Genesys Skills Management Automated Install and Upgrade Guide

Genesys Skills Management 9.0

1/18/2022

Table of Contents

Genesys Skills Management Automated Install and Upgrade Guide

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

[+] Note about Performance DNA in Genesys Engage cloud

As of March 2019, Performance DNA (PDNA) is only available as a Genesys Engage cloud product supporting hybrid architectures. This change is applicable to new customers only.

- If you are an existing Genesys Engage on-premises customer and are looking to add PDNA functionality, you can now use PDNA through a hybrid architecture with PDNA hosted on standalone cloud.
- If you are an existing PDNA on-premises customer, you can continue to use the software in an on-premises deployment. Security updates and hot fixes for critical defects will still be provided and you can still buy additional licenses if more are required.
- If you are interested in migrating from the on-premises version of PDNA to the Genesys Engage cloud version, contact your account representative.

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.

Database Server Software Prerequisites

- **Windows Server 2008 R2 / 2012** (or higher) with latest available updates.
- **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 Agent should be running on the server.

Web Server Software Prerequisites

- **Windows Server 2008 R2 / 2012** (or higher) with latest available updates.
- **Microsoft .NET Framework 4.7.2** 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:
  - For **Crystal Reports Runtime**, download **SP20** from: https://www.tektutorialshub.com/crystal-reports/how-to-download-and-install-crystal-report-runtime/#hownbspto-download
    - 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
      - Application Initialization (for Server 2012+)
- Features
  - .NET Framework 3.5
  - .NET Framework 4.5 features
    - .Net Framework 4.5
    - ASP.NET 4.5
    - World Wide Web Services
      - Common HTTP features
        - Static content
    - WCF Services
      - HTTP Activation
      - Named Pipe Activation

- 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.

> **Tip**
>
> 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).

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.

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 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 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.

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.

Azure

If you are installing PDNA to Azure web application, ensure that the client machine running the powershell scripts must have .NET 4.7.2 installed.

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.

Install or Upgrade process

If the previous version of the software was installed/upgraded via the automated installer then follow the procedure Upgrading from a previous automated install/upgrade. Alternatively, if either Performance DNA or Training Manager was installed/upgraded manually, follow the procedure Upgrading from a manual installation/upgrade to prepare the application server for an automated install/upgrade.

> **Important**
>
> When upgrading (either manual or automated), ensure that all Login Ids within the system are unique. If there are duplicate Login Ids, the Performance DNA installer will not allow you to proceed with the upgrade until you resolve the duplicates. You can view the duplicate Login Ids in the installer's log file. The Login Ids within the system must be unique for both on-premise and Azure installations.

Upgrading from a manual installation/upgrade

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

- Ensure that all prerequisites 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.

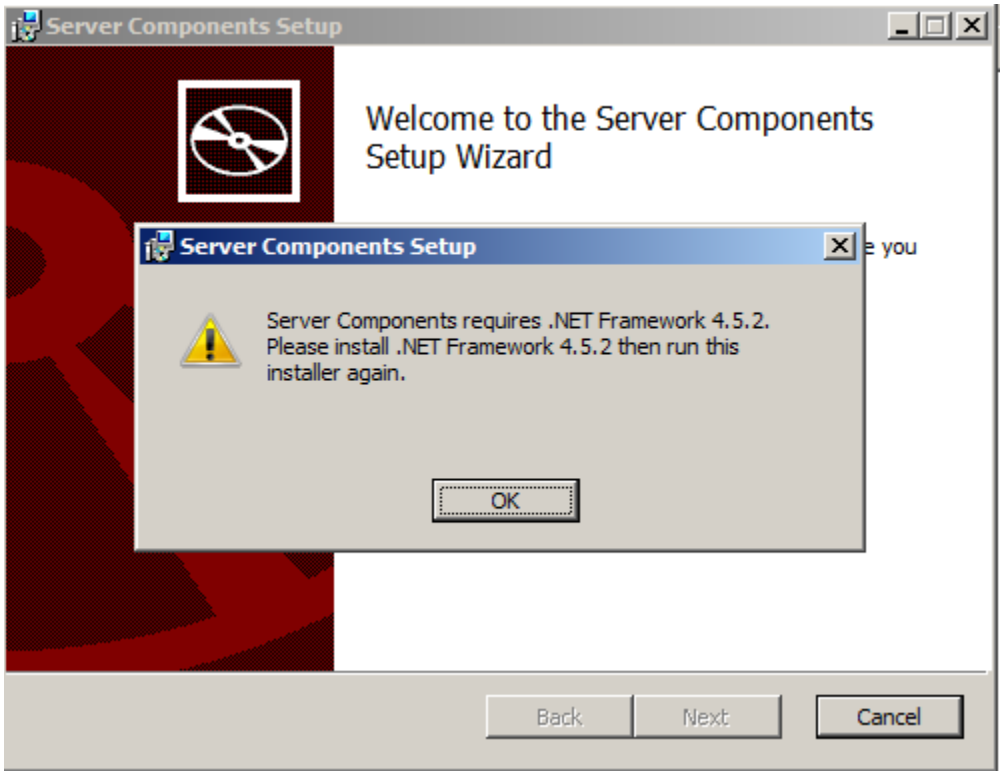
Once these steps have been performed, continue with the steps in the following section.

Upgrading from a previous automated install/upgrade

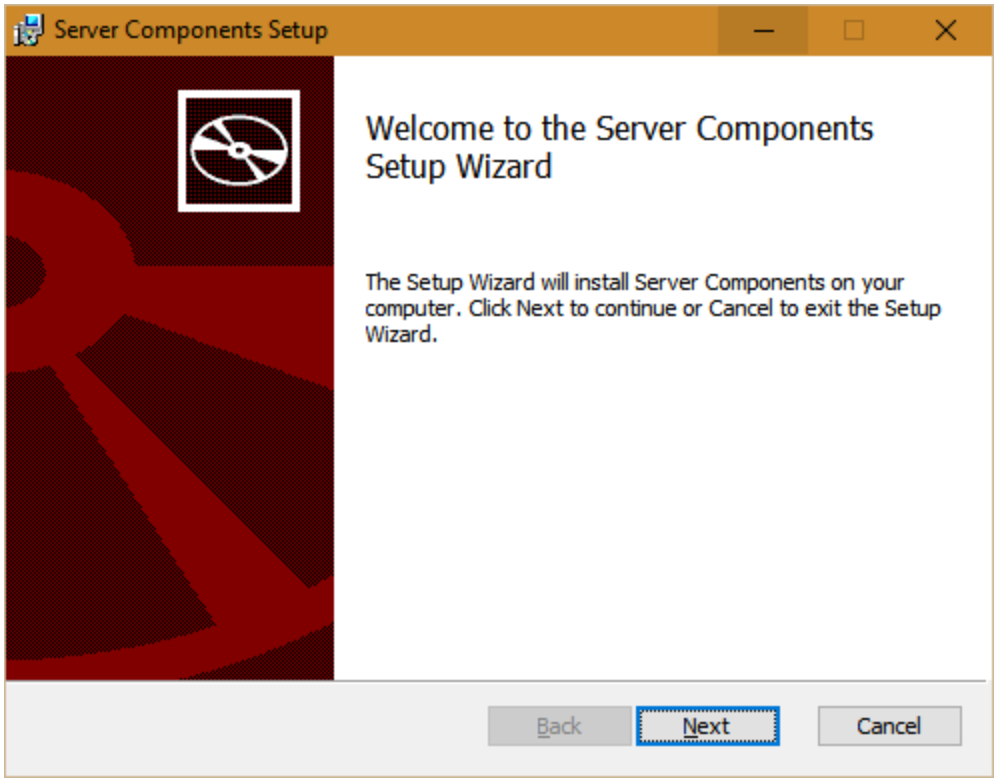
> **Tip**
>
> If you wish to upgrade Skills Management from version 4.2.0 or earlier you must first

> 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.



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**.



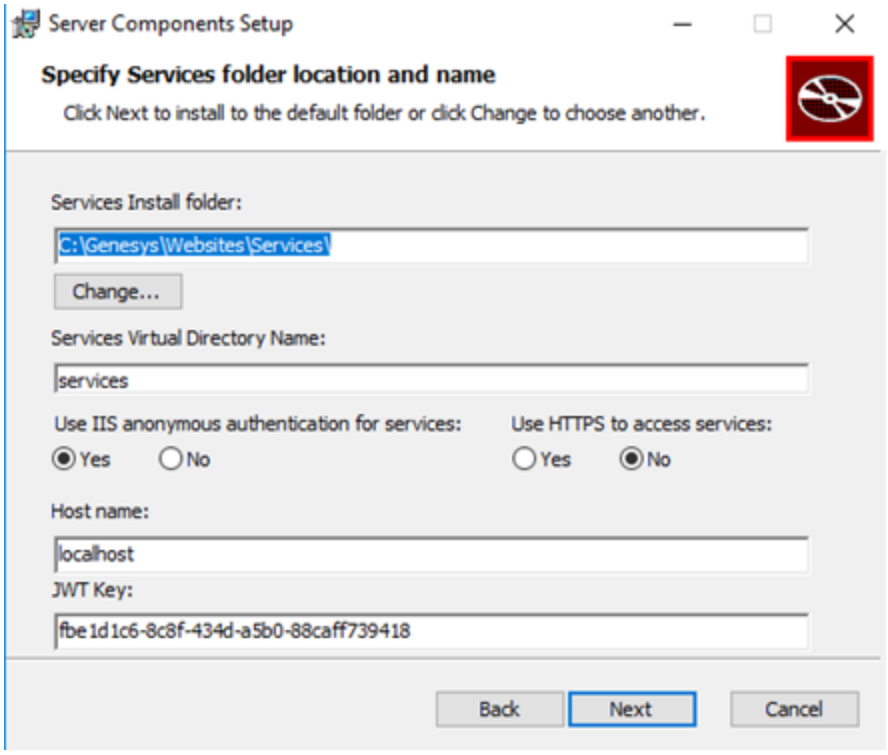
Click **Next** on the first screen.

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.

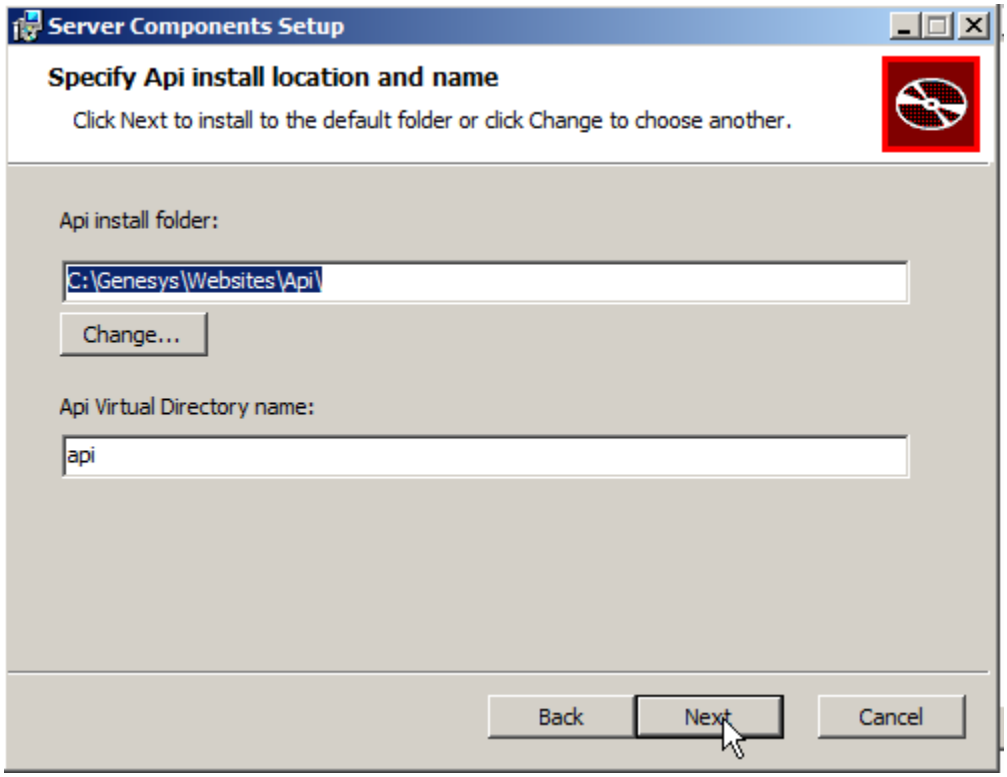
If you select the **Use HTTPS to access services** option, then all the applications and services will be configured in IIS to use HTTPS rather than HTTP. Note that in this event, you should ensure that your webserver has a valid HTTPS binding, and that the host name you enter is valid for the certificate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

The GUID for the field **JWT Key** is unique for each installation and is used to authenticate communication between front-end and back-end services and service-to-service communications. After installation is complete, a new GUID will be added to the web.config files and used to log in to PDNA, API, and the underlying service applications.

> ### Important
> The GUID is generated automatically in the installer. But, it can be overridden with a custom GUID.

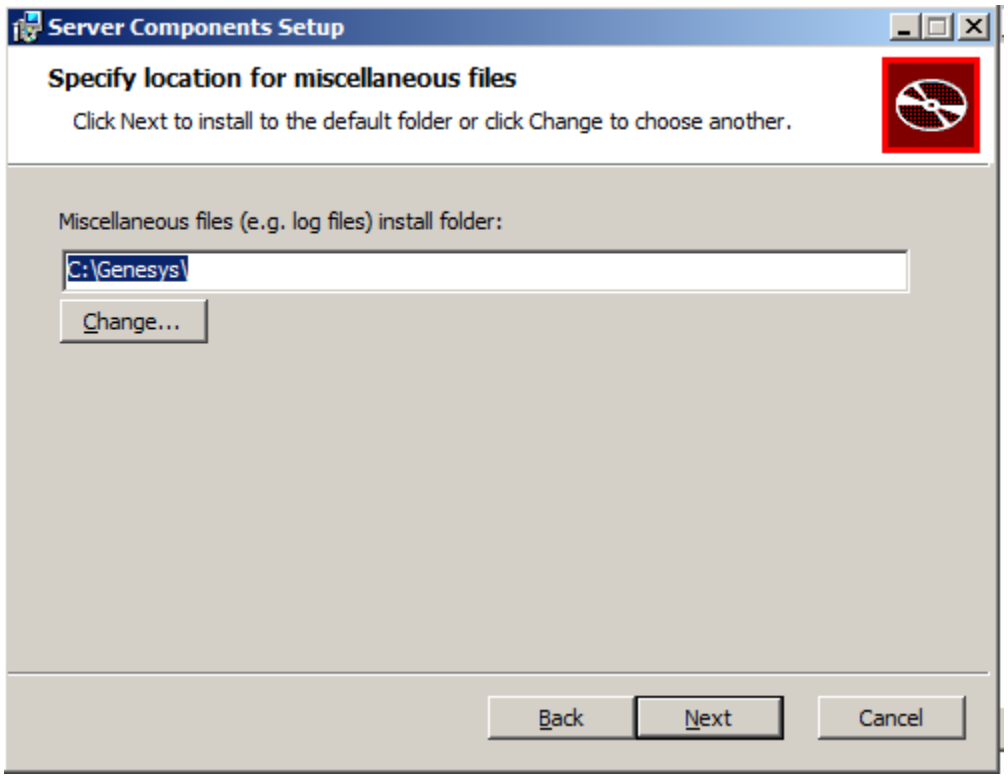


Update the settings as required, then click **Next**.

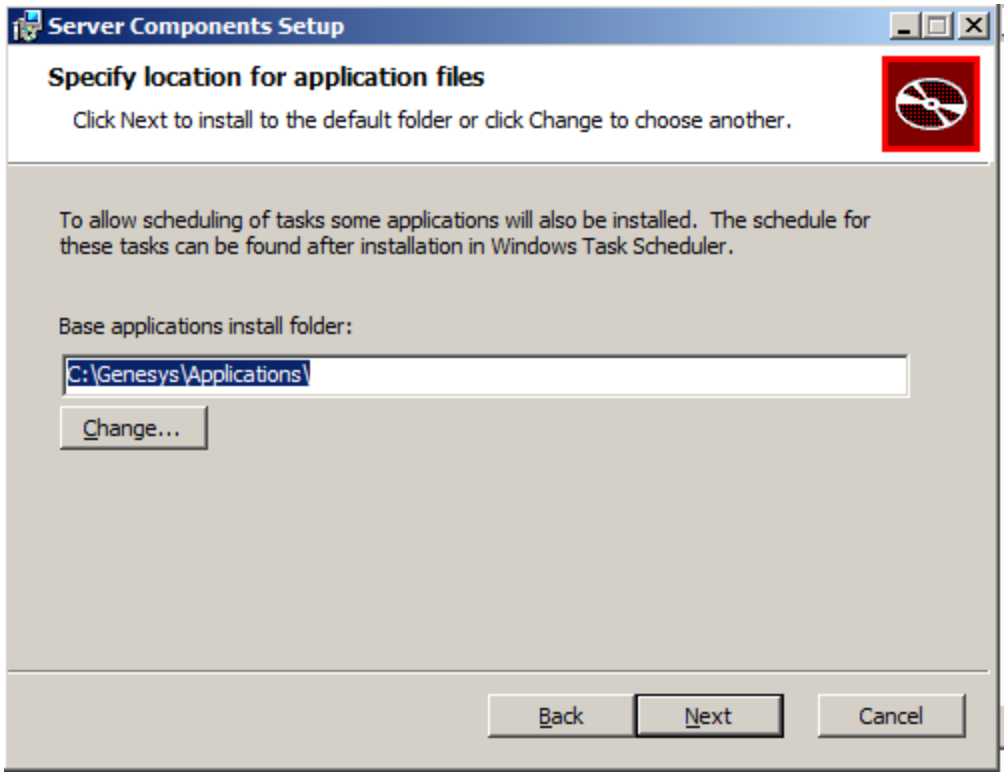


The next screen allows you to specify the physical location and virtual directory name of the Skills Management API. The values on this screen can be left at their default values. Click **Next** once you have specified these values.

