TRAKA WEB INSTALLATION GUIDE

TD0013

03/05/19

VERSION 6.4

VERSION HISTORY

Version	Date	Who	Description of Changes	Approved By
1.0	13/06/11	DJW	Initial version of document	
1.1	27/06/11	AJP	Document Detail	
1.2	30/06/11	AJP	Various Updates	
1.3	04/07/11	DJW	Revised various sections and added section for Traka Touch Setup	
1.4	14/07/11	AJP	Revised Certificate install instructions, Section 7 Added for Windows 2003 IIS6 installation instructions.	
1.5	17/08/11	AJP	Revised Certificate install instructions	
1.6	19/09/11	AJP	Various Additions to Admin Application Section	
1.7	3/11/11	AJP	Various Additions and Authentication Options, Email Options	
1.8	4/11/11	AJP	Various Updates	
1.9	11/01/12	AJP	SSL Certificates Section Added	
2.0	26/10/12	AJP	Update for new Traka Web Version 01.04.0003	
2.1	15/03/13	AJP	Added product editor section	
2.2	10/05/13	AK	Added IIS install on Windows 7	
2.3	15/05/13	AK	Various Updates	
2.4	28/05/13	DJW	Various Updates	
2.5	29/05/13	SD	Various Updates	
2.6	05/06/13	SD	Updated IIS prerequisites for Windows 7 and Windows Server 2008	
2.7	08/05/14	AK	Updated step eight in section 4.2 (Database Setup) to reference the authentication section.	
2.8	29/08/14	AK	Updated the required version of .NET	
2.9	01/09/14	SD	Updated system requirements. Added upgrade, section 4. Added link and file name for .NET 4.5. Added details for changing the default Traka Web language.	
2.10	09/09/14	DW	Updated section 4.1 detailing the need to change the default language in Web.Config after upgrade.	
2.11	11/09/14	DW	Updated link and filename for .NET 4.5	
3.0	07/11/14	AK	Updated the windows server installation requirements.	
3.1	07/05/15	DW & AK	Corrected mistakes in referencing section 5 as section 4. Added information on email notifications to section 8.	
3.2	16/06/15	JO'C	Corrected general mistakes	
3.3	02/07/15	LN	Updated the System Setup section to suit new product designer	
3.4	15/07/15	LN	Notes added to highlight supported products in Product Designer section	
3.5	06/08/15	LN	Relocated Error 0x800F0906 section	
3.6	12/08/15	LN	Restructured prerequisites section. Added note on uninstalling security certificates in Upgrade section.	
3.7	14/10/15	LN	Added separate section for Windows Server 2012 and Windows 8.1 in prerequisites.	
3.8	02/12/15	JO	Updated Traka Web prerequisites.	
3.9	20/01/16	LN	Added 'Enabling HTTPS (SSL)…' section 7.4.	
4.0	/16	RC	Added 'Updating the Database' Section 3.4. Added description for 'Allow Ping' and 'Online' in the System set up – Section 5.5. Updated image in section 5.2, Connecting to the Business Engine. Document changed from UD0016 to TD0013	
4.1	26/07/16	RC	Removed section on SSL – section 7.4, pending further information.	
4.2	01/08/16	RC/JO	Updated Traka Web prerequisites – Section 2	
4.3	05/09/16	RC	Added new section for Transferring a Traka Web Database to a New Server to section 4.10	
4.4	27/01/17	RC	Updated Screen image in section 5.2 for the database config setup. Included an instruction for clicking on 'create new' button.	
4.5	30/01/17	RC	Added enabling windows features for Windows 10. Section 2.5.	
4.6	06/02/17	RC	Added section for saving Product Type in Traka Web Admin. Section 5.5.2	
4.7	15/03/17	RC	Added reference information for 16bit support installation. Updated Admin App screen shots.	

4.8	07/04/17	RC	Added information on System Viewer grid to section 5.5.3	
4.9	25/04/17	RC	Added Win 10 information to Section 1.7	
5.0	03/05/17	RC	Amendment to section 5 for Business Engine to be used for Integrated Authentication into SQL	MS & SD
5.1	24/05/17	RC	Additional Windows 10 information added to section 1.7	
5.2	14/09/17	RC	Added 'Enabling HTTPS (SSL) to section 7.3 with new changes	
5.3	06/12/17	SD	Section 5 updated to correspond correctly with TD0149 and TD0150	
5.4	24/01/18	RC	Added Traka Web Admin Job Scheduler to Section 8.3	
5.5	27/03/18	JO	Updated section 1.7 - Traka Web Pre-requisites	
5.6	11/04/18	RC	Added Windows Authentication information to sections 4.1 & 7.2.1. Also updated screen shots throughout document. Server specifications updated in section 1.7	JL
5.7	09/05/18	JO	Corrections to section 5.2.1	
5.8	17/05/18	WT	Restructure layout. Upgrade of existing Database and Transfer of a Database now moved from middle of installation to their own procedures 7 & 8. Windows 10 IIS Settings made clearer to follow.	
5.9	14/6/18	RC	Added notes to Certificate installation. Sections 3.2, 3.4, 3.6 & 3.8	
6.0	26/9/18	JO	Added IIS settings for Windows Server 2016	
6.1	16/10/18	WT	Fix incorrect references to sections within document	
6.2	12/11/18	JO	Added new languages into list	
6.3	08/02/19	JO	Changes to Traka Web installation section	
6.4	03/05/19	JO	Minimum SQL & OS versions supported changed	

CONTENTS

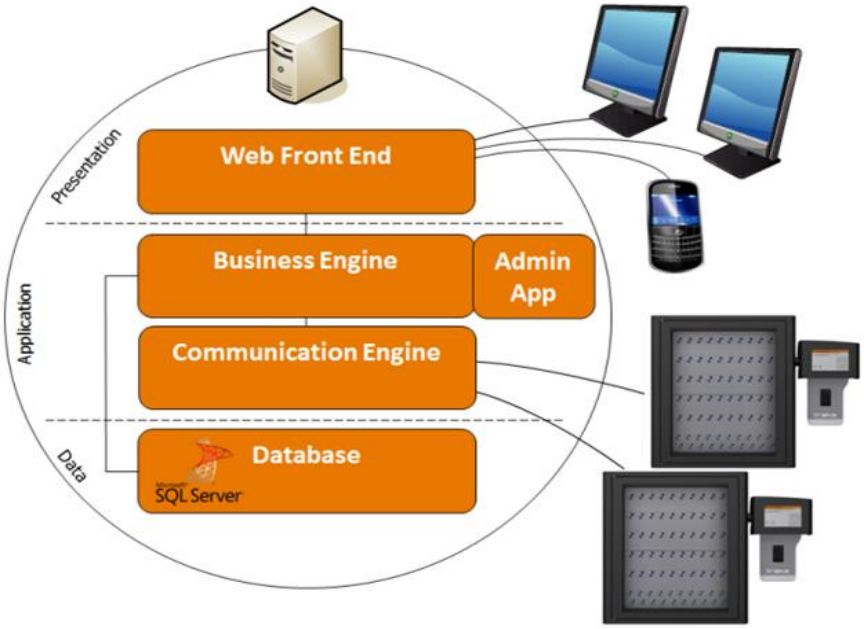
1. INTRODUCTION

This document provides an overview of Traka Web and explains in detail how to install and configure the various components that make up the Traka Web distributed Key Management Administration system.

The Traka Web system is made up of 6 separate components:

- Web Front End
- Business Engine Service
- Communication (Comms) Engine Service
- Admin Application
- Database
- Traka Touch

Architecture Diagram:



1.1 WEB FRONT END

The Web Front End is a 'Web based Application' built using the Microsoft .NET Framework and forms the presentation layer of the Traka Web system.

This Web Application allows the securely logged-in user to oversee and administer associated Traka Touch systems. Depending on the permissions granted, administrators can perform tasks such as editing and configuring User, iFob and Item records, plus configure access permissions individually or via groups. A dashboard provides a quick overview of individual Traka Touch systems showing current status and various activities. A full audit trail is available along with various statistics which provide administrators with all the tools required to manage the systems on a daily basis.

The Web Front End can authenticate users using either basic authentication where the user is asked for a username and password, or using Windows authentication where the user is authenticated automatically using their Windows Domain credentials.

The Web Front End connects to the Business Engine Service via a secured connection using an X509 certificate.

The Web Front End must be run on a Web Server that has access to the server that the Business Engine Service will be running on.

1.2 BUSINESS ENGINE SERVICE

The Business Engine Service is the business layer of the Traka Web system and runs as a Windows service.

The Traka Web Business Engine Service is central to the Traka Web system and provides the Traka Web Front End with all of its required data and services. As well as connecting to the Traka Web Front End the Business Engine Service also connects to the backend database and the Comms Engine Service via a secured connection using an X509 certificate.

The Business Engine Service must be run on a server that has access to the server running the Comms Engine Service.

1.3 COMMS ENGINE SERVICE

The Comms Engine Service is the communication layer of the Traka Web system and runs as a Windows service.

The Comms Engine Service controls all of the communication to and from the Traka Touch Systems and transmits this information back to the Business Engine where it is processed.

The Comms Engine Service must be run on a server that has access to the server running the Business Engine Service and the Comms Engine Service must be able to connect to the Traka Touch Systems.

1.4 DATABASE

The first release of Traka Web supports Microsoft SQL Server 2012 and above (including the Express edition) as its backend database server.

The Business Engine Service is the only component that connects to the database using a single secure account that is configured via the Admin Application. The Admin Application can connect to the database, but only has access to administration functions.

1.5 ADMIN APPLICATION

The Admin Application is a Windows based administrative tool that allows the initial setup and configuration of the Traka Web system. This application provides the ability to create the Traka Web database from scratch, as well as creation and configuration of the Business Engine, Comms Engine and Traka Touch system records.

The Admin Application can be run on any server that has access to the Business Engine Service.

1.6 TRAKA TOUCH SYSTEMS

The Traka Touch systems provide the physical element of the Traka solution for managing items such as keys and other assets. The Traka Touch systems are modular, and come in a variety of shapes and sizes depending on customer requirements. Below represents an example of the Traka Touch S-Series with 70 keys.

1.7 INFRASTRUCTURE CONSIDERATIONS (TYPICAL SYSTEM REQUIREMENTS)

Before installing the Traka Web system, consideration should be made to the size of the system, e.g. total number of Traka Touch systems and total number or users expected to be setup on the system to decide how the system infrastructure should be arranged.

It is possible to run all of the Traka Web components on the same server if required. The guidance below assumes that the Traka Web components are the only additional software (over and above the OS) installed on the server. They should serve as a guide only. Please contact Traka Technical Support or your Account Manager to discuss your specific requirements. Listed below are typical server specifications:

- **Windows Server 2016 with IIS10**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows Server 2012 R2 with IIS8.5**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows Server 2012 with IIS8**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows 10 (Professional or Enterprise editions) with IIS10**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **Windows 8.1 (Professional or Enterprise editions) with IIS8.5**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **Windows 8 (Professional or Enterprise editions) with IIS8**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **Windows 7 SP1 (Professional or Enterprise editions) with IIS7.5**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **32 or 64 bit support**
  Physical or Virtual machine support

2. PREREQUISITES

The following Client Browsers are supported:

Internet Explorer (v9 minimum but latest version recommended)

Google Chrome (latest version recommended)

Mozilla Firefox (latest version recommended)

Safari (latest version recommended)

The following Databases are supported:

SQL Server 2012 and above (incl. Express version) and may be configured to **'Mixed Mode Authentication' or 'Windows Authentication'.**

This document describes how to setup the Traka Web software components. It is assumed that the installer already has some knowledge of managing and administering a Windows based computer.

The following items should be checked before beginning the installation of Traka Web:

Install Microsoft.NET Framework 4.5 by running the following file on your server – NDP451-KB2858728-x86-x64-AllOS-ENU.exe. This file is included with the Traka Web install files inside the 'Prerequisites' folder, but can also be downloaded here: http://www.microsoft.com/en-us/download/details.aspx?id=40779. If you encounter Error 0x800F0906 during the installation of Microsoft.NET on Windows 8 then please follow the procedure outline in the 'Troubleshooting' section of this document.

NOTE: Traka recommends that you have the latest Microsoft Windows Security fixes applied via Windows Update to ensure optimal compatibility with the Traka Web installation for supported Operating Systems.

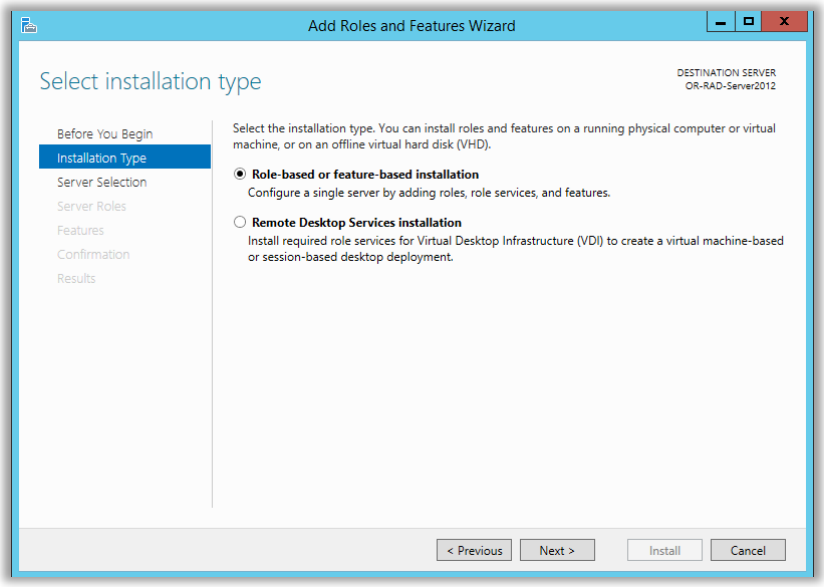
2.0 WINDOWS SERVER 2012 R2

This section describes the steps required following a new installation of Windows Server 2012 R2.

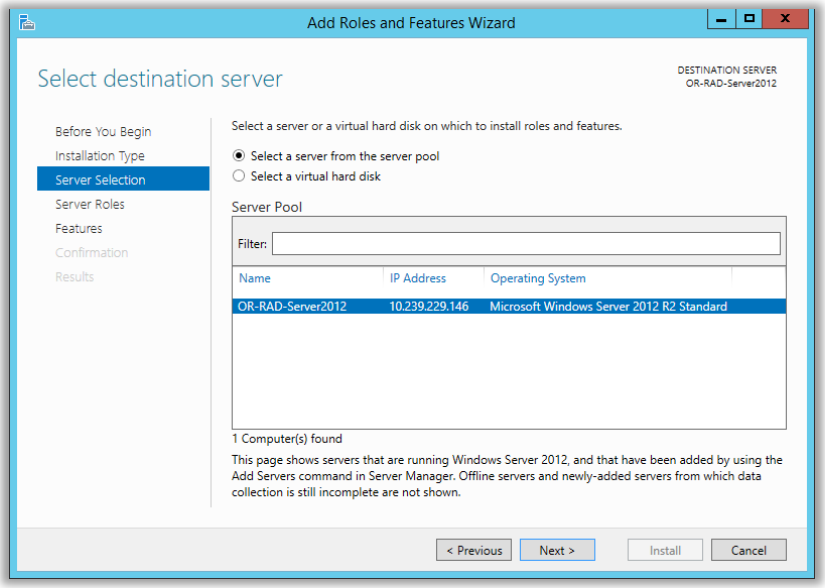
The server operating system should have all of the latest updates from Microsoft installed.

2.0.1 IIS

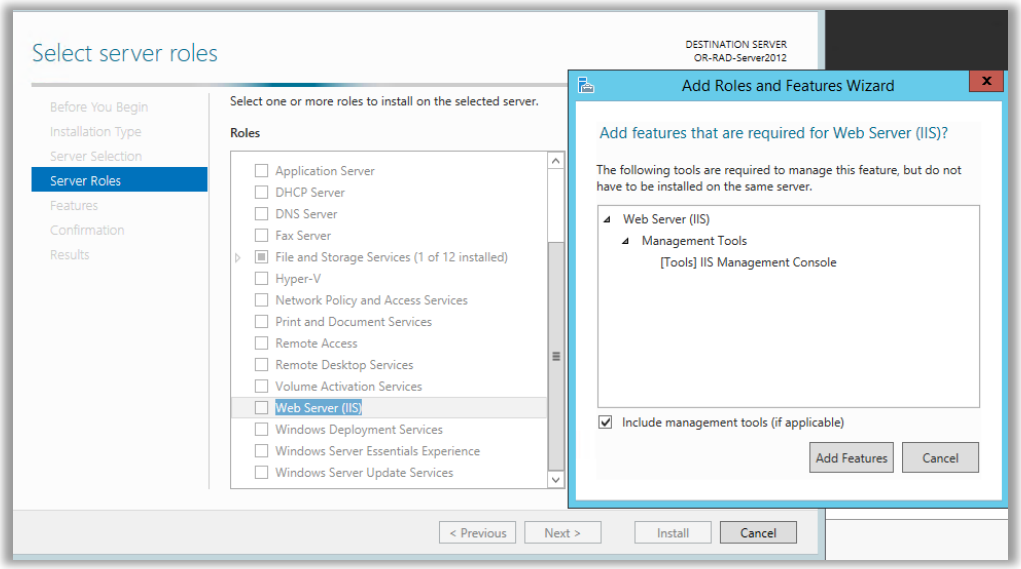
1. Go to: Server Manager > Add Roles and Features.
2. Navigate to the Installation Type page of the Wizard and select 'Role-based or feature-based installation'.



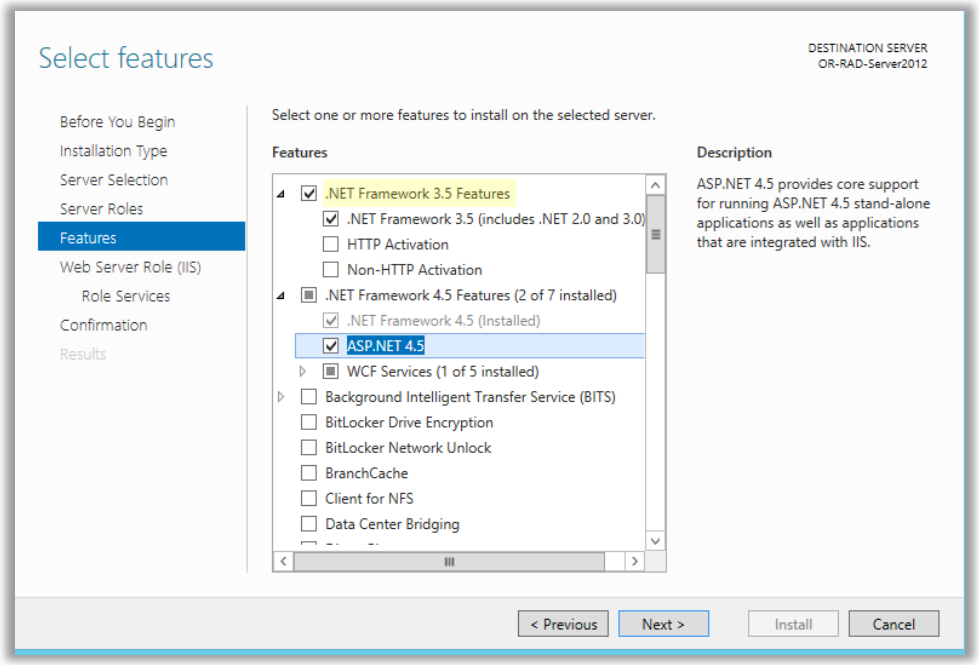
3. Click **Next** and then select the '**Select a server from the server pool**' option from the Server Selection page.



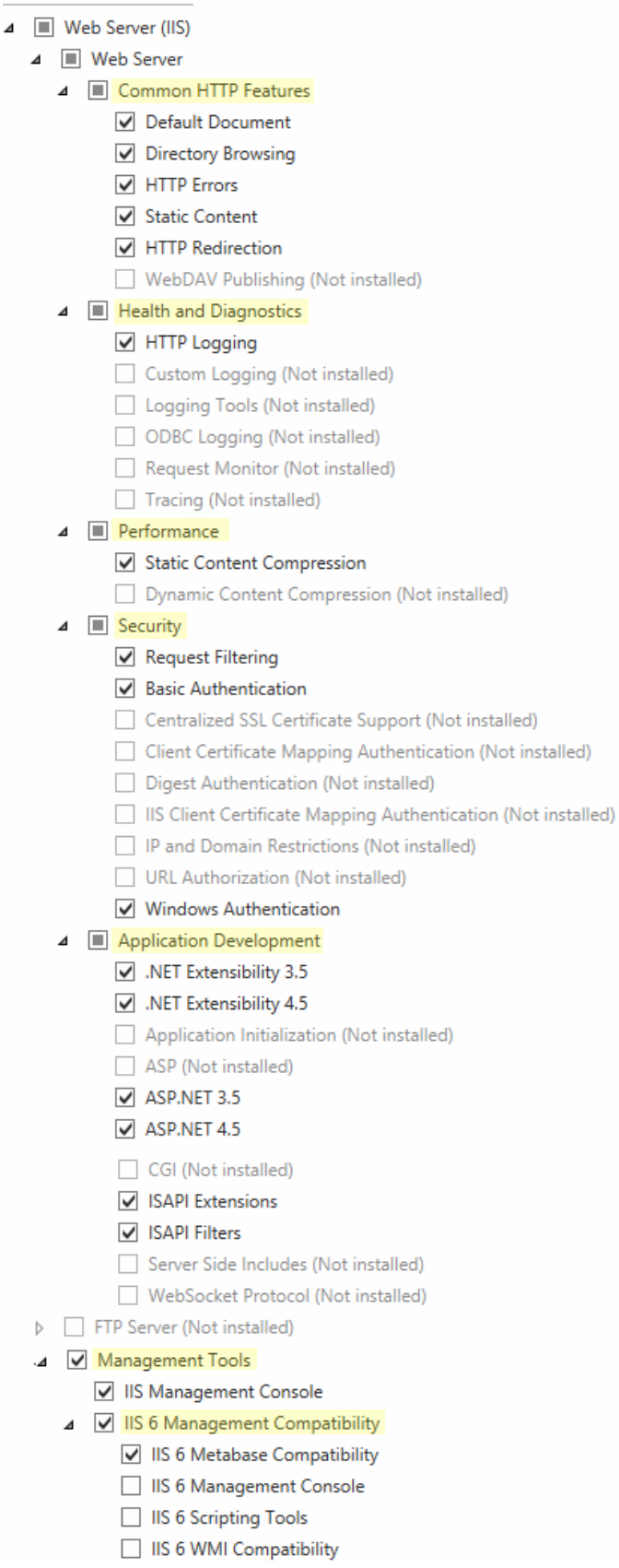
4. Select the required server from the list and click **Next**.
5. From the Server Roles page click '**Web Server (IIS)**' and a popup will appear as shown below. Click **Add Features** and then click **Next**.



6. Expand **.NET framework 3.5 and 4.5 Features** and tick the boxes shown below.



7. Click **Next**, and **Next** again to get to the Role Services page. From here select all the options that are ticked in the image below.



8. Click **Next** and then **Install**.

9. Please now refer to the Installation section.

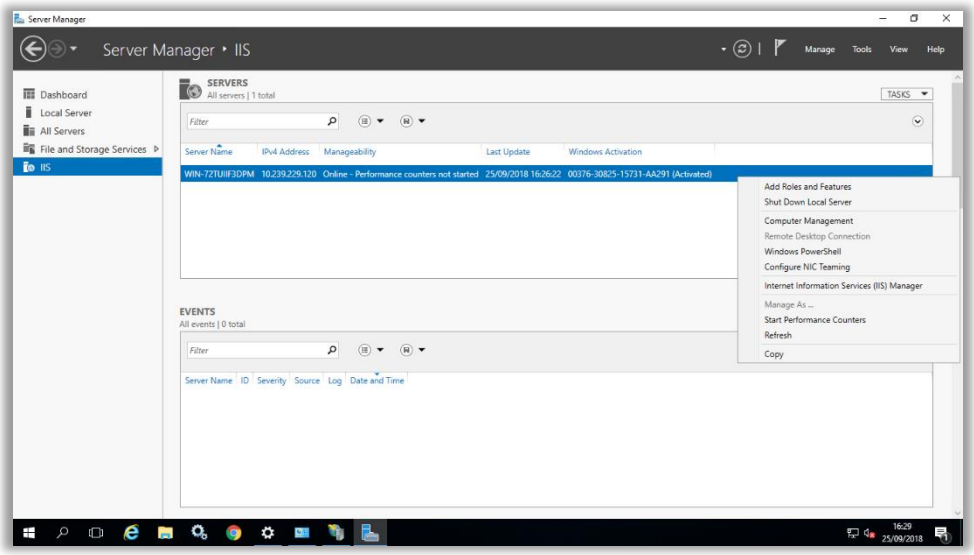
2.1 WINDOWS SERVER 2016

This section describes the steps required following a new installation of Windows Server 2016.

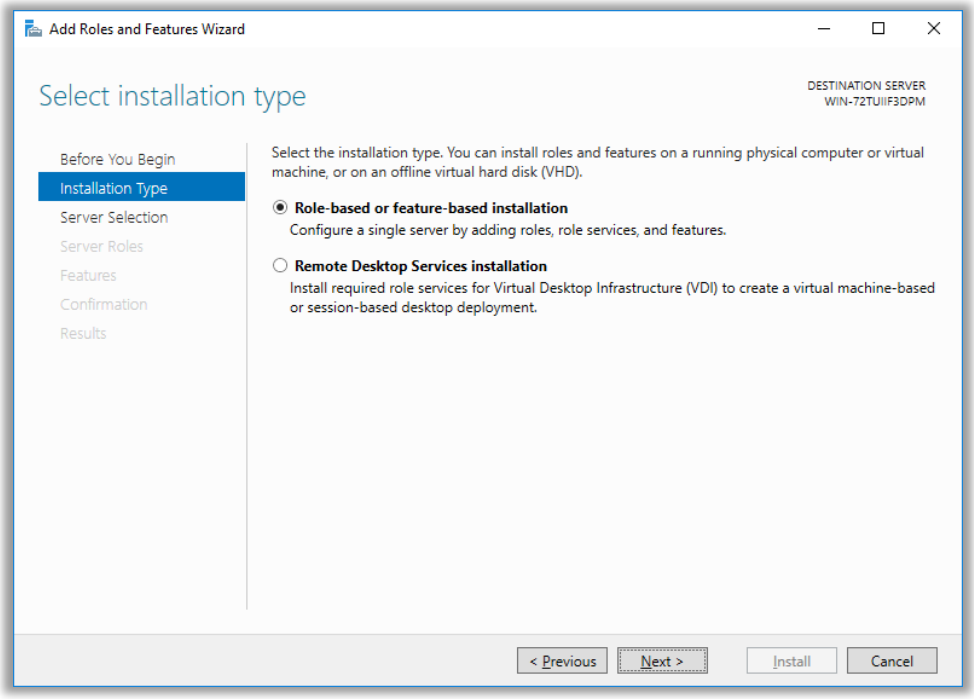
The server operating system should have all of the latest updates from Microsoft installed.

2.1.1 IIS

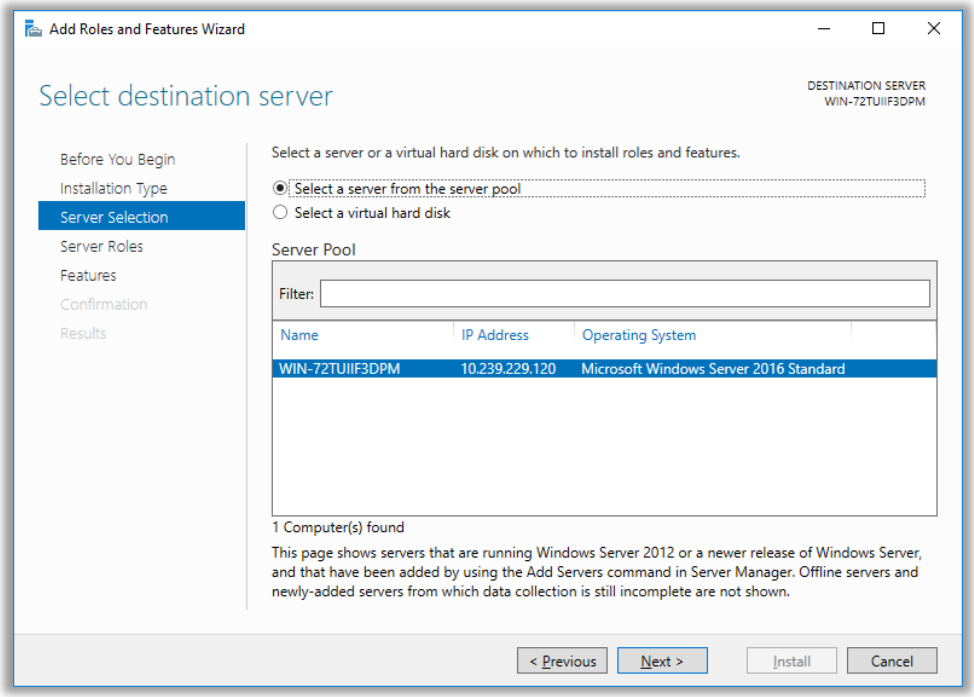
1. Go to: Server Manager > IIS.
2. Select the required server and right click. Next select '**Add Roles and Features'** from the list.



3. Navigate to the Installation Type page of the Wizard and select '**Role-based or feature-based installation'**.

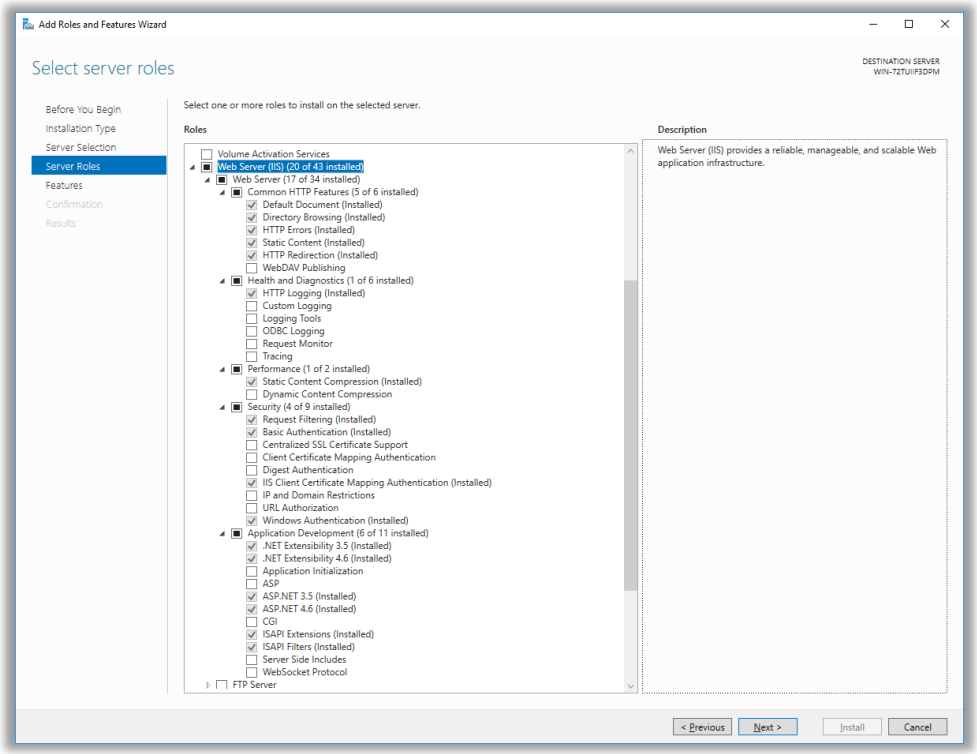


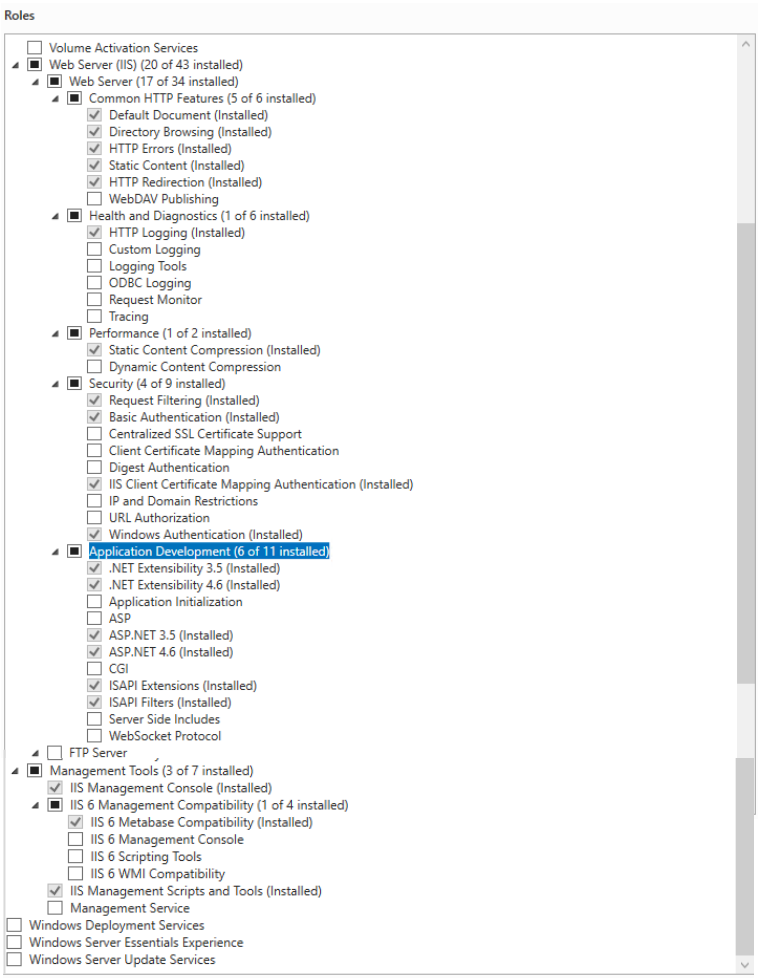
4. Click **Next** and then select the '**Select a server from the server pool'** option from the Server Selection page.



