Skills Management 9.0.0

Automated Install and Upgrade Guide

About Genesys
Genesys powers 25 billion of the world's best customer experiences each year. Our success comes from connecting employee and customer conversations on any channel, every day. Over 10,000 companies in 100+ countries trust our #1 customer experience platform to drive great business outcomes and create lasting relationships. Combining the best of technology and human ingenuity, we build solutions that mirror natural communication and work the way you think. Our industry-leading solutions foster true omnichannel engagement, performing equally well across all channels, on-premise and in the cloud. Experience communication as it should be: fluid, instinctive and profoundly empowering. Go to www.genesys.com for more information.

Each product has its own documentation for online viewing at the Genesys Documentation website.

Notice
Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc. cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security
You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks
Genesys and the Genesys logo are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other company names and logos may be trademarks or registered trademarks of their respective holders. © 2017 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Technical Support from VARs
If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Ordering and Licensing Information
Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide***.

Released by: Genesys Telecommunications Laboratories, Inc. **http://www.genesys.com/**

Document Version: 90_skillsmanagement_automated-install-upgrade_06-2018_v9.0.001.00-B

Contents

Table of Figures

1 Introduction

This guide provides instructions for installing/upgrading the Skills Management suite via the Skills ManagementSetup_v9.0.0.0.msi application.

2 Prerequisites

If you are upgrading Skills Management, ensure that all Skills Management services on the web servers have been stopped prior to the upgrade, including IIS application pools and the Skills Management Invoker Service.

2.1 Database Server Software Prerequisites

- **Windows Server 2008 / 2008 R2 / 2012** (or higher) with latest available updates and service packs (for SQL2008R2 Service Pack 3 is required).
- **Microsoft SQL Server** of the following version / service pack (or higher)
    - **2012 RTM**
    - **2014 RTM**

- Administrator access to the SQL Server.
- SQL Server Collation settings:
    - Database level collation: The collation setting of the Skills Management databases must match the collation of the SQL Server instance.
- SQL Server Analysis Services should be available on the server.
- SQL Server Agent should be running on the server.

2.2 Web Server Software Prerequisites

- **Windows Server 2008 / 2008 R2 / 2012** (or higher) with latest available updates.
- **Microsoft .NET Framework 4.5.2** with latest available updates including **KB 2656351** (if available for your OS) **and KB2468871**.
- **Internet Information Services (IIS)**
    - IIS must be configured to allow **ASP.NET v4.0.30319**. For more information see: http://msdn.microsoft.com/en-us/library/k6h9cz8h.aspx
    - The IIS server role should have **Windows Authentication** installed (through **Add Roles and Features** in **Server Manager**, then choosing **Web Server (IIS) > Web Server > Security** in **Server Roles**).
    - The application pools used for the web applications and services must allow 32 bit processes.
- **Microsoft Windows Identity Foundation (KB974405)** for the appropriate Windows version/architecture
    - For operating systems prior to Server 2012, the download required is available here: http://www.microsoft.com/en-gb/download/details.aspx?id=17331
        - Ensure you download the appropriate version for your web server.
    - For Windows Server 2012: Run Server Manager, select the **Add Roles and Features Wizard** and enable **Windows Identity Foundation 3.5** in the **Features** Tab. Click **Next** and continue to complete the feature installation.

- The following additional runtimes must also be installed to support the Crystal Reports functionality:
    - **Crystal Reports Runtime**, available from: http://downloads.businessobjects.com/akdlm/cr4vs2010/CRforVS_redist_install_32bit_13_0_20.zip
- The following Server Roles/Features are required:
    - Server Roles
        - Web Server (IIS)
            - Web Server
                - Security
                    - Windows Authentication
                - Application Development
                    - ASP .NET 3.5
                    - ASP .NET 4.5
    - Features
        - .NET Framework 3.5
        - .NET Framework 4.5 Features
            - .Net Framework 4.5
            - ASP.NET 4.5
            - WCF Services
                - HTTP Activation
                - Named Pipe Activation
    - Windows Identity Foundation 3.5
- Administrator access to the server
- Sticky sessions must be enabled for load balanced environments where there is more than one web server.
- If you are installing the Training Manager client, note that both the Training Manager client and Skills Management web services must have network connectivity to the WFM.

Browser support: Web applications are supported in latest versions of Microsoft Internet Explorer, latest versions of Chrome and Firefox. If using Internet Explorer, ensure that compatibility mode is disabled, and that it set to use the latest possible standards mode.

Note: If your default web site does not have a port 80 HTTP binding, you must create one prior to running the installer. The binding can be safely removed after the install (provided you install the site with HTTPS enabled).

2.3 Service account considerations

The user account used to run the Skills Management services must have both **Log on as a batch job** and **Log on as a service** rights. You can use a local machine account for this provided that:

- The computer is not a member of a domain

  or

- The computer is a member of a domain and there is no group policy defining which accounts are able to log on as a batch job / service.

In the latter case, you **must** use a domain account as the service account.

2.3.1 Local user account

To give an existing local user account permissions to logon as a batch job and service:

1. Run **secpol.msc** or open **Local Security Policy** from **Control Panel / Administrative Tools**
2. In the left pane, expand **Local Policies** and select **User Rights Assignment**
3. On the right, locate the **Logon as a batch job** entry, and double-click on it.
4. If the user account in question does not appear in the list, add it using the **Add User or Group** option.
5. Click **OK** to close the dialog box.
6. Double-click on the **Logon as a service** entry.
7. If the user account in question does not appear in the list, add it using the **Add User or Group** option.
8. Click **OK** to close the dialog box.

2.3.2 Domain user account

Your domain administrator will need to allow the account in question permissions to log on as a batch job and as a service.

If you are installing Skills Management in a multi-server environment, a domain account is recommended for ease of configuration.

2.4 Networking pre-requisites

To allow DNA to be enabled, the MSTDC service on the database server must be accessible over the network from the web application server (i.e. not blocked by a firewall) – for details on checking MSDTC connectivity, see:
http://blogs.msdn.com/b/distributedservices/archive/2008/11/12/troubleshooting-msdtc-issues-with-the-dtcping-tool.aspx

2.5 Email Messaging Service

If upgrading from a release prior to v9.x the old Email Messaging Service will need to be uninstalled.

As part of the v9.x release this functionality is included within the main installer and is configured through the user interface.

