Genesys Skills Management Installation and Configuration Guide for Active Directory

Genesys Skills Management 9.0

1/22/2022

Table of Contents

Genesys Skills Management Installation and Configuration Guide for Active Directory SSO

Welcome to the *Genesys Skills Management Installation and Configuration Guide for Active Directory*. Here you will find all the resources needed to setup an Active Directory authentication using the Secure Token Service (STS).

Prerequisites

Minimum System Requirements

- Operating System: Microsoft Windows Server 2008/2008 R2
- Microsoft .NET Framework 4

Windows Identity Framework

This guide provides instructions for setting up the Secure Token Service (STS) on Windows Server 2008 OS or above.

The web server needs to have the Windows Identity Foundation (**KB974405**) installed for the appropriate windows version/architecture.

- The download required is available from: http://www.microsoft.com/en-gb/download/details.aspx?id=17331
- Ensure you download the appropriate version for your web server.

SSL Certificate

The web server that is going to host the services must have an HTTPS binding. The certificate used for SSL can also be used for the encryption and signing of the services.

Windows Authentication

To support single sign on, the **Windows Authentication** role service for the **Web Server (IIS)** role must be installed. This can be found in the **Security** section of the role services.

Active Directory Login User Field

Performance DNA will need to be configured with a mapping between users' Active Directory (AD) accounts and their Performance DNA accounts. This can be defined either as the login ID in Performance DNA for new deployments (which must then match the users' AD login accounts) or as an additional Performance DNA user field which must then be populated with AD account names for upgrades.

Important

If you are accessing the services through a **FQDN**, you should ensure that clients see that **FQDN** as a local intranet site, otherwise windows will not pass the users credentials to the site. These settings may be found in Internet Options and will apply to all supported browsers other than Mozilla Firefox.

To support AD authentication via Firefox, follow the instructions for configuring Firefox to use Kerberos for SSO (https://docs.fedoraproject.org/en-US/Fedora//html/Security_Guide/sect-Security_Guide-Single_Sign_on_SSO-Configuring_Firefox_to_use_Kerberos_for_SSO.html).

Configuring IIS

Configuring IIS involves creating an application pool and granting certificate permissions.

Application Pools

For the services, create an application pool (called, for example, 'Services'). The application pool should use the **.NET Framework v.4.0.30319**, and be set to **integrated** mode.

Once you've created the application pool, go into the Advanced settings or properties for the pool and change the **Identity** to the account that you want to use, for example **Network Service**.

If you do not already have a separate application pool to run Portal, it is recommended that you do so now. Portal requires **.NET Framework v.4.0.30319**, and uses **integrated** mode. Similarly, you should then set the Identity for the pool to the account you want to use.

Certificate Permissions

The identities that run the services, Performance DNA, and Portal need access to the private key of the certificate that is used to sign the requests (for the STS) and encrypt the token requests (for Portal, Performance DNA, and the notification service).

Granting certificate permissions

1. Click **Start**.
2. Search for **mmc.exe** (Windows 7) or open a command line console via `start > run > cmd.exe`
3. Run **mmc.exe** or type `mmc.exe` into the command line console and press **Enter**.
4. Add the **Certificates snap-in** (choosing to manage certificates for the local computer account when asked) by clicking **File, Add/Remove Snap-in** and selecting the **Certificates** option from the **Available** snap-ins section.
5. Select **computer account**.
6. Under the **Certificates (Local Computer)** hierarchy expand the **Personal** node and click **Certificates**.
7. Right-click the certificate used for the web server, and choose **All Tasks > Manage Private Keys**.
8. If the application pool users do not appear in the list, click **Add** to add them.
9. Give the new user accounts **Read** access in the permissions list.
10. Click **OK** to save changes.
11. Right-click the certificate used for the web server and select **Copy**.

12. Browse to the **Trusted People/Certificates** folder and paste the certificate to this folder
13. Close **mmc.exe**.

Creating the Services

The procedures on this page assumes that all websites and services are created in **C:\Websites**; if this differs on your system, adjust these instructions accordingly.

1. Create a folder in **C:\Websites** (or your equivalent) called **Services**.
2. Copy the **STS** folder to the **Services** folder.
3. Copy the **NotificationService** folder to the **Services** folder.
4. In IIS, create a virtual directory in the root folder of the default website called **Services**. The folder should be **C:\Websites\Services** (or your equivalent).

Creating the STS application

1. In IIS, locate the **STS** folder within the **Services** virtual directory.
2. Right-click the **STS** folder and choose **Convert to application**.
3. Click the **Select** button and select the appropriate application pool from the list.
4. In the IIS **Authentication** feature for the application, ensure that both **Anonymous Authentication** and **Windows Authentication** are enabled.

