

# Server Installation in Azure

# 1 Contents

1	Introduction.....	2
2	Overview.....	2
3	Prerequisites.....	3
3.1	MS SQL Server and Database .....	3
3.2	Virtual Machines.....	4
3.3	Azure Active Directory.....	4
3.3.1	Install Azure Active Directory Connect.....	4
3.3.2	Enable Single Sign On.....	4
4	Installing QualiWare Software.....	5
4.1	Synchronize with Azure Active Directory .....	5
4.1.1	Active Directory Connection.....	5
4.1.2	Azure Active Directory Connection.....	5
4.2	Enable HTTPS.....	6
4.2.1	Request an Internet Server Certificate.....	7
4.2.2	Install an Internet Server Certificate .....	7
4.2.3	Configure an HTTPS Binding .....	7
4.3	Configure redirection .....	7
4.3.1	Register DNS Name.....	7
4.3.2	Configure redirection.....	7
4.4	Create Web Application .....	10

# 1 Introduction

This document describes prerequisites for installing QualiWare in Azure, installation and configuration process. Installation and configuration process is very close to the process in on-premises environment. For this reason, where applicable, you will find references to the standard server installation document.

# 2 Overview

Below is comparison of QualiWare in on-premises and Azure environment.

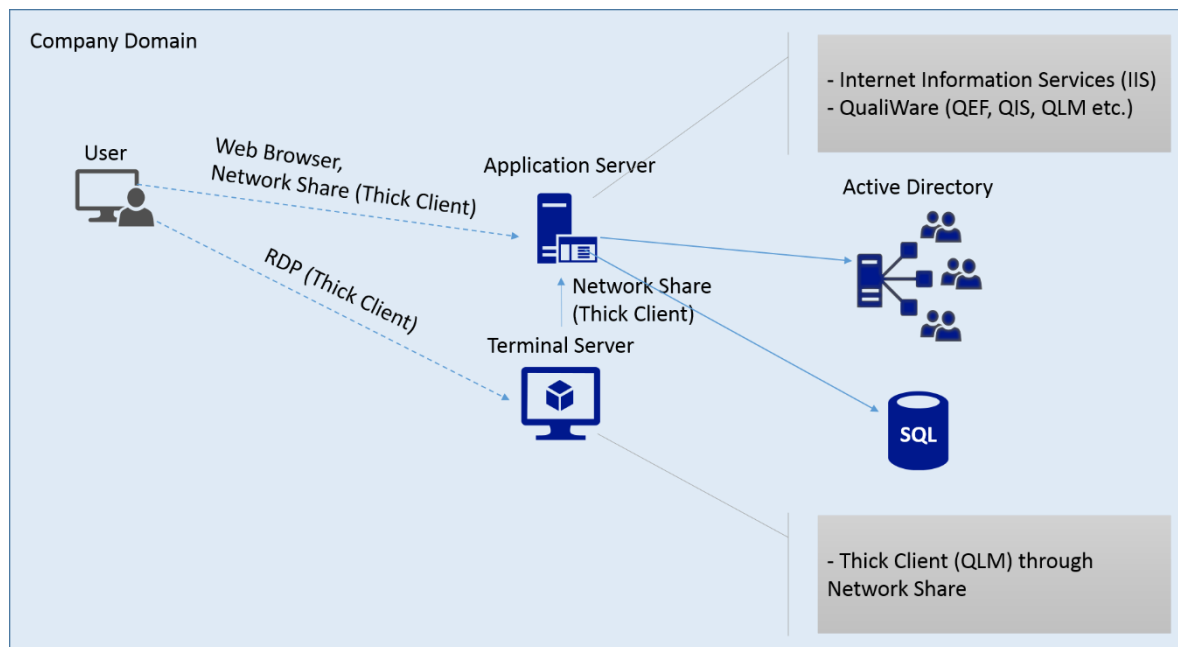


Figure 1 QualiWare in on-premises environment.

