

OpenText™ Database Activity Monitoring

Installation Guide

Version : 25.2

PDF Generated on : 25/06/2025

Table of Contents

1. Installation Guide	3
1.1. Prerequisites	4
1.2. Requirements	5
1.2.1. Supported Operating System	6
1.2.2. Disk Partitioning	7
1.2.3. Static IP Address Settings	8
1.2.4. Region and Timezone Settings	9
1.2.5. Administrative Privileges	10
1.3. Configuration	11
1.4. Installation	14
1.5. Licensing	15
1.6. Elasticsearch Security Configuration	16
1.7. Upgrading DAM Components	17

1. Installation Guide

OpenText™ Database Activity Monitoring (DAM) is a security solution used to monitor and analyze database activity for potential security threats or policy violations. DAM captures events in real-time, allowing organizations to detect and respond to suspicious activities and compliance violations. With the increasing volume and complexity of data and database systems, DAM has become essential in protecting sensitive information and ensuring regulatory compliance.

This document provides information about:

- meeting installation prerequisites
- configuration settings for installation
- installing Database Activity Monitoring

Abbreviations

Information about the abbreviations used in this guide are given in the table below.

Abbreviations	Definition
DAM	Database Activity Monitoring
IIS	Internet Information Services
IP	Internet Protocol
IPv4	Internet Protocol Version Four
SSMS	SQL Server Management Studio

1.1. Prerequisites

Before installing Database Activity Monitoring, you must make sure that you have met the following prerequisites on the machine on which the installation is performed.

This section includes:

- [Obtain OpenText™ Database Activity Monitoring software](#)
- [Database Activity Monitoring installation overview](#)

Obtain OpenText™ Database Activity Monitoring software

The latest software for OpenText™ Database Activity Monitoring `DAM_25.2.0_Installation.zip` can be found on OpenText Software Support Online.

Starting with Database Activity Monitoring 25.1.0, a setup script has been designed to facilitate the installation of all DAM components and compatible third-party applications.



Important

It is recommended to contact OpenText support to make configuration changes in the script.

Database Activity Monitoring installation overview

Before you can use Database Activity Monitoring to monitor and analyze database activity, you need to install the software.

1. Download `DAM_25.2.0_Installation.zip` to the **C:** drive and extract it to the same location.
2. The **C:\DSMedia** folder extracted from `DAM_25.2.0_Installation.zip` contains all the setup files required for installation.
3. Installation files for **Agent** are available in the location **C:\DSMedia\agent**. To install Agent, refer to the *OpenText™ Database Activity Monitoring Admin Guide*.
4. Installing Database Activity Monitoring must meet the requirements for your machine. See [Requirements](#).

1.2. Requirements

The following are the system requirements:

- [Supported Operating System](#)
- [Disk Partitioning](#)
- [Static IP Address Settings](#)
- [Timezone Settings](#)
- [Administrative Privileges](#)

1.2.1. Supported Operating System

The installation script is compatible exclusively with the following Windows Server versions:

- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

1.2.2. Disk Partitioning

The system partition resides on Disk **C**, which serves as the primary drive for the operating system.

Partition the remaining disks according to the recommended specifications below to optimize product performance and security.

Purpose of use	Drive	Min. Disk Capacity	Min. Disk Performance
DAM Real-time Data	E: (ESDATA)	500GB	1000(MB/s)
DAM Backup Data	F: (ESBACKUP)	250GB	250(MB/s)
DAM Archive Data	S: (ESARCHIVE)	250GB	250(MB/s)
Product Configuration	G: (SQL)	50GB	250(MB/s)
Microsoft Messaging Queuing	Q (MSMQ)	50GB	1500(MB/s)

**Tip**

To measure disk performance, use the application `C:\DSMedia\tools\DiskInfo.exe`. Measurements are made in megabytes per second (MB/s).

1.2.3. Static IP Address Settings

Before starting the installation process, make sure that the machine running the script has a static IP address configured.

Assigning the Static IP Address

To get the IP address of the machine,

1. Open the Command Prompt, type `ipconfig`, and press **Enter**.
2. Copy the address of **IPv4 Address**.

To define IPv4 Address as a static IP address,

1. Go to **Control Panel > All Control Panel Items > Network Connections**.
2. Right click **Ethernet1** and choose **Properties**.
3. Clear **Internet Protocol Version 6 (TCP/IPv6)**.
4. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
5. Choose **Use the following IP address**.
6. Paste or type the following fields of the machine:
 - IP address
 - Subnet mask
 - Default gateway
7. Click **OK**.
8. Check statistics of IP using the `ping` command.