3 Install/Upgrade process

If the previous version of the software was installed/upgraded via the automated installer then follow the steps in section 3.2. Alternatively, if either Performance DNA or Training Manager was installed/upgraded manually, follow the steps in section 3.1 to prepare the application server for an automated install/upgrade.

3.1 Upgrading from a manual installation/upgrade

Follow the steps below to prepare the server for installation/upgrade:

- Ensure that all prerequisites listed in the previous pages are present and at minimum supported version (unless specified)
- Backup up all databases (Performance DNA, Training Manager, DNA, ReportingDB/Skills ManagementReports), leave the existing databases on the database server, they will be automatically upgraded via the installer/upgrader.
- Back up all web server application files, including: sites, web services, storage folders: QMedia, crystal reports, custom company logos in Portal (if applicable), log files
- Remove all sites, services, virtual directories and related application pools from IIS and remove the original directories from the web server

Once these steps have been performed, continue with the steps in the following section.

3.2 Upgrading from a previous automated install/upgrade

Note: If you wish to upgrade Skills Management from version 4.2.0 or earlier you must first uninstall the old Skills Management server components via Control Panel -> Programs and Features.

Copy the release package to the web server and run the Skills ManagementSetup_v9.0.0.0.msi executable. On execution, the installer will check that the required version of .NET Framework is installed.

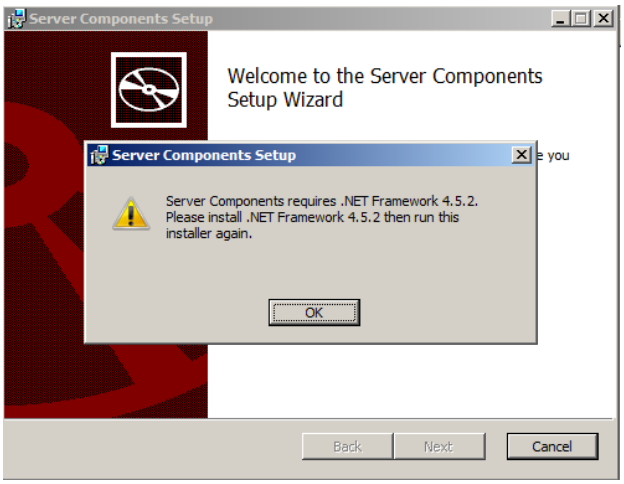


Figure 1: .Net Framework warning

Click OK then Finish to exit the installer before upgrading to the required version of .Net Framework and re-running Skills ManagementSetup_v9.0.0.0.msi.

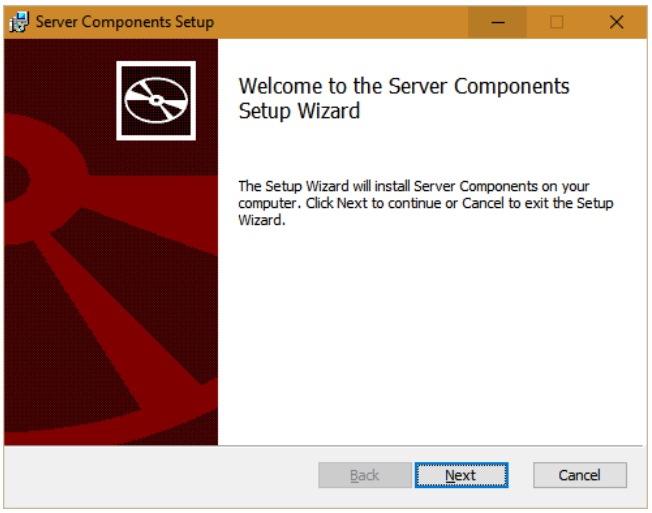


Figure 2: Welcome Screen

Click **Next** on the first screen.

The next screen allows you to modify the location of the web services, the virtual directory name for the web services and the hostname of the web server. There is also an option to enable IIS anonymous authentication for services (default). Unchecking this option will result in windows authentication being used for the services.

If you tick the “Use HTTPS to access services” option, then all the applications and services will be configured in IIS to use HTTPS rather than HTTP. Note that in this event, you should ensure that your webserver has a valid HTTPS binding, and that the host name you enter is valid for the certificate configured for the site in IIS.

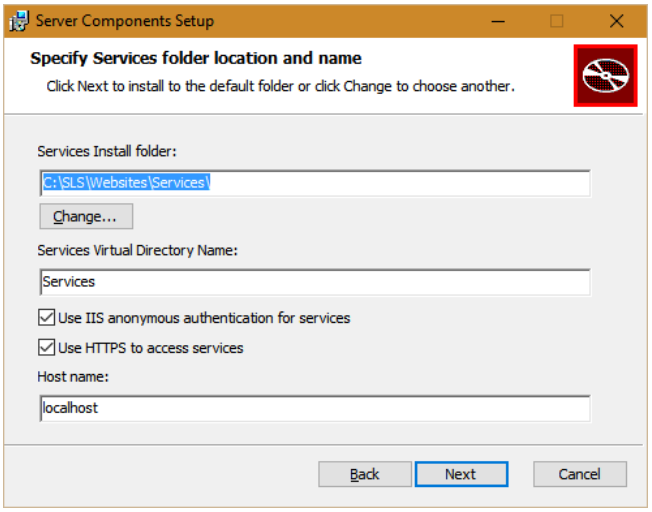
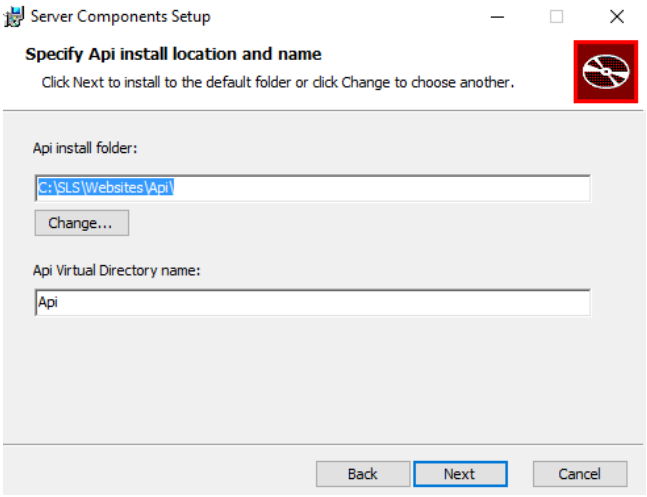


Figure 3: Web server settings

Update the settings as required, then click **Next**.