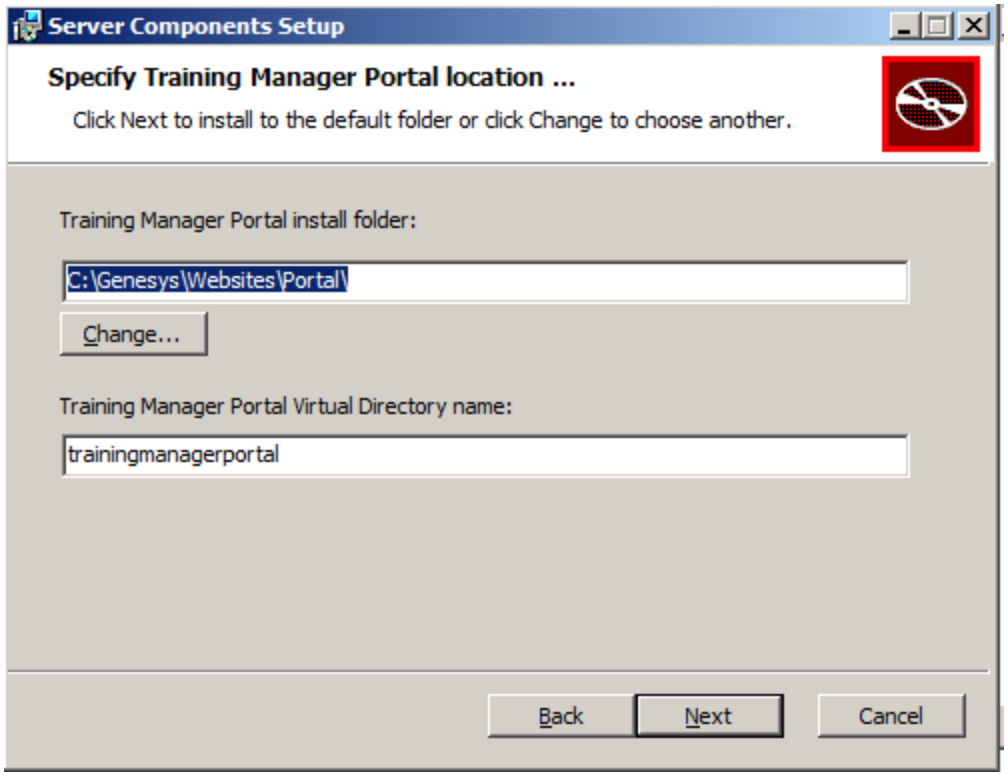
The next screen allows the updating of the path for the miscellaneous files folder. Update the path if required, then click **Next**.



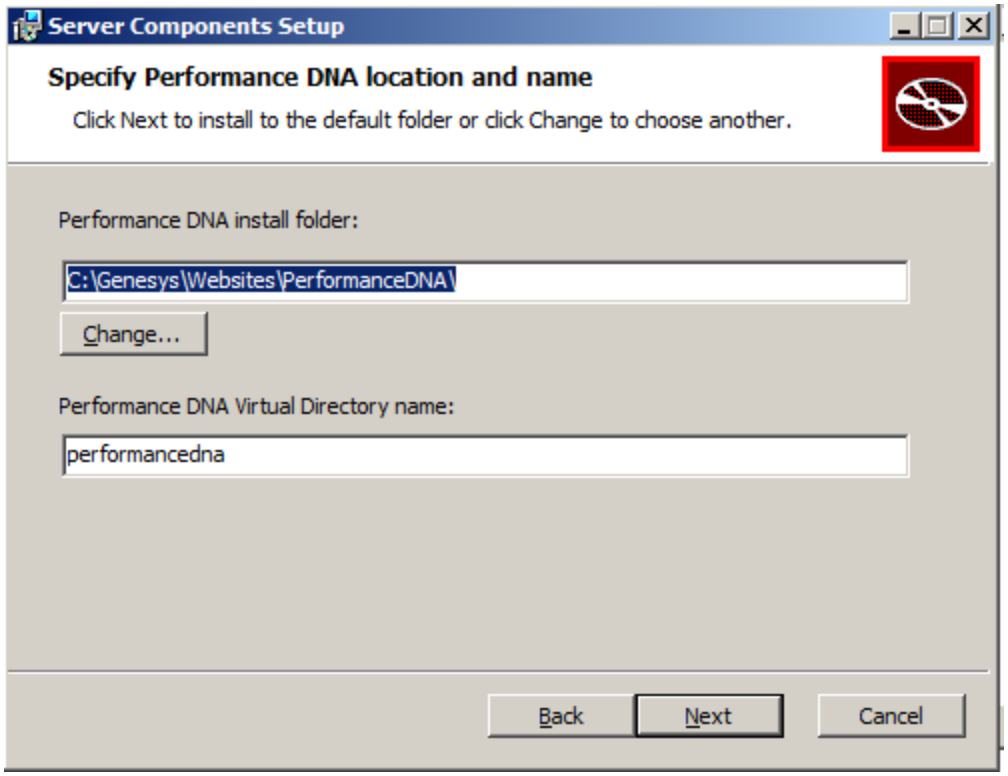
The next screen allows the updating of the path for the Applications folder. Edit the details if required, then click **Next**.



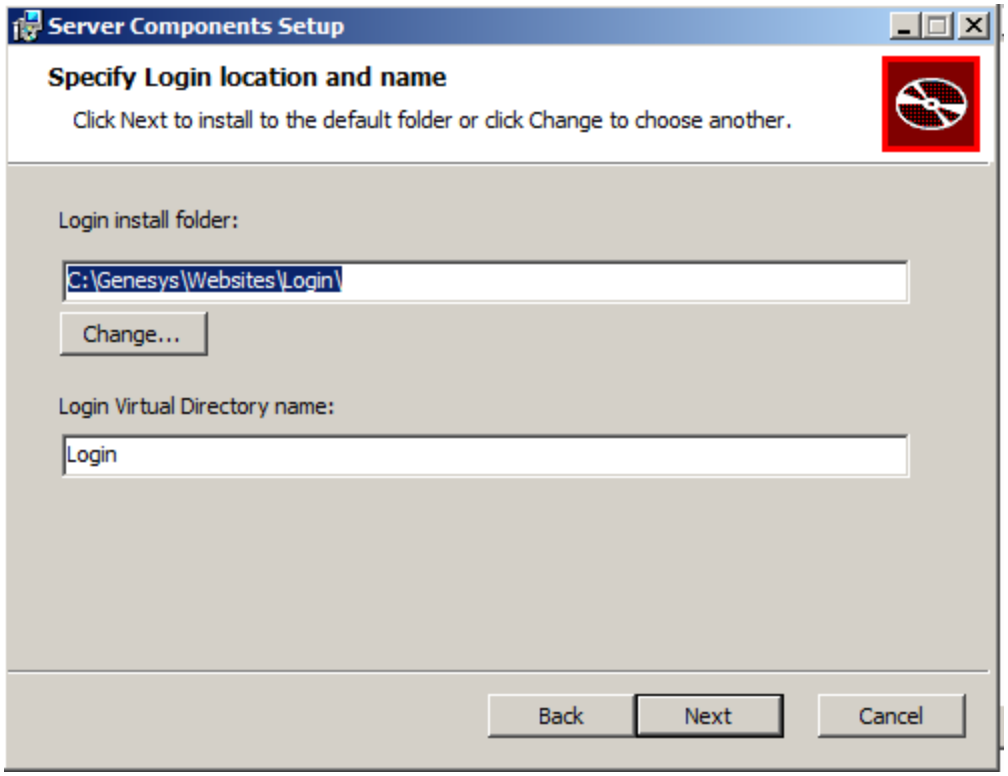
The next screen allows the updating of the path to the Training Manager Portal folder on the web server and the name of the Training Manager Portal IIS virtual directory. Edit the details if required, then click **Next**.



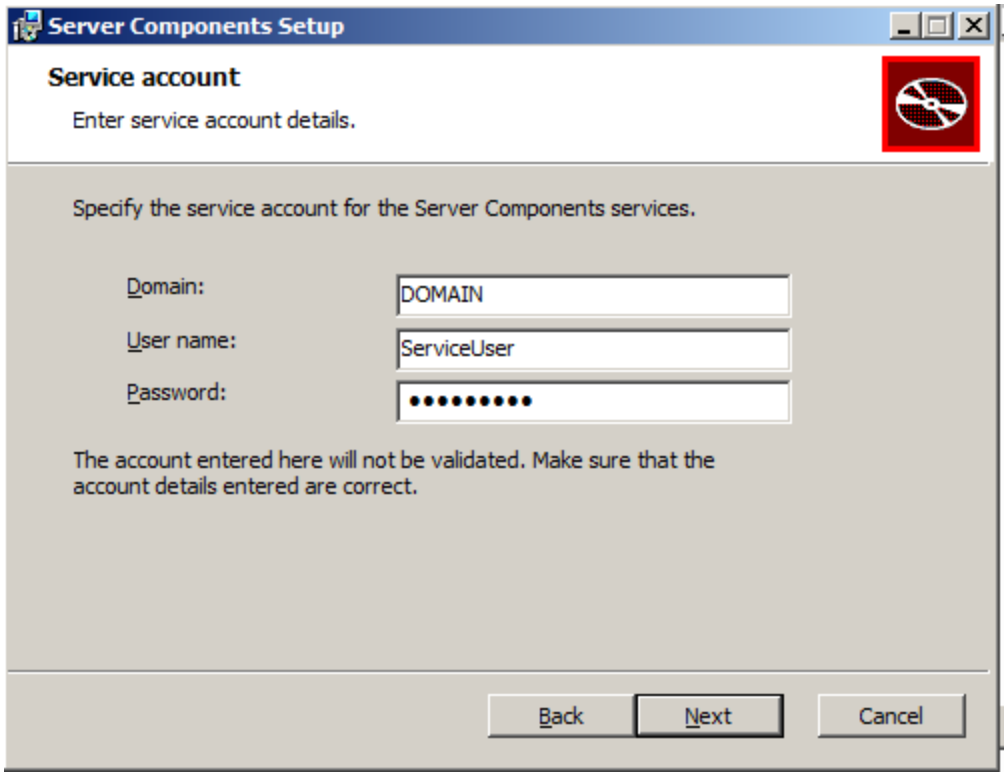
The next screen allows the updating of the path and IIS virtual directory for the Performance DNA site. Update the details if required, then click **Next**.



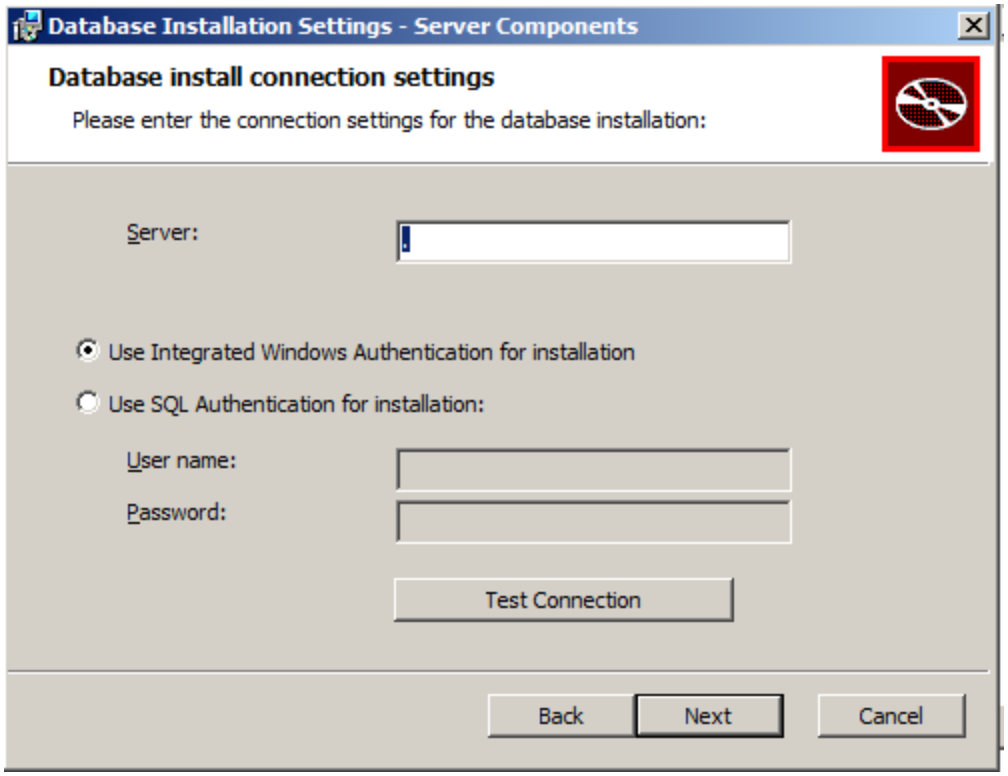
The next screen allows the updating of the path and IIS virtual directory of the Login site. Update the details if required, then click **Next**.



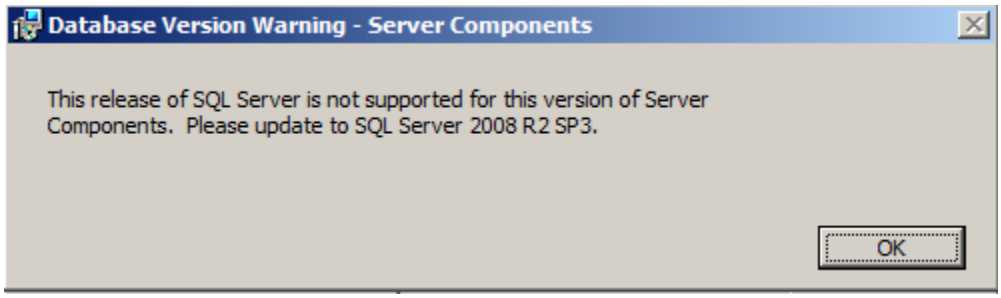
The next screen requires the provision of a service account which is used to install the services. This account should exist on the machine and have local administrator privileges. As mentioned in the prerequisites, the account must have “log on as a service” permissions.



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.

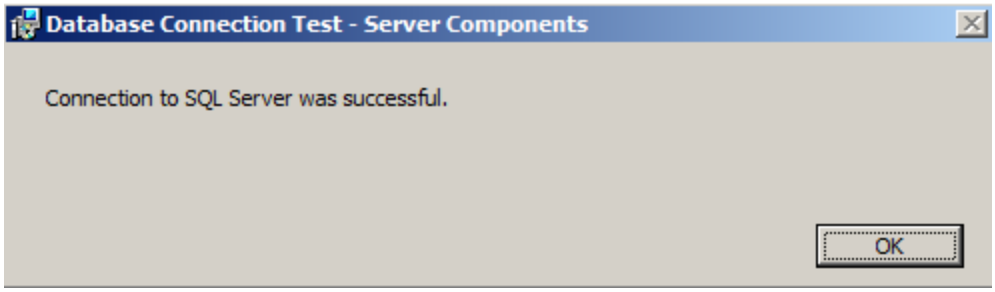


If the SQL Server release is not supported a Database version warning will be given.

