

QEF Console

1 Contents

1	Introduction.....	3
2	Working with Modules.....	3
2.1	Module general info.....	3
2.2	Module configuration.....	4
2.3	Dependencies.....	6
2.4	Detailed version info.....	7
3	Installing QIS, RA and Web Forms Modules.....	8
3.1	Preface.....	8
3.2	Prerequisites.....	8
3.3	Module Description.....	9
3.4	Installing and Updating QIS, RA and Web Forms Modules.....	9
3.5	Installing and Updating QLM Module.....	17
4	Installing QCL Engine (QCLE).....	25
4.1	Preface.....	25
4.2	Prerequisites.....	25
4.3	Module Description.....	25
4.4	Installing and Updating QCLE Module.....	26
4.5	Advanced Setup.....	31
4.6	Data Migration.....	32
5	SharePoint.....	34
5.1	Preface.....	34
5.2	Prerequisites.....	35
5.3	Supported Servers.....	35
5.4	Installation of QualiWare Document Connector.....	35
5.5	Configuration of List of SharePoint Servers.....	35
5.6	Permissions.....	36
5.7	Configuration of Single Sign-On.....	36
5.7.1	Prerequisites.....	36

5.7.2	Log on as for Windows Service.....	36
5.7.3	Update Configuration Files.....	37
5.7.4	Internet Information Services (IIS) Configuration	39
5.7.5	Create SPNs	47
5.7.6	Trust for Delegation.....	49
5.7.7	Enable Integrated Windows Authentication (Kerberos) in SharePoint	51
5.7.8	Legend	53
5.7.9	References.....	53

1 Introduction

QEF console is a web based interface used to setup parts of QualiWare handled by QEF. An internet shortcut to the console can be found in the QualiWare group of start menu on the computer that QEF was installed on.

QEF is responsible for handling:

- Users and groups
- Active Directory Synchronization of users and groups
- Licenses
- Logging
- Modules

2 Working with Modules

The modules tab in QEF Console shows an overview of installed modules. From here modules can be installed, uninstalled, started and stopped. Updating a module is simply done by installing it again (no uninstall is necessary).

During module installation, you will be asked if you want to reuse existing settings for the module, if such exists. Also when uninstalling a module, you will be asked if you want to keep settings for module, so they can be used again if installing module again later.

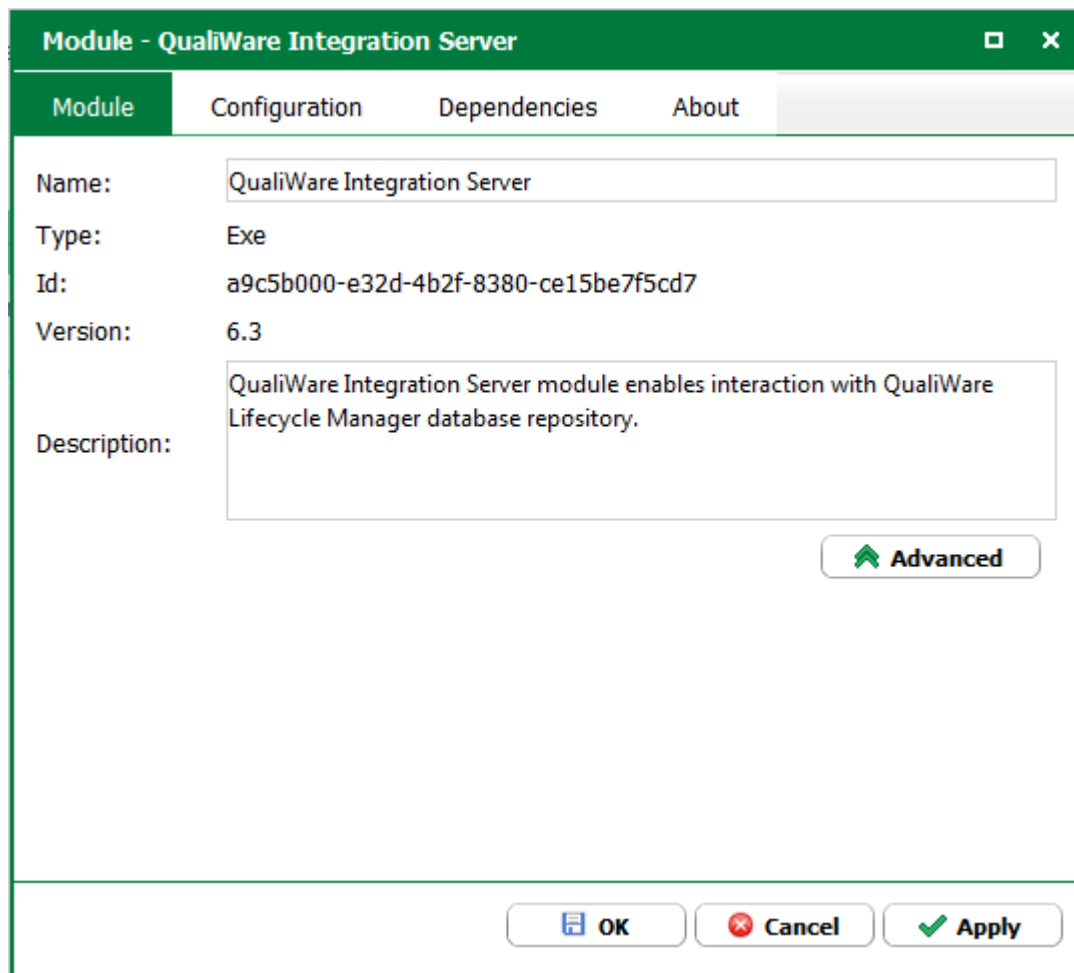
Settings available for modules differ, but some are currently available for all modules:

- Module: Basic information of module
- Configuration: Automatic start, logging and monitoring, restart on fail behavior
- Dependencies: Information on dependencies between modules
- About: Version information for module

For web modules (modules used through a web interface), the name is shown underlined. If the module is running, the name works as a link to the start page of that module.

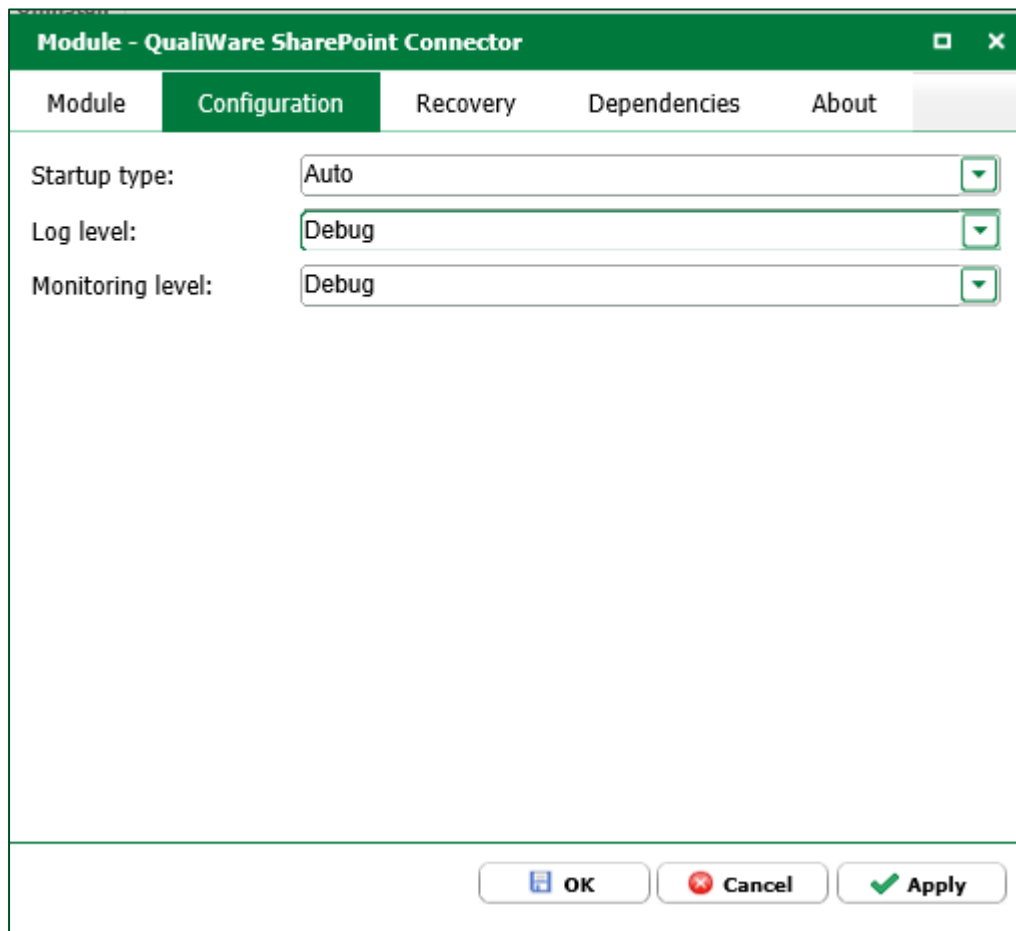
2.1 Module general info

Below is how module settings page looks like (main module info):



2.2 Module configuration

Each module has **Configuration** tab where can be specified its Startup type, Log level, Monitoring level and Restart on fail behavior:



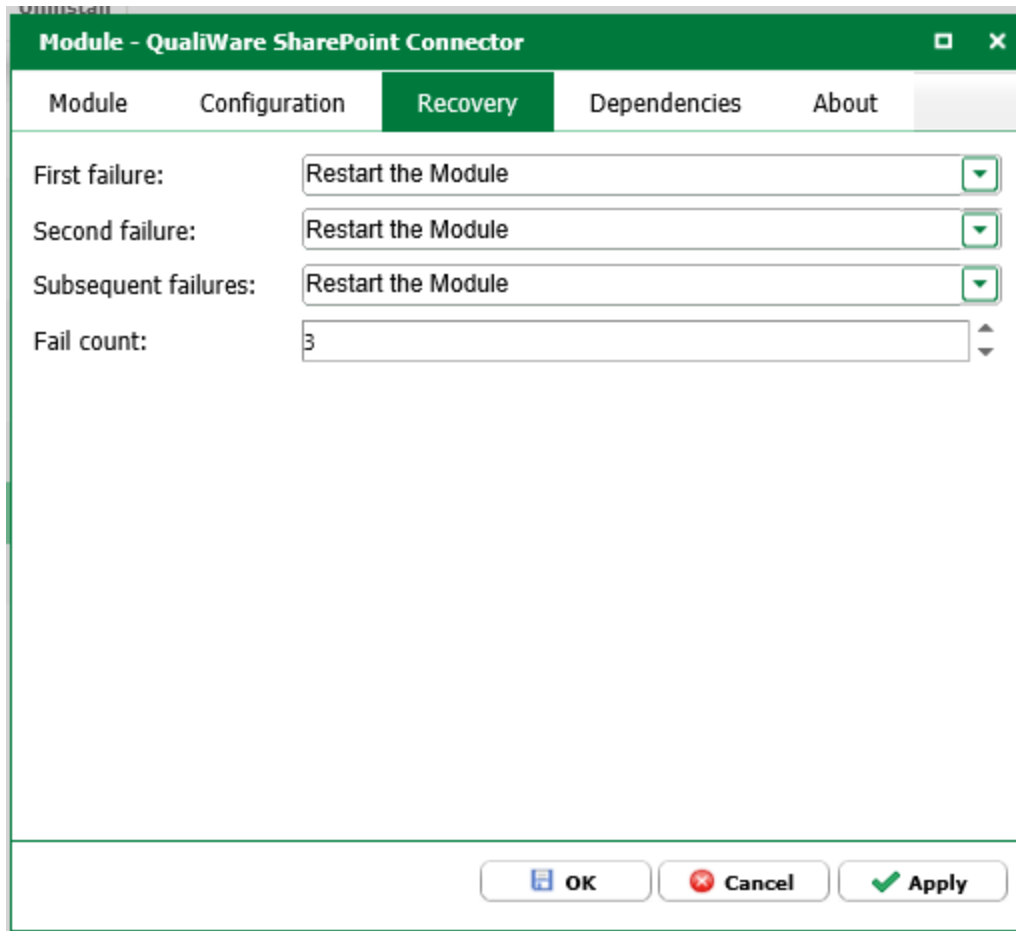
Startup types:

- Manual: a module won't start when QEF service starts
- Auto: a module will be started when QEF service starts

Default is Manual.

Log level defines the lowest log record type to be written to the QEF Log from a module. Default is Debug.

Monitoring level the lowest log record type to be monitored by QEF monitoring service.

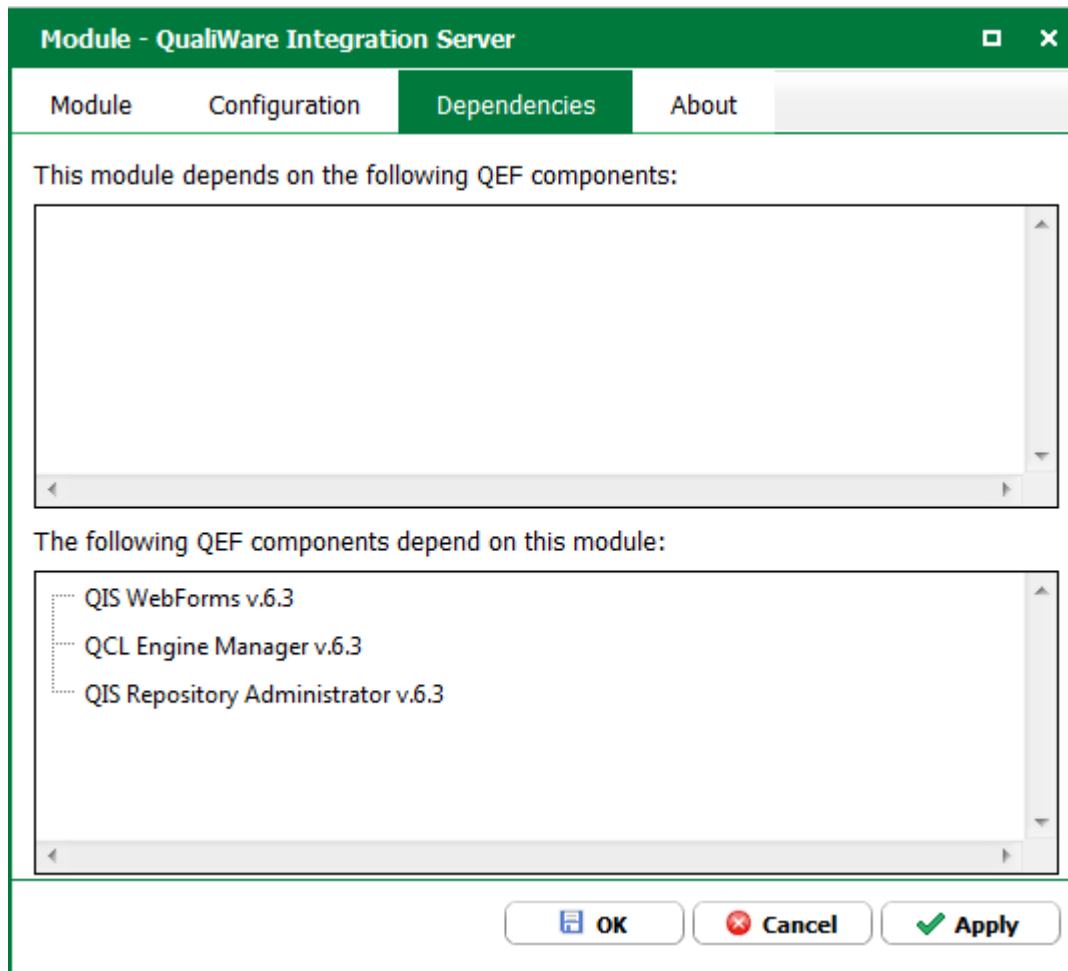


Restart on fail defines whether to try to restart a module once its fail is detected.

Restart after consequent fails defines whether to keep trying to restart a module after fail after **Maximum restart tries** were unsuccessful.

2.3 Dependencies

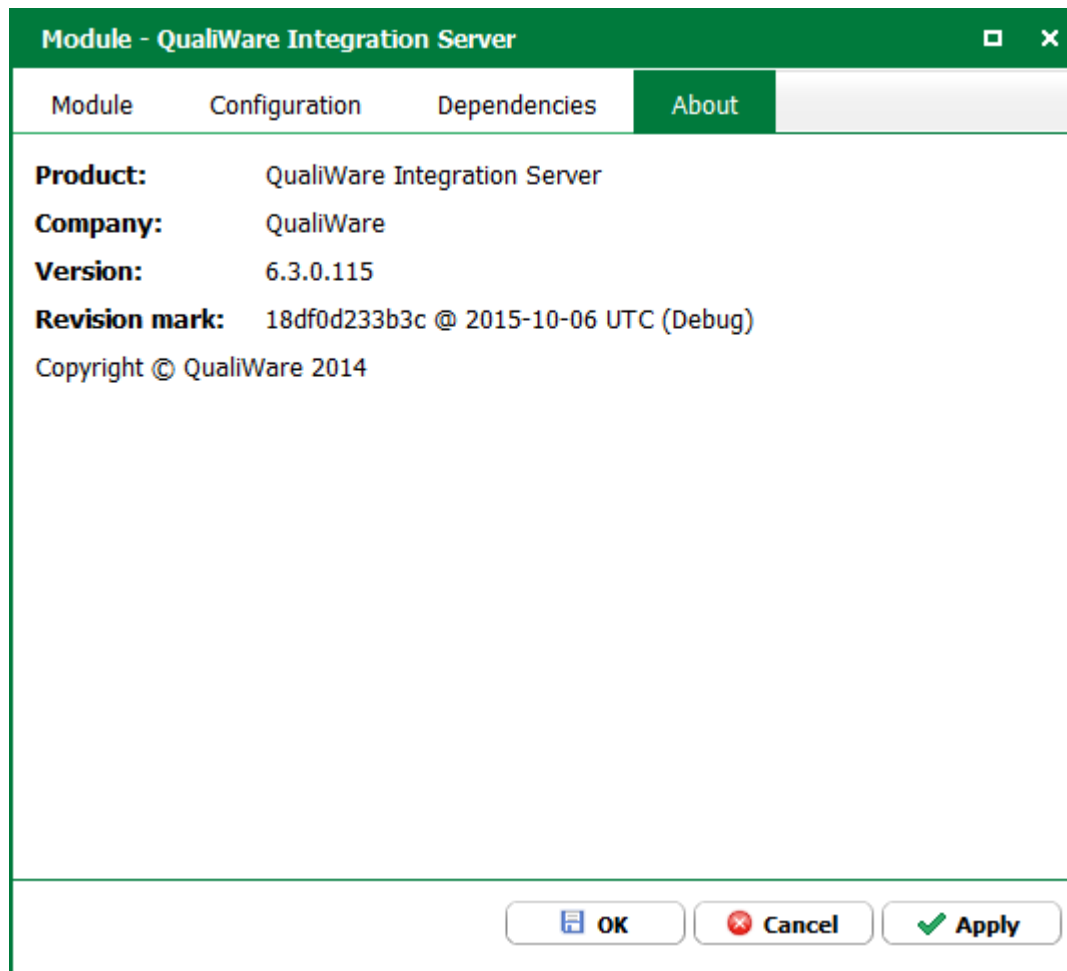
Dependencies tab displays modules dependent on a particular module and modules the module depends on:



When starting a module QEF also tries to start the dependencies if they are not started yet.

2.4 Detailed version info

About tab contains detailed version information including build revision and hash:



Please see the following sections for details on how to install and configure specific modules.

3 Installing QIS, RA and Web Forms Modules

3.1 Preface

This document describes the steps necessary to install or update **QualiWare Integration Server** (hereinafter QIS), **Repository Administrator** (hereinafter RA) and **Web Forms** modules.

3.2 Prerequisites

QEF is installed and running.

3.3 Module Description

QIS, RA and Web Forms are the main modules that provide access and control of objects and repositories.