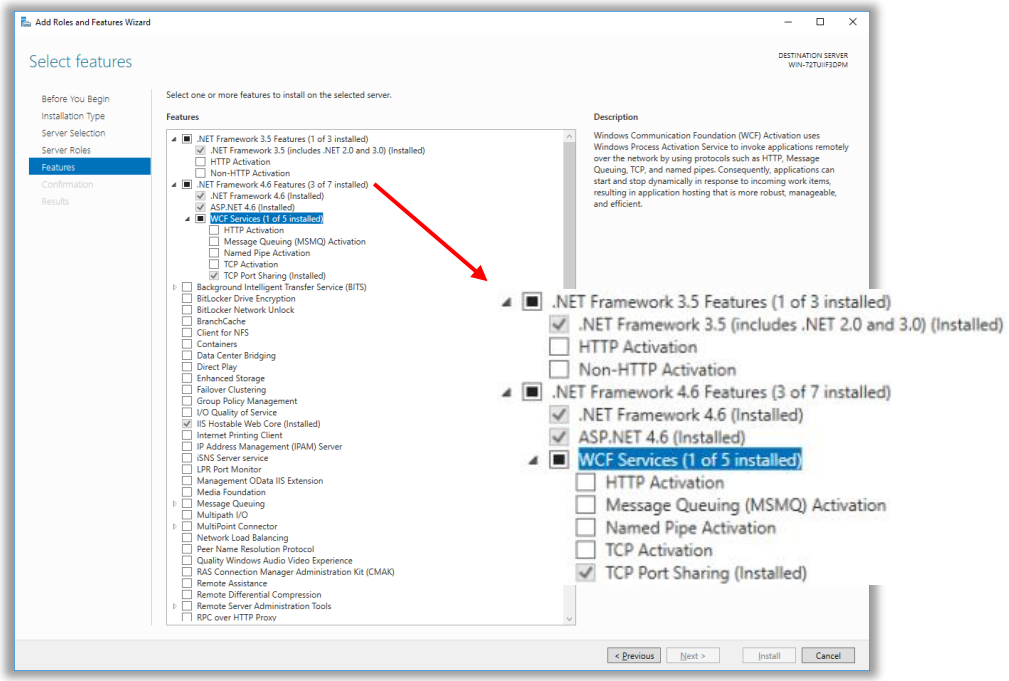
5. Select the required server from, the list and click **Next**.

6. From the Server Roles page click to expand '**Web Server (IIS)**'. From here select all the options that are ticked in the image below and the next page.





7. From the Features page click to expand **.NET Framework 3.5 and 4.5** Features and tick the boxes shown below.



8. Click **Next** and then **Install**.

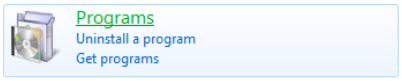
9. Please now refer to the Installation section.

2.2 WINDOWS 7

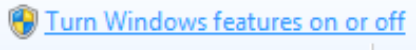
The following sections describe the steps required following a new installation of Windows 7, Windows 8 and Windows 10.

2.2.1 IIS

1. Open the Control Panel.
2. Select on Programs and Features.



3. Click on Turn Windows features on or off.



4. Expand all the options available under the 'Internet Information Services' feature and make sure all the tick boxes are ticked as shown below and then click OK.

NOTE: If any of the options listed below are already selected, do not turn them off.

A - Web Management Tools
IIS 6 Management Compatibility
- IIS 6 Management Console
- IIS Metabase and IIS 6 configuration compatibility
- IIS Management Console
- IIS Management Scripts and Tools

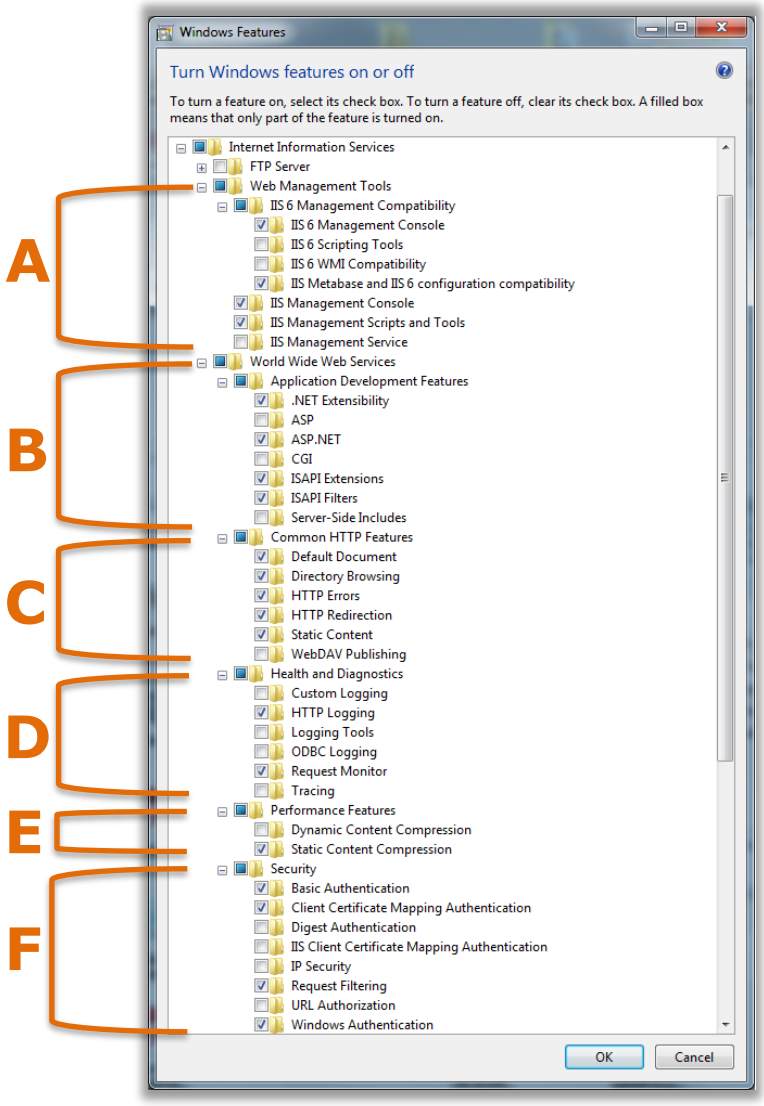
B - WWW Services
Application Development Features
- .NET Extensibility (.NET Extensibility 3.5 & .NET Extensibility 4.5 on Windows 8)
- ASP.NET (ASP.NET 3.5 & ASP.NET 4.5 on Windows 8)
- ISAPI Extensions
- ISAPI Filters

C - Common HTTP Features
- Default Document
- Directory Browsing
- HTTP Errors
- HTTP Redirection
- Static Content

D - Heath & Diagnostics
- HTTP Logging
- Request Monitor

E - Performance Features
- Static Content Compression

F - Security
- Basic Authentication
- Client Certificate Mapping Authentication
- Request Filtering
- Windows Authentication



5. Please now refer to the Installation section.

2.3 WINDOWS 8.1

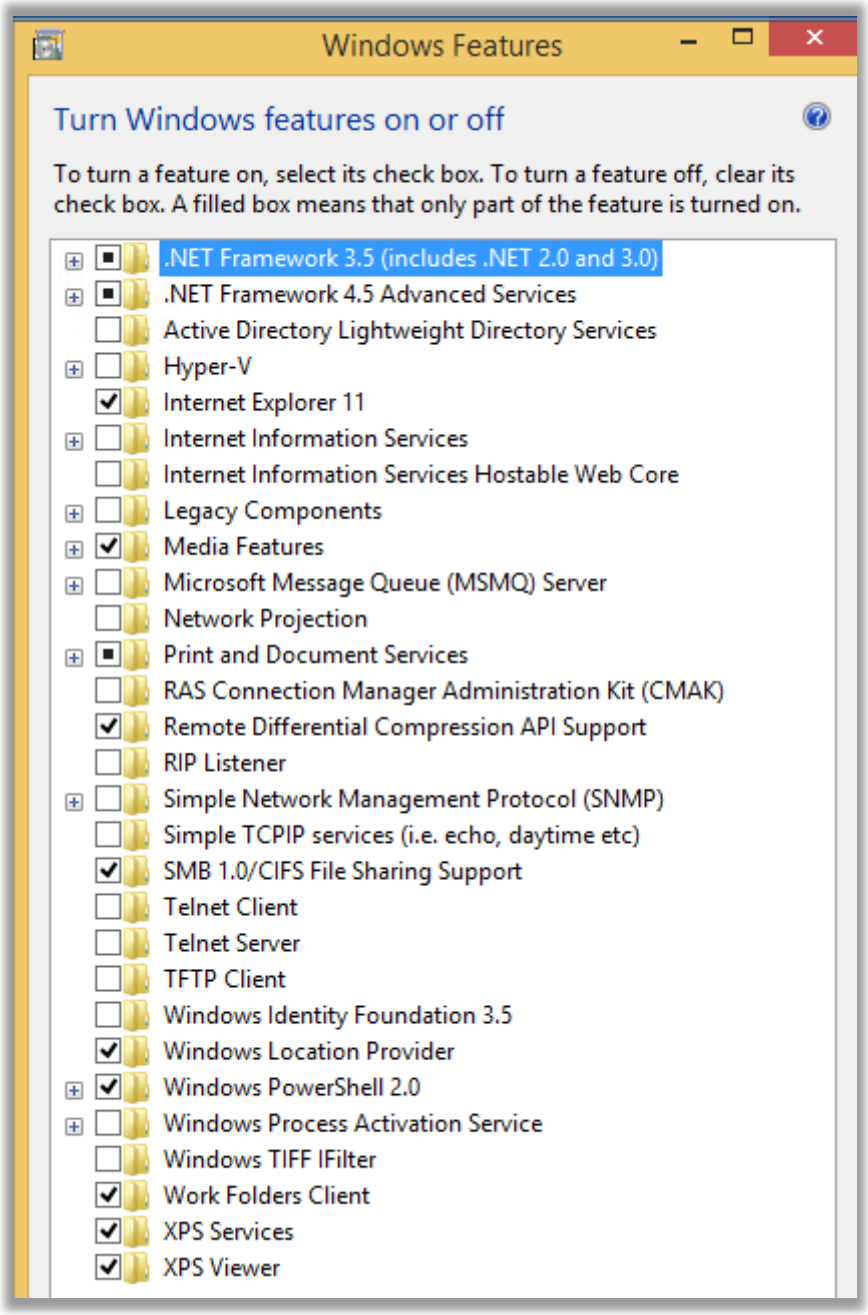
This section describes the steps required following a new installation of Windows 8.1.

2.3.1 IIS

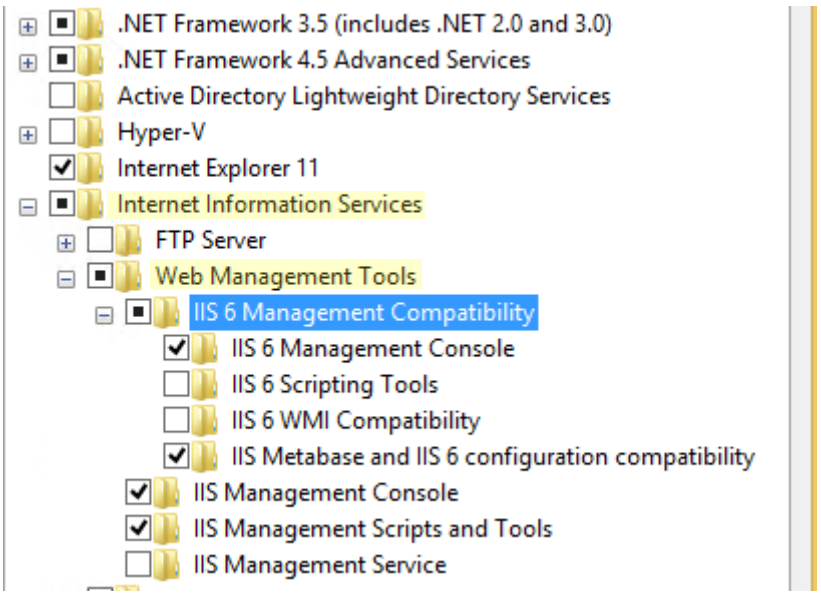
1. Go to: Control Panel > Programs and Features > Turn Windows Features On or Off.
2. Expand and select all of the options shown in the images below.

NOTE: If any of the options listed below are already selected, do not turn them off.

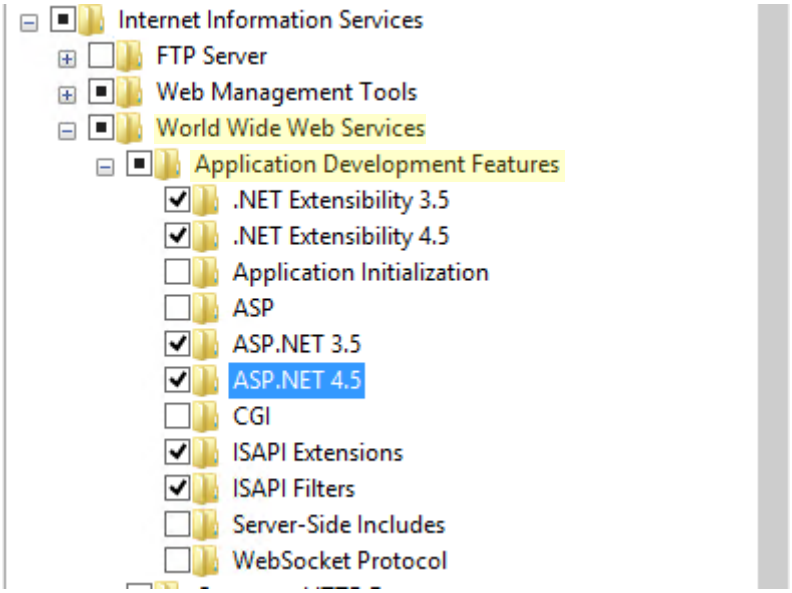
3. Tick **.NET Framework 3.5**.



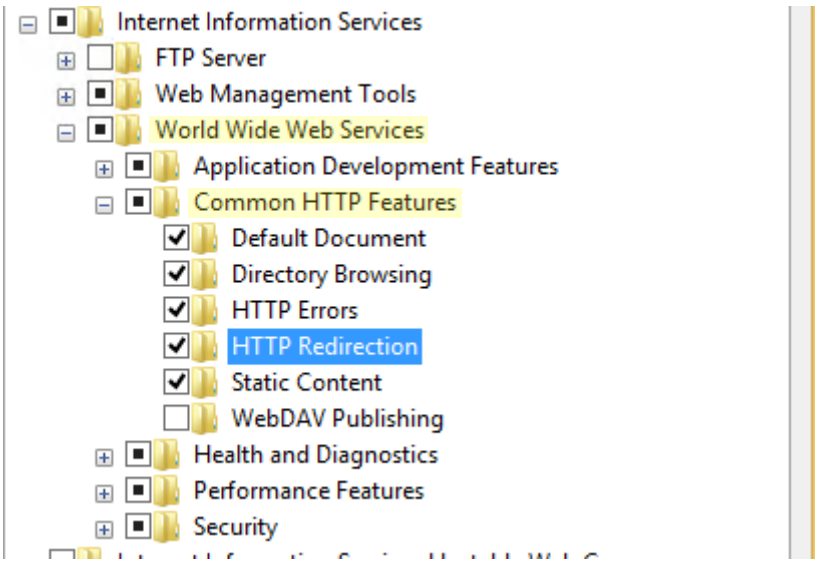
4. Expand '**Internet Information Services**', '**Web Management Tools**', '**IIS 6 Management Compatibility**' and then tick the features as shown below.



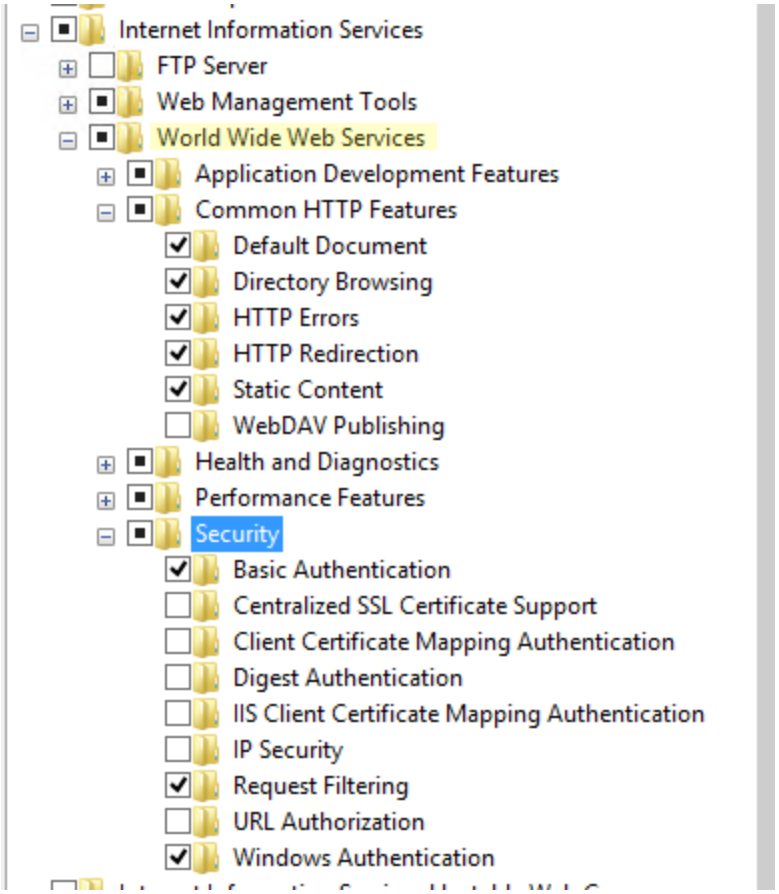
5. Expand '**World Wide Web Services**' and '**Application Development Features**' and then tick the features as shown below.



6. Expand '**World Wide Web Services**' and '**Common HTTP Features**' and then tick the boxes as shown below.



7. Expand '**World Wide Web Services**' and '**Security**' and then tick the boxes as shown below.



8. Please now refer to the installation section.

2.4 WINDOWS 10

This section describes the steps required following a new installation of Windows 10

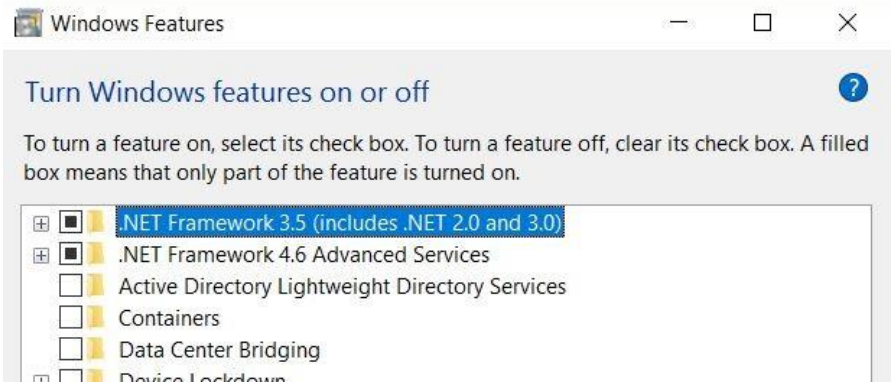
2.4.1 IIS

9. Go to: Control Panel > Programs and Features > Turn Windows Features On or Off.

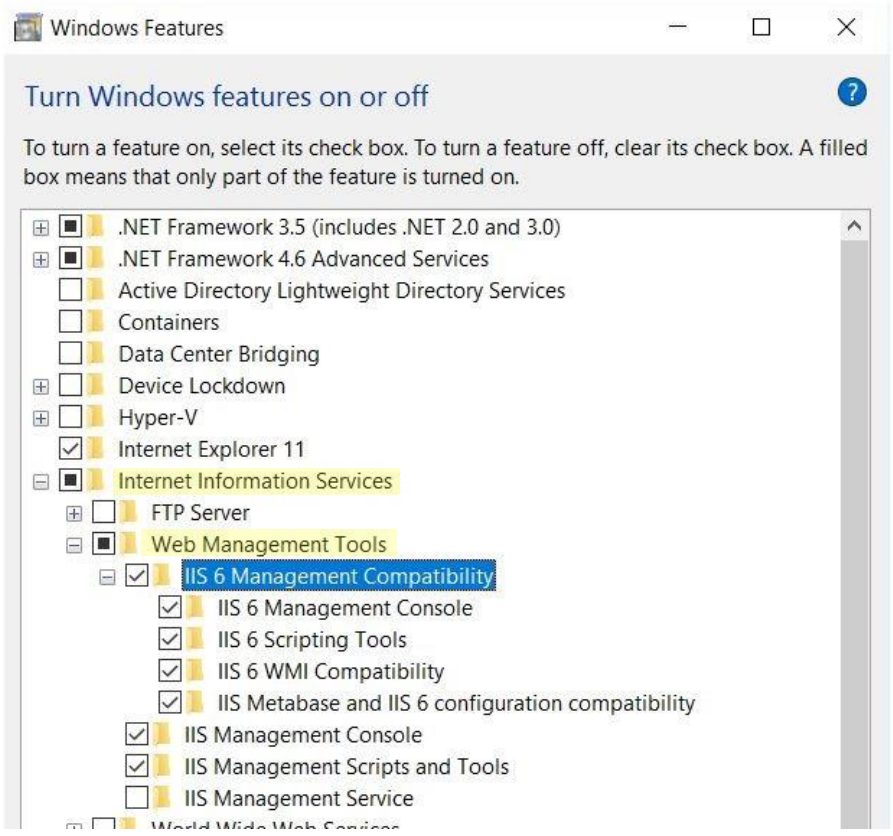
10. Expand and select all of the options shown in the images below.

NOTE: If any of the options listed below are already selected, do not turn them off.

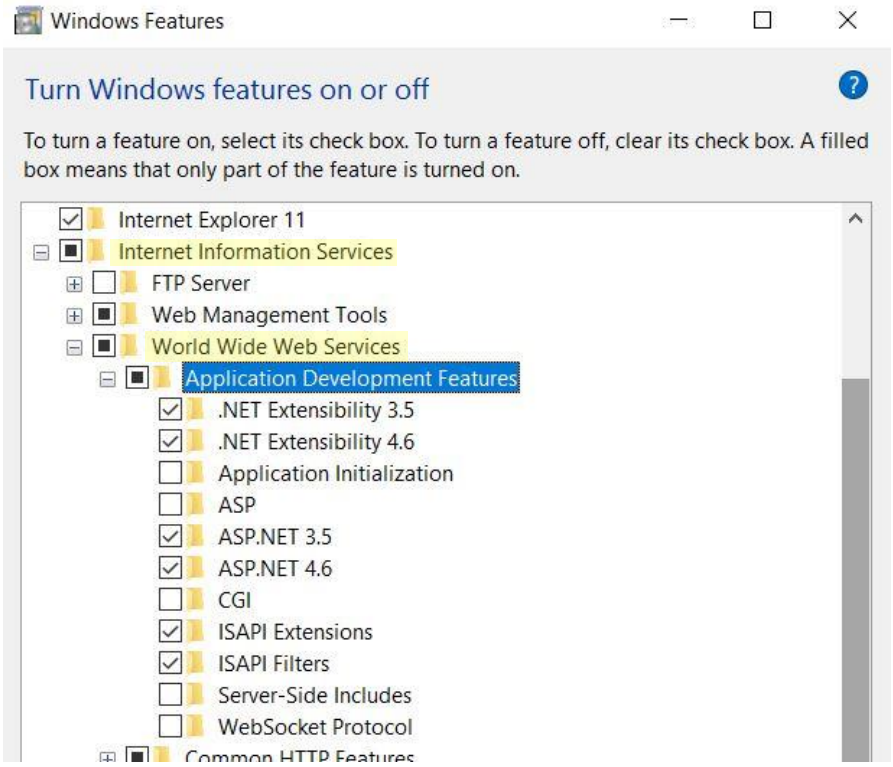
11. Tick **.NET Framework 3.5**.



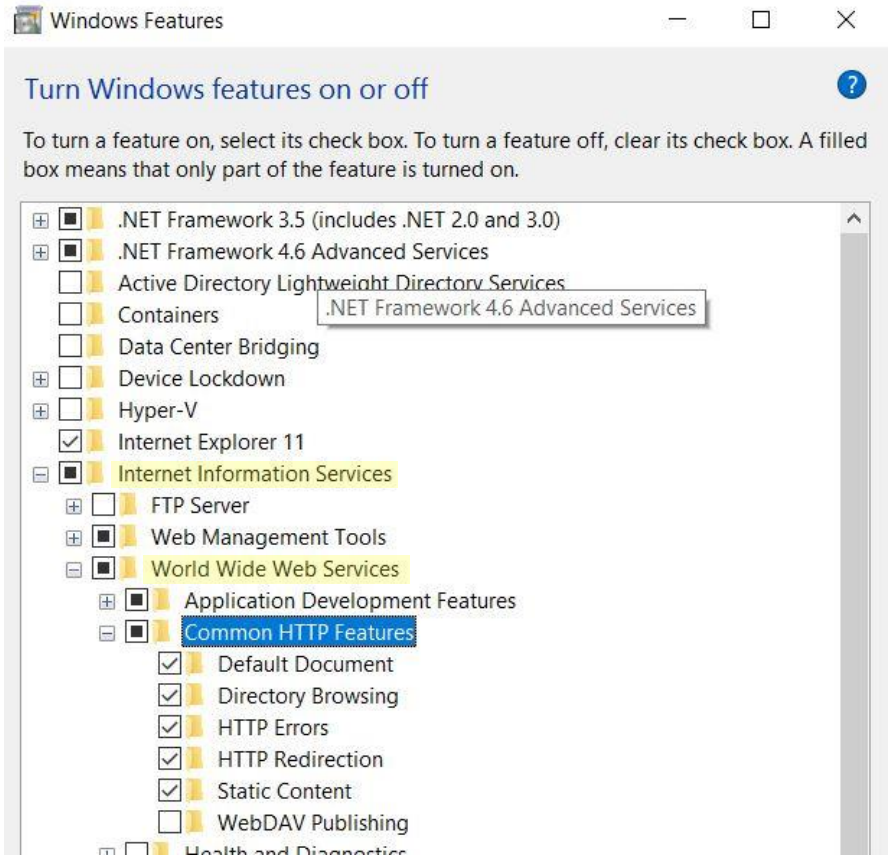
1. Expand '**Internet Information Services**', '**Web Management Tools**', '**IIS 6 Management Compatibility**' and then tick the features as shown below.



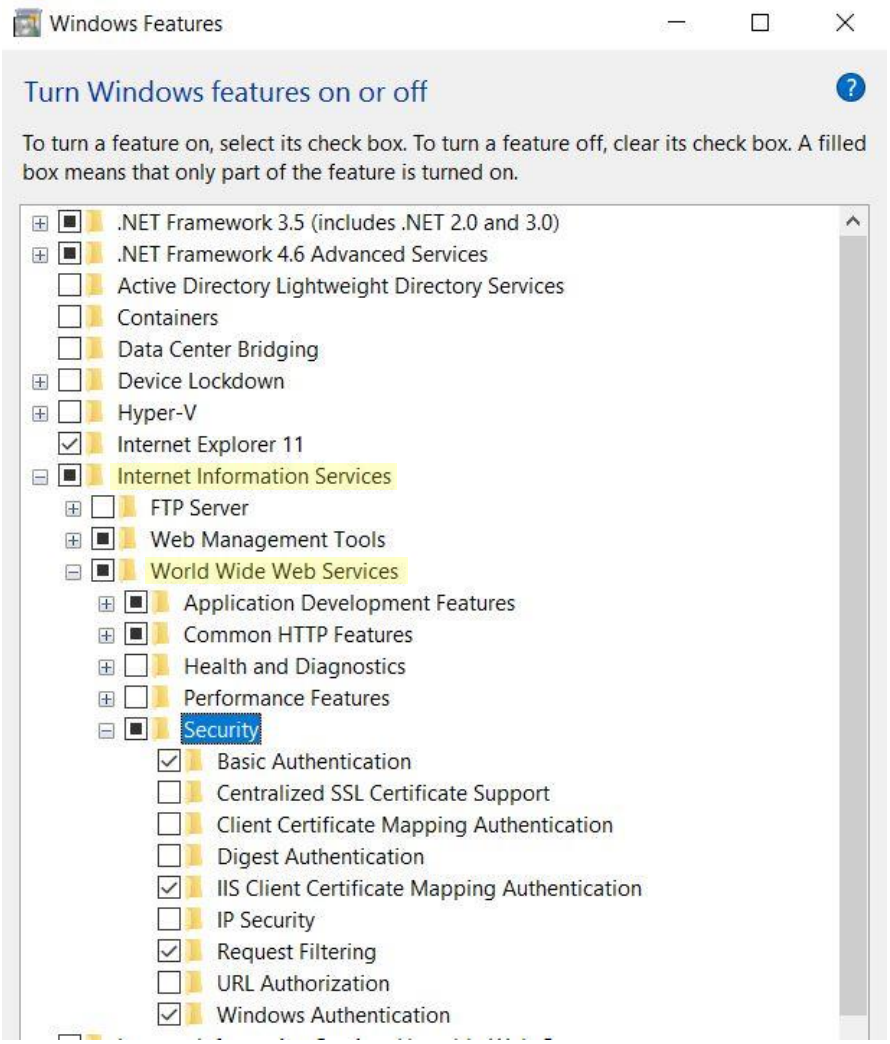
2. Expand '**Internet Information Services**', '**World Wide Web Services**' and '**Application Development Features**' and then tick the features as shown below.



3. Expand '**Internet Information Services**', '**World Wide Web Services**' and '**Common HTTP Features**' and then tick the boxes as shown below.



4. Expand '**Internet Information Services**', '**World Wide Web Services**' and '**Security**' and then tick the boxes as shown below.



5. Please now refer to the installation section.

2.5 TROUBLESHOOTING

2.5.1 ERROR 0X800F0906 WITH WINDOWS 8

NOTE: Follow this procedure only if you encountered Error 0x800F0906 during the installation of Microsoft.NET on Windows 8. Otherwise proceed to the next step.