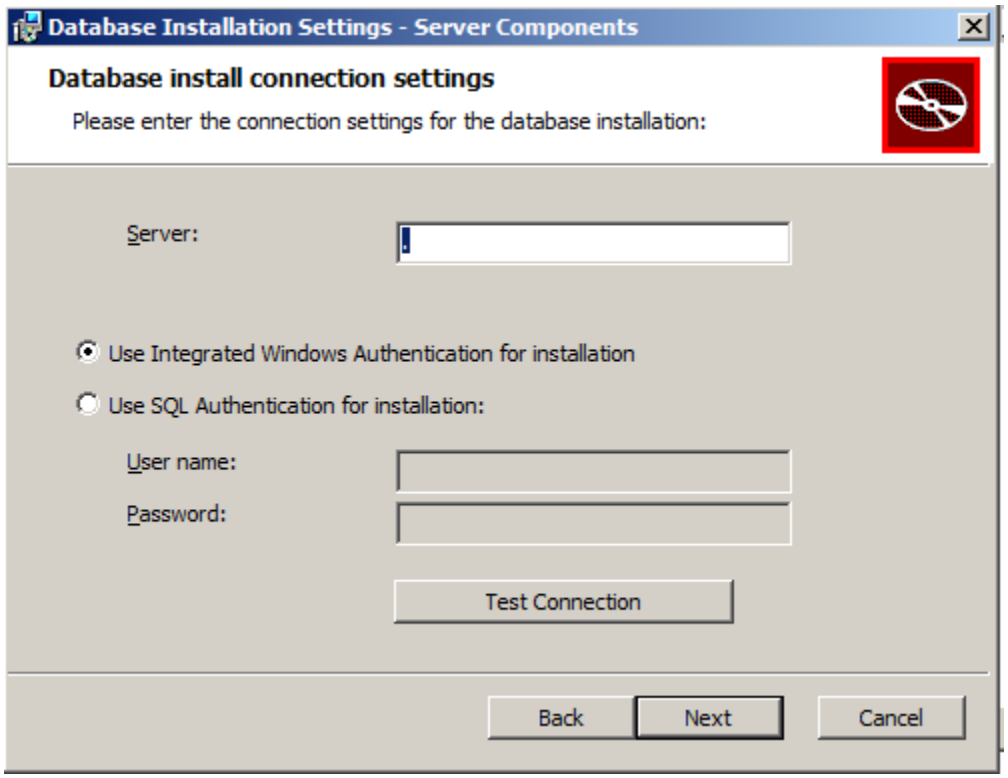


If a warning is given, click OK and cancel the install process before completing the required SQL server upgrade. Following the SQL Server upgrade re-run the **Skills ManagementSetup_v9.0.0.0.msi**

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

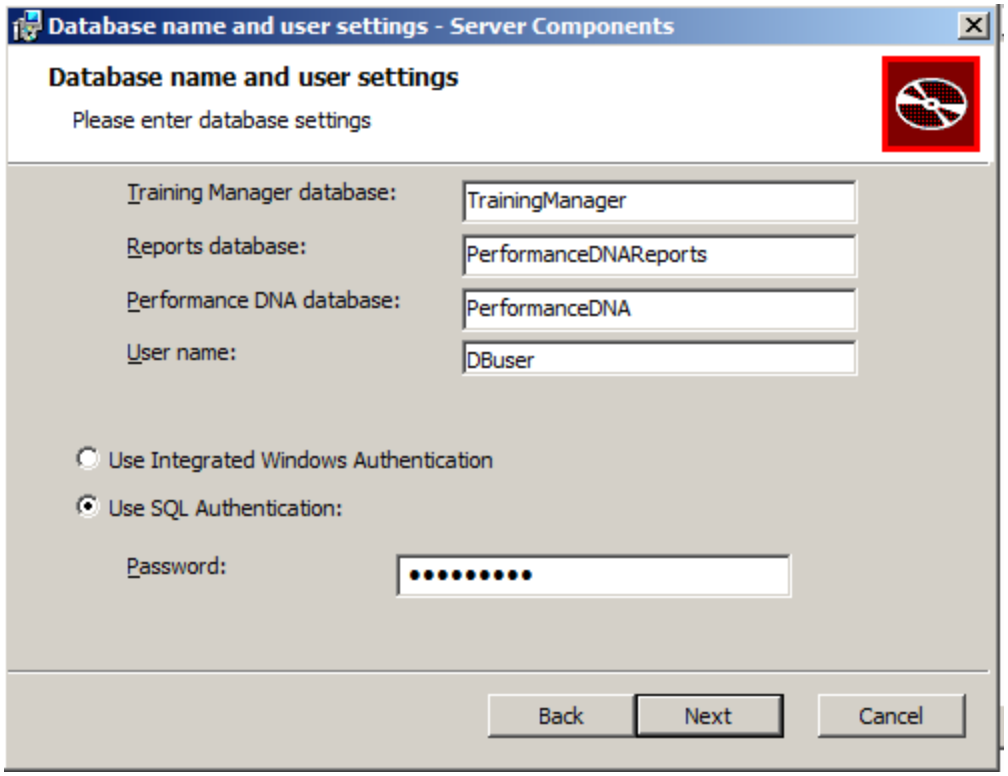


Click **OK** to continue with the installation.

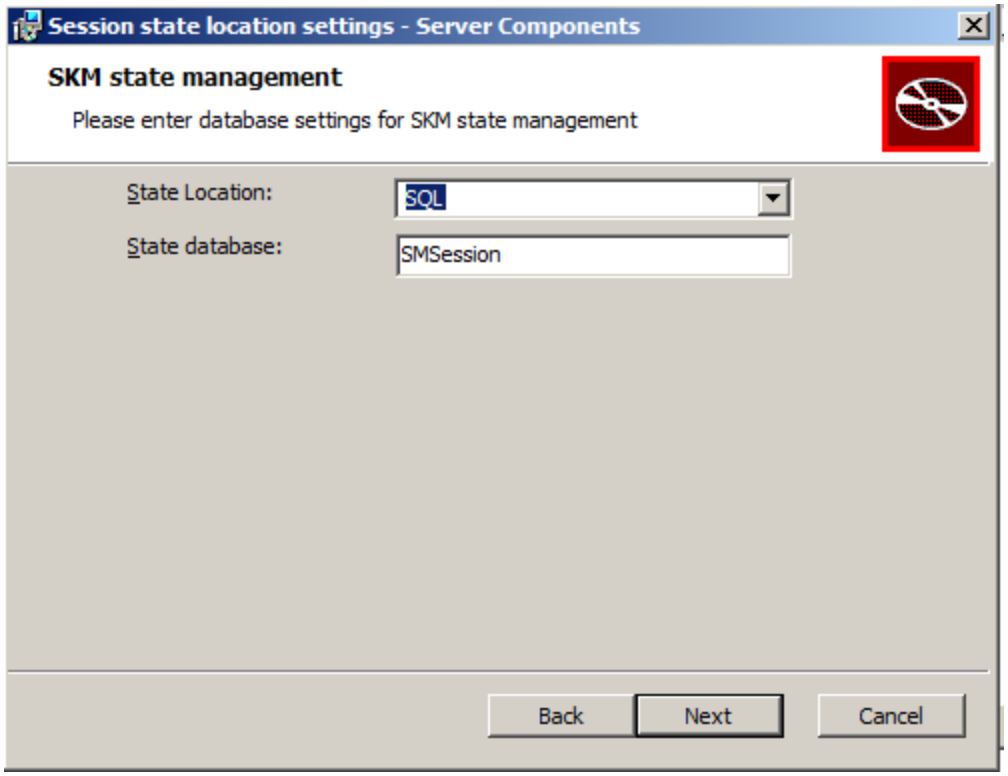


Following a successful connection test click **Next**.

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.



Update these fields as required, then click Next to move to the SKM state management screen.



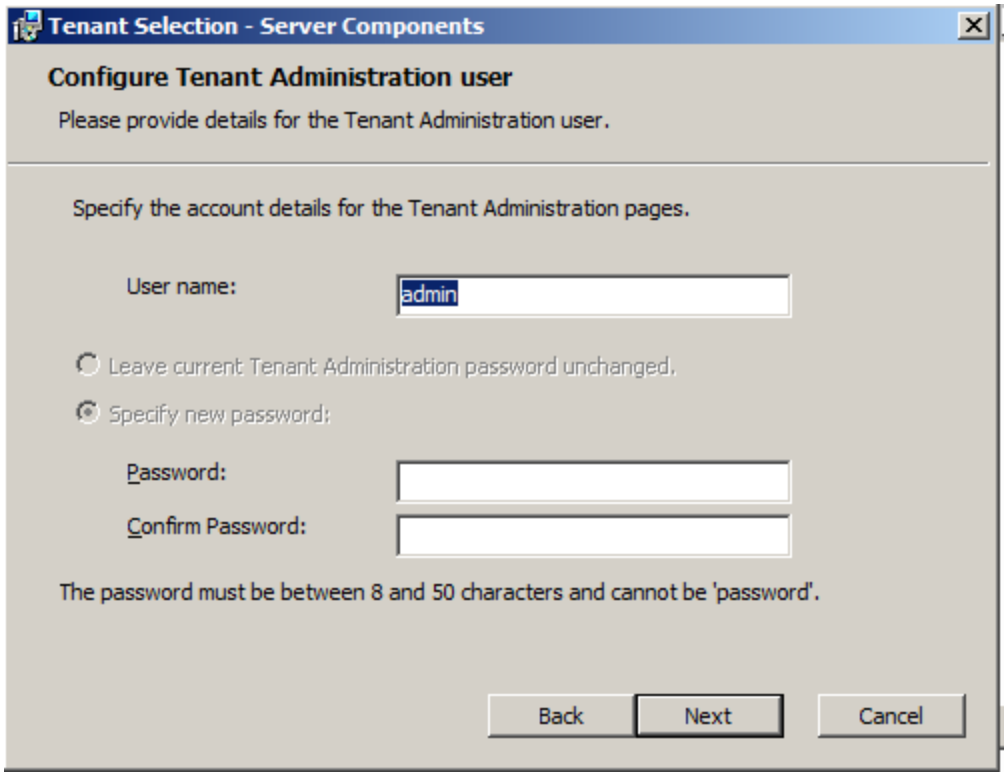
On this screen, you can select the type of State location that must be used:

- **SQL** - Select this option for multi-server environments or any environment that uses a load balancer.
- **Memory** - Select this option for smaller single server environments.

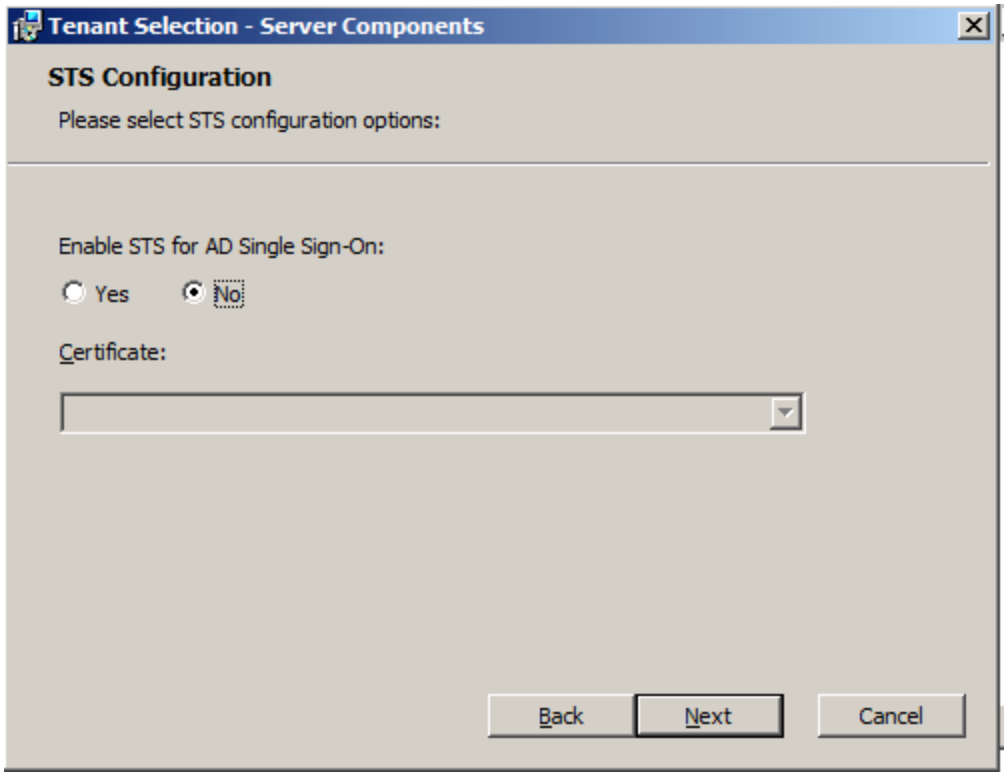
When selecting SQL as the state location update the State database with the name of the database that will be used/created for the session states.

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.



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

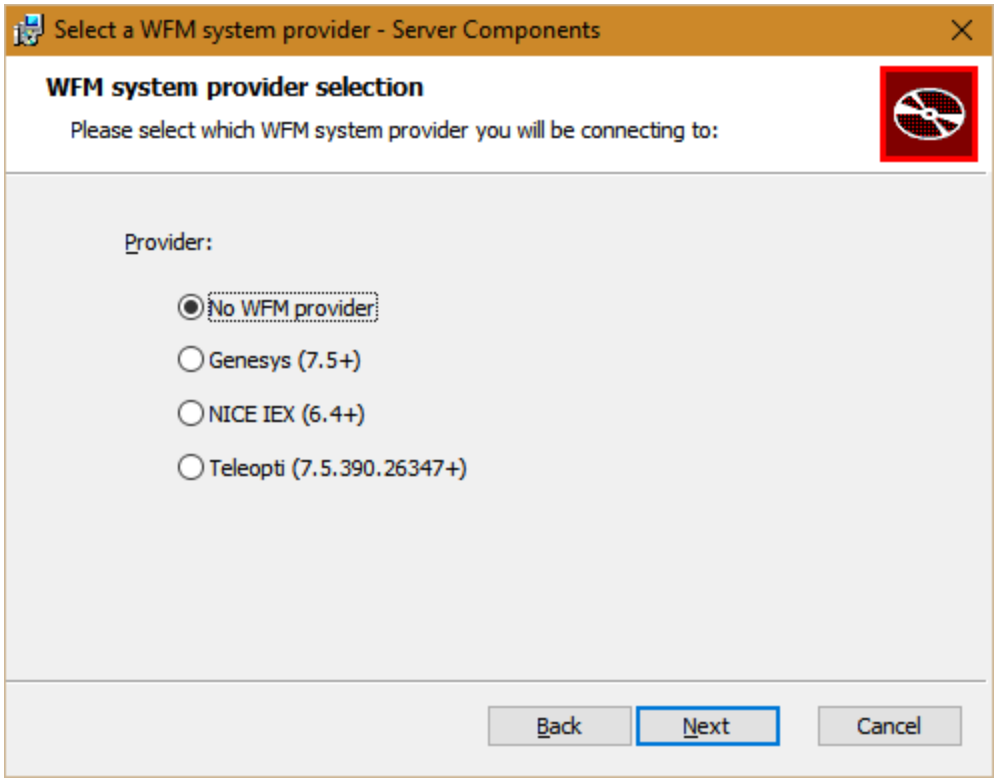


If you wish to use Active Directory authentication via the STS service for authenticating users, click the Yes option in this screen and specify the certificate that you wish to use and the Site administration domain group that will have administrator access to the suite.

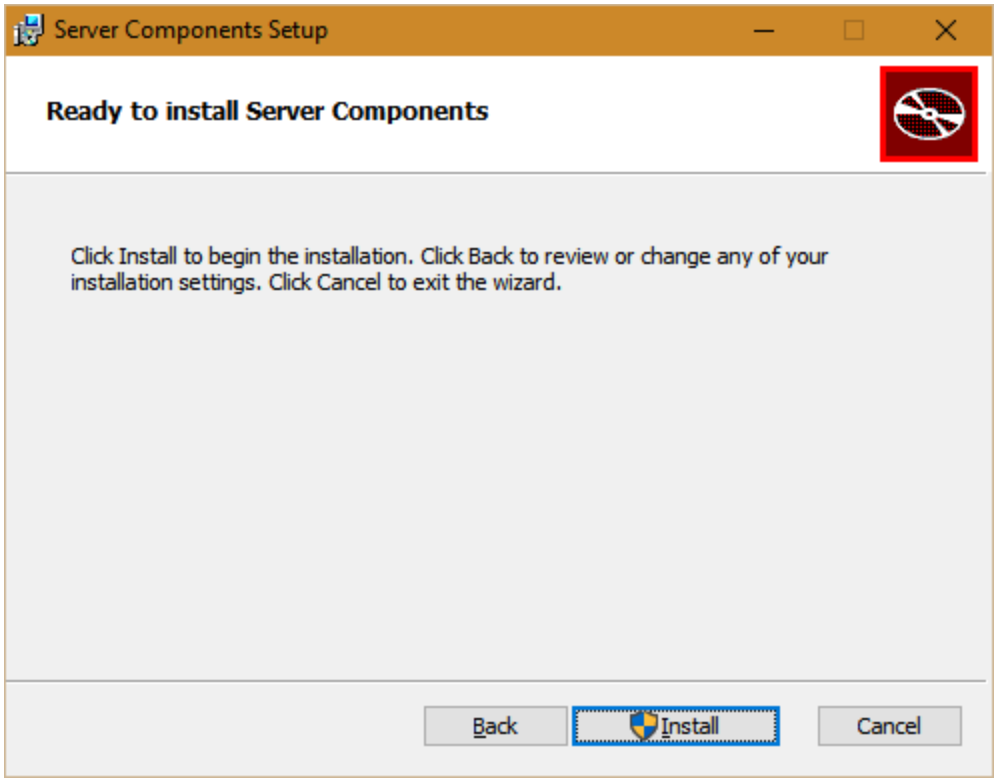
If you are upgrading a Skills Management instance that was previously using the STS service, tick Yes in this screen and specify the certificate and Site Administration Domain Group that you wish to use.

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 Genesys Skills Management Installation and Configuration Guide for Active Directory SSO document to complete the STS Service configuration.

