on the size of your repository database and the number of monitored database instances. ⓘ Upgrades will require database monitoring to be offline for a short period of time.
☐	**Notify** your company of the upgrade schedule and maintenance window. If you need additional help, contact and allocate specific staff to be available.

How long does an upgrade take?

DPA upgrades typically take fewer than 10 minutes. The time it takes to complete an upgrade depends on:

- Hardware
- DPA server performance
- Repository database server performance and database size
- Number of monitored database instances

Because every configuration is different, we cannot predict exactly how long your upgrade will take.

ⓘ If you are upgrading on a Linux server and FindSQL index files are stored in the `ignite_config` folder (which is the default location), copying the `ignite_config` folder can take more than 10 minutes because of the index file sizes.

Prepare your environment to upgrade

When you are ready to upgrade, complete these steps. They include the common actions you need to complete before upgrading DPA.

If you have a test or staging environment, we highly recommend testing the upgrade first. You cannot roll back an installation once completed.

☐	Back up your DPA server. If you have your DPA server on a VM, create a snapshot or copy of your VM.
☐	Back up your repository database. If you need help, please check your vendor's site for documentation and instructions. ⚠ You cannot roll back an upgrade. Always create a repository database backup.
☐	Stop DPA.

Upgrade DPA

Follow the upgrade instructions based on the operating system of your DPA server:

1. Select your environment below to upgrade DPA.
   - Upgrade DPA on Windows
   - Upgrade DPA on Linux
   - Upgrade DPA on an Amazon Machine Image instance
   - Upgrade DPA on an Azure VM
2. If you have the DPA Integration Module in the SolarWinds Platform Web Console, upgrade that after the DPA upgrade is complete.

After the upgrade, check your system

Open DPA and verify the version displayed on the login screen or in the header on the home page. Try current and new features to check performance and expected functionality.

Upgrade DPA on Windows

⚠ If you are upgrading from DPA 2022.3 and you configured DPA 2022.3 for SAML authentication, be aware that DPA 2022.4 and later include changes to the SAML configuration. After the upgrade, no one will be able to log in with SAML until you update the configuration.

- **Before** you upgrade, make sure you have a local login available.
- **After** the upgrade, log in as a local user and complete the steps under "SAML configuration changes" in the DPA 2022.4 Release Notes to update the SAML configuration.

ⓘ The log created during a Windows installation is located in `C:\Programdata\Solawinds\DPA\installer\log`.

1. Review the upgrade checklist and prepare your environment.
2. Download the most recent version of DPA from the SolarWinds Customer Portal.
3. Log in to the Windows server as an administrator.
4. Run the installer.
5. Extract the contents of the downloaded installation ZIP file.
6. Run `SolarWindsDPASetup-x64.exe`. When the installer starts, click Next.
7. If you accept the terms of the license agreement, select I accept. Click Next.
8. Click Next, and then click Install to start the upgrade.
9. When the upgrade is complete, click Finish.

> If one or more DPA licenses are expired, you must remove the expired licenses before DPA can complete the repository upgrade. When all licenses are compliant, you can complete the upgrade process by opening DPA and clicking Proceed with upgrade.

Upgrade DPA on a Linux-based OS

> If you are upgrading from DPA 2022.3 and you configured DPA 2022.3 for SAML authentication, be aware that DPA 2022.4 and later include changes to the SAML configuration. After the upgrade, no one will be able to log in with SAML until you update the configuration.
>
> - **Before** you upgrade, make sure you have a local login available.
> - **After** the upgrade, log in as a local user and complete the steps under "SAML configuration changes" in the DPA 2022.4 Release Notes to update the SAML configuration.

1. Review the upgrade checklist and prepare your environment.
2. Download the most recent version of DPA from the SolarWinds Customer Portal.
3. Log in to the DPA server as a user that owns all of the files in the DPA installation directory.

   If the Find SQL indexes were moved to a custom location, the user must also own all of the files in the custom location.

To determine if the Find SQL indexes were moved and where, open the following file in a text editor:

`/home/solarwinds/dpa_V_v/DPA/iwc/tomcat/ignite_config/idc/system.properties`

Look for either of the following lines:

- `com.solarwinds.dpa.findSql.index.location=`*`your_custom_location`* (if all indexes were moved to the same directory)
- `com.solarwinds.dpa.findSql.index.location.`*`db_id`*`=`*`your_custom_location`* (if indexes for a specific database were moved)

If neither of those lines are present, the indexes are in the default location:

`/home/solarwinds/dpa_V_v/DPA/iwc/tomcat/ignite_config/lucene-index/`

4. Install the new version in a new directory on your existing server.
5. Run `./shutdown.sh` from the old installation directory.
6. Locate the directory that was created when you installed the new version:

   `/home/dpa_`*`x_x`* = old installation home

   `/home/dpa_`*`y_y`* = new DPA home
7. Copy or move these directories from the old installation to the new:

   ```
   /iwc/tomcat/conf/
   /iwc/tomcat/ignite_config/
   /iwc/tomcat/logs/
   /iwc/tomcat/licensing
   ```

   Do not copy hotfix files.

