

OpenText™ Database Activity Monitoring

Software Version 24.4.0

Installation Guide

opentext™

Document Release Date: October 2024
Software Release Date: October 2024

Legal notices

Copyright 2023 - 2024 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Except as specifically indicated otherwise, this document contains confidential information and a valid license is required for possession, use or copying. If this work is provided to the U.S. Government, consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

Support

Visit the [MySupport portal](#) to access contact information and details about the products, services, and support that OpenText offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

Contents

Introduction	4
Obtain OpenText™ Database Activity Monitoring software	4
Prerequisites	4
Assigning the Static IP Address	4
Disabling Firewall	5
Controlling User Accounts	5
Region Settings	5
Checking chcp	6
Disabling IE Enhanced Security Configuration	6
Installing .Net 4.8, Chrome and Notepad++	6
Setting the machine name	7
Setting Host Configurations	7
Naming the created disks	8
Activating server roles	9
Running the preparation script	10
Editing IIS settings	10
Rechecking the prerequisites	10
SQL Server Installation	11
SSMS Installation	11
DAM Installation	13
Database Setup	13
Configuring IIS Certificate	13
Web Service Setup	14
OpenText Service Setup	16
ElasticSearch Setup	17
Sense Installation	18
Elasticsearch Security Installation (Optional)	23
Console and Control Panel Setup	24
Console Setup	24
Control Panel Setup	25
Licensing	28

Introduction

This document describes how to install OpenText™ Database Activity Monitoring (DAM).

Obtain OpenText™ Database Activity Monitoring software

The latest software for OpenText™ Database Activity Monitoring DAM_24.4.0_Installation.zip can be found on OpenText Software Support Online.

Prerequisites

Before starting the installation of OpenText™ Database Activity Monitoring, the following actions and feature changes must be made as a prerequisite on the machine on which the installation is made:

- Use Windows Server 2022 or higher versions for the operating system.
- Create E, F, G and H disks in the Virtual Machine.
 - Static IP Assignments
- Disabling Firewall
- Control User Accounts
- Transfer all the required setup files to the Virtual Machine.

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.

Disabling Firewall

To disable the firewall

1. Go to **Control Panel > Windows Defender Firewall**.
2. From the left pane of the window, click **Turn Windows Defender Firewall on or off**.
3. Choose the option, **Turn off Windows Defender Firewall**.
4. Click **OK**.

NOTE:

- After the installation, it is recommended to enable firewall choosing **Turn o Windows Defender Firewall**.
- If the machine is under a domain controller, it is recommended to turn off the **Domain Firewall**.

Controlling User Accounts

1. Go to **Control Panel > All Control Panel Items > User Accounts**.
2. Click **Change User Account Control Settings** option.
3. Move the marker down to **Never notify**.
4. Click **OK**.

NOTE: After installation, it is recommended to turn on the notifications again.

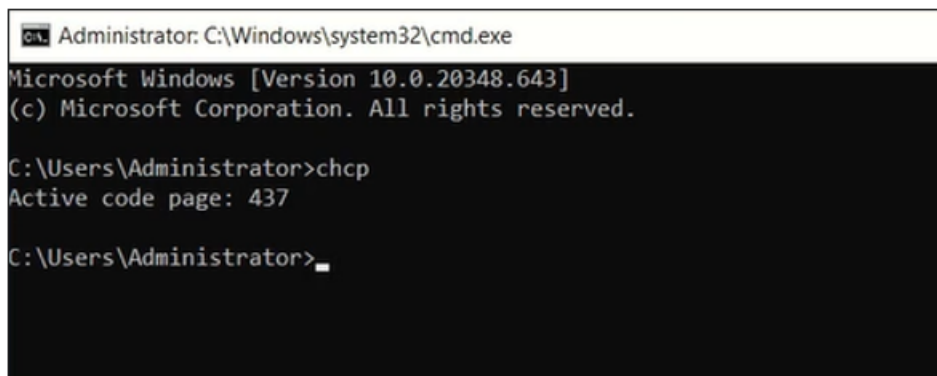
Region Settings

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.

Checking chcp

1. Open Command Prompt and run the command chcp.
2. Verify, **Active code page** is 437.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.643]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>chcp
Active code page: 437

C:\Users\Administrator>
```

Disabling IE Enhanced Security Configuration

1. Go to **Server Manager > Local Server**.
2. Turn off **IE Enhanced Security Configuration** for both **Administrator** and **Users**.

Installing .Net 4.8, Chrome and Notepad++

1. Open Registry Editor, and check .Net 4.8 Version existence.
2. Go to the path `HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full` and verify the version is 4.8 or later.

If it does not exist, get the installation package

- Double click the following files and follow the basic installation steps.

`\InstallMedia\Stage1\ndp48-x86-x64-allos-enu.exe`

3. Go to **InstallMedia\AdministrativeTools**
4. Double click the following files to install.
 - `ChromeStandaloneSetup64.exe`
 - `npp.7.6.4.Installer.exe`

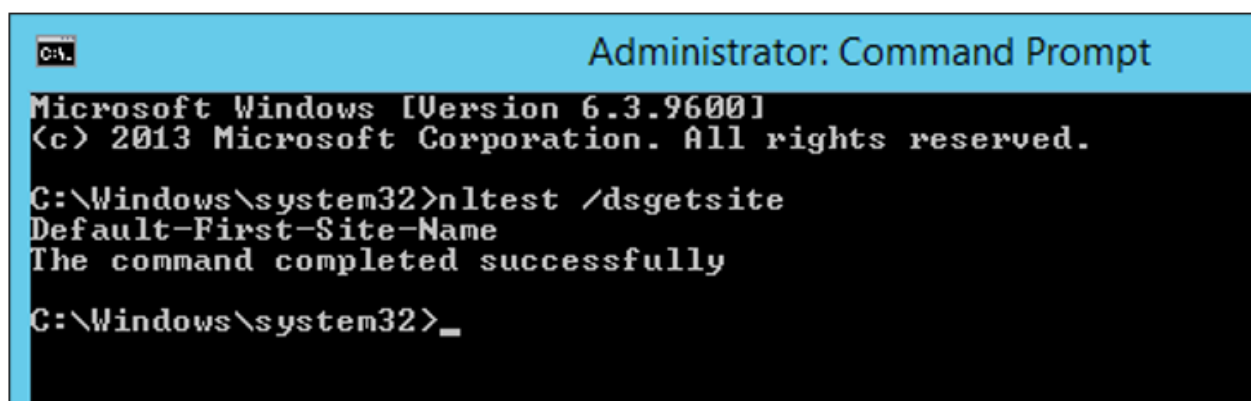
NOTE: You can use any editor, but for Notepad editor, it must be Notepad ++.

Setting the machine name

1. Go to **Control Panel>System>About**
2. Click **Rename this PC**.
3. Enter a machine name and click **Next**.
4. Click **Restart now**.

Setting Host Configurations

1. Go to C:\Windows\System32\drivers\etc.
2. Right click hosts and choose **Edit with Notepad++**.
3. Check if the machine is included in any Active Directory Site and Services.
 - a. If there is any site information, this value should be added to the host file.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nltest /dsgetsite
Default-First-Site-Name
The command completed successfully

C:\Windows\system32>_
```

