This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

SpeechMiner Administration Guide

Install and Configure Elasticsearch

6/13/2026

Install and Configure Elasticsearch

Elasticsearch 5.x

1. Download and run **java x64 JVM** version 8 or later.
2. Set the **JAVA_HOME** system environment variable:
   a. Enter the Variable name **JAVA_HOME**.
   b. Enter the Variable value. That is, the location of the **Destination Folder** in which you installed **java x64 JVM** version **8** or later. For example, C:\Program Files\Java\jre1.8.0_161
3. Download the **Elasticsearch Installer** from **`https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.6.16.msi`**.
4. Run **`Elasticsearch.msi.`**
5. Click **Next** in the **Locations** tab.
6. Click **Next** in the **Services** tab.
7. Set the **Configuration** tab as follow:
   - **Cluster Name:** Select a unique name.

     > **Important**
     > Use the same name in all the **ES Nodes** you install.

   - **Node Name:** Enter your computer name.
   - **Role:** Select **Master** or **Data** as needed and deselect **Ingest**.

     > **Important**
     > Elasticsearch should include at least one Data node and one Master node.

   - **Memory:** Select **`~40%`** of your available RAM memory and mark **Lock JVM** memory to prevent the **Elasticsearch** memory from being swapped.
   - **Network host:** Enter the server's **Hostname** or **IP Address**.
   - **Discovery:** Enter the **`(number of master nodes) / 2 + 1`**.
     For example, set **2** if there are 3 master nodes in your cluster.
   - **Unicast Hosts:** Add all the **`master nodes host:port`** to your cluster.

> **Important**
>
> If you choose to first create Data node, you can configure **Unicast Hosts** later in **`C:\ProgramData\Elastic\Elasticsearch\config\elasticsearch.yml`**

8. Click **Next > Install**.
9. Verify that Elasticsearch is functioning successfully:
   a. Open your Browser and in the **Address** field type **`http://<ElasticsearchMachineName>:9200/_cluster/health`**.
   Elasticsearch is working as expected if the page opens and the **Status** attribute is green or yellow.
   If the page does not open or the Status attribute is red, contact Genesys Customer Care for assistance.
10. Install **SpeechMiner**. For details refer to installation#Installing SpeechMiner.
11. Configure **SpeechMiner**. For details refer to configuration#Configuring SpeechMiner.
12. Verify that the Indexer is running and is able to connect to Elasticsearch:
    a. Enter **`http://<IndexerHostName>/indexer/api/v1/status`**. The Indexer is running and is able to connect to Elasticsearch if you see **`isAvailable:true`**.

Configure Elasticsearch on Windows

> **Important**
>
> - Edit your Elasticsearch configuration only in rare cases. For example, when adding an additional Master node to the system.
> - You can change the Data nodes indexer after the Indexer installation is complete. To do this, change the **esNodes Environment** value in the Indexer machine. You must use the following format: http://ES1:9200;http://ES2:9200;http://smithES2:9200
> - The number of shards and replicas are configured in the SpeechMiner database in the **indexParamsTbl** table in the **numberOfShards** and **numberOfReplicas** columns. You must configure the number of shards and replicas before you run UPlatform for the first time.
> - If the customer runs a Migration process, the number of shards and replicas should also be configured in the **LuceneToESMigration** tool configuration file.

1. Open **`C:\ProgramData\Elastic\Elasticsearch\config\elasticsearch.yml`**.
   a. Change the following settings:
      - **`cluster.name`**
      - **`node.name`**
      - Set **`bootstrap.memory_lock`** to **`true`**.

- Set **network.host** as the hostname or the server IP address.
- Set **discovery.zen.minimum_master_nodes** to (number of master-eligible nodes / 2 + 1). For example, if there are three **Master-Eligible** nodes, then **discovery.zen.minimum_master_nodes** should be set to **2**.
- Set **discovery.zen.ping.unicast.hosts** to a list of **Master-Eligible** nodes.

b. By default, a node is a **Master-Eligible** node, a **Data** node and an **Ingest** node.

- To create a dedicated **Master-Eligible** node, add the following settings to the **[node]** section:
  node.master: true
  node.data: false
  node.ingest: false
- To create a dedicated **Data** node, add the following settings to the node section:
  node.master: false
  node.data: true
  node.ingest: false

2. Open **C:\ProgramData\Elastic\Elasticsearch\config\jvm.options**.
   a. Change the **JVM heap' *size to ~40% of your RAM memory. For example, if you have 32 GB RAM, ensure that both -Xmx and -Xms values are set to 12g. For example,* -Xms12g** and **-Xmx12g**.
3. Restart the **Elasticsearch** service from the **Services** window to update the settings.