1. Run '**gpedit.msc**'.
2. Open Computer Configuration\Administrative Templates and select System.
3. In the right panel, scroll down until you see 'Specify settings for optional installation and component repair'.
4. Right-click and edit this option.
5. Select the 'Enabled' radio button.

Tick the box for 'Contact Windows Update directly to download repair content instead of Windows Server Update Services'.

3. INSTALLING TRAKA WEB COMPONENTS

This section describes how to install each of the components of the system. This section should be read after ensuring that all the prerequisites have been met, see section **2** above.

3.1 WEB FRONT END SECURITY CERTIFICATE INSTALLATION

To install the required security certificates for the Traka Web Front End to enable it to communicate securely with the Traka Business Engine.

NOTE: It is recommended that you only install security certificates that apply to the version of Traka Web that you wish to install. If you are upgrading to a later version, uninstall the existing certificates and install the versions applicable to the upgrade.

NOTE: Please also install the security certificates first before the relevant software described below.

1. Obtain the Traka Web Front End Certificates.msi installation file from the Traka Support Web Site http://support.traka.com and save it to the server that now has the Traka Web Front end installed.

2. Run this file and follow the onscreen instructions to install the required security certificates.

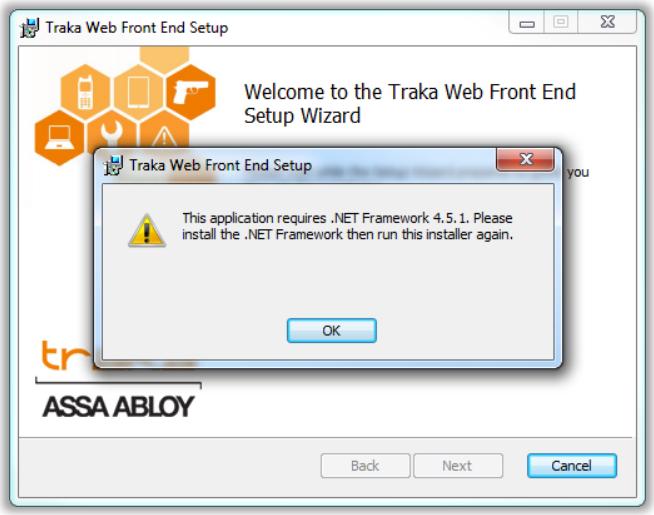
3.2 WEB FRONT END INSTALLATION

The following section describes how to install the Traka Web Front end using the MSI installation file provided by Traka.

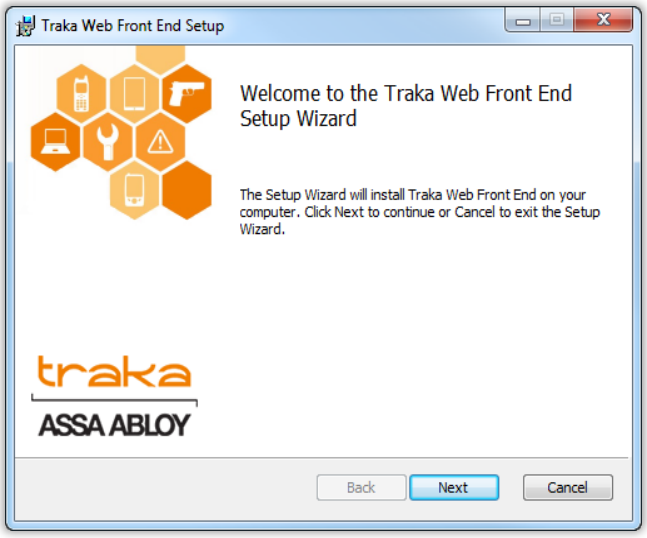
1. Obtain the Traka Web Front End MSI installation file from the Traka Web Support site at http://support.traka.com and save it to the Web server where you wish to install Traka Web Front End.

2. Run the file and following the instructions below. If any of the prerequisites that are required for Traka Web are missing, then an appropriate message will be displayed, please follow section 2 of this manual for the set-up of the operating system specific prerequisites.

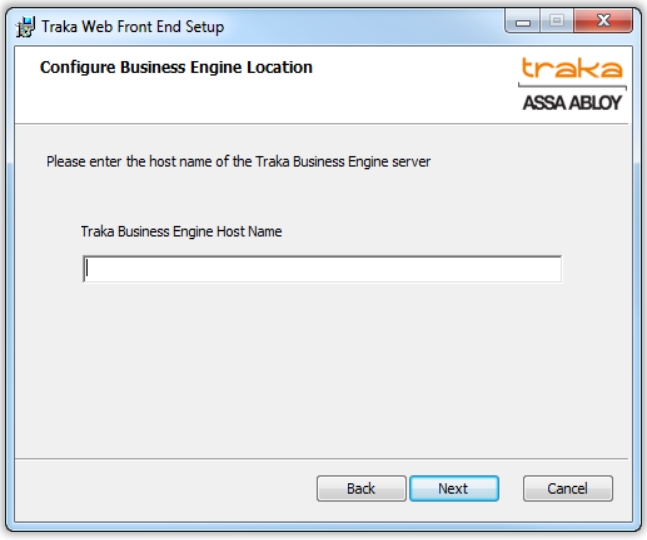
3. The Traka Web Installer may also prompt you that it needs to enable ASP.NET v4.5.1 since this is not installed by default. See picture below:



4. Once installed your Traka Web Front End is now setup and you should be able to browse to the Traka Web login page at http://*servername*/TrakaWeb/. You will not be able to login to the Traka Web Front End until your Business Engine is installed, configured and available on the network, which is described in the following sections.

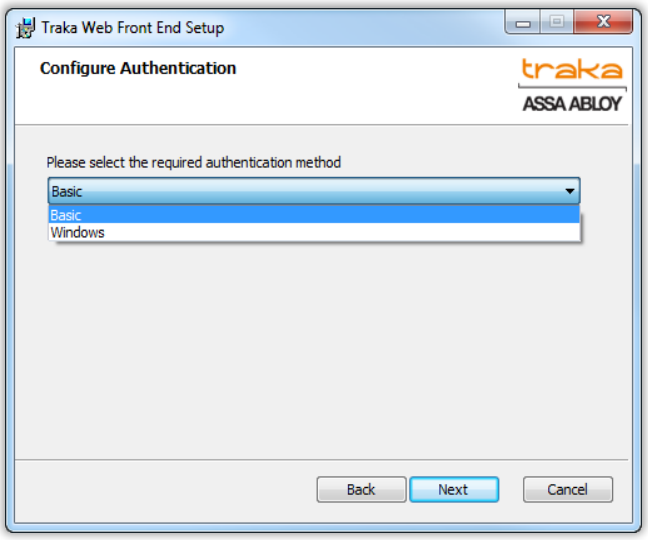


1. Click **Next** and accept the **'End-User License Agreement'** on the next screen to continue.



5. Enter your Traka Business Engine host name (computer name). This should be the name of the Windows Server where your Traka Business Engine is installed.

6. Click **Next**.

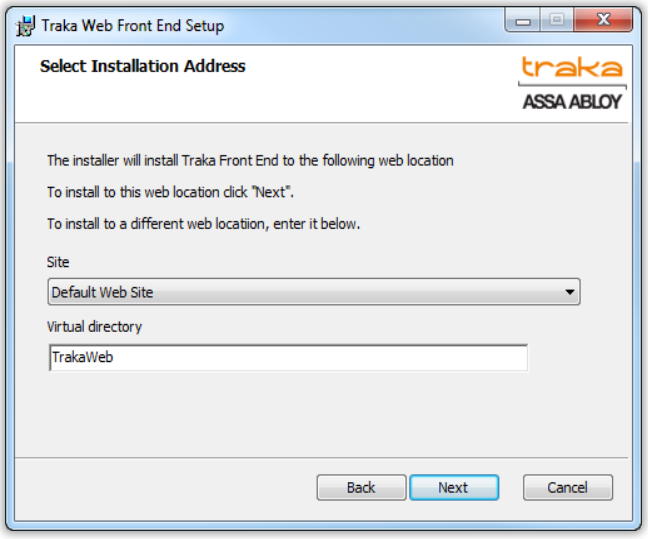


7. Select Basic Authentication or Windows Authentication. More information of which one you should choose can be found in **section 6**, Authentication Options. If you are unsure, choose Basic Authentication.

NOTE: If you choose the Windows Authentication option, the IIS server is configured automatically.

If you have completed the installation using Basic Authentication, it is possible to change the configuration to Windows Authentication through the Internet Information Services (IIS). For more information on this process, refer to **section 6.2**.

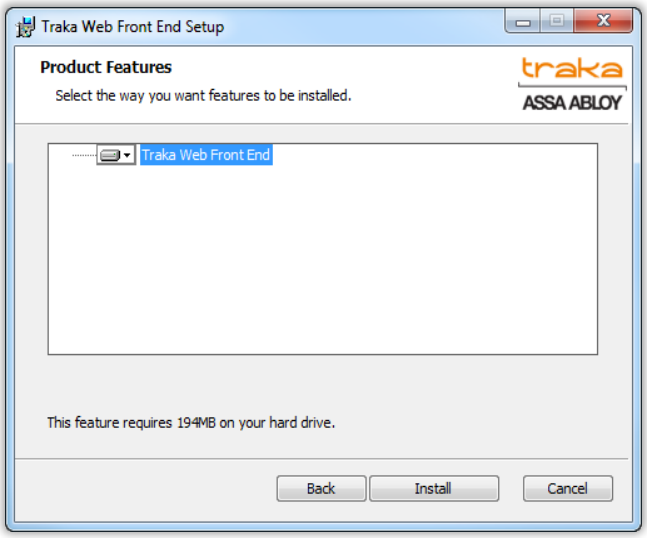
8. Click **Next**.



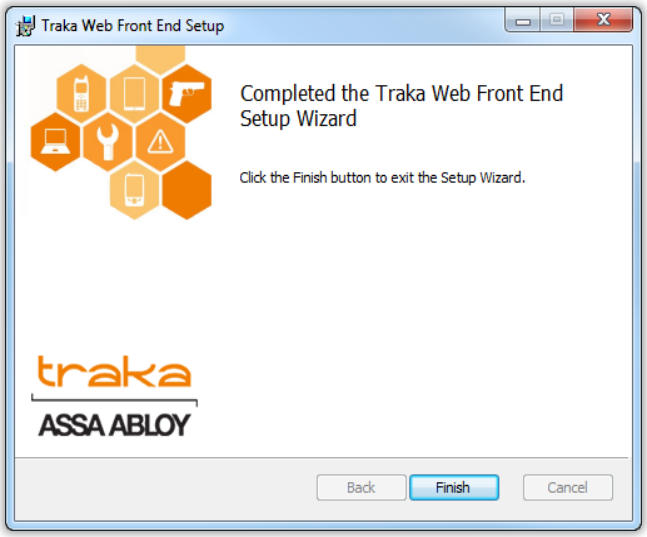
9. Choose the Web Site instance that Traka Web will installed into, optionally specify the virtual directory name if you do not wish to use the default value of 'TrakaWeb'. This virtual directory name will form part of the URL for accessing Traka Web, e.g. if your Web Site URL is www.myintranet.com, the URL to your installation of Traka Web will be www.myintranet.com/TrakaWeb.

10. Click **Next** to continue.

NOTE: The Application pool "TrakaWebPool" will automatically be created by the installer with the correct settings required to run the Traka Web Front End Web Site.



11. Select **Install** to continue with the installation.



12. Once the installation is complete the window can be closed by selecting **Finish**.

13. If you require the Traka Web website to default to a language other than English (UK), you should modify the XML Configuration file 'web.config' file located in the folder: c:\inetpub\wwwroot\trakaweb\

    a. Take a copy of the file in case you make any mistakes. (Optional)
    b. Open the 'web.config' file using a text editor.
    c. Locate the 'DefaultCulture' appSettings key.

    d. Modify the 'value' from 'en-GB' according to desired language from the supported languages table below:
    e. Save changes made to the file and navigate to the Traka Web URL.

Language code	Language name	Note
en-GB	English (GB)	
en-US	English (US)	
ar-AE	Arabic	
zh-TW	Chinese	
cs-CZ	Czech	
da-DK	Danish	
nl-NL	Dutch	
fi-FI	Finnish	
fr-FR	French	
de-DE	German	
el-GR	Greek	
he-IL	Hebrew	
hu-HU	Hungarian	
it-IT	Italian	
ja-JP	Japanese	
ko-KR	Korean	
lt-LT	Lithuanian	
nb-NO	Norwegian-Bokmal	
pt-PT	Portuguese	
ro-RO	Romanian	
ru-RU	Russian	
pl-PL	Polish	
sk-SK	Slovak	
sl-SL	Slovenian	
es-ES	Spanish	
sv-SE	Swedish	
tr-TR	Turkish	

3.3 BUSINESS ENGINE SECURITY CERTIFICATE INSTALLATION

To install the required security certificates for the Traka Business Engine to enable the Business Engine to communicate securely with the Traka Comms Engine and Traka Web Front End.

NOTE: It is recommended that you only install security certificates first that apply to the version of Traka Web that you wish to install. If you are upgrading to a later version, uninstall the existing certificates and install the versions applicable to the upgrade.

NOTE: Please also install the security certificates first before the relevant software described below.

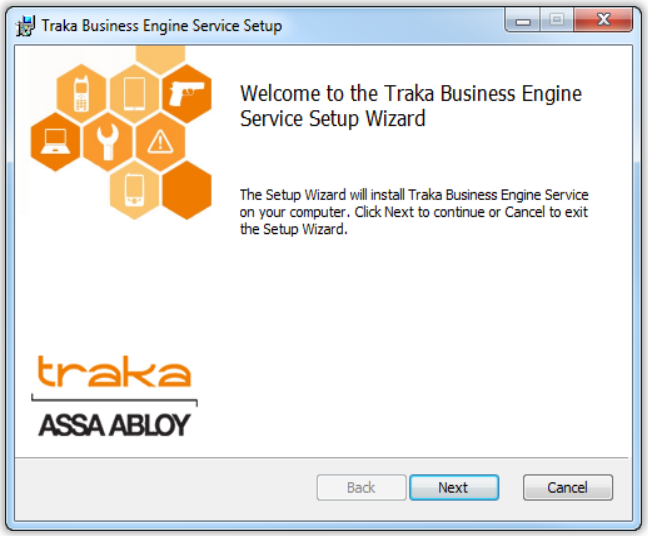
1. Obtain the Traka Business Engine Certificates.msi installation file from the Traka Support Web Site http://support.traka.com and save it to the server that now has the Traka Business Engine installed.

2. Run this file and the required security certificates will be installed.

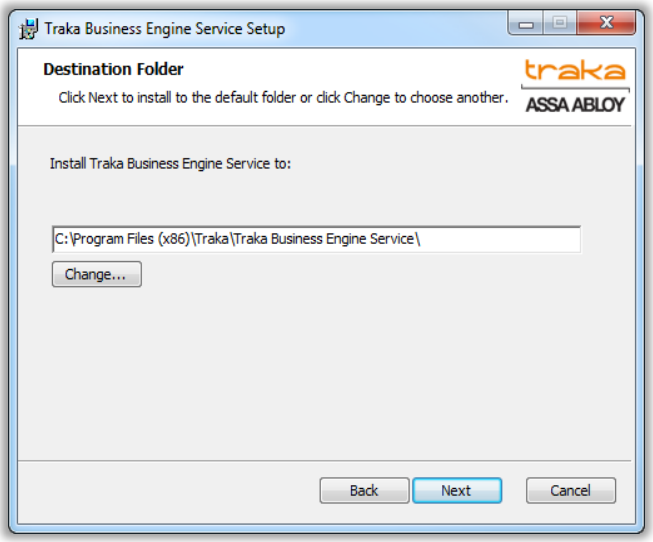
3.4 BUSINESS ENGINE SERVICE INSTALLATION

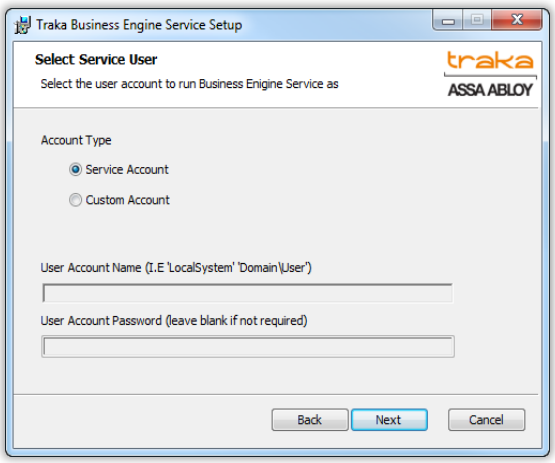
1. Obtain the Traka Business Engine Service MSI installation file from the Traka Support Web Site http://support.traka.com and save it to the server where you wish to install Traka Business Engine Service.

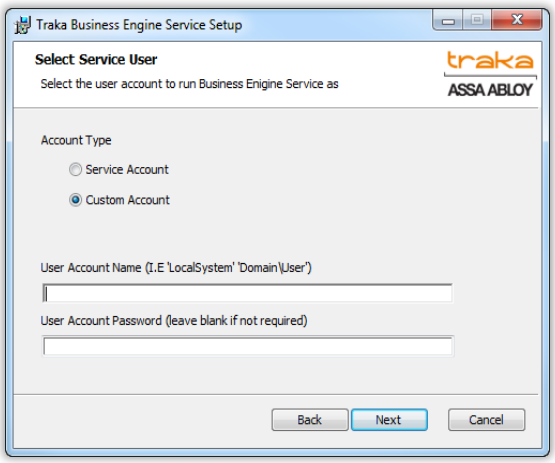
2. Run the file and follow the instructions below:



3. Click **Next** and accept the **'End-User License Agreement'** on the next screen to continue.

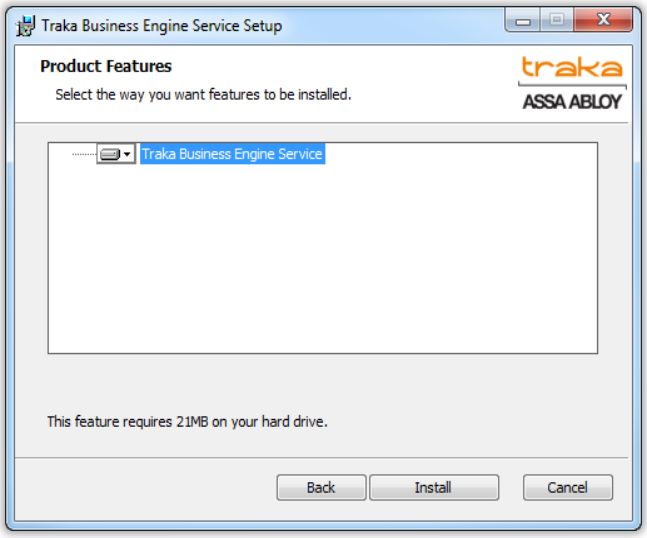




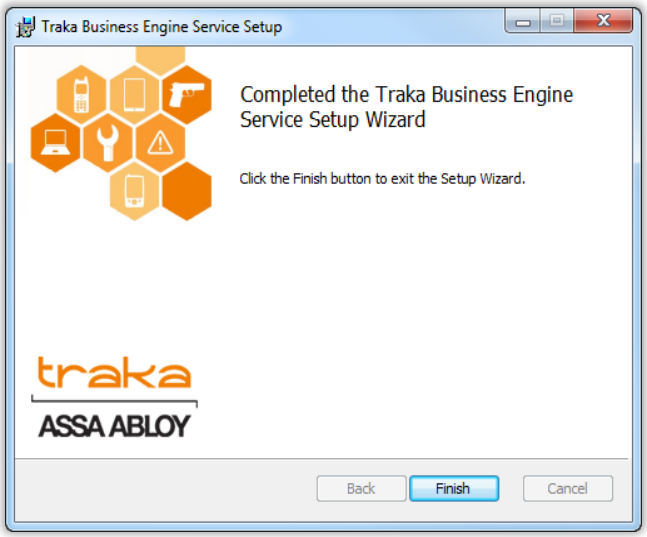


4. Select where you would like to install the Traka Business Engine followed by **Next**.

5. Select the Account Type User Account to run the Business Engine Service as followed by **Next**.



6. Select **Install** to continue with the installation.



7. Select **Finish** to complete the Business Engine installation.

3.5 COMMUNICATION ENGINE SECURITY CERTIFICATE INSTALLATION

To install the required security certificates for the Traka Comms Engine to enable the Traka Comms Engine to communicate securely with the Traka Business Engine and Traka Touch.

NOTE: It is recommended that you only install security certificates that apply to the version of Traka Web that you wish to install. If you are upgrading to a later version, uninstall the existing certificates and install the versions applicable to the upgrade.

NOTE: Please also install the security certificates first before the relevant software described below.

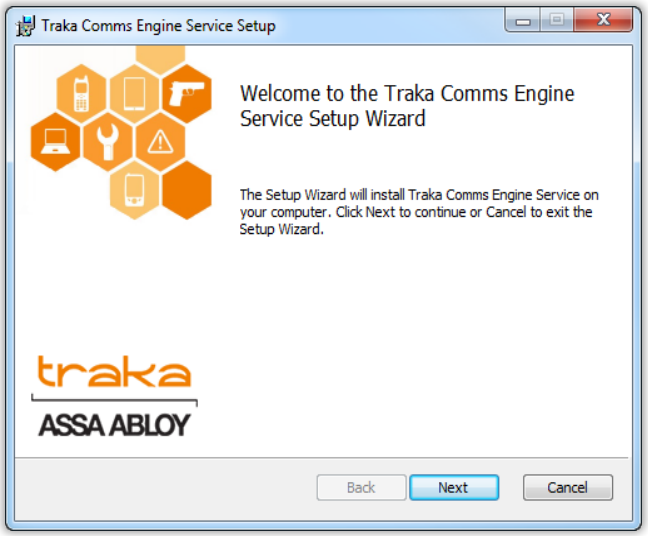
1. Obtain the Traka Comms Engine Certificates.msi installation file from the Traka Support Web Site http://support.traka.com and save it to the server that now has the Traka Comms Engine installed.

2. Run this file and the required security certificates will be installed.

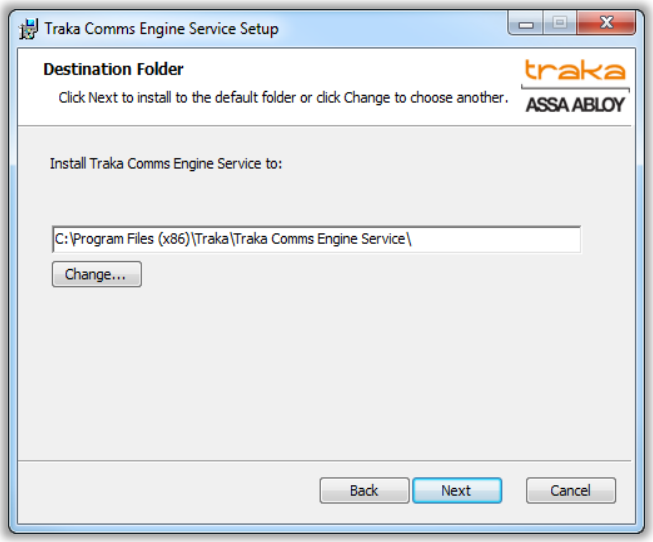
3.6 COMMUNICATION ENGINE SERVICE INSTALLATION

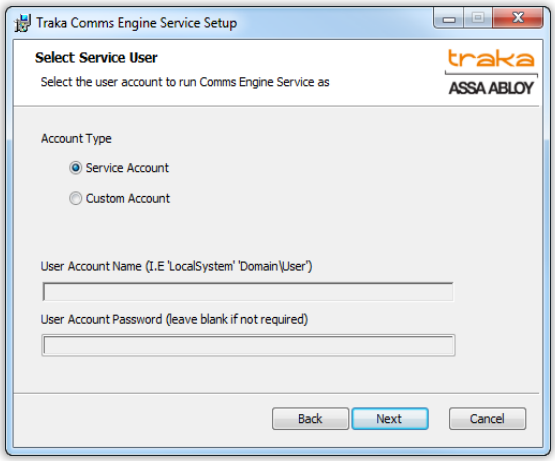
1. Obtain the Traka Comms Engine MSI installation file from the Traka Support Web Site http://support.traka.com and save it to the server where you wish to install the Traka Comms Engine.

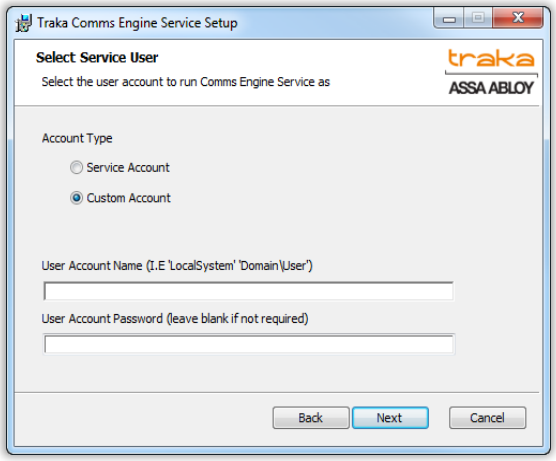
2. Run the file and follow the instructions below:



3. Click **Next** and accept the **'End-User License Agreement'** on the next screen to continue.

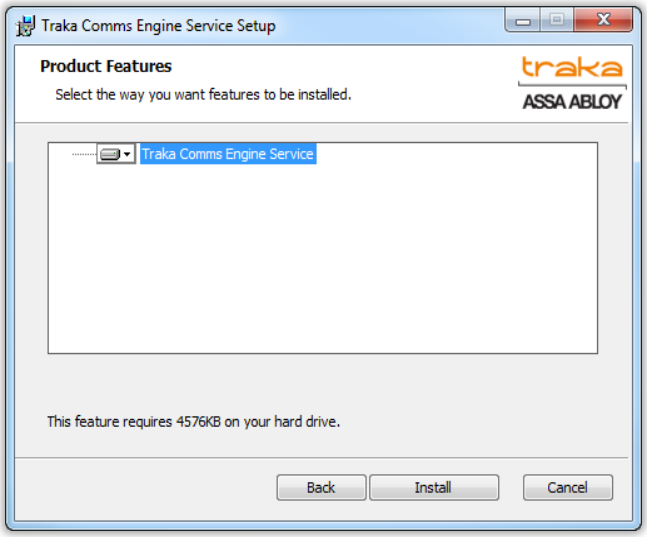




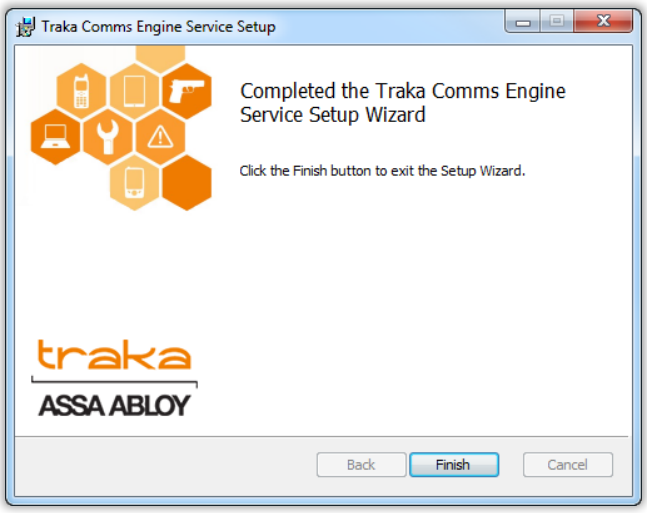


4. Select where you would like to install the Traka Comms Engine followed by **Next**.

5. Select the Account Type User Account to run the Comms Engine Service as followed by **Next**.



6. Select **Install** to continue with the installation.



7. Select **Finish** to complete the Business Engine installation.

3.7 ADMIN APPLICATION CERTIFICATE INSTALLATION

It is normally expected that the Admin Application will be run from the same server that is running the Business Engine, although it is possible that the Admin Application can be run from another computer. If the Admin Application will be run from another computer it will require the security certificates to be installed on that computer.

NOTE: It is recommended that you only install security certificates that apply to the version of Traka Web that you wish to install. If you are upgrading to a later version, uninstall the existing certificates and install the versions applicable to the upgrade.

NOTE: Please also install the security certificates first before the relevant software described below.

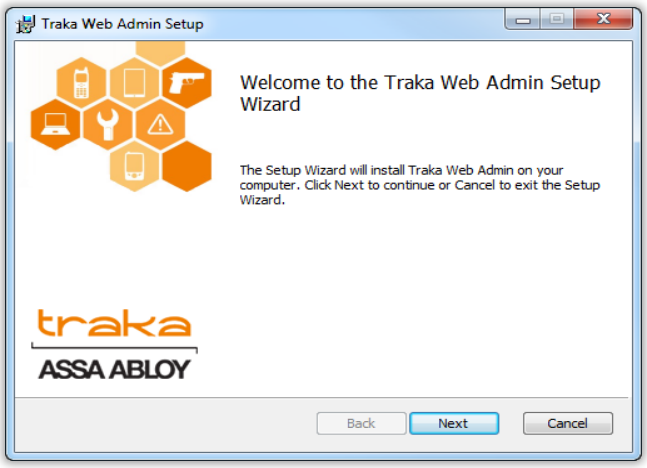
1. Obtain the Traka Business Engine Certificates.msi installation file from the Traka Support Web Site http://support.traka.com and save it to the server that now has the Traka Admin Application installed.

2. Run this file and the required security certificates will be installed.

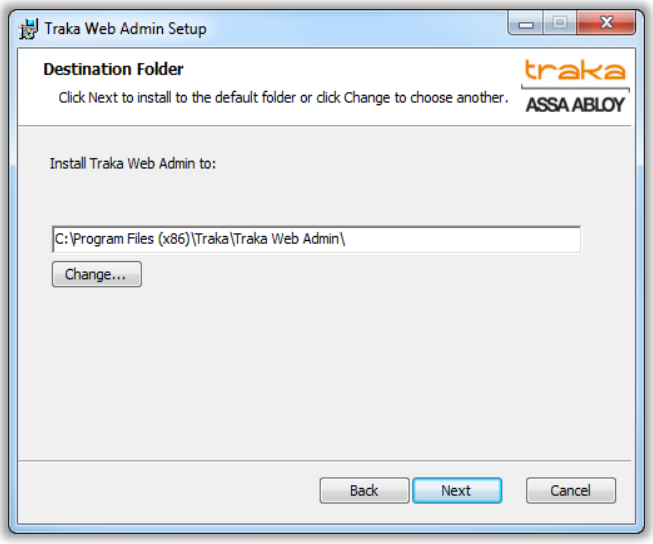
3.8 ADMIN APPLICATION

1. Obtain the Traka Web Admin Application MSI installation file from the Traka Support Web Site http://support.traka.com and save it to the server where you wish to install the Traka Web Admin Application.

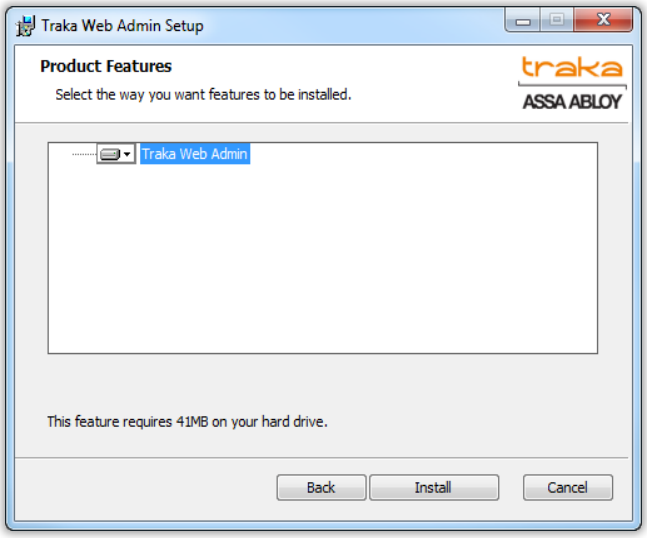
2. Run the file and follow the instructions below:



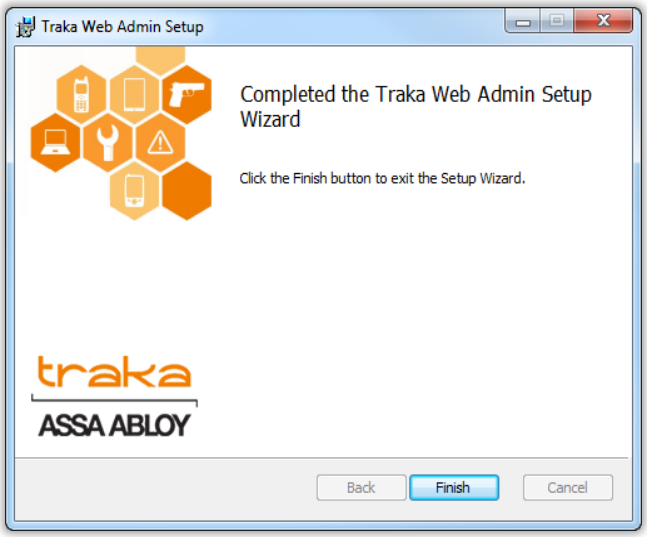
1. Click **Next** and accept the **'End-User License Agreement'** on the next screen to continue.