For example, the output was California.

The record in the host file should be as follows:

<IP Address> California_elfws California_elfupdate <MachineName>

- b. If no result is returned (i.e. default is returned), the normally written version should be used.

```
Administrator: C:\Windows\system32\cmd.exe
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.50.1

C:\Users\Administrator>ping _elfws

Pinging _elfws [192.168.50.4] with 32 bytes of data:
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.50.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping _elfupdate

Pinging _elfws [192.168.50.4] with 32 bytes of data:
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128
Reply from 192.168.50.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.50.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

4. Add the line <IP address> _elfws_elfupdate

```
192.168.50.4 _elfws_elfupdate
```

Naming the created disks

Give the name of the disks as

- E: ESDATA
- F: ESARCHIVE&ESBACKUP
- G: SQL
- H: MSMQ

NOTE:

- Disk C is the system disk.
- Disk E is the ESData disk.
- Disk F is the ESArchive and ESBackup disk. However, in client production environments, it would be better to create these files separately.
- Disk G is the configs disk.
- Disk H is the MSMQ disk. This disk should be SSD if possible. During the first installation, MSMQ comes to the C disk, and in client production environments, MSMQ must be moved to the separately provided SSD disk.



Activating server roles

1. Go to **Server Manager > Dashboard**.
2. Click **Manage > Add roles and features**.
3. On the **Before You Begin** window, click **Next**.
4. On the **Installation Type** window, choose **Role-based or feature-based installation** and click **Next**.
5. On the **Server Selection** window, choose **Select a server from the server pool**, select **DAM** from the **Server Pool** and click **Next**.
6. On the **Server Roles** window, select **File and Storage Services** and click **Next**.
7. On the **Features** window, select **.NET Framework 3.5 Features** and **.NET Framework 4.8 Features** with their sub-features.
8. Select **HTTP Support and Message Queuing Triggers** sub-features under **Message Queuing** menu
9. Click **Next**.
10. On the **Web Server Role (IIS)** window, click **Next**.
11. On the **Role Services** window, choose the option following and click **Next**.
 - Web Server
 - Management Tools
 - IIS Management Console
 - IIS 6 Management Compatibility > IIS 6 Metabase Compatibility
12. On the **Installation Selection** window, click **Specify an alternate source path**.

13. Copy and paste the sxs file location to the **Path** and click **OK**.

NOTE: The path to the location of the sxs file in the source folder of the mounted Windows ISO must be entered in this field.



14. Click **Install**.
15. On the **Installation Progress** window, click **Close** after the installation completed.

NOTE: Windows ISO must be mounted, check the status and change it to mounted if it is not.

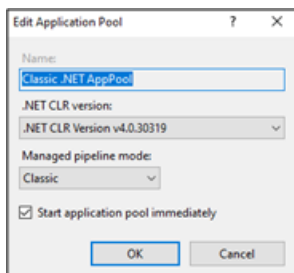
Running the preparation script

1. Go to `InstallMediaStage1`.
2. Right click on `preparation.cmd` and choose **Run as administrator**.
3. On the command prompt, if asked, press `y` to restart the system.

