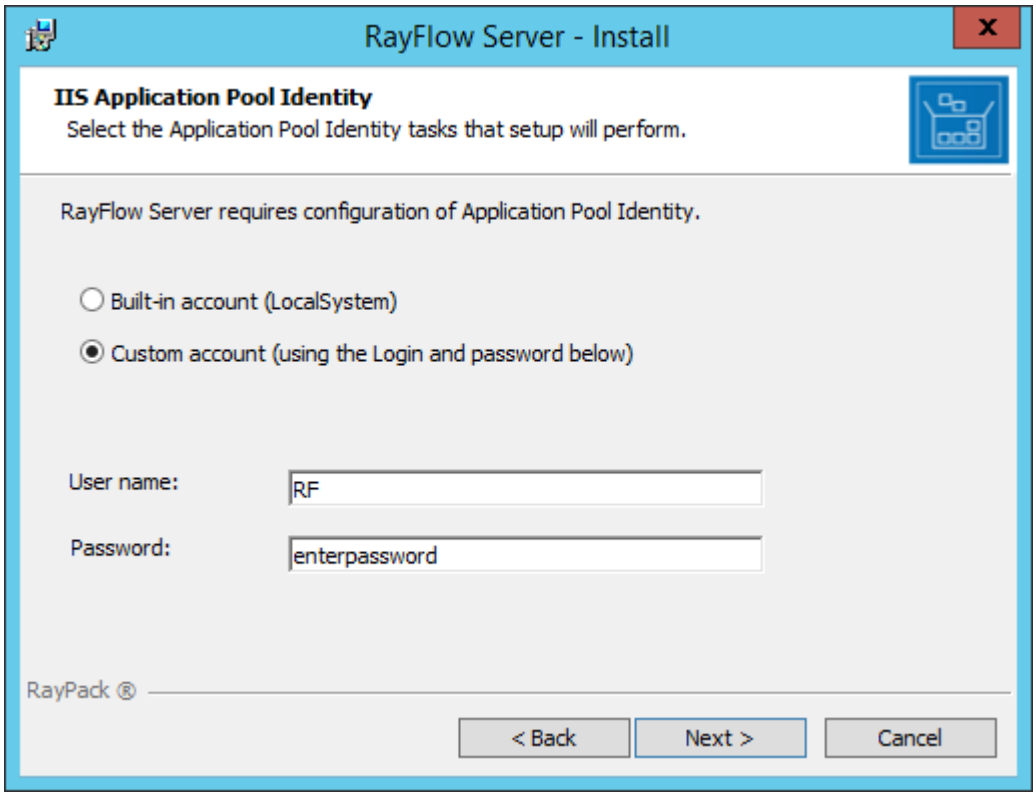
How to secure the RayFlow Server

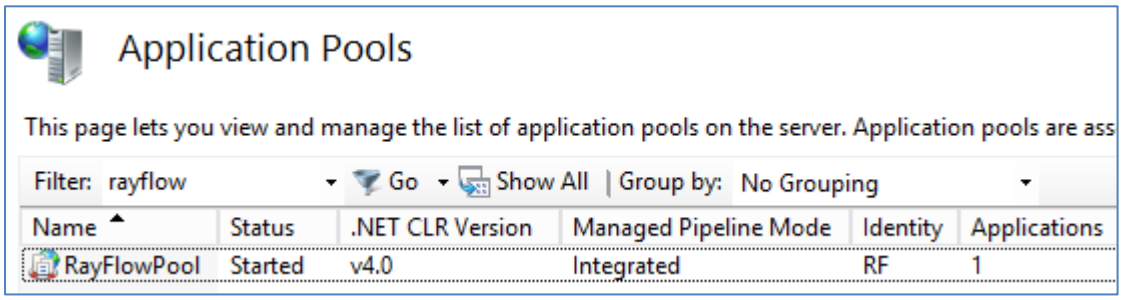
Application Pool Identity

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:

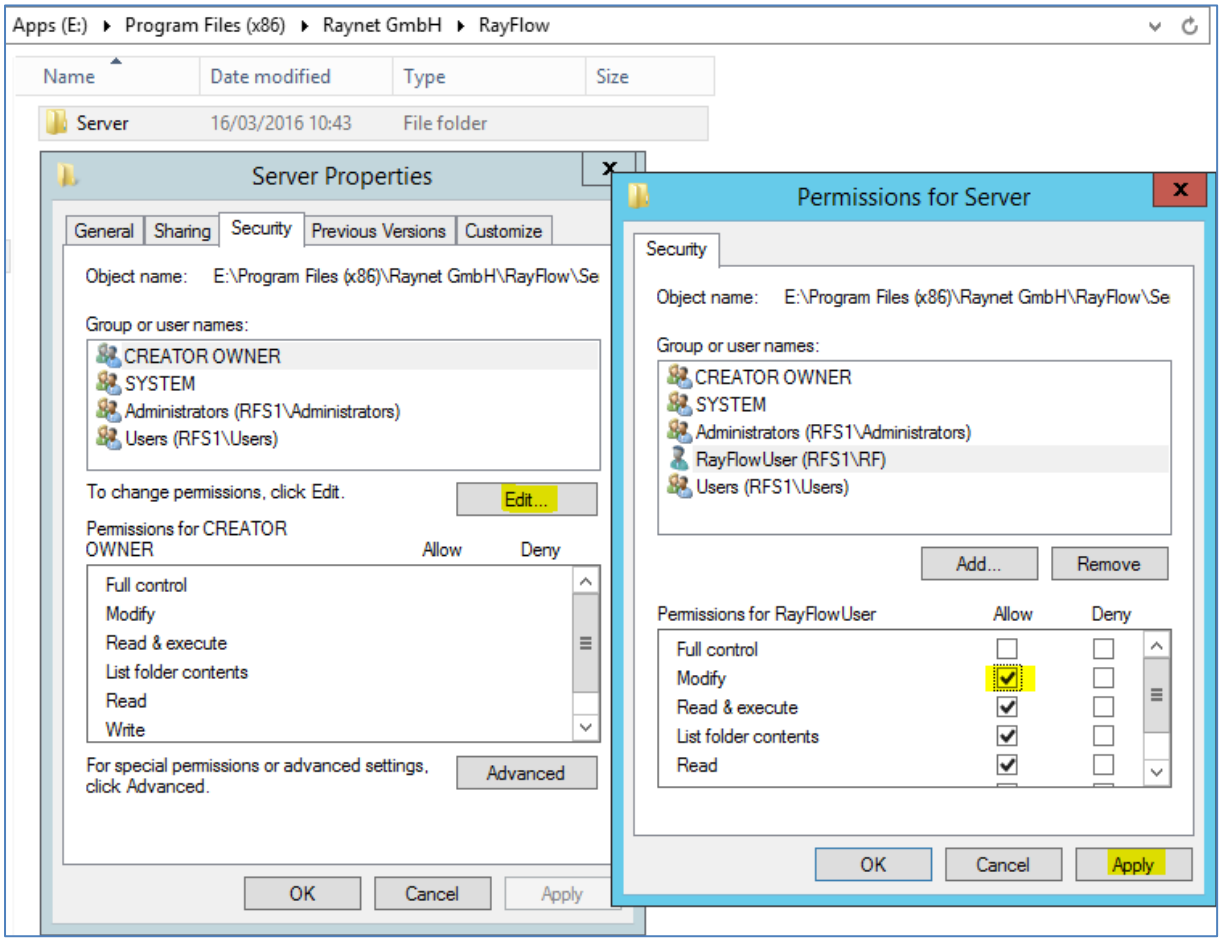


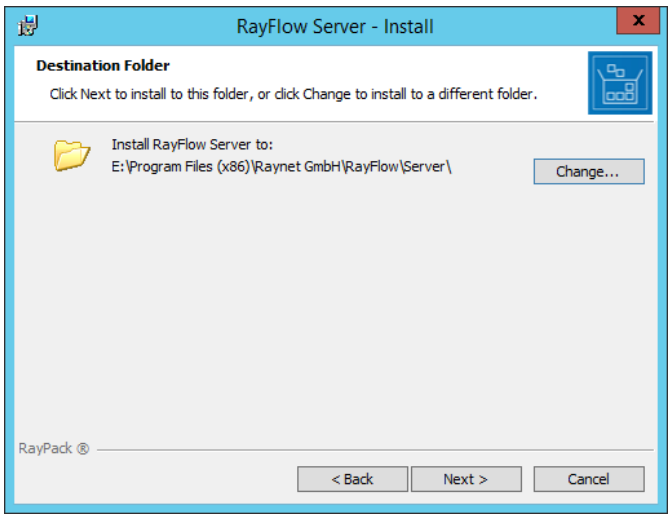


NTFS Permissions

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.