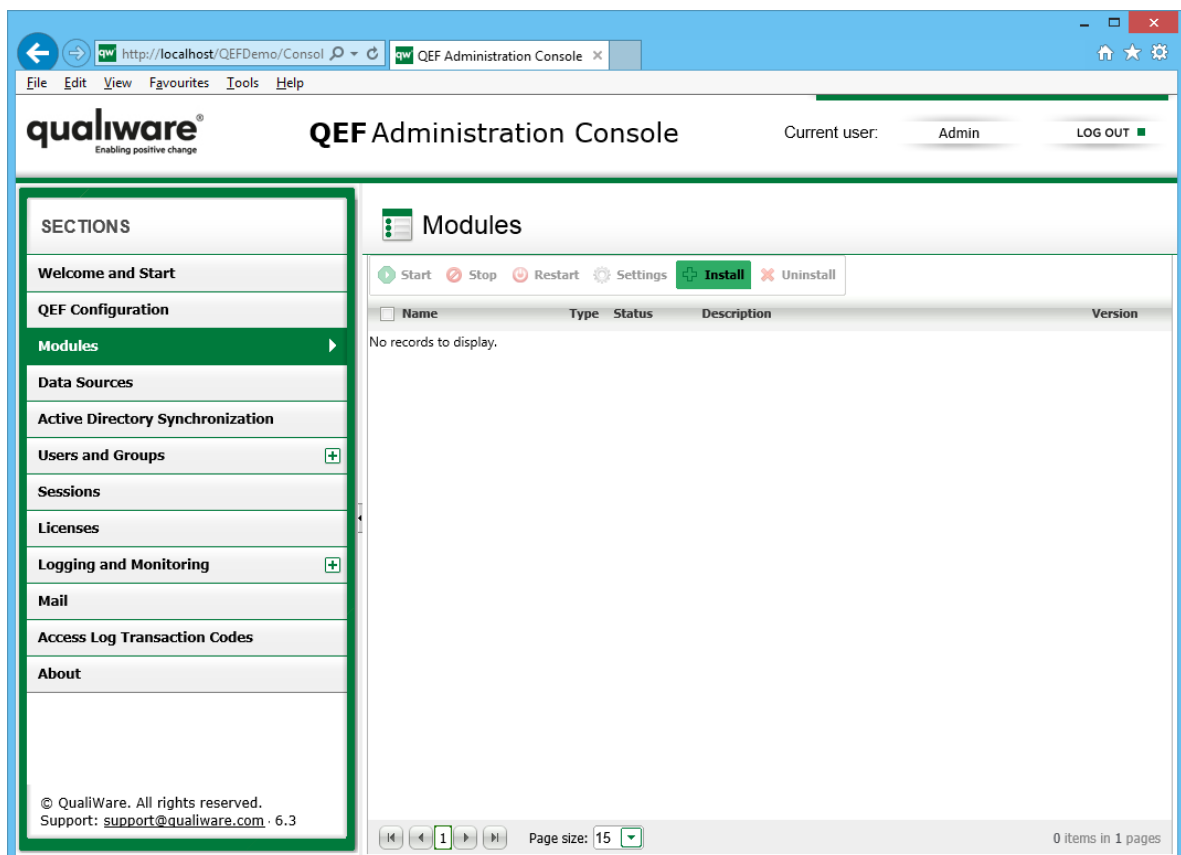
RA enables management of QIS repositories.

Web Forms enables access to repositories with objects through QIS from Web.

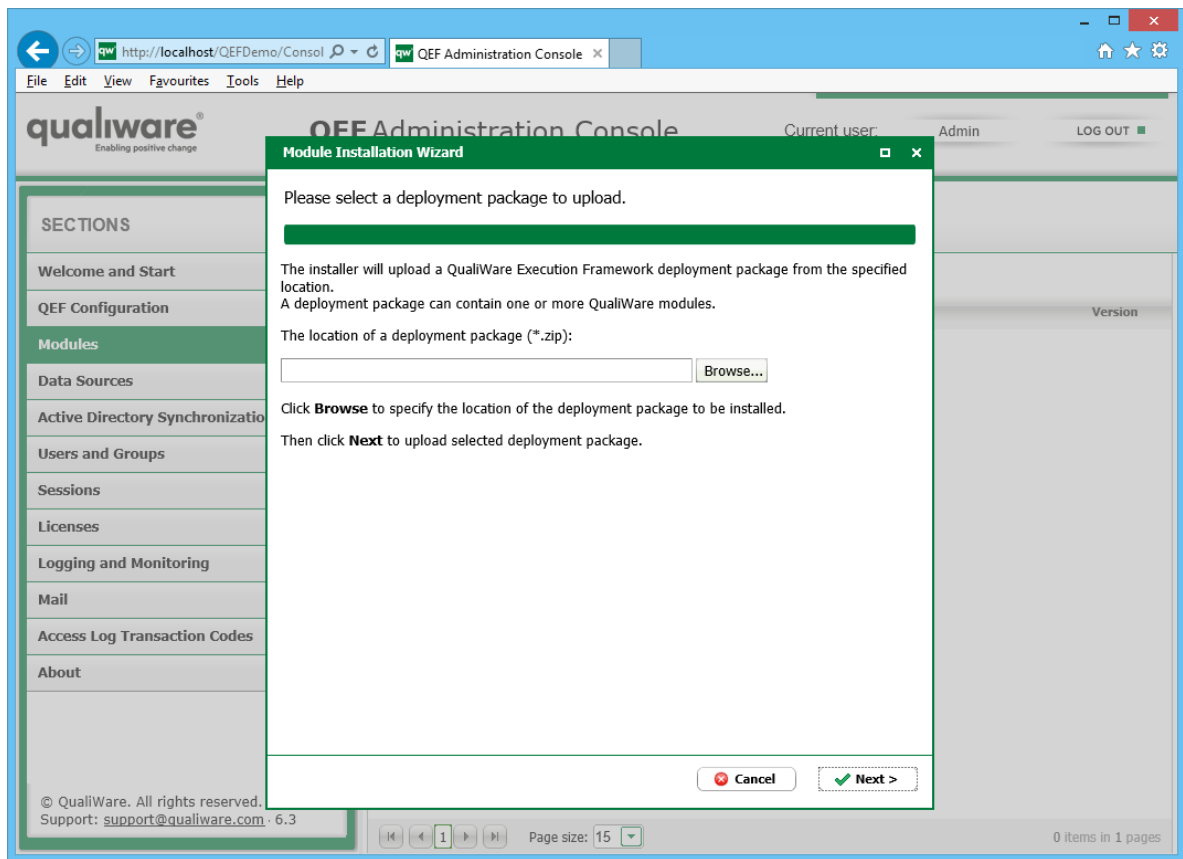
3.4 Installing and Updating QIS, RA and Web Forms Modules

Below are the steps to install and update modules:

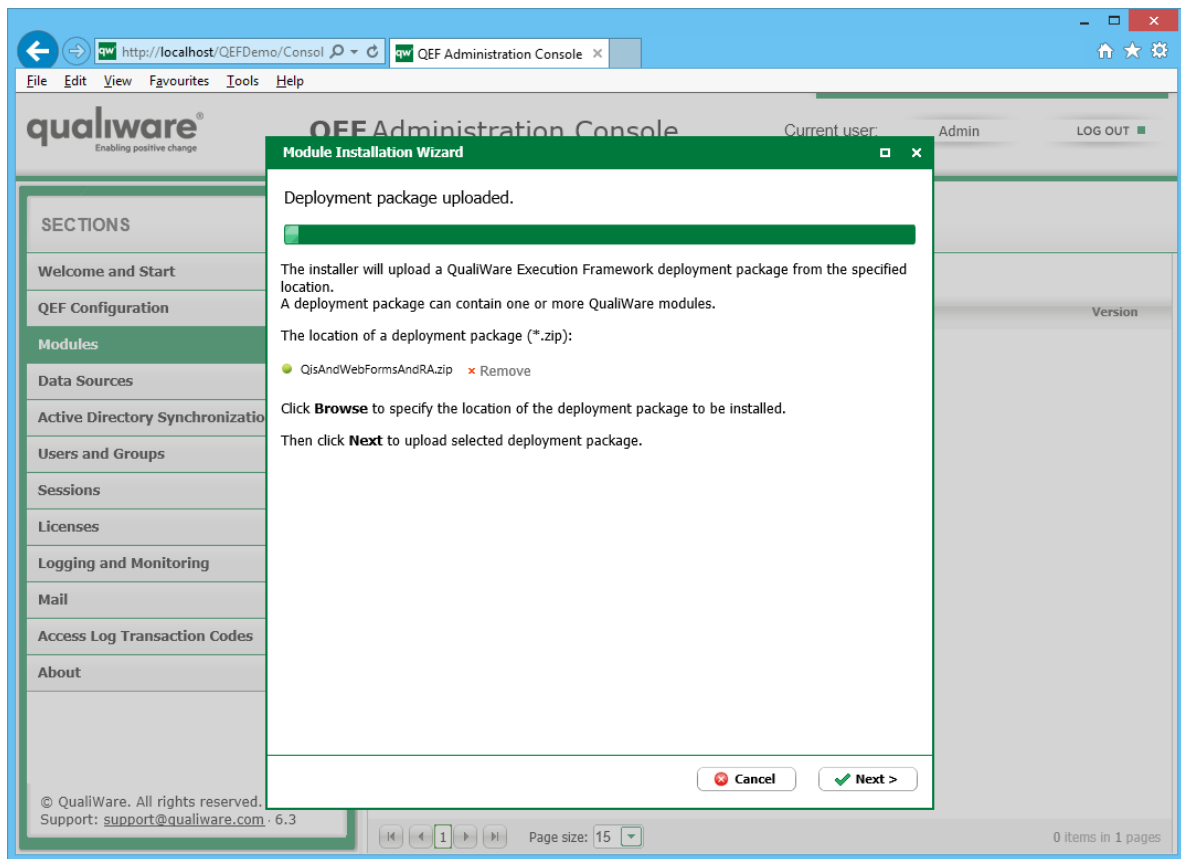
1. Open **Admin Console -> Modules**.
2. Click **Install**.



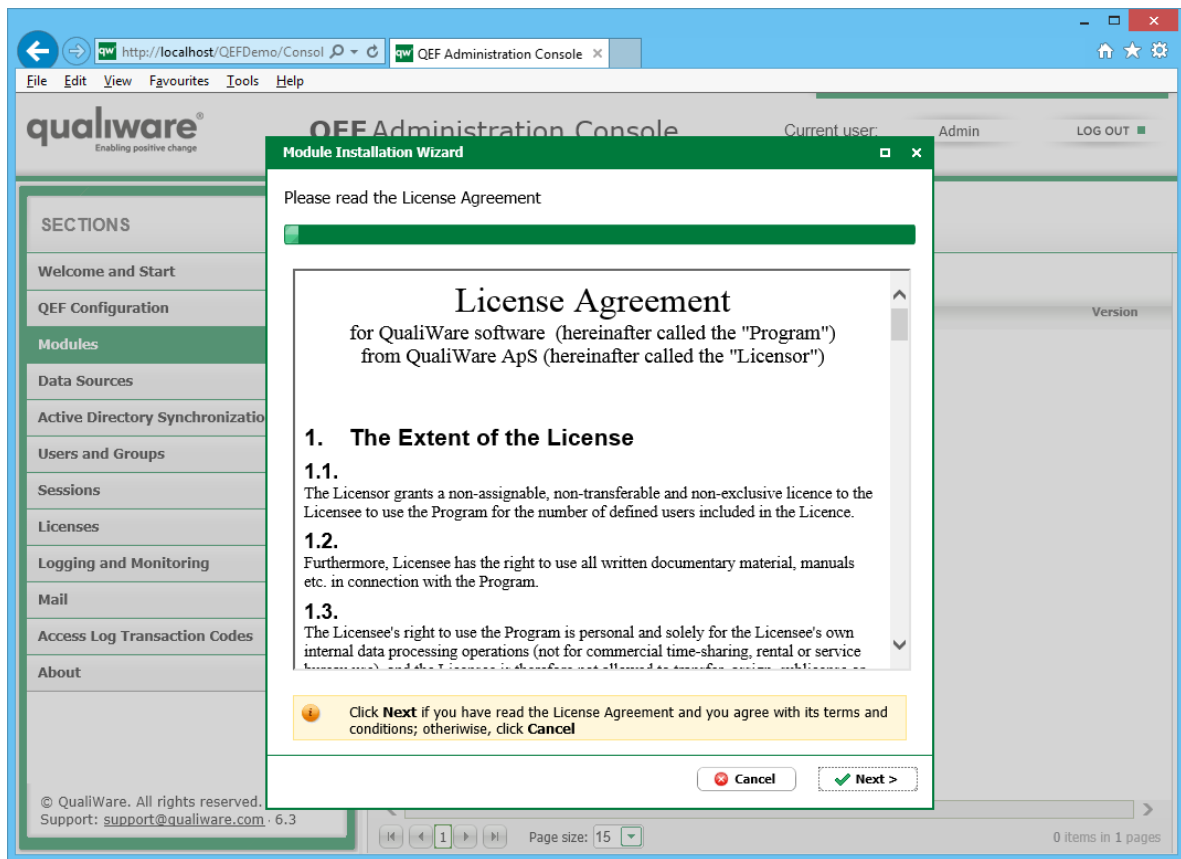
3. Click **Browse** and select modules deployment package (zip archive).



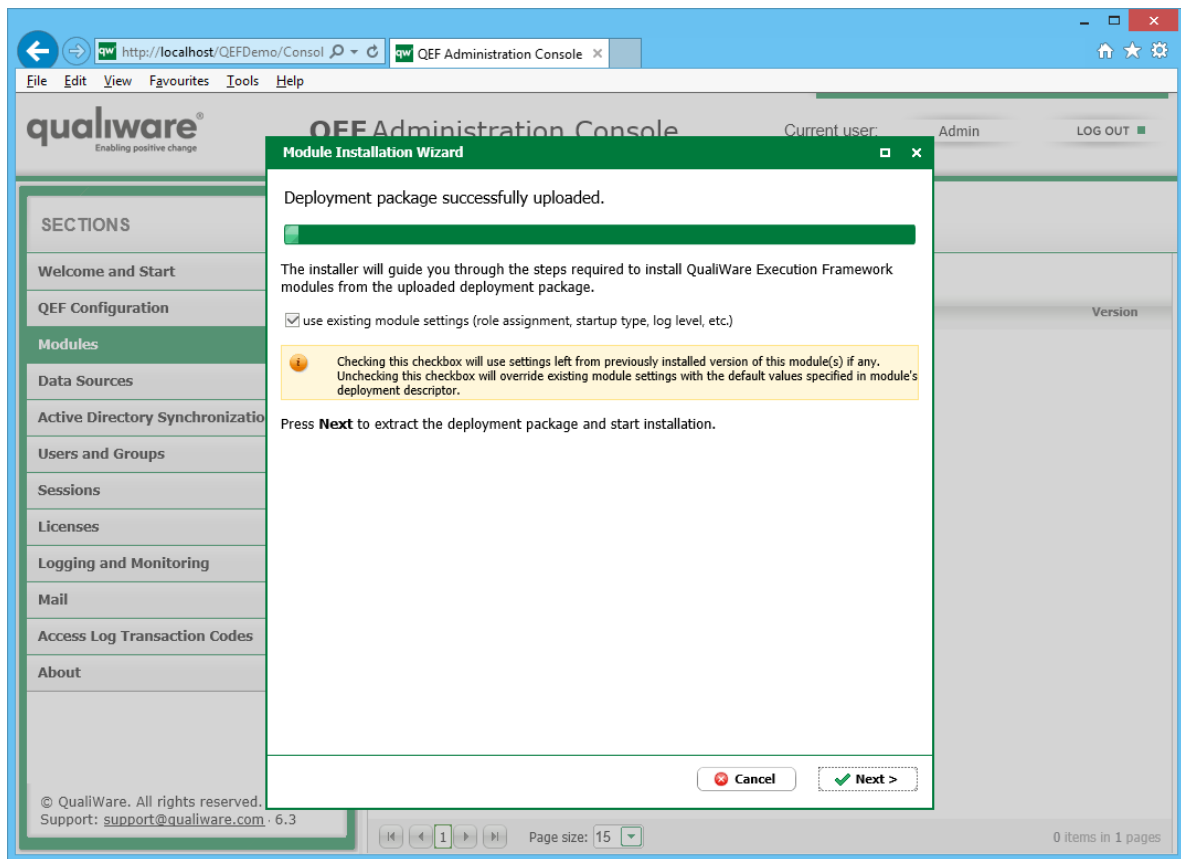
4. When deployment package is uploaded, click **Next**.



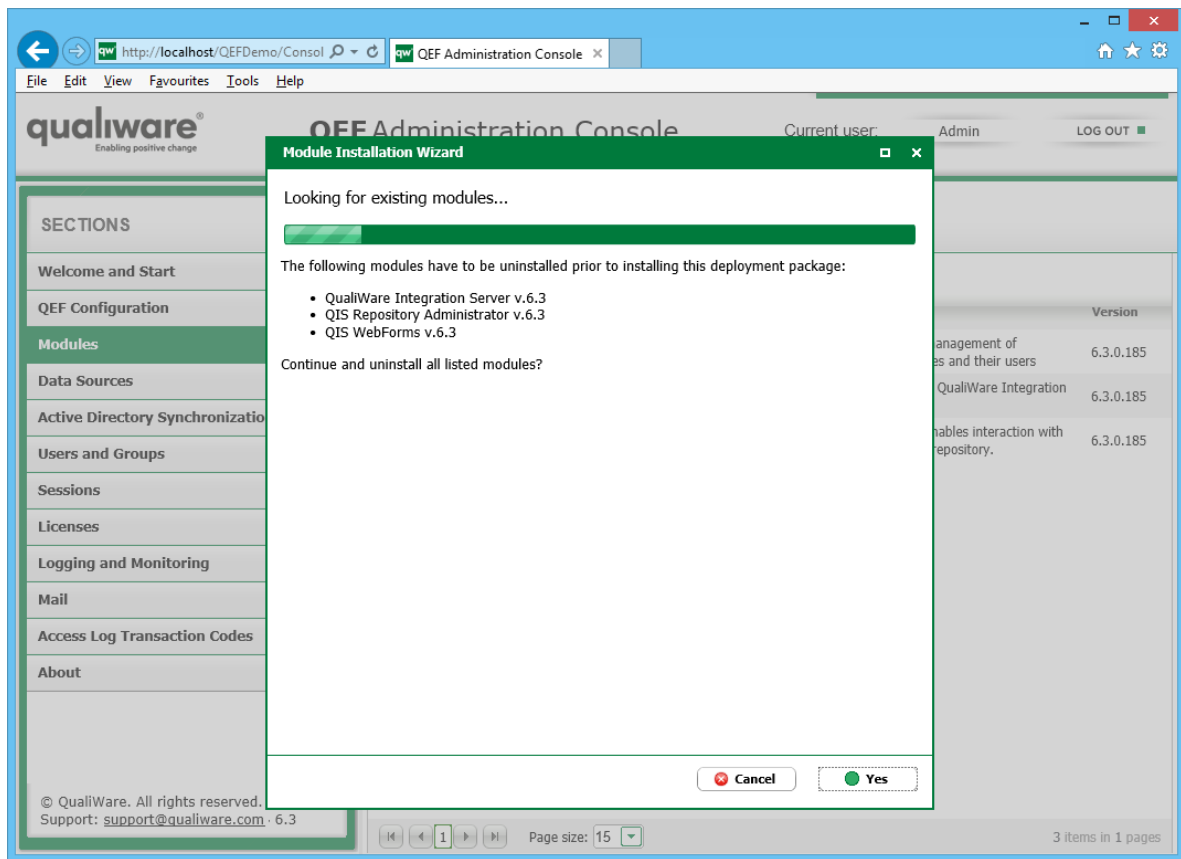
5. After reading the license agreement click **Next**.