The next screen allows you to specify the physical location and virtual directory name of the Skills Management API. The values on this screen can be left at their default values. Click **Next** once you have specified these values.

The next screen allows the updating of the path for the miscellaneous files folder. Update the path if required, then click **Next**.

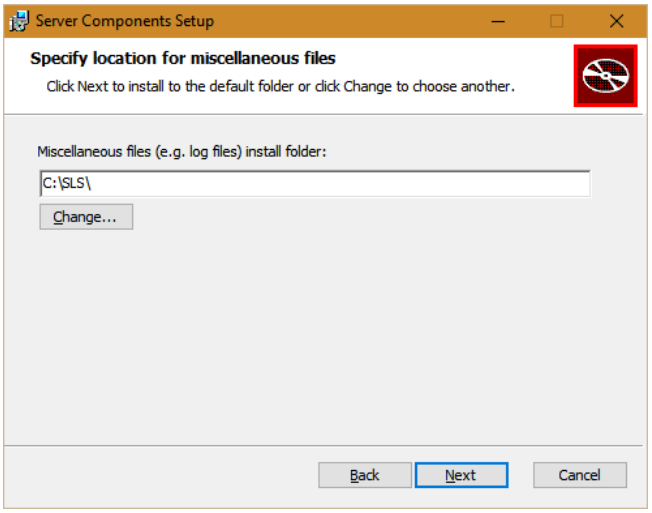


Figure 4: Miscellaneous files path

The next screen allows the updating of the path for the Applications folder. Edit the details if required, then click **Next**.

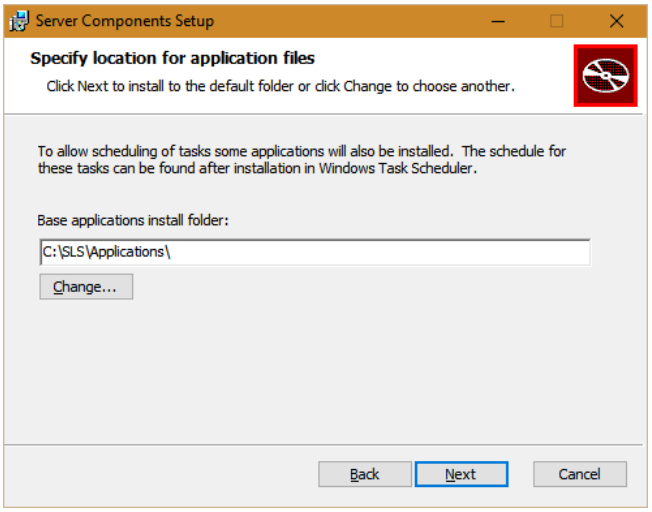


Figure 5: Applications folder file path

The next screen allows the updating of the path to the Portal folder on the web server and the name of the Portal IIS virtual directory. Edit the details if required, then click **Next**.

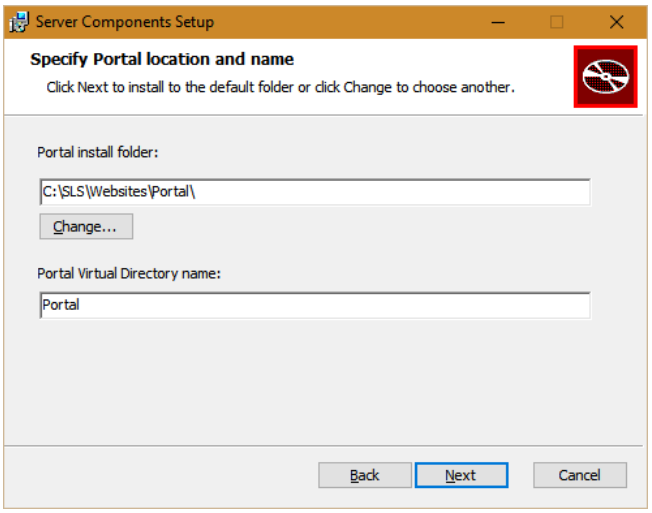


Figure 6: Portal path and IIS virtual directory

The next screen allows the updating of the path and IIS virtual directory for the Performance DNA site. Update the details if required, then click **Next**.

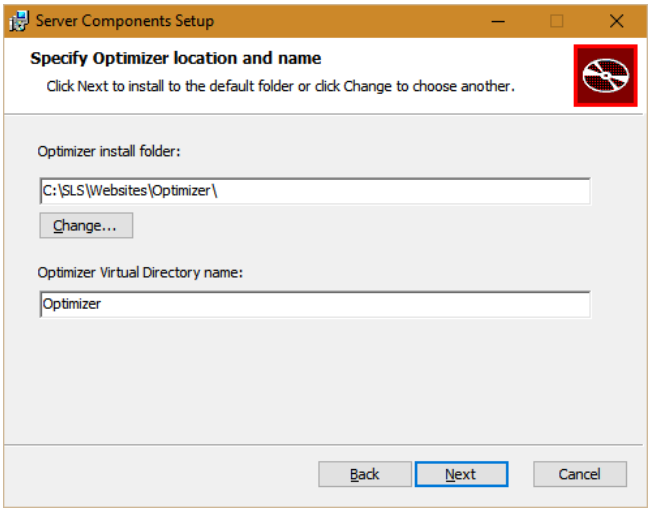


Figure 7: Performance DNA path and IIS virtual directory

The next screen allows the updating of the path and IIS virtual directory of the Login site. Update the details if required, then click **Next**.

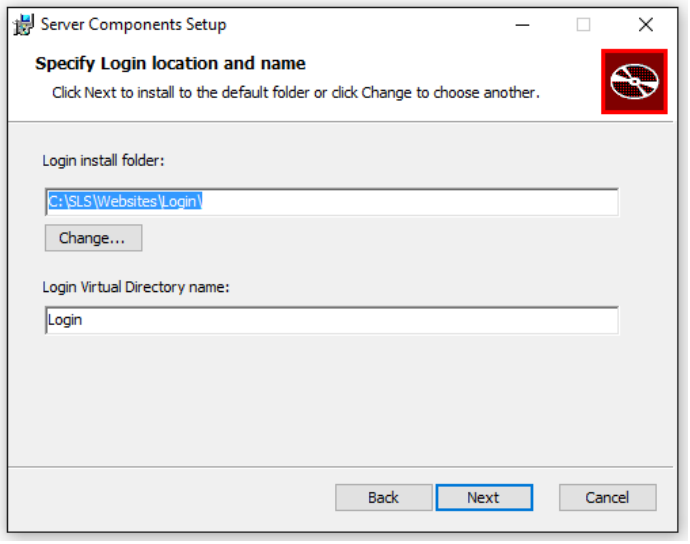


Figure 8: Login path and IIS virtual directory

The next screen requires the provision of a service account which is used to install the services. This account should exist on the machine and have local administrator privileges. As mentioned in the pre-requisites, the account must have “log on as a service” permissions.