Elasticsearch 7.x

> **Important**
> Elasticsearch is built using Java and includes a bundled version of OpenJDK. To use your own version of Java, set the **ES_JAVA_HOME** environment variable. If you use a version of Java that is different from the bundled JVM, we recommend using a supported version of Java. Elasticsearch will not run if an unsupported version of Java is used. You may remove the bundled JVM directory when using your own JVM.

Install Elasticsearch 7.17.6

To download Elasticsearch,

1. Download **elasticsearch-7.17.6-windows-x86_64.zip** from Elasticsearch 7.17.6. **Note**: Select the **Windows** option to download a zip package.
2. Unzip it with your unzip tool. This creates a folder called **elasticsearch-7.17.6**.

To install Elasticsearch as a Windows service, do the following steps:

1. Open **Command Prompt** and navigate to the **elasticsearch-7.17.6** > **bin** folder.
2. Run the command, `elasticsearch-service.bat install`. This command installs Elasticsearch as a

Windows service.

3. Press **Windows**+**R** and type **services.msc**, and press **Enter**. This opens the **Services** window that lists all Windows services.
4. Verify that Elasticsearch 7.17.6 service is available and then start the service.

> **Important**
>
> You can also refer to the official Elasticsearch documentation on how to install it on Windows.

After the installation is completed, proceed to the **Configure Elasticsearch on Windows** section below for instructions on configuring Elasticsearch.

Install Elasticsearch 7.16.3

1. Download the **Elasticsearch Installer** from **`https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.16.3.msi`**
2. Run **`Elasticsearch.msi`.**
3. Click **Next** in the **Locations** tab.
4. Click **Next** in the **Services** tab.
5. Set the **Configuration** tab as follow:
   - **Cluster Name:** Select a unique name, for example elasticsearch.

     > **Important**
     >
     > Use the same name in all the **ES Nodes** you install.

   - **Node Name:** Enter your computer name.
   - **Role:** Select **Master** or **Data** as needed and deselect **Ingest**.

     > **Important**
     >
     > Elasticsearch should include at least one Data node and one Master node.

   - **Memory:** Select **`~40%`** of your available RAM memory and mark **Lock JVM** memory to prevent the **Elasticsearch** memory from being swapped.
   - **Network host:** Enter the server's **Hostname** or **IP Address**.
   - **HTTP port:** Set as **9200**.

- **Transport port:** Set as **9300**.
- (Optional) **This is the first master in a new cluster:** Leave it empty.
- **Seed Hosts:** Add all the **`master nodes host:port`** to your cluster.

> **Important**
>
> If you choose to first create Data node, you can configure **Seed Hosts** later in **`C:\ProgramData\Elastic\Elasticsearch\config\elasticsearch.yml`**

6. Click **Next > Install**.
7. Verify that Elasticsearch is functioning successfully:
   a. Open your Browser and in the **Address** field type **`http://<ElasticsearchMachineName>:9200/_cluster/health`**.
   Elasticsearch is working as expected if the page opens and the **Status** attribute is green or yellow.
   If the page does not open or the Status attribute is red, contact Genesys Customer Care for assistance.
8. Install **SpeechMiner**. For details refer to installation#Installing SpeechMiner.
9. Configure **SpeechMiner**. For details refer to configuration#Configuring SpeechMiner.
10. Verify that the Indexer is running and is able to connect to Elasticsearch:
    a. Enter **`http://<IndexerHostName>/indexer/api/v1/status`**. The Indexer is running and is able to connect to Elasticsearch if you see **`isAvailable:true`**.

Configure Elasticsearch on Windows

> **Important**
>
> - Edit your Elasticsearch configuration only in rare cases. For example, when adding an additional Master node to the system.
> - You can change the Data nodes indexer after the Indexer installation is complete. To do this, change the **esNodes Environment** value in the Indexer machine. You must use the following format: ;http://ES1:9200/
> - The number of shards and replicas are configured in the SpeechMiner database in the **indexParamsTbl** table in the **numberOfShards** and **numberOfReplicas** columns. You must configure the number of shards and replicas before you run UPlatform for the first time.
> - If the customer runs a Migration process, the number of shards and replicas should also be configured in the **LuceneToESMigration** tool configuration file.

1. Open **`C:\ProgramData\Elastic\Elasticsearch\config\elasticsearch.yml`**.

a. Change the following settings:

- **`cluster.name`**
- **`node.name`**
- Set **`bootstrap.memory_lock`** to **`true`**.
- Set **`network.host`** as the hostname or the server IP address.
- Set **`cluster.initial_master_nodes`** as the name of the master nodes. This name is the host name that you provided during the installation of Elasticsearch.
- Set **`discovery.seed_hosts`** to a list of **Master-Eligible** nodes.

b. By default, a node is a **Master-Eligible** node, a **Data** node and an **Ingest** node.