```
Operation is completed. You should restart your machine. Proceed? (Y/N)?y
```

Editing IIS settings

1. Open **IIS Manager** and edit `app.pool`.
2. Choose `.NET CLR version` as `v4.0.30319`.



3. From the Action pane, click **Set Application Pool Defaults...**
4. Select **True** value for the **Enable 32-Bit Applications** field.
5. Select **Classic** value for **Managed Pipeline Mode** field.
6. Choose **LocalSystem** for **Identity** field under **Process Model**.
7. Click **OK**.

Rechecking the prerequisites

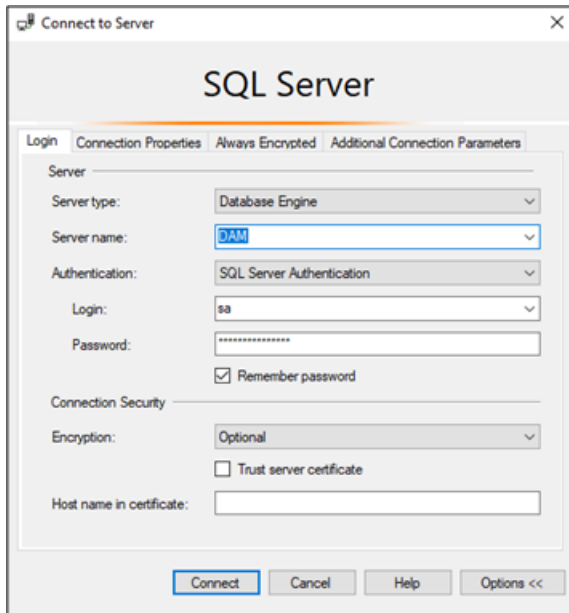
Check firewall, UACs, region and language changes.

SQL Server Installation

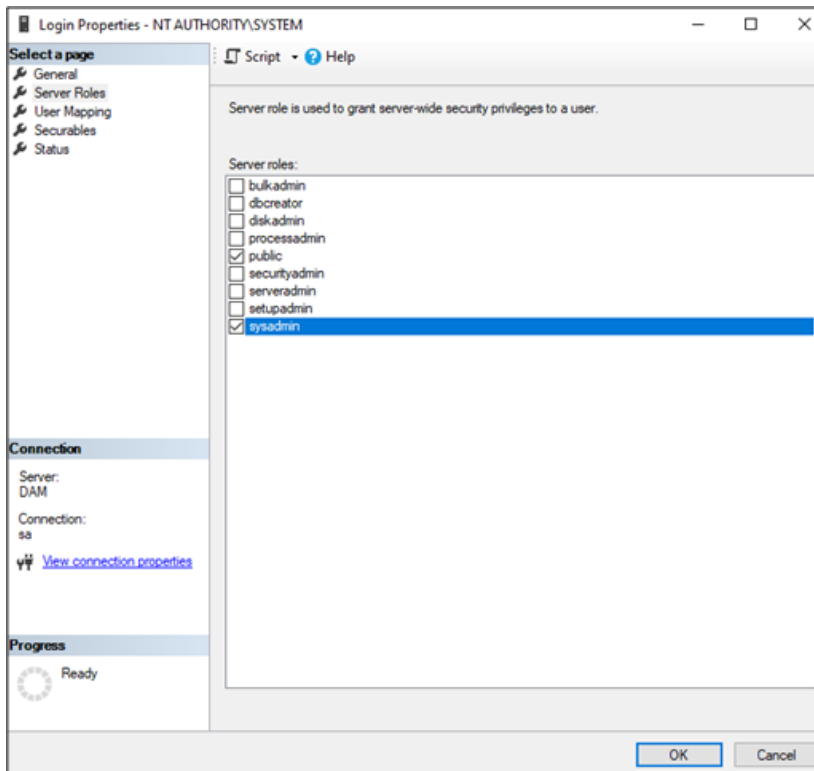
1. Go to `\InstallMedia\Stage2\SQLServerExpress`.
2. Run `SQLEXPRADV_x64_ENU.exe`.
3. Choose directory for extracted files and click **OK**.
4. Choose **New SQL Servers stand-alone installation** or **add features to an existing installation**.
5. Check **I accept the license terms and Privacy Statement** and click **Next**.
6. On **Global Rules** window, click **Next** if all the results are passed.
7. On **Microsoft Update** window, click **Next**.
8. On **Product Updates** window, click **Next**.
9. On **Installation Setup Files** window, click **Next**.
10. On **Installation Rules** window, click **Show Details**.
11. On **Features Selection** window, select **Database Engine Services** and **Full-text and Semantic Extractions...** and click **Next**.
12. On the **Instance Configuration** window, select **Default instance**, enter **Instance ID** and click **Next**.
13. On the **Server Configuration** window, change the **Account Name** as **NT AUTHORITY\SYSTEM** and click **Next**.
14. On the **Customization** window, select **Latin1_General** from the **Collation designator** drop-down and check the **Accent-sensitive**. Click **OK**.
15. On the **Database Engine Configuration** window, select **Mixed Mode** and define a password. Click **Next**.
16. Click **Close**, once all features have **Succeeded** status.

SSMS Installation

1. Go to `\InstallMedia\Stage2\SQLServerExpress`
2. Right click `SSMS-Setup-ENU.exe` and select **Run as administrator**.
3. On the **Welcome** window, click **Install**.
4. Click **Restart**.
5. Open **SSMS** and log in with user ID and password.



6. Open **Security > NT AUTHORITY\SYSTEM – Server Roles** and allow **sysadmin** to authorize the system.



DAM Installation

Follow the below instructions to install OpenText™ Database Activity Monitoring.

Database Setup

1. Create a folder as **OpenTextDAM_DB** in **SQL (G:) Disk**.
2. Create the following folders in **OpenTextDAM_DB**
 - SQLDATA
 - SQLFT
 - SQLHS
 - SQLLOG
3. Go to **InstallMedia\Stage2\ProductComponents** and right click **DAM_DatabaseSetup.msi** and run as an administrator via **Windows PowerShell**, switch to command prompt.
4. On **DAM Wizard**, click **Next**.
5. Choose **I Agree on License Agreement** and click **Next**.
6. Copy and paste the file location into the installation path for which of the required fields.
 - Database Path: G:\OpenTextDAM_DB\SQLDATA
 - Database Log Files Path: G:\OpenTextDAM_DB\SQLLOG
 - Full Text Catalog Path: G:\OpenTextDAM_DB\SQLFT
 - History Path: G:\OpenTextDAM_DB\SQLHS
7. Enter **Instance Name and Password** for Server Configuration. The instance name is "." The password is the previously determined **sa password**.
8. Click **Next** to confirm the installation. On the **Installation Completed** window, click **Close**.
9. Verify each folder after installation.
10. Verify in the **SSMS if AuditDB** file got located.

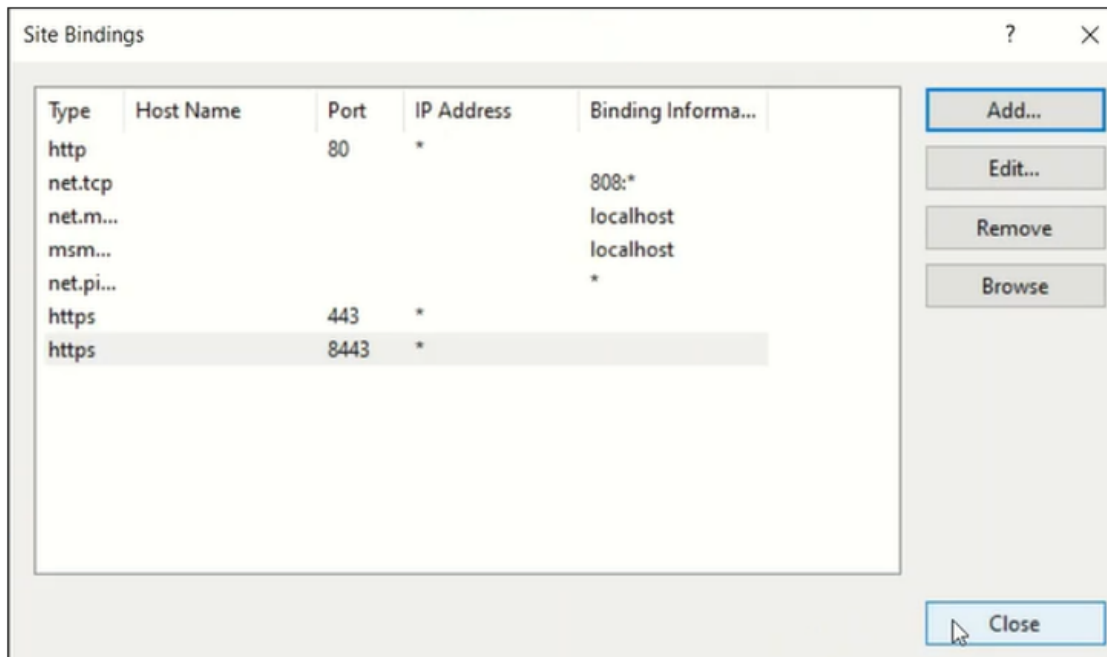
Configuring IIS Certificate

1. Open **IIS Manager > Default Web Site** and click **Edit Site Bindings**.
2. From Action pane on the left, under **Edit Site**, click **Bindings**.
3. Click **Add** to add new one for 443 port channel.

The Type should be https and the **Default IIS Certificate** or a **Custom** created certificate should be added and saved.

4. Click **Add** again to add another one for 8443 port channel.

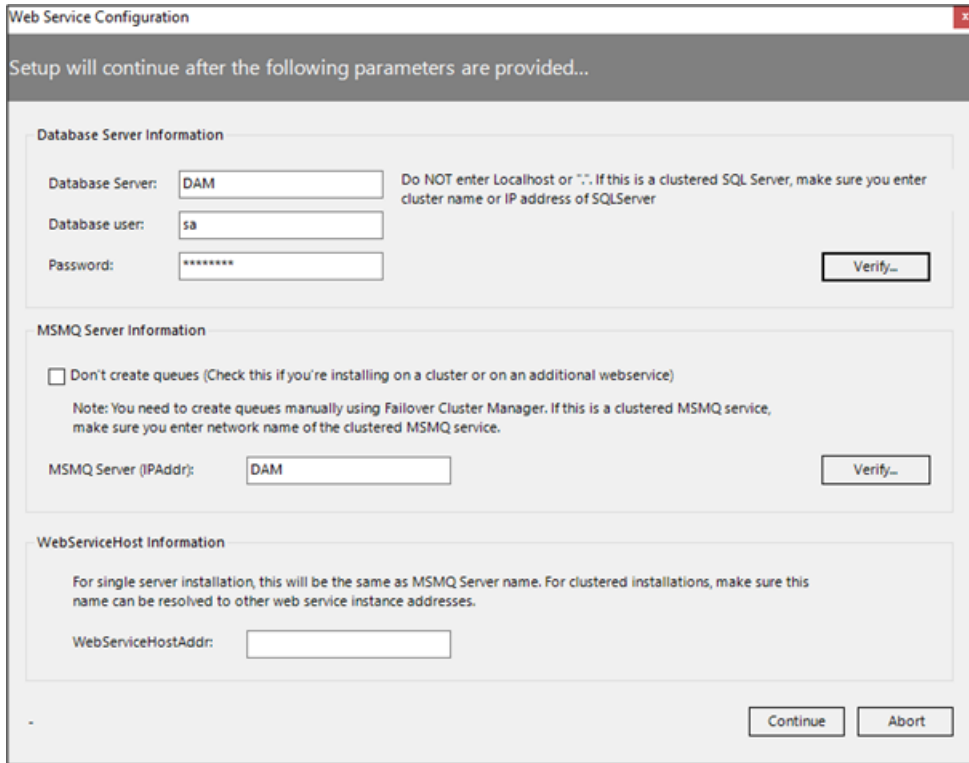
The **Type** should be **https** and the **Default IIS Certificate** or a **Custom** created certificate should be added and saved.



Web Service Setup

1. Go to **InstallMediaStage2ProductComponents**.
2. Right click **DAM_WebService.msi** and select **Run as administrator**.
3. On **DAM Webservice Setup** wizard, click **Next**.
4. On **Select Installation Address** window,
 - a. Choose **Default Web Site** from the **Site** drop-down.
 - b. Enter **ElfWebService** to **Virtual directory** field.
 - c. Choose **DefaultAppPool** from the **Application Pool** drop-down and click **Next**.
5. On the **License Agreement** window, choose **I agree** and click **Next**.
6. On the **Confirm Installation** window, click **Next**.
7. On the **Installation Completed** window, click **Close**.
8. Verify account by entering **Database user** and **Password**.

The password is the previously determined **sa password**.