3. Select where you would like to install the Traka Web Admin followed by **Next**.



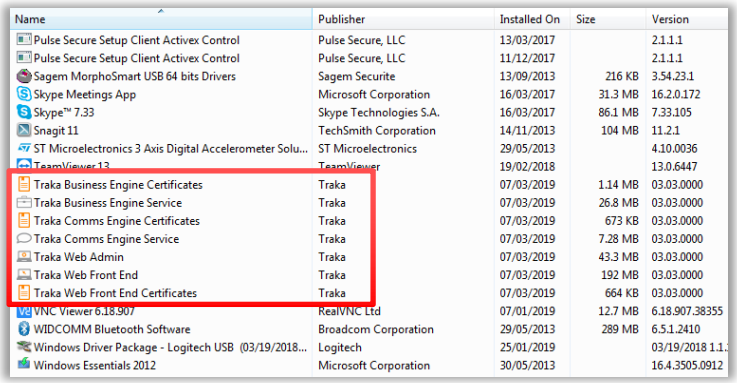
4. Select the way you want features to be installed followed by **Install.**



5. Select **Finish** to complete the installation.

3.9 CONFIRMING ALL SOFTWARE COMPONENTS ARE INSTALLED

This step simply shows you how to confirm that all the software components and their certificates have been correctly installed. Go to: Control Panel > Programs and Features



3.10 DATABASE

This document does not cover installation of the database server. Please refer to the database vendor's installation guidance notes. The configuration section below will provide details on how to connect and create a database with the database server via the Traka Web Admin utility.

Please note that the database authentication mode may be configured to **'Windows Authentication Mode or SQL Server'** (Mixed mode authentication) or **'Windows Authentication Mode'**. Guidance is provided in Section 5 in relation to how to configure the Business Engine Service to authenticate with the SQL Server, depending on the authentication mode selected. If you are not sure which mode to select, use mixed mode authentication.

3.10.1 SQL SERVER TIPS AND TRICKS

The Traka Business Engine relies on an operational Database to function. Below are a series of checks that should be made to ensure a trouble free installation.

3.10.1.1 SERVER TIME

An important factor is the Database Server and Business Engine Server's time synchronisation.

If the server time is out by more than 5 seconds, a warning will be present in the Business Engine logs. You should ensure wherever possible when the Business Engine and Database Server are installed on different machines that the servers are joined to domain or you use an NTP Server.

3.10.1.2 SQL SERVER MEMORY USAGE

In resource constrained environments, for example, where all Traka Web components are installed on the same machine, or installations where Traka Web is the only database installed on a SQL Express instance, it may be necessary to limit the amount of memory available to the SQL Server Database to ensure that SQL Server does not take too much memory resource away from other Applications.

Whilst there is no right or wrong answer, in the scenario where the SQL Database, Business Engine, Comms Engine and Traka Support Web Site are installed to the same server, which has only 4GB of RAM available, it is recommended that you limit the memory allocation.

Please see the following articles for further information:

http://msdn.microsoft.com/en-us/library/ms178067.aspx

3.10.1.3 SQL RECOVERY MODEL

In certain Traka Web environments, where SQL Express is being used and the user is not familiar with SQL Server administration, Traka recommends that you set the database recovery model to **'Simple'**. This mode limits the amount of disk space used by SQL Server, by disabling the 'transaction log'.

The following article discusses the various pros and cons of the available SQL recovery models:

http://msdn.microsoft.com/en-us/library/ms189275.aspx

The article below describes how to change the recovery model:

http://msdn.microsoft.com/en-us/library/ms189272.aspx

3.11 FIREWALL CONSIDERATIONS

Where a firewall is being used, the following port numbers should be opened to permit the various Traka Web components to communicate effectively:

From	To	Protocol	Destination Port
Business Engine	SQL Server	TCP	1433
Business Engine	Comms Engine	TCP	9997
Comms Engine	Business Engine	TCP	10500, 10501, 10503
Comms Engine	Traka Touch	TCP	9998
Traka Touch	Comms Engine	TCP	10601
Admin Application	Business Engine	TCP	10500, 10501, 10503
Traka Web Front End	Business Engine	TCP	10500, 10501, 10503

4. CONFIGURATION

Once all the Traka Web components have been installed, the system must be configured using the Admin Application.

This configuration can only happen when the Business Engine Service has been started.

This is required because the Admin Application connects to the Business Engine in order to configure its settings.

The following sections will guide you through the entire configuration process to get Traka Web up and running.

4.1 CONFIGURING AND STARTING SERVICES

Check that the Business Engine Service and the Comms Engine Service have been started.

You can either run the Business Engine Service and Comms Engine Service under their default account identities (Local System), or run them under a specific Windows User account identity.

Both approaches are documented below in Sections 4.1.1 and 4.1.2. If you are unsure which option to choose, leave both services to run under their default identity (Section 4.1.1).

NOTE: If you intend for the Business Engine Service to authenticate to the SQL Server using Windows Authentication, then you must run the Business Engine Service under a specific Windows User account identity.

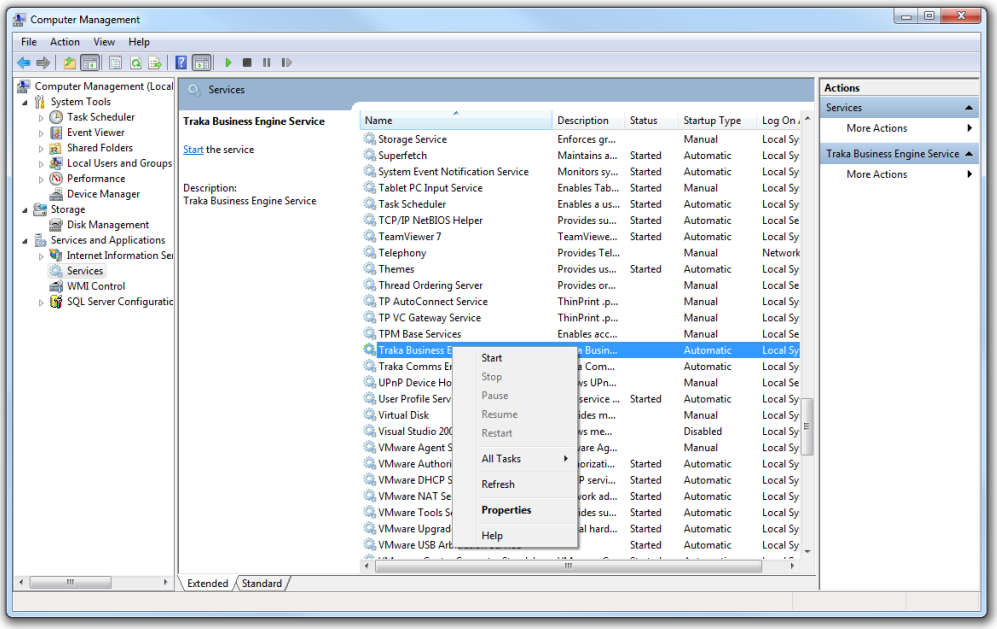
4.1.1 STARTING SERVICES USING LOCAL SYSTEM (DEFAULT)

1. Open the Computer Management window to access the services list. This can be found by typing **'Services'** into **'Search programs and files'**. Alternatively, go to Start -> Run and type **'services.msc'** then press **'OK'**.

2. In the list of services you will see the Traka Business Engine Service and the Traka Comms Engine Service.

NOTE: Depending on your configuration, these services may be installed on separate servers.

3. If the service has not been started then right click on 'Traka Business Engine' and choose **'Start'**.



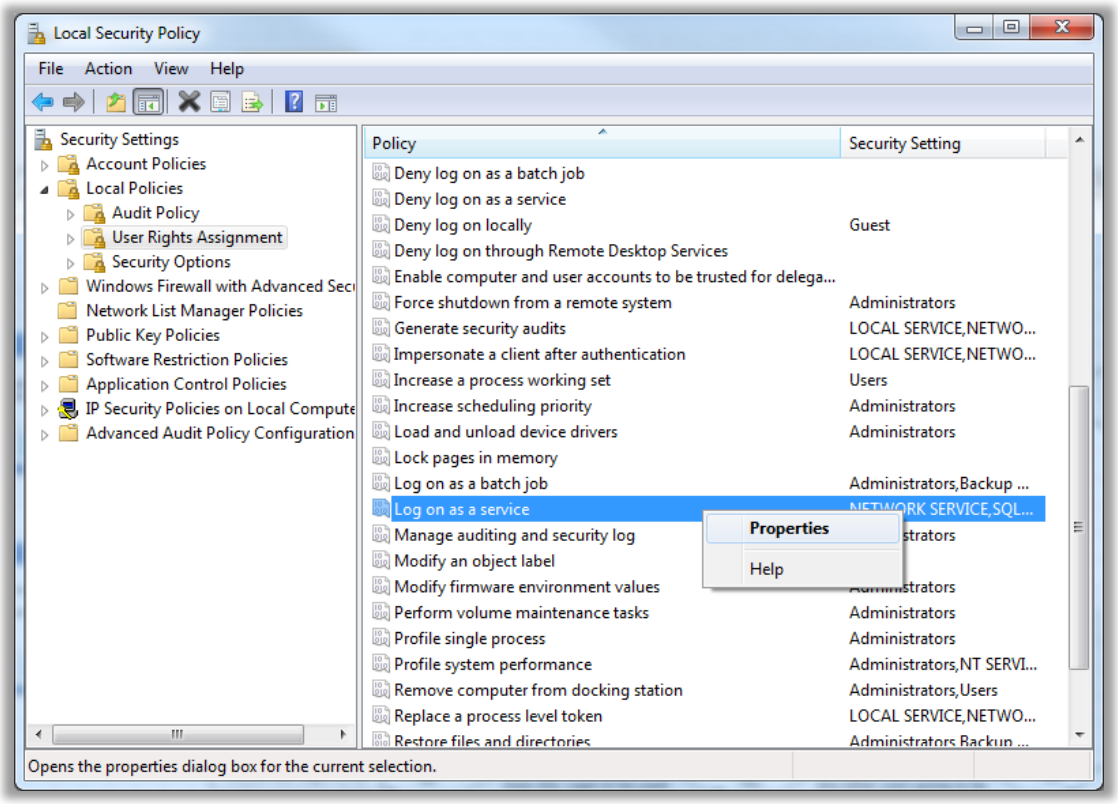
4. Perform the same with the 'Traka Comms Engine' if necessary.

4.1.2 STARTING SERVICES USING WINDOWS AUTHENTICATION

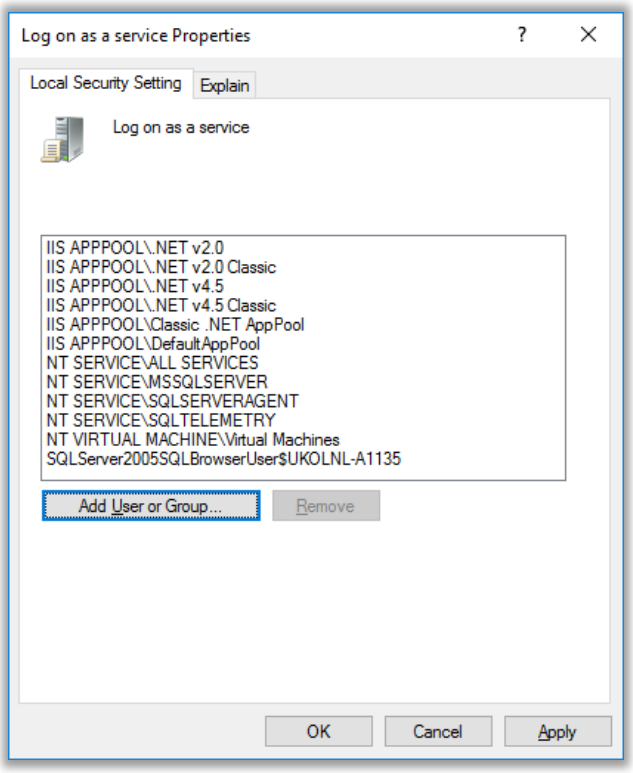
You may wish to run the Business Engine Service and Comms Engine Service using a Windows User identity.

NOTE: As discussed at the beginning of this section, this step is mandatory for the Business Engine Service if you wish the Business Engine to connect to the SQL Server using Windows Authentication. However, it is optional for the Comms Engine Service since it does not directly connect to the SQL database.

1. Open Local Security Policy, this can be located by typing **'Local Security'** into **'Search programs and files'.**
2. On the left navigation bar, navigate to **'Local Policies'** and then **'User Rights Assignment'**.
3. In the list of policies you will see the **'Logon as a service'**.
4. Right click on the policy and choose '**Properties'**.



5. From here you will be given the option to add the domain user to be used for running the Business Engine and/or Comms Engine Services.

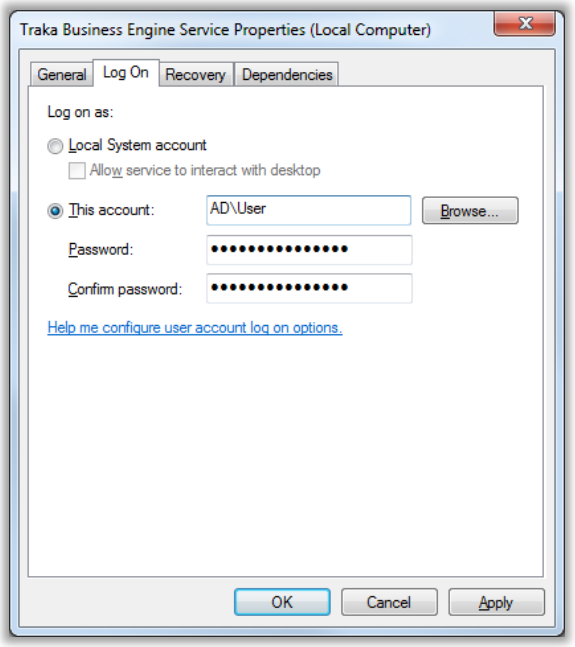


6. Next, open the Services program, this can be located by typing **'Services'** into **'Search programs and files'**.

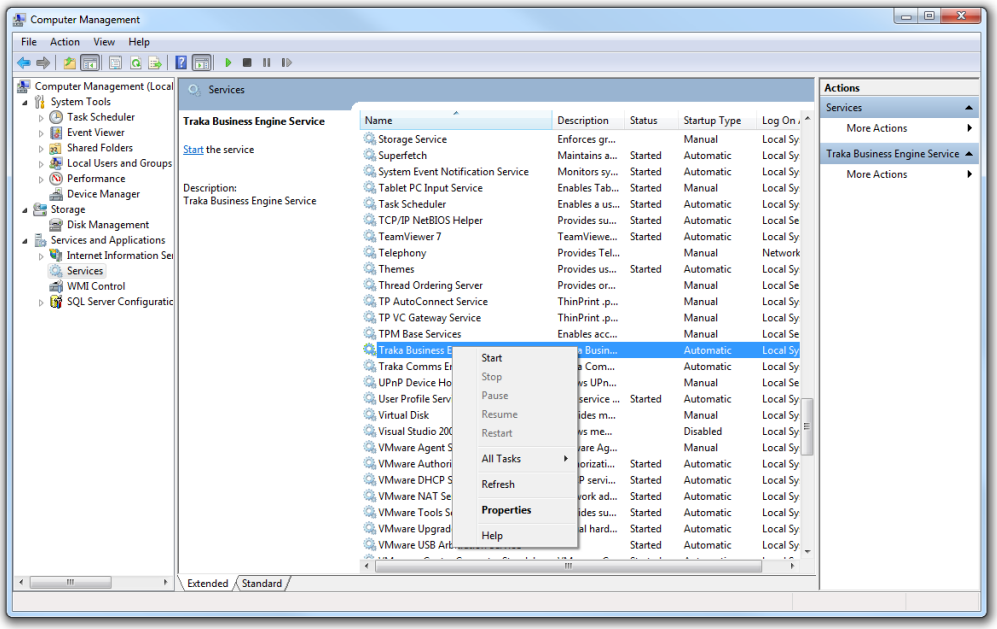
7. In the list of services you will see the **Traka Business Engine Service** and the **Traka Comms Engine Service**, although depending on your configuration these services may be installed on separate servers.

8. Right click on Traka Business Engine and choose '**Properties'** and then navigate to the **'Log On'** tab.

9. Enter the appropriate details into the username and password fields for the user that was granted the **'Logon as a service'** policy in step 4 and then press **OK**.



10. To start the Business Engine and Comms Engine Services, right click on the Business Engine and Comms Engine respectively and click '**Start'**.



4.2 DATABASE SETUP AND CREATION

The Traka Web Admin application will guide you through the process of creating and initialising a new Traka Web database automatically.

You must also decide how you require the Business Engine to authenticate to the SQL Server. The options are detailed in sections 4.2.1 below.

Please note that if you wish to create the Traka Web database and its contents manually, this is also possible but is covered under separate documentation:

- For instructions on how create a Traka Web database manually where the Business Engine is authenticating to the SQL Server using SQL Authentication, please refer to document **TD0149 - Traka Web Manual Database Creation guide using SQL Authentication**.
- For instructions on how create a Traka Web database manually where the Business Engine is authenticating to the SQL Server using Windows Authentication, please refer to document **TD0150 - Traka Web Manual Database Creation guide using Windows Authentication**.

4.2.1 BUSINESS ENGINE DATABASE AUTHENTICATION OPTIONS

Depending upon how you have configured the Business Engine Service in Section 4.1 above, will influence how the Business Engine authenticates with the SQL Server.

You can either choose for the Business Engine to connect to SQL Server using a SQL Username and Password (this is the default choice for standard installations) – see Section 4.2.1.1 below, or you can choose for the Business Engine to connect to the SQL Server using Integration Windows Authentication – see Section 4.2.1.2.

4.2.1.1 SQL USERNAME AND PASSWORD AUTHENTICATION TO SQL SERVER

If the Business Engine Service is running under the default 'local system' account identity (default) and you wish to authenticate to the SQL Server using a SQL Username and Password, in order to achieve automatic database creation, a SQL Server login is required with database administration permissions.

This is the standard choice for most installations.

Please note that the supplied privileged SQL credentials are only used once during database creation, and an account named 'Traka BE' will be used for normal connectivity to the SQL Server by the Business Engine when in SQL Server authentication mode. This is discussed in more detail in Section 4.2.2.1 below.

4.2.1.2 INTEGRATED WINDOWS AUTHENTICATION TO SQL SERVER

If the Business Engine Service is running under a named Windows User Account identity and you wish to authenticate with the SQL Server using Windows Authentication, then the Windows Account that you assigned in section 4.1.2 will require database administration permissions.

4.2.2 ADMIN APPLICATION DATABASE CONFIGURATION

Depending upon how you configured the Business Engine Service in Section 4.1 above influences how the database is configured within the admin application.

If you require database authentication using "SQL Server Authentication" (default option) please proceed to Section 4.2.2.1 below.

If you require database authentication using "Windows Authentication" please proceed to Section 4.2.2.2 below.

4.2.2.1 ADMIN APPLICATION DATABASE CONFIGURATION (SQL AUTHENTICATION)

1. Run the Admin Application.

   NOTE: This can be found under the Start menu, All Programs, Traka, Traka Web Admin.

2. When running the Admin application for the first time, you may ignore the 'Username' and 'Password' fields but you must select the authentication type from the drop-down menu next to Authentication Mode. Next, press the **'Connect'** button, which will automatically start the database creation wizard.

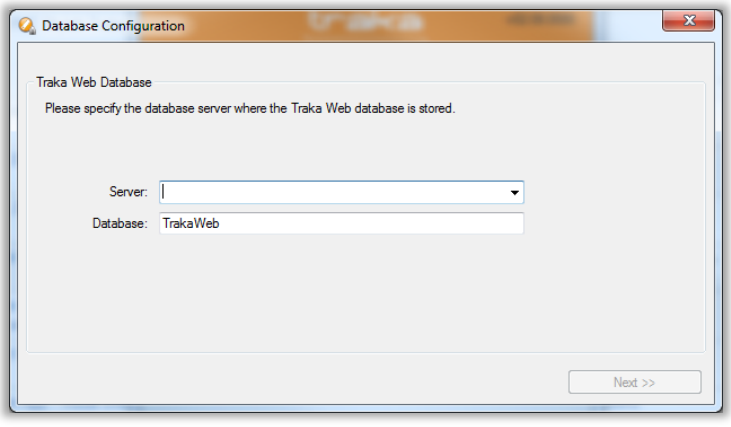
3. Choose the database server from the Server drop down list. Alternatively you can manually type the server you wish to connect to. Please note that if your SQL Server is installed under a 'named instance' you should enter the Server name as 'ServerName\InstanceName'.

   NOTE: The drop down list may take a few moments to load.

4. Enter the name of the database into the Database Field. Traka recommend a default name of **'TrakaWeb'**.

   NOTE: This database should not already exist and will be created by the Admin application, unless you are attempting to use an existing Traka Web database or have created the database manually.

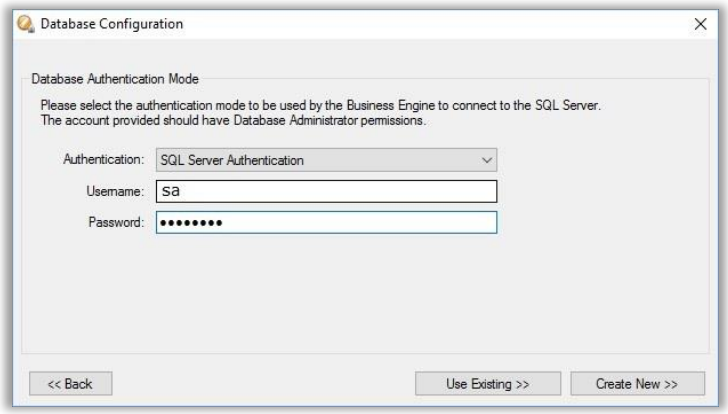
5. Click **Next**.



6. The next screen requires you to select the desired Database Authentication mode for the Business Engine to connect to the Database Server. Following this section assumes that SQL Server Authentication is being used so this will need to be selected.
7. **If you are using an existing database**, or have created a database manually by following the **TD0149** guide as outlined in **Section 4.2**; enter "Traka BE" (or other user you have configured with TrakaAdmin and TrakaReadWrite roles) into the username and the password you created for that user. Press the **'Use Existing'** button and then **go to step 8.**

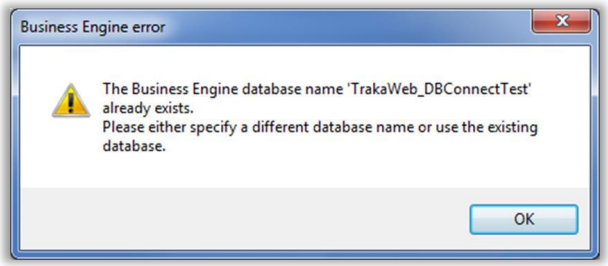
   Otherwise, **if you are creating a new database**, you will need to provide a Database Administrator username and password in order to verify the connection to the database. The supplied credentials needs to be a SQL Server login on the database and will **only** be used once as a dedicated BE user will be created (if it hasn't already).

   - The SQL Server must also be configured to '**Mixed Mode Authentication**' when using a SQL Username and Password.
   - This needs to be a SQL Server login on the database server and **must** have permissions to create and administer a new database.
   - Ensure that the SQL Server login used to connect to between the Business Engine and SQL server has the **'dbcreator'** and **'securityadmin'** server roles assigned (or simply the **'sysadmin'** server role).
   - Alternatively, or if you are not sure, you can simply use the SQL Server system administrator (**sa**) account.
   - **NOTE: These elevated permissions can be removed after the database is created by assigning the 'public' permission to the SQL Server login as it will no longer be used.**

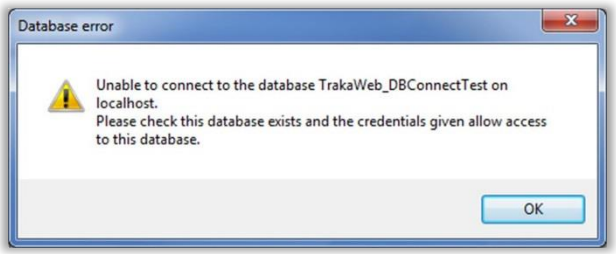


   Press the **'Create New'** button.

NOTE: If you choose the 'Create New' option and you have entered incorrect details in the Database Configuration, you will receive the following error message.



NOTE: If you have entered incorrect details in the Database Configuration, you will receive the following message. It is assumed that you have either entered your database details incorrectly or that there is no database present on the server in which case you will be required to create a new database configuration via the 'Create New' option.

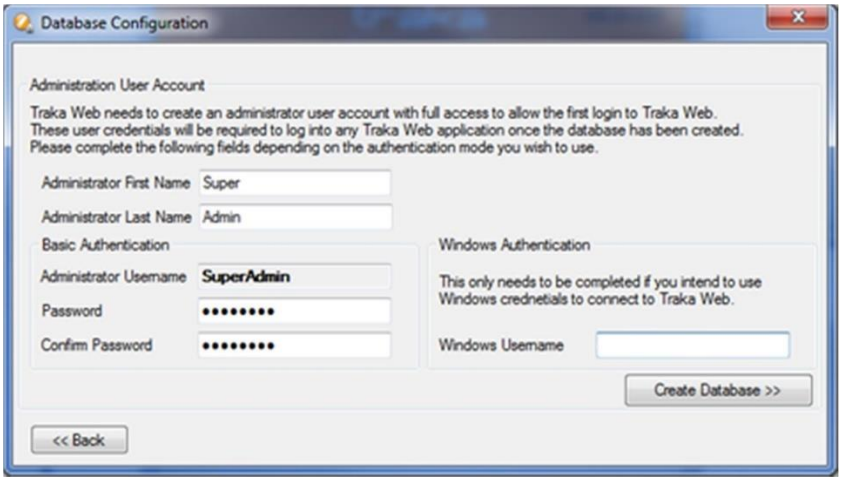


8. Once the correct Database Configuration details have been entered you will proceed to the Administration User Account details.

9. Traka Web requires a Super Administration account to be created for the purposes of system administration, for example, creating new users and assigning permissions. For more information, please review the Authentication Options section.

NOTE: You will need the Super Administrator Username and Password when you first login to Traka Web.

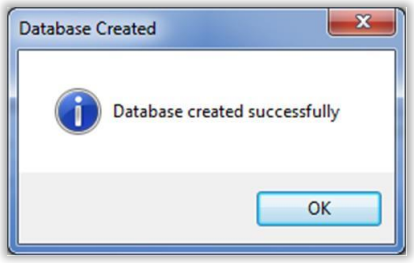
10. Enter the First Name and Last Name for your Super Administration user.



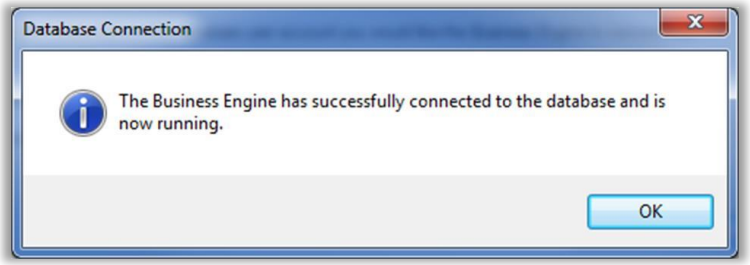
11. If you will be using Windows authentication as your authentication method to login to Traka Web (not to be confused with the separate connection to the SQL server described in more detail above) you should enter the Windows Username for the user that you wish to be associated with the Traka Web Super Admin account. If you are not using Windows authentication as your authentication to login to Traka Web, leave the Windows Username field blank.

12. Enter the Password to be used for the Super Administration account.

13. If you are creating the database, press the '**Create Database**' button and if all details have been entered correctly, the Admin application will start the process to create the Traka Web Database. A progress bar will be displayed and you will see a **'Database Created'** message once completed as shown below. Click '**OK**' to continue.



If you are using an existing database, press the '**Fix Database**' button and if all details have been entered correctly, the Admin application will start the process to update the Traka Web Database. A progress bar will be displayed and you will see a **'Database Connection'** message once completed as shown below. Click '**OK**' to continue.

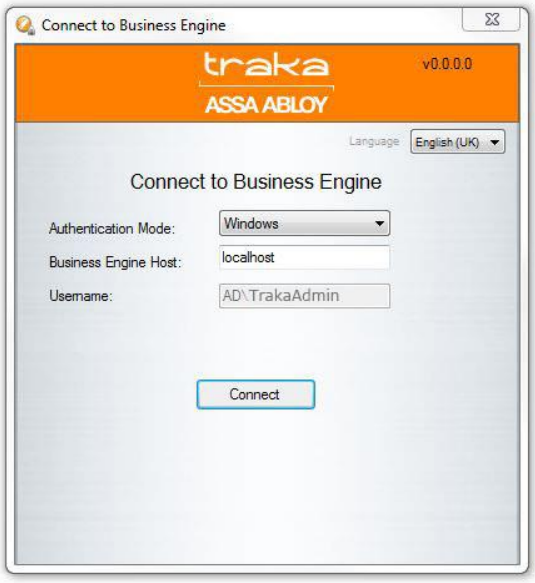


14. You will then be shown the Admin application login screen with the details already populated to connect to the Business Engine.

4.2.2.2 ADMIN APPLICATION DATABASE CONFIGURATION (WINDOWS AUTHENTICATION)

1. Run the Admin Application.

   NOTE: This can be found under the Start menu, All Programs, Traka, Traka Web Admin.



2. When running the Admin application for the first time, select the Windows option from the drop-down menu next to Authentication Mode. Next, press the **'Connect'** button, which will automatically start the database creation wizard.

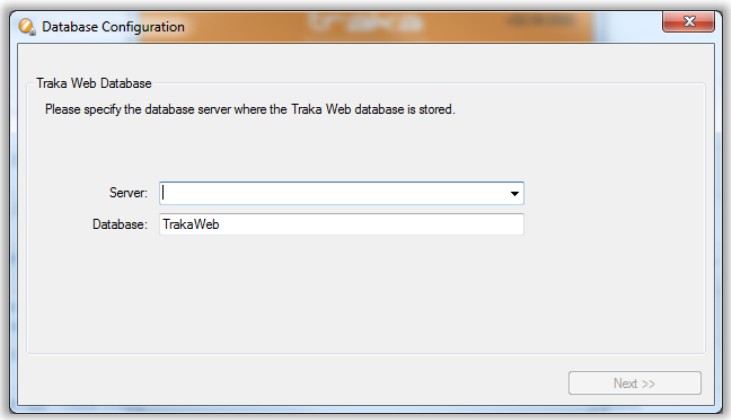
3. Choose the database server from the Server drop down list. Alternatively you can manually type the server you wish to connect to. Please note that if your SQL Server is installed under a 'named instance' you should enter the Server name as 'ServerName\InstanceName'.

   NOTE: The drop down list may take a few moments to load.