- To create a dedicated **Master-Eligible** node, add the following settings to the **[node]** section:
  `node.master`: true
  `node.data`: false
  `node.ingest`: false
- To create a dedicated **Data** node, add the following settings to the node section:
  `node.master`: false
  `node.data`: true
  `node.ingest`: false

2. Open **`C:\ProgramData\Elastic\Elasticsearch\config\jvm.options`**.
   a. Change the **JVM heap' *size to*** *`~40%`* ***of your RAM memory. For example, if you have 32 GB RAM, ensure that both*** *`-Xmx`* ***and*** *`-Xms`* ***values are set to*** *`12g`***. For example,** **`-Xms12g`** and **`-Xmx12g`**.
3. Restart the **Elasticsearch** service from the **Services** window to update the settings.

Elasticsearch 8.x

> ## Important
>
> Elasticsearch 8.x enables security (TLS/SSL and user authentication) by default. Applications must be configured to use **https://** and handle authentication.
>
> **SpeechMiner Compatibility:** This version of SpeechMiner supports both Elasticsearch 7.x and Elasticsearch 8.x.
>
> **Java Requirement:** Elasticsearch 8.x includes a bundled version of OpenJDK. To use your own version of Java, set the **ES_JAVA_HOME** environment variable. If you use a different JVM, Only supported Java versions (11 and 17) are allowed. Elasticsearch will not run if an unsupported version of Java is used. You may remove the bundled JVM directory when using your own JVM.

Install Elasticsearch 8.x

To download Elasticsearch,

1. Download **elasticsearch-8.18.0-windows-x86_64.zip** from Elasticsearch 8.18.0. **Note**: Select the **Windows** option to download a zip package.
2. Unzip it with your unzip tool. This creates a folder called **elasticsearch-8.18.0**.

To install Elasticsearch as a Windows service, do the following steps:

1. Open **Command Prompt** and navigate to the **elasticsearch-8.x.x** > **bin** folder.
2. Run the command, `elasticsearch-service.bat install`. This command installs Elasticsearch as a Windows service. Note: During this initial run, the console will display an enrollment token and a password for the elastic superuser. Copy and save these securely. You will need them for configuration and client connections.
3. Press **Windows**+**R** and type **services.msc**, and press **Enter**. This opens the **Services** window that lists all Windows services.
4. Verify that Elasticsearch 8.x.x service is available and then start the service.

> **Important**
>
> You can also refer to the official Elasticsearch documentation on how to install it on Windows.

5. Verify that Elasticsearch is functioning successfully:
   a. Open your Browser and in the **Address** field type **`https://<ElasticsearchMachineName>:9200/_cluster/health`**.
      - **Note:** You will need to accept any certificate warnings and provide the elastic username and its generated password when prompted.
   b. **Elasticsearch** is working as expected if the page opens and the **Status** attribute is green or yellow.
   c. If the page does not open or the Status attribute is red, contact Genesys Customer Care for assistance.
6. Install **SpeechMiner**. For details refer to installation#Installing SpeechMiner.
7. Configure **SpeechMiner**. For details refer to configuration#Configuring SpeechMiner.
8. Indexer **appsettings.json** configuration parameters should be configured according to the below table:

Parameter Name	Default value	Description	Valid values
IsSSLEnabled	true	Should be set to **true**, if ES8 **xpack.security.http.ssl.enabled** parameter is set to true	true,false
IsSecurityEnabled	true	Should be set to **true**, if ES8 **xpack.security.enabled** parameter is set to true	true,false

9. Verify that the Indexer is running and is able to connect to Elasticsearch:
   a. Enter **`http://<IndexerHostName>/indexer/api/v1/status`**. The Indexer is running and is able to

connect to Elasticsearch if you see **`isAvailable:true`**.

After the installation is completed, proceed to the **Configure Elasticsearch on Windows** section below for instructions on configuring Elasticsearch.

Configure Elasticsearch on Windows

> **Important**
> Edit your Elasticsearch configuration only in rare cases. For example, when adding an additional Master node to the system.