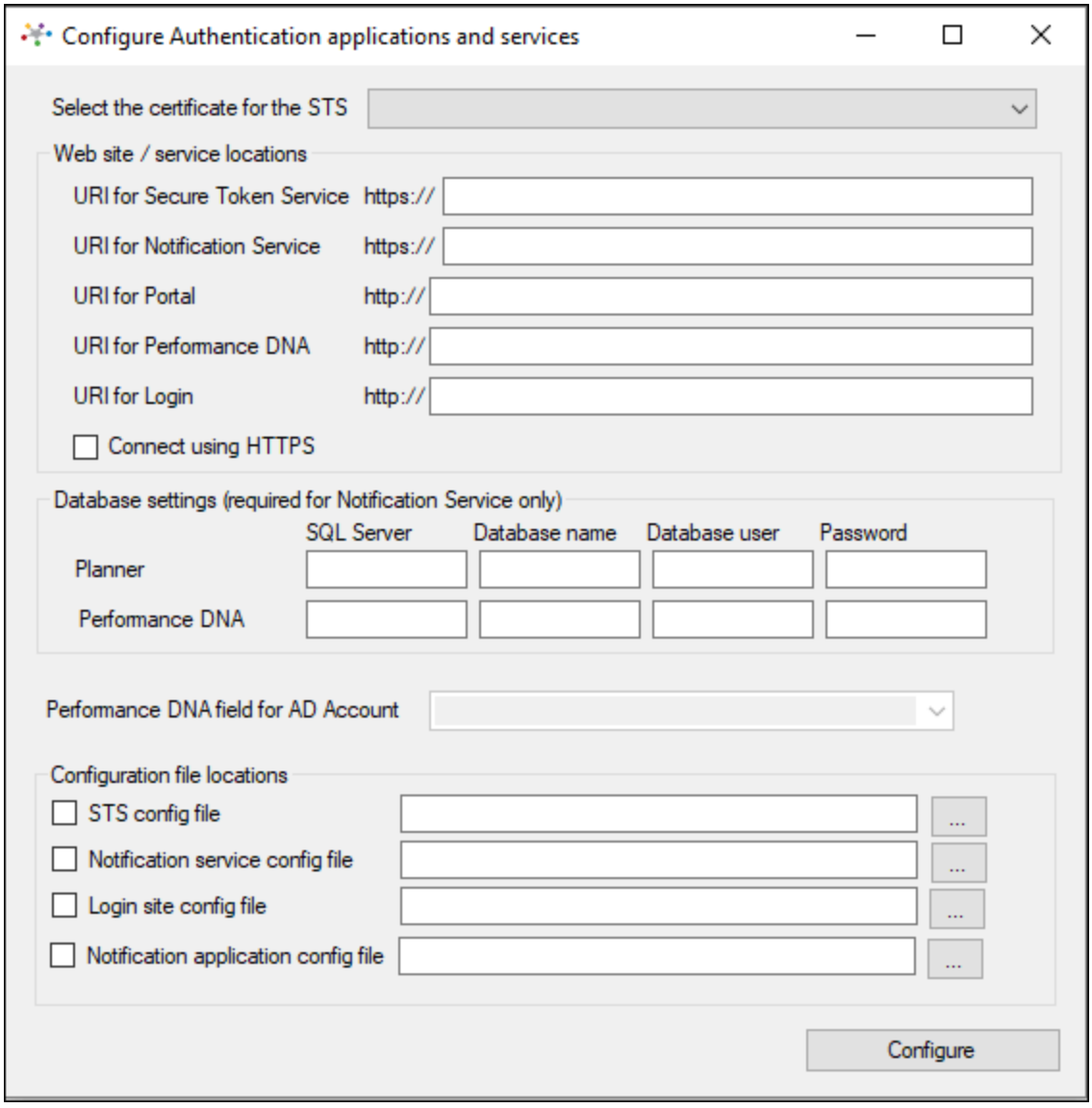
Creating the Notifications application

1. In IIS, locate the **NotificationService** folder within the **Services** virtual directory.
2. Right-click the **NotificationService** folder and choose **Convert to application**.
3. Click the **Select** button and select the appropriate application pool from the list.
4. In the IIS **Authentication** feature for the application, ensure that **Anonymous Authentication** is enabled.

Configuring the Services

You can configure the services using the **STS Configuration** Application. This application is available from the **STS Configuration** folder.

> **Important**
>
> Run the STS Configuration Application with the same username as was used for the PDNA installation.



Select the certificate to be used for signing and encryption of secure tokens from the **Select the certificate for the STS** drop-down. This should be the same certificate that the private key permissions were configured on previously.