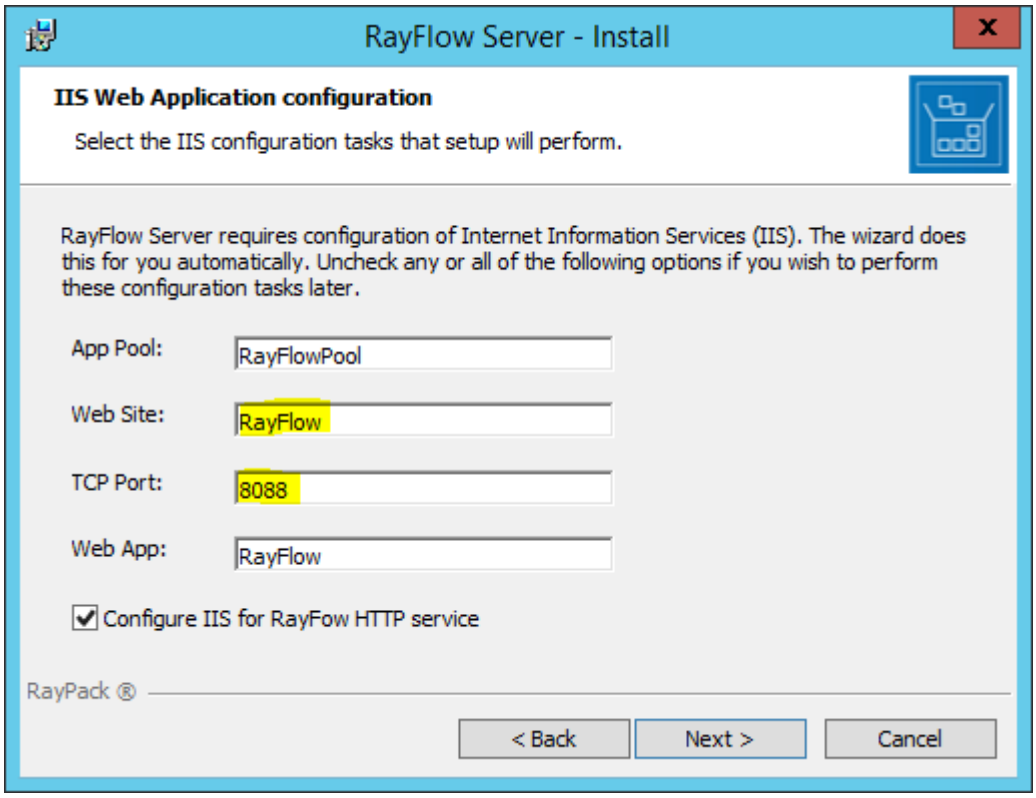


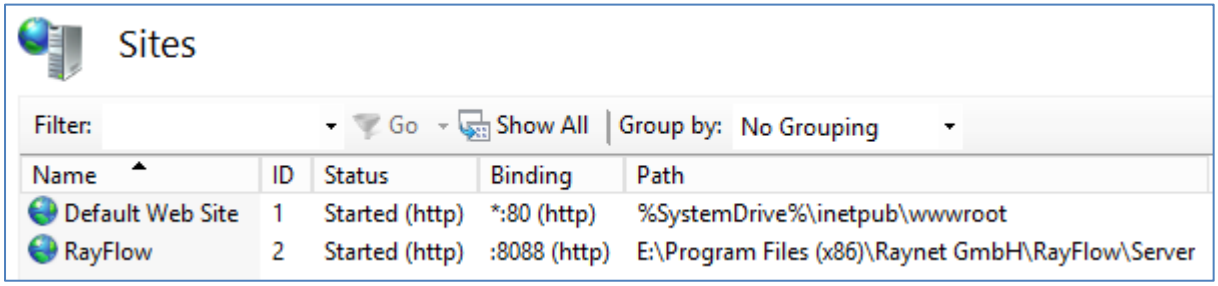
As all temporary file creation actions take place within the RayFlow IIS Application Pool's identity's temp directory, it is recommended to change that user's TEMP & TMP environment variables to target a different drive instead of its default C: drive location.

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.