The image shows a 'Web Service Configuration' dialog box with a title bar containing a close button. The main area has a grey header with the text 'Setup will continue after the following parameters are provided...'. Below this are three sections: 'Database Server Information', 'MSMQ Server Information', and 'WebServiceHost Information'. The 'Database Server Information' section contains three text boxes: 'Database Server:' with 'DAM', 'Database user:' with 'sa', and 'Password:' with '*****'. A 'Verify...' button is to the right. The 'MSMQ Server Information' section has a checkbox 'Don't create queues (Check this if you're installing on a cluster or on an additional webservice)', a note about manual queue creation, and an 'MSMQ Server (IPAddr):' text box with 'DAM' and a 'Verify...' button. The 'WebServiceHost Information' section has a note about host names and a 'WebServiceHostAddr:' text box. At the bottom right are 'Continue' and 'Abort' buttons.

Web Service Configuration

Setup will continue after the following parameters are provided...

Database Server Information

Database Server: Do NOT enter Localhost or ". If this is a clustered SQL Server, make sure you enter cluster name or IP address of SQLServer

Database user:

Password:

MSMQ Server Information

Don't create queues (Check this if you're installing on a cluster or on an additional webservice)

Note: You need to create queues manually using Failover Cluster Manager. If this is a clustered MSMQ service, make sure you enter network name of the clustered MSMQ service.

MSMQ Server (IPAddr):

WebServiceHost Information

For single server installation, this will be the same as MSMQ Server name. For clustered installations, make sure this name can be resolved to other web service instance addresses.

WebServiceHostAddr:

OpenText Service Setup

1. Go to `\\InstallMediaStage2\ProductComponents`
2. Right click `DAMServer.msi` and Run as administrator.
3. On the **DAM Server Setup Wizard**, click **Next**.
4. On **Select Installation Folder** window, enter the folder path to install **DAM Server**.
5. Select **Everyone for Install DAM Server for yourself, or for anyone who uses this computer** field and click **Next**.
6. On the **License Agreement** window, choose **I agree** and click **Next**.
7. On the **Confirm Installation** window, click **Next**.
8. When you see the **Installation Completed** window, click **Close**.
9. On the **Server Configuration** window, verify account by entering **Username** and **Password**.
The password is the previously determined `sa` password.

The screenshot shows the 'Server Configuration' window with two tabs: 'Required Settings' and 'Optional Settings'. The 'Required Settings' tab is active and contains two sections: 'Staging Server Settings' and 'Database Connection Settings'. In the 'Staging Server Settings' section, there is a checkbox for 'This is a staging server' which is unchecked, a text box for 'Parent WebService IP or Host Address' with a 'Validate' button, and a time range selector for 'Transfer events between' set to '00:00:00' and '23:59:59' hours. The 'Database Connection Settings' section includes a 'Database Server' dropdown set to 'DAM', a 'Username' text box containing 'sa', and a 'Password' text box with masked characters. A 'Validate DB Credentials' button is located to the right of the password field. Below these fields, a status message reads 'Connected. WebService reports 'DAM' as the database server.' At the bottom of the window, there is a footer instruction: 'Provide the required parameters and click Continue. If this is a frontend (staging) server, just provide the 'Staging Server Settings'.' and two buttons: 'Continue' and 'Cancel'.

ElasticSearch Setup

1. Create the following folders and their sub folders in (E:) and (F:) disks as follows:

E Disk

- ESDATA
 - ESDATA

F Disk

- ESARCHIVE&ESBACKUP
 - ESARCHIVE
 - ESHOTARCHIVE
 - ESWARMARCHIVE
 - ESBACKUP

2. Right click on each of the files, select **Properties > Sharing >** and click **Share** to share each folders
3. Go to **\\InstallMedia\Stage2\ElasticSearch7** and copy the **elasticsearch-7.16.3** folder into the C disk.
4. Go to **C:\elasticsearch-7.16.3 > config**. Right click on **jvm.options** and choose **Edit with Notepad++**.
5. Delete **##** sign at the beginning of the **Xms4g & Xmx4g** lines in **jvm.options** file and **Save**.

NOTE: Define the memory usage as either half of the total memory of the machine or 1-2 GB less of the half. If the total RAM of the machine is 16, elastic tries to allocate half of it to itself, 8 GB should be given to each. For better practice, it should be 1-2 GB less.

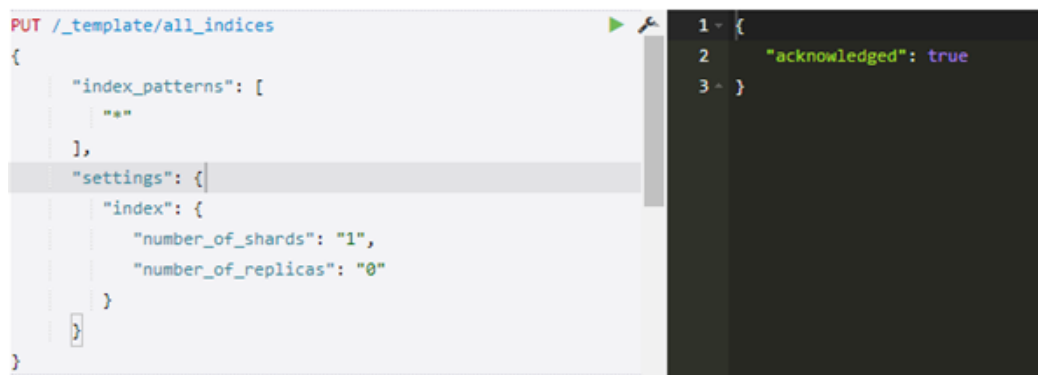
6. Go to **\\InstallMedia\Stage2\ElasticSearch7**, right click on **elasticsearch.yml** and choose **Edit with Notepad++**.
7. Copy and paste the content into the file in C disk located **elasticsearch.yml** file.
8. Make the changes in the lines as shown on the figures given below [**Cluster.name, node.name, node.master, node.data, network.publish_host, path.repo, discovery.type**].
9. Go to **C:\elasticsearch-7.16.3\bin**.
10. Open command prompt from the folder and enter the command given below.