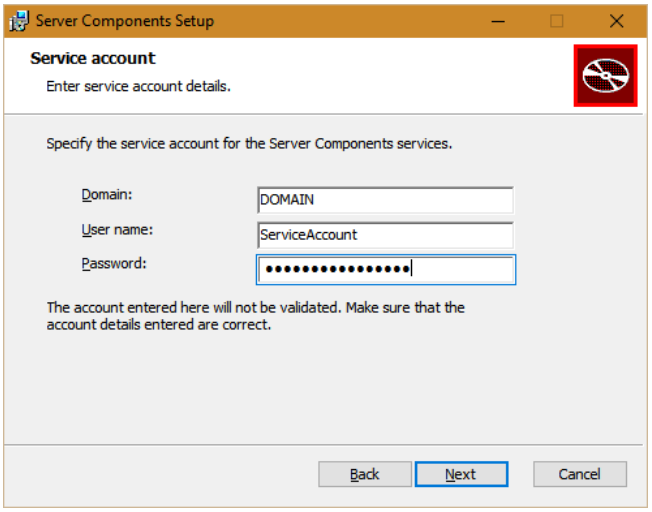


Figure 9: Service account details

The next screen allows for changes to be made to the database settings. Edit the changes if required, then click **Test Connection** to validate the connection settings and SQL Server release.

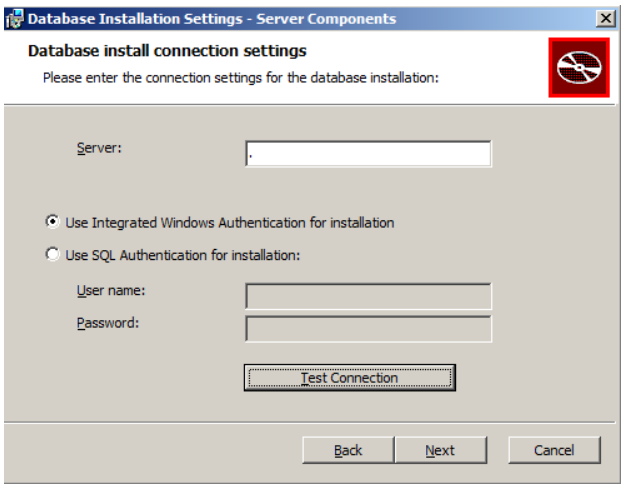


Figure 10: Database server and user account details

If the SQL Server release is not supported a Database version warning will be given.

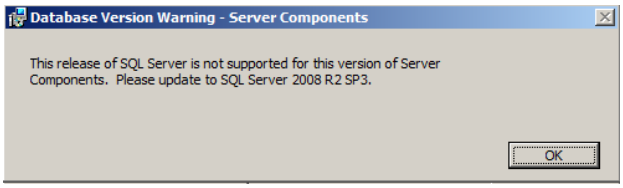


Figure 11: Example Database Version Warning

If a warning is given Click OK and cancel the install process before completing the required SQL server upgrade. Following the SQL Server upgrade re-run the Skills ManagementSetup_v9.0.0.0.msi

If the SQL Server release is supported and the details provided are valid you will receive the following confirmation:

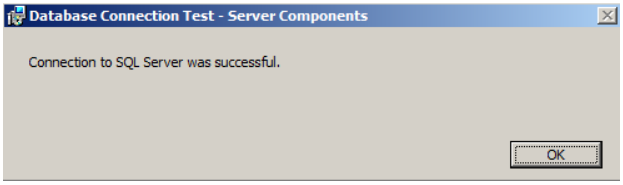


Figure 12: Database server and user account details

Click **OK** to continue with the installation.

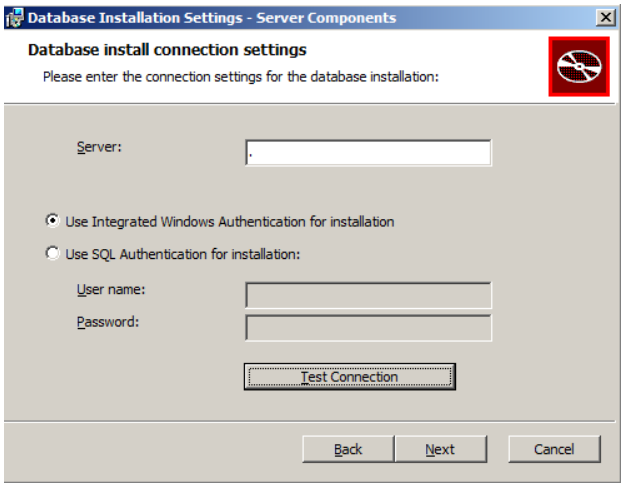


Figure 13: Database server and user account details

Following a successful connection test click **Next**.

The following screen allows for changes to be made to the database names and the database account used to login to the databases. If you are installing the software for the first time, the values in these fields should be left at their defaults. If you are upgrading the product, ensure that the databases specified match the names of your existing databases and that you enter the existing database user's details in the user name and password fields correctly.

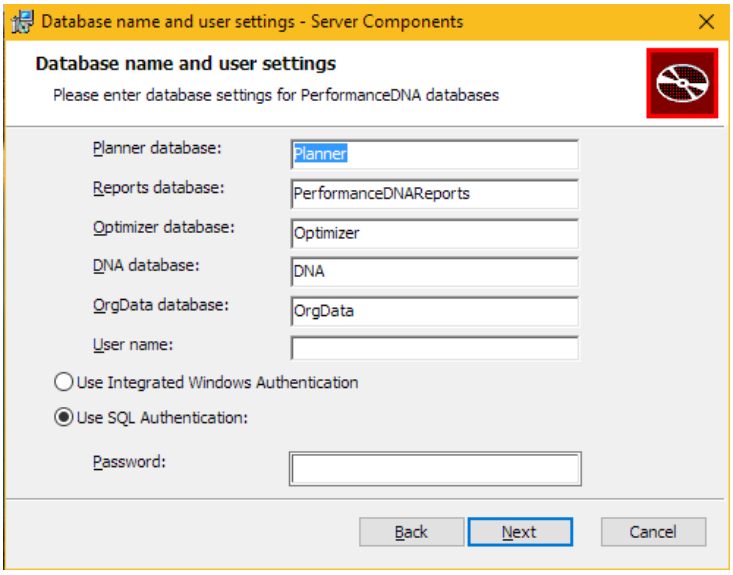


Figure 14: Databases and account details

Update these fields as required, then click Next to move to the Configure Tenant Administration user screen.

