

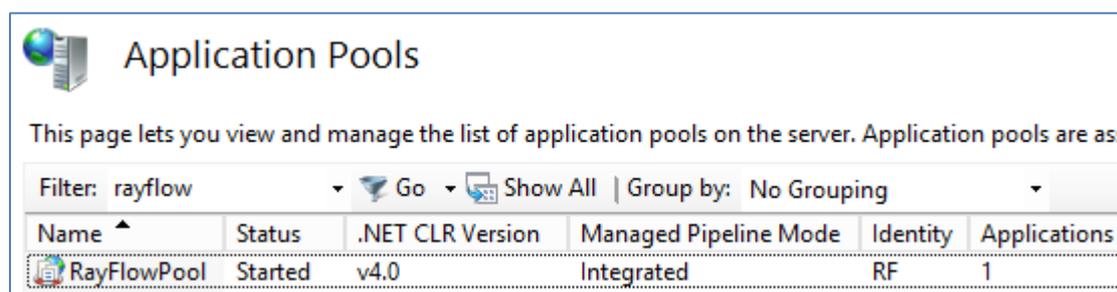
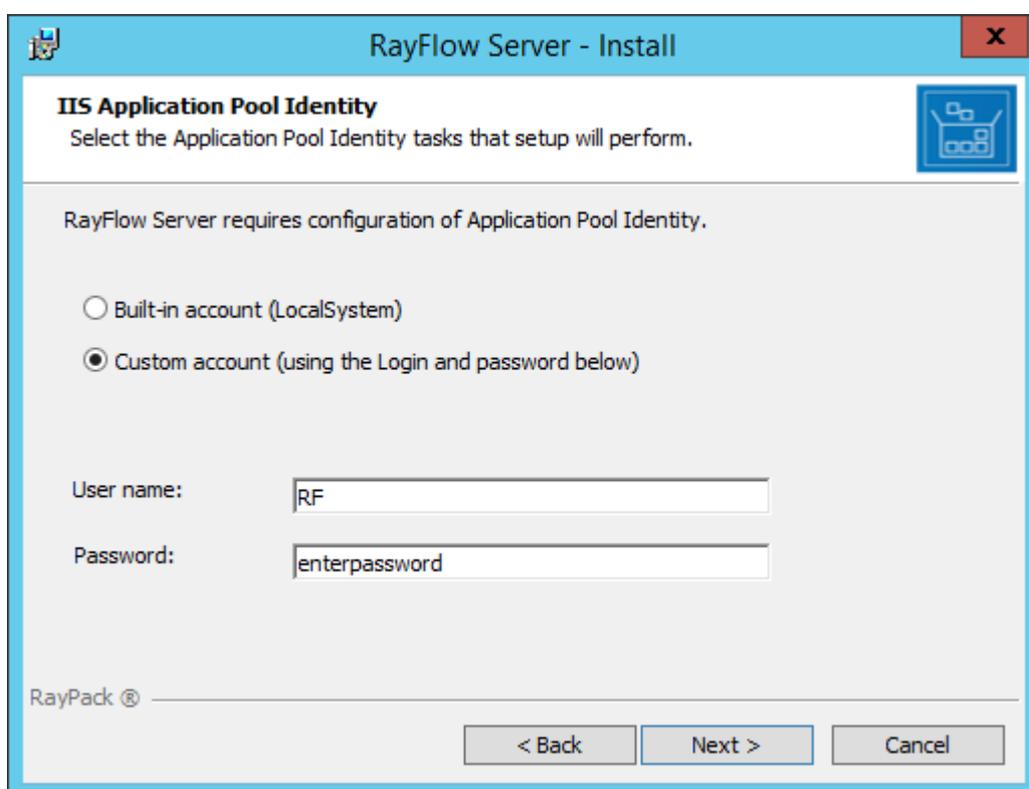
How to secure the RayFlow Server

Application Pool Identity

The default identity for the RayFlow Application Pool is LocalSystem; however, to increase security it is recommended to use a local user account instead.

If either certain application folders or the SQL Server will reside on a different server, then this local user (including its password) can be created on the additional servers, or, a domain user can be used for the Application Pool identity instead.

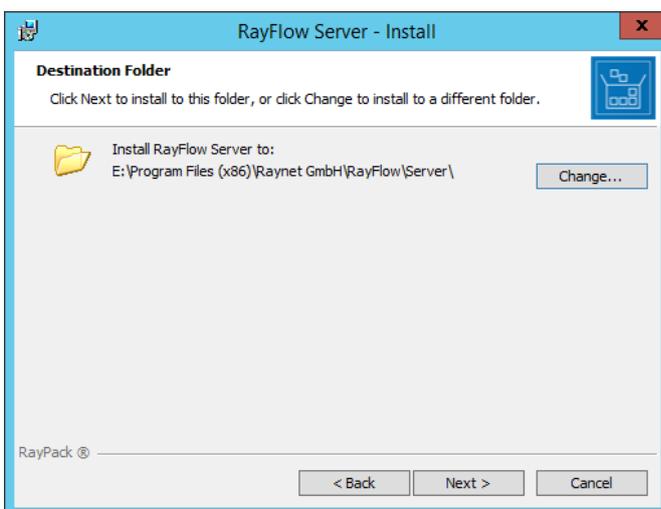
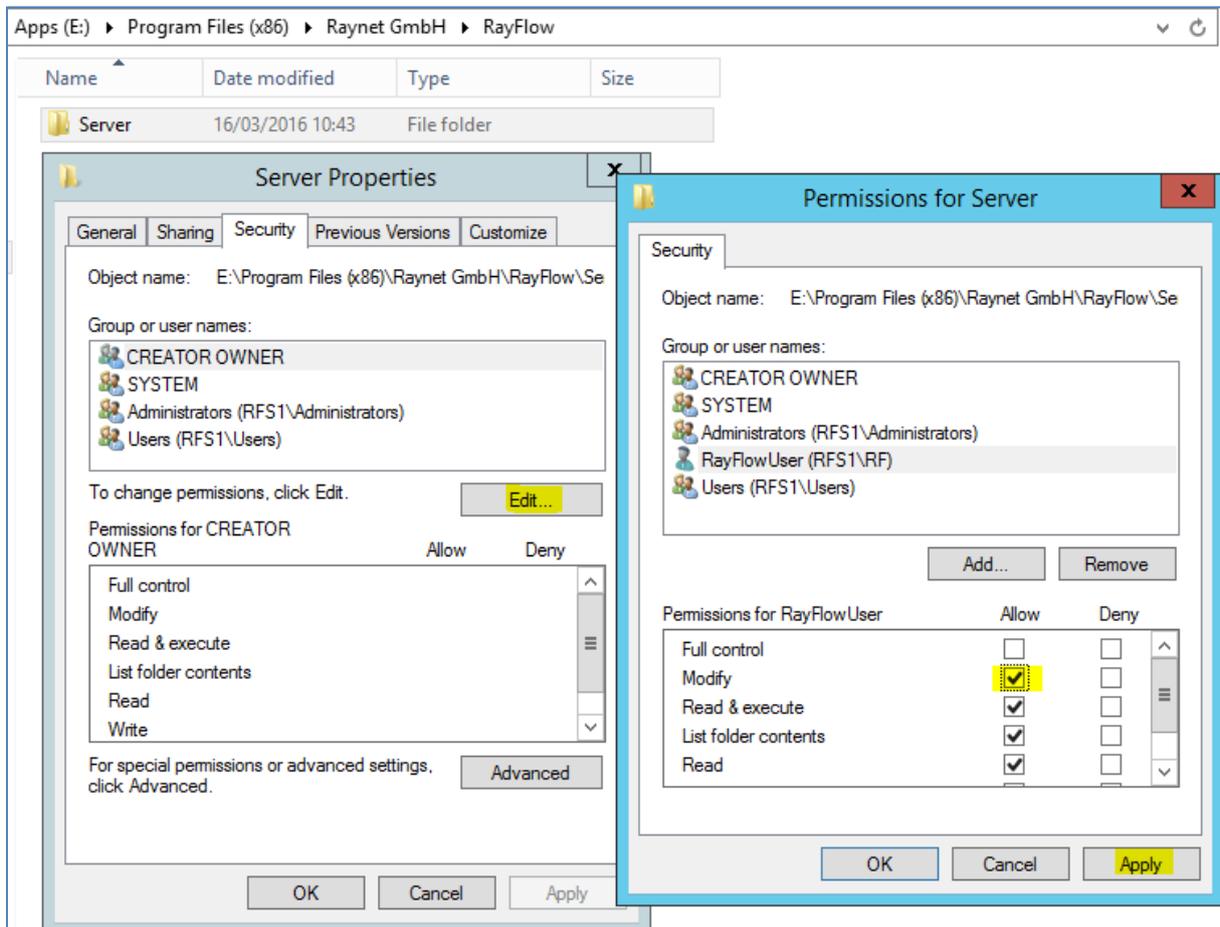
This restricted identity can be specified during the MSI installation:



NTFS Permissions

The RayFlow IIS Application Pool's identity requires the Modify permission to the RayFlow Server product's installation directory.

This can be achieved by creating the installation directory and assigning that permission to the relevant user before running the MSI routine.

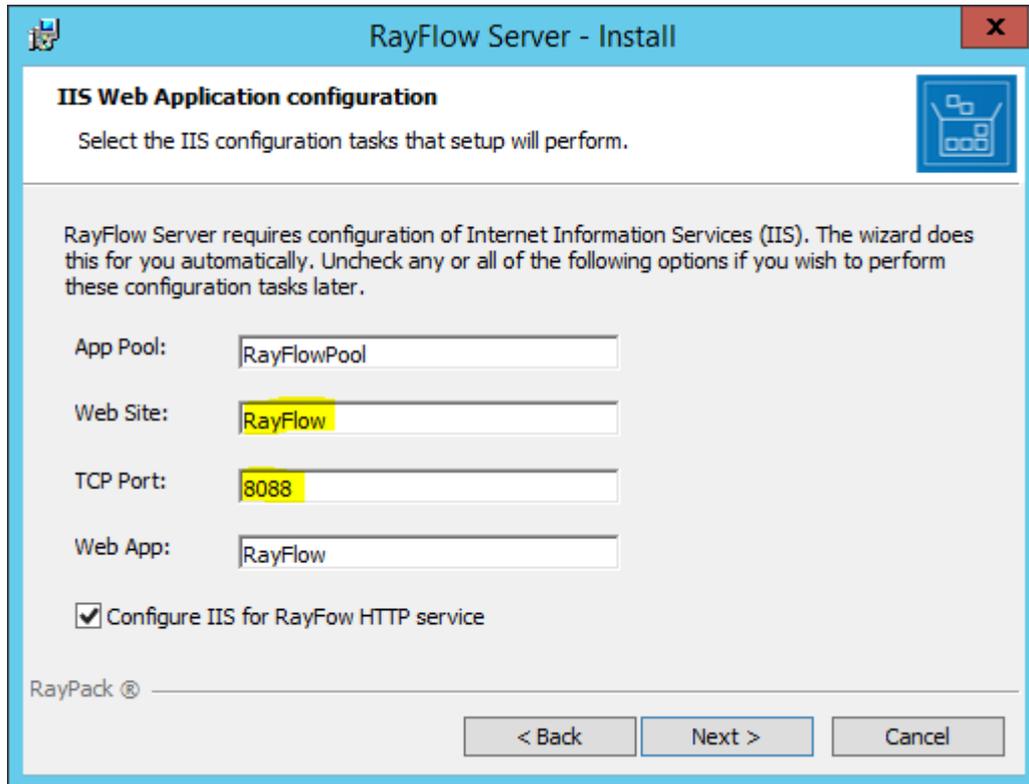


As all temporary file creation actions take place within the RayFlow IIS Application Pool's identity's temp directory, it is recommended to change that user's TEMP & TMP environment variables to target a different drive instead of its default C: drive location.

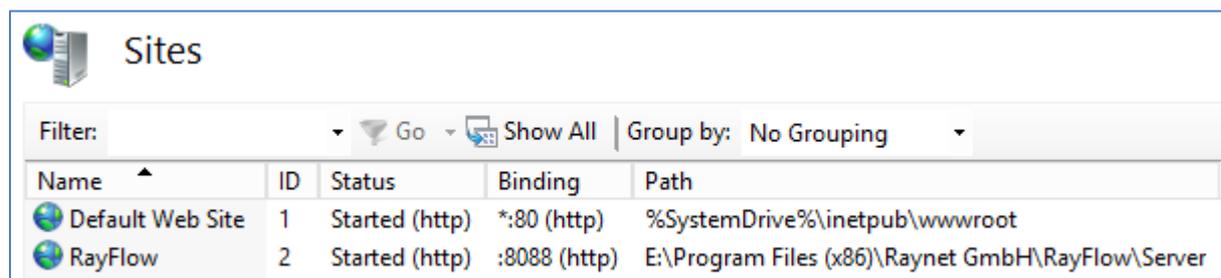
IIS Web Application

Choosing a non-default port number for the web application will cause the MSI installation to create a new web site for the RayFlow Server instead of an application object.

If an application object is required, then use the default port number and then configure IIS after the installation has been completed.



The screenshot shows the 'RayFlow Server - Install' wizard window. The title bar reads 'RayFlow Server - Install'. The main window has a blue header with the title and a close button. Below the header, the title 'IIS Web Application configuration' is displayed, followed by the instruction 'Select the IIS configuration tasks that setup will perform.' and a blue icon of a server rack. A paragraph explains: 'RayFlow Server requires configuration of Internet Information Services (IIS). The wizard does this for you automatically. Uncheck any or all of the following options if you wish to perform these configuration tasks later.' Below this, there are four input fields: 'App Pool:' with 'RayFlowPool', 'Web Site:' with 'RayFlow', 'TCP Port:' with '8088', and 'Web App:' with 'RayFlow'. A checkbox labeled 'Configure IIS for RayFlow HTTP service' is checked. At the bottom left is 'RayPack ©' and at the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.



The screenshot shows the 'Sites' view in IIS Manager. It features a filter bar with 'Filter:', 'Go', 'Show All', and 'Group by: No Grouping'. Below is a table with the following data:

Name	ID	Status	Binding	Path
Default Web Site	1	Started (http)	*:80 (http)	%SystemDrive%\inetpub\wwwroot
RayFlow	2	Started (http)	:8088 (http)	E:\Program Files (x86)\Raynet GmbH\RayFlow\Server

HTTPS

To implement HTTPS, you can either create a self-signed TLS certificate via the RayFlow web site itself, or utilise a TLS certificate from an internal or external Certificate Authority.

Database

Create a SQL Server Security Login for the RayFlow Application Pool's identity with the following settings (the default options have not been highlighted), so that a Security User is created within the RayFlow database:

Login - New

Select a page: General, Server Roles, User Mapping, Securables, Status

Script Help

Login name: RFS1\RF Search...

Windows authentication
 SQL Server authentication

Password:
Confirm password:
 Specify old password
Old password:

Enforce password policy
 Enforce password expiration
 User must change password at next login

Mapped to certificate
 Mapped to asymmetric key
 Map to Credential Add

Mapped Credentials

Credential	Provider
------------	----------

Remove

Default database: RayFlow
Default language: <default>

OK Cancel

Connection
Server: RFS1
Connection: RFS1\Administrator
[View connection properties](#)

Progress
Ready

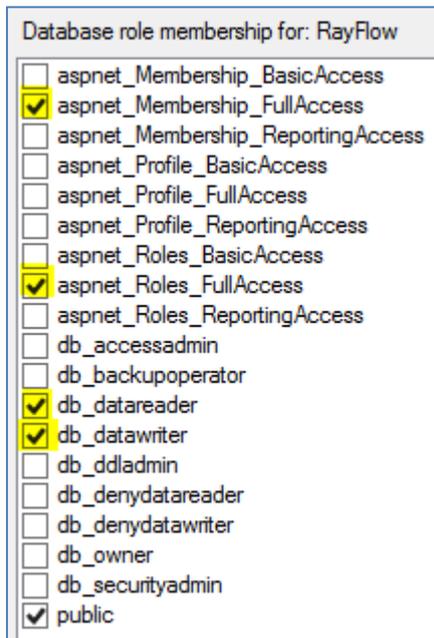
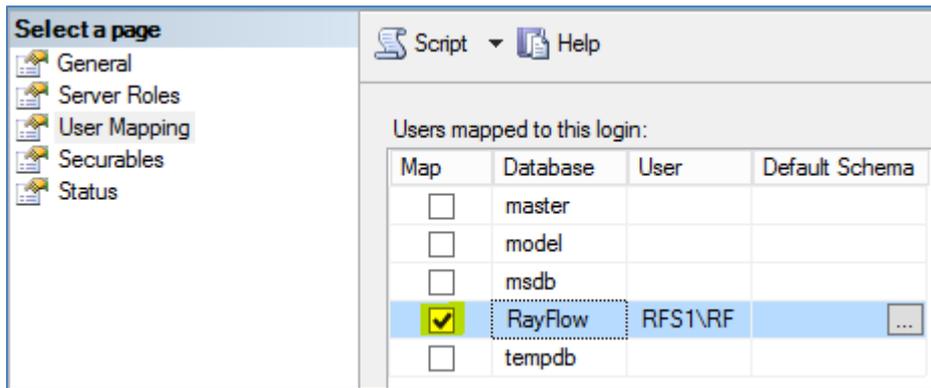
Select a page: General, Server Roles, User Mapping, Securables, Status

Script Help

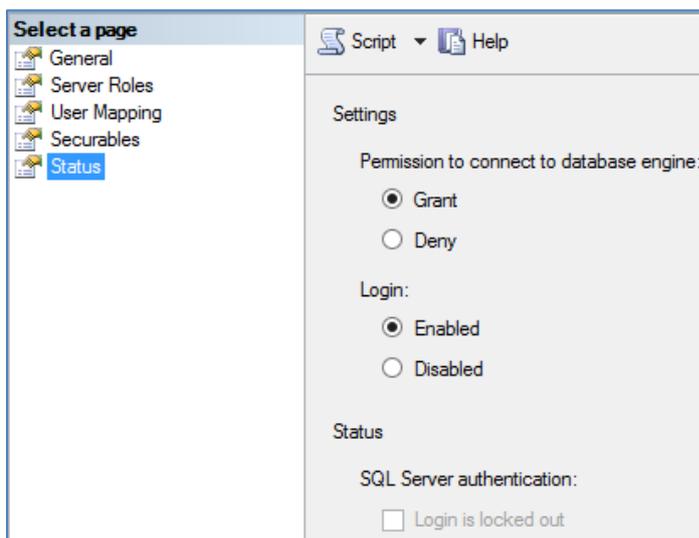
Server role is used to

Server roles:

- bulkadmin
- dbcreator
- diskadmin
- processadmin
- public
- securityadmin
- serveradmin
- setupadmin
- sysadmin



RayFlow Application Pool's identity requires the ability to create aspnet users and groups, assigning it to the aspnet_Membership_FullAccess & aspnet_Roles_FullAccess SQL Server Security Database Roles, automatically assigns it to their BasicAccess & ReportingAccess roles once the login is created.



Strengthening the login password for RayFlow users

Password complexity options can be configured via the web.config file, and are described in this knowledge base article:-

<https://raynetgmbh.zendesk.com/hc/en-us/articles/208097736>

Encrypting the web.config files connection string

You can improve the security of sensitive information stored in a connection string, such as the database name, user name, password, and so on, by encrypting the connection string section of the Web.config file using protected configuration.

The following Microsoft article describes how one can accomplish this task:-

<https://msdn.microsoft.com/en-us/library/dx0f3cf2%28v=vs.85%29.aspx>