```
C:\elasticsearch-7.16.3\bin\elasticsearch-service.bat install DAMES7
```
11. Change **Startup type** as **Automatic (Delayed Start)** in the Windows service and start the service.

12. Go to **Services > Elasticsearch** and check if the service **Elasticsearch 7.16.3 (DAMES7)** is running.

Sense Installation

1. Open Chrome and write **localhost:9200** to address line.
2. Click **Chrome > Extensions > Manage Extensions**.
3. Open the **Developer mode**.
4. Click **Load unpacked** and choose the setup file `InstallMedia\AdministrativeTools\sense-chrome-1.0.1`
5. Activate the **sense extension** and pin it to the taskbar. Then, click it and make the extension available.
6. Go to `\\InstallMedia\Stage2\ElasticSearch7` and open the `ESTemplates.docx`.
7. Copy the **All indices** script from **ESTemplates**.
8. Paste script into the white side of the page as shown in the figure below.
9. Click play button and see the **“acknowledged”: true reply**.



The screenshot shows the Sense web interface. On the left, a PUT request is shown for the endpoint `PUT /_template/all_indices`. The request body is a JSON object with the following structure:

```
{
  "index_patterns": [
    "*"
  ],
  "settings": {
    "index": {
      "number_of_shards": "1",
      "number_of_replicas": "0"
    }
  }
}
```

On the right, the response is shown in a dark-themed console. The response is a JSON object with the following structure:

```
1 - {
2   "acknowledged": true
3 }
```

10. Copy the **Events template** script from **ESTemplates**.
11. Paste script into the white side of the page as shown in the figure below. Click **Play** button and see the **“acknowledged”: true reply**.



The image shows a REST client interface with two panes. The left pane displays a PUT request to the endpoint `PUT /_template/events_template`. The request body is a JSON object with the following structure:

```
PUT /_template/events_template
{
  "index_patterns": [
    | "events_*"
  ],
  "settings": {
    | "index": {
    | | "refresh_interval": "1s",
    | | "mapping.total_fields.limit": 2000
    | }
  },
  "mappings": {
    | "numeric_detection": false,
    | "dynamic_templates": [
    | {
    | | "strings": {
    | | | "mapping": {
    | | | | "norms": false,
    | | | | "fields": {
    | | | | | "raw": {
    | | | | | | "ignore_above": 250,
    | | | | | | "type": "keyword"
    | | | | | }
    | | | | }
    | | | | },
    | | | | "type": "text"
    | | | }
    | | | "match_mapping_type": "string",
    | | | "match": "*"
    | | }
    | ]
  },
  "date_detection": false,
  "properties": {
    | "TimeCreated": {
    | | "type": "date"
    | },
    | "TimeInserted": {
    | | "type": "date"
    | }
  }
}
```

The right pane shows the response, which is a JSON object with a single field:

```
1 {
2   "acknowledged": true
3 }
```

12. Copy the **Alerts template** script from **ESTemplates**.
13. Paste script into the white side of the page as shown in the figure below. Click **Play** button and see the **"acknowledged": true** reply.