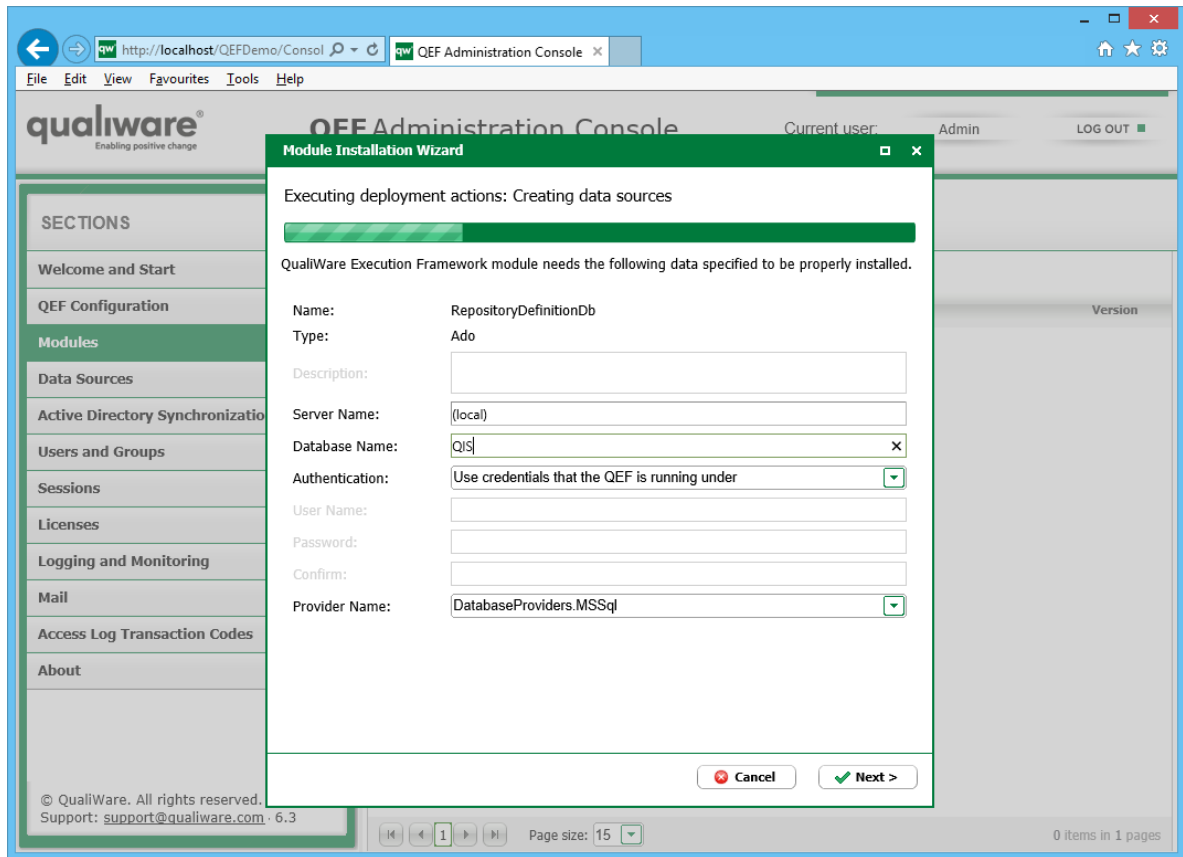
6. Enable or disable **use existing module settings**. Enabling it allows use of module settings from the previous installation. Click **Next**.



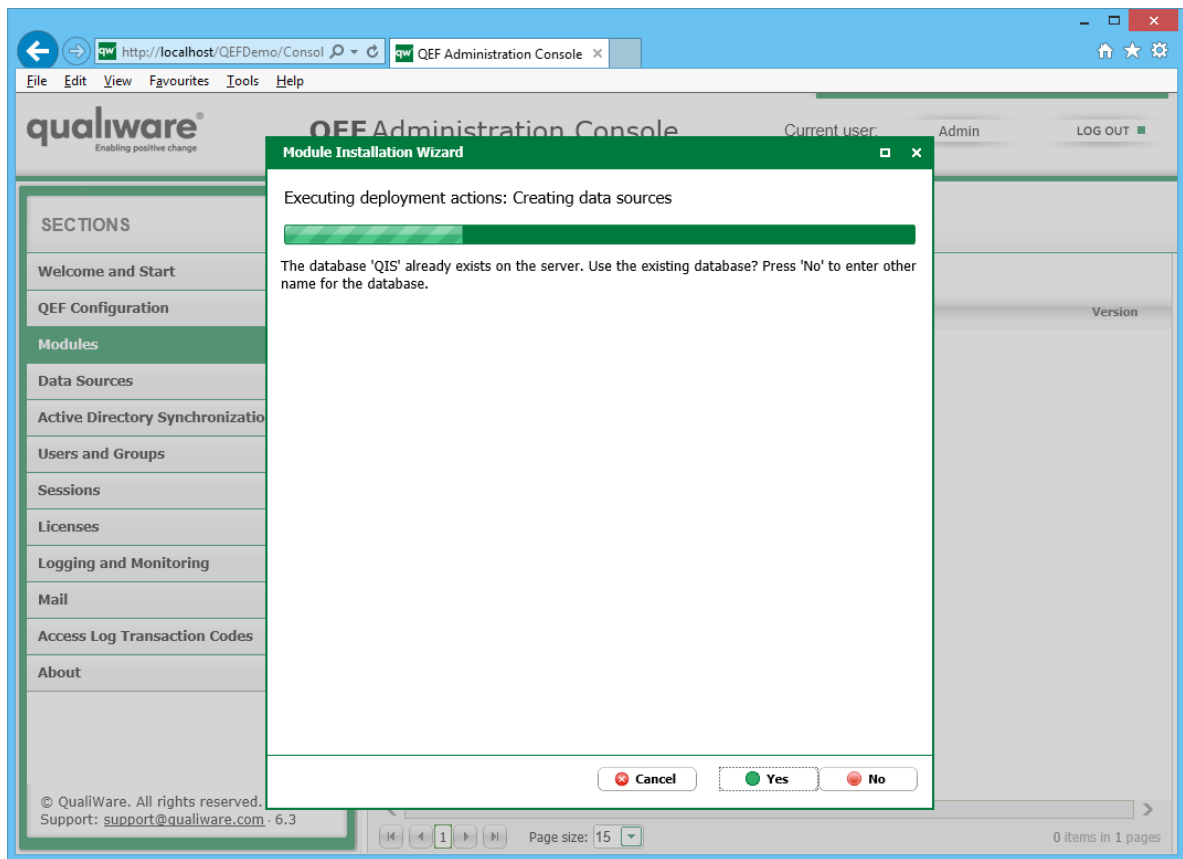
7. If it is an update, click **Yes** to confirm uninstall of previously installed modules.



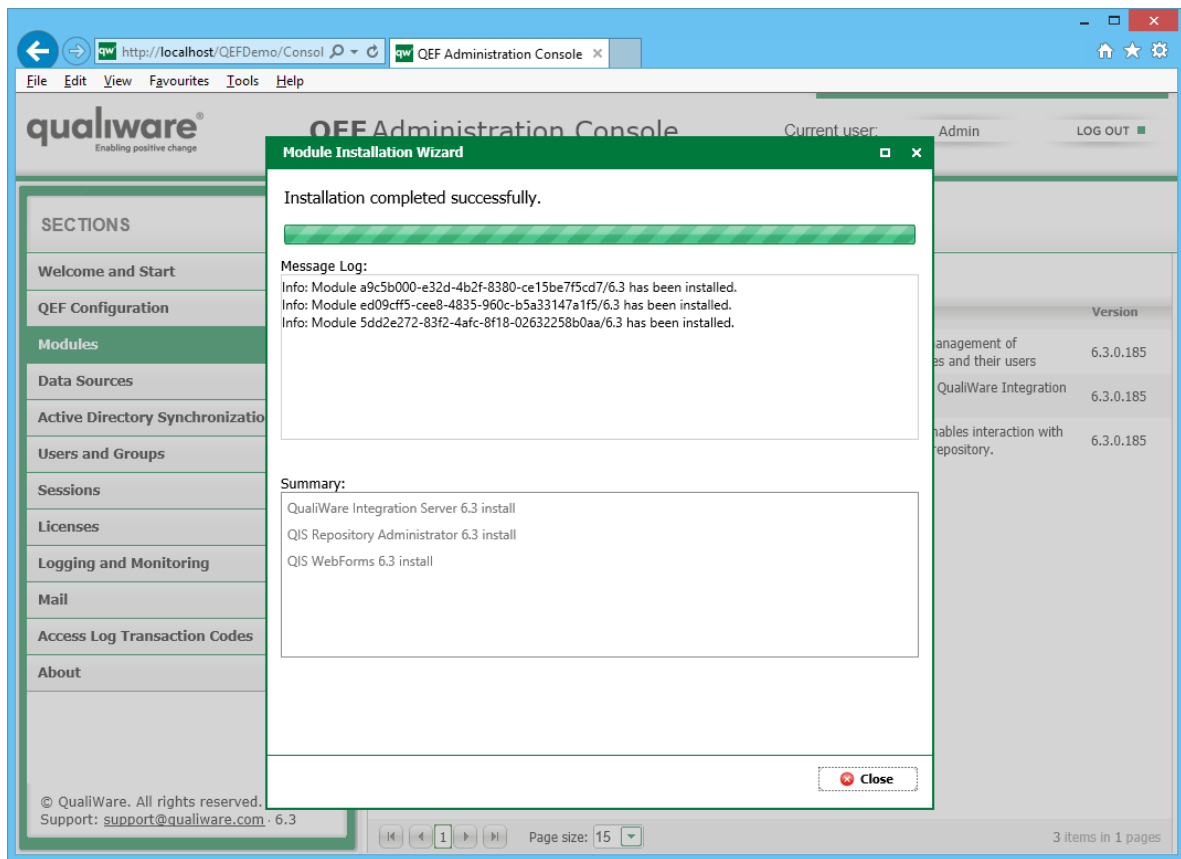
8. If it is a first-time installation or in step 6 **use existing module settings** was disabled, enter database settings and click **Next**.



9. If database already exists, press **Yes** to confirm install using existing database.



10. Review installation log and click **Close**. If installation fails, see QEF log for error details.



3.5 Installing and Updating QLM Module

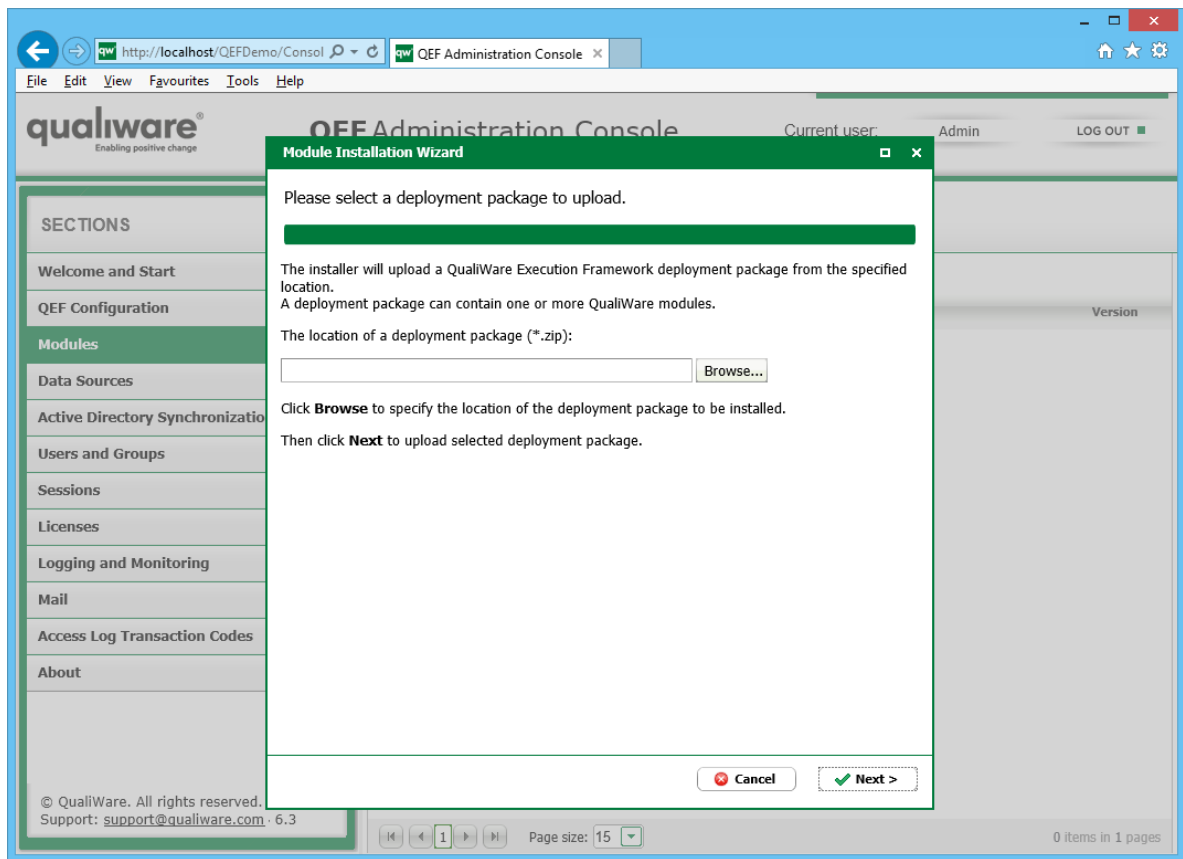
Below are the steps to install and update QLM module:

11. Open **Admin Console -> Modules**.
12. Click **Install**.

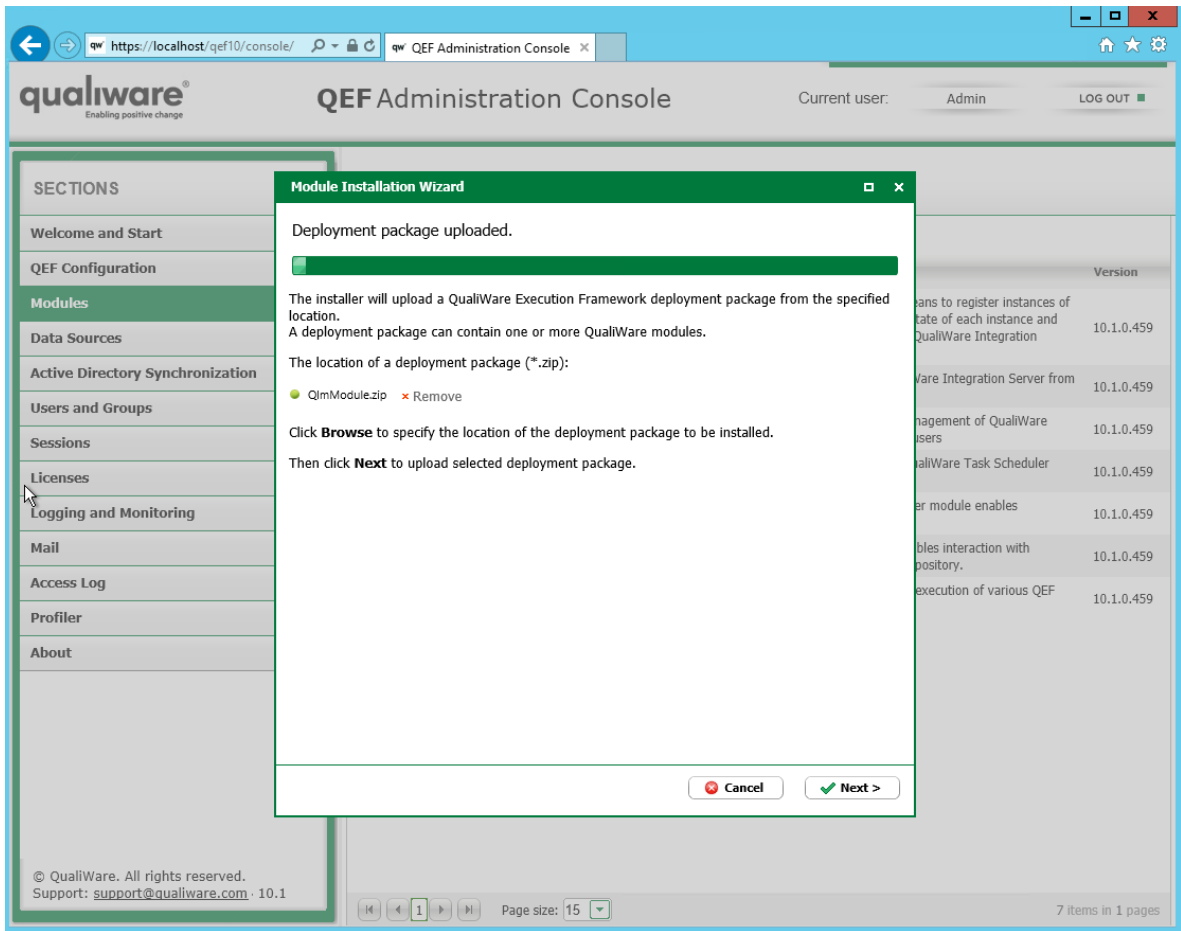
The screenshot shows the QualiWare QEF Administration Console interface. The top navigation bar includes the QualiWare logo, the title 'QEF Administration Console', the current user 'Admin', and a 'LOG OUT' button. A left-hand sidebar lists various sections, with 'Modules' selected and highlighted in green. The main content area displays a table of installed modules, all of which are in a 'Running' status. At the top of the module list, there are control buttons: Start, Stop, Restart, Settings, Install (highlighted with a mouse cursor), and Uninstall. The footer of the console shows copyright information and a page size of 15.

Name	Type	Status	Description	Version
<input type="checkbox"/> QCL Engine Manager	Exe	Running	QCL Engine Manager module provides means to register instances of QCL Engine in RA. It also monitors the state of each instance and ensures that it is in synchronization with QualiWare Integration Server.	10.1.0.459
<input type="checkbox"/> QIS Client	Web	Running	QIS Client enables interaction with QualiWare Integration Server from Web.	10.1.0.459
<input type="checkbox"/> QIS Repository Administrator	Web	Running	QIS Repository Administrator enables management of QualiWare Integration Server repositories and their users	10.1.0.459
<input type="checkbox"/> QTS Manager	Web	Running	QTS Manager enables management of QualiWare Task Scheduler tasks	10.1.0.459
<input type="checkbox"/> QualiWare Connector for SharePoint Server	Exe	Running	QualiWare Connector for SharePoint Server module enables interaction with Microsoft SharePoint.	10.1.0.459
<input type="checkbox"/> QualiWare Integration Server	Exe	Running	QualiWare Integration Server module enables interaction with QualiWare Lifecycle Manager database repository.	10.1.0.459
<input type="checkbox"/> QualiWare Task Scheduler	Exe	Running	QualiWare Task Scheduler allows to plan execution of various QEF module commands.	10.1.0.459

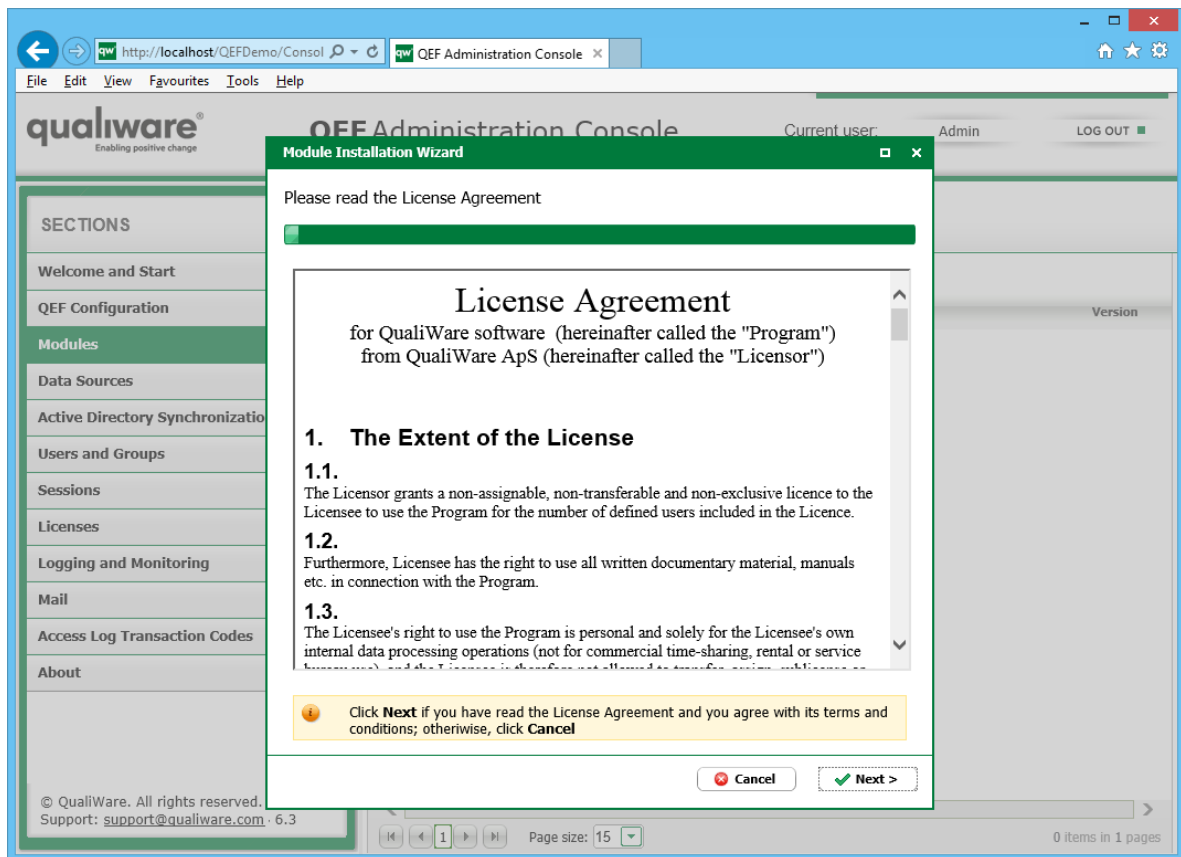
13. Click **Browse** and select QLM module deployment package (zip archive).