4. Enter the name of the database into the Database Field. Traka recommend a default name of **'TrakaWeb'**.

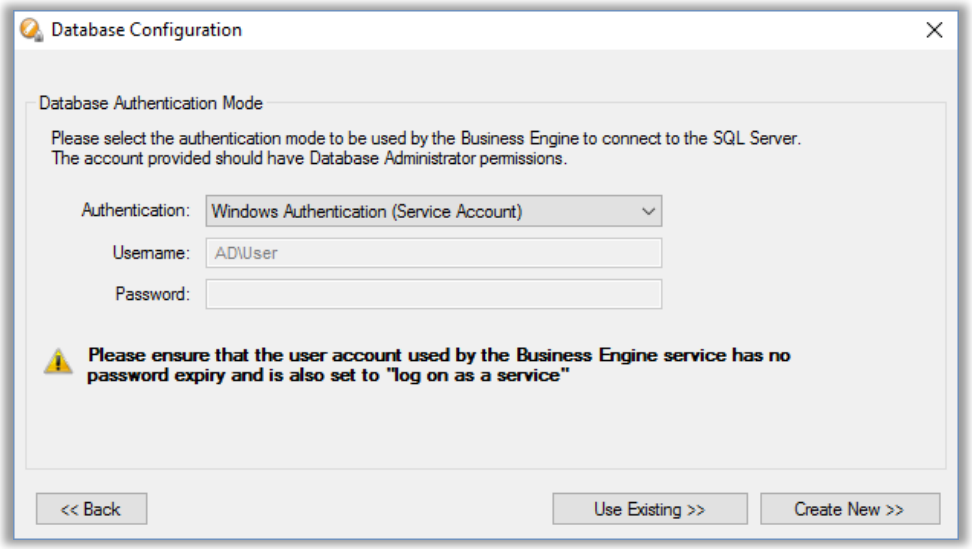
   NOTE: This database should not already exist and will be created by the Admin application, unless you are attempting to use an existing Traka Web database or have created the database manually.

5. Click Next.



6. The next screen requires you to select the desired Database Authentication mode for the Business Engine to connect to the Database Server. Following this section assumes that Windows Authentication is being used so this will need to be selected.

7. The credentials used for the domain account running the Business Engine Service will be utilised which should have been set up as shown in section 4.1.2. As a result, no credentials will be required to be entered at this stage and the domain user account that the Business Engine service is running under will be displayed in the 'Username' textbox as shown below.

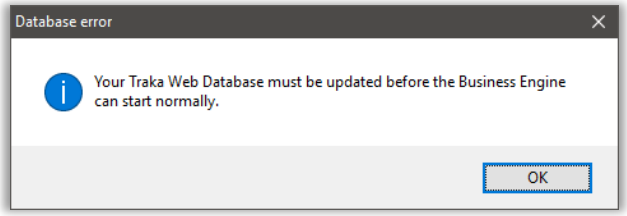


If there is no existing TW database (where the "Create New" option is planning to be used), ensure that the domain user account that the Business Engine service is running under has the **'dbcreator'** and **'securityadmin'** server roles assigned (or simply the **'sysadmin'** server role).

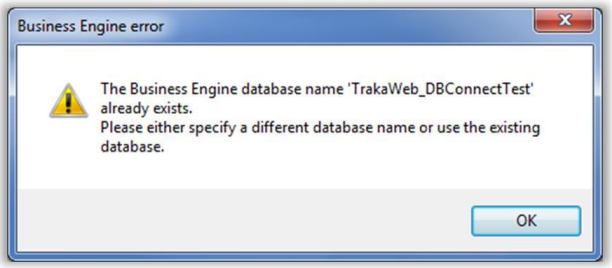
8. If you are attempting to create a new Traka Web database then continue by pressing the **'Create New'** button otherwise you should continue by pressing the **'Use Existing'** button.

NOTE: The 'Use Existing' option should also be used if the database was created manually using TD0150 in Section 4.2.

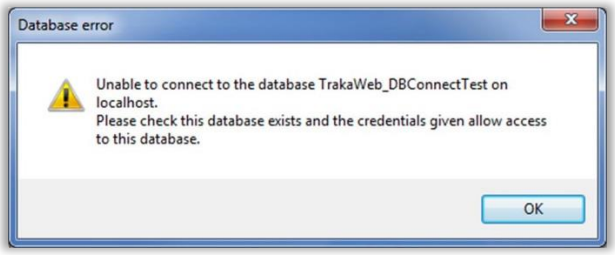
If the **'Use Existing'** option is used and successful, the following message will be displayed.



NOTE: If you choose the 'Create New' option and you have entered incorrect details in the Database Configuration, you will receive the following error message.



NOTE: If you choose the 'Use Existing' option and you have entered incorrect details in the Database Configuration, you will receive the following message. It is assumed that you have either entered your database details incorrectly or that there is no database present on the server in which case you will be required to create a new database configuration via the 'Create New' option.



9. Once the correct Database Configuration details have been entered you will proceed to the Administration User Account details.

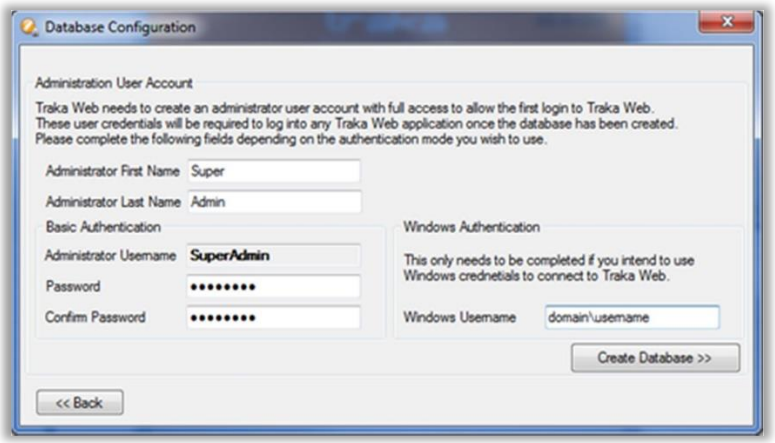
10. Traka Web requires a Super Administration account to be created for the purposes of system administration, for example, creating new users and assigning permissions. For more information, please review the Authentication Options section.

NOTE: You will need the Super Administrator Username and Password when you first login to Traka Web.

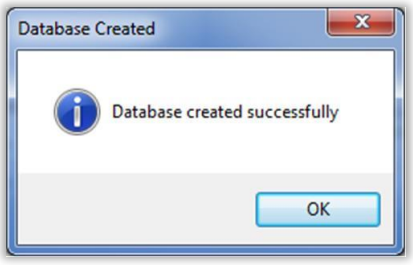
11. Enter the First Name and Last Name for your Super Administration user.

12. If you will be using Windows authentication as your authentication method to login to Traka Web (not to be confused with the separate connection to the SQL server described in more detail above) you should enter the Windows Username for the user that you wish to be associated with the Traka Web Super Admin account. If you are not using Windows authentication as your authentication to login to Traka Web, leave the Windows Username field blank.

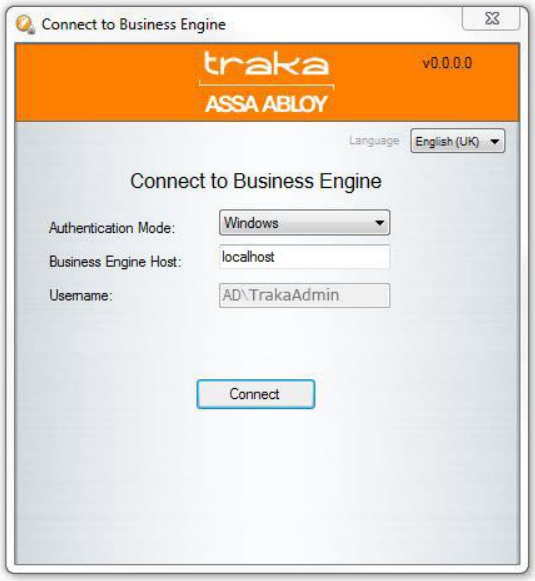
13. Enter the Password to be used for the Super Administration account.



14. Press the Create Database button and if all details have been entered correctly, the Admin application will start the process to create the Traka Web Database. A progress bar will be displayed and you will see a **'Database Created'** message once completed as shown below. Click '**OK**' to continue.



15. You will then be shown the Admin application login screen with the details already populated to connect to the Business Engine.

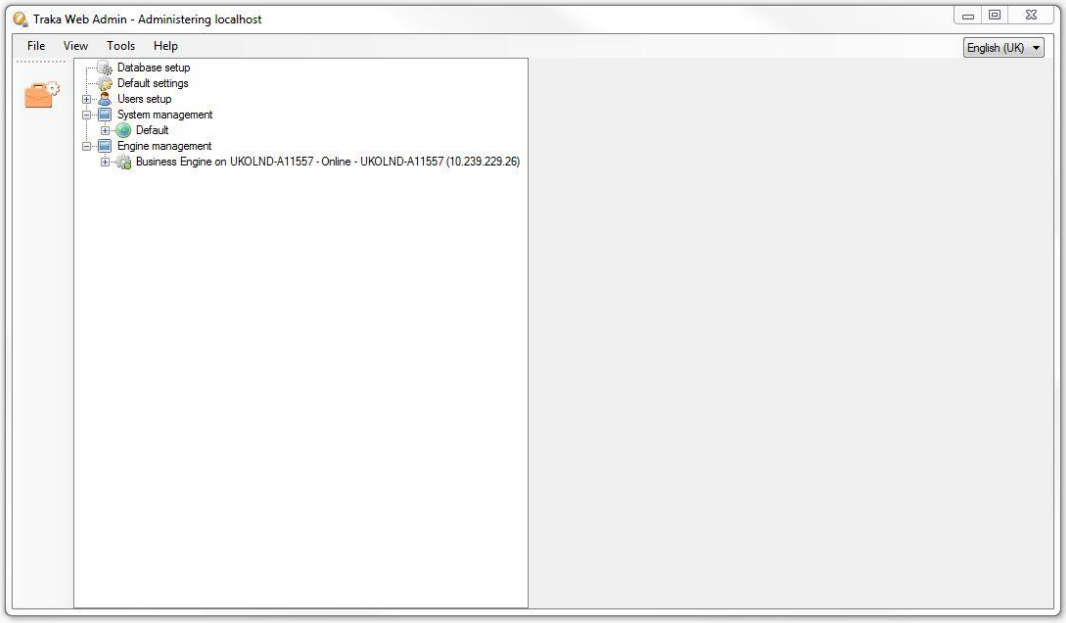


4.3 BUSINESS ENGINE SETUP

1. Run the Admin Application again and login using the Super Administrator account created in the database setup section of this document.

2. Click Connect.

3. Once logged into the Admin application you will see a tree structure on the left half of the screen.



4. Expand "Engine Management" and click on the Business Engine in the tree view, where you will see the Business Engine Details screen on the right.

5. Check that the Host Name is showing the correct Host Name of the server where the Business Engine is running. It is possible to right click on the Host Name Field to show a menu that will allow you to automatically enter the host name and IP address of the current server.

NOTE: 'localhost' should not be used in this field.

6. Check that the IP Address is correct for your server.

7. The Engine State button should be showing as offline (red). Click the status button to toggle it to online (green).

8. Press the save button to save the settings, status and to bring the Business Engine online.

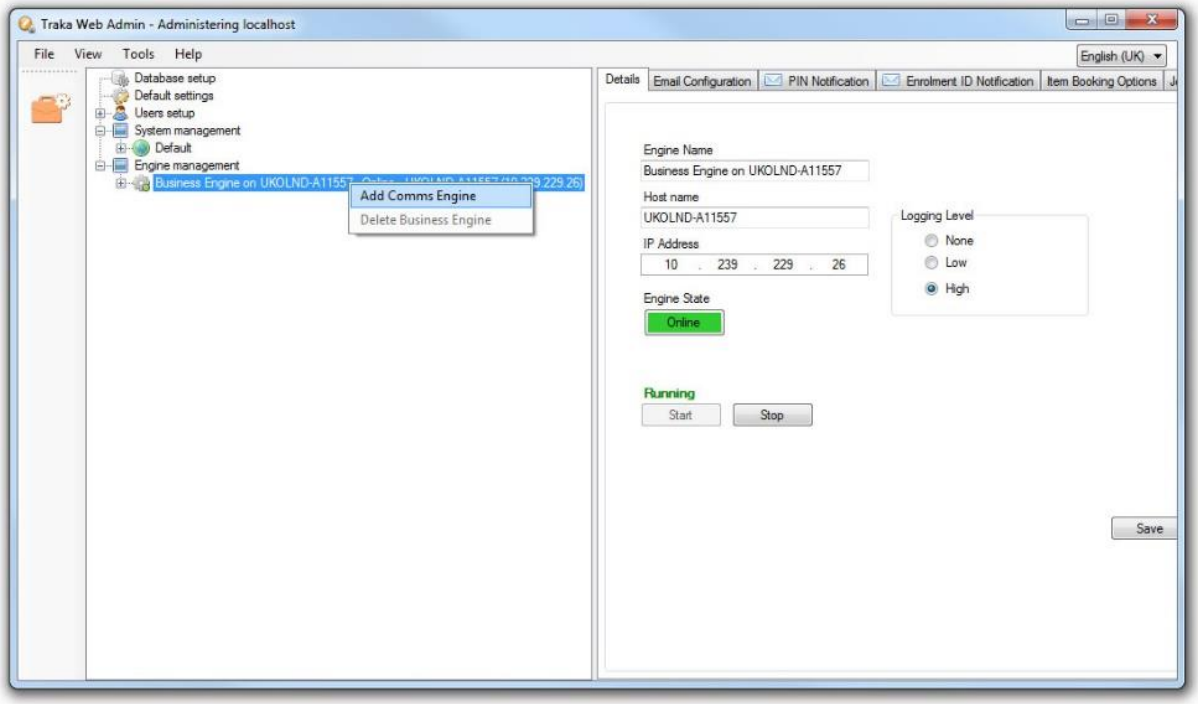
9. The Business Engine is now set up and online, you should proceed to **section 4.4** Comms Engine Setup

NOTE: Refer to Section 5 for information regarding Email Configuration

4.4 COMMS ENGINE SETUP

1. In the Admin application tree view, expand the Engine Management section.

2. Right click on the Business Engine for which you want to add a Comms Engine and click on Add Comms Engine.

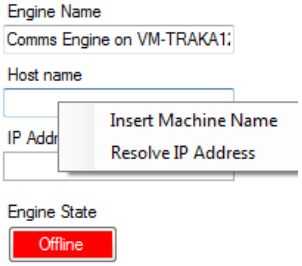


3. Once the new Comms Engine has been added, the details of the engine can be seen on the right.

4. Enter a Name for the Comms Engine.

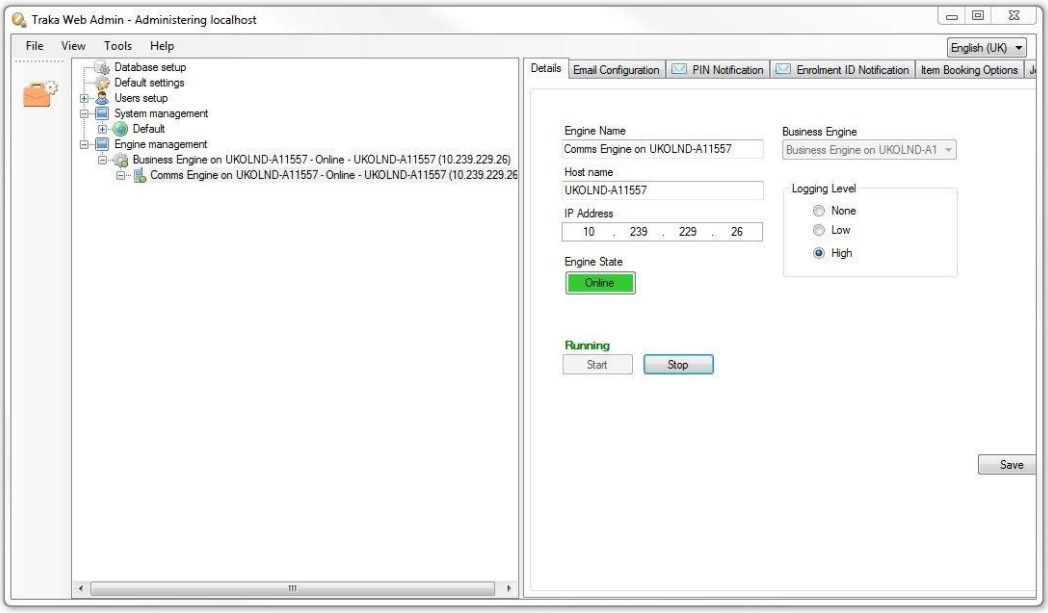
5. Enter the Host Name of the server running the Comms Engine. It is possible to right click on the Host Name Field to show a menu that will allow you to automatically enter the host name and IP address of the current server.

NOTE: 'localhost' should not be used in this field.



6. Enter the IP Address of the server running the Comms Engine.

7. If your Comms Engine Service is running on the same server as the Business Engine Service, you should enter the same Hostname and IP Address as the Business Engine.



8. The Engine State button should be showing as offline (red). Click the status button to toggle it to online (green).

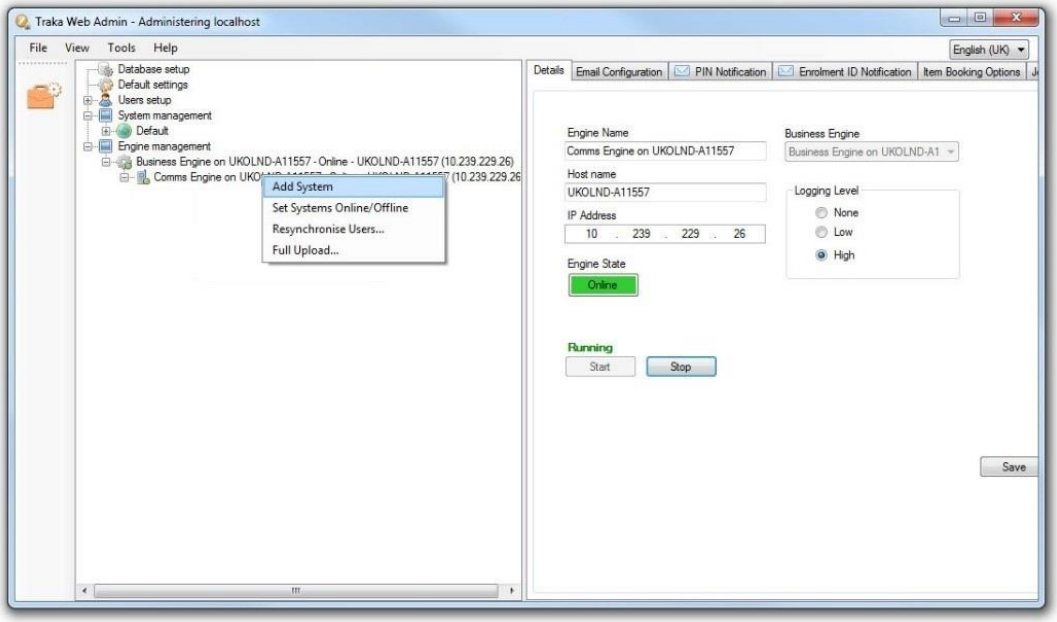
9. Press the save button to save the settings and bring the Comms Engine online.

4.5 SYSTEM SETUP

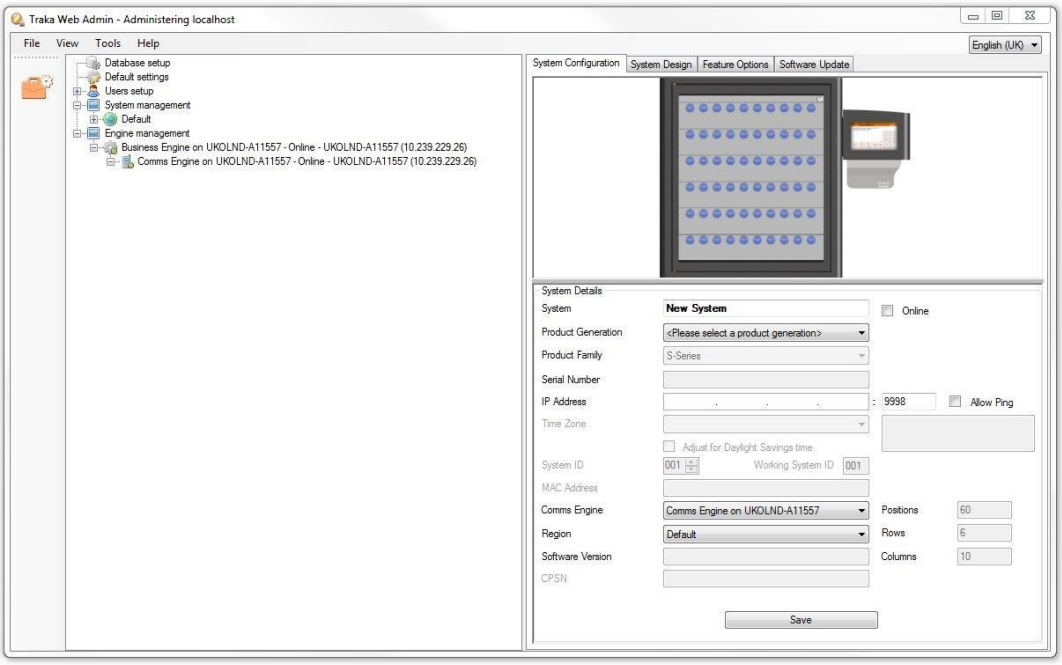
The Traka Web Admin App supports both Traka Touch and 16bit systems. The process for setting up both types is the same. For full details on how to setup a 16bit cabinet or locker system using the Admin App, refer to **TD0128 – Connecting a 16bit System to Traka Web.**

1. In the Admin application tree view, click on the Engine Management section.

2. Right click on the Comms Engine for which you want to add a system and click on Add System.



3. You will then see the System Configuration screen as shown below. You will need to determine whether the system is a 16bit or a Traka Touch system from the Product Generation drop down menu. To configure your system you will also need to fill in the relevant details on both the 'System Configuration' and 'System Design' tabs.



4. Check the 2 boxes for 'Online' and 'Allow Ping'.
   The 'Online' setting determines whether the Comms engine will try to communicate with the cabinet. This will set the cabinet as active so that email notifications can be used.

   The 'Allow Ping' setting will determine if the Comms engine will attempt to ping an address when it's unable to connect to the system.

4.5.1 SYSTEM CONFIGURATION

1. Enter a 'System' name for your new system. For example 'Reception'.

2. Choose a 'Product Family' for your new system. For example 'S-Series'.

NOTE: The default system shown may not match the exact configuration of your system. This can be edited on the next tab 'System Design' as explained in the next section.

3. Choose the Comms Engine from the drop down list; this will be the Comms Engine that you want this system to communicate with.

4. Enter the IP Address of the system.

5. Ensure the '**Online**' and '**Allow Ping**' checkboxes are ticked.

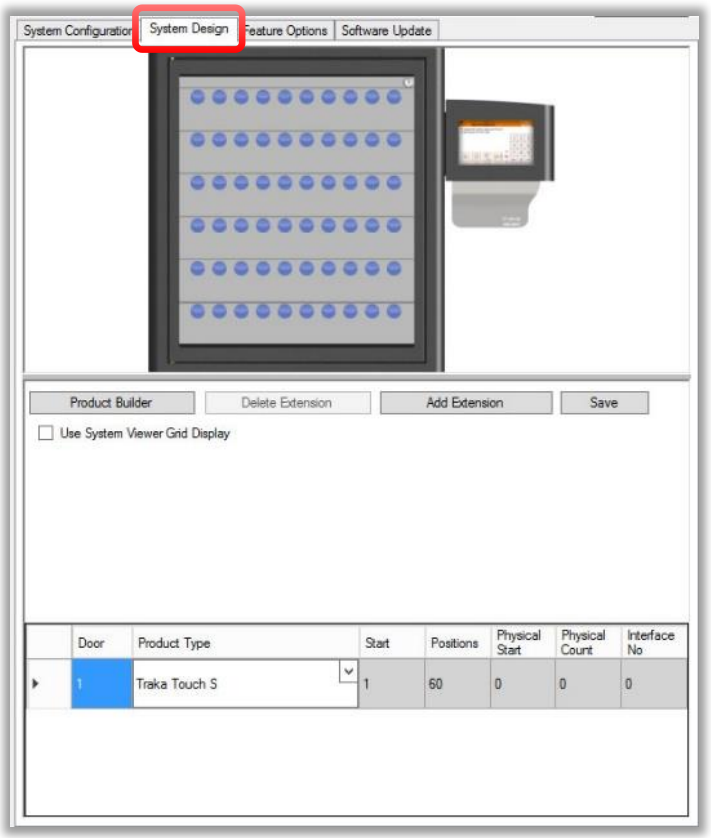
6. Select a Region.

7. Click the '**Save**' button and you will see a confirmation popup box. Your system is now setup.

8. If you wish to edit the design of your system including changing the number of positions, or adding extension cabinets move on to the next section.

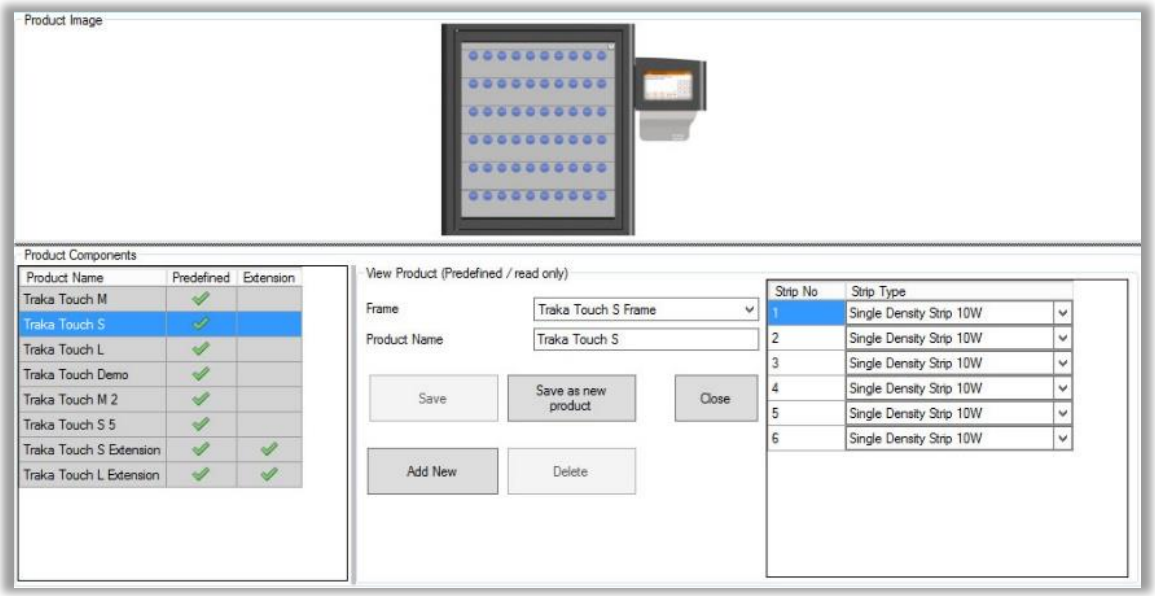
4.5.2 SYSTEM DESIGN

1. To edit the system image to match the configuration of your Traka Touch System, select the '**System Design**' tab.



2. The dropdown list in the 'Product Type' column shows a list of the existing product types within the selected Product Family. If none of these product types match your system, a custom product type will need to be created. To do this, click the '**Product Designer**' button and you will be presented with the following window.

NOTE: The product designer currently has limited support for Lockers.

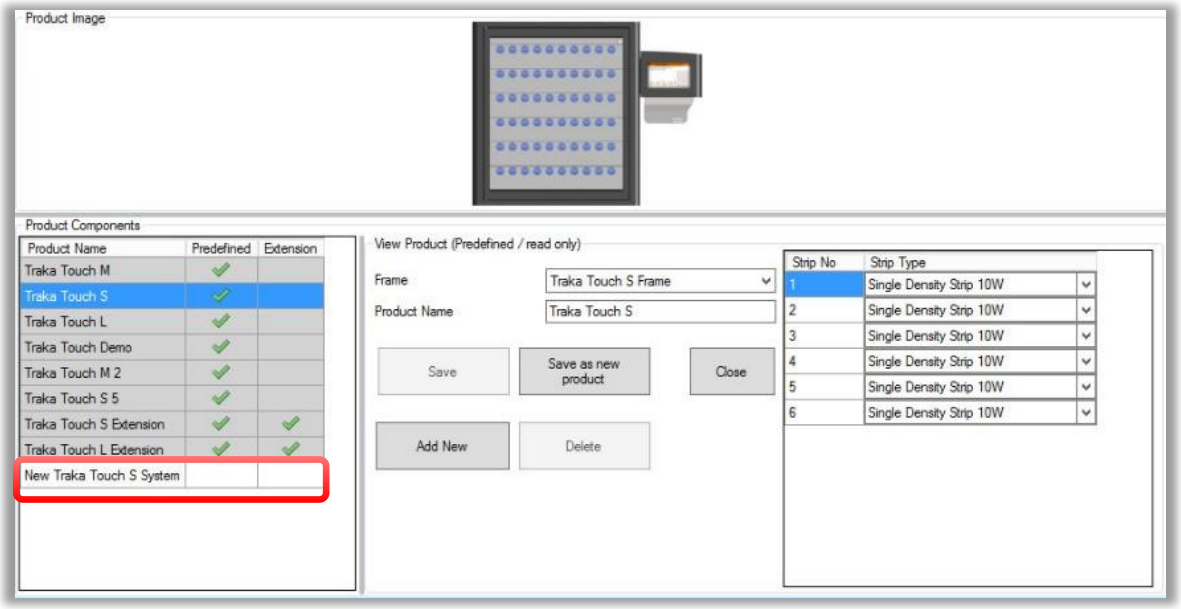


3. Select the required Frame type from the dropdown list in the centre of the screen.

4. Enter a Product Name.

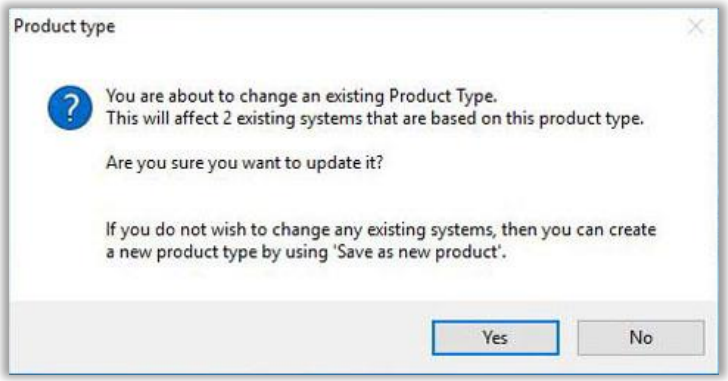
5. Select the type of receptor strip or blank for each strip position from the table on the right. The image will update with each selection.

6. Click '**Save as new product**'. A pop up will ask you to confirm. Once the product has been created it will be added to the list of product types on the left of the screen.