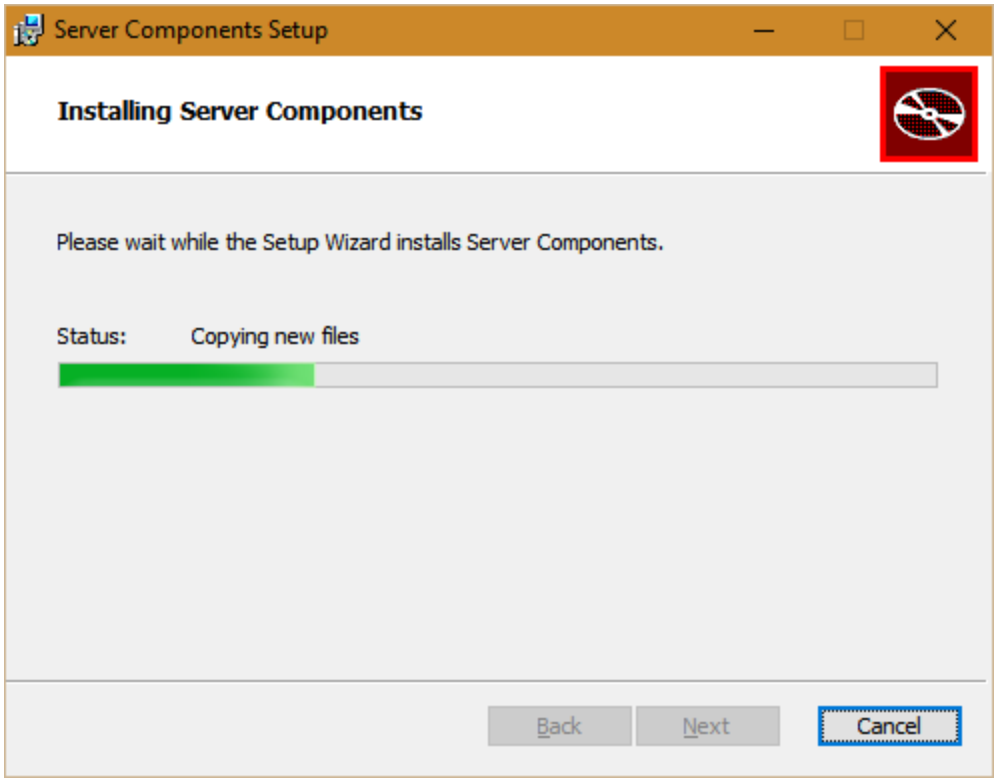
Update these fields as required, then click **Next** to move to the WFM system provider selection screen.



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



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



The final screen will confirm that the install/upgrade of the sites and services was completed. In version 9.0 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 require STS and/or the Notifications client, follow the steps in the Genesys Skills Management Installation and Configuration Guide for Active Directory SSO and Genesys Skills Management 9.0 Notifications Client Installation Guide documents.

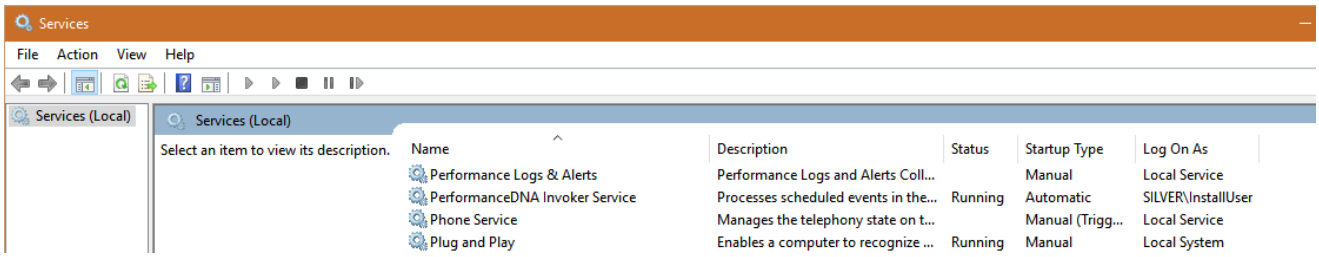
For **OrgData** please read OrgData section.

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.

Enabling Automatic Application Startup

If the server has IIS 7.5, then you must install the out-of-band module. If the server has IIS 8+, then you must initialize the application by following the instructions at https://www.iis.net/downloads/microsoft/application-initialization. Once either the application initialization (IIS 8+) or the out-of-band module (IIS 7.5) is installed, you must modify the **applicationHost.config** and application's **web.config** files by following the procedures described below.

Configuring IIS

To configure IIS

1. Open IIS and expand the root node.
2. Select **Application Pools** and right click any application pool that the application uses by selecting **Advanced Settings**.
3. Set **start mode** to `always running`.
4. You must configure at least one site in each application pool to preload. You can do this by,
    1. Search the required application under the **Sites** node.
    2. Right click the application and select **Manage Application > Advanced Settings**.
    3. Change **Preload Enabled** to `True`.

Configuring web.config file

For the application that is set to preload, you must specify the application initialization details in the corresponding **web.config** file.

1. In IIS, right-click the Application that is set to preload and select **Explore**.
2. Locate the **web.config** file and open it in a text editor.

3. Locate the `system.webServer` section of the XML and add the following `<applicationInitialization>` section:

```
<system.webServer> <br>
<applicationInitialization >  <br>
<add initializationPage="xxxxxx"/> <br>
</applicationInitialization> <br>
</system.webServer>
```

Where, you should replace **xxxxxx** with one of the following values, depending on the type of service:

- **WCF**: `/{servicename}.svc` (or, if `/default.aspx` is available then an svc file is not required)
- **REST**: `/HealthCheck` {creating in another task}
- **Web application**: **"/"**

> **Important**
>
> Repeat this process for all the Applications that are set to preload.

Command Line Installation

Copy the release package to the web server. Start a command line console (cmd.exe) window in administrator mode.

Run msiexec with the name of the Skills ManagementSetup_v4.1.0.msi to begin the installation, e.g.:

```
msiexec /i Skills ManagementSetup.msi
```

Ensure that the “Skills ManagementSetup.msi” value is modified to match

Additional parameters can also be used to provide values for variables required by the installer. The following table provides information about these additional parameters.

Parameter	Default value	Explanation
SERVICESFOLDER	x:\SLS\Websites\Services	The folder in which the services will be installed.
SERVICESVIRTUALDIR	Services	The virtual directory that will be created in IIS that points to the services folder.
PORTALFOLDER	x:\SLS\Websites\Portal	The folder in which the Portal website will be created.
PORTALVIRTUALDIR	Portal	The virtual directory that will be created in IIS that points to the Portal folder.
PERFDNAFOLDER	x:\SLS\Websites\performancedna	The folder in which the Performance DNA website will be created.
PERFDNAVIRTUALDIR	performancdna	The virtual directory that will be created in IIS that points to the Performance DNA folder.
LOGINFOLDER	X:\SLS\Websites\Login	The folder in which the Login website will be created.
LOGINVIRTUALDIR	Login	The virtual directory that will be created in IIS that points to the Login folder.
MISCFOLDER	x:\SLS\	The folder in which the Reports, Logs and QMedia folders will be created.
DBSERVER	.	The database server name to use for configuration and installation of databases.
TRAINING MANAGERDB	Training Manager	The name for the Training Manager database
REPORTSDB	Skills ManagementReports	The name for the Reporting database
PERFDNADB	PerformanceDNA	The name for the Performance

Parameter	Default value	Explanation
		DNA database
DNADB	DNA	The name of the DNA database
DBAUTH	SQL	The authentication method to use in the connection strings created in the various service / website configuration files. Can be either **SQL** or **WIN** (SQL Server authentication or Windows authentication).
DBUSER		The user to create in SQL Server, and the user to use in connection strings if the selected DB authentication method is **SQL**.
DBPASSWORD		The password to use for the DBUser, if DB authentication is **SQL**.
DBINSTALLAUTH	WIN	The authentication method to use whilst installing the database. As per DBAUTH.
DBUNINSTALLAUTH	WIN	(Uninstall only) The authentication method to use whilst uninstalling the database. As per DBAUTH.
DBINSTALLUSER		If the install/uninstall authentication mode is **SQL**, this is the username used to install the database.
DBINSTALLPASSWORD		If the install authentication mode is **SQL**, this is the password used to install the database.
SITEHOSTNAME	localhost	The site name that the services will be registered against in the config files, and the hostname used when showing the post-install page.
SERVICEALLOWANON	Yes	**Yes** if the services should be configured to run under anonymous access, anything else if the services should be configured to use Windows Authentication. Note that the **Yes** is *case-sensitive.*
USEHTTPS		**Yes** if the websites and services should be configured to run under HTTPS, anything else if the services should be configured to use HTTP. Note that the **Yes** is *case-sensitive.*
REMOVEDBS		(Uninstall only) **Yes** if the databases

Parameter	Default value	Explanation
		should be removed by the installer. Anything other than **Yes** will mean the databases are left as they are. Note that the **Yes** is *case-sensitive.*
REMOVEUSER		(Uninstall only) **Yes** if the SQL server user should be removed by the installer (only has any effect if REMOVEDBS is also **Yes**). Anything other than **Yes** will mean the users are left as they are. Note that the **Yes** is *case-sensitive.*
STSENABLED		Set this property to **Yes** if you want to enable AD authentication via the STS service. Note that the **Yes** is *case-sensitive.*
STSCERTTHUMBPRINT		Set this property to the certificate thumbprint of the certificate that you want to use. This should be a single string with no spaces. Also, ensure that you delete the invisible character at the beginning of the string if you copy and paste it from the certificate properties.
TENANTADMINLOGIN		Set this property to the tenant administration administrator username.
TENANTADMINPASSWORD		Set this property to the tenant administration password.

Additional options

Logging

To get a complete log of all output from the install, you should include:

/l*v *logFileName.txt*

UI visibility

/q – don’t show the user interface

/passive – shows a basic progress bar

Advanced installation

This installation specifies a value for all the properties. No user interface will be displayed and all installer steps are logged to log.txt.

```
msiexec /i Skills ManagementSetup.msi

PERFDNAVIRTUALDIR="performancedna" PORTALVIRTUALDIR="trainingmanagerportal"
LOGINVIRTUALDIR"Login" SERVICESVIRTUALDIR="services" PLANNERDB="TrainingManager"
PERFDNADB="PerformanceDNA" REPORTSDB="PerformanceDNAReports" DNADB="DNA"
MISCFOLDER="C:\Genesys\Misc" PORTALFOLDER="C:\Genesys\Websites\Portal"
PERFDNAFOLDER="C:\Genesys\Websites\PerformanceDNA" LOGINFOLDER="C:\Genesys\Websites\
Login SERVICESFOLDER="C:\Genesys\Websites\Services" DBUSER="pdnauser"
DBPASSWORD="pdn4u53r" DBSERVER="localhost" DBAUTH="SQL" DBINSTALLAUTH="SQL"
DBINSTALLUSER="sa" DBINSTALLPASSWORD="sa" SITEHOSTNAME="www.blue.com"
SERVICEALLOWANON="Yes" USEHTTPS="No" TENANTADMINLOGIN="admin"
TENANTADMINPASSWORD="notpassword" STSENABLED="No" STSCERTTHUMBPRINT="" /q /l*v
log.txt
```

> ### Tip
> If you set the USEHTTPS parameter to “Yes” 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.

> ### Tip
> 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 before running the installer/installing via the command line parameters.

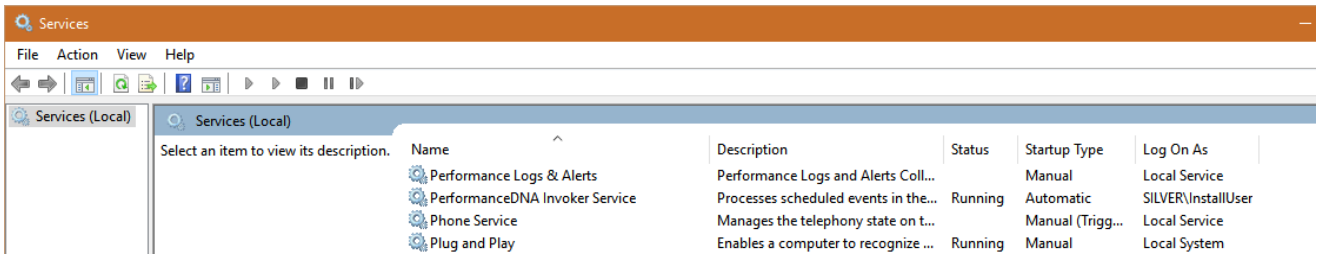
If you’ve previously installed/upgraded the software via the automated setup application or command line program, ensure that you input the same command line settings when upgrading to a newer version.

If you require 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 Service** and **Notifications 1.0 Client v9.0.0.0 Installation Guide** documents.

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.

Exported Portal Users

The upgrade to Skills Management 9.0 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.

OrgData

What is Orgdata?

OrgData is a utility that can be used to manage user and hierarchy data within Performance DNA, as an alternative to manually managing that information.

This includes addition and removal of users, and maintaining the user hierarchy, which is used for system access (permissions) and reporting.

While OrgData uses a number of standard product components it usually involves a custom configuration to support the HR file structure and requirements of each organisation. Typically, this configuration is carried out by Genesys professional services or a trained services partner.

What is OrgData Process?

The **OrgData Process** enables you to manage HR data within Skills Management. This includes addition and removal of users, and maintaining the user hierarchy, which is used for access and reporting.

How OrgData is used

OrgData is used as a replacement for manually uploading user information into the Skills Management System. It is configured to regularly (usually every night) synchronize the user hierarchy with a data feed from one or more parent systems. It is designed to be configurable and customizable, so that the data which is imported can be tailored to the requirements of each individual deployment of Skills Management.

OrgData works by reading files which are written to a particular directory and/or by reading users stored in a WFM system. It runs as a scheduled task.

High Level Data Structure

Like Skills Management, OrgData can be configured to import a wide variety of different User fields. There are a number of core fields which need to be provided. These are:

Field	Notes
Line Manager ID	ID of the manager (normally direct supervisor) of the employee

Field	Notes
PositionName	Name of the position
EmployeeID	ID of the employee
FirstName	Employee’s first name
LastName	Employee’s last name.

Additional fields can be used to create user data, such as email addresses, phone numbers, IM names, or other identifying information.

Setting up OrgData Process

The **OrgData Process** enables you to manage HR data within Skills Management. This includes addition and removal of users, and maintaining the user hierarchy, which is used for access and reporting.

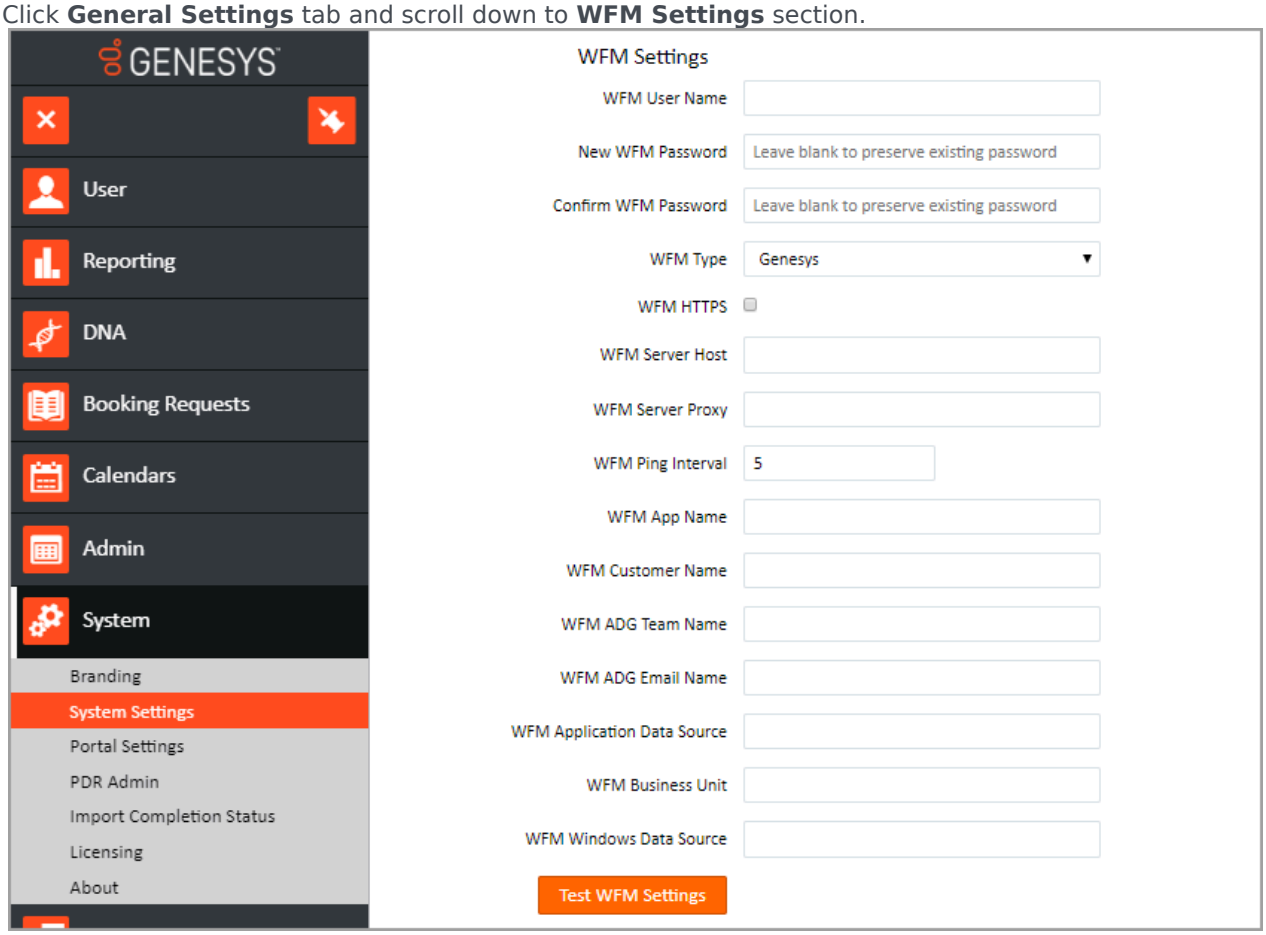
Before running the OrgData Process, you must configure the following values in Skills Management.