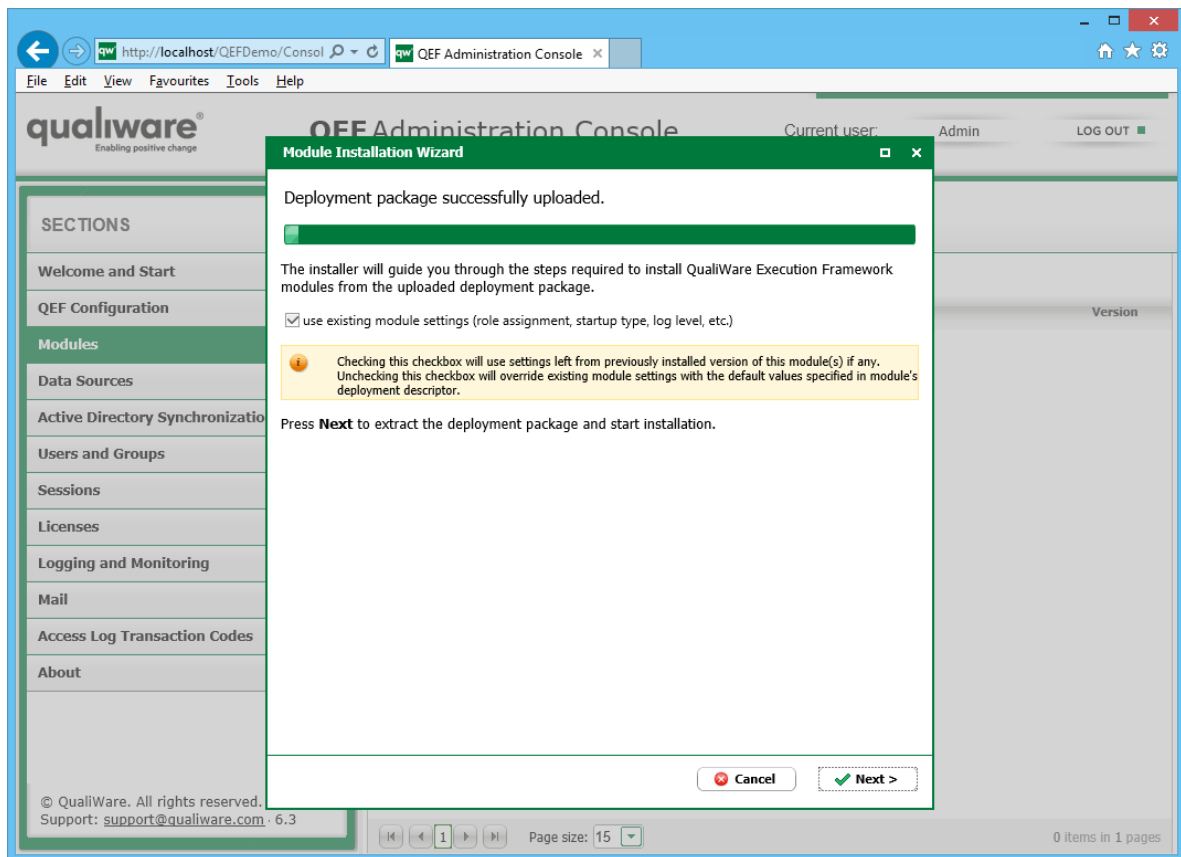
14. When deployment package is uploaded, click **Next**.



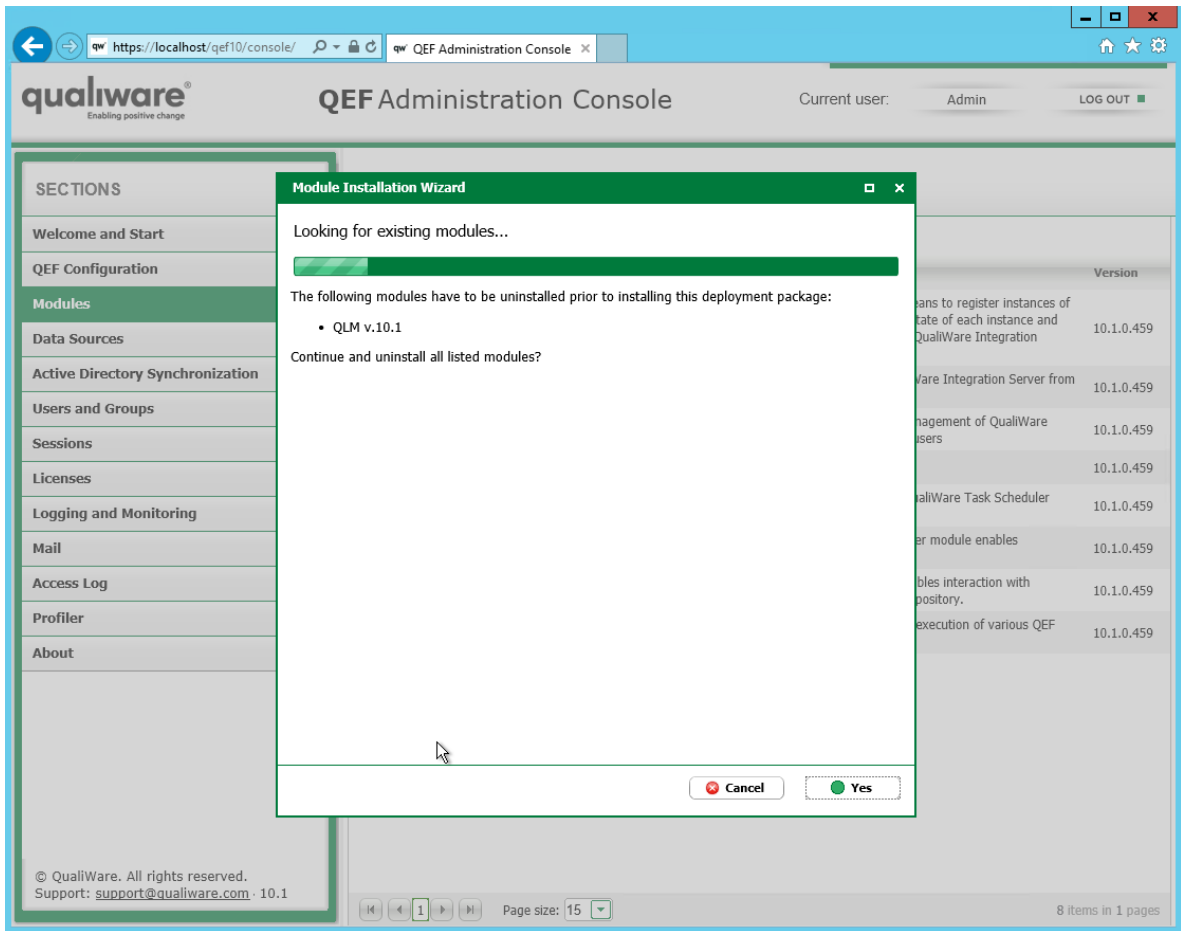
15. After reading the license agreement click **Next**.



16. Enable or disable **use existing module settings**. Enabling it allows use of module settings from the previous installation. Click **Next**.



17. If it is an update, click **Yes** to confirm uninstall of previously installed modules.

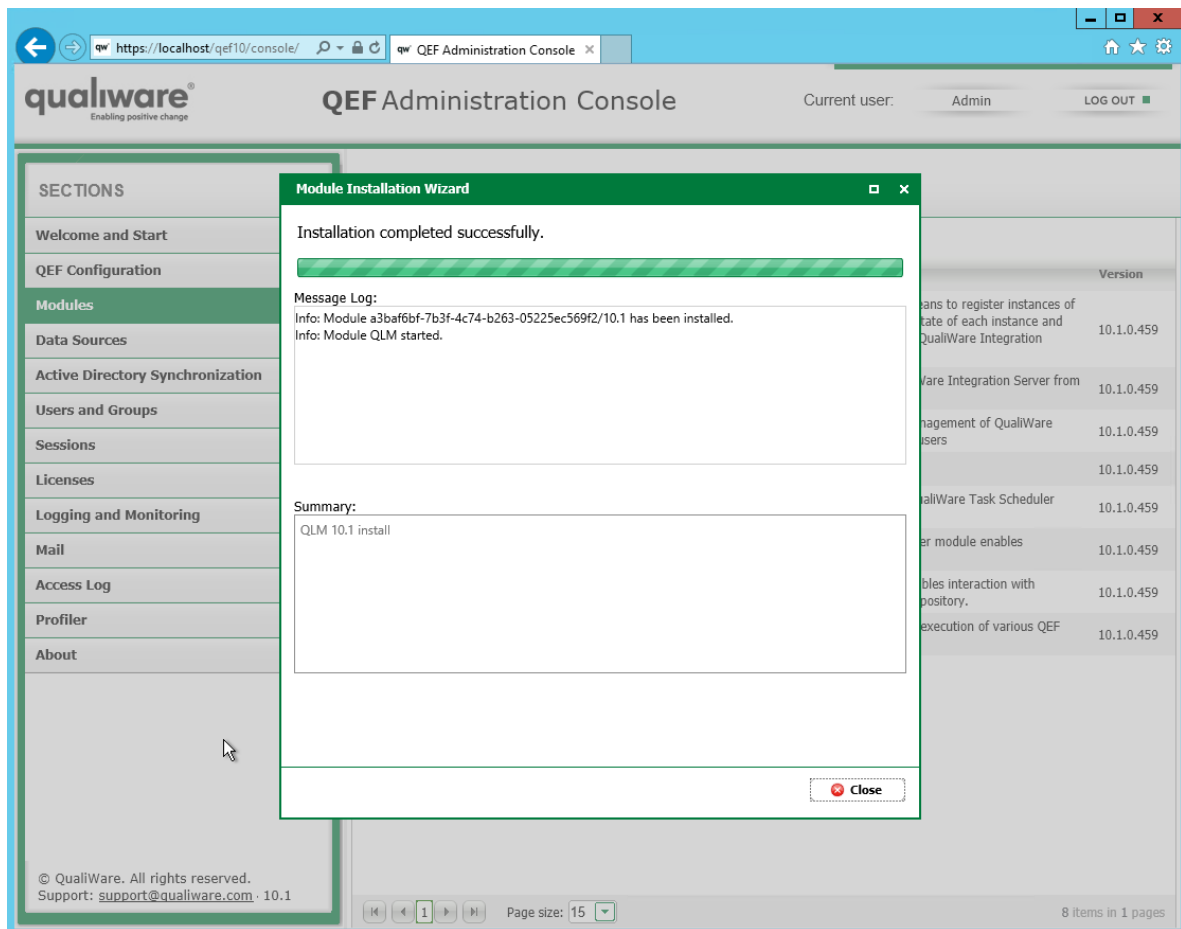


18. Edit the share to your liking and click on **Next**.

The screenshot displays the QualiWare QEF Administration Console interface. A 'Module Installation Wizard' dialog box is open, showing the progress of 'Executing deployment actions: Creating shared folders'. The wizard includes a progress bar and a checkbox labeled 'create shared folder to be used by the module'. A yellow warning box contains the text: 'Checking this checkbox will create shared folder with readonly access permissions. Please change folder permissions after installation is finished if needed.' Below the warning, there are input fields for 'Share name' (containing 'QLM X') and 'Share description' (containing 'QLM share'). At the bottom of the dialog are 'Cancel' and 'Next >' buttons.

The background interface shows the 'QEF Administration Console' with the current user 'Admin' and a 'LOG OUT' button. A sidebar menu lists sections such as 'Welcome and Start', 'QEF Configuration', 'Modules', 'Data Sources', 'Active Directory Synchronization', 'Users and Groups', 'Sessions', 'Licenses', 'Logging and Monitoring', 'Mail', 'Access Log', 'Profiler', and 'About'. A table on the right side of the console lists various modules and their versions, including 'QualiWare Integration', 'QualiWare Integration Server from', 'Management of QualiWare users', 'QualiWare Task Scheduler', 'er module enables', 'bles interaction with repository.', and 'execution of various QEF'.

19. Review installation log and click **Close**. If installation fails, see QEF log for error details.



4 Installing QCL Engine (QCLE)

4.1 Preface

This document describes steps necessary to install or update **QCL Engine** (hereinafter QCLE) module.

4.2 Prerequisites

In order to install and update QCLE module, the following requirements must be met:

- QEF and QEF Admin Console are installed and accessible;
- QIS module is installed;

4.3 Module Description

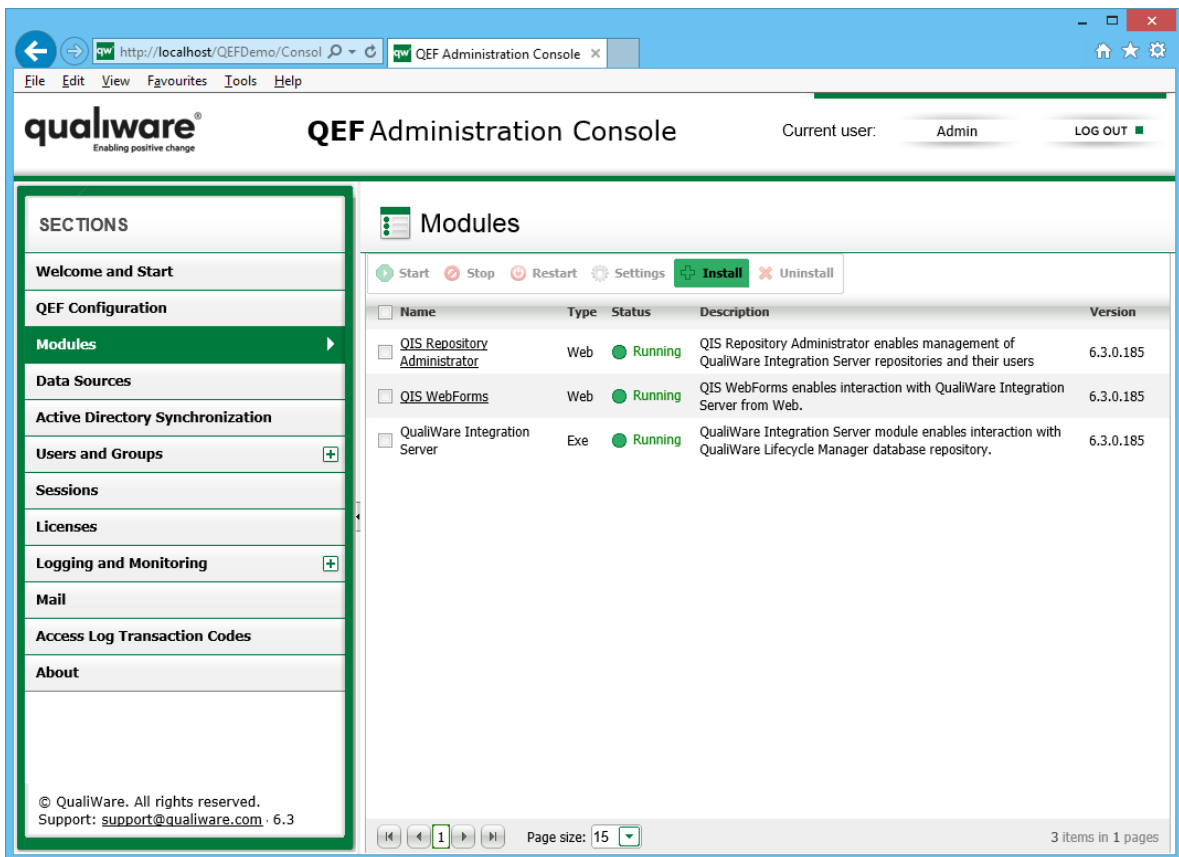
QCLE module is used to run and maintain QCLE instances. It performs the following tasks:

- Provisioning different QCLE instances;
- Starting/stopping QCLE instance processes;
- Maintaining QCLE instance states after unexpected crashes;
- Monitoring and reporting of QCLE instance configuration changes;
- Serving QCLE instance requests.