1. Open **`C:\ProgramData\Elastic\Elasticsearch\config\elasticsearch.yml`**.
   a. Change the following settings:
      - **`cluster.name`**
      - **`node.name`**
      - Set **`bootstrap.memory_lock`** to **`true`**.
      - Set **`network.host`** as the hostname or the server IP address.
      - Set **`cluster.initial_master_nodes`** as the name of the master nodes. This name is the host name that you provided during the installation of Elasticsearch.
      - Set **`discovery.seed_hosts`** to a list of **Master-Eligible** nodes.
      - **HTTP port:** Set as **9200**.
      - **Transport port:** Set as **9300**.
   b. By default, a node is a **Master-Eligible** node, a **Data** node and an **Ingest** node.
      - To create a dedicated **Master-Eligible** node, add the following settings to the **[node]** section:
        `node.master`: true
        `node.data`: false
        `node.ingest`: false
      - To create a dedicated **Data** node, add the following settings to the node section:
        `node.master`: false
        `node.data`: true
        `node.ingest`: false
2. Open **`C:\ProgramData\Elastic\Elasticsearch\config\jvm.options`**.
   a. Change the **JVM heap' *size to* `~40%` *of your RAM memory. For example, if you have 32 GB RAM, ensure that both* `-Xmx` *and* `-Xms` *values are set to* `12g`*. For example,* `-Xms12g`** and **`-Xmx12g`**.
3. Restart the **Elasticsearch** service from the **Services** window to update the settings.

Configure Users and Certificates for Elasticsearch 8.x

> **Important**
> The steps described in this procedure are meant to be an example for developers and should not be used in production. For a production environment, you should follow your own company's security policies for creating and signing certificates and creating users.

When securing your Elasticsearch 8.x cluster, you need to set up both:

- users & passwords for authentication
- SSL/TLS certificates for HTTPS and inter-node security

Below are the steps for both manual and automatic approaches.

Default Certificates (Windows):

During the first startup, Elasticsearch automatically generates self-signed certificates for HTTP and Transport Layer Security (TLS). These certificates are typically stored in the **<ES_HOME>\config\certs** directory. The **http_ca.crt** file is the CA certificate used to sign the HTTP layer certificates. You may need to import this into your client applications' trust stores for **https** connections if they don't trust self-signed certificates by default. **To download SSL Certificate**

1. Open Elasticsearch URL in browser: **https://<ElasticsearchMachineName>:9200**
2. A certificate warning will appear. Click on **"Not Secure" > Certificate (Invalid) > View Certificate.**
3. Click **Details > Copy to File.**
4. Follow the wizard to export as **Base-64 encoded X.509 (.CER)** format.

SSL/TLS Certificate Generation:

If you need to generate new self-signed certificates for HTTP communication (e.g., with custom hostnames or to replace the defaults):

1. Run the **certutil** helper:
   a. Navigate to **<ES_HOME>\bin** in Command Prompt (as Administrator).
   b. Run:

      ```
      elasticsearch-certutil http
      ```

   c. You will be prompted to:
      - Generate new CA or use existing.
      - Enter node hostnames/IPs that Elasticsearch will use.
      - Choose an output filename (e.g., **http-certs.zip** by default).
   d. This command generates a ZIP file containing the CA certificate and the node certificates.

2. Extract the certificates:
   a. Navigate to the directory where **http-certs.zip** was generated.
   b. Run:

      ```
      powershell Expand-Archive -Path http-certs.zip -DestinationPath certs
      ```

   c. This will create a **certs** folder (or overwrite an existing one) containing the extracted certificates (e.g., **ca.crt**, **node-1.p12**). Copy this **certs** folder to **<ES_HOME>\config**.
3. Configure HTTPS in **elasticsearch.yml**:
   a. Open **C:\elasticsearch-8.x.x\config\elasticsearch.yml**.
   b. Add/Modify the following settings to point to your newly generated certificates:

      ```
      xpack.security.enabled: true
      xpack.security.http.ssl.enabled: true
      xpack.security.http.ssl.keystore.path: certs/node-1.p12
      xpack.security.http.ssl.truststore.path: certs/node-1.p12
      # If your .p12 requires a password, add it securely to the keystore:
      # cd <ES_HOME>\bin
      # elasticsearch-keystore add xpack.security.http.ssl.keystore.secure_password
      ```

   c. Note: node-1.p12 is a common default filename; use the actual name if different.

How to add the Certificate to the Trust Store:

1. Open **Run** (Win + R) and type mmc.
2. Go to **File > Add/Remove Snap-in > Certificates > Add > Computer Account.**
3. Expand **Trusted Root Certification Authorities > Certificates.**
4. Right-click **Certificates > All Tasks > Import.**
5. Select your saved .cert file and complete the import wizard.
6. Restart browser and verify the certificate is now trusted.

Create a New user:

1. Open Command Prompt as **Administrator** and navigate to the **elasticsearch-8.x.x** > **bin** folder.
2. Run the command:

   ```
   elasticsearch-users useradd smuser123 -p smuser123 -r superuser
   ```

   Important: Replace smuser123 with a strong, unique password.

   Note: Please ensure user passwords do not contain the "@" symbol.

Below are some **useful references** from the official Elastic documentation and community resources:

- How to enable security, passwords, HTTPS, etc. → Set up minimal security for Elasticsearch
- Details about the elasticsearch-certutil helper script. → Elasticsearch certutil documentation
- Which users and roles are already available. → Built-in users and roles