1.2.4. Region and Timezone Settings

Make sure that the **Region and Time Zone Settings** of the server are configured appropriately according to your local time zone.

**Important**

The timezone setting directly impacts the timestamp of DAM logs.

Setting the machine Timezone

To set the Timezone of the machine:

1. Go to **Control Panel > All Control Panel Items > Region**.
2. In the **Formats** tab, from the **Format** drop down, select English (US) or English (UK).
3. Click **Apply**.
4. In the **Administrators** tab, click **Copy settings**.
5. Select the following check boxes of **Copy your current settings to**:
 - **Welcome screen and system accounts**
 - **New user accounts**.
6. Click **OK**.
7. Go to **All settings > Time & Language**.
8. Choose the **Time Zone** as your local time zone.

1.2.5. Administrative Privileges

**Important**

Make sure you have the administrator access to the machine where you want to install DAM, otherwise the installation script execution fails with warning

1.3. Configuration

The configuration application **ConfigEditor** handles all configuration settings required during the installation process.

1. Navigate to **C:\DSMedia\tools**.
2. Launch **ConfigEditor**.
3. Enter the required values in the following fields:
 - **Host IP address** - If the server does not have at least one static IP address configured, the **Host IP address** field is automatically set to **127.0.0.1** and this value cannot be modified.
 - **Mandatory** - These fields must be configured separately, as they may differ from installation to installation.

Field	Function	Configuration
ipaddress	Static IP Address of the main Server	Valid IP address must be provided (i.e., 192.168.1.100)
msmsg.storage	Queue Storage folder path for DAM Data	Path must be provided (i.e., Q:\MSMQ\Storage)
msmsg.Logs	Storage path for MSMQ logs	Path must be provided (i.e., Q:\MSMQ\Logs)
msmsg.transaction	MSMQ transaction data storage path	Path must be provided (i.e., Q:\MSMQ\Transaction)
sql.username	SQL Server admin username	Default value is given a sa admin can be changed
sql.password	SQL Server admin password	Provided by customer during the installation
sql.datapath	Storage path for SQL Server data	Path must be provided (i.e., G:\SQL)
sql.logpath	Storage path for SQL Server log data	Path must be provided (i.e., G:\SQL)
sql.historypath	Storage path for SQL Server historical records	Path must be provided (i.e., G:\SQL)
sql.fulltextpath	Storage path for SQL Server full text indexes	Path must be provided (i.e., G:\SQL)

elasticsearch.configuration.esUrl	URL Address for Elasticsearch service	In cluster installations, it is essential to enter the server's static IP address (default value is set to http://127.0.0.1:9200)
elasticsearch.clusterName	Definitive name for Elasticsearch Cluster	Private name must be provided by customer (i.e., DS_Cluster)
elasticsearch.nodeName	Definitive name for Elasticsearch node	Private name must be provided by customer (i.e., DS_Node1)
elasticsearch.networkHost	Network connection address of Elasticsearch	URL must be provided (i.e., 127.0.0.1)
elasticsearch.pathData	Main data folder	Path must be provided (i.e., E:\ESDATA)
elasticsearch.esHotArchive	Archive folder (Data older than the current day's data will be archived daily at 01:00 AM)	Path or UNC file path must be provided (i.e., F:\ESARCHIVE or \\NASSERVER\ESREPO\HOTARCHIVE)
elasticsearch.esBackup	Backup folder (The data will be backed up daily at 01:00 AM.)	Path or UNC file path must be provided (i.e., F:\ESBACKUP)
elasticsearch.hotCapacity	Daily Hot data capacity (The live data allows for searches to be conducted for the last <hotcapacity> number of days on the search screen)	Adjustable numeric field (default value is 180)
elasticsearch.warmCapacity	Daily Warm data capacity (The live data allows for searches to be conducted for the number of days specified by <warmcapacity> prior to the HOT data on the search screen)	Adjustable numeric field (default value is 180)

elasticsearch.archiveCapacity	Daily Archive capacity	Adjustable numeric field (default value is 735)
elasticsearch.shardcount	Index shard count (The index shard count specifies how many different data nodes a single day's data will be divided into.)	The default value is set to "1". In cluster installations, it should be equal to the number of data nodes.
elasticsearch.replicacount	Data replication factor	The default value is set to "0". If there is a need for data replication (High Availability), it can be adjusted to "1".