- WFM fields
- OrgData Unique user fields
- OrgData Required fields

Configuring WFM Settings

You must connect OrgData to the WFM solution. You can configure WFM settings from the Skills Management web portal by completing the following procedure:

1. Navigate to **System > System Settings** page.
2. Click **General Settings** tab and scroll down to **WFM Settings** section.



3. Specify the WFM values in the below fields:
    - **WFM User Name** – Enter the user name of the WFM account that Skills Management will use to connect to the WFM solution.
    - **New WFM Password** – Enter the WFM user's password.
    - **Confirm WFM Password** – Re-enter the WFM user's password.
    - **WFM Type** - From the drop down, select the WFM provider that you are using.
        - Genesys
        - Teleopti

    - IEX (NICE)
- **WFM HTTPS** – Check, if the WFM API is running over HTTPS.
- **WFM Server Host** – Enter the hostname / URL of the WFM solution. For Genesys WFM the port will need to be included i.e. wfm.genesyslab.com:5007
- **WFM Server Proxy** – If using a proxy please enter the Proxy server details.
- **WFM Ping Interval** – By default, this is set as 5. You can change this only on the advice of the Genesys Care Team.
- **WFM App Name** – This field is specific to Teleopti WFM users.
- **WFM Customer Name** – This field is specific to NICE IEX users.
- **WFM ADG Team Name** – Please enter the IEX ADG that is used to identify Team Names.
- **WFM ADG Email Name** – Please enter the IEX ADG that is used to store Email addresses.
- **WFM Application Data Source** – As a Teleopti WFM user enter 1 if the username provided is an application login ID.
- **WFM Business Unit** – As a Teleopti WFM User enter the GUID of the Business Unit.
- **WFM Windows Data Source** – As a Teleopti WFM user enter 1 if the username provided is a Windows login ID.

> **Important**
>
> Before saving the WFM settings click the **Test WFM Settings** button. If successful a green **WFM Settings Test Successful** message will be displayed.

4. Scroll down to the bottom of the General Settings tab and click “Save Changes”.

Configuring OrgData Unique User Field

Before configuring OrgData Process values, you must configure the **OrgData Unique User Field** that will be used as the unique identifier during the OrgData import process.

You can configure this field by navigating to **System > System Settings > General Settings tab > Other Settings**.

From the **OrgData Unique User Field** drop down, you can select a value which will be used as the unique identifier and click **Save Changes**.

Configuring OrgData Required Fields

As a minimum requirement, you must configure and map the following data fields:

- Login ID (unique identifier) - By default, the Login ID is an email address.
- First Name
- Last Name
- Position ID
- Position Name

Configuring Data Sources for Import

You can either set the WFM fields or a CSV file as a data source for importing OrgData. After you set the data source fields, you must map those fields to the user fields in Skills Management.

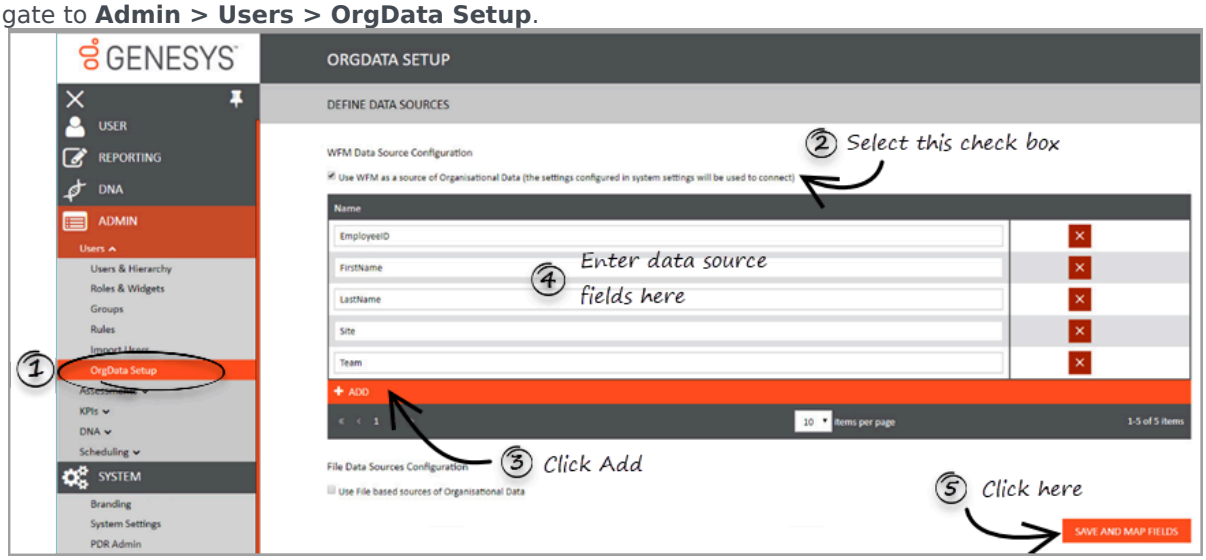
You can configure data source by using the following procedures:

- Configuring WFM as data source
  - Mapping WFM data source fields to user fields
- Configuring CSV file as data source
  - Mapping CSV data source fields to user fields

Configuring WFM Fields as Data Source

Follow the steps below to configure WFM as the data source for OrgData.

1. Navigate to **Admin > Users > OrgData Setup**.



2. On the **Define Data Sources** page, in **WFM Data Source Configuration** section, select the check box **Use WFM as a source of Organisational Data (the settings configured in system settings will be used to connect)**.
3. Click **+ Add** to create a new WFM data source.
4. Enter the name of the WFM data source field or column that will be used.

> ### Important
>
> UserId, EmployeeId, FirstName, LastName and CacheData are default fields in WFM, out of which CacheData is automatically mapped and you do not have to setup explicit mapping.
>
> Note that some fields are specific to a WFM application. Such fields are:
>
> 1.
> - Genesys-specific fields: `Site, Team, Email`
> - Teleopti-specific fields: `Site, Team, Email, ADLogin, AppLogin`
> - NICE (IEX)-specific fields: `MUName`

1. Repeat steps 3 and 4 until you add all the required WFM data source fields that you wish to import.
2. Click **Save and Map Fields**.

Updating WFM Data Source Fields

The WFM specific data source fields are case sensitive. Hence, Genesys recommends to use the source field names carefully during configuration.

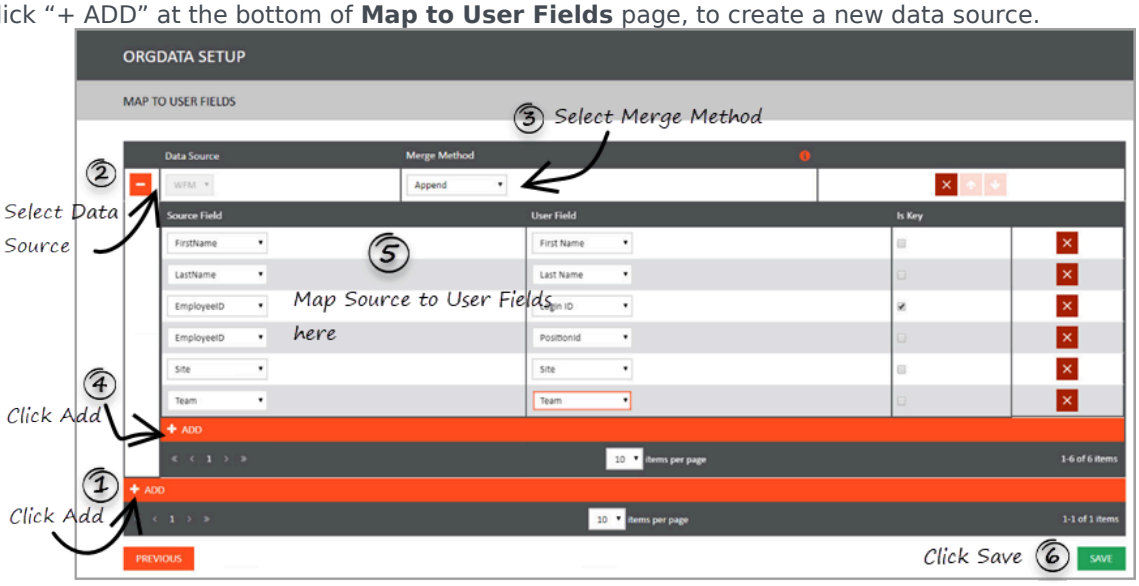
In case you want to update or correct any data source field, follow the below procedure.

1. Navigate to the **Define Data Sources** page and delete the incorrect data source by clicking the **X** (delete) button.
2. Click **Save and Map Fields**.
3. Click **Previous**.
4. Refresh the **Define Data Sources** page by pressing **F5** or **Ctrl + R** keys.
5. Add the data source fields again with the correct spelling and case by following Configuring WFM Data Source Fields procedure.
6. Re-map the data source fields to the User Fields.
7. Click **Save**.

Mapping WFM Data Source to User Fields

You can map the WFM data source fields to the Skills Management User Fields by performing the following procedure. Note that, this procedure is a continuation of Configuring Data Source Fields procedure. You can map the data source fields only at the end of configuration procedure, that is, while saving them.

1. Click "+ ADD" at the bottom of **Map to User Fields** page, to create a new data source.



2. In the **Data Source** column, select the source from which you will import the data. You can either select **WFM** or a **File Name** based on your configuration in the **Define Data Sources** page.
3. In the **Merge Method** column, select the method which must be applied to merge the Data

Source to User Fields. You can select:

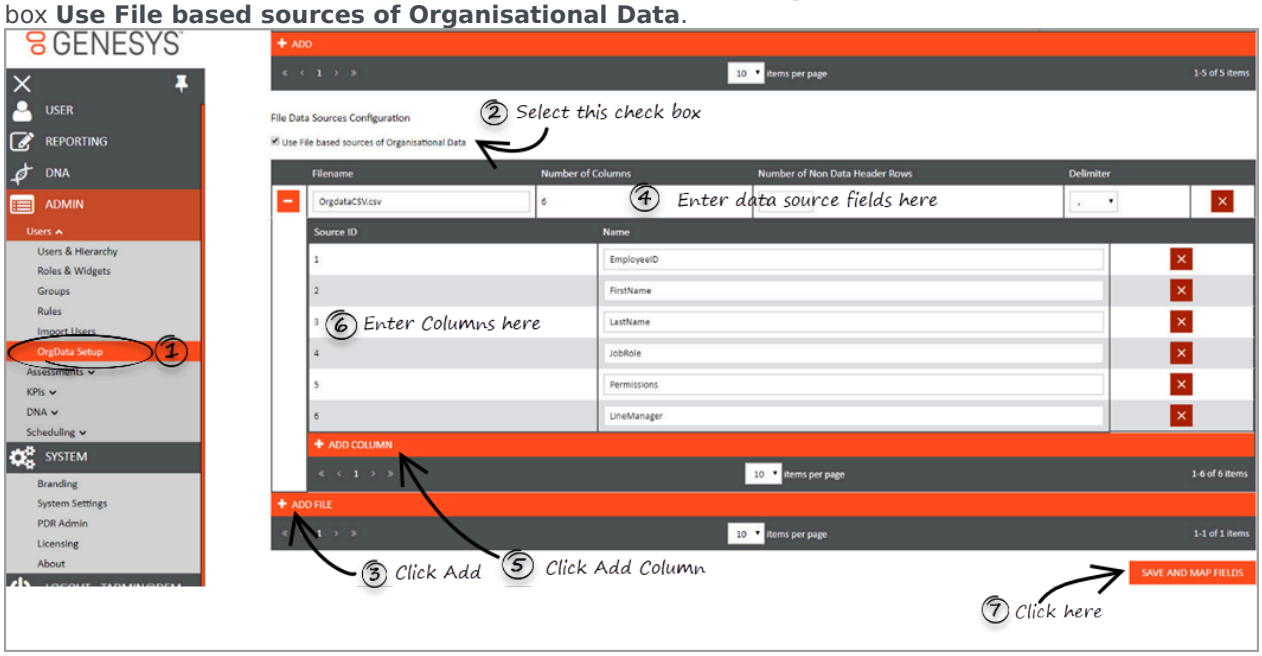
- **Append** – this method adds all new data source fields to the existing User Fields.
- **Update and Append** – this method updates existing User Fields with the imported changes and creates new User Fields.
- **Update Only** – this method updates existing User Fields with imported changes and does not create new User Fields.
- **New Rows Only** – this method only creates new User Fields.

4. Click "+ ADD" within the inner table to create a new Source to User Field mapping. You can do the mapping by specifying the following fields:
    - **Source Field** column – select the WFM field from the drop down.
    - **User Field** column – select the corresponding Skills Management field from the drop down.
    - **Is Key** – select this check box if you want to use the current field as the Unique Identifier. For example, Login ID field.
5. Repeat the above step until you configure all the User Fields that must be imported from the WFM application.
6. Click **Save**.

Configuring a CSV File as Data Source

You can also configure a CSV file as a data source for importing OrgData. Follow the steps below to configure a CSV file as a data source.

1. Navigate to **Admin > Users > OrgData Setup**.
2. On the **Define Data Sources** page, in **File Data Sources Configuration** section, select the check box **Use File based sources of Organisational Data**.



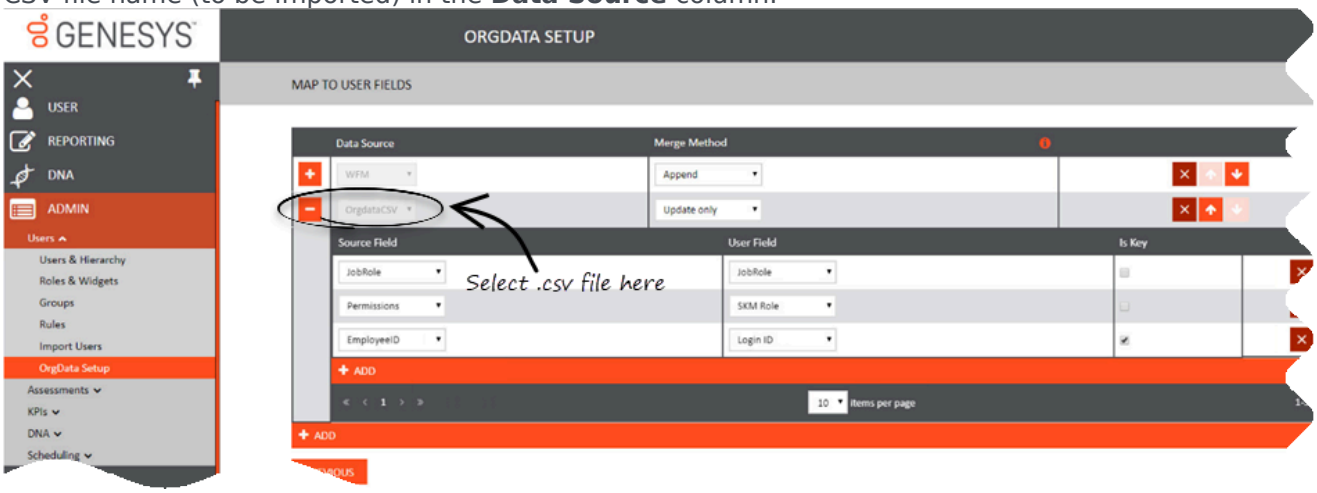
3. Click **+ ADD FILE** to define a new file source.
4. Enter the CSV file related values in the following fields:
    - **Filename** – enter the name of the file to be imported along with its extension. For example, OrgdataCSV.csv
    - **Number of Columns** – this field will be automatically updated based on the source file configuration.
    - **Number of Non Data Header Rows** – enter the number of rows that are not part of the data rows. Most often, these rows are at the beginning of the file and used as an header or to explain any important information.
    - **Delimiter** – select the delimiter that must be used to separate the data values.
5. Click **+ ADD Column** to define each data column within the file.
6. Enter the column values in the following fields:
    - **Source ID** – enter the column number for a specific field within the file.
    - **Name** – enter an user friendly name for the column.
7. Repeat steps 5 and 6 until you add all columns in the file.

> **Important**
>
> During the file import and processing, the **Number of Columns** value is used to validate the file. Hence, Genesys recommends to configure all the columns from CSV file in PDNA even though they might not be used.

8. Click **SAVE AND MAP FIELDS**.

Mapping CSV Data Source to User Fields

Mapping CSV data source fields to Skills Management User Fields is similar to mapping WFM data source fields to Skills Management User Fields. However, the exception is that you must select the CSV file name (to be imported) in the **Data Source** column.



In a practical use case, WFM is the master source of data and it manages:

- New user creation
- Hierarchy reorganisation
- Archiving of leavers

> **Important**
>
> - The CSV file is generally used to update existing users with their Job Role and User Permissions Role.
> - You can set a default password for all the users from the CSV data source file and map it to the **Password** field in PDNA. While creating a default password, ensure that it

adheres to the password rules set in the **Password Settings** (in **General Settings** tab) as the system validates the imported password by using the password rules.

Importing OrgData Through CSV Files

Following the configuration of the data source fields, you can import the OrgData file. Whenever there is an update in the data source, you must import the recently updated OrgData file in Skills Management system for accurate maintenance of data.