```
PUT /_template/alerts_template
{
  "index_patterns": [
    | "alerts_*"
  ],
  "settings": {
    | "index": {
    | | "refresh_interval": "1s"
    | }
  },
  "mappings": {
    | "numeric_detection": false,
    | "date_detection": false,
    | "properties": {
    | | "AlertName": {
    | | | "type": "keyword"
    | | },
    | | "AlertOwner": {
    | | | "type": "keyword"
    | | },
    | | "Events": {
    | | | "dynamic": true,
    | | | "type": "object",
    | | | "properties": {
    | | | | "TimeCreated": {
    | | | | | "type": "date"
    | | | | }
    | | | }
    | | },
    | | "AlertSeverity": {
    | | | "type": "keyword"
    | | },
    | | "AlertSiteCode": {
    | | | "type": "keyword"
    | | },
    | | "AlertComputer": {
    | | | "type": "keyword"
    | | }
    | }
  }
}
```



```
1 - {
2   "acknowledged": true
3 ~ }
```

14. Copy the **Inventory template** script from **ESTemplates**.
15. Paste script into the white side of the page as shown in the figure below. Click **Play** button and see the **“acknowledged”: true reply**.

```
PUT /_template/inventory_indices_template
{
  "index_patterns": [
    "inventory7_*"
  ],
  "settings": {
    "index": {
      "refresh_interval": "1s"
    }
  },
  "mappings": {
    "numeric_detection": false,
    "dynamic_templates": [
      {
        "strings": {
          "mapping": {
            "norms": false,
            "fields": {
              "raw": {
                "type": "keyword"
              }
            },
            "type": "text"
          },
          "match_mapping_type": "string",
          "match": "*"
        }
      }
    ],
    "date_detection": false
  },
  "aliases": {
    "inventory_alias" : {}
  }
}
```

```
1 {
2   "acknowledged": true
3 }
```

16. Copy the **Repositories** script from **ESTemplates**.
17. Paste script into the white side of the page as shown in the figure below. Click **Play** button and see the **"acknowledged": true** reply.

CAUTION: The location paths are shown as examples below. These paths must match the path.repo values in the \InstallMedia\Stage2\ElasticSearch7\elasticsearch.yml file. These values may vary depending on the customer environment.

```
PUT /_snapshot/infraskope_live_backup
{
  "type": "fs",
  "settings": {
    "location": "\\DAM\\esbackup",
    "compress": true
  }
}

PUT /_snapshot/infraskope_hot_repository
{
  "type": "fs",
  "settings": {
    "location": "\\DAM\\esarchive\\ESHOTARCHIVE",
    "compress": true
  }
}

PUT /_snapshot/infraskope_warm_repository
{
  "type": "fs",
  "settings": {
    "location": "\\DAM\\esarchive\\ESWARMARCHIVE",
    "compress": true
  }
}
```

```
1 - {
2   "acknowledged": true
3 - }
```

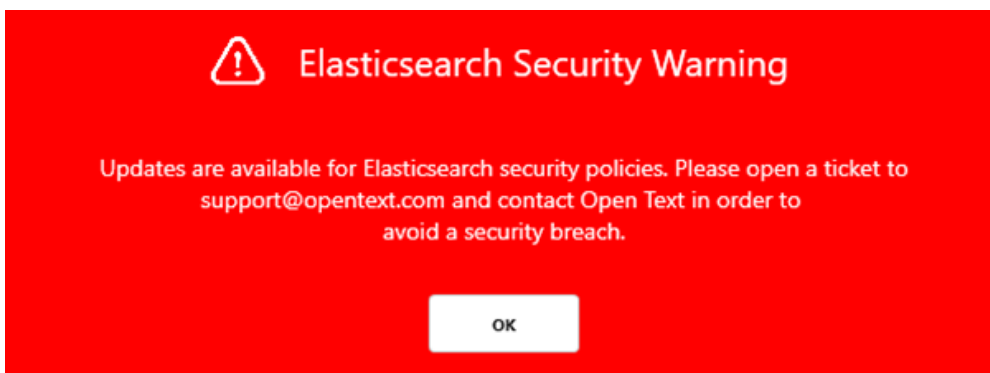
NOTE: After the necessary scripts are run in Sense Chrome, it is checked whether the commands are working correctly by typing the commands starting with GET.

```
GET /_template/all_indices
```

```
1 - {
2   "all_indices": {
3     "order": 0,
4     "index_patterns": [
5       "*"
6     ],
7     "settings": {
8       "index": {
9         "number_of_shards": "1",
10        "number_of_replicas": "0"
11      }
12    },
13    "mappings": {},
14    "aliases": {}
15  }
16 }
```

Elasticsearch Security Installation (Optional)

When Elasticsearch Security is not installed, the DAM application displays the following warning every time it is opened. The user can proceed by clicking the OK button.



If you want to install Elasticsearch Security, follow the steps below:

1. Extract the \InstallMedia\Stage2\ElasticsearchSecurity\Elasticsearch Security Tool.zip file into the C:\elasticsearch-7.16.3 folder.
2. Open PowerShell as an administrator and navigate to the C:\elasticsearch-7.16.3 folder.
3. Run the command .\Infraskope.ES.Elastic.Security.exe auto in the command prompt.
4. Enter the following information in the command prompt as Elasticsearch is being installed: **Elastic service name, Elastic URL, SQL Server name, SQL Server username, and password.**

NOTE: After installation elastic search security lines are added to the elasticsearch.yml file as follows.

