



Skills Management 9.0.0

Automated Installation and Upgrade Guide (Command Line)

Information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

Copyright © 2017 Genesys Telecommunications Laboratories, Inc. All rights reserved.

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_command-line_06--2018_v9.0.001.00-B

Contents

1	Introduction	4
2	Prerequisites	5
2.1	Database Server Software Prerequisites	5
2.2	Web Server Software Prerequisites	5
2.3	Service account considerations	7
2.3.1	Local user account.....	7
2.3.2	Domain user account	7
2.4	Networking pre-requisites	7
2.5	Email Messaging Service	7
3	Installation	9
3.1	Additional options.....	11
3.1.1	Logging	11
3.1.2	UI visibility.....	11
3.1.3	Advanced installation.....	12
3.1.4	Check service credentials.....	12
4	Exported Portal Users	14
5	Additional steps required to complete an upgrade to version 4.8.....	15
6	Post upgrade steps	16
6.1	Removing artefacts from previous installations	16
6.1.1	Microsoft Analysis Server Databases	16
6.1.2	DNA Databases.....	16
6.1.3	Deprecated scheduled tasks for Performance DNA	16
6.2	Configure Training Manager-Performance DNA Integration.....	16
6.3	3rd Party Authentication	17
6.3.1	Performance DNA Configuration	17
6.3.2	Portal Configuration (via Training Manager)	17
6.3.3	Setting the e-mail ADG for IEX WFM	18
6.4	Configuring Updating Routing Skills.....	18
6.4.1	Connectivity Overview	18
6.4.2	Configuring Performance DNA to work with GIS	18
7	Licensing	19
7.1	Licensing Performance DNA.....	19
7.1.1	Tenant Administration	19
7.2	Licensing Training Manager	20

1 Introduction

This guide provides instructions for installing or upgrading the Skills Management suite via the Skills Management Setup MSI application in command line mode.

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)
 - 20 kuJ
 - 20 kuJ
- 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 4.9.x the old Email Messaging Service will need to be uninstalled.

As part of the 4.9.x release this functionality is included within the main installer and is configured through the user interface.

3 Installation

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

Run msixec 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\Website s\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\Website s\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\Website s\performance dna	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\Website s>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

Parameter	Default value	Explanation
REPORTSDB	Skills Management Reports	The name for the Reporting database
PERFDNADB	PerformanceDNA	The name for the Performance 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 <i>case-sensitive</i> .

Parameter	Default value	Explanation
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 <i>case-sensitive</i> .
REMOVEDBS		(Uninstall only) Yes if the databases should be removed by the installer. Anything other than Yes will mean the databases are left as they are. Note that the Yes is <i>case-sensitive</i> .
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 <i>case-sensitive</i> .
STSENABLED		Set this property to Yes if you want to enable AD authentication via the STS service. Note that the Yes is <i>case-sensitive</i> .
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.

3.1 Additional options

3.1.1 Logging

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

```
/!*v logFileName.txt
```

3.1.2 UI visibility

/q – don't show the user interface

/passive – shows a basic progress bar

3.1.3 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" STSENBLED="No"
STSCERTTHUMBPRINT="" /q /l*v log.txt
```

Note: 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.

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 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.

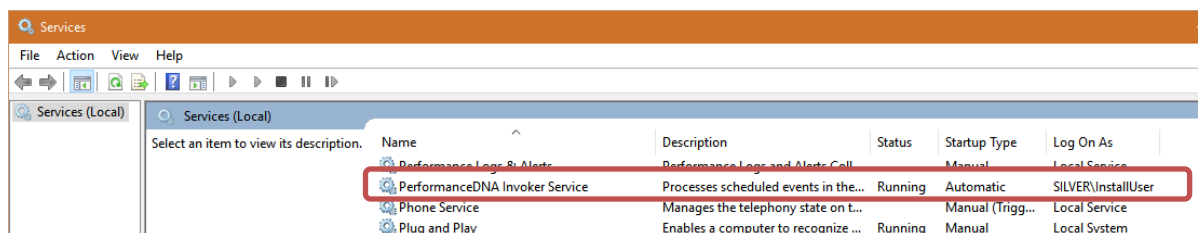
If you require DNA, follow the steps to configure DNA from the **Performance DNA v9.0.0.0 Manual Installation Guide**.

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.

3.1.4 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:

Performance DNA URL	<input type="text" value="http://www.blue.com/performancedna/"/>
Enable Third-Party Authentication	<input checked="" type="checkbox"/>
Third-Party Authentication Login Page URL	<input type="text" value="http://localhost/mockslauth/userlogin/authenticate"/>
Third-Party Authentication Logout Page URL	<input type="text" value="http://localhost/mockslauth/userlogin/logout"/>

- 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:

<input checked="" type="radio"/> SLS Third Party	Authenticate with	User Name
	Login URL	http://localhost/mockslsauth/userlogin/authenticate
	Logout URL	http://localhost/mockslsauth/userlogin/logout

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

6.3.3 Setting the e-mail ADG 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 SkillsPortal 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 SkillsPortal settings screen after upgrading.

6.4 Configuring Updating Routing Skills

6.4.1 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 **CSPProxyService** service to retrieve and update information in CME.

6.4.2 Configuring Performance DNA to work with GIS

6.4.2.1 Enabling GIS

Before the configuration options for GIS will appear in Performance DNA, a new record needs adding 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).

Manage Your Licenses

Click on any of the licenses below to view.

- [www.blue.com](#)

Add New License

 Required fields

Please fill in the details you have been supplied by Silver Lining Solutions. If you do not have these details, please contact us.

Company Name	<input type="text"/>
Number of Licensed Users	<input type="text"/>
License Expiry Date (e.g. 31 December 2010)	<input type="text"/>
Host Name or IP Address (e.g. mycompany.com)	<input type="text"/>
Enter License Key	<input type="text"/>

[Return to the Web Service Home Page](#)

The system will be available once you have either as 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 have full access to the widgets of both products. Other users' access is restricted based on the widgets available to their assigned roles.