4.4 Installing and Updating QCLE Module

QCLE module installation/update procedure is typical. The following are the steps necessary:

1. Open Admin **Console** -> **Modules**.
2. Click **Install**.

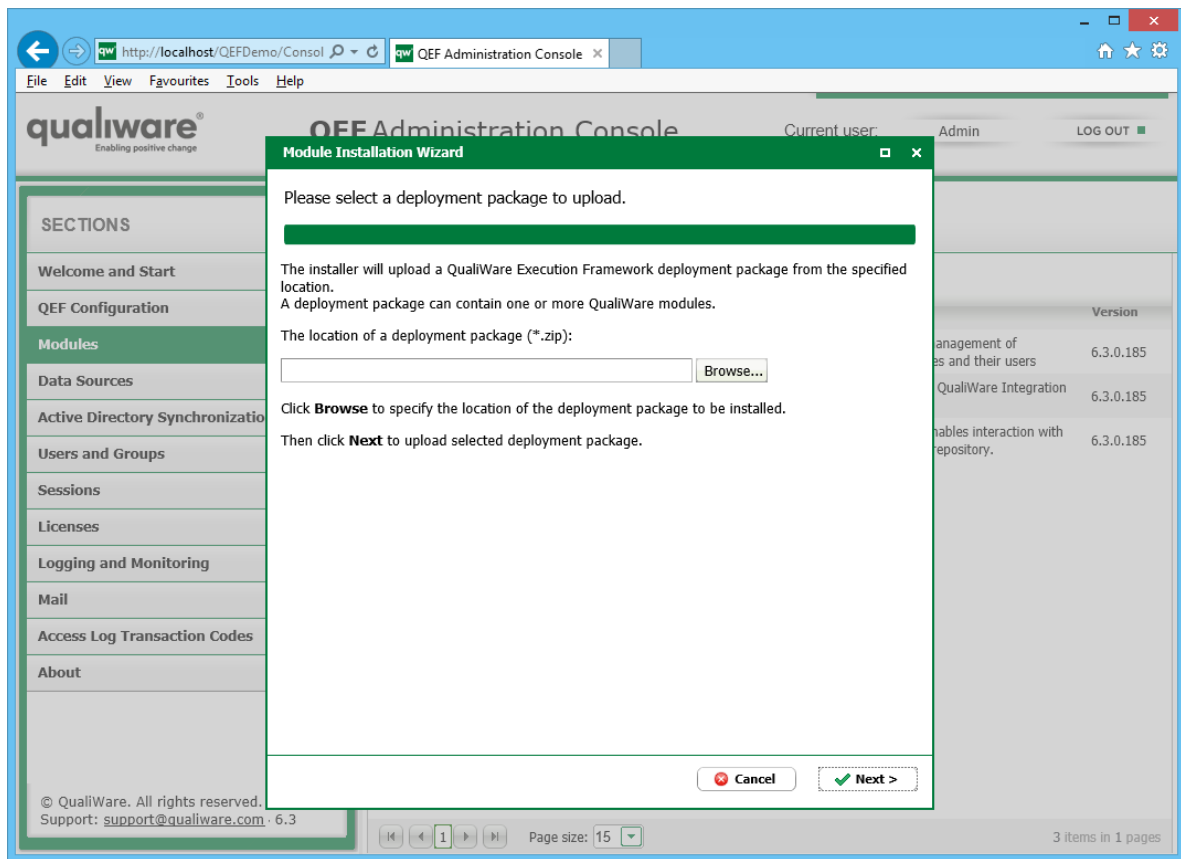


The screenshot shows the QualiWare QEF Administration Console interface. The left sidebar contains a 'SECTIONS' menu with 'Modules' highlighted. The main area is titled 'Modules' and features a toolbar with 'Start', 'Stop', 'Restart', 'Settings', 'Install', and 'Uninstall' buttons. Below the toolbar is a table of installed modules:

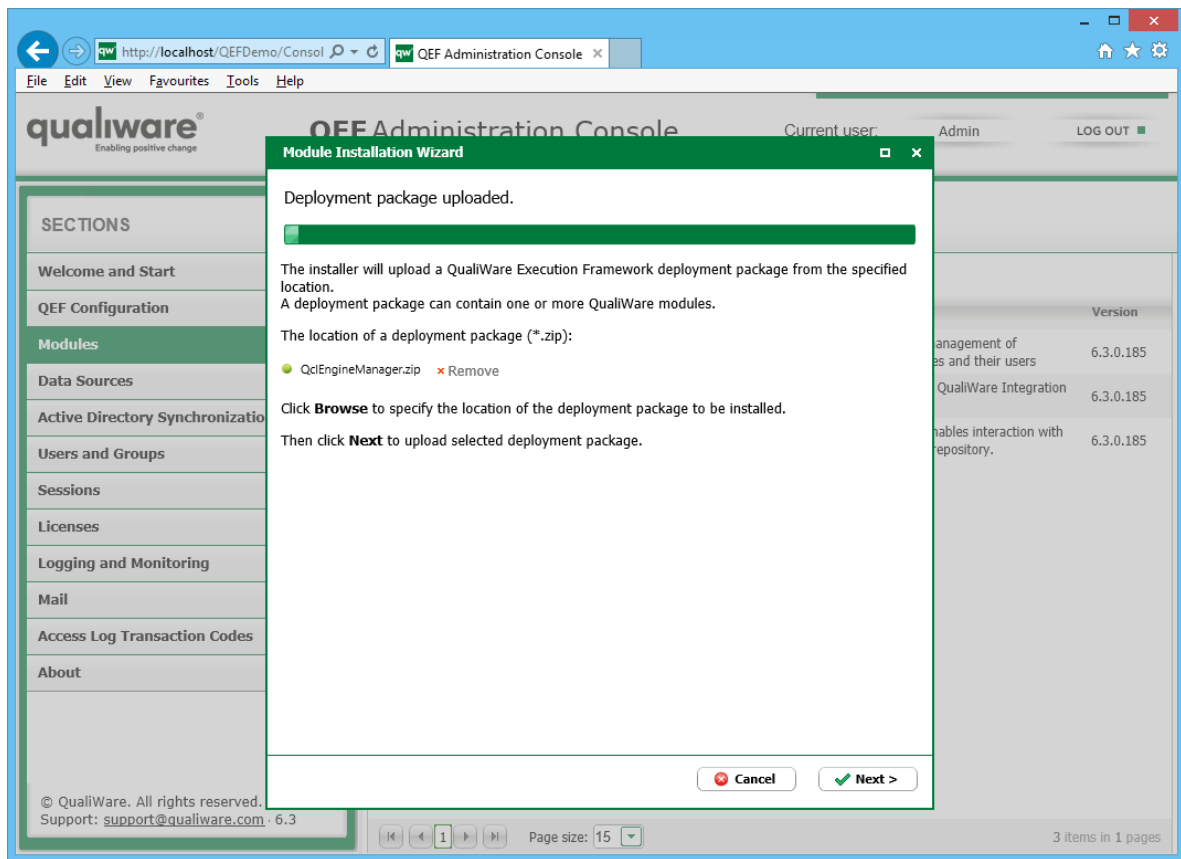
Name	Type	Status	Description	Version
<input type="checkbox"/> QIS Repository Administrator	Web	Running	QIS Repository Administrator enables management of QualiWare Integration Server repositories and their users	6.3.0.185
<input type="checkbox"/> QIS WebForms	Web	Running	QIS WebForms enables interaction with QualiWare Integration Server from Web.	6.3.0.185
<input type="checkbox"/> QualiWare Integration Server	Exe	Running	QualiWare Integration Server module enables interaction with QualiWare Lifecycle Manager database repository.	6.3.0.185

At the bottom of the console, there is a footer with copyright information: © QualiWare. All rights reserved. Support: support@qualiware.com · 6.3. Page size is set to 15, and there are 3 items in 1 page.

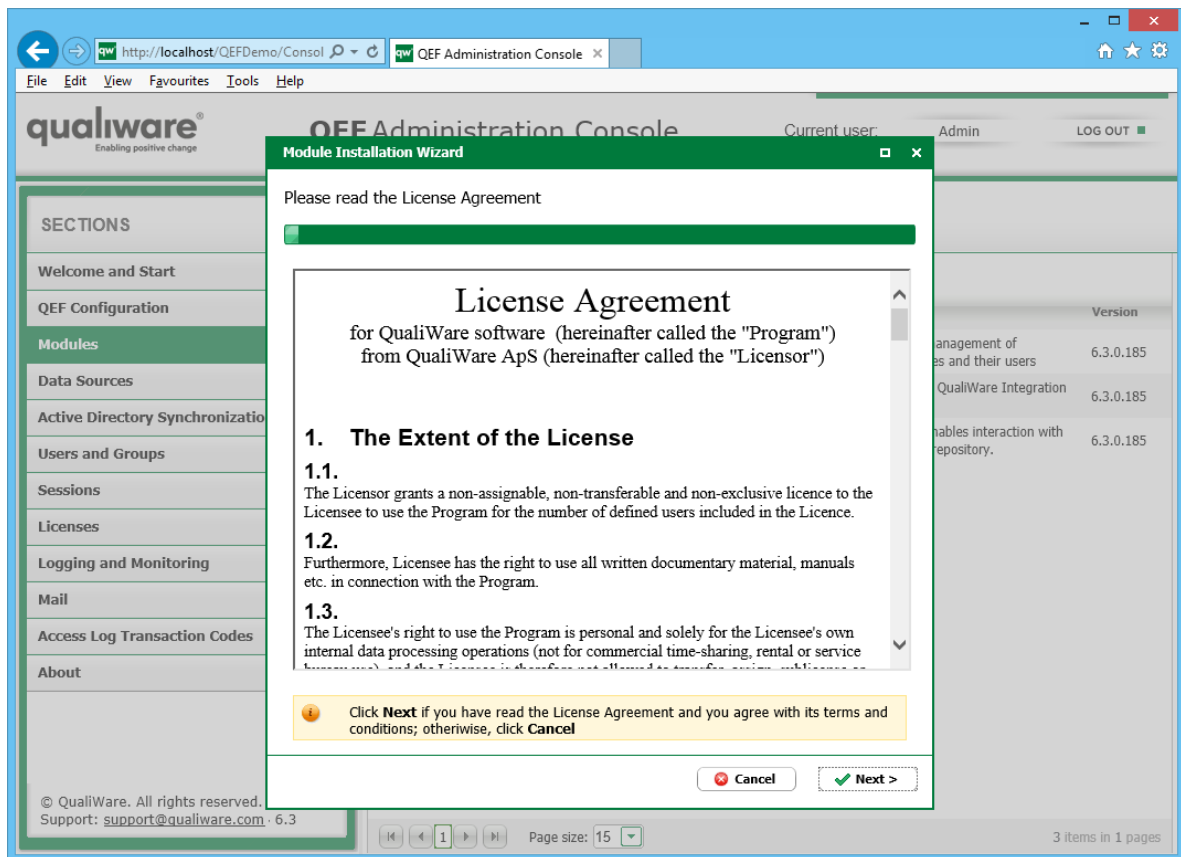
20. Click **Browse** and select modules deployment package (zip archive).



3. When deployment package is uploaded, click **Next**.

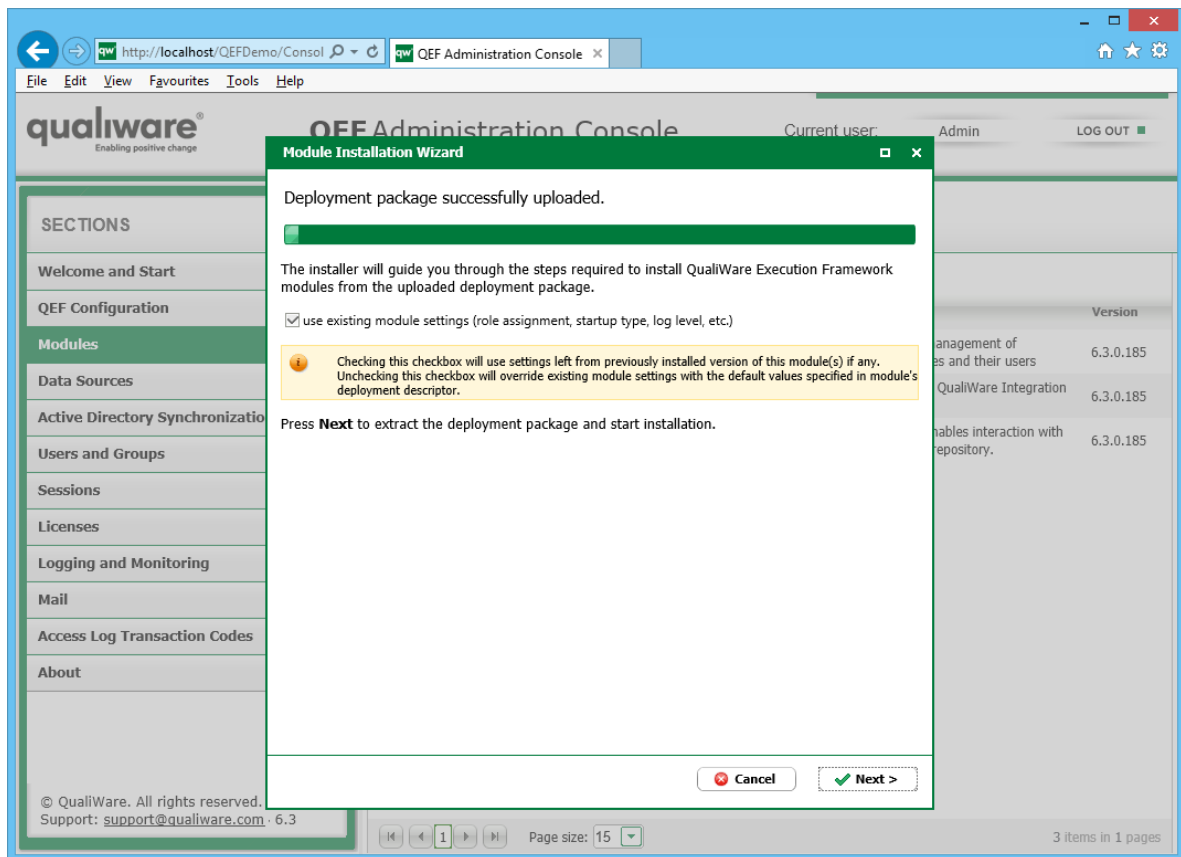


4. After reading the license agreement click **Next**.

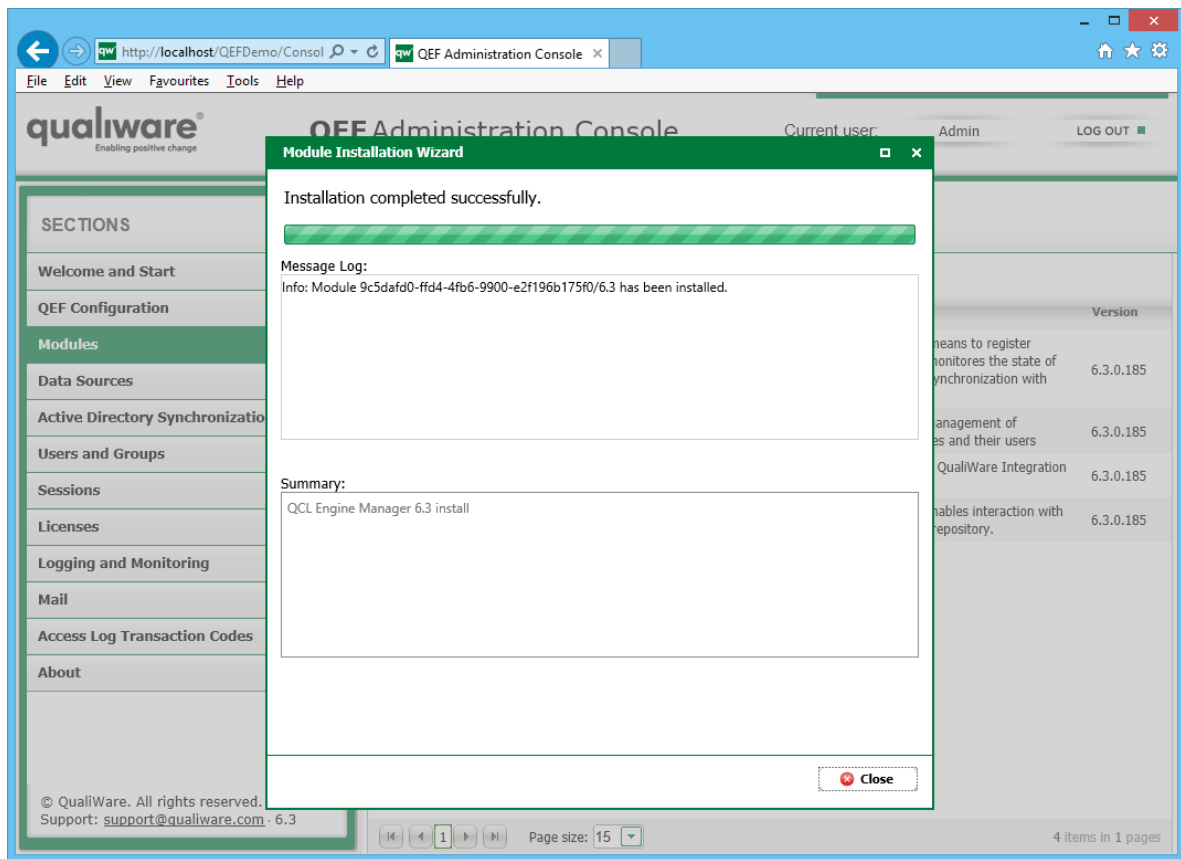


5. Enable or disable **use existing module settings**. Enabling it allows use of module settings from the previous installation. Click **Next**.

NOTE: In case the module update is performed, it is advised to use existing module settings in order to persist registered QCL Engine instances data and other module settings; otherwise, the data will be destroyed.



- Review installation log and click **Close**. If installation fails, see QEF log for error details.



4.5 Advanced Setup

QCLE module maintains a connection with all QCLE instances in order to issue commands or serve requests. In order to perform this task, local named pipe channel is setup every time instance is started by means of QCLE module. Named pipe channel is created with the use of Microsoft WCF technology and is configured the same way any other channel is.

By default, channel will have unique auto-generated name. In case there is a compelling need to change this behavior, please perform the following:

1. Open **Explorer**.
2. Go to **QEF Installation Folder**.
3. Go to **Modules**.
4. Go to **QCL Engine Manager**. Open the version you're configuring.
5. Edit **Qem.Module.exe.config** file, **serviceModel** section, **endpoint** configurations.

NOTE: In case of erroneous channel specification QCLE instances will be stopped and restarted invariably.

4.6 Data Migration

NOTE: It is highly recommended to avoid tampering with internal QCLE data since it is prone to change; for migration purposes, simple **upgrade procedure would suffice in most scenarios.**

QCLE module doesn't create its own data storage, instead it utilizes settings to store data. To access internal QCLE data, following steps are to be performed:

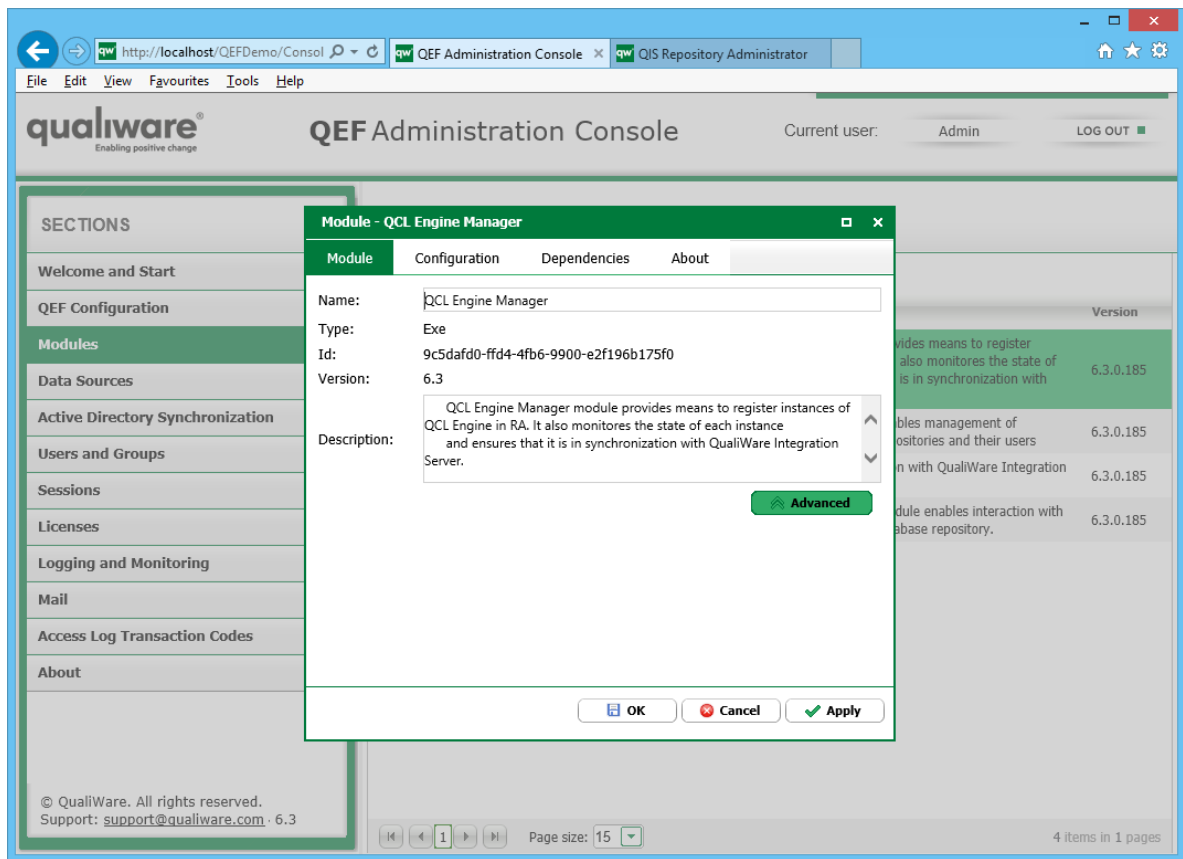
1. Open Admin **Console** -> **Modules**.
2. Select **QCLE Manager**.
3. Click **Settings**.