- **Optional** - User can choose to configure this or use the default values. Contact OpenText support for any changes required in this configuration settings.
- **Advanced** - You must use the default values. Contact OpenText support for any changes required in this configuration settings.
- **Other** - You must use only the default values.

1.4. Installation

Follow the instructions below to install Database Activity Monitoring:

1. Navigate to the location **C:\DSMedia**.
2. Open the Windows Powershell with administrative privileges.
3. Run the below command to execute script **setup-script.ps1**.
`.\setup-script.ps1`
4. Once the installation starts, all required components and third-party components will be installed one at a time.



Note

- During the installation process, the system may require several restarts. After restarting the system, the installation will resume after logging in to the server.
- If an error occurs during the installation process, a detailed explanation of the error is displayed in the PowerShell console. You can also view the error details in the log file available in C:\DSMedia\logs directory.

5. When the installation is successful, the following window appears. This shows that all required configurations have been made and the installation is successful

```
Event sent successfully. ID: 1rHN_JMB1_ySfAzxvINK
Running Curator Task
SUCCESS: Attempted to run the scheduled task "InfraskopeESCuratorTask".
'InfraskopeESCuratorTask' task successfully started.
Installing Console
The IS Console has been successfully installed.
Installing ISServer
The DAM Server has been successfully installed.
Installing DAM Collector
The DAM Collector has been successfully installed.
Configuring antivirus exceptions...
True
Product Installation completed successfully!
Installing additional tools. You can start using DAM Server!
Installing SQL Server Management Studio
SSMS installed successfully.
True
Installing Notepad++...
Installing Notepad++
Notepad++ has been installed successfully.
True
Installing Chrome
Installation completed successfully!
Please restart your computer to finish installation. Press Enter to exit..:
```

6. Restart the server

1.5. Licensing

A 14-day trial license is provided for the Database Activity Monitoring. The license file `app.license` available in **C:\DSMedia** are copied to **C:\inetpub\wwwroot\ElfWebService** during installation.

1. Open dashboard from the Database Activity Monitoring desktop icon.
2. Enter the following:
 - **Server Name** : hostname / IP
 - **User Name** : logadmin
 - **Password** : password1

**Note**

It is recommended to change the default password after the first login.

3. After successful login, license expiration and Product Installed information are displayed on the dashboard.

opentext | Database Activity Monitoring | Evaluation | 14 days left.

Once the trial period expires, a notification appears during the login.

The screenshot shows a login interface with a dark blue background. At the top, there is a warning message in a light blue box: "License expired or invalid." Below this, there are three input fields: the first contains "localhost", the second contains "logadmin", and the third contains a masked password ".....". Below the password field is a checkbox labeled "Remember me". At the bottom, there is a white "Sign in" button.

4. Replace the trial license file located in folder **C:\inetpub\wwwroot\ElfWebService** with the license file you purchased from OpenText.

You can purchase the license before the trial version expires.

1.6. Elasticsearch Security Configuration



Important

It is recommended to change the default password to avoid the significant security vulnerabilities. Make sure that this step is not missed and that a strong, secure password is used instead.

To change the default password:

1. Navigate to **Settings > Storage**.
2. Select the **Security** tab.



Note

The **Old Password** information can be obtained from the System Administrator or through the **C:\DSMedia\tools\ConfigEditor.exe** application by clicking the **Copy EsPassword** to Clipboard button.

1.7. Upgrading DAM Components

If you already have an older version of the product installed on your server, you can upgrade it directly to the latest version using the component installers.

Upgrading DAM Web Service

1. Double click on the **C:\DSMedia\components\elfwebservice_o_win64_*.msi** file.

The advanced installer will start.