```
cluster.name: DAMES7
node.name: "DAMES7_Master_Node"
node.master: true
node.data: true
node.ingest: false
path.repo: ["\\\\\\Dam\\esarchive\\ESHOTARCHIVE", "\\\\\\Dam\\esarchive\\ESWARGARCHIVE", "\\\\\\Dam\\esbackup"]
path.data: E:\ESDATA
network.host: 0.0.0.0
indices.breaker.fielddata.limit: 40%
indices.fielddata.cache.size: 20%
index.codec: best_compression
action.auto_create_index: +inventory*,+alerts_*,+events_*,.security*,.monitoring*,.watches,.triggered_watches,.watcher-history*,.ml*,-*
node.ml: false
xpack.ml.enabled: false
indices.query.bool.max_clause_count: 2048
transport.tcp.port: 9300
http.port: 9200
discovery.type: single-node
bootstrap.memory_lock: true

xpack.security.enabled: true
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.keystore.path: elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: elastic-certificates.p12
```

IMPORTANT: When the process is completed, the password created for Elastic will appear on the command screen. It is important to take note of this password.

```
Administrator Windows PowerShell
PS C:\elasticsearch-7.16.3> .\Infraskope.ES.Elastic.Security.exe auto
Infraskope Elasticsearch Security Tool
(c) 2024 Karmasis Inc,Ltd. All Rights Reserved.
Version: 7.11.33.47
*****
Elasticsearch Service Name: DAME57
Elasticsearch URL (http://localhost:9200): http://localhost:9200
*****
SQL Server Name: DAM
SQL Server User Name: sa
SQL Server Password: *****
Connecting to SQL Server...
SQL Server connection successful.
*****
Elasticsearch.yml file updated.
*****
Creating certificate...
Certificate created.
*****
Elasticsearch service restarting...
Stopped Elasticsearch service.
Starting Elasticsearch service...
Started Elasticsearch service.
Elasticsearch service restarted.
*****
Elasticsearch password creating (This may take some time)...

Your cluster health is currently RED.
This means that some cluster data is unavailable and your cluster is not fully functional.

It is recommended that you resolve the issues with your cluster before running elasticsearch-setup-passwords.
It is very likely that the password changes will fail when run against an unhealthy cluster.

Elasticsearch password created.