Website / service locations

Complete the 5 URIs in this section, that is, the **STS**, the **Notification service, Portal, Login**, and **Performance DNA**, if applicable.

An example configuration would look like:

- https://<base URL>/services/xxxx

- https://<base URL>/TrainingManagerPortal
- https://<base URL>/PerformanceDNA
- https://<base URL>/Login

The **Portal** and **Performance DNA URI** fields are used to configure the Notification service so it will generate the correct launch URLs. They are also used in the site configuration files to set the valid URLs that the STS can use for Portal and Performance DNA.

It is recommended that the Secure Token Service and Notification Service URIs use the same SSL certificate. It is possible to use different URIs, however, this would require the creation of separate IIS sites and SSL certificates for each service.

> **Important**
>
> Ensure that the base URLs for the Notification Service and Performance DNA URIs are the same as this is required to allow the notification service access to the correct Performance DNA tenant. Also note that URIs are case-sensitive, that is, the settings entered into the configuration application must match the case of the folder names used in IIS.

By default, many customers use HTTP for their installation and required endpoints. If you're using HTTPS for the Training Manager Portal and Performance DNA sites, select the **Connect using HTTPS** check box.

Database settings (required for Notification Service only)

The database settings are required only for the Notification Service. The Notification Service is a stand-alone app and it's connection parameters are not configured anywhere during the installation of the solution. Therefore, you must set the **Planner** and **Performance DNA** database credentials here to build the Notification Service connection details.

Fill in the database connection details for Training Manager and / or Performance DNA depending on your configuration. Once you have completed all 4 boxes for one of the systems and clicked out of the field, the configuration application will try to connect to the database using the settings provided; if the connection succeeds you will see a green tick. If a cross appears, you can hover over it to view details of the issue.

Ensure that you set the **Performance DNA User Field for AD Account** value to the Performance DNA user field being used to hold users' Active Directory account names.

> **Important**
>
> If the name of the site used for the STS does not match the name of the web server, you will need to apply one of the solutions described in: http://support.microsoft.com/kb/896861 in order to allow administrators to login to Performance DNA directly on

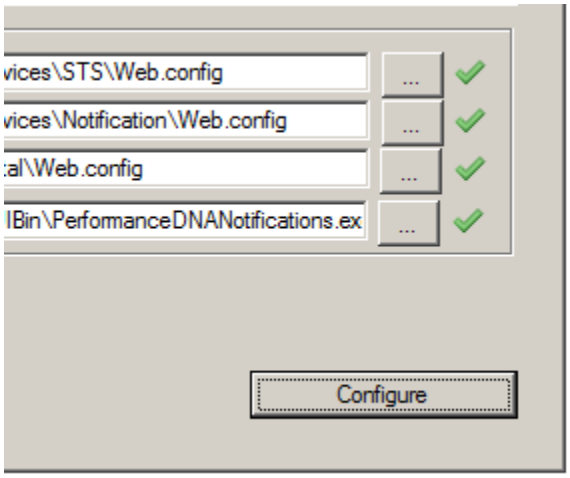
> the web server.

Configuring file locations

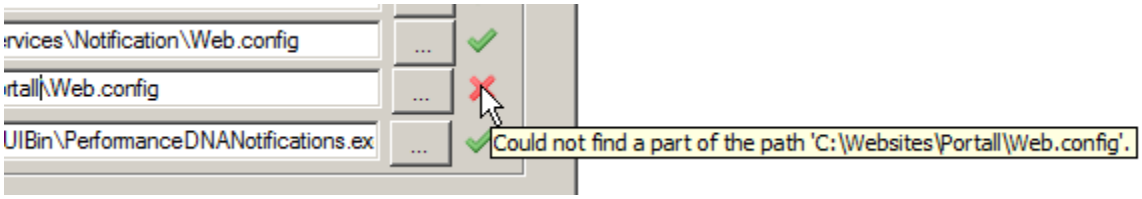
Using the […] buttons at the end of each field, browse for each of the specified configuration files (or type them into the boxes if you prefer).

If you want to omit a file at this time you can do so by leaving the field blank. For example, you may not have the notifications application on the server to configure. However, if you take a copy of the configuration from a client and configure it using this tool, you can then use that as a base configuration for all the notification client applications.

Once you have selected all the configurations, click the **Configure** button. A green tick will appear against each configuration you have selected that was configured successfully.



Should any of the configurations fail, you will receive a notification message, and a red ‘x’ will appear against the item that failed. If you hover the mouse pointer over the ‘x’, information will be shown as to the reason for the failure:



Once you have successfully installed and configured the STS service, users should be able to use their Active Directory credentials to login to Performance DNA and/or Portal automatically.