2. Click **Next** on the opened page.
3. The End-User License Agreement page will open. Accept the license agreement and click **Next**.
4. The Installation Folder page will open. Select the folder where you want to install the software and click **Next**.
5. The Ready to Install page will open. Click **Install** to start the update.
6. Once the upgrade has been completed, click **Finish** to exit the installer.
7. Once the upgrade is completed successfully, the following code should be added just before the `</configuration>` line in the **web.config** file:

```
<runtime>
  <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
      <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe"
        publicKeyToken="b03f5f7f11d50a3a" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Serilog" publicKeyToken="24c2f752a8e58a10"
        culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-4.2.0.0" newVersion="4.2.0.0" />
    </dependentAssembly>
  </assemblyBinding>
</runtime>
```

8. After the addition, the content of the **web.config** file should look like the following.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>...</configSections>
  <appSettings>...</appSettings>
  <connectionStrings />
  ...
  <system.web>...</system.web>
  <applicationSettings>...</applicationSettings>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe" publicKeyToken="b03f5f7f11d50a3a" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="Serilog" publicKeyToken="24c2f752a8e58a10" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-4.2.0.0" newVersion="4.2.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
</configuration>
```

**Note**

After the Web service upgrade is completed, [Steps 7](#) and [8](#), which are usually done manually, can be performed automatically using the PowerShell script below: `fix-webservice-after-update.ps1`

Upgrading DAM Server

1. Double click on the **C:\DSMedia\components\isserver_o_win64_*.msi** file.
The advanced installer will start.
2. Click **Next** on the opened page.
3. The End-User License Agreement page will open. Accept the license agreement and click **Next**.
4. The Installation Folder page will open. Select the folder that you want to install and click **Next**. The Database Connection page will open.
5. Enter Database Server, Username, and Password.

DAM Server Setup

Database Connection

Provide the required information and verify the database connection.

Database Server:

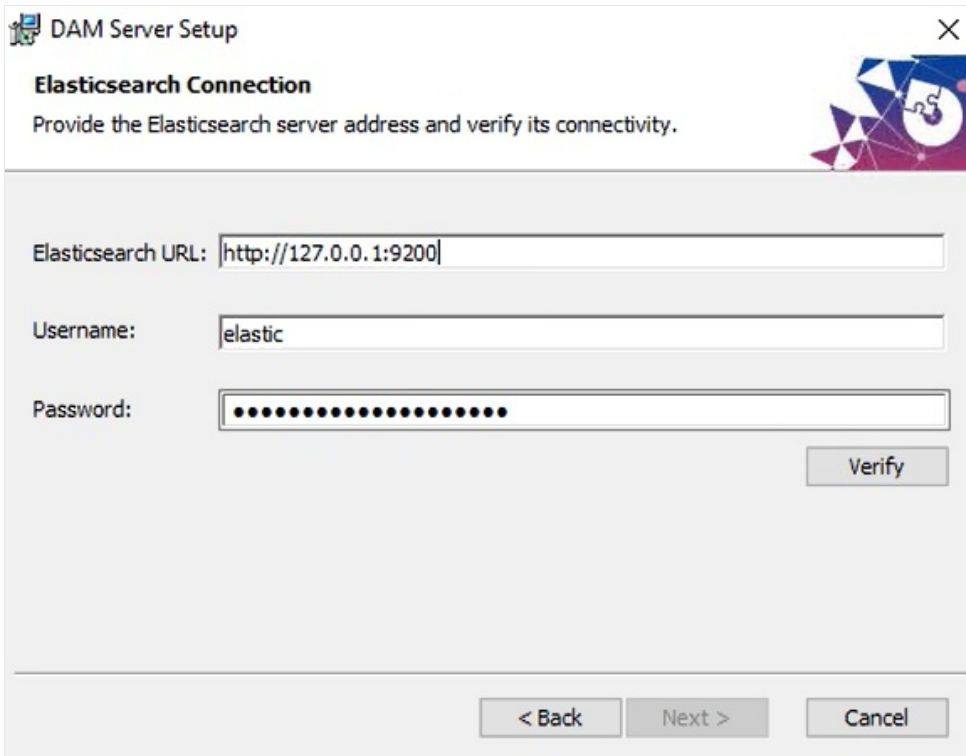
Username:

Password:

Verify

< Back Next > Cancel

- Click **Verify** to check the connection. If the connection is successful, then click **Next**.
The Elasticsearch Connection page will open.
- Enter Elasticsearch URL, Username, and Password.



DAM Server Setup

Elasticsearch Connection
Provide the Elasticsearch server address and verify its connectivity.

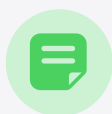
Elasticsearch URL:

Username:

Password:

- Click **Verify** to check the connection. If the connection is successful, then click **Next**.
The Ready to Install page will open.
- Click **Install** to start the update.
- Once the upgrade is complete, click **Finish** to exit the installer.

Upgrading DAM Collector



Note