Please note your user name and password!
User name: elastic
Password: 05XI0h0JVTkq2DojtGg
*****
Security settings completed. Press 'C' key to exit...
```

5.

Console and Control Panel Setup

Console Setup

1. Go to `\\InstallMediaStage2\ProductComponents`.
2. Double click `DAM_Console.msi`.
3. On the **DAM Monitoring Setup Wizard** window, click **Next**.
4. On the **Select Installation Folder** window, enter the folder path to install **DAM Console**.
5. Select **Everyone** for **Install VDAM Server for yourself, or for anyone who uses this computer** field and click **Next**.
6. On the **License Agreement** window, choose **I agree** and click **Next**.
7. On the **Confirm Installation** window, click **Next**.
8. On the **Installation Completed** window, click **Close**.

Control Panel Setup

1. Go to **\\InstallMedia\Stage2\ProductComponents**.
2. Double click **DAM_ControlPanel.msi**.
3. On the **DAM Control Panel Setup Wizard** window, click **Next**.
4. On the **Select Installation Folder** window, enter the folder path to install **DAM Control Panel**.
5. Select **Everyone** for **Install DAM Server for yourself, or for anyone who uses this computer** field and click **Next**.
6. On the **License Agreement** window, choose **I agree** and click **Next**.
7. On the **Confirm Installation** window, click **Next**.
8. On the **Installation Completed** window, click **Close**.
9. After the Installation, open **Control Panel** from the **DAM Control Panel** desktop icon.
10. Enter **Server Name** as the given static IP of the machine

User Name : logadmin


Password : password1

Please provide your credentials

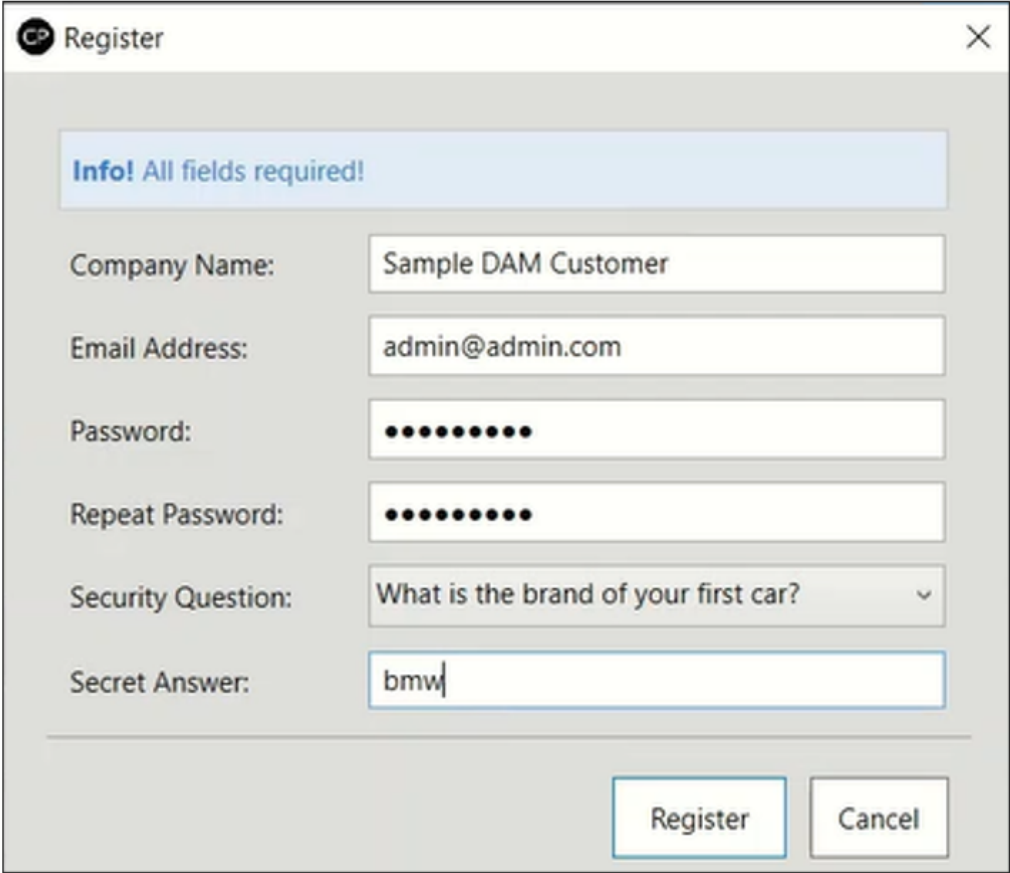
Server Name

User Name

Password

sign in 

11. Enter the text areas on the **Register** box.



The image shows a 'Register' dialog box with a title bar containing a logo and the text 'Register' and a close button. Below the title bar is a blue information bar that reads 'Info! All fields required!'. The main area contains several input fields: 'Company Name' with the value 'Sample DAM Customer', 'Email Address' with 'admin@admin.com', 'Password' and 'Repeat Password' both masked with ten black dots, 'Security Question' with a dropdown menu showing 'What is the brand of your first car?', and 'Secret Answer' with the value 'bmw'. At the bottom right are two buttons: 'Register' and 'Cancel'.

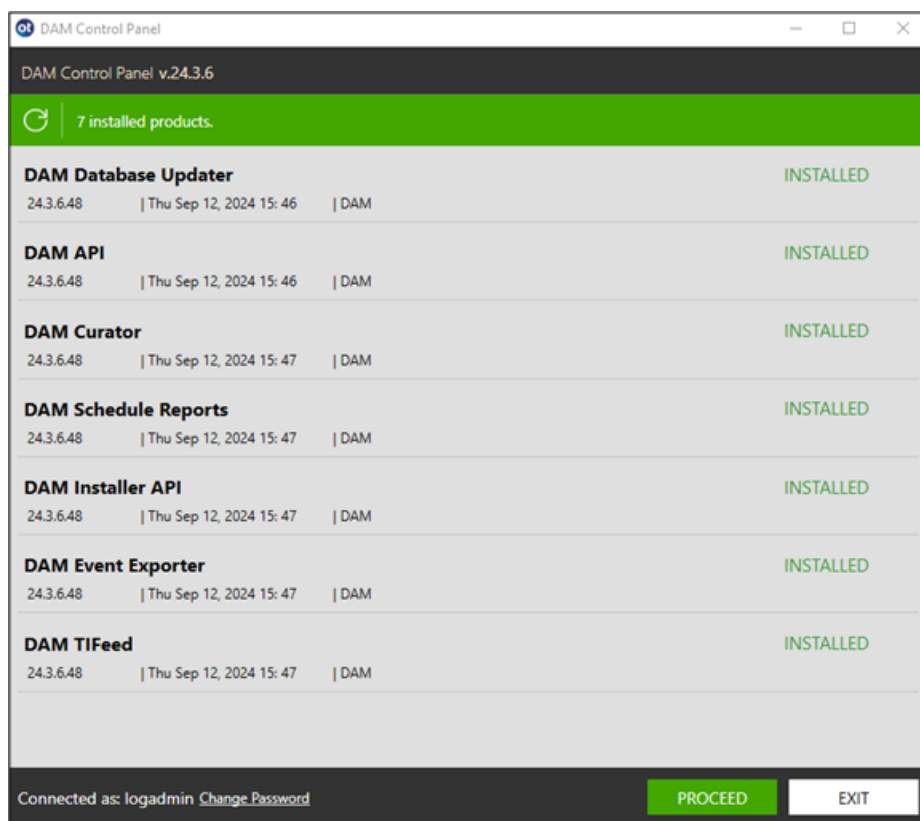
Company Name:	Sample DAM Customer
Email Address:	admin@admin.com
Password:	••••••••••
Repeat Password:	••••••••••
Security Question:	What is the brand of your first car? ▾
Secret Answer:	bmw

Licensing

Transfer the license documents to your virtual machine.

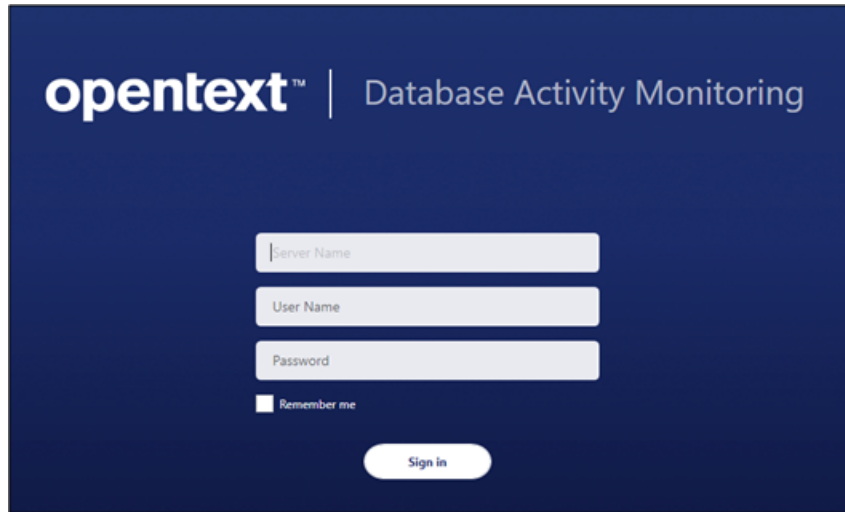
NOTE: The license must be located in C:\inetpub\wwwroot\ElfWebService folder path with app.license name.

1. When the license got taken and pasted as declared, the process would move on. Complete the installation through control panel as shown.



2. After the Installation, open dashboard from the OpenText Database Activity Monitoring desktop icon.
3. Enter the following:
 - **Server Name** : hostname / IP
 - **User Name** : logadmin

- **Password** : password1



The image shows a login interface for OpenText Database Activity Monitoring. The background is dark blue. At the top left, the 'opentext™' logo is displayed in white, followed by a vertical line and the text 'Database Activity Monitoring'. Below the header, there are three light gray input fields stacked vertically, labeled 'Server Name', 'User Name', and 'Password'. Under the 'Password' field, there is a small square checkbox followed by the text 'Remember me'. At the bottom center, there is a white rounded rectangular button with the text 'Sign in' in dark blue.