> ## Important
> For OrgData configurations that use a daily update or file produced by a third party system, you can use the Orgdata API to upload the OrgData file automatically in regular intervals

To import the OrgData file,

1. Navigate to **Admin > Users > Import Users**.
2. On the **IMPORT USERS** page, click **CHOOSE FILE** in the **Upload** column.
3. Navigate and locate the corresponding OrgData CSV file from your computer.
4. Select the file and click **Open**.
5. Click **SUBMIT** to upload the file. When the OrgData import is complete, you can notice a green **SUCCESS** button in the **Result** column.
   Note: If the **SUBMIT** button is disabled, it means there is a mismatch in the filename displayed in **Name** column and the filename you selected. Resolve this mismatch by updating the filename and upload it again.

> ## Important
> The **Import Users** feature doesn't support upload or creation of Users or User Hierarchy. However, you can upload the CSV files as part of **OrgData Process**.

Importing OrgData through APIs

The OrgData API calls allow you to automatically import the most recently updated data from the data sources based on OrgData Process configuration.

Based on the OrgData configuration, you can also validate the imported data using the API. You can make API calls using the browser or third-party API tools. Within Skills Management, basic Swagger API tools are built into the solution and can be accessed through:

```
<Base URL>/api/swagger/ui/index
```

Under OrgData, you can run the following API calls:

- **Get UserFields** – returns the user fields created for a given tenant.
- **Post Validate** – validates the current OrgData configuration.
- **Post Process** – runs the OrgData process.
- **Put Upload** – uploads OrgData data file.
- **Get OrgData** – returns the current OrgData configuration.
- **Put OrgData** – uploads the configuration xml.

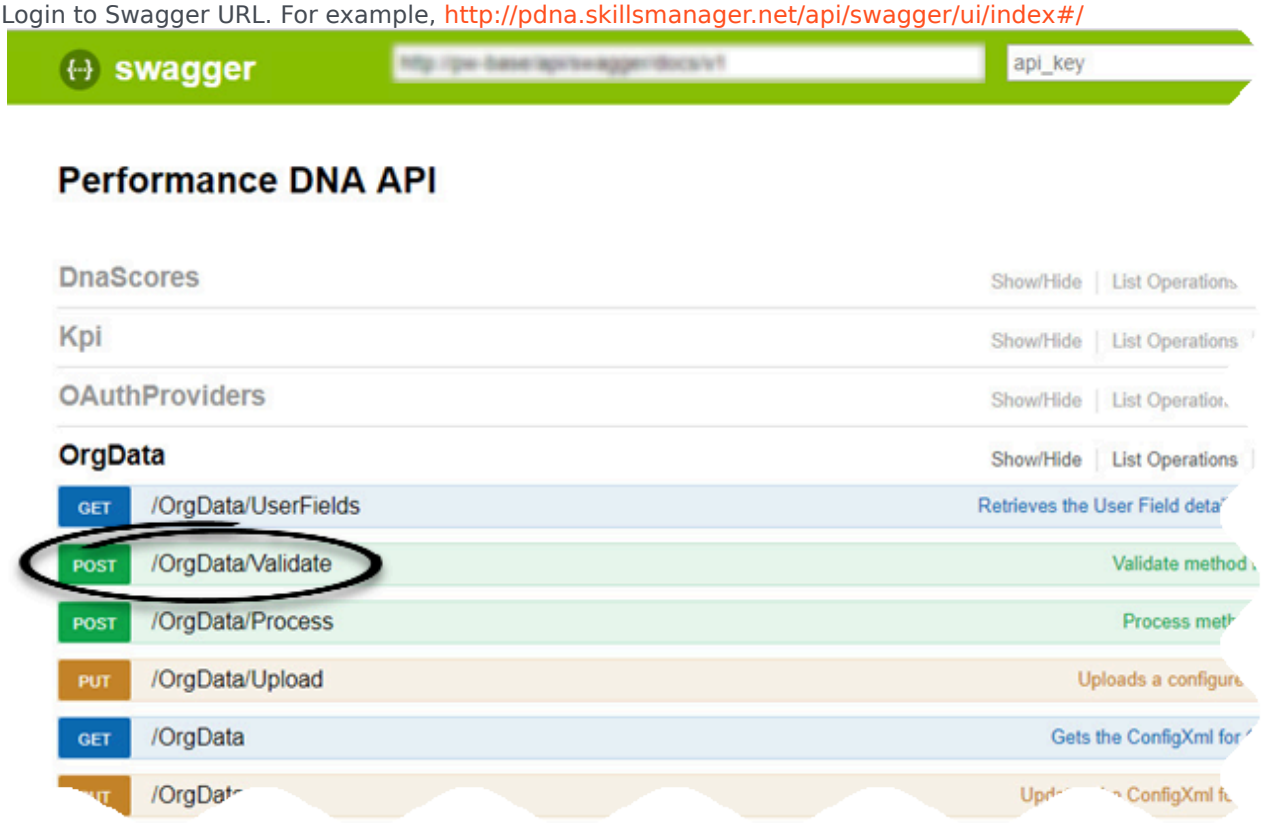
> ### Important
> If you have configured OrgData through the PDNA UI, then uploading OrgData configuration through **Put OrgData API** will overwrite the existing configuration and vice versa. Genesys recommends to always use the same process to manage your OrgData configuration, that is, either through the PDNA UI or API. Also, updating configuration through API will overwrite the user friendly metadata names that you might have created in the PDNA UI with defaults.

More information about the OrgData API is available in your API Help page, `<Base URL>/API/help`. Replace **Base URL** with the host name where you hosted the Skills Management application.

Validating OrgData Configuration

You can validate your current OrgData configuration by running the following procedure.

1. Login to Swagger URL. For example, http://pdna.skillsmanager.net/api/swagger/ui/index#/



2. Click and expand OrgData API set.
3. Click **/OrgData/Validate** POST method.
4. Click **Try it Out!** to run the validation. This will run the validation and display the results.
    - If you receive a *Response Class (Status 200)*, your OrgData configuration is valid.
    - If you receive a *Response Class (Status 400)*, your OrgData configuration is invalid.
5. Check the **Response Body** section for other validation errors and modify the **OrgData Setup** settings accordingly to correct the configuration.

> ### Tip
> Genesys recommends to batch the information that is sent to the API for validation. The Tenant Landlord can configure this batch size in the **Validate User Field Batch**

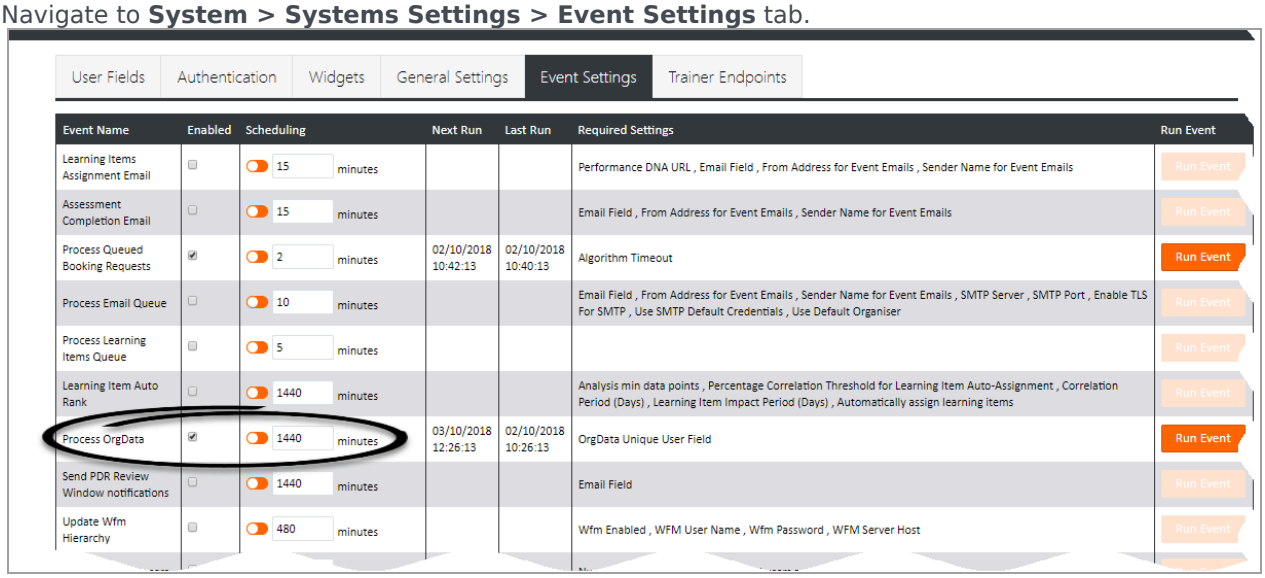
> **Size** field on the **System > Global Settings** page.

Running OrgData

In Skills Management application, you must define the timing or duration in which the OrgData process must run.

To define OrgData process

1. Navigate to **System > Systems Settings > Event Settings** tab.



2. In the **Event Settings** table, select the check box in **Enabled** column for **Process OrgData** event. By default, **Process OrgData** is disabled.
3. In the **Scheduling** column, you can either define a duration or a specific time on the server by using the toggle switch. The OrgData process will run based on the schedule you setup in this column.
    - Enter the minutes such that the event runs for every *X* minutes. By default, the event is set to run every 1440 minutes.
    - By toggling the switch, you can change the schedule from every *X* minutes to a specific time on the server.
4. Click **APPLY CHANGES** to save the schedule.

> ## Important
>
> You can explicitly run the OrgData process as an one-off event by clicking **RUN EVENT** or by using the **/OrgData/Process API** from Swagger.

Additional steps required to complete an upgrade to version 9.0

Upgrading from versions prior to 8.5 to 9.0 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, for example 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.

> ### Tip
>
> - 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 9.0 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.

Post upgrade steps

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.

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.

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.

> **Tip**
> 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.

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, for example “PerformanceDNA” (this may vary depending on the installer used)

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.

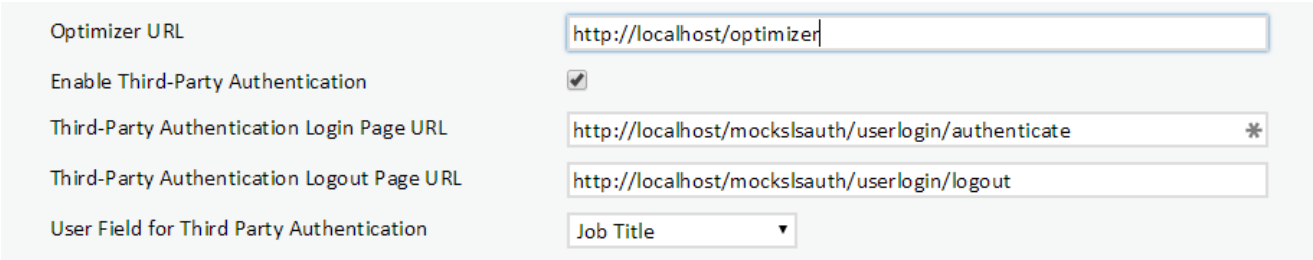
3rd Party Authentication

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.

Configuring Performance DNA

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.

Configuring Portal (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.

E-mail ADG Setting for IEX WFM

In previous versions the IEX email ADG was specified via the SkillsManagerWS/WebSettings.config file. This setting has been removed from this file. The email 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.

OAuth2 Authentication

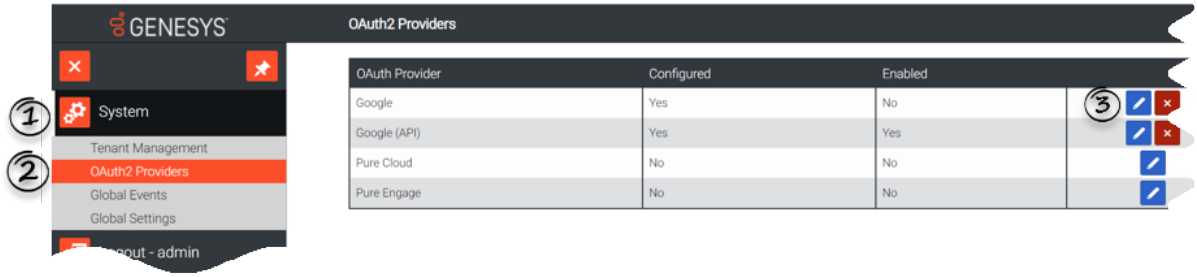
Configuring OAuth2 authentication for your users involves two steps:

1. Configuring an OAuth2 provider
2. Configuring Tenants with an OAuth2 provider

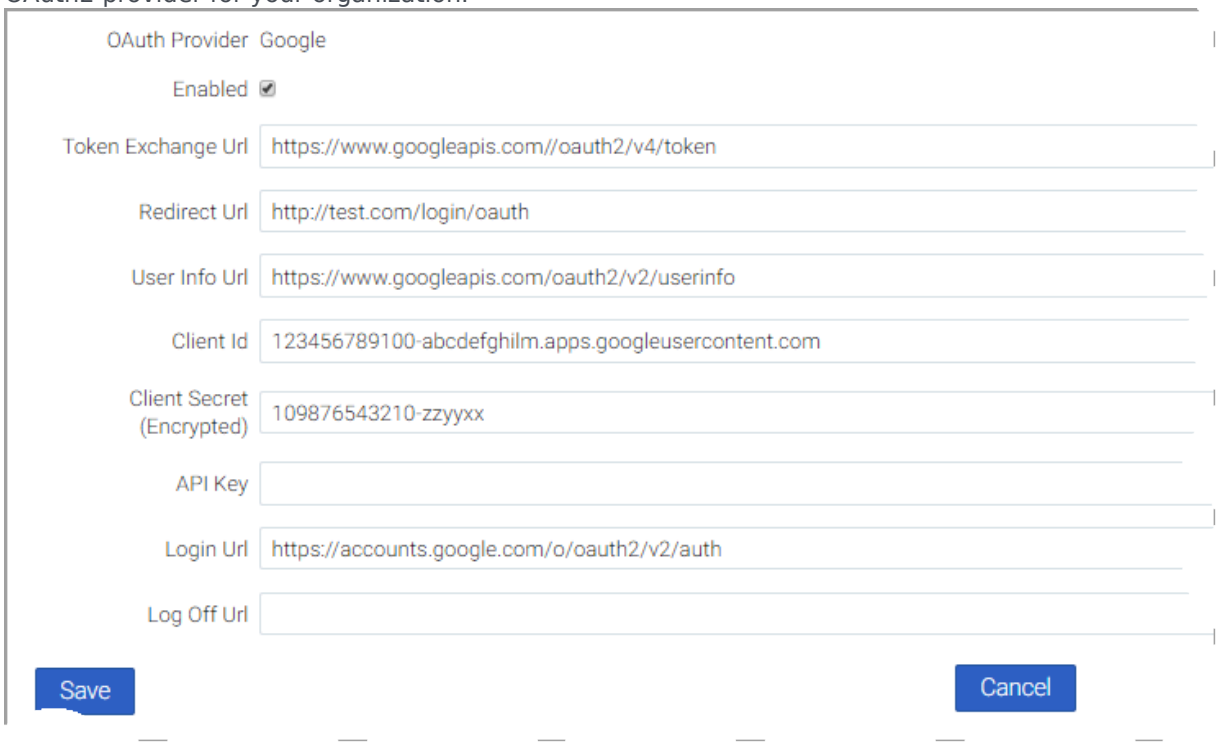
Configuring an OAuth2 Provider

You can configure the OAuth2 providers (for example, Google) for your organization from the OAuth2 Providers widget. Note that, you must be a Landlord to perform this procedure.

1. Login to **Performance DNA** as a Landlord.
2. Navigate to **System > OAuth2 Providers** widget. You will see a list of OAuth2 Providers that are currently supported such as Google, Genesys Cloud, and Genesys Engage.



3. Now click  for the OAuth2 provider you want to configure. You can configure only one provider type.
4. In the **Edit OAuth Providers** screen displayed below, select the check box **Enabled** to enable this OAuth2 provider for your organization.



5. Specify the URL details required for the OAuth2 provider. Ensure that you specify all mandatory fields (highlighted in red) with appropriate values. The mandatory fields are:
    - Token Exchange Url
    - Redirect Url

- User Info Url
- Client Id
- Client Secret (Encrypted)
- Login Url

6. Click **Save**.

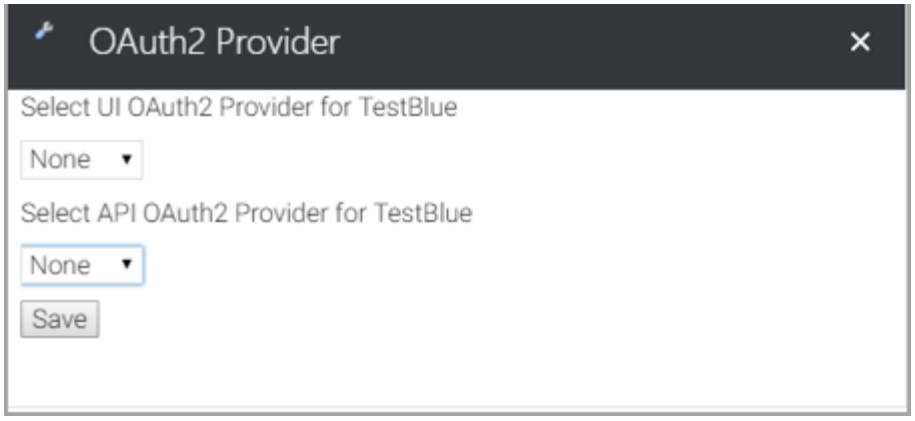
> **Important**
>
> - You cannot modify an OAuth2 Provider configuration if you have assigned Tenants. If you want to remove or modify an OAuth2 provider, you must first remove all the Tenants assigned to it, by navigating to **System > Tenant Management** widget.
> - GSM versions prior to **9.0.101** did not require **User Info Url** configuration in their OAuth setup. If the OAuth feature was configured prior to **9.0.101**, and you are upgrading the software to version **9.0.101** or above, then you must ensure that you configure a new parameter **User Info Url** before using any OAuth feature.