Before updating the DAM Collector, you must back up the `Karmasis.Dataskope.Collector.exe.config` file. After the update, the settings file will be reset to default values. The settings from the section must be restored from the backed-up configuration file.

- Backup the **Karmasis.Dataskope.Collector.exe.config** file before starting the update process.
- Double click on the **C:\DSMedia\components\damclassiccollector_o_win64_*.msi** file.
- The advanced installer will start. Click **Next** on the opened page.
- The End-User License Agreement page will open. Accept the license agreement and click **Next**.
- The Installation Folder page will open. Select the folder where you want to install the software and click **Next**.
- The Ready to Install page will open. Click **Install** to start the update.

7. Once the upgrade is complete, click **Finish** to exit the installer.
8. Open the **Karmasis.Dataskope.Collector.exe.config** file and change the **<appSettings>** section with the information from the backed-up file.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- The number of concurrent connections the collector can have -->
    <add key="quartz.threadPool.threadCount" value="330" />
    <!-- Determines how quickly the collector connects to the agents in seconds -->
    <add key="quartz.jobs.delay" value="5" />
    <!-- If disabled, the collector will re-connect to the agent after a message files is processes -->
    <add key="process.files.read.count.enabled" value="false" />
    <!-- Maximum number of files to process before the collector resets the connection -->
    <add key="process.files.read.count" value="2" />
    <!-- Debug mode will activated for the given agents. Multiple agent names (hostname) can be added w
    <add key="debugMode.agentList" value="Agen1|Agent2" />
    <!-- Maximum size of a log file before it is rotated -->
    <add key="trace.archiveAboveSize" value="2000000" />
    <!-- Number of log files should be stored. It is like rotation -->
    <add key="trace.maxArchiveFiles" value="2" />
    <!-- When enabled, a log file is created with a pattern like "agenthostname_collectorpid" and relat
    <add key="trace.logServers.enabled" value="false" />
    <!-- If the file is empty, corrupted or unreadable, delete it when set to true -->
    <add key="deleteWhenCorruptedFileReceived" value="true" />
    <!-- Detect below SQL Injection Attempts -->
    <add key="isAntiSqlInjectionEnabled" value="true" />
    <add key="antiSqlInjection.CheckAlwaysFalseCondition" value="true" />
    <add key="antiSqlInjection.CheckAlwaysTrueCondition" value="true" />
    <add key="antiSqlInjection.CheckCommentAtTheEndOfStatement" value="true" />
    <add key="antiSqlInjection.CheckNotInAllowedStatement" value="true" />
    <add key="antiSqlInjection.CheckPiggybackedStatement" value="true" />
    <add key="antiSqlInjection.CheckStackingQueries" value="true" />
    <add key="antiSqlInjection.CheckSyntaxError" value="true" />
    <add key="antiSqlInjection.CheckUnionSet" value="true" />
    <!-- When maintenance mode is active, the collector will not process messages; the message files wi
    <add key="maintenance.enabled" value="false" />
    <!-- If maintenance.LimitByCursorValue is set to true, the collector will only process message file
    <add key="maintenance.LimitByCursorValue" value="false" />
  </appSettings>
</configuration>
```