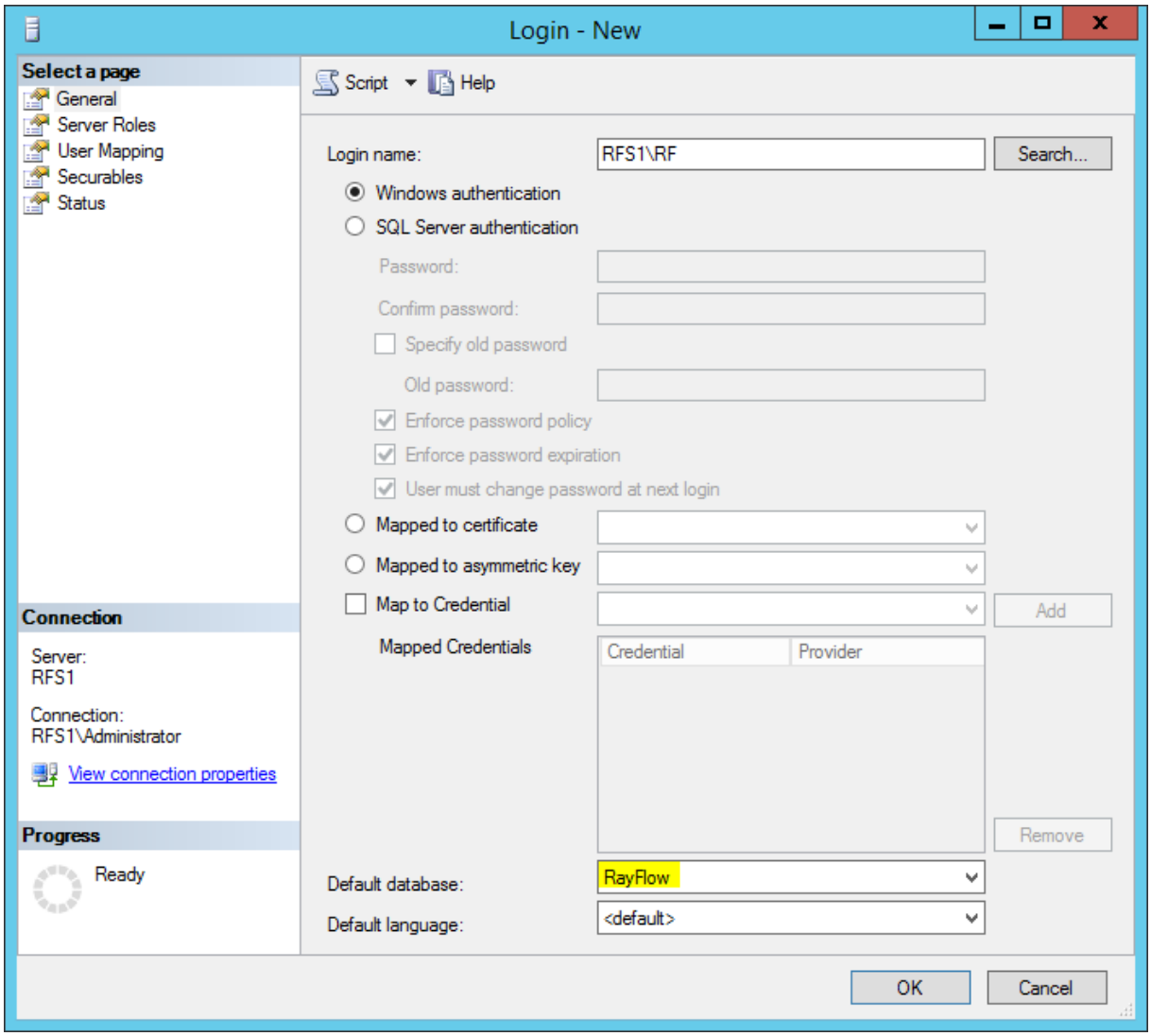


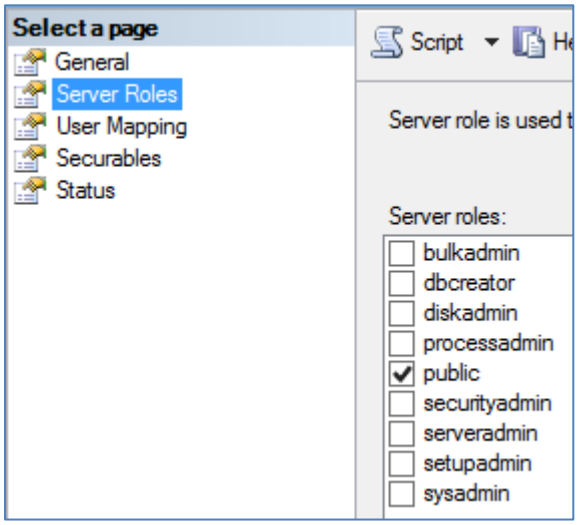
HTTPS

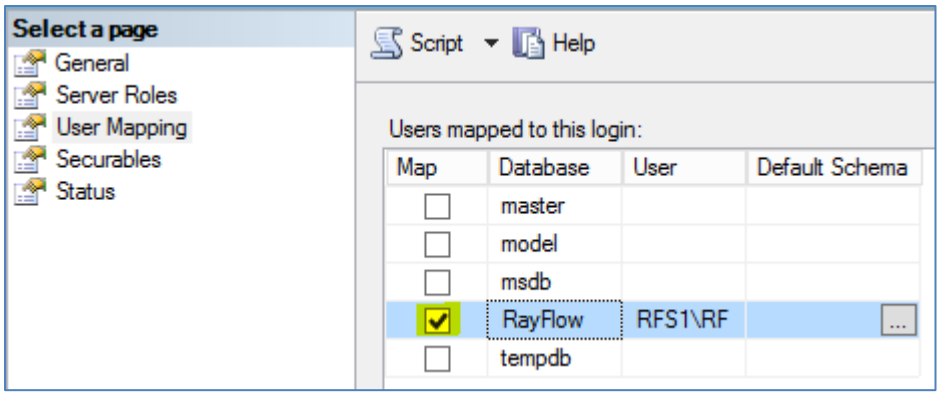
To implement HTTPS, you can either create a self-signed TLS certificate via the RayFlow web site itself, or utilise a TLS certificate from an internal or external Certificate Authority.

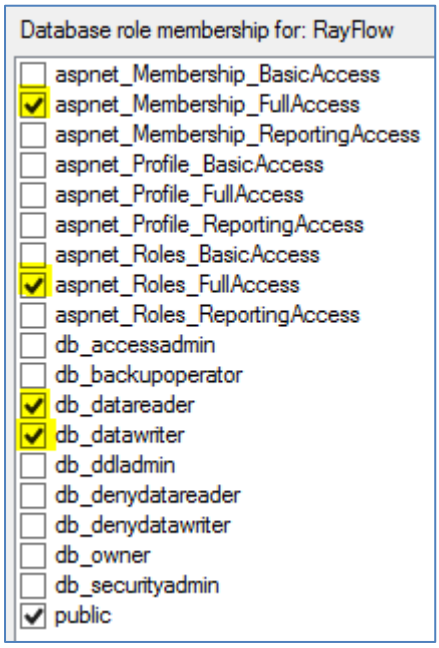
Database

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:

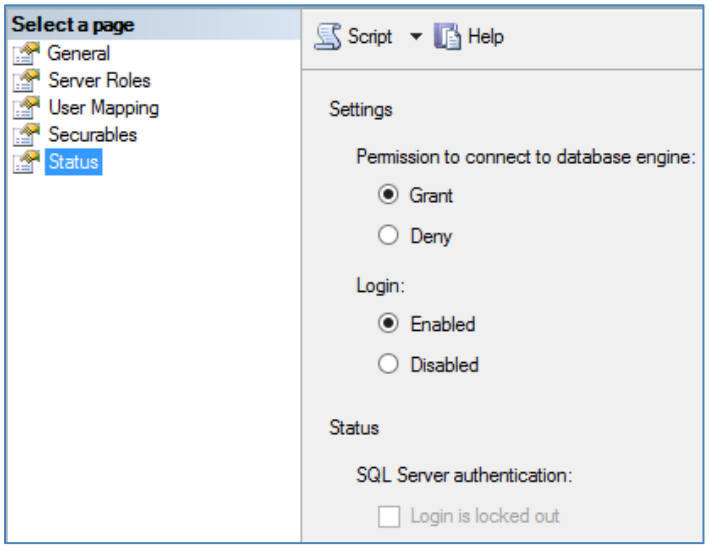








RayFlow Application Pool's identity requires the ability to create aspnet users and groups, assigning it to the aspnet_Membership_FullAccess & aspnet_Roles_FullAcess SQL Server Security Database Roles, automatically assigns it to their BasicAcess & ReportingAccess roles once the login is created.



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