Configuring Tenants with an OAuth2 Provider

The next step in configuring OAuth2 authentication is to assign the OAuth2 Provider for your Tenants. Once you assign an OAuth2 Provider for a Tenant, the tenant's users are enforced with OAuth2 authentication method.

Note: You can create an OAuth2 Provider using the **OAuth2 Providers** widget. Follow the procedure Configuring an OAuth2 provider if you have not created an OAuth2 provider so far.

1. Login to **Performance DNA** as a Landlord.
2. Navigate to **System > Tenant Management** widget.
3. From the list of Tenants, click **Edit** for the Tenant for which you want to assign the OAuth2 Provider. You can see the **OAuth2 Provider** modal window.
4. On the **OAuth2 Provider** modal window, you can assign the OAuth2 Provider either for an user interface (UI) developed by your organization or an API.
   Note: The OAuth2 Providers listed in the drop-down fields are configured and enabled from the **OAuth2 Providers** widget. If a provider is not listed here, check if you have enabled the provider by using the OAuth2 Providers widget. Genesys supported authentication providers are Google, Genesys Cloud, and Genesys Engage.



5. Click **Save**.

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 the System Settings widget under the System section of the menu.
3. Click 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.

Configuring Updating Routing Skills

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.

Configuring Performance DNA to work with GIS

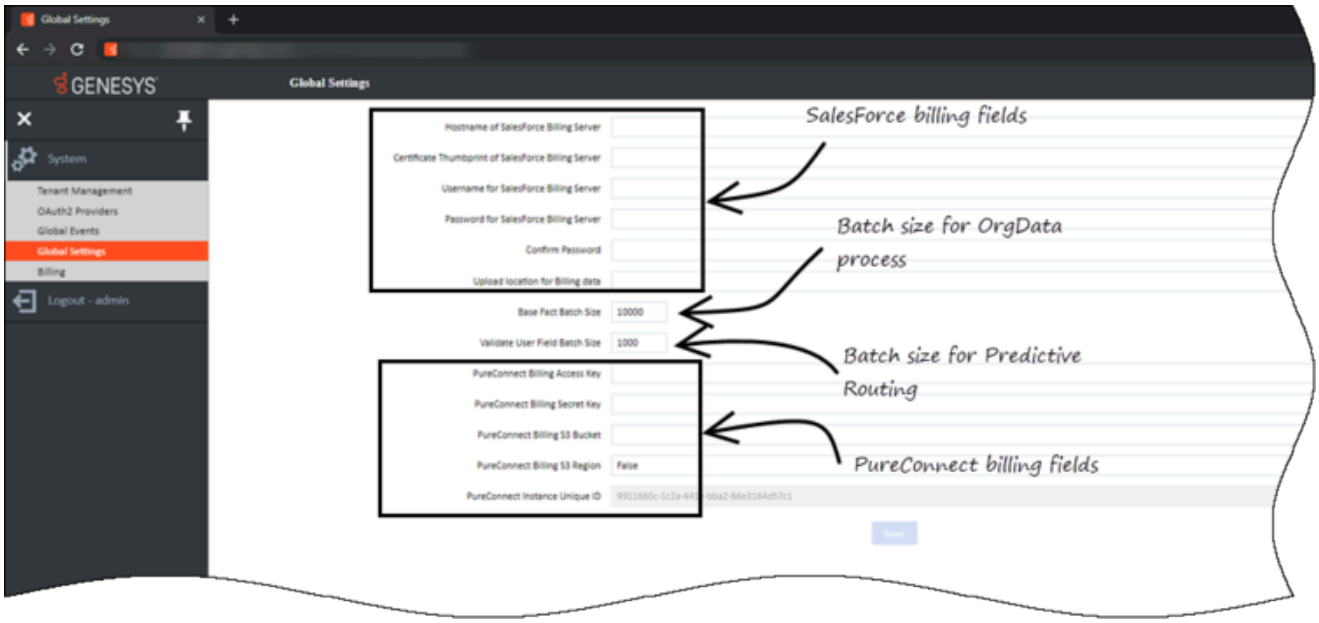
Enabling GIS

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.

Managing Global Settings

On this page, you can configure the following settings that are common to your organization.

- Salesforce Billing Server configuration
- PureConnect Billing Server configuration
- Batch size for OrgData processing and
- Batch size for Predictive Routing



Configuring Salesforce Billing Server

Follow the steps below to configure the Salesforce Billing Server details in Skills Management. Note that you must be a Landlord to perform this procedure.

- Navigate to **System** > **Global Settings** page.
- Enter the Salesforce Billing Server details in the following fields and click **Save**.
  - Hostname of SalesForce Billing server
  - Certificate Thumbprint of SalesForce Billing server
  - Username for SalesForce Billing server
  - Password for SalesForce Billing server
  - Confirm Password

- Upload location for Billing Data

Once you configure the server details, go to the Global Events page and setup the billing process that runs at scheduled intervals.

Configuring PureConnect Billing Server

The steps to configure PureConnect Billing Server in Skills Management are same as configuring Salesforce Billing Server. Note that you must be a Landlord to perform this procedure.

For PureConnect billing purposes, configure the following PureConnect specific fields on the **Global Settings** page.

- PureConnect Billing Access Key
- PureConnect Billing Secret Key
- PureConnect Billing S3 Bucket
- PureConnect Billing S3 Region - specify the S3 Region's code for this field, not it's name. For example, if your S3 Region is *EU (London)*, the related Region code you must specify is *eu-west-2*.
- PureConnect Instance Unique ID - this field is set as read-only on purpose.

Once you configure the server details, go to the Global Events page and setup the billing process that runs at scheduled intervals.

Configuring Batch Size for OrgData Processing

Base Fact Batch Size field allows you to set the maximum records that can be processed in a batch process while processing OrgData. The default value is `10000`.

Configuring Batch Size for Predictive Routing

Validate User Field Batch Size field allows you to set the maximum records that can be sent for Predictive Routing in a batch process. The default value is `1000`.

Managing Global Events

This page allows you to set events that are common to your organization. For example, setting Salesforce or PureConnect billing process.

> **Important**
> Events listed on this page are accessible only by a Landlord / Tenant Admin.

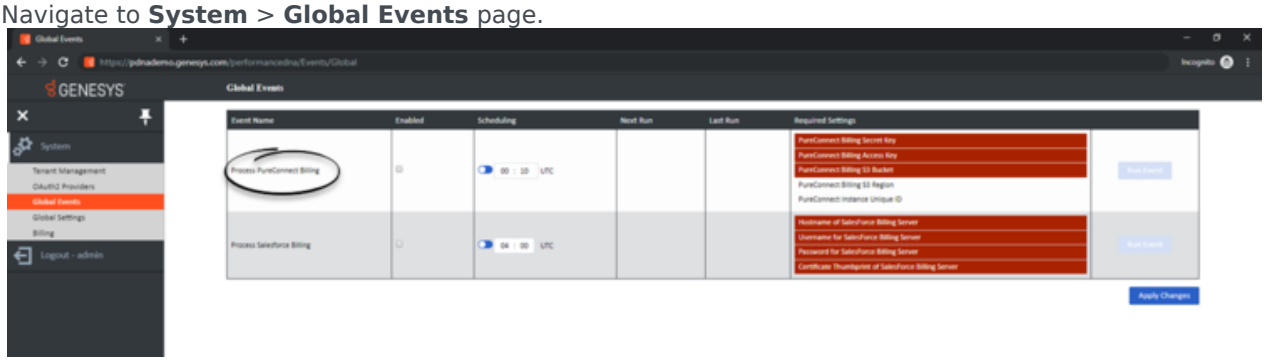
Configuring PureConnect Billing Process Event

Follow the steps below to configure the PureConnect billing process event in Skills Management. Note that you must be a Landlord / Tenant Admin to perform this procedure.

Prerequisite

Ensure that you have configured PureConnect Billing Server details in the **Global Settings** page.

1. Navigate to **System** > **Global Events** page.



2. Select the check box in the **Enabled** column for **Process PureConnect Billing** event. By default, this field is disabled.
3. In the **Scheduling** column, you can either define a duration or a specific time on the server by using the toggle switch. The **Process PureConnect Billing** event will run based on the schedule you setup in this column.
    - Enter the minutes such that the event runs for every *X* minutes, for example, 360 minutes. By default, the event is set to run every 1440 minutes.
    - By toggling the switch, you can change the schedule from every *X* minutes to a specific time on the server.
4. Click **Apply Changes** to save the settings.

> **Important**
> Once configured, you can also run the process manually by clicking the **Run Event** button.

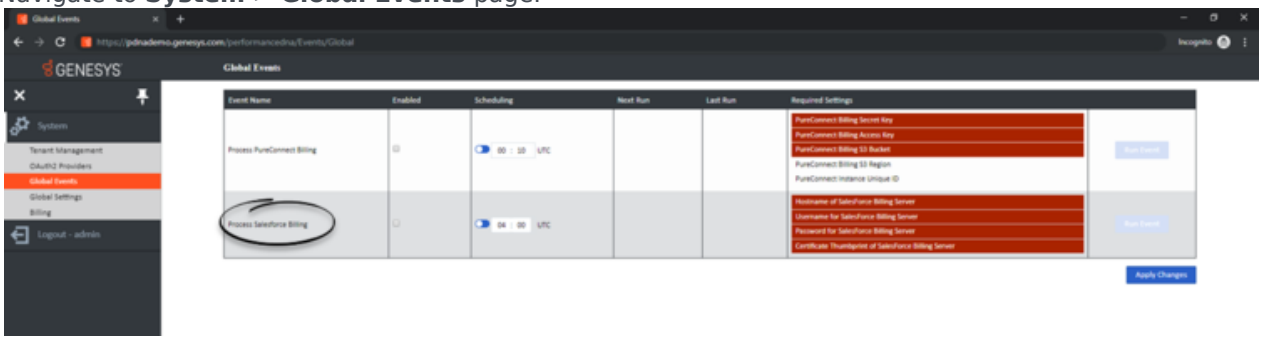
Configuring Salesforce Billing Process Event

Follow the steps below to configure the Salesforce billing process event in Skills Management. Note that you must be a Landlord / Tenant Admin to perform this procedure.

Prerequisite

Ensure that you have configured Salesforce Billing Server details in the **Global Settings** page.

1. Navigate to **System** > **Global Events** page.



2. Select the check box in the **Enabled** column for **Process Salesforce Billing** event. By default, **Process Salesforce Billing** is disabled.
3. In the **Scheduling** column, you can either define a duration or a specific time on the server by using the toggle switch. The **Process Salesforce Billing** event will run based on the schedule you setup in this column.
    - Enter the minutes such that the event runs for every *X* minutes, for example, 360 minutes. By default, the event is set to run every 1440 minutes.
    - By toggling the switch, you can change the schedule from every *X* minutes to a specific time on the server.
4. Click **Apply Changes** to save the settings.

> **Important**
> Once configured, you can also run the process manually by clicking the **Run Event** button.

Billing

Performance DNA offers billing capabilities for users who access the application from **Salesforce** and **PureConnect**. You can configure the corresponding server details in Performance DNA which enables you to setup and run billing processes automatically.

Next Steps

- Salesforce billing configuration
- PureConnect billing configuration

Salesforce Billing Configuration

Follow the procedures below to configure Salesforce billing information from Skills Management.

1. Create Tenant billing information from **Tenant Management** page.
2. Configure Salesforce billing server details from **Global Settings** page.
3. Enable Salesforce billing process from **Global Events** page.

Configuring Tenant Billing Details

When you create a Tenant, you can configure the billing details for the Tenant using **Tenant Management** page. This configuration automatically uploads the billing information of the tenant into Salesforce when the Salesforce billing process runs.

To configure Tenant billing details,

1. Login to Skills Management as a Landlord or Tenant Admin.
2. Navigate to **System > Tenant Management**.
3. Click **Edit** for the Tenant that you want to specify the billing details.
   For new tenants, you can specify the billing details when you create the Tenant.

4. Select the **Billable** check box.
5. Enter values for the following fields:
   - Tier1 Account Id
   - Tier2 AccountId
   - Tier3 Account Id

- External Id
- Source Id

Note: If you have an on premise installation, leave the above fields blank. If you are a cloud customer, enter the account details provided by the Genesys finance team.

6. Click **Next** to save the billing information.

PureConnect Billing Configuration

Follow the procedures below to configure the PureConnect billing information from Skills Management.

1. Configure the Tenant billing information from the **Tenant Management** page.
2. Configure the PureConnect billing server details from the **Global Settings** page.
3. Enable the PureConnect billing process from the **Global Events** page.

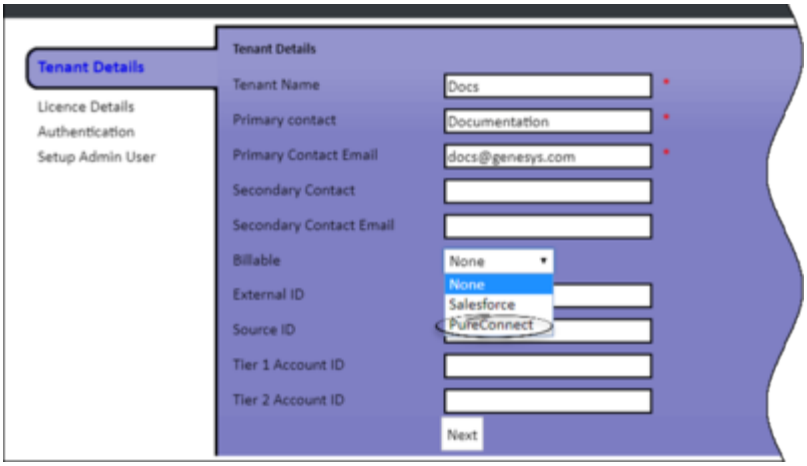
> **Important**
>
> You can also configure the PureConnect billing information through the relevant Tenant APIs. For more information on these APIs, see the Swagger API documentation help setup for your organization.

Configuring Tenant Billing details

When you create a Tenant, you can configure the billing details for the Tenant using the **Tenant Management** page. This configuration automatically uploads the billing information of the tenant to an Amazon Web Services (AWS) S3 bucket when the PureConnect billing process runs.

To configure Tenant billing details,

1. Login to Skills Management as a Landlord or Tenant Administrator.
2. Navigate to **System** > **Tenant Management.**
3. Click **Edit** for the Tenant that you want to specify the billing details.
   For new tenants, you can specify the billing details when you create the Tenant.



4. On the **Tenant Details** tab, select **PureConnect** from the **Billable** drop down.
5. Enter values for the following fields:
    - Tier1 Account Id
    - Tier2 AccountId
    - Tier3 Account Id
    - External Id
    - Source Id

    Note: If you have an on premise installation, leave the above fields blank. If you are a cloud customer, enter the account details provided by the Genesys finance team.
6. Click **Next** to save the billing information.

Viewing PureConnect Billing

Performance DNA allows a Landlord and Tenant Administrator to view the PureConnect billing information. The billing information is available for those Tenants that are configured as *PureConnect billable* in the Tenant Management dialog.

As a Landlord or Tenant Administrator, you can retrieve the billing information by navigating to the **System** > **Billing** menu. However, the options presented and the billing data will be different for your roles. See the sections below for more detail.

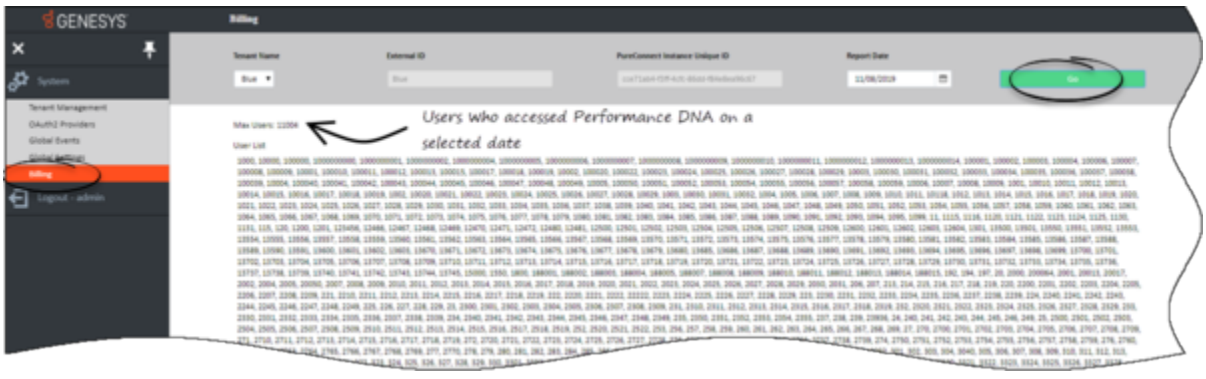
Note that you can view the PureConnect billing details only for the past six months.