7. If you wish to add any more custom product types, click '**Add New**' and repeat this process.

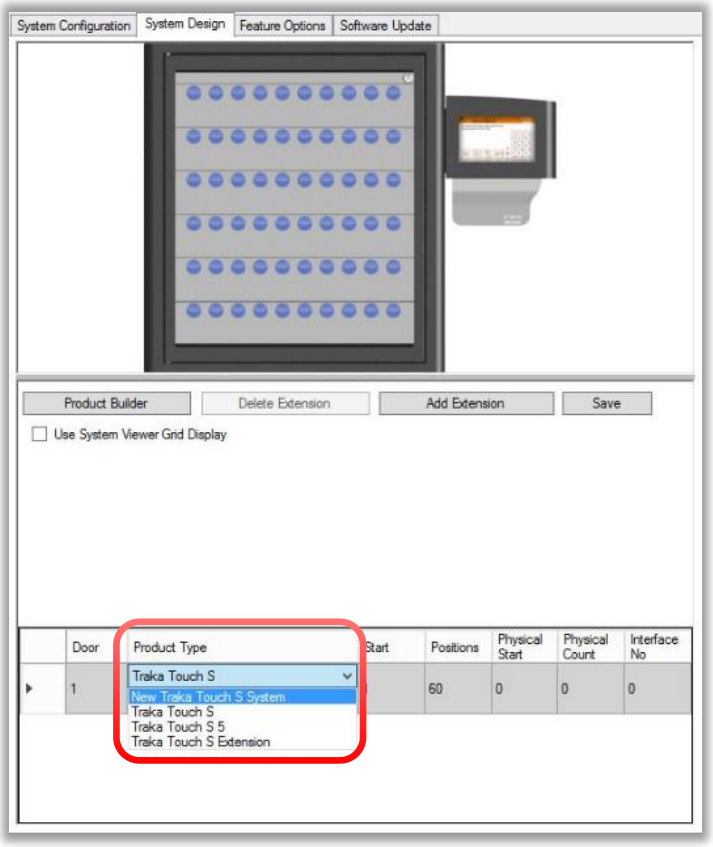
8. To edit a custom product type, select the product from the list on the left. Make the required changes and then click '**Save**'.
   A popup window will appear showing a count of all the systems that will be affected by the change. Clicking on 'Yes' will save each of the affected systems. Should you not wish to save the changes to the systems, click on '**No**' to cancel and then click on '**Save as new product**'.



9. To delete a custom product type, select the product from the list on the left and click '**Delete**'.

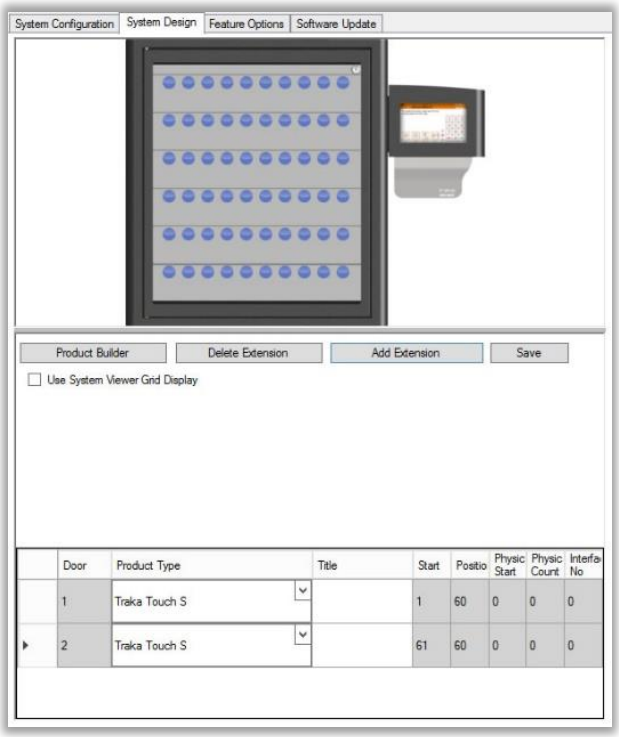
10. Once finished click '**Close**' and you will return to the System Design screen.

11. You will now be able to select the custom product type(s) you created from the dropdown list.



12. If you need to add an extension cabinet, click '**Add Extension**'. A second row will appear for you to select the product type for the extension. You also now have the option to enter a title for each of the cabinets.

NOTE: Extensions are only supported for 'L' and 'S' systems.



13. Once finished click '**Save**'.

4.5.3 TRAKA WEB SYSTEM VIEWER GRID

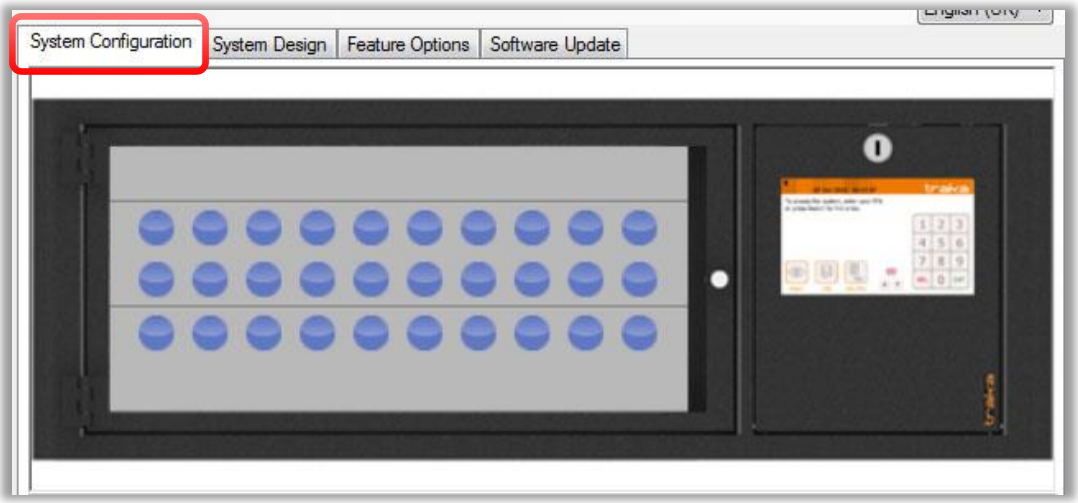
Due to the many permutations of physical locker designs, it is not always possible to display the interactive image of the locker within the Traka Web system viewer. Currently, there are only a subset of locker images available to use and so to resolve the issue, a System Viewer Grid is used. The System Viewer Grid shows the status of the physical system within Traka Web without having to display an image of the actual locker or cabinet.

Configuration of the System Viewer Grid is done within Traka Web Admin on a per-system basis. Although the option is available for both cabinets and lockers, the option to customise the Traka Web System Viewer Grid is specific to lockers only.

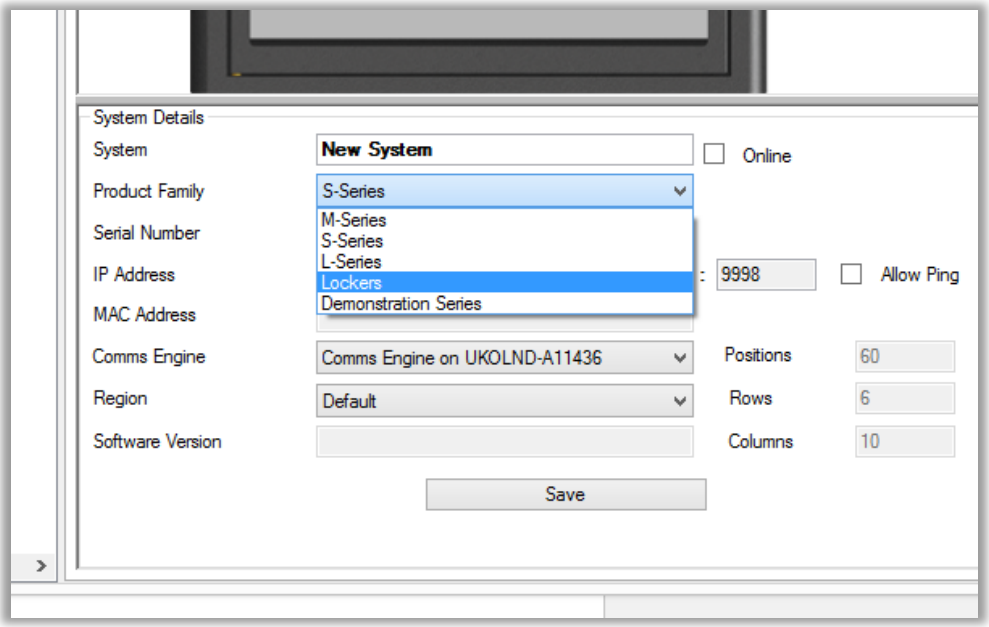
NOTE: When configuring cabinets, a user has the option to either view the system viewer grid or the interactive image within the system viewer in Traka Web.

System View Option and Custom Product Type

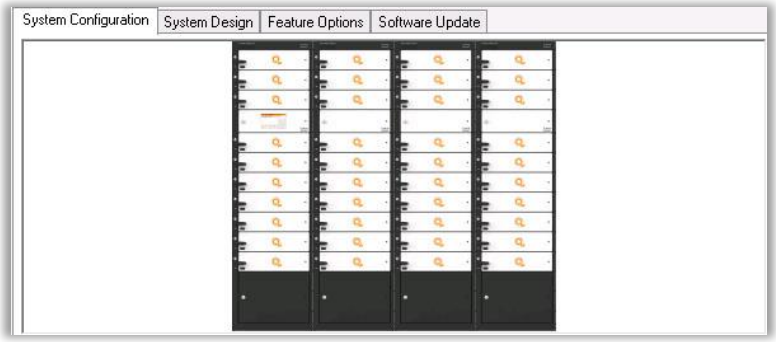
After launching the Traka Web Admin Application, the System Configuration screen will be displayed.



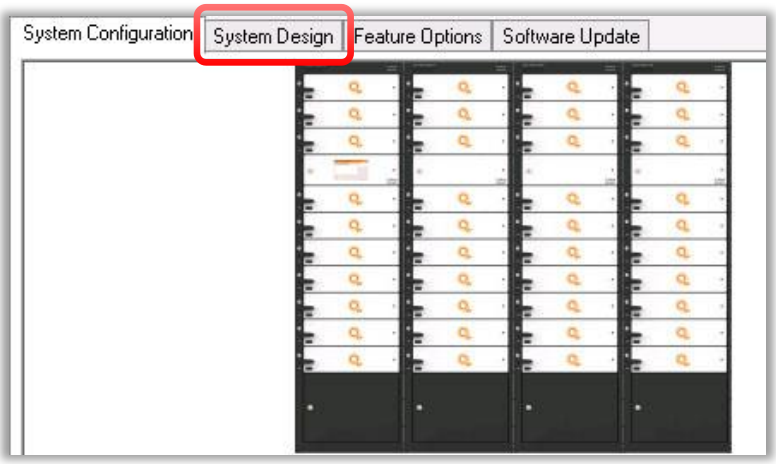
1. Locate the Product Family drop down menu to choose a specific system type.



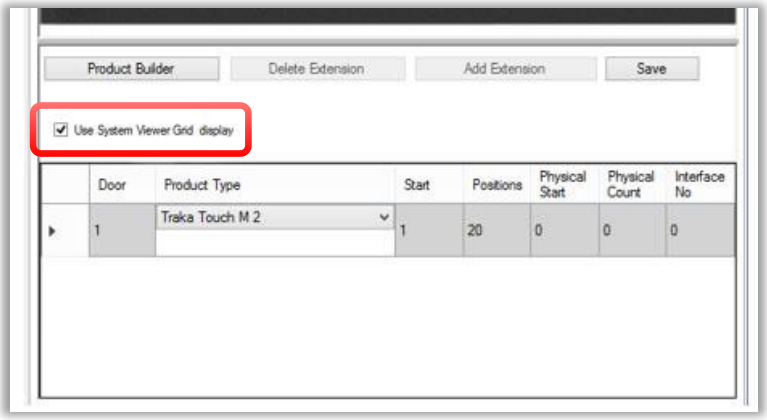
The screen will change to display the default locker image.



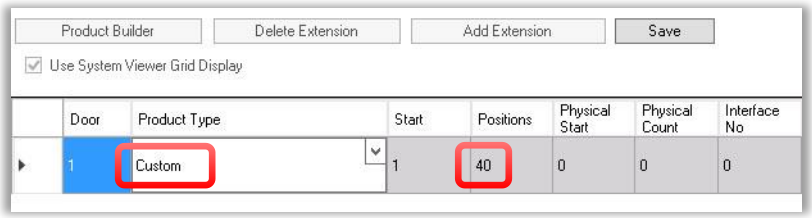
2. Click on the '**System Design**' tab to edit the selected system type.



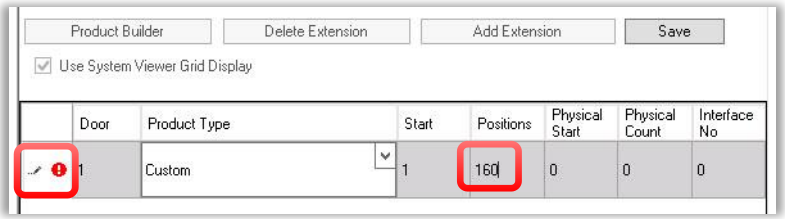
3. Within the System Design tab, click on the '**Use System Viewer Grid display**' tick box.

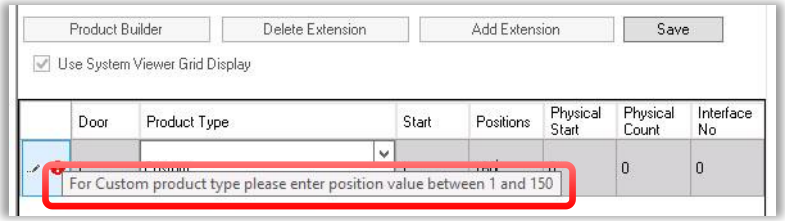


If the system to be configured is a locker, the 'Custom' option will be made available from the Product Type drop down menu. The custom product type is a product type that should be used when there is no system image available for the locker. When using the custom product type the user will be required to manually enter a number into the 'Positions' field for this system. The maximum value that can be entered will be 150.



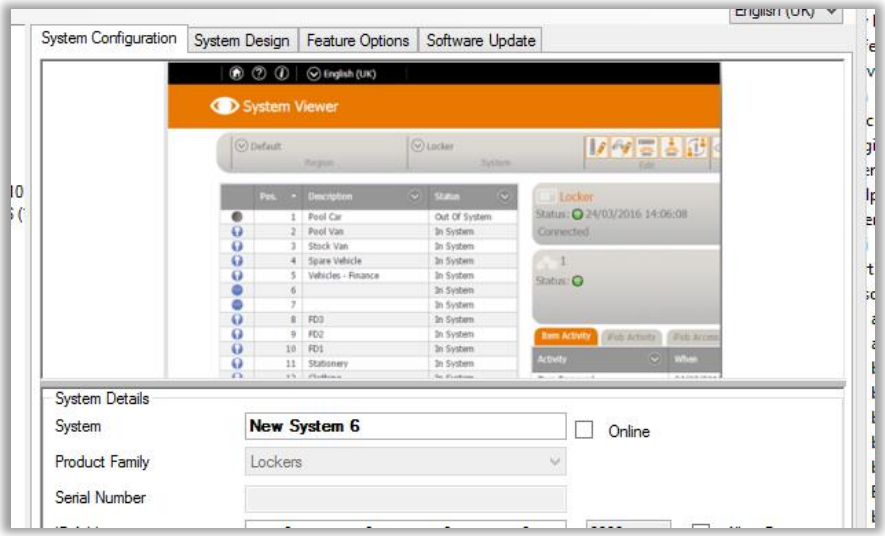
NOTE: The maximum value that can be entered within the 'Positions' field is 150. If this value is exceeded, an icon will appear in the left hand box. Hovering the mouse cursor over the icon will display a message informing the user of this.





NOTE: If 'Custom' has been selected, the 'System Viewer Grid' must be used with that particular system. The tick box to select the 'Use System Viewer Grid Display' will be ticked and greyed out and the Product Builder will also be disabled.

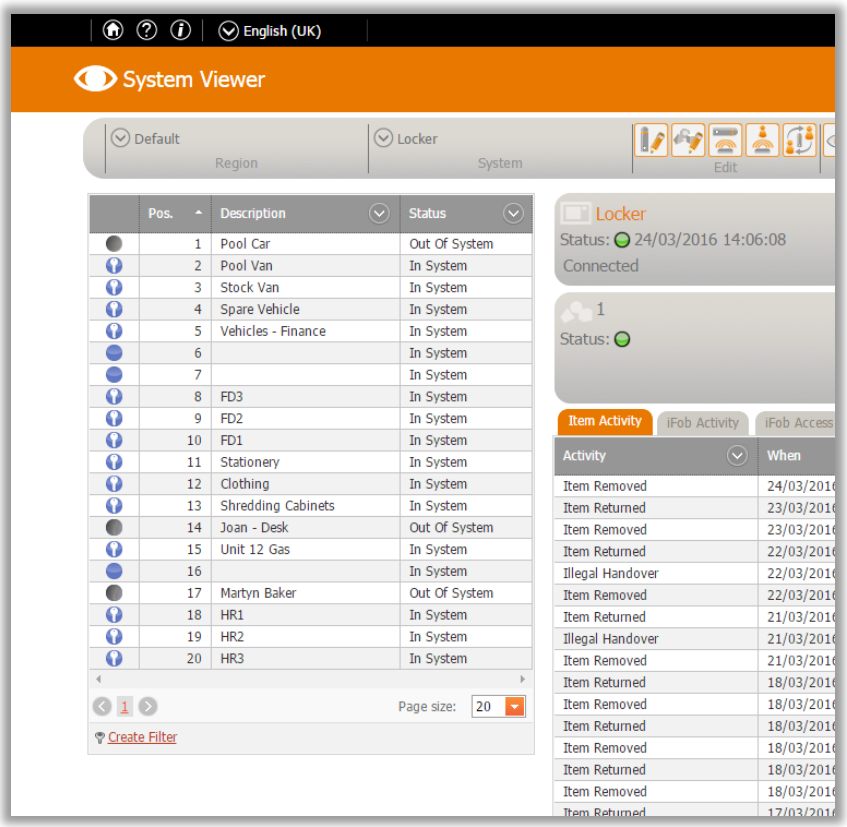
With the 'Custom' option enabled, a generic image will be displayed in place of the usual system image to indicate that this system is a custom type and that no image is currently available.



4.5.4 TRAKA WEB SYSTEM VIEWER

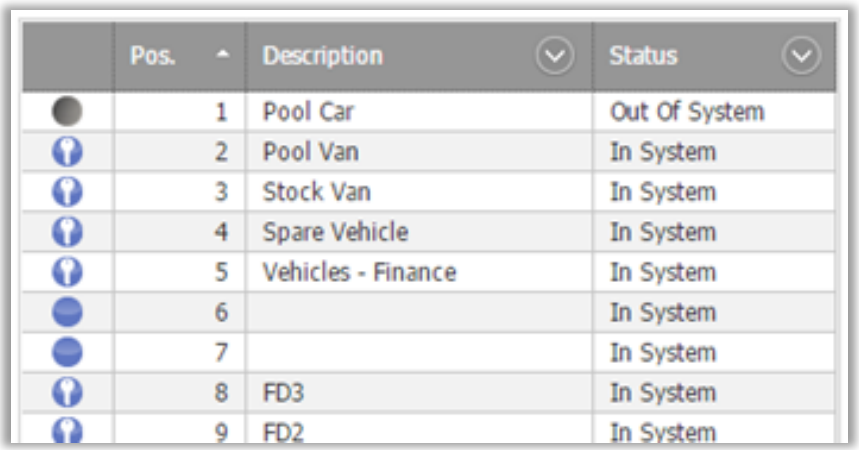
When Traka Web is launched, the System Viewer page will check to see if the current system should be displayed by an image or a System Viewer Grid as it loads. If the System Viewer Grid display is to be used then the status information will relocate from the bottom left of the page to the top right of the page above the activity grids location.

The System Viewer Grid layout will change depending on which return type the system has been assigned. A typical System Viewer Grid may appear as shown below:



Fixed Return

For a fixed return system, each physical position will be represented by a row within the System Viewer Grid. Each row will be divided into columns as shown below.



Random Return to Single System and Multiple Systems

For a Random Return to Single System and Multiple Systems, each physical position in the system will be represented by a row in the System Viewer Grid. A row will also be displayed for each iFob that is not in the system.

When an iFob is removed from the system, its position will remain but its icon will turn grey to show that the iFob is not in the system. A new row will then be added to the bottom of the grid to show which particular iFob has been removed. It's Index, Description and Status will also be displayed. This is shown in the example below.

The iFob's in position 6 and 7 have been removed from the system. Two new rows are created at the bottom of the grid reflecting their current status. Please refer to the Traka Web User Guide – UD0018 for more information.

	Pos.	Index	Description	Status
	1	1	Silver Ford Focus	In System
	2	2	Red Ford Focus	In System
	3	3	Silver Ford Focus	In System
	4	4	Silver Mercedes	In System
	5	5	Grey Audi	In System
	6			Out Of System
	7			Out Of System
	8	8		In System
	9	9		In System
	10	10		In System
		6	Transit Van 2	Out Of System
		7	Transit Van 1	Out Of System

4.6 TRAKA TOUCH NETWORK SETUP

In order for Traka Touch to accept an incoming connection from Traka Web, the Traka Web option must be enabled in the Traka Touch Application.

1. Login to Traka Touch.

NOTE: The user must be an administrator.

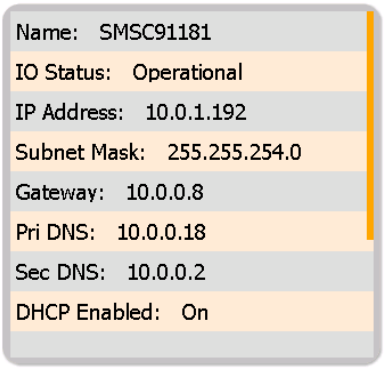
2. Select the Administration option.

3. From the Administration screen select the Network option.

4. Set the "Enable communication to Traka Web" option to: 

5. To configure the IP Address of the Traka Touch, click on the NIC button.

6. The network settings window appears.



7. To enable DHCP, select the DHCP Enabled to toggle DHCP On and Off.

8. To specify a static IP Address toggle DHCP to Off, then select each of the following in turn and edit using the on screen Numeric Keypad.

    a. IP Address (IP4)
    b. Subnet Mask
    c. Gateway
    d. Primary DNS (if required)
    e. Secondary DNS (if required)

9. Click Settings button to return to the Network setting page.

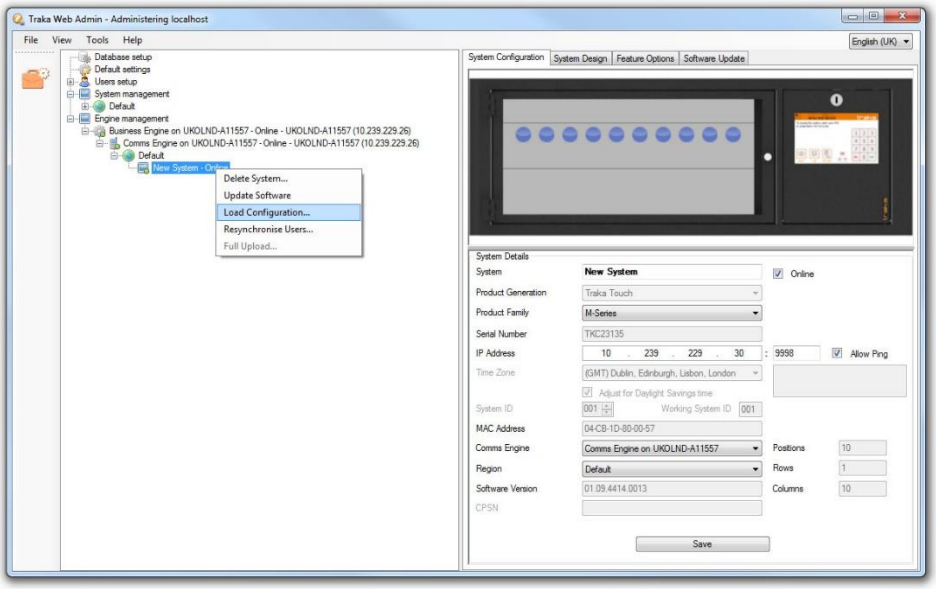
10. Click **Save**.

4.7 LOADING A CONFIGURATION FILE

When adding a system into Traka Web, it may be necessary to load or replace the configuration file in the Traka Touch System.

1. Run the Admin application and navigate to the systems in the tree view, from there highlight the desired system.

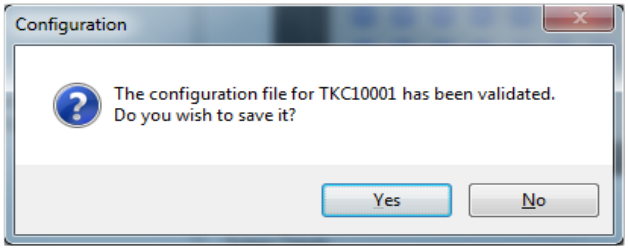
2. Right click and select '**Load Configuration**'.



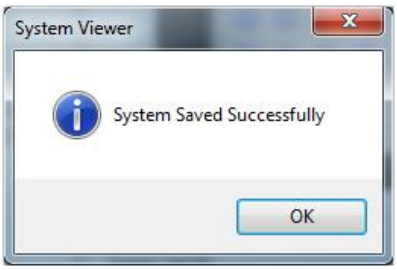
3. A window will appear allowing you to navigate to the appropriate location of the configuration file.

4. Highlight the configuration file and Select '**Open**'.

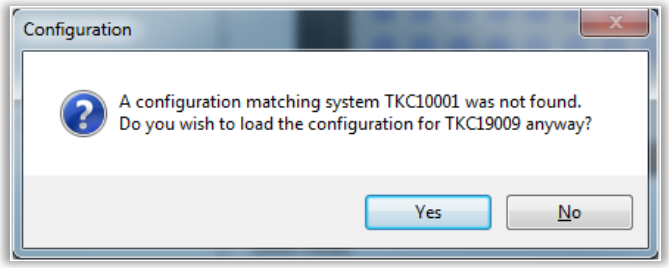
5. If the configuration file is acceptable then a message will appear telling you that the file has been validated. Click '**Yes**' to save the file to the database and Traka Touch, and continue.



6. A message will appear stating System Saved Successfully, click '**OK**'.

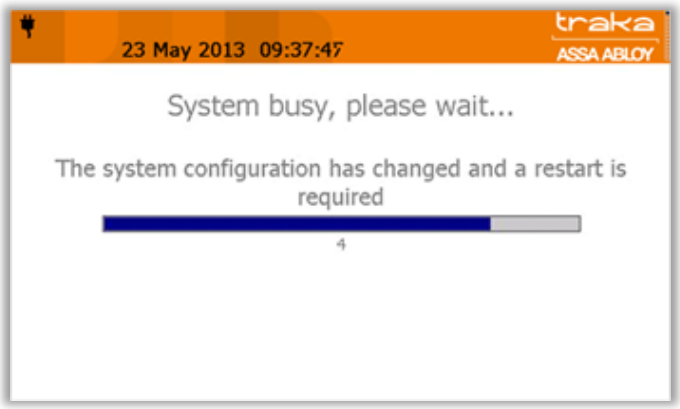


NOTE: If the configuration file you are attempting to load doesn't match the serial number of the system, you will receive the following message.



The configuration file will load into the system but any and all 'cost options' you previously had on your system will be disabled. Reload the correct configuration file to restore your system options.

7. The Traka Touch system will automatically begin the configuration update. A progress bar will represent how far through the process the system is. Once completed you will be presented with the default login screen.



NOTE: For the config update to automatically run, a Traka Touch user must not be logged in. If the Traka Touch system is in use, the update will commence once all activity is completed and they have logged out.

NOTE: If the configuration file you are attempting to load doesn't match the serial number of the system, you will receive a message stating that the serial number doesn't match the config file or that the config MAC address doesn't match the hardware. Click OK to continue to use the system.

5. EMAIL CONFIGURATION

Traka Web has the ability to email a user's PIN and/or Enrolment ID as well as send Email notifications. In order for the email facility to operate, the Business Engine must be configured using the Admin Application.

When a user is defined, Traka Web can email a user's PIN and/or Enrolment ID to them if the Email PIN check box is ticked and an email address has been entered into the user details.

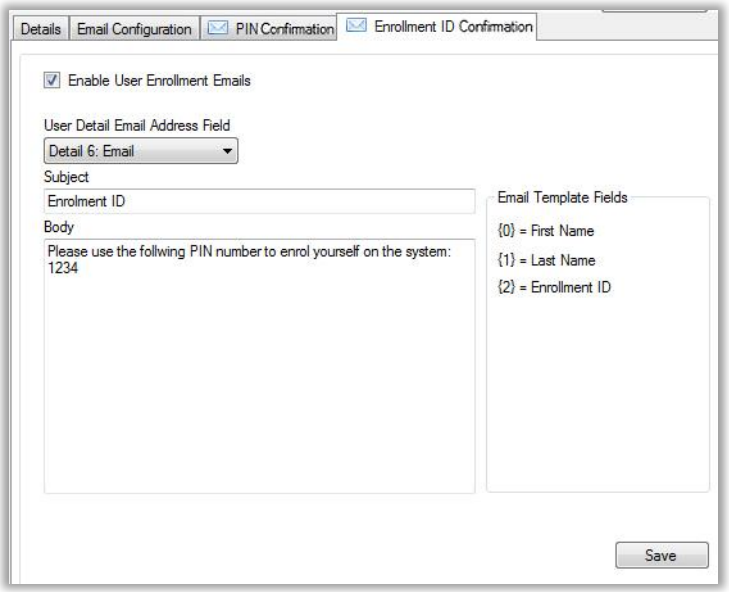
Once the settings below have been configured, you can create email notifications to trigger under specific circumstances from the Traka Web front end. Please review the latest version of UD0018 - Traka Web User Guide for more details on Email Notifications.

5.1 ADMIN APPLICATION SETUP

1. Access the Business Engine within Traka Web Admin and then select the '**Enrolment ID Confirmation**' tab.
2. Tick the box next to '**Enable User Enrolment Emails**'.
3. In the dropdown box under '**User Detail Email Address Field**' change to '**Detail 6: Email**'.

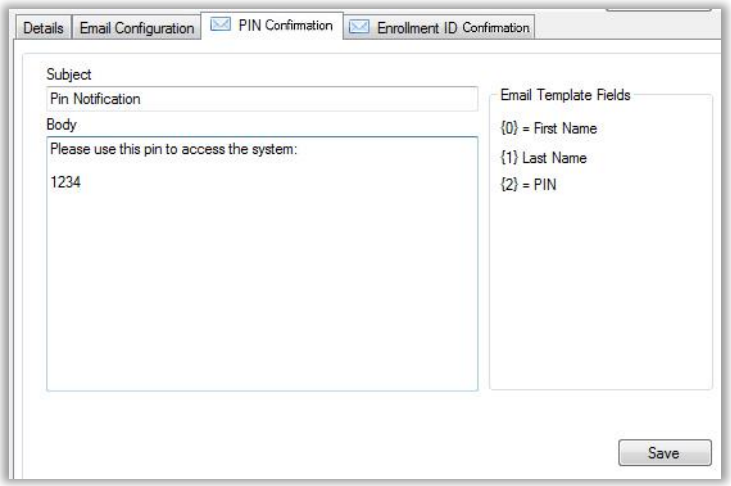
NOTE: By default, the email field is set to 'Field 6'. This can be customised by editing the 11 definable User Fields within Traka Web.

4. Complete the '**Subject**' and '**Body**' fields as required.
5. Click on '**Save**'.

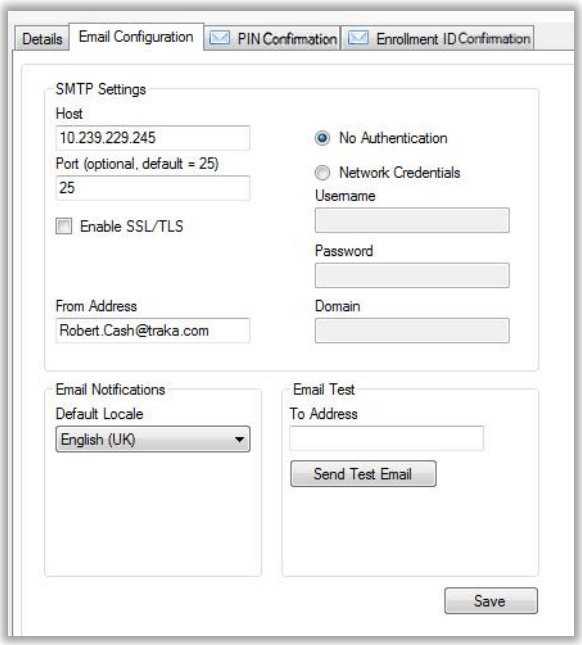


NOTE: If you only wish to send a PIN Confirmation you are still required tick the box for 'Enable User Enrolment Emails' within the 'Enrolment ID Confirmation' tab.