The screenshot shows the QualiWare QEF Administration Console interface. On the left, a sidebar menu lists various sections, with 'Modules' highlighted. The main content area displays a table of installed modules. The 'QCLE Manager' module is checked and its status is 'Running'. Below the table, there are navigation controls and a footer with copyright information.

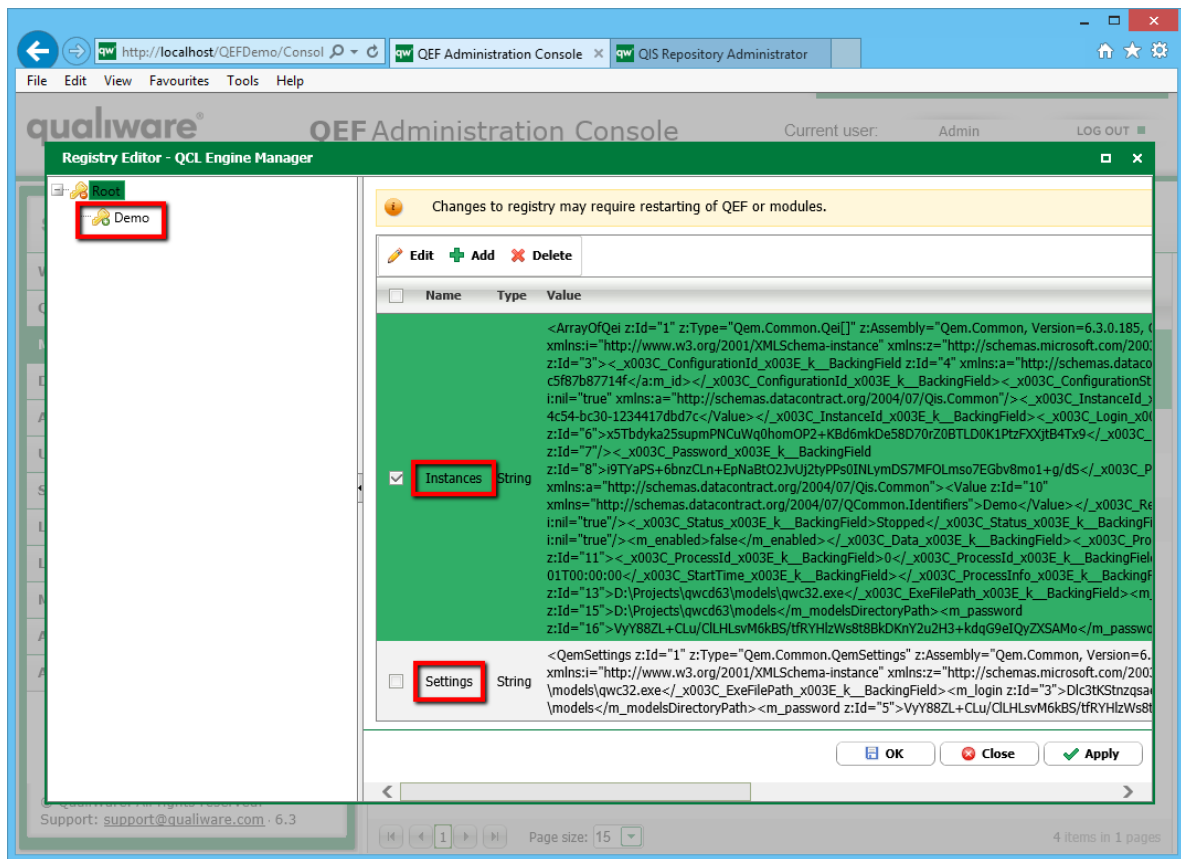
Name	Type	Status	Description	Version
<input checked="" type="checkbox"/> QCL Engine Manager	Exe	Running	QCL Engine Manager module provides means to register instances of QCL Engine in RA. It also monitors the state of each instance and ensures that it is in synchronization with QualiWare Integration Server.	6.3.0.185
<input type="checkbox"/> QIS Repository Administrator	Web	Running	QIS Repository Administrator enables management of QualiWare Integration Server repositories and their users	6.3.0.185
<input type="checkbox"/> QIS WebForms	Web	Running	QIS WebForms enables interaction with QualiWare Integration Server from Web.	6.3.0.185
<input type="checkbox"/> QualiWare Integration Server	Exe	Running	QualiWare Integration Server module enables interaction with QualiWare Lifecycle Manager database repository.	6.3.0.185

© QualiWare. All rights reserved.
Support: support@qualiware.com · 6.3

4. Click **Advanced**.



For each repository, a separate key in the registry is created. Registry key is named after repository identifier.



Each registry key contains 2 settings – **Instances** and **Settings**. **Instances** contain data for all QCLE instances (configuration identifier, username, password, working directory); **Settings** contain instance-agnostic data – path to QEI executable.

NOTE: Any changes to settings may cause QCLE module to crash and is not currently supported. Use at your own discretion.

To execute a migration, full structural contents copy should be executed manually.

5 SharePoint

5.1 Preface

This document describes installation and configuration of QualiWare Document Connector (hereinafter QDC).

5.2 Prerequisites

The document assumes that QualiWare Execution Framework (hereinafter QEF) is installed. As a client Web Forms and/or QualiWare Lifecycle Manager (hereinafter QLM) may be installed, but not required.

License in QEF is required for QDC to work with SharePoint server.

Some of the configuration steps may require domain administrator permissions.

5.3 Supported Servers

Supported server operating systems: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2.

Supported SharePoint Servers: SharePoint Server 2010, SharePoint Server 2013.

5.4 Installation of QualiWare Document Connector

// TODO

5.5 Configuration of List of SharePoint Servers

Before QDC can connect to any SharePoint server, a list of SharePoint servers must be defined.

To define list of SharePoint servers follow these steps:

1. Open **Admin Console** -> **Modules**.
2. Select **QualiWare SharePoint Connector**.
3. Click **Settings**.
4. On **Module** tab click **Advanced** button.
5. Click **Add**.
6. Set name **Settings**, select type **String**.
7. Insert this string in JSON format and change Urls and names to yours:

```
{
  "Servers": [
    {
      "Name": "Friendly name for server 1",
      "Url": "your server 1 address here",
      "Type": "Qdc.QualiWare.Connectors.SharePoint"
    },
    {
      "Name": "Friendly name for server 2",
      "Url": "your server 2 address here",
      "Type": "Qdc.QualiWare.Connectors.SharePoint"
    }
  ],
  "ContentProvider": "Qdc.Providers.QualWare"
}
```

Example:

```
{
  "Servers": [
    {
      "Name": "Default SharePoint Server",
      "Url": "http://sharepoint/",
      "Type": "Qdc.QualiWare.Connectors.SharePoint",
      "Path": "Test/Shared Documents"
    }
  ],
  "ContentProvider": "Qdc.Providers.QualWare",
  "DefaultServerName": "Default SharePoint Server"
}
```

List can contain any number of servers. Add them in a similar way.

Make sure addresses that are set above are the same as in module license(s).

8. Click **Add**.
9. Click **OK**.

5.6 Permissions

In order for user to browse SharePoint libraries using QualiWare SharePoint Connector module (Document Browser), user must have read permission. **Read Permission Level** by default does not include **Browse Directories** permission. To grant minimal read permission:

1. Open SharePoint site.
2. Go to **Site Actions -> Site Permissions -> Permission Levels**.
3. Click on **Read** permission level.
4. Click **Copy Permission Level**.
5. Give name to new permission level.
6. Check **Browse Directories** under **Site Permissions**.
7. Click **Submit**.
8. Assign created permission level to user or group, which needs read access to SharePoint site.

5.7 Configuration of Single Sign-On

QDC supports Single Sign-On when no password is required to connect to SharePoint server.

5.7.1 Prerequisites

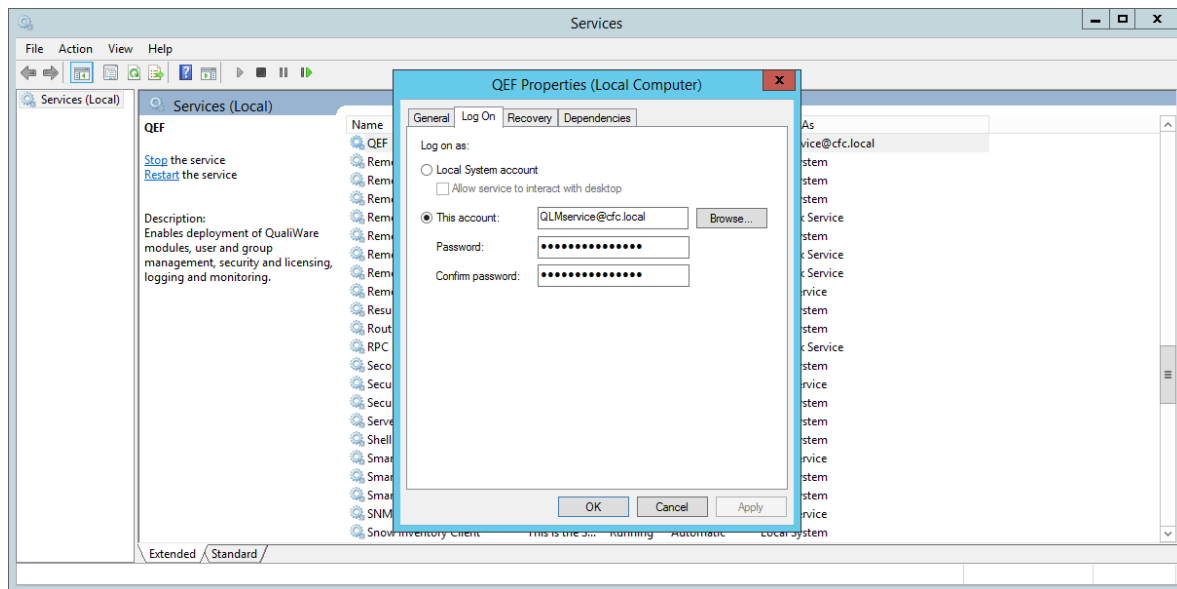
By default **QEF** Windows service is run using **LocalSystem** account and all Application Pools in IIS are run under **ApplicationPoolIdentity**. Despite the fact that this is a correct configuration, it is advised to use domain service account to run **QEF** Windows service and Application Pool.

5.7.2 Log on as for Windows Service

It is advised to specify domain service account used to run **QEF** Windows service during **QEF** installation. Otherwise the setting will be restored back to its original value, when **QEF** is re-installed, upgraded or re-configured.

To set domain service account as account to run **QEF** Windows service:

1. Open **Windows Services**.
2. Right-click **QEF** Windows service and select **Properties**.
3. Open **Log On** tab.
4. Select **This account**.
5. Enter domain service account credentials.



6. Click **OK**.
7. Restart **QEF** Windows service.

5.7.3 Update Configuration Files

1. .NET Remoting must be setup to use secure channel. Modify:
 - **Program Files\QualiWare\QEF\Bin\Qef.exe.config**
 - Configuration files of all installed modules and QLM

Section:

```
<configuration>
  <system.runtime.remoting>
    <application name="QEF">
      <channels>
        <channel secure="true"/>.
      </channels>
    </application>
  </system.runtime.remoting>
</configuration>
```

2. Impersonation level must be set to impersonate. Modify:
 - **Program Files\QualiWare\QualiWare Execution Framework\Bin\Qef.exe.config**
 - **Program Files\QualiWare\QualiWare Execution Framework\Modules\QualiWare Integration Server\6.0\Qis.exe.config**
 - **Program Files\QualiWare\QEF\Web\Console\Web.config**
 - **Program Files\QualiWare\QEF\Web\WebModules\QIS WebForms\6.0\Web.config**

Section:

```
<configuration>
  <system.runtime.remoting>
    <application name="QEF">
      <channels>
        <channel secure="true" tokenImpersonationLevel="impersonation">
```

3. Impersonation must be enabled. Modify:

- **Program Files\QualiWare\QEF\Modules\QualiWare SharePoint Connector\6.0\Bin\Qdc.Module.exe.config**

Section:

```
<configuration>
  <system.runtime.remoting>
    <application name="QEF">
      <channels>
        <channel secure="true" impersonate="true">
```

4. Impersonation level must be set to delegation and **servicePrincipalName** must be set to server or domain service account. Modify:

- **Program Files (x86)\QualiWare\QLM\models\qwcd32.exe.config**

- a. SPN of server where **QEF** Windows service is running, if it is running under **LocalSystem** account.

Section:

```
<configuration>
  <system.runtime.remoting>
    <application name="QEF">
      <channels>
        <channel secure="true" tokenImpersonationLevel="Delegation"
servicePrincipalName="HTTP/<server_name>">
```

- b. Domain service account, if **QEF** Windows service is running under domain service account.

Section:

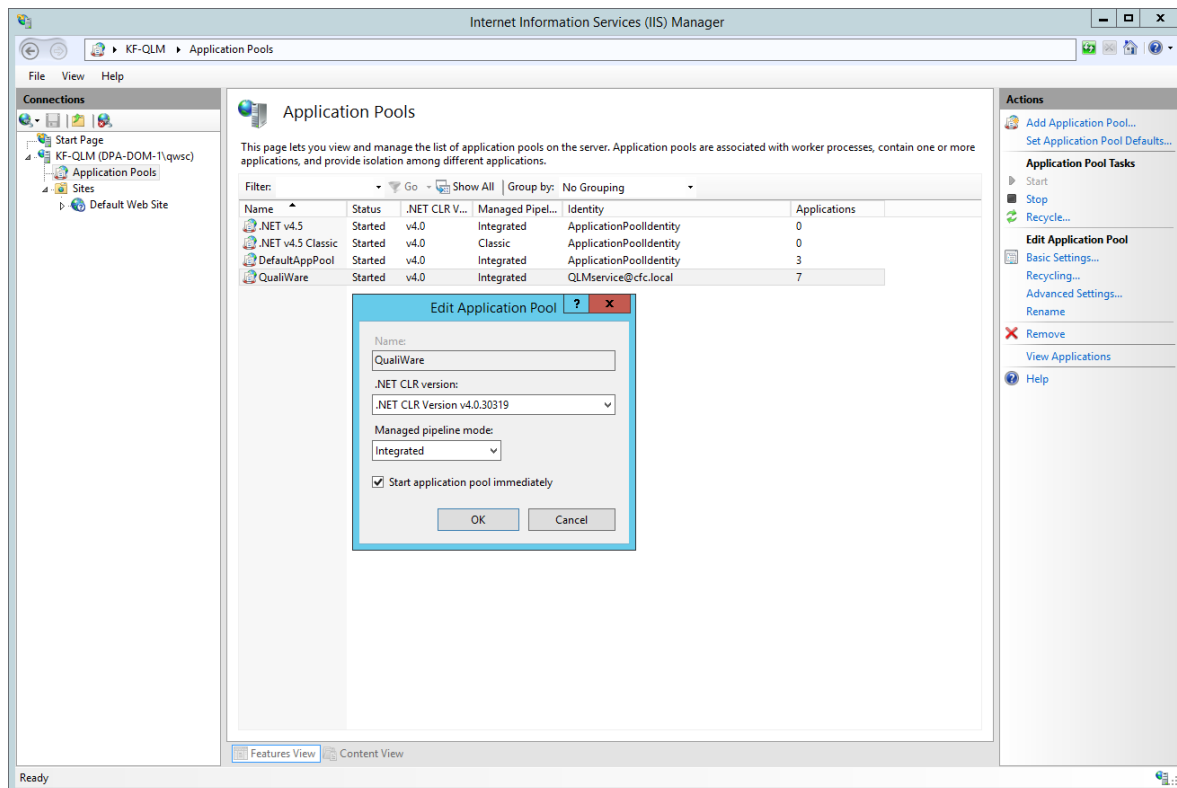
```
<configuration>
  <system.runtime.remoting>
    <application name="QEF">
      <channels>
```

```
<channel secure="true" tokenImpersonationLevel="Delegation"
servicePrincipalName="<qef_account>@<domain_name>">
```

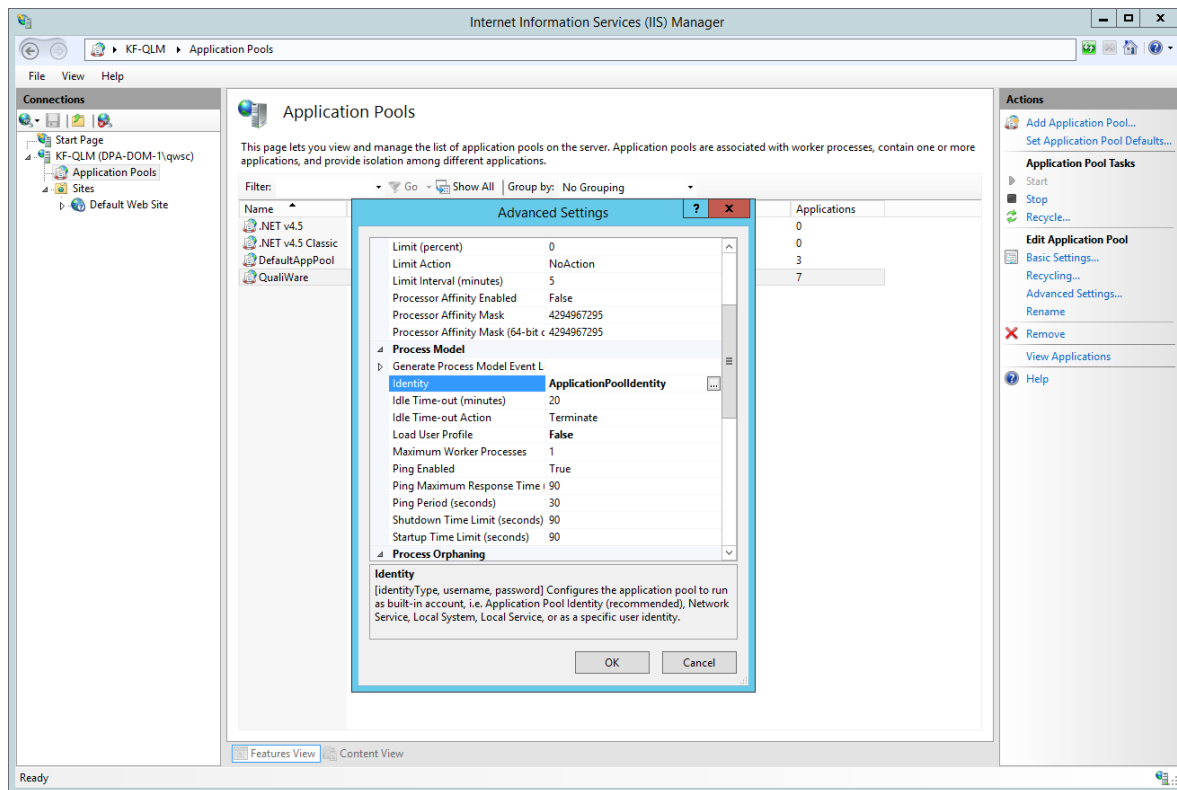
5.7.4 Internet Information Services (IIS) Configuration

5.7.4.1 IIS Application Pool

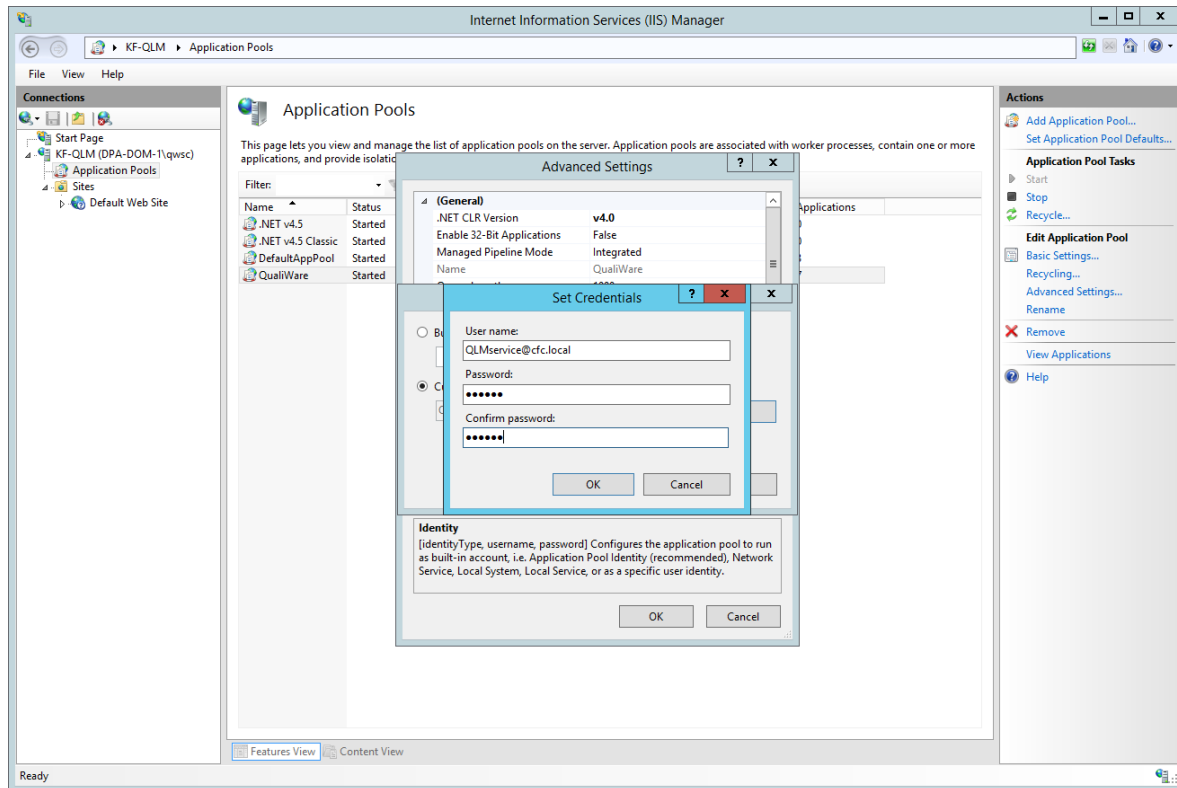
1. Open **Internet Information Services (IIS) Manager**.
2. Select **Application Pools**.
3. Click **Add Application Pool...** action.
4. In **Name** enter **QualiWare**.
5. In **.NET Framework version** select the **.NET Framework v4.0**.
6. In **Managed pipeline mode** select **Integrated**.