   For example:

   `mv `*`OLD_home`*`/iwc/tomcat/ignite_config/* `*`NEW_home`*`/iwc/tomcat/ignite_config/`

   or

   `cp -rp `*`OLD_home`*`/iwc/tomcat/ignite_config/* `*`NEW_home`*`/iwc/tomcat/ignite_config/`

   Copying Find SQL index data might take some time.

8. If you are upgrading from **DPA 2023.2.100 or earlier** to **DPA 2023.4** or later, complete the following steps:
   a. Open `/iwc/tomcat/conf/context.xml` in a text editor.
   b. Delete the following string:

      ```
      useRelativeRedirects="false"
      ```

      This string fixed an issue in previous versions of Tomcat. It is no longer needed, and it should be removed for security reasons.

   c. Save the file.
9. If you encrypted the keystore password for SSL/TLS in the Tomcat server configuration file used by DPA, copy or move the following file from the old installation to the new:

   ```
   /iwc/tomcat/lib/swdpa-customutil-1.0.0.jar
   ```

10. If you changed the default SolarWinds DPA ports, then you must modify the `server.xml` file in the new installation to incorporate the port changes from your earlier installation.
11. Run `./startup.sh` from the new directory.

To complete the upgrade:

- Update any system startup files or cron job scripts that were created for the older version.
- Ensure the older version of DPA cannot start because this will cause conflicts with your ports, monitored instances, and the repository.
- If you have configured DPA to use a custom certificate for SSL/TLS, migrate the custom certificate.

If one or more DPA licenses are expired, you must remove the expired licenses before DPA can complete the repository upgrade. When all licenses are compliant, you can complete the upgrade process by opening DPA and clicking Proceed with upgrade.

Upgrade DPA on an Amazon Machine Image instance

⚠ If you are upgrading from DPA 2022.3 and you configured DPA 2022.3 for SAML authentication, be aware that DPA 2022.4 and later include changes to the SAML configuration. After the upgrade, no one will be able to log in with SAML until you update the configuration.

- **Before** you upgrade, make sure you have a local login available.
- **After** the upgrade, log in as a local user and complete the steps under "SAML configuration changes" in the DPA 2022.4 Release Notes to update the SAML configuration.

If you're using DPA in Amazon Web Services (AWS) with AWS Marketplace Metering Service, complete the following steps to upgrade to the latest version.

1. Open a remote connection (SSH) and log in to your DPA instance in Amazon EC2.
2. Download the most recent version of SolarWinds DPA. Use the link provided in the new version notification banner.

   ⓘ If the server you are upgrading on has Internet access, you can download DPA directly to that server. If not, you can download DPA to a different computer and then use SCP to transfer it.

3. Enter the following command to turn off the scheduled job that restarts DPA if it stops:

   ```
   cmd> crontab -r
   ```

4. Install the new version in a new directory on your existing server.
5. Run `./shutdown.sh` from the old installation directory.
6. Locate the directory that was created when you installed the new version:

   `/home/dpa_x_x_xxx` = old installation home

   `/home/dpa_12_x_xxx` = new DPA home

7. Copy or move these directories from the old installation to the new:

   ```
   /iwc/tomcat/ignite_config/
   /iwc/tomcat/logs/
   ```

   ⚠ Do not copy hotfix files.

   For example:

   ```
   mv OLD_home/iwc/tomcat/ignite_config/* NEW_home/iwc/tomcat/ignite_config/
   ```

or

```
cp -rp OLD_home/iwc/tomcat/ignite_config NEW_home/iwc/tomcat/ignite_config
```

8. If you changed the default SolarWinds DPA ports, then you must modify the `server.xml` file in the new installation to incorporate the port changes from your earlier installation.
9. Run `./startup.sh` from the new directory.
10. Turn the cron job back on:
    a. Open crontab in edit mode:

    ```
    cmd> crontab -e
    ```

    b. Add the following line:

    ```
    * * * * * <FULL_PATH_TO_STARTUP_SCRIPT> > <FULL_PATH_TO_STARTUP_LOG>
    2>&1
    ```

    For example:

    ```
    * * * * * /home/ec2-user/dpa_12_0_3074/startup.sh > /home/ec2-user/dpa_
    12_0_3074/startup.log 2>&1
    ```

    c. Save your changes.

Resize to a larger Amazon AWS instance type

The t2.medium Amazon EC2 instance type is sufficient only for monitoring up to 20 database instances. Resize your AWS instance type as your monitoring needs grow.

For more information, search "Resizing Your Instance" at http://aws.amazon.com/documentation.

Upgrade DPA on an Azure VM

⚠ If you are upgrading from DPA 2022.3 and you configured DPA 2022.3 for SAML authentication, be aware that DPA 2022.4 and later include changes to the SAML configuration. After the upgrade, no one will be able to log in with SAML until you update the configuration.

- **Before** you upgrade, make sure you have a local login available.
- **After** the upgrade, log in as a local user and complete the steps under "SAML configuration changes" in the DPA 2022.4 Release Notes to update the SAML configuration.

1. Review the upgrade checklist and prepare your environment.
2. Open a remote desktop session and log in to your DPA instance in the Azure Marketplace.

3. Download the most recent version of DPA from the SolarWinds Customer Portal.
4. Run the installer, and follow the wizard.