6. Click on the '**PIN Confirmation Tab**'.
7. Complete the '**Subject**' and '**Body**' fields as required.
8. Click on '**Save**'.



9. Click on the '**Email Configuration**' tab.



10. This window allows you to configure the SMTP Settings.

SMTP Settings

Host
Input the host name of your Email Server.

Port
Enter the TCP port number that your SMTP email server accepts messages on. You should set this to 25 unless you use a non-standard port number.

Enable SSL/TSL
Enable this option to encrypt messages between the Business Engine and Email Server.

NOTE: You may need to change the port number from the default 25 for this to work.

From Address

Enter the email address which email notifications should appear from.

No Authentication
By selecting this option, no SMTP authentication will be used.

Network Credentials
This will cause the Business Engine to authenticate to the named SMTP server using the supplied credentials.

Email Notifications

Default Locale
Select the appropriate language locale. This will translate text within the email to the selected language.

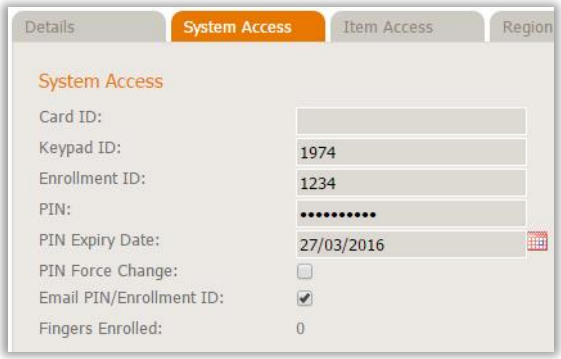
Email Test

To Address
You can test the SMTP settings that have been entered by putting an email address in the 'To' field and clicking the Send Test Email button.

11. The PIN & Enrolment ID Notification tabs allow you to enter a subject and message template that will be the content for every email sent to a user.

5.2 TRAKA WEB SETUP

12. Log into Traka Web.
13. Navigate to the user list.
14. Highlight the desired user and click the edit button.
15. Select the System Access tab. A tick box named **Email PIN/Enrolment ID** will now be visible.
16. Enter the appropriate details i.e. a PIN or Enrolment ID. Then select the save button.



17. Traka Web will now send an email to the user stating their PIN and/or Enrolment ID.

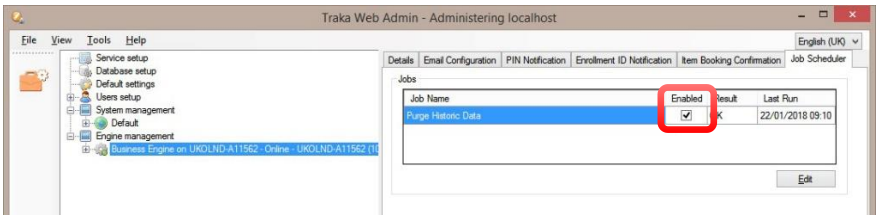
The next time the user is edited the Email Pin check box will not be checked and must be checked and saved again if you wish to send another email.

5.3 TRAKA WEB ADMIN JOB SCHEDULER

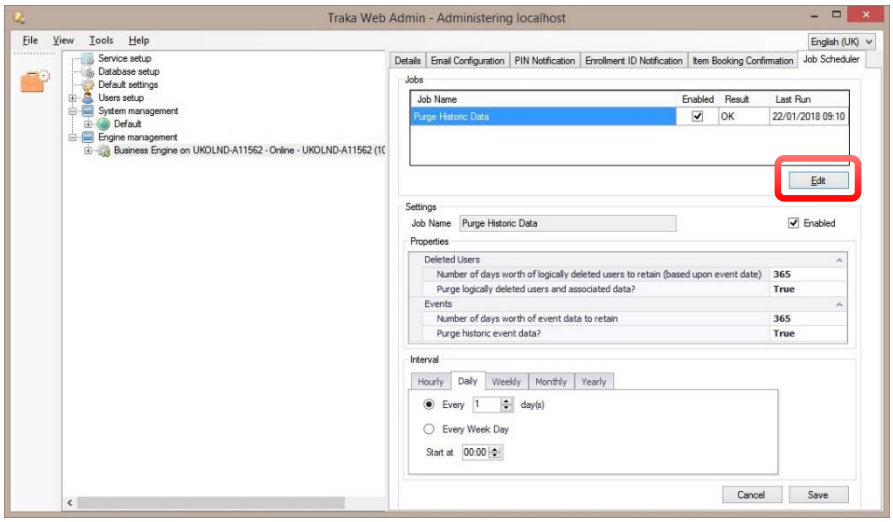
Within the Traka Web Admin App, it is possible to configure a Job Scheduler. This will make it possible to clear data from the system at specific times which can be enabled by the System Administrator.

The tab for the job scheduler is located by selecting the Business Engine. By default each job schedule will be disabled.

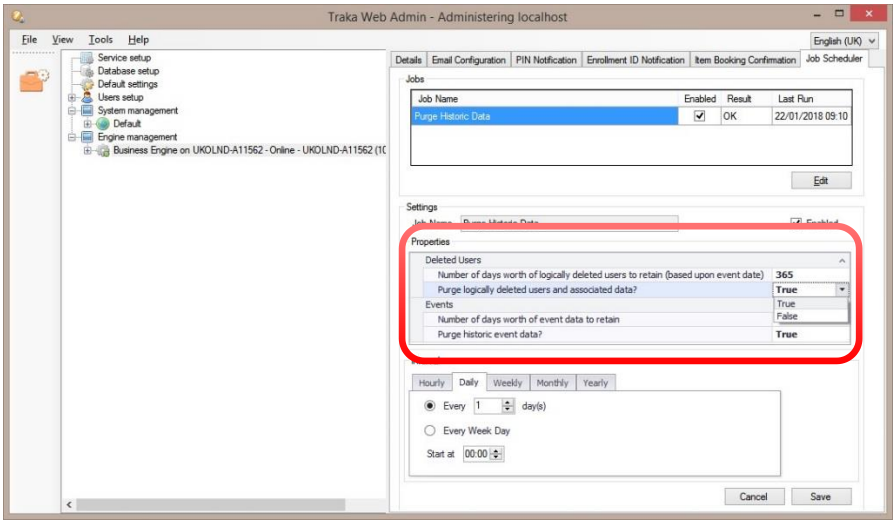
1. Select the **Business Engine** followed by the **Job Scheduler** tab. In the Jobs window, select the **Enabled** check box for the specific job to be activated.



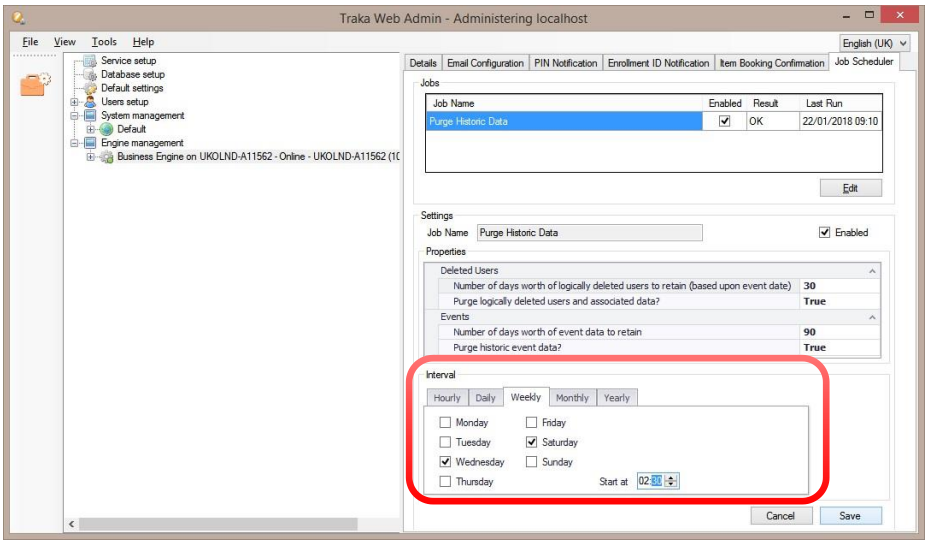
2. Clicking on the **Edit** button will enable you to change the parameters for the selected Jobs



3. Within the Properties box, change the setting to **True** to enable the parameter.



4. The lower box will allow you to change the interval for when you wish the Schedule to be run.



5. Once complete, click the **Save** button.

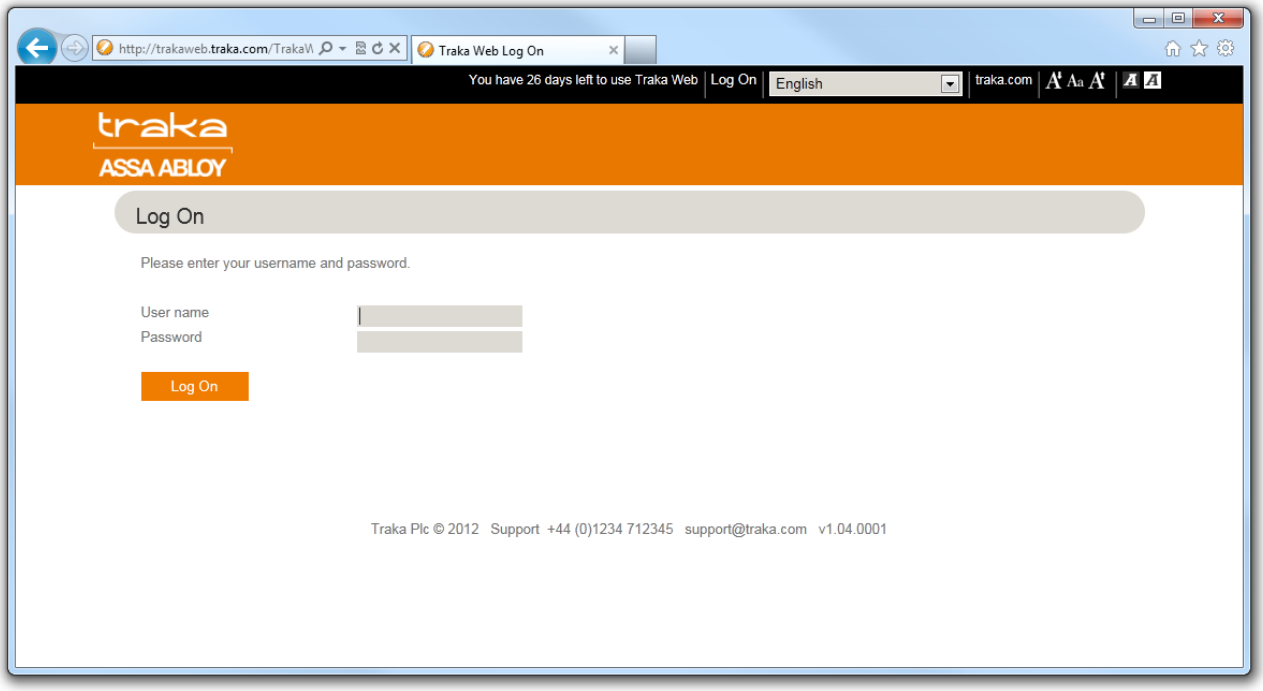
6. USING TRAKA WEB

You should now be able to login to the Traka Web Front End using the System Administration account that you set up in section **4.2.1.1**.

Navigate to your Traka Web URL (http://*servername*/TrakaWeb) and you should see the login page as shown below.

For basic authentication, simply type in your username and password, and click Log On.

If you are using windows authentication you should be logged in automatically as long you are already logged into your workstation as the windows user associated with your super administration account as setup in section **4.2.1.1**.

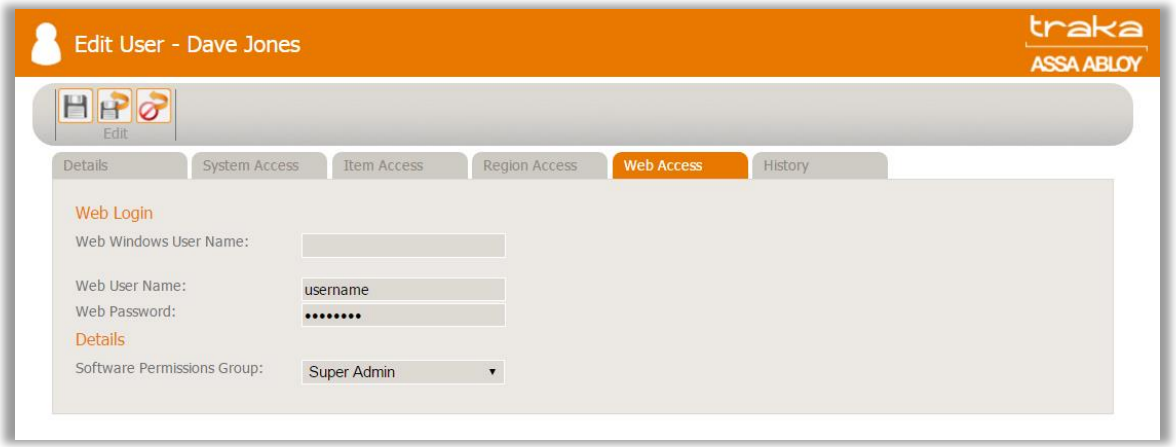


Once logged into the system you should consult the Traka Web User guide for further help in using the Traka Web Software.

6.1 BASIC AUTHENTICATION

While using basic authentication your Traka Web users will be prompted for their username and password via the Traka Web Front End login page. Users are given a username and password on the Edit User page in the Software Access tab.

The Software User Name and Software Password fields should be completed for each user that you wish to log on to the Traka Web Front End Web Site.



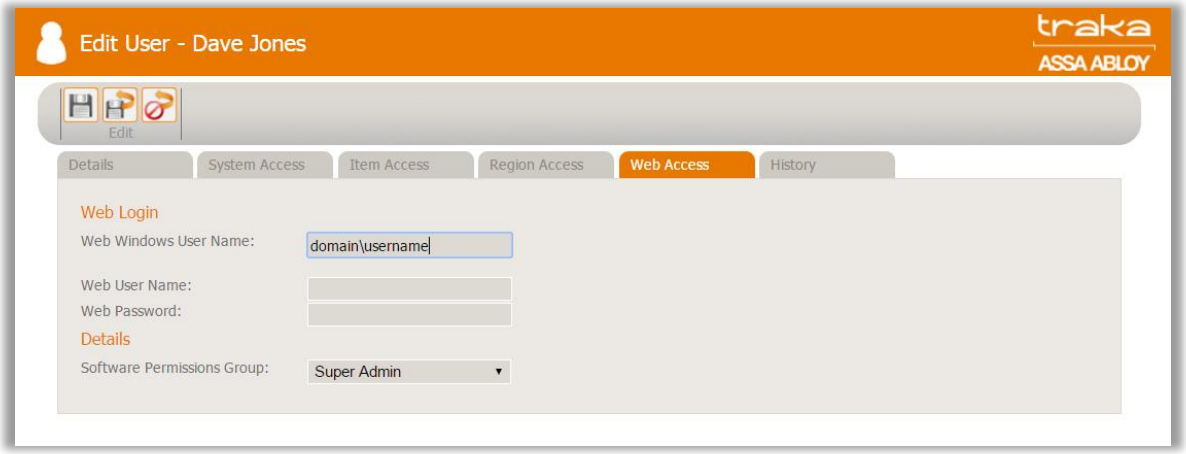
6.2 WINDOWS AUTHENTICATION

While using Windows Authentication, Traka Web Front End will authenticate users against their Windows credentials for the current Windows user. Users on Traka Web are associated with Windows credentials (as above). The Software Windows User Name should be completed for each user that you wish to login to the Traka Web Front End Web Site.

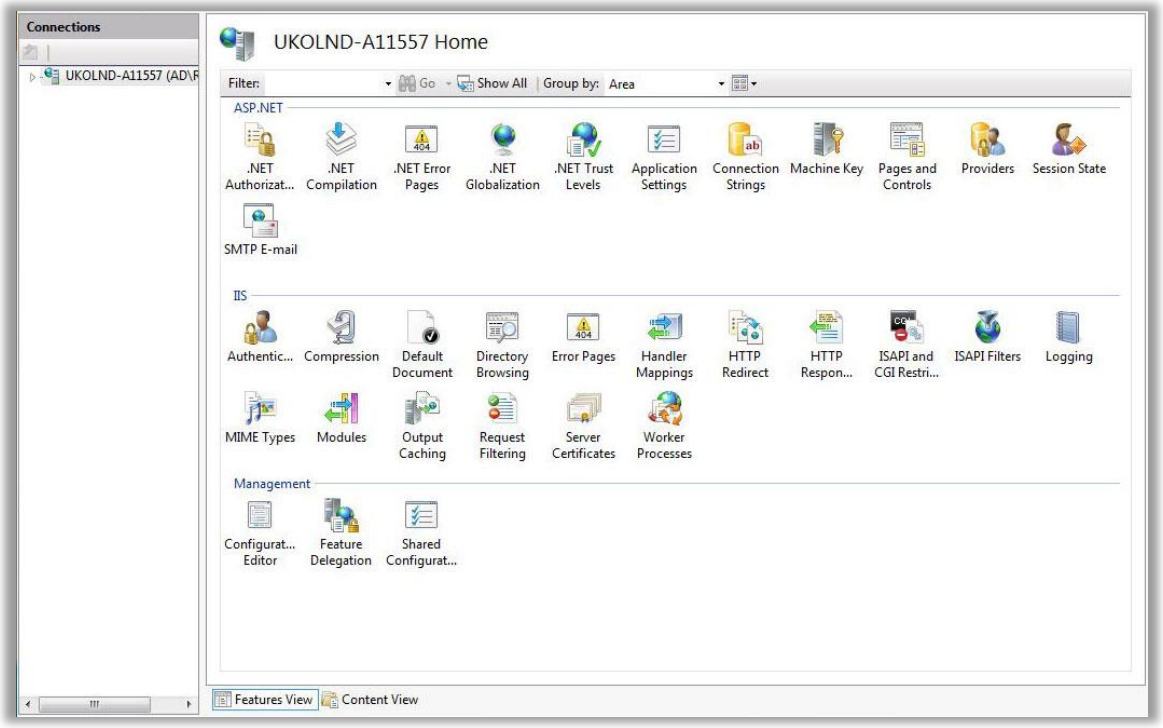
6.2.1 CONFIGURE WINDOWS AUTHENTICATION THROUGH IIS

If your Traka Web Front end has been set up with Basic Authentication and you wish to configure it using Windows Authentication, there are 2 solutions: You can simply uninstall Traka Web Front End and reinstall using the Windows Authentication option or you can change the configuration through the Internet Information Services (IIS) as follows.

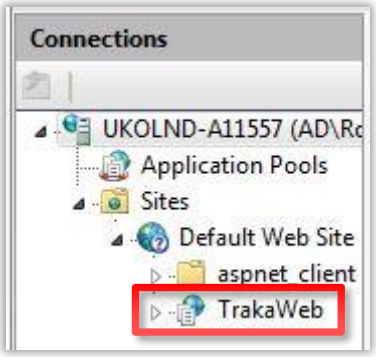
Note: If you are configuring Windows Authentication through IIS, it is important that at least 1 admin user has already been setup within Traka Web, User Web Access with their correct domain credentials otherwise Traka Web cannot be accessed.



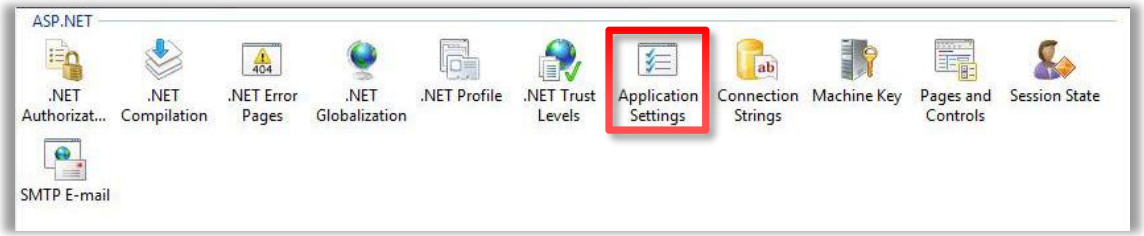
1. Open the Internet Information Services (IIS) Manager.



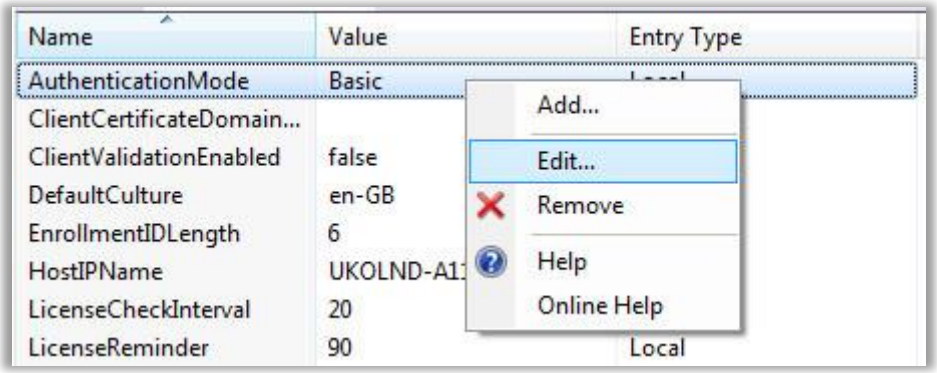
2. In the left window, expand the tree to the Traka Web level and select it.



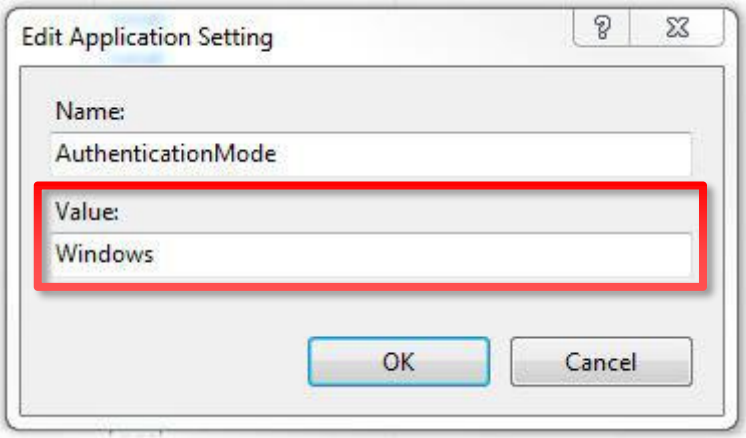
3. In the main window under ASP.NET, double click on the **Application Settings** icon.



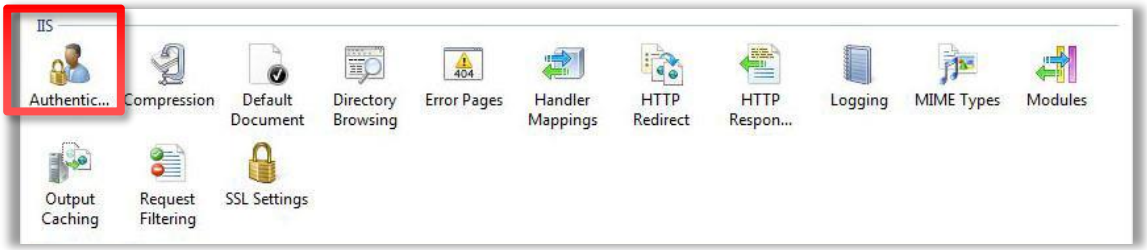
4. A new window will appear. At the top of the list, right click on **AuthenticationMode** and select **Edit**.



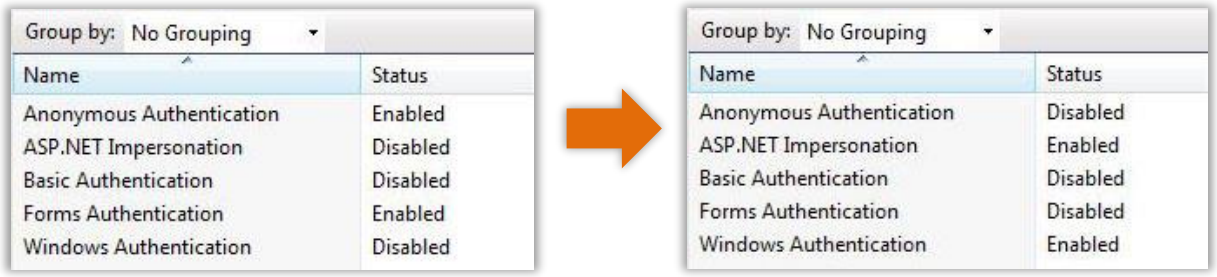
5. The Value field will currently be set to **Basic**. You will need to manually change this to **Windows** to allow for Windows Authentication. When complete, click on **OK**.



6. Click on the Back arrow to return to the main screen.
7. Under the IIS section of the main screen, double click on the **Authentication** icon.



8. A new window will appear displaying the current Status settings. Right click on the Status settings to **Enable** or **Disable** as shown below.



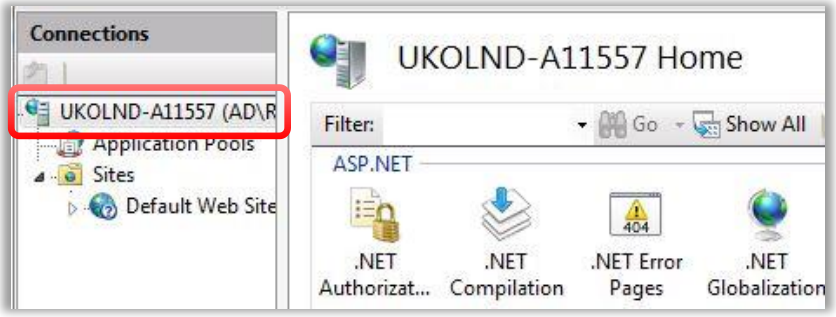
9. Close the IIS Manager and launch Traka Web. All users with Windows Authentication will automatically log in.

6.3 ACCESSING TRAKA WEB OVER HTTPS WITH AN SSL CERTIFICATE

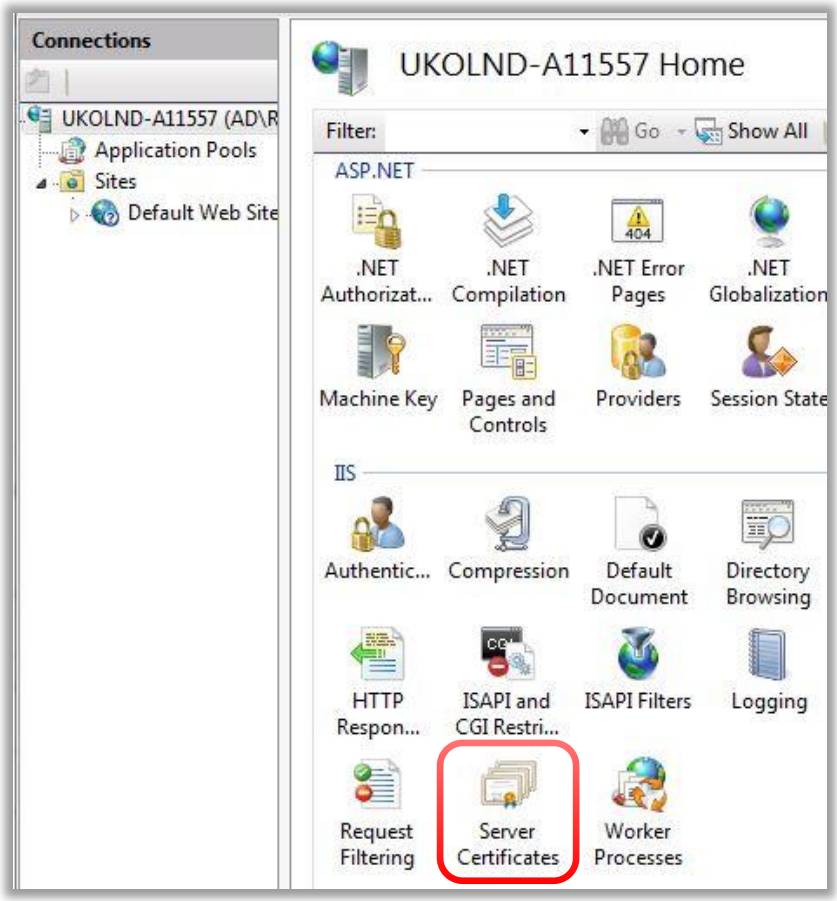
6.3.1 SELF-SIGNED CERTIFICATES

For testing purposes it is possible to create a Self-Signed Certificate. This will not be valid in live installations as the certificate has not been verified in the 'Trusted Root Certification Authorities' store. It will however indicate if your site is functioning via https.

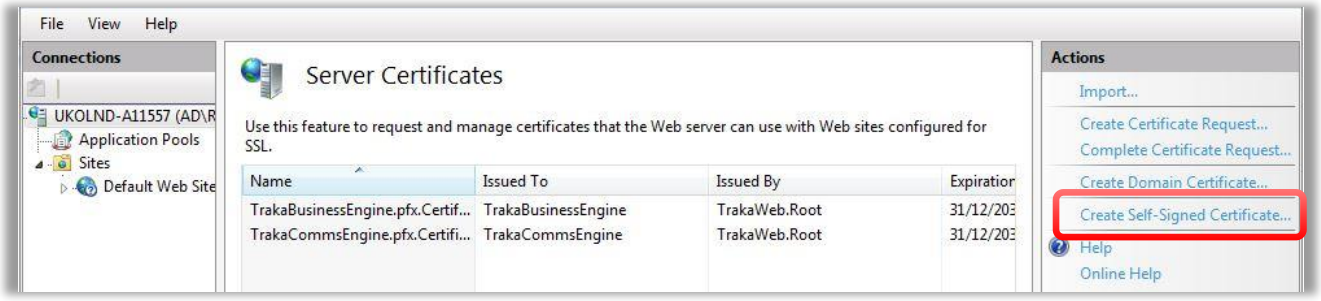
1. Open **IIS Manager** and select your server from the left side of the window.



2. In the **IIS** section in the main window, double-click on **Server Certificates**.



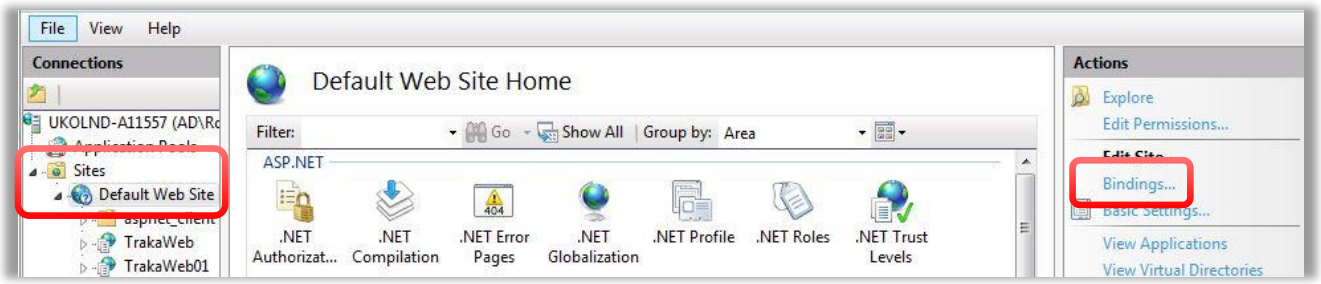
3. Now click on **'Create Self-Signed Certificate...'**



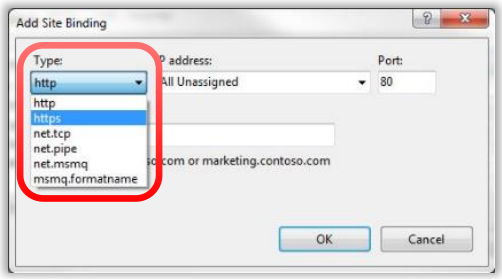
4. Choose a name for the certificate (something easy to remember) and leave the drop-down as **Personal** and click **OK**.