This screen is used to specify the username and password for the tenant administration area. If you have already specified a password other than 'password' for the tenant administration area, you can leave this form with default values, or modify the username and/or password.

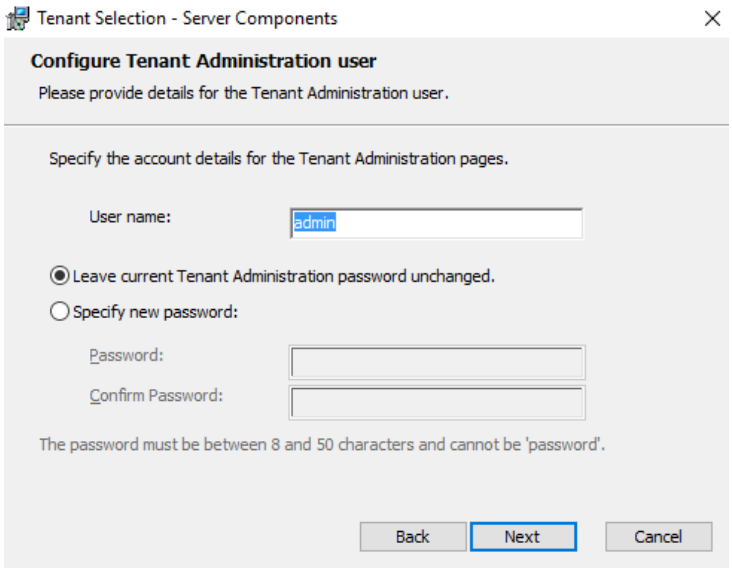


Figure 15: Databases and account details

Update these fields as required, then click Next to move to the STS Configuration screen.

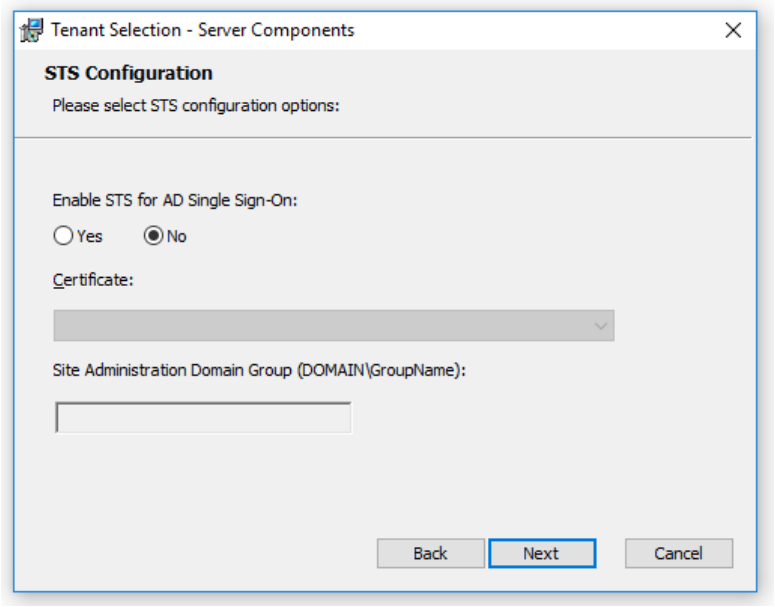


Figure 16: STS Configuration screen

If you wish to use Active Directory authentication via the STS service for authenticating users, click the Yes option in this screen and specify the certificate that you wish to use and the Site administration domain group that will have administrator access to the suite.

If you are upgrading a Skills Management instance that was previously using the STS service, tick Yes in this screen and specify the certificate and Site Administration Domain Group that you wish to use.

If you are installing a new Skills Management instance and wish to use the STS service, tick Yes in this screen, specify the certificate you want to use, specify the site administration domain group and click next. Proceed with the installation. Once it has completed, run the STSConfiguration application from the Release/STSConfig folder and follow the steps specified in the Installing and configuring AD authentication via the SLS Secure Token Service document to complete the STS Service configuration.

Update these fields as required, then click **Next** to move to the WFM system provider selection screen.

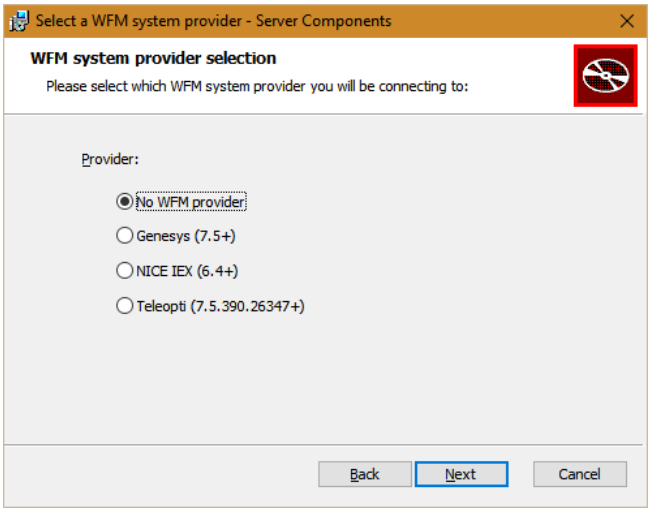


Figure 17: WFM system provider selection

Select a WFM system provider if required, then click **Next**.