Landlord billing view

If you are a Landlord, you can view the PureConnect billing information of the Tenants assigned to you. To retrieve the billing details, select the **Tenant Name** from the drop-down list and the **Report Date** for which you want to know the user details.

> ### Tip
> The **Tenant Name** drop-down list displays only those tenants that are configured as *PureConnect billable*.

Click **Go**, to see the maximum number of users that logged into Performance DNA on the selected date, and a list of user IDs that can be used for auditing purposes.

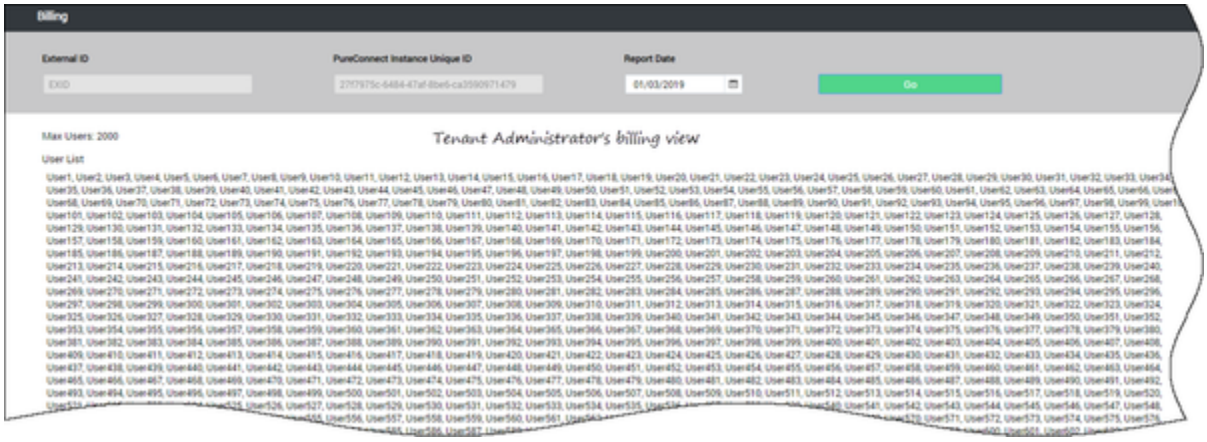


Tenant Administrator billing view

As a Tenant Administrator, you can view the PureConnect billing information of users belonging to

your Tenant only. To retrieve the billing details, select the **Report Date** and click **Go**.

You can see the maximum number of users that logged into Performance DNA on the selected date, and a list of user IDs that can be used for auditing purposes.



Licensing

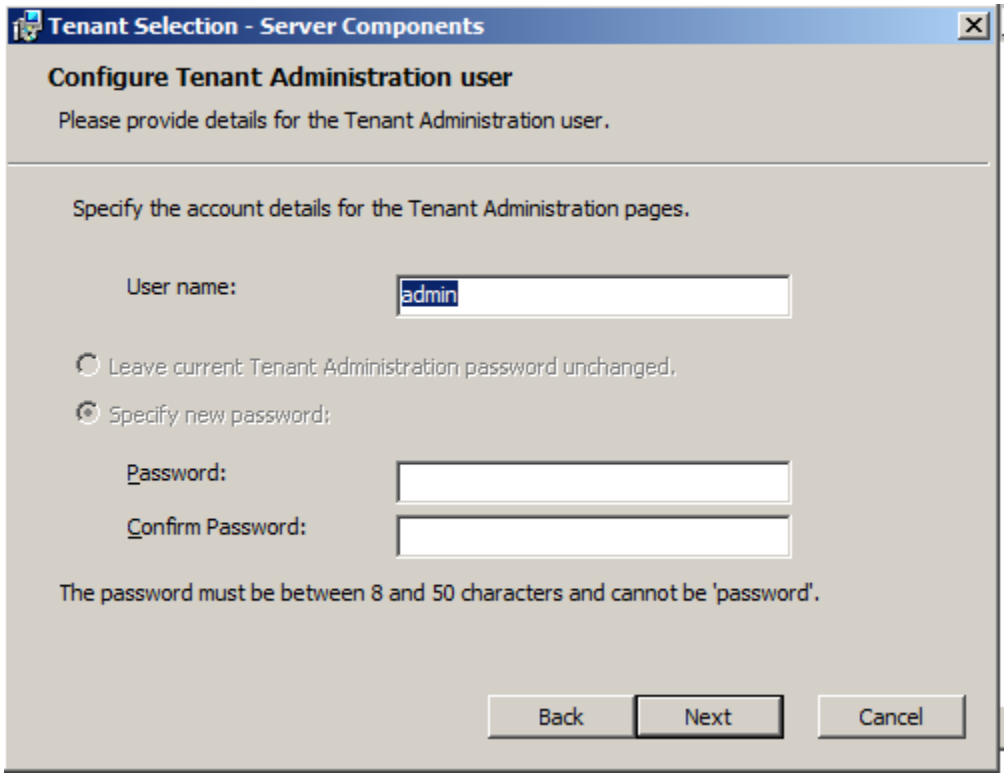
The following sections describe the licensing options in Performance DNA and Training Manager. If you have upgraded your product and your licences are still valid, there is no need to modify your existing licensing settings.

Licensing Performance DNA

Tenant Administration

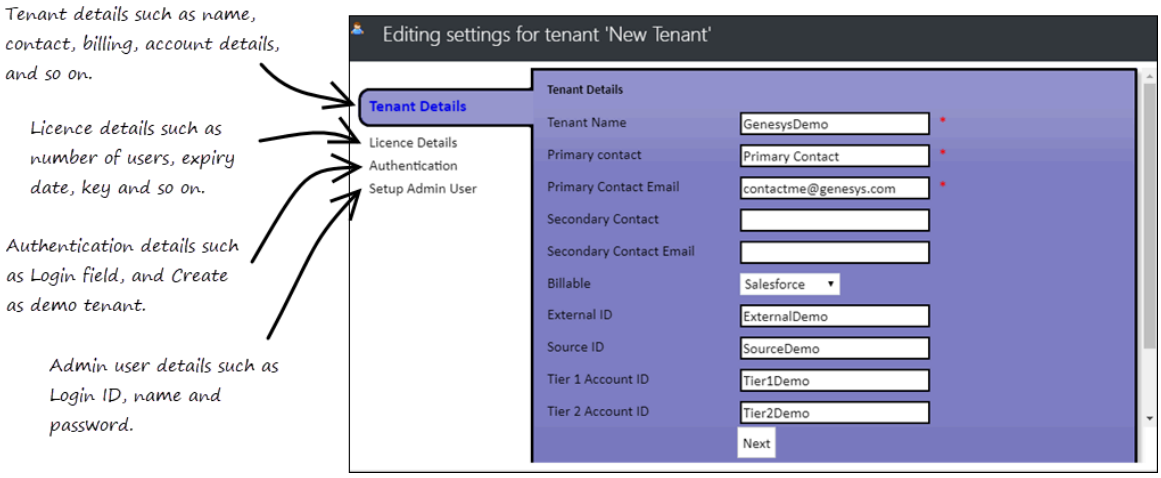
The Tenant Administration part of the Performance DNA application is accessible through the web server's hostname/login/admin, for example http://yourserver/login/admin.

To log in 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 that 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 **Create New Tenant**.



2. On the **Tenant Details** tab, enter the **Tenant Name** and **Primary Contact** details for the tenant that will be using the application. You can also specify the billing information from the **Billable** drop down before you click **Next**.
3. On the **Licence Details** tab, enter the license details for this tenant such as **Company name**, **Number of licenced users**, **Licence expiry date**, **Host name** and **Licence key** and click **Next**. Note that the number of licensed users are validated against the actual users of the system and you must resolve it when there is a license breach or violation. See License Validation for more information.

> **Important**
>
> If you have access only to Training Manager, specify only the **Host name**, and a **Licence expiry date**, for example 01/01/2050 and leave the remaining licence fields blank. This will enable only core Skills Management functionality to be available in the web portal. It will be necessary to enter your Training Manager licence (via the steps in the following section) to use the system.

4. On the **Authentication** tab, select the user field from the **Login field** drop down that will be used for authentication purpose and click **Next**. Note that the selected user field must be a field in an email format. Currently, Login Id is defaulted and is recommended for this purpose.
   Select **Create as demo tenant** if this tenant will be used for demo purposes. If selected, the system populates the tenant with the default demo data. This is an advanced feature recommended only for experienced users who will be showcasing the system. It should not be used for standard customer installations.

> **Important**
>
> Ensure to review the choices made on this screen, because the choices once submitted cannot be undone or modified in any way.

5. On the **Setup Admin User** tab, enter the administrator user details to create a new administrator for the tenant.
6. Click **Finish** to close the wizard and create a new standard or demo tenant.

Note that if the option **Create as demo tenant** was selected, the process to create a demo tenant will take an extra few minutes; otherwise, you will get the tenant details immediately.

7. When the tenant setup is complete, you will see the tenant details in the **Tenant Administration** screen.

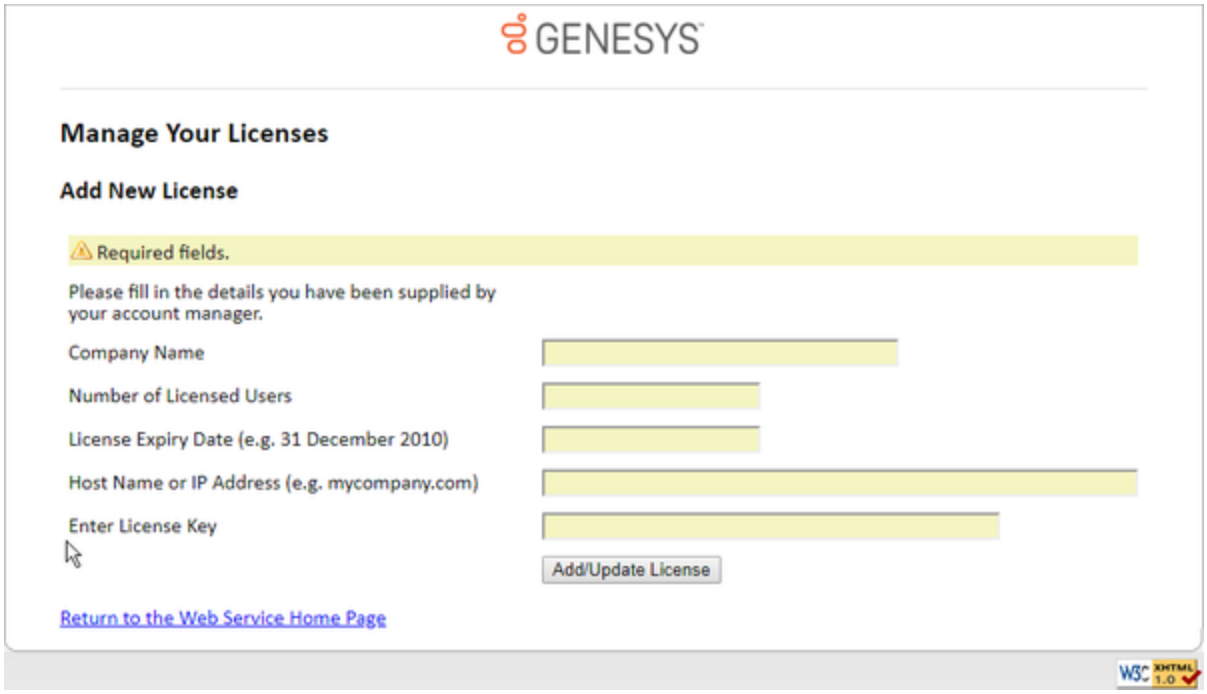
> **Important**
>
> If the tenant that is being created is a demo tenant, you will see the **Add Demo Data** option. Clicking this button generates demo data for a 6-week window in the past. This process can take several minutes to complete. The button will then update to **Refresh Unavailable** when you refresh the page. After 6-weeks have elapsed the button will change to **Refresh Demo Data**. Clicking the button will once again generate new demo data in a new 6 week window from the current date. If the users in a demo tenant need to be refreshed for any reason then edit the tenant and click through from next to finish. This will kick off another user creation run. Note that this process will take several minutes to complete generating the new data before the wizard closes.

If you wish to convert Performance DNA to use Active Directory authentication rather than the default form-based login system, refer to the Installation and Configuration Guide for Active Directory via the SLS Secure Token Service.

Licensing Training Manager

To set up your Training Manager license open a web browser and navigate to the **SkillsManagerWS** application, for example http://localhost/services/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).



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.

License Validation

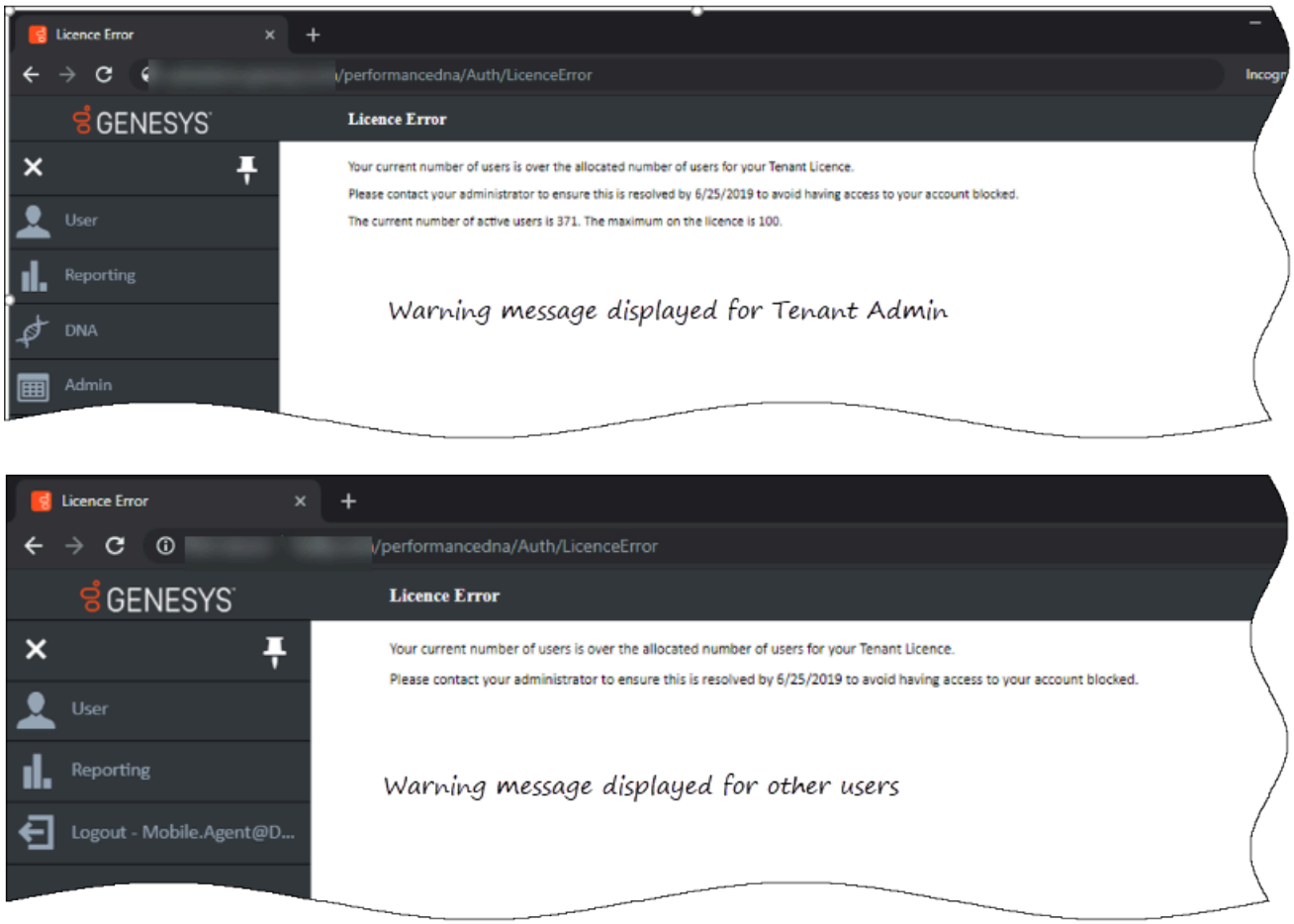
Performance DNA validates the number of active users for a Tenant against the number of users allocated for their license. Users that log in after a license breach are detected. A license breach Warning message is displayed to them. However, Performance DNA allows the user to ignore the Warning message and continue working in the application for **7** continuous days which is the *license breach active period*.

Disclaimer

- If breaching licenses are not resolved within the *license breach active period*, users are **blocked** from using the application.
- *Archived* users are not considered for license validation.

Tenant Administrator login

If a Tenant Administrator logs in to the application during the license breach active period, Performance DNA displays the license information, such as the **current active users** and the **maximum allowed users** along with the license breach Warning message displayed for other users.



How to resolve the license breach

To resolve the license breach, the Tenant Administrator can update the number of licenses from the Tenant Administration dialog or reduce the number of active users when the breach is active. If this issue is not resolved within the license breach active period (**7** days), users attempting to login to the system thereafter will be **blocked** from using the system.

Disclaimer

The Tenant Administrator must resolve the licensing issue during the license breach active period, after which only a Landlord can update the breaching Tenant's license.