**Important**

The other sections in the file should remain the same.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>...</appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.8" />
  </startup>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-13.0.0.0" newVersion="13.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="System.Memory" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-4.0.1.2" newVersion="4.0.1.2" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
  <system.web>
    <membership defaultProvider="ClientAuthenticationMembershipProvider">
      <providers>
        <add name="ClientAuthenticationMembershipProvider" type="System.Web.ClientServices.Providers.ClientAuthenticationMembershipProvider, System.Web.ClientServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
      </providers>
    </membership>
    <roleManager defaultProvider="ClientRoleProvider" enabled="true">
      <providers>
        <add name="ClientRoleProvider" type="System.Web.ClientServices.Providers.ClientRoleProvider, System.Web.ClientServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
      </providers>
    </roleManager>
  </system.web>
</configuration>
```

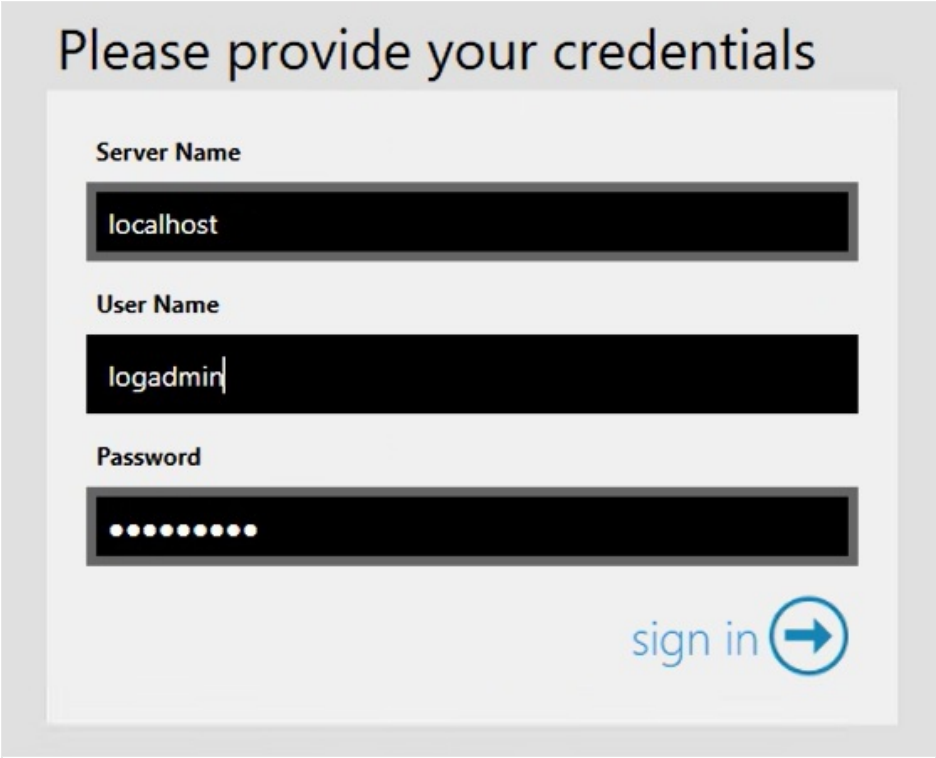
Upgrading DAM Console Components

Installation of DAM Control Panel

1. Double click on the **C:\DSMedia\components\controlpanel_o_win64_*.msi** file.
2. The advanced installer will start. Click **Next** on the opened page.
3. The End-User License Agreement page will open. Accept the licence agreement and click **Next**.
4. The Installation Folder page will open. Select the folder where you want to install the software and click **Next**.
5. The Ready to Install page will open. Click **Install** to start the update.
6. Once the upgrade is complete, click **Finish** to exit the installer.

Upgrading DAM Console Components using Control Panel

1. Double click on the **Control Panel** icon on the Desktop.
2. Enter the **Server Name**, **User Name**, and **Password**.



Please provide your credentials

Server Name


localhost

User Name

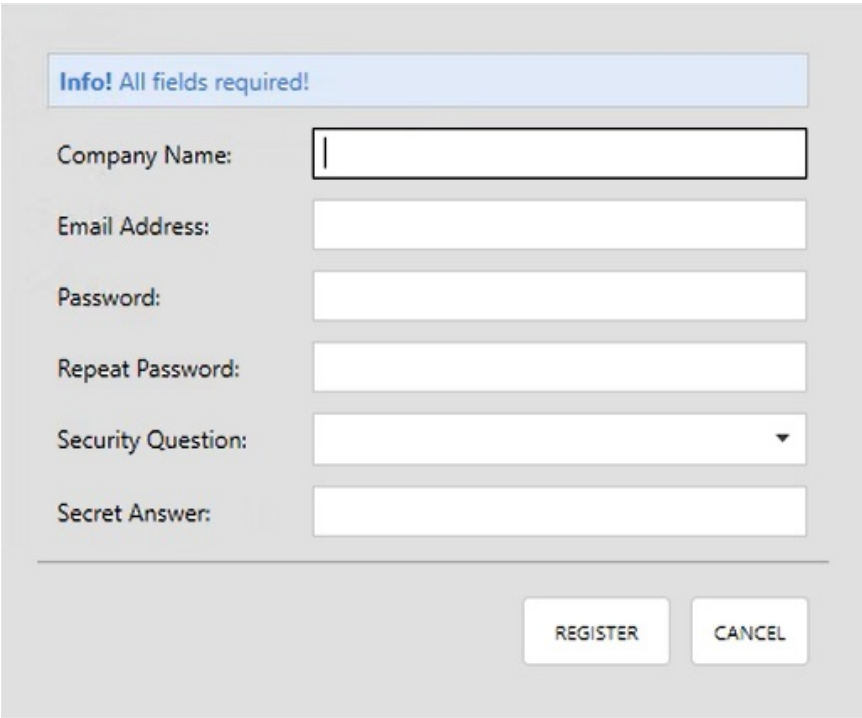
logadmin

Password

••••••••

sign in 

3. Click **sign in**.
4. If you are installing for the first time, you should enter the Company Info details and click **REGISTER**.



Info! All fields required!

Company Name:

Email Address:

Password:

Repeat Password:

Security Question:

Secret Answer:

REGISTER CANCEL