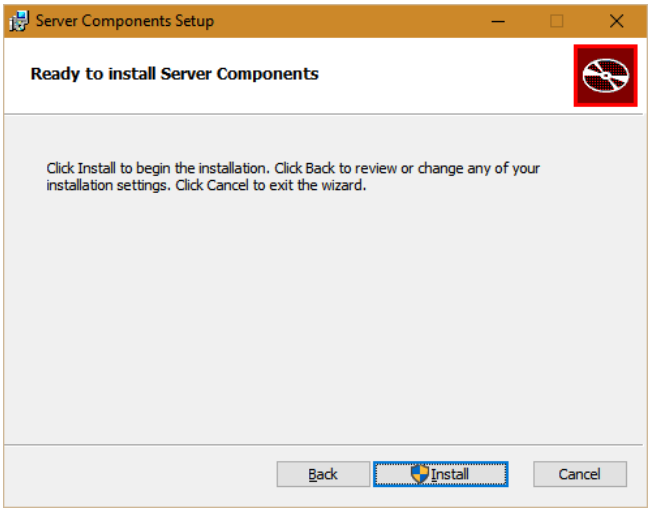


Figure 18: Install confirmation

Click **Install** on the next screen to begin the install/upgrade process.

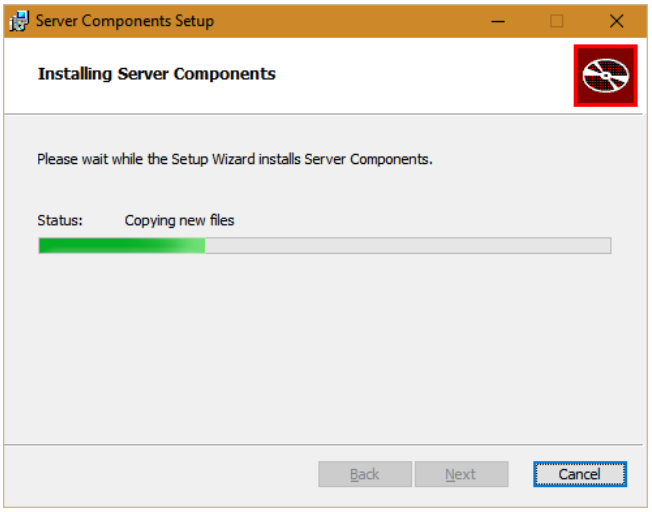


Figure 19: Install in progress

The final screen will confirm that the install/upgrade of the sites and services was completed. In version 4.8 this message will also contain the path to the PortalUsers.csv file which is required to complete the upgrade. Click **Finish** to close the application. The SkillsManagerWS Diagnostics page will launch allowing you to set up a license for Training Manager.

If you have run the setup program to upgrade your application from a previous version that was either installed/upgraded manually, ensure you copy the content of the following folders to the new folders created by the automated setup program:

- QMedia
- CrystalReports/Reporting
- Logs
- Skills Portal custom company logo

If you need to install DNA, follow the steps to configure DNA from the **Performance DNA v9.0.0.0 Manual Installation Guide**.

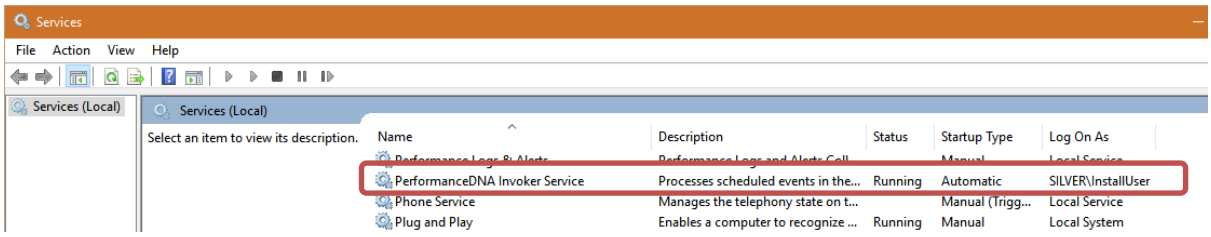
If you require STS and/or the Notifications client, follow the steps in the **Installing and configuring AD authentication via the SLS Secure Token** and **Notifications v9.0.0.0s Client Installation Guide** documents.

For **OrgData** please read **Org Data Import Configuration** document.

3.2.1 Check service credentials

Verify the credentials you entered were correct by checking the **Services** Administrative Tool.

Locate the **Skills Management Invoker Service** in the list of services, and ensure it is running. If it is not, this may be because the service account was not given log on as a service rights.



If the service is not running and you are using a local computer account (rather than a domain account) you can double-click the service and correct the credentials in the **Log On** tab.

If you are using a domain account, ensure that it has the rights to log on as a service and refresh the local group policy by running **gpupdate /force** from an elevated command prompt.

4 Exported Portal Users

The upgrade to Skills Management 4.8 creates a backup file containing Portal users which must be imported via Performance DNA in order to complete the upgrade process. Running the Skills ManagementSetup_v9.0.0.0, entering the required information in each screen will result in a final 'Completed the Server Components Setup Wizard' screen. This screen will also contain the path to the exported Portal users file, called PortalUsers.csv. Once the upgrade is completed, login to Performance DNA as an administrator and follow the wizard to complete the upgrade process. This will require importing the PortalUsers.csv file.

If you are upgrading an Azure instance of Skills Management, the PortalUsers.csv file will be created in the directory from which you ran the Setup-Skills ManagementAzure.ps1 PowerShell script.

5 Additional steps required to complete an upgrade to version 4.8

Upgrading from versions prior to 4.7 to 4.8 requires additional steps to import Training Manager users into Performance DNA. After finishing the Skills Management upgrade (via the installer or PowerShell script for Azure deployments), a file will be created (named PortalUsers.csv) which contains all of the Portal users that need to be imported into Performance DNA to complete the upgrade. This file will be created in the directory where the Skills Management installer/azure script is located and is required to complete the upgrade process. It is important that the user performing the upgrade has write permissions to the folder from which the installer/Azure script is executed to ensure that this file is written successfully. If the release package was provided on a non-writeable medium, e.g. DVD, ensure that the installer/Azure script are copied to a writeable location before running them.

Follow the steps below to complete the upgrade process.