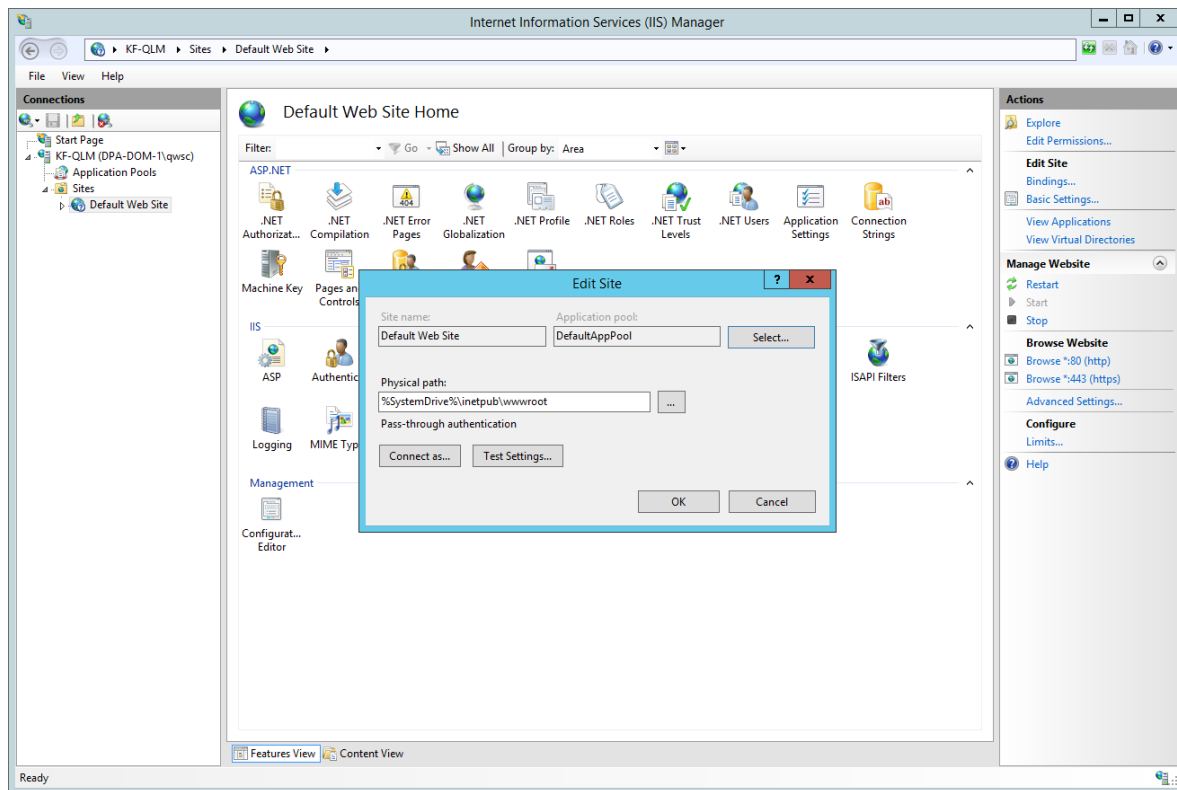
7. Click **OK**.
8. Click on the application pool and click **Advanced Settings...** action.
9. Select Identity setting and click **Browse...** button.



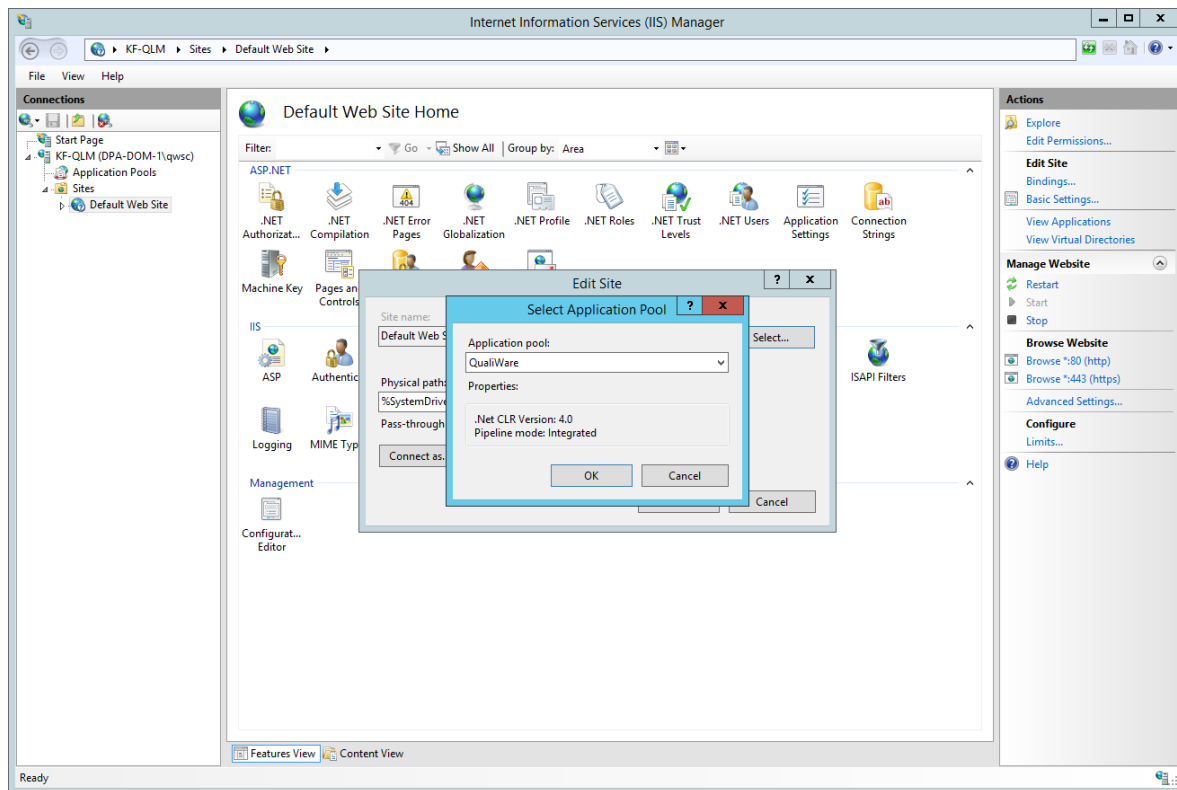
10. Select **Custom Account** and click **Set...** button.
11. Enter domain service account credentials and click **OK**.



12. Select **Default Web Site**.
13. Click **Basic Settings...** action.
14. Click on the **Select...** button.



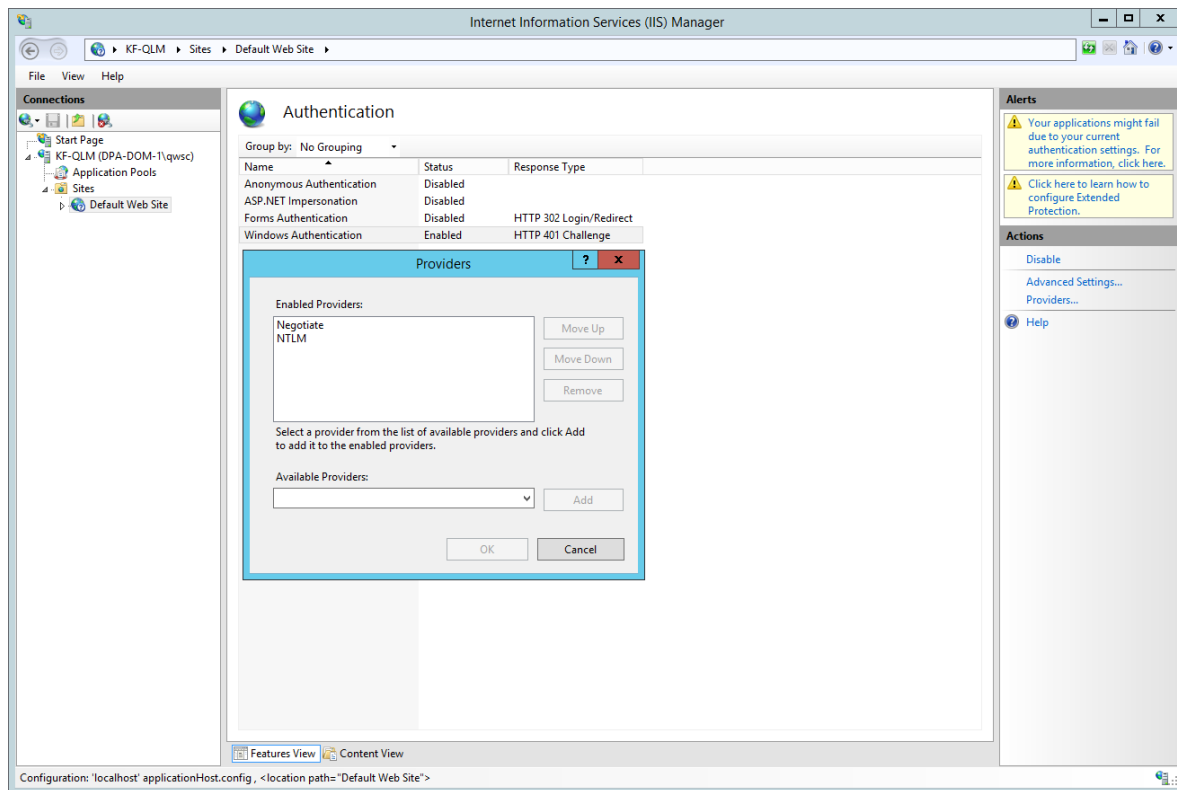
15. Select the application pool named **QualiWare** and click **OK**.



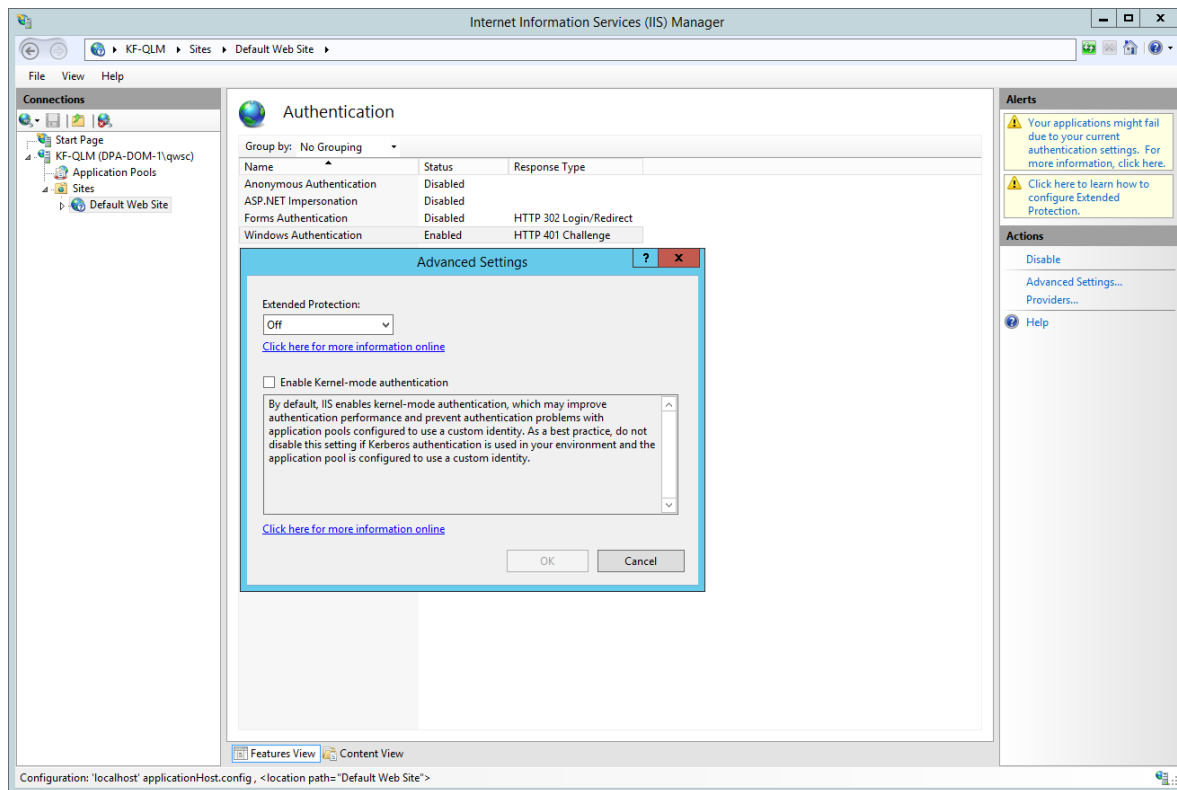
16. Ensure that the Application Pool is used by all virtual directories. By default it should be automatically inherited.

5.7.4.2 Enable Windows Authentication.

1. Open **Internet Information Services (IIS) Manager**.
2. Select **Default Web Site**.
3. Double-click **Authentication**.
4. Right-click on **Windows Authentication** and select **Enable**.
5. Select **Windows Authentication** and click **Providers...** action.
6. Ensure **Negotiate** is in the list of **Enabled Providers** and select it.
7. Click **Move Up** button to move **Negotiate** to the top and click **OK**.



8. Click **Advanced Settings...** action.
9. Ensure **Enable Kernel-mode authentication** is unchecked and click **OK**.



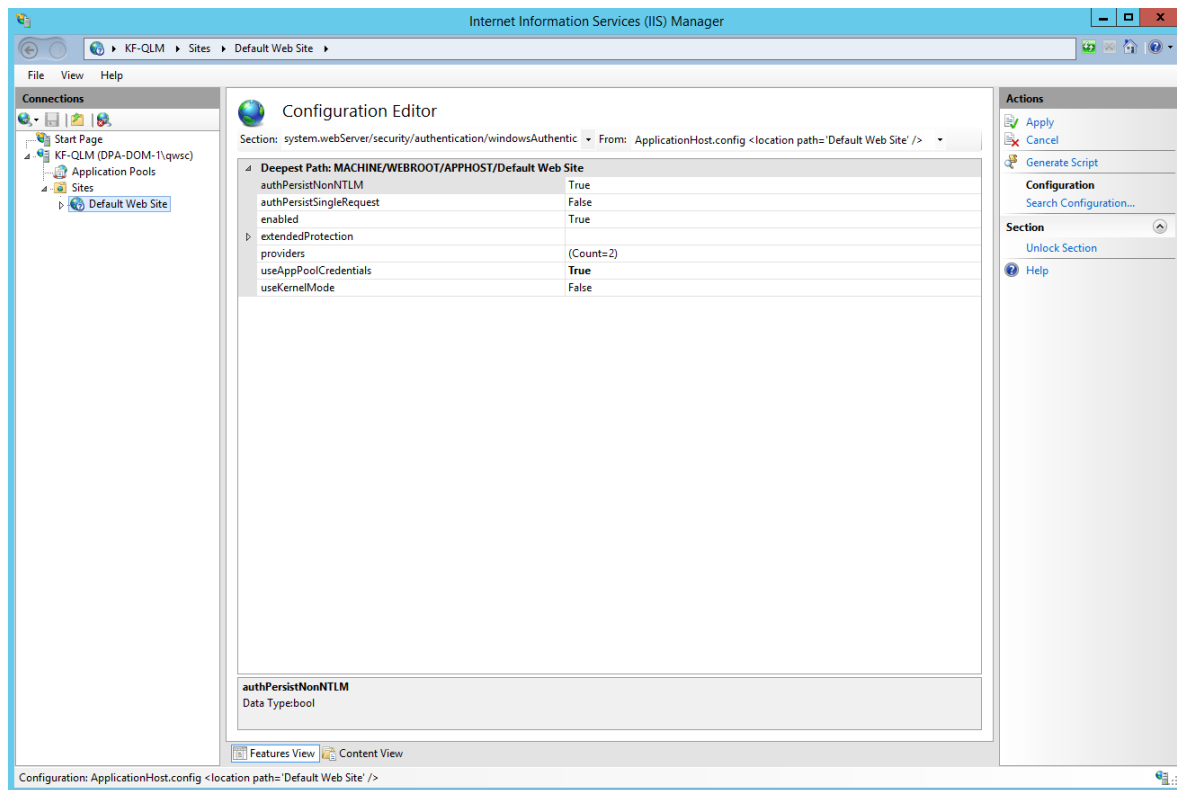
10. Select **Default Web Site**.
11. Double-click **Configuration Editor**.
12. Select in **Section**:

system.webServer/security/authentication/windowsAuthentication

13. Select in **From**:

ApplicationHost.config

14. Set **useAppPoolCredentials** to **True**.
15. Set **useKernelMode** to **False**.

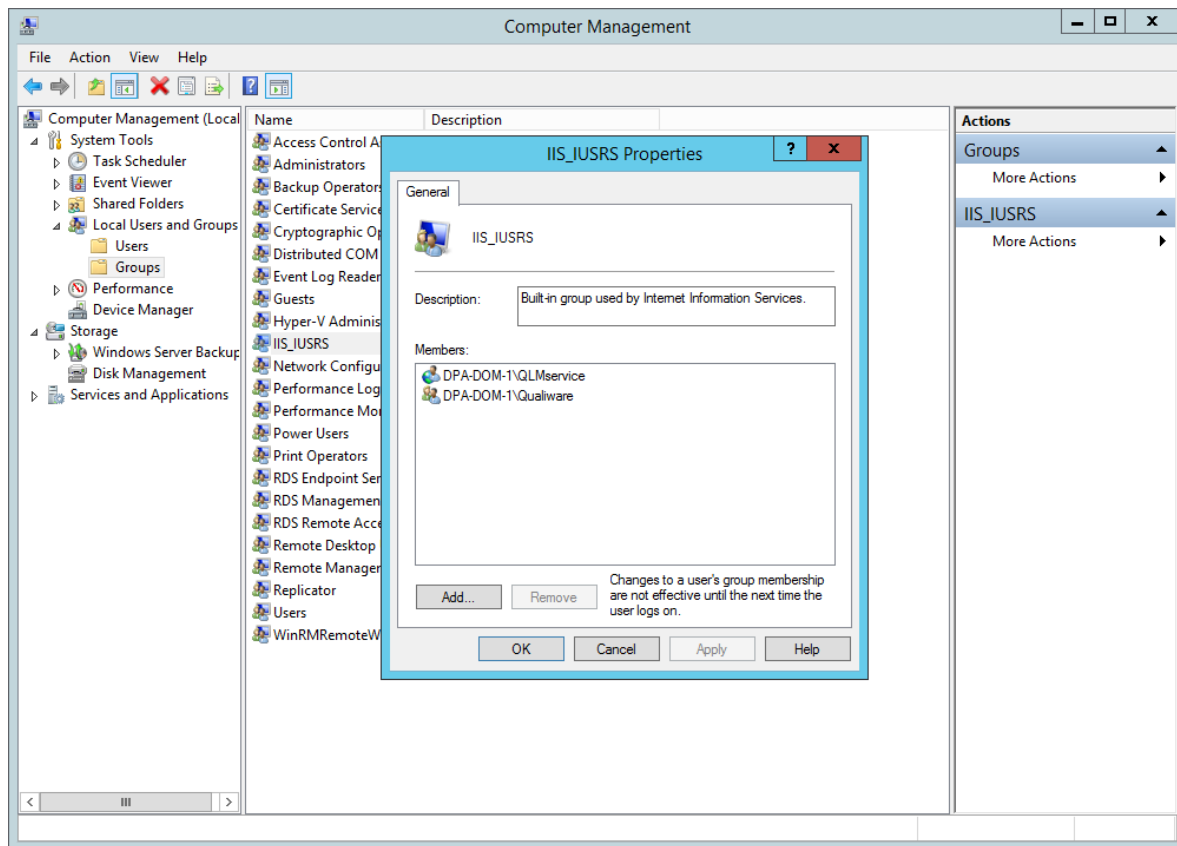


16. Click **Apply** action.

17. Ensure that the Windows Authentication settings are used by all virtual directories. By default they should be automatically inherited.