5. Product list will be displayed. Select the components that you want to update and click **Proceed**.

DAM Control Panel v.25.20.2

1 product available to install. 6 products updates available. SELECT ALL ☒

DAM Database Updater	UPDATE <input checked="" type="checkbox"/>
25.1.5.48 Tue Apr 29, 2025 10: 22 AUTOMATEDTESTS2	
DAM API	UPDATE <input checked="" type="checkbox"/>
25.1.5.48 Tue Apr 29, 2025 10: 22 AUTOMATEDTESTS2	
DAM Curator	UPDATE <input checked="" type="checkbox"/>
25.1.5.48 Tue Apr 29, 2025 10: 22 AUTOMATEDTESTS2	
DAM Scheduled Reports	INSTALL <input checked="" type="checkbox"/>
DAM Installer API	UPDATE <input checked="" type="checkbox"/>
25.1.5.48 Tue Apr 29, 2025 10: 22 AUTOMATEDTESTS2	
DAM Event Exporter	UPDATE <input checked="" type="checkbox"/>
25.1.5.48 Tue Apr 29, 2025 10: 22 AUTOMATEDTESTS2	
DAM TIFeed	UPDATE <input checked="" type="checkbox"/>
25.1.5.48 Tue Apr 29, 2025 10: 22 AUTOMATEDTESTS2	

Connected as: logadmin [Change Password](#) PROCEED EXIT

6. Enter **Currently connected server**, **Database username**, and **Password**.

Verification is required for the selected Infraskope API and Infraskope Installer API services' database connection string. If you wish, you can modify this connection string.

Currently connected server:

Database user name:

Password:

TEST CONNECTION CHANGE

Provide the required parameters and click Save. SAVE CLOSE

7. Click **TEST CONNECTION**. After the connection is successful, click **Save**.
This opens the Register page.

DAM Control Panel v.25.20.2

7 installed products.

DAM Database Updater			INSTALLED
25.20.1.0	Tue Apr 29, 2025 11: 09	AUTOMATEDTESTS2	
DAM API			INSTALLED
25.20.5.0	Tue Apr 29, 2025 11: 09	AUTOMATEDTESTS2	
DAM Curator			INSTALLED
25.20.2.0	Tue Apr 29, 2025 11: 09	AUTOMATEDTESTS2	
DAM Scheduled Reports			INSTALLED
25.20.3.0	Tue Apr 29, 2025 11: 09	AUTOMATEDTESTS2	
DAM Installer API			INSTALLED
25.20.3.0	Tue Apr 29, 2025 11: 09	AUTOMATEDTESTS2	
DAM Event Exporter			INSTALLED
25.20.1.0	Tue Apr 29, 2025 11: 10	AUTOMATEDTESTS2	
DAM TIFeed			INSTALLED
25.20.3.0	Tue Apr 29, 2025 11: 10	AUTOMATEDTESTS2	

STATUS

Updating DAM Database Updater
DAM Database Updater Updated
Updating DAM API
DAM API Updated
Updating DAM Curator
DAM Curator Updated

Connected as: logadmin [Change Password](#)

EXIT

- Once the upgrade is completed, click **Exit** to exit the installer.



© Copyright 2025 Open Text
For more info, visit <https://docs.microfocus.com>