1. Login to the Performance DNA tenant administration area (via the 'localhost' address).
2. Click the Tenant Management option in the menu. On the right side of the Manage Tenants page.
3. Select the tenant that you have mapped to your Training Manager deployment and click its associated **Import Portal Users** link.
4. A Settings page will appear, requiring the selection of relevant user fields for the Portal Username, Portal Employee ID, Email and Location fields. Either select the relevant fields using the associated select box or click the **New** button to create a new user field which will be used for the mapping of the relevant list item. The location delimiter specifies the character that you wish to use to delimit locations. Click **Next**. The validation process may take several minutes to complete.
   Note: You must map one or more fields to the LoginId.
5. In the Import page, click the **Choose File** button to select the portal users file. Click the **Next** button.
6. The **Import Preview** page will display a table of the number of users that will be created or updated in each Portal role and the total number of created/updated users. This page will also display any validation errors that were identified in the import file. At this point it is possible to end the process without completing the user import in order to make corrections to the import file. Alternatively, click the **Import** button to import the users. Depending on the number of users in Portal and Performance DNA, the upgrade may take several minutes to complete.
7. Once the import has completed, a confirmation message will be displayed. Click the Finish button to complete the upgrade process. Performance DNA tenants will now be available for use again. If the Import is unsuccessful, correct your user import file and repeat the process.

Notes:

- All Performance DNA tenants will be unavailable following the upgrade until the Portal users file has been imported. Training Manager users should not be modified until the Portal users file has been imported into Performance DNA.

- When upgrading Skills Management to version 4.8 it is not possible to include fields that contain different data into a single field, i.e. mapping UserName and EmployeeID into LoginID. If any of the data in these fields is different the import will fail.

6 Post upgrade steps

6.1 Removing artefacts from previous installations

If you are upgrading from a version prior to 9.0, there may be items left behind after the upgrade that can be safely removed. Genesys recommend taking a backup of any database before permanently deleting it.

6.1.1 Microsoft Analysis Server Databases

These will typically have a name of the format **DNACube_**<Unique Name>**_**<Number>. These databases were required by the old "DNA Cube" functionality which has been superseded by the Data Warehouse.

The Performance DNA service user account will no longer require access to the Analysis Server. Provided the account is not shared with other systems, the user can be removed from the Analysis Server Administrators role.

6.1.2 DNA Databases.

These databases can be identified because they will contain, amongst others, the tables:

- **DNA**
- **DNAComponent**
- **DNACube**
- **DNAUserDetails**

These databases were created per-tenant, and have been superseded by the Data Warehouse.

Note: If you locate a candidate DNA database and it contains more than 50 tables then you should not delete it without first checking with Genesys as it may be being used for data other than legacy DNA data.

6.1.3 Deprecated scheduled tasks for Performance DNA

Some of the scheduled tasks created by previous releases of Performance DNA are no longer required. These will be called

- **<SystemName> Process Queues**
- **<SystemName> DNA Cube Refresh**

where <SystemName> is the name of the system, e.g. "PerformanceDNA" (this may vary depending on the installer used)

6.2 Configure Training Manager-Performance DNA Integration

In previous versions, the Training Manager-Performance DNA integration (the setting of the Performance DNA URL and tenant ID) was configured via the SkillsManagerWS web.config file. These settings have been moved to the Settings page in Portal and must be replaced after an upgrade. To update these settings:

1. Login to portal as an Administrator
2. Click the system settings page link
3. Set the Performance DNA URL. Once this has been set the Tenant dropdown will be populated with a list of tenants.
4. Select the Tenant that Training Manager should integrate with.
5. Click the Save button.

Training Manager client users will then be able to connect to the Performance DNA tenant specified.

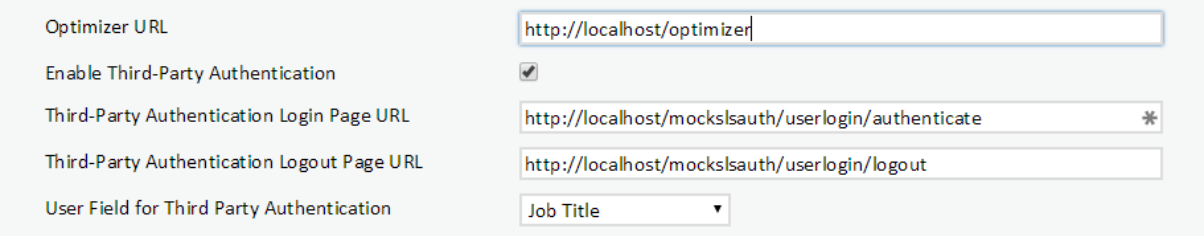
6.3 3rd Party Authentication

The latest version of Performance DNA and Portal now allow for a 3rd party authentication scheme. This requires a software component provided by a customer to authenticate against a customer's database of users. This facility is provided as an alternative to the STS configuration.

When configured correctly the login screen will re-direct to a customer provided web site to enter user credentials. The 3rd party application will need to call a Web service provided by Silver Lining with an authentication token when the user is authenticated. The 3rd Party Application will then re-direct back to a landing page which will validate the authentication token and log the user in to the system.

6.3.1 Performance DNA Configuration

The following settings must be provided in the System Settings for Performance DNA to enable 3rd Party Auth:



- A Tick box to enable 3rd Party Auth, this makes the other fields appear.
- The 3rd Party Auth login page.
- The 3rd Party Auth logout page.
- The user field in Performance DNA to use for choosing which user to login.

6.3.2 Portal Configuration (via Training Manager)

The following settings must be provided in the Portal Settings page of Training Manager to enable 3rd Party Auth:

- A drop down so you can choose whether to user the user name or employee name for authentication.
- The 3rd Party Auth login page.
- The 3rd Party Auth logout page.

6.4 E-mail ADG Setting for IEX WFM

In previous versions the IEX e-mail ADG was specified via the SkillsManagerWS/WebSettings.config file. This setting has been removed from this file. The e-mail ADG is now set in the Training Manager Portal screen of the Training Manager client (labelled “Email ADG Name”). The upgrade process does not retain this value, therefore, it is necessary to replace it in the Training Manager Portal settings screen after upgrading.

6.5 Configuring Updating Routing Skills

6.5.1 Connectivity Overview

Performance DNA updates routing skills in Genesys through the GIS SOAP webservice interface. Firstly a connection is made to the **SessionService** service to get a GIS Session token, then various calls are made to the **CSProxyService** service to retrieve and update information in CME.

6.5.2 Configuring Performance DNA to work with GIS

6.5.2.1 Enabling GIS

6.5.2.2 ***Before the configuration options for GIS will appear in Performance DNA,GIS needs to be enabled. This can be done on the General Settings tab within System Settings.***

For further instructions on setting up GIS Authentication options, please see the Performance DNA Administrator guide.