5.7.4.3 Add domain Service Account to IIS_IUSRS Group

1. Open **Computer Management** MMC and navigate to **Local Users and Groups -> Groups**
2. Double-click on the **IIS_IUSRS** local group.



3. Add domain service account to the group and click **OK**.

5.7.5 Create SPNs

Service Principal Name (SPN) must be created, if **QEF** Windows service is running under domain service account.

5.7.5.1 Server and Domain Service Account

Create SPN for domain service account under which **QEF** Windows service and IIS Application Pool are running. SPN is registered with **setspn** command (this command is performed on computer in the same domain as the target computer by domain administrator):

```
setspn -A http/<qef_server_name> <domain_name>\<qef_account>
```

<qef_server_name> – domain name of the machine, where QEF is running

<qef_account> – domain account, under which QEF is running

Important: SPN must be registered for NetBIOS and UPN names of server. The same is applied to SharePoint server (see below). For viewing existing SPNs, use one of the following commands:

```
setspn -L <domain_name>\<qef_account>
```

```
setspn -Q http/<qef_server_name>
```

To register SPNs, use the following commands:

```
setspn -S http/rctest <domain_name>\<qef_account>  
setspn -S http/rctest.qualiware.local <domain_name>\<qef_account>
```

Note: For Windows Server 2003 use:

```
setspn -L <domain_name>\<qef_account>  
setspn -A http/rctest <domain_name>\<qef_account>  
setspn -A http/rctest.qualiware.local <domain_name>\<qef_account>
```

5.7.5.2 SharePoint

When SharePoint server is installed, SPN is set for the server automatically. Make sure that SPN for SharePoint server is registered for NetBIOS and UPN names of server. For viewing existing SPNs, use one of the following commands:

```
setspn -L <domain_name>\<qef_account>  
setspn -Q http/<sharepoint_server_name>
```

To register SPNs, use the following commands:

```
setspn -S http/sharepoint2010 <domain_name>\<sharepoint_account>  
setspn -S http/sharepoint2010.qualiware.local <domain_name>\<sharepoint_account>
```

Note: For Windows Server 2003 use:

```
setspn -L <domain_name>\<sharepoint_account>  
setspn -A http/sharepoint2010 <domain_name>\<sharepoint_account>  
setspn -A http/sharepoint2010.qualiware.local <domain_name>\<sharepoint_account>
```

Example of correct SPNs for server, domain service account and SharePoint:

```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>setspn -Q */kf-qlm
Checking domain DC=cfc,DC=local
CN=KF-QLM,OU=KFServerAuto05,OU=KF Computers,DC=cfc,DC=local
    WSMAN/kf-qlm.cfc.local
    WSMAN/kf-qlm
    TERMSRU/KF-QLM
    TERMSRU/KF-QLM.cfc.local
    RestrictedKrbHost/KF-QLM
    HOST/KF-QLM
    RestrictedKrbHost/KF-QLM.cfc.local
    HOST/KF-QLM.cfc.local
CN=Qualiware service bruger,OU=SystemUsers,DC=cfc,DC=local
    http/kf-qlm
    http/kf-qlm.cfc.local
    http/kf-qlmtest.cfc.local
    http/kf-qlmtest

Existing SPN found!

C:\Windows\system32>setspn -L QLMservice
Registered ServicePrincipalNames for CN=Qualiware service bruger,OU=SystemUsers,
DC=cfc,DC=local:
    http/kf-qlm
    http/kf-qlm.cfc.local
    http/kf-qlmtest.cfc.local
    http/kf-qlmtest

C:\Windows\system32>setspn -Q */pelsen.kopenhagenfur.com
Checking domain DC=cfc,DC=local
CN=svcSPapp13,OU=SP2013,DC=cfc,DC=local
    http/admin
    http/admin.kopenhagenfur.com
    http/Projectflow
    http/Projectflow.kopenhagenfur.com
    http/inside.kopenhagenfur.com
    http/inside
    http/pelsen
    http/pelsen.kopenhagenfur.com
    http/root
    http/root.kopenhagenfur.com

Existing SPN found!

C:\Windows\system32>_

```

5.7.6 Trust for Delegation

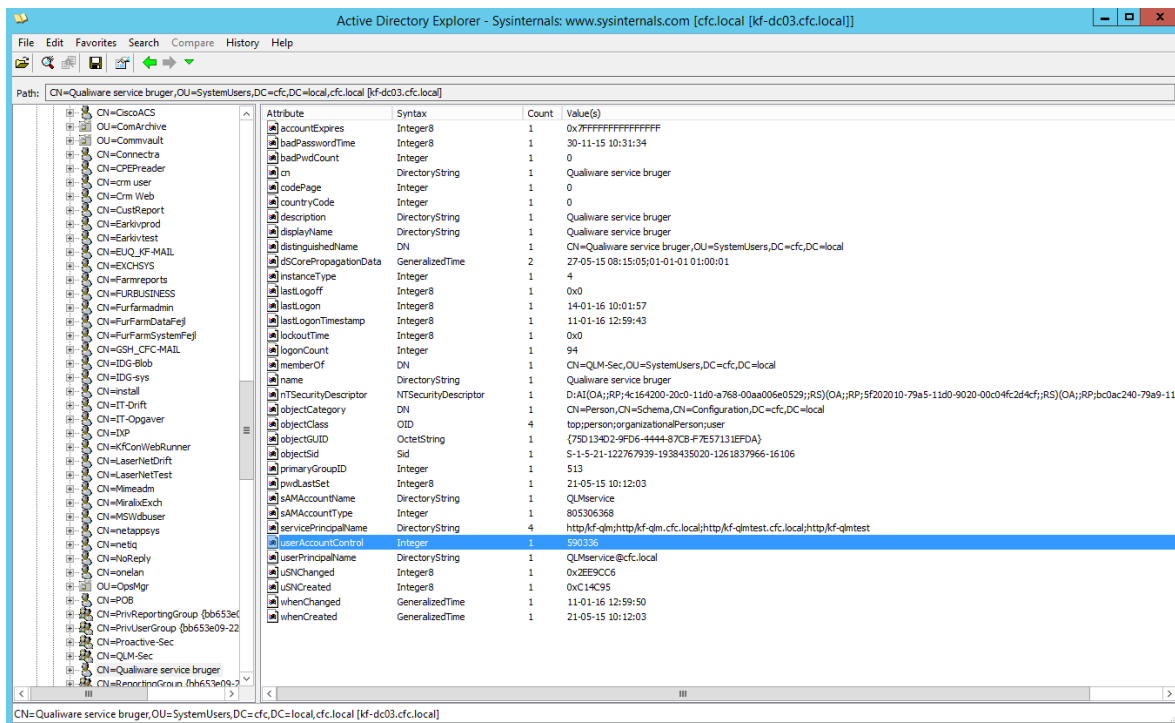
Server and domain service account must be enabled to be trusted for delegation.

5.7.6.1 Enable Server to be Trusted for Delegation

Setup server on which QEF is installed to be trusted for delegation. This action is performed on domain controller computer by domain administrator. For this:

2. Select domain and under **Users** node find domain service account.
3. Right-click the user and select **Properties**.
4. On Delegation tab select **Trust this user for delegation to any service (Kerberos only)**.
5. Click **OK**.

It is often that only domain administrator has access to domain controller. This makes it time-consuming to check that domain service account is enabled to be trusted for delegation. Alternatively to check if domain service account is enabled to be trusted for delegation, **ADExplorer** (from Sysinternals) can be used. To do so, connect to domain controller with **ADExplorer** and find domain service account. Inspect the value of **userAccountControl** property. If the value is less than 524288, it is an indication of that server is not enabled to be trusted for delegation.



For list of possible flags for **userAccountControl** property, refer to

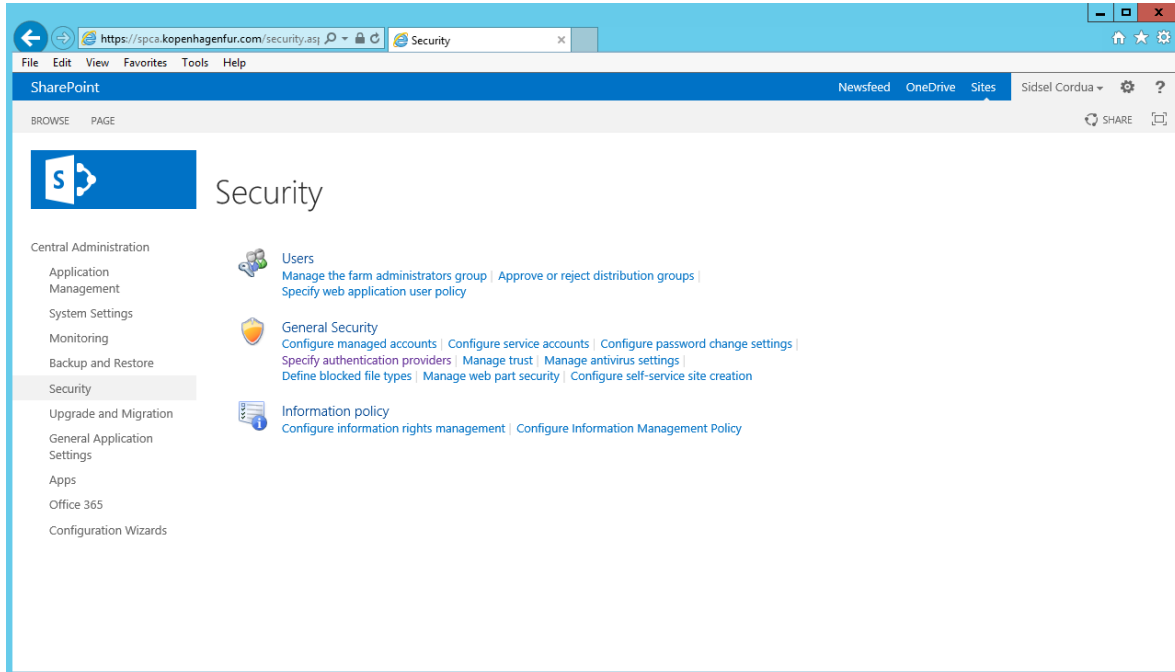
<https://support.microsoft.com/en-us/kb/305144>

5.7.7 Enable Integrated Windows Authentication (Kerberos) in SharePoint

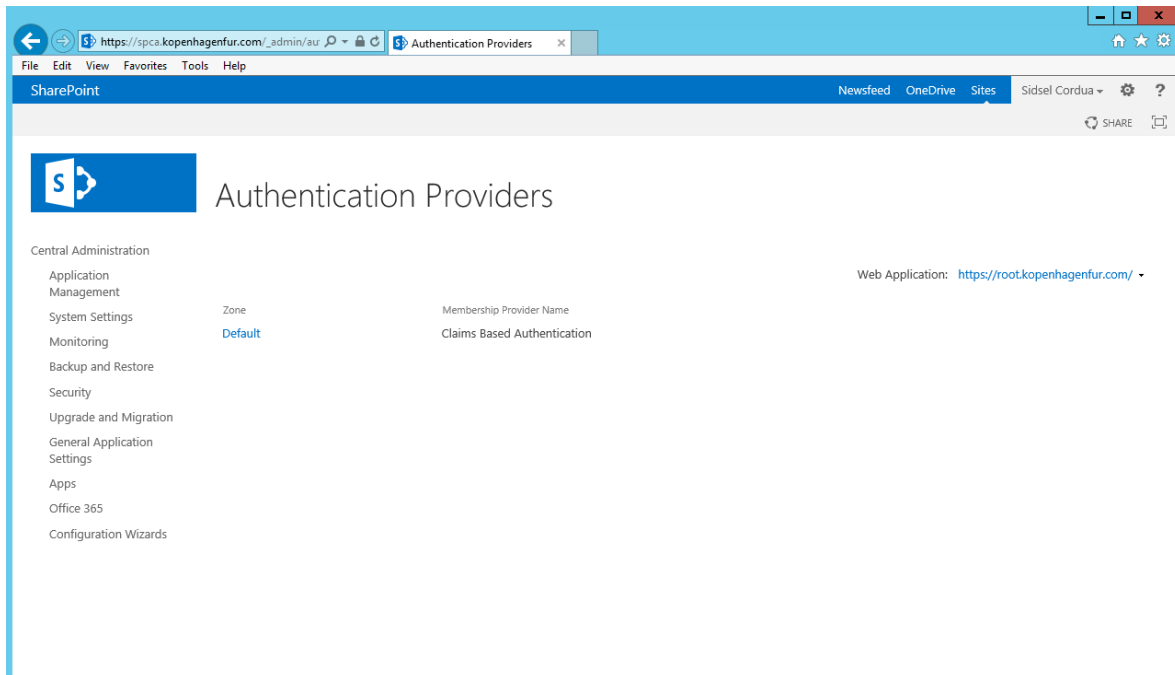
By default SharePoint uses NTLM provider for Windows authentication. To make SharePoint use Kerberos provider for Windows authentication:

1. Go to server where SharePoint is installed.
2. From Start menu open **SharePoint Central Administration**.

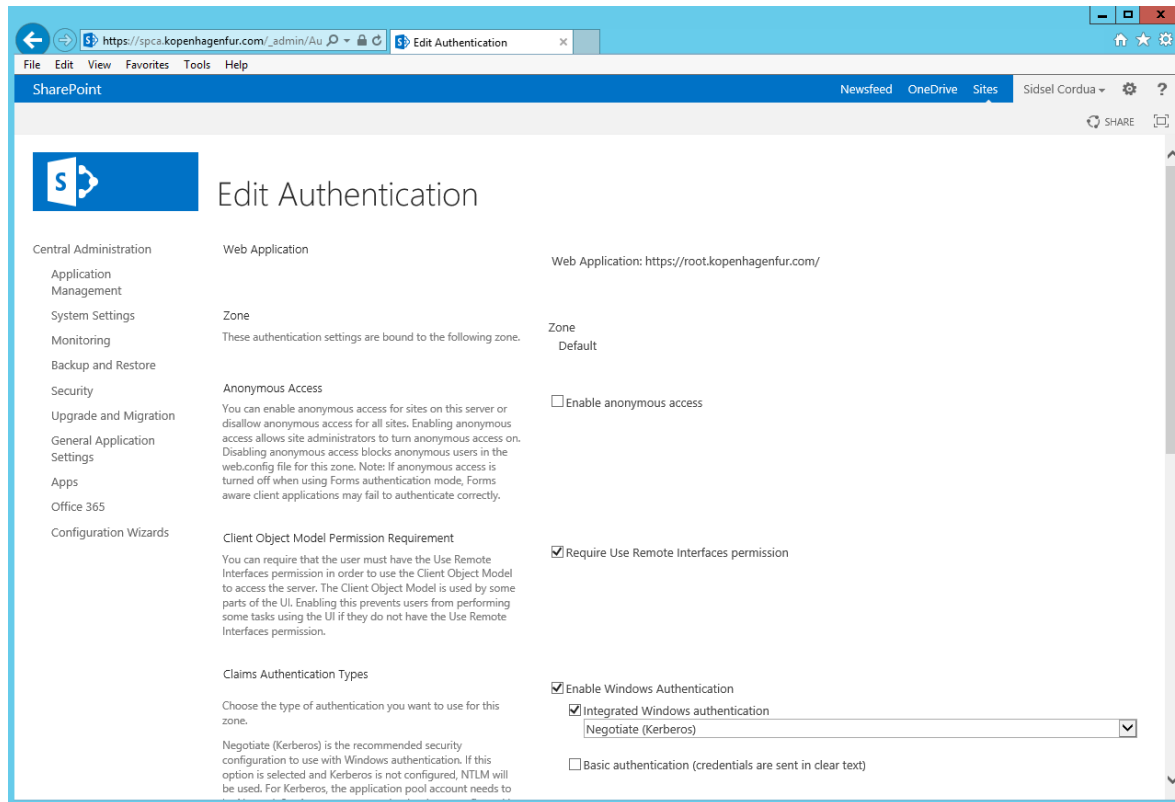
3. Go to **Security** -> **General Security** -> **Specify authentication providers**.



4. Click **Default** zone.



- Under **Claim Authentication Types** make sure that **Enable Windows Authentication** and **Integrated Windows authentication** are enabled and **Negotiate (Kerberos)** is selected.



- Click **OK**.

5.7.8 Legend

Screenshots are taken from the environment with the following data:

Domain: cfc.local (DPA-DOM-1)

Server name: kf-qlm

QEF service account: QLMservice@cfc.local

QualiWare application pool account: QLMservice@cfc.local

5.7.9 References

<http://blogs.msdn.com/b/chiranth/archive/2014/04/17/setting-up-kerberos-authentication-for-a-website-in-iis.aspx> - Describes how to configure Kerberos for IIS.

<http://blogs.msdn.com/b/friis/archive/2009/12/31/things-to-check-when-kerberos-authentication-fails-using-iis-ie.aspx> - Check list for Kerberos.

<https://platformadmin.com/blogs/paul/2012/03/sas-and-iwa-verify-trusted-for-delegation/> - Describes how to check if computer or user is enabled to be trusted for delegation.

<https://support.microsoft.com/en-us/kb/305144> - Describes values of **userAccountControl** property for computer and user in Active Directory.

<http://blogs.msdn.com/b/friis/archive/2013/01/08/asp-net-authentication-test-page.aspx> - Test page outputting information about authentication method used by current request.