6.3.2 BINDINGS

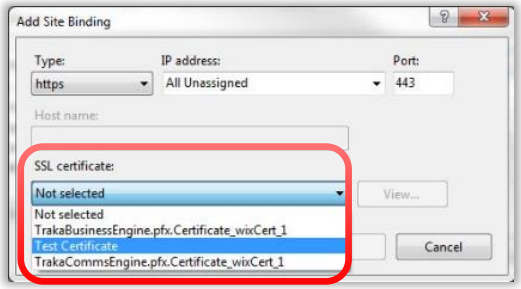
1. In the Sites section located in the left window, select **Default Web Site** and then click on **Bindings** from within the window to the right.



2. Click **Add** and then change the **Type** drop-down to **https**.



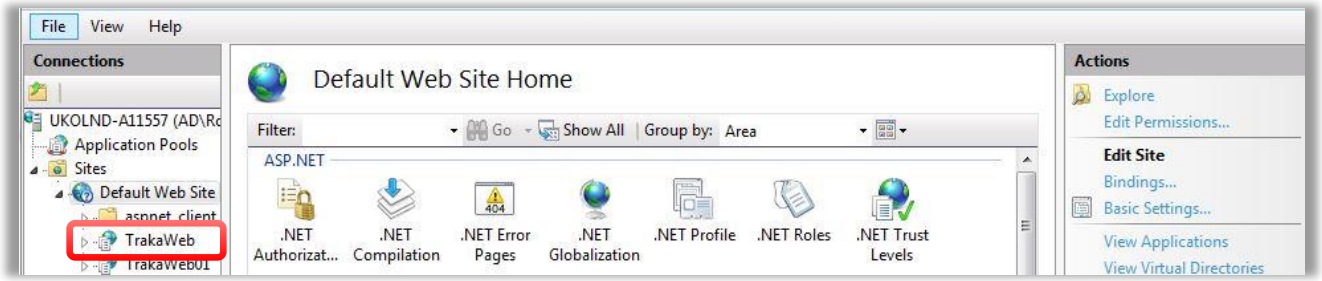
3. Next, select your certificate from the **SSL certificate**: drop-down and then click **OK**.



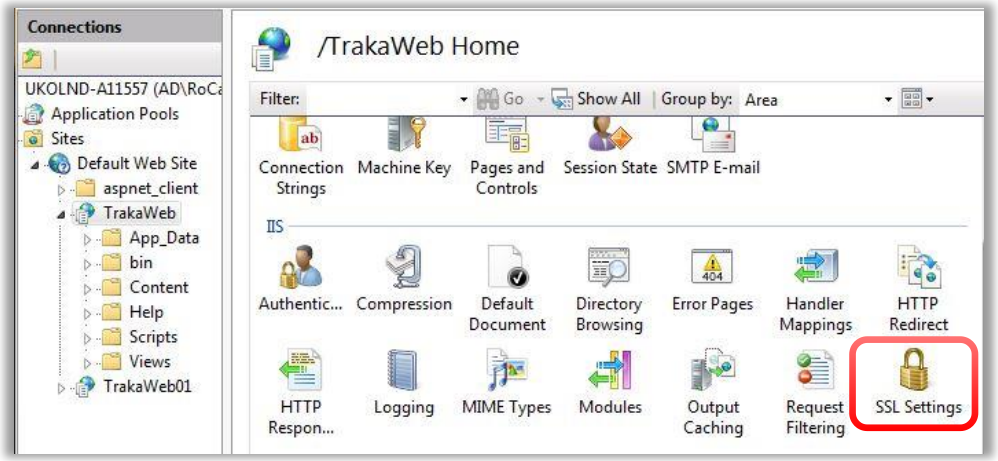
NOTE: A self-signed certificate is ok for testing. However if a customer intends to make their Traka Web install live using SSL they will need an official certificate for this section.

6.3.3 ENABLE SSL ON THE TRAKAWEB SITE

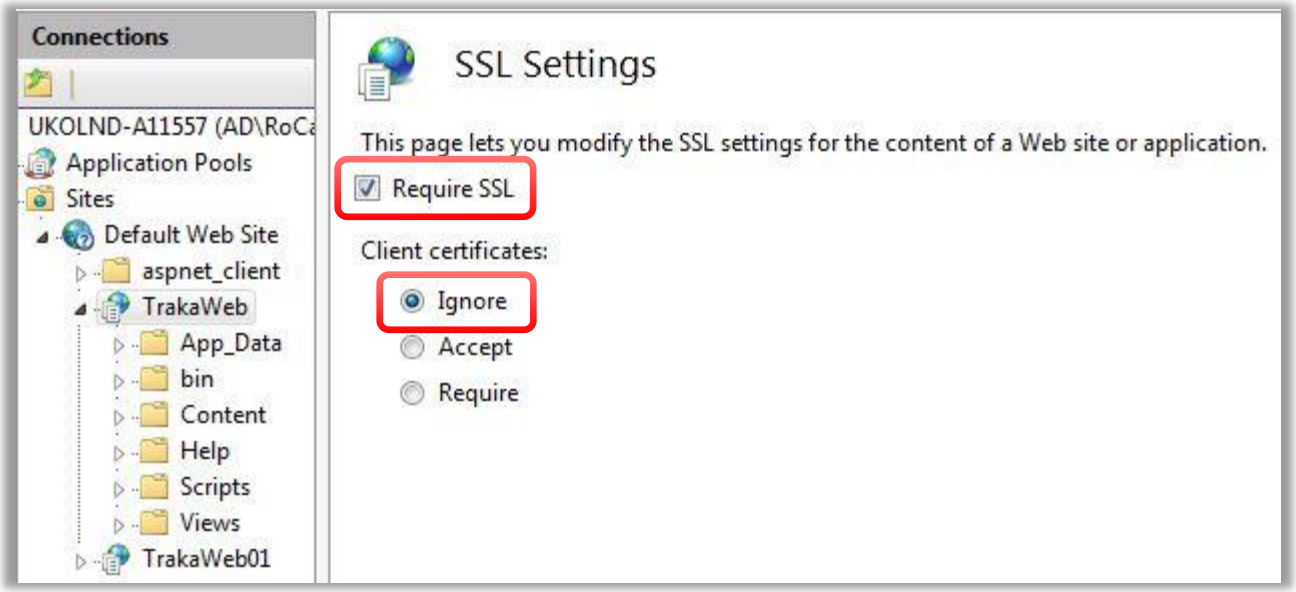
1. Select the **TrakaWeb** section from the window to the left.



2. Next, double click on the **SSL Settings** icon in the main window.



3. Tick the **Require SSL** checkbox and select whether to Ignore, Accept or Require Client Certificates. For this purpose we will choose **Ignore**. Click **Apply** to save the changes.



6.3.4 CONFIRM SSL IS ACTIVE

If you are using a self-signed certificate, the web browser will display a warning that the site is not secure. This can be rectified by adding an exception to the browser so that you may continue.

When using approved certification, the warning will not be displayed. The search bar will also display a padlock icon showing that the site is secure.

7. UPGRADING AN EXISTING TRAKA WEB INSTALLATION

If you already have any of the Traka Web software components installed, please use "Add / Remove Programs" or "Programs and Features" found in the Control Panel to remove all of the components of Traka Web including the associated security certificates.

Install the new version of Traka Web familiarising yourself with the installation process for each software component described in section **2** above.

7.1 UPGRADING THE TRAKA WEB FRONT END AND ADMIN APPLICATIONS

PLEASE NOTE: Upgrading the Traka Web Front End will overwrite the installed "web.config" XML Configuration file where the 'Default Culture' is set. Therefore, if the Traka Web installation is not installed as English (GB), then after the upgrade the Default Culture will need to be setup again as per step 14 of section 3.1.

7.2 UPGRADING THE BUSINESS ENGINE AND COMMS ENGINE SERVICES

It is recommended that you stop the relevant service (Business Engine or Comms Engine) prior to upgrading.

You should do this from the 'Services' icon, located within 'Administrative Tools' in the Control Panel (Control Panel/System and Security for Windows 7 & 8), or run 'services.msc'. Right click and choose Stop to disable the service and then run the installer to perform an upgrade.

~~7.4~~7.3 UPGRADING SECURITY CERTIFICATES

Before upgrading any of the security certificates, any previous versions must be uninstalled. Locate All Programs via the Control Panel to uninstall the Security Certificates.

~~7.5~~7.4 UPDATING THE DATABASE

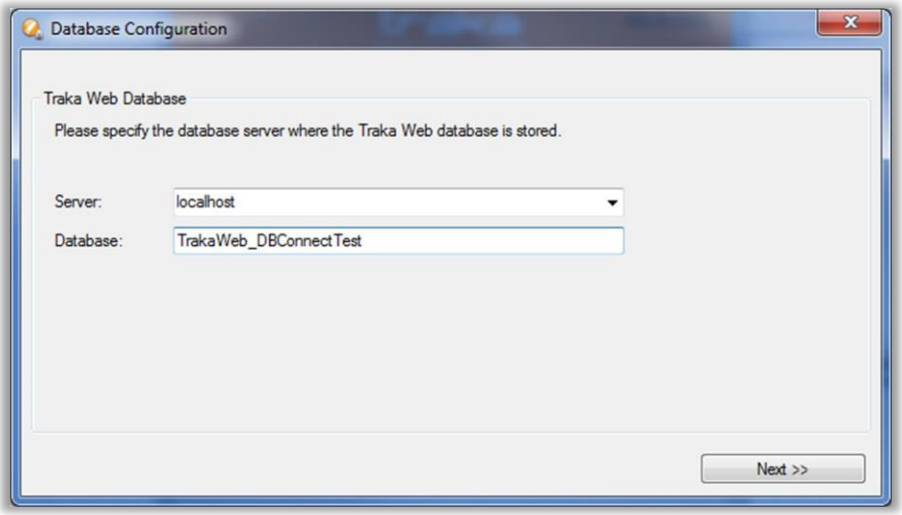
The following section details the process of updating the Traka Web database after an upgrade of the Traka Web software has been installed onto an existing database.

NOTE: You should ensure that your current database has been backed up before continuing.

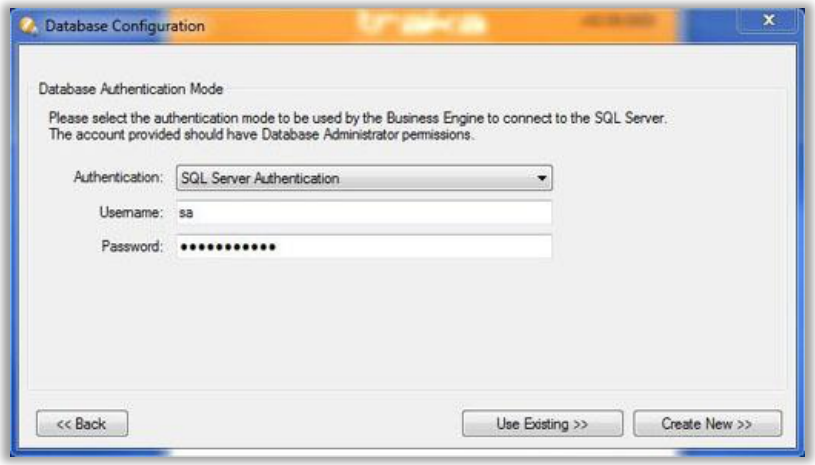
~~7.5.1~~7.4.1 UPDATING THE DATABASE

1. After completing the software upgrade, restart the Traka Business Engine Service and the Traka Comms Engine Service and then launch the Traka Web Admin application as normal.

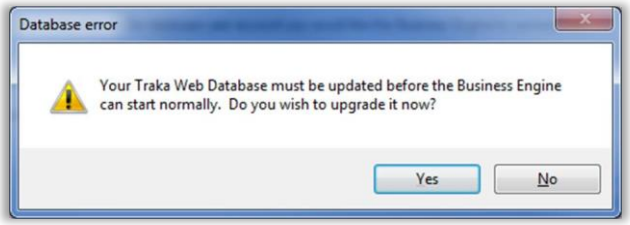
2. You will first be required to enter the Server and Database Details as shown below. Click '**Next**' to continue.



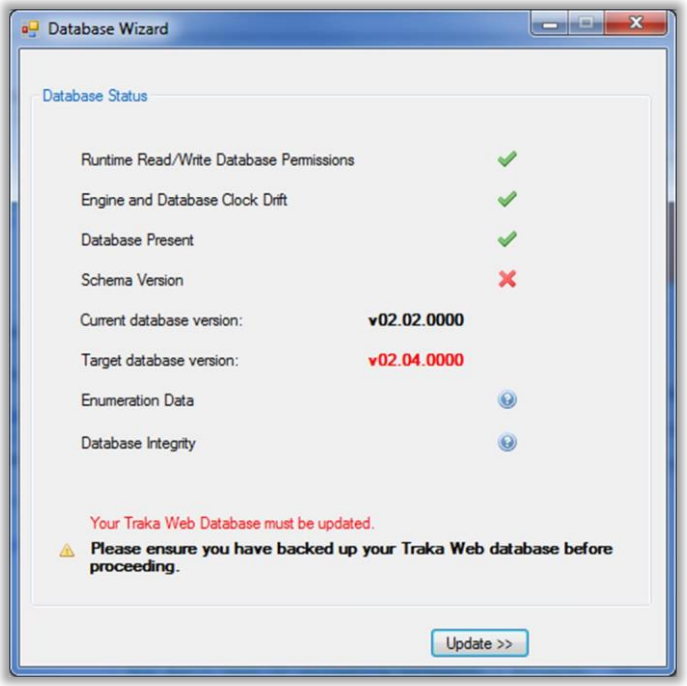
3. A window will appear requiring your Database Administrator Credentials. You may either choose '**Use Existing**' if connecting to an existing database or '**Create New**'.



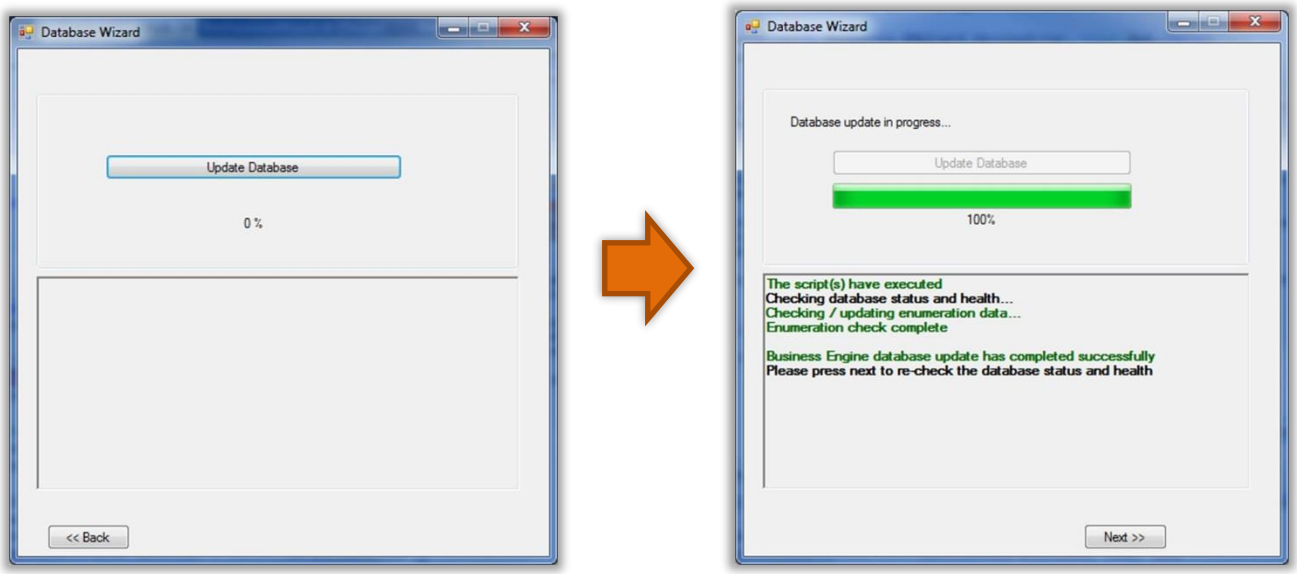
4. A Database error message will appear, click '**Yes**' to proceed.



5. The Database Wizard window will appear which provides information regarding the current 'Database Status'. The 'Target Database Version' is shown in red text. Click on the '**Update**' button to continue.

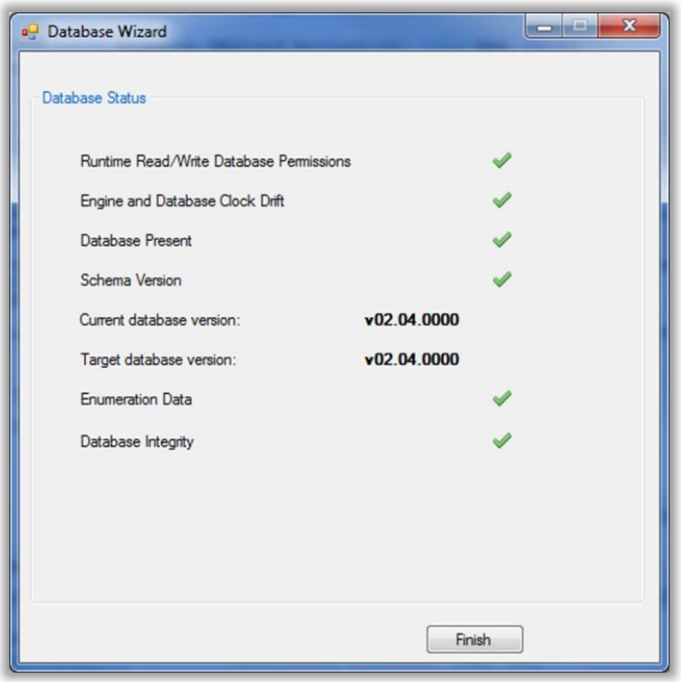


6. Click on the '**Update Database**' button. The '**Database Wizard**' will now install the update and perform any necessary checks prior to completion. Once the update has completed, click on the '**Next**' button.



7. The 'Database Wizard' will show an updated 'Database Status' as shown below. Click on the '**Finish**' button to return to the 'Traka Web Admin' connection screen.

~~7.5.2~~7.4.2 COMPLETING THE DATABASE UPDATE

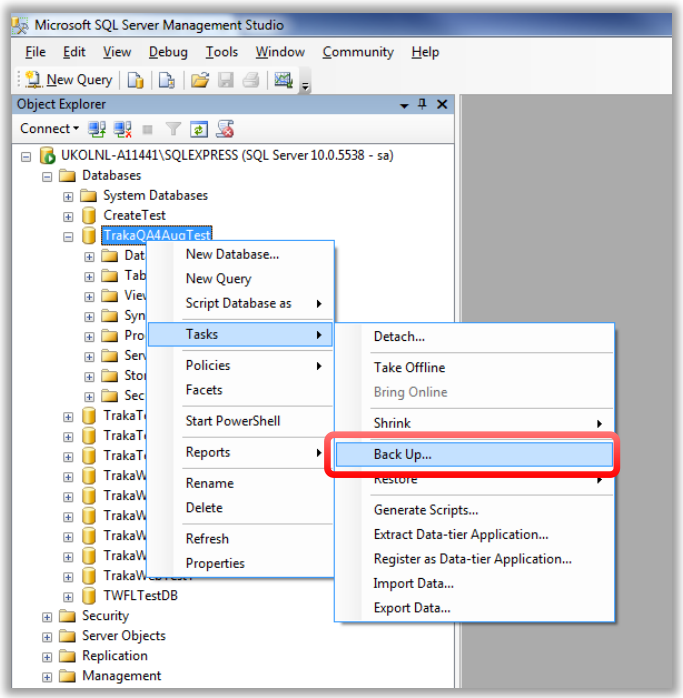


1. Unless you wish to make any changes within Traka Web Admin, close the window and continue to use Traka Web as normal.

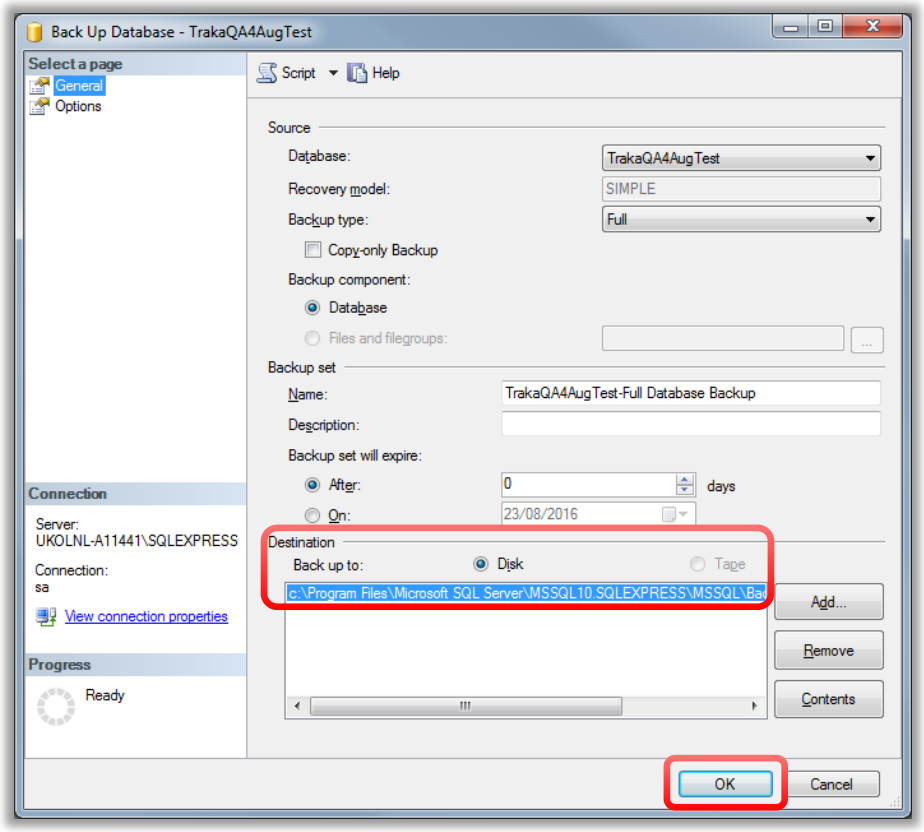
8. TRANSFER A TRAKA WEB DATABASE TO A NEW SERVER

The following procedure outlines the process required to transfer an existing Traka Web database to a new server.

1. Start SQL Server Management Studio on the current server and select the database to be backed up. Right click on the specific database and go into Tasks -> **'Back Up'**.

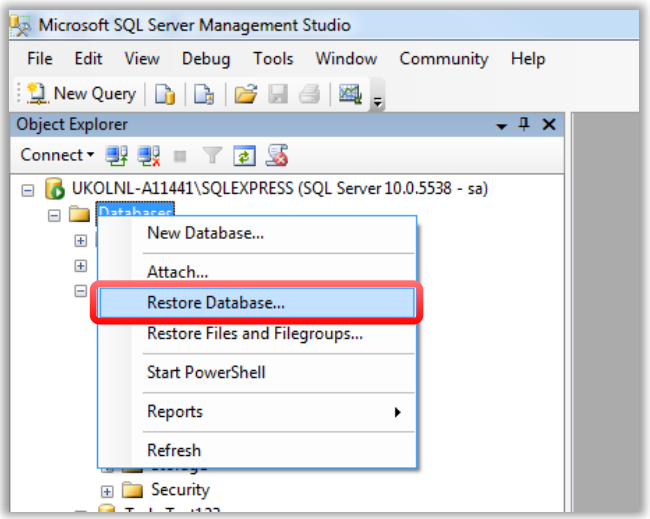


2. The following pop up window will be displayed. Here you can choose the location where you want to back up the database. This would ideally be an external drive of some sort with the intention of transferring the database to another server. Press **'OK'**.



Now you can open SQL Management Studio on the server you wish to move the database to.

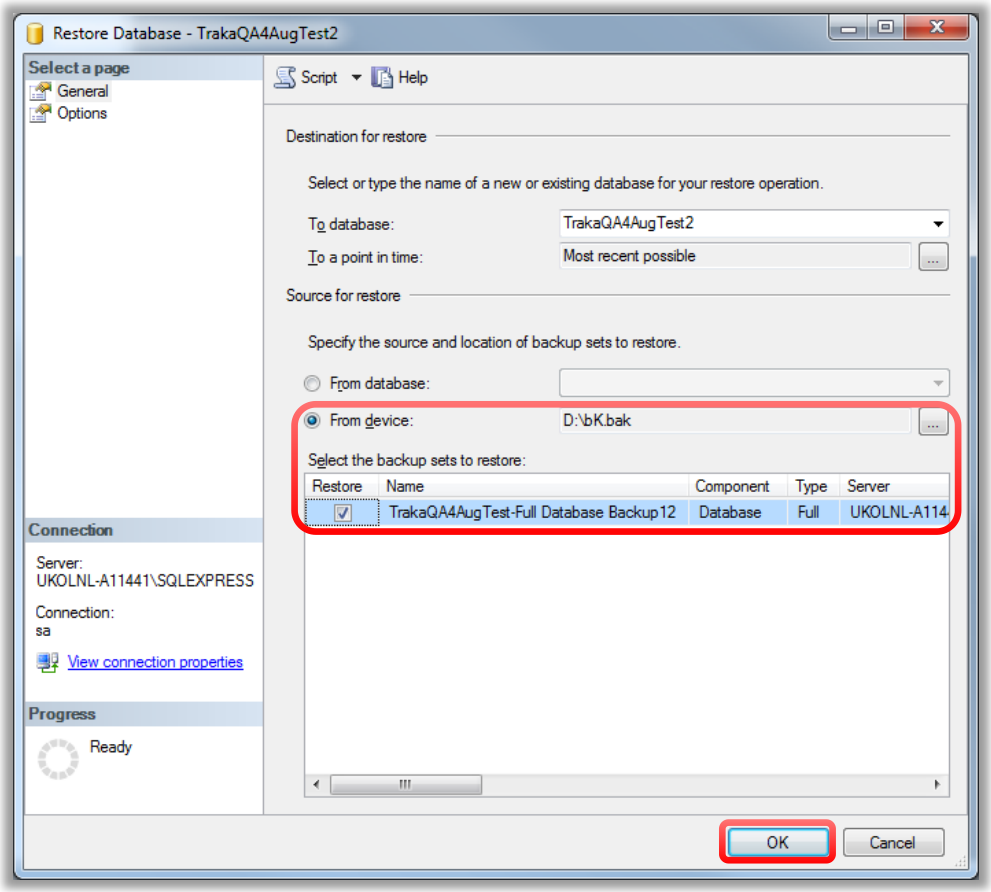
3. Right click on the Databases tab to allow the restoration of the database.



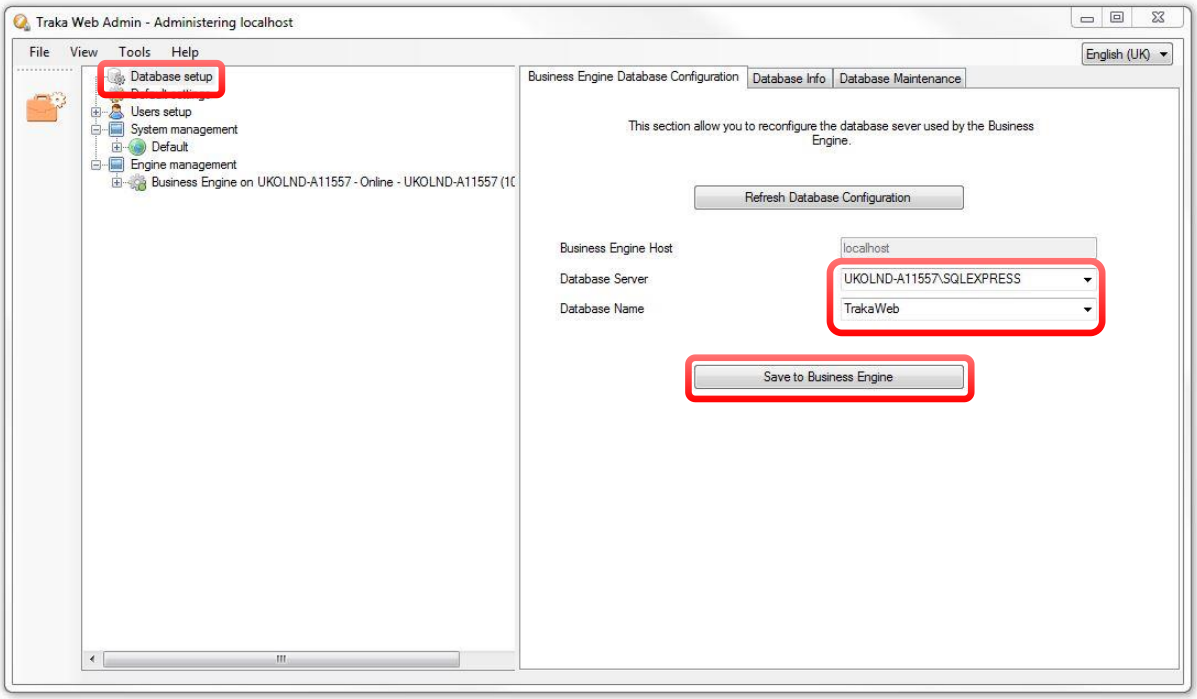
4. A new window will be displayed to the user where the option is given to choose which database the restore should be mapped to. In this case, type a new name for an unused database on the server.

5. Most likely the database would be coming from an external source such as an external drive, therefor 'From device' should be selected in order to navigate to the server to import.

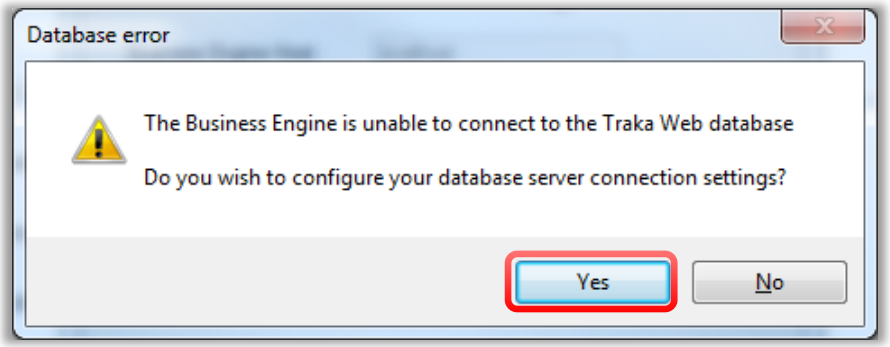
6. The backup set should be shown at this point and the user can select the specific version to restore. Press **'OK'**.



7. Go into the Database Setup tab in Traka Web Admin and change the database server and name to match the names to the newly moved server and database name. Now select 'Save to Business Engine'.



8. A message will be displayed asking you to configure the database due to the change, select **'Yes'**.



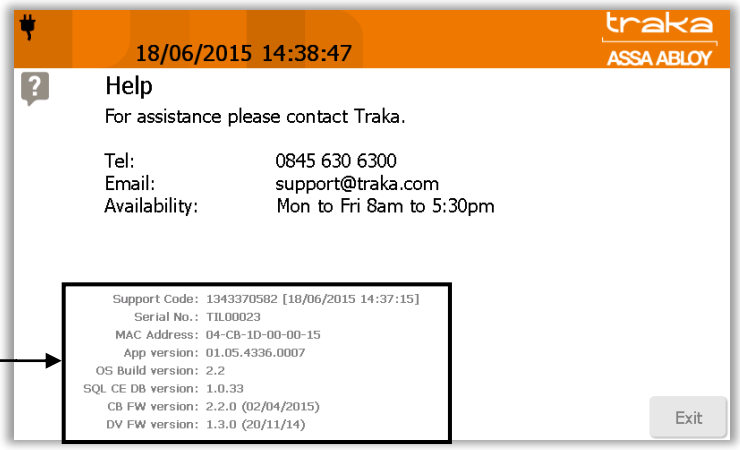
9. Continue through the Wizard and enter the DB Server 'sa' equivalent credentials.

The wizard should bring the database online correctly.

9. TECHNICAL SUPPORT

If you need to contact Traka/distributor for technical support, navigate to the Help section at the main screen and provide the following details:-

- Support Code
- Serial Number
- App Version
- SQL CE DB Version
- CB FW Version
- DV FW Version



Technical Support Information

Telephone: **0333 355 3641** (from inside the UK)

Telephone: **+44 333 355 3641** (from outside the UK)

Email: **support@traka.com**

Web: **support.traka.com**