7 Licensing

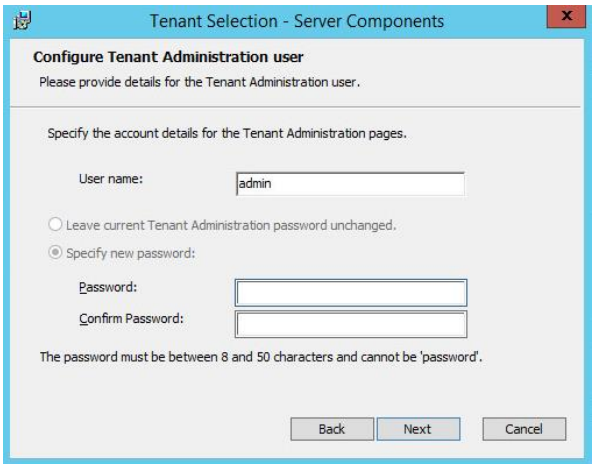
The following sections describe the licensing options in Performance DNA and Training Manager. If you have upgraded your product and your licences are still valid, there is no need to modify your existing licensing settings.

7.1 Licensing Performance DNA

7.1.1 Tenant Administration

The Tenant Administration part of the application is accessible through the web server's hostname/login/admin, e.g. http://yourserver/login/admin.

To login to the tenant administration area, use the tenant administration account details that were specified during the install/upgrade process (see below screenshot of the relevant installer screen, note – this screen will not be available if using the command-line only installer or Azure install/upgrade script).



Once logged in you should see the Tenant Management screen.

1. Click the **Create New Tenant** button.
2. Enter the name and primary contact details for the tenant that will be using the application, then click **Next**.
3. Enter the license details for this tenant into the boxes provided then click **Next**. If you do not have a licence for Performance DNA but have a licence for Training Manager, complete the host name and specify a licence date, e.g. **01/01/2030.** The remaining licence fields should be left blank. This will result in only core Performance DNA functionality being available. It will be necessary to enter your Training Manager licence (via the steps in the following section) in order to use the system.
4. Enter the administrator user details to create a new administrator for the tenant.
5. Click **Finish** to close the wizard.

If you wish to convert Performance DNA to use Active Directory authentication rather than the default form-based login system, please consult the **Installing and configuring AD authentication via the SLS Secure Token Service** document.

7.2 Licensing Training Manager

To set up your Training Manager license open a web browser and navigate to the **SkillsManagerWS** application, e.g. http://localhost/SkillsManagerWS/Default.aspx (or right-click the **SkillsManagerWS** folder within IIS, and then select **Browse**).

Click the **Manage Your Licenses** link. A form will appear allowing you to enter your Training Manager product license. Complete the form and click the **Add/Update License** button to add a new product license. Alternatively, if you have already added licenses, click one of the links at the top of the form to view and/or edit the existing license(s).

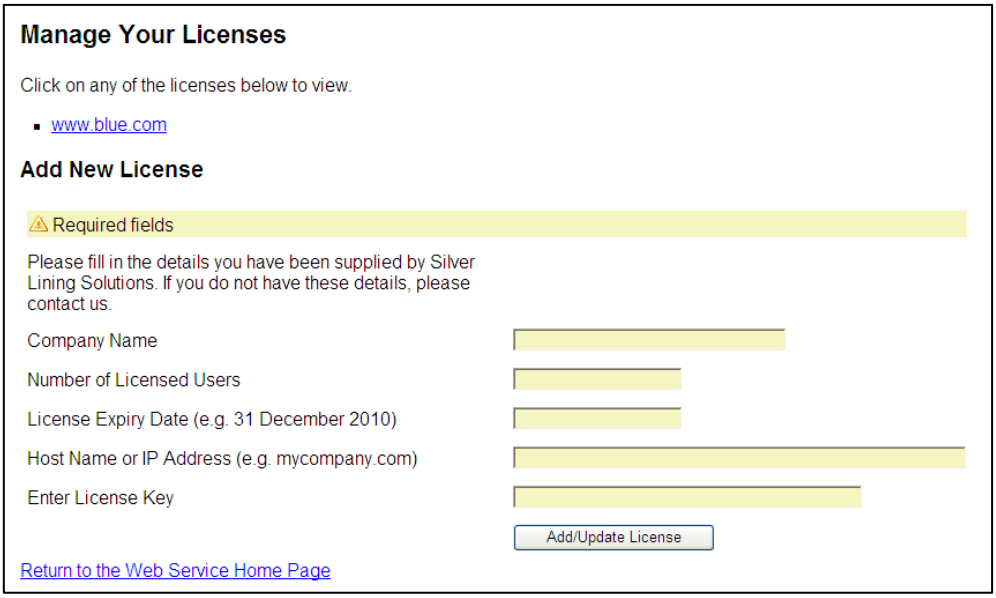


Figure 20: Licensing

The system will be available once you have either a Performance DNA licence, Training Manager licence or both. The widgets that are available in the system will be based on the licence status, i.e. all widgets for both Performance DNA and Portal will only be available if you have a valid licence for both products. If you have one valid product licence, only the widgets that are related to that product will be available. Performance DNA administrators will be able to see all Performance DNA widgets. Similarly, Portal Administrators will be able to see all Portal widgets. If you have both Performance DNA and Training Manager licences, it will be possible to assign users to both Performance DNA and Portal administrator roles so that they will be have full access to the widgets of both products. Other users' access is restricted based on the widgets available to their assigned roles.

7.3 Configuring SAML authentication

Performance DNA can be configured to use SAML authentication to authenticate users. Follow the steps below to configure the required Performance DNA settings to enable SAML authentication.

1. Login to the Performance DNA tenant that you wish to configure for SAML authentication as a tenant administrator.
2. Click on the System Settings widget under the System section of the menu.
3. Click on the Authentication tab at the top of the page.
4. Click the '+ Add' button.
5. Complete the form with the relevant details. The Authenticating field should be set to the user field that contains the login names that are to match the SAML login requests.
6. Click the Save button.

The Authentication tab in the System Settings page lists saved SAML authentication providers. These can be edited via the edit button, deleted using the 'X' button and re-prioritised using the up and down arrows. Providers can also be enabled/disabled using the Enabled checkbox in the create/edit form.

If more than one provider is present and enabled, Performance DNA will attempt to log users in using the provider with the highest priority first. If this fails, the next provider available enabled provider will be used until the user is logged in successfully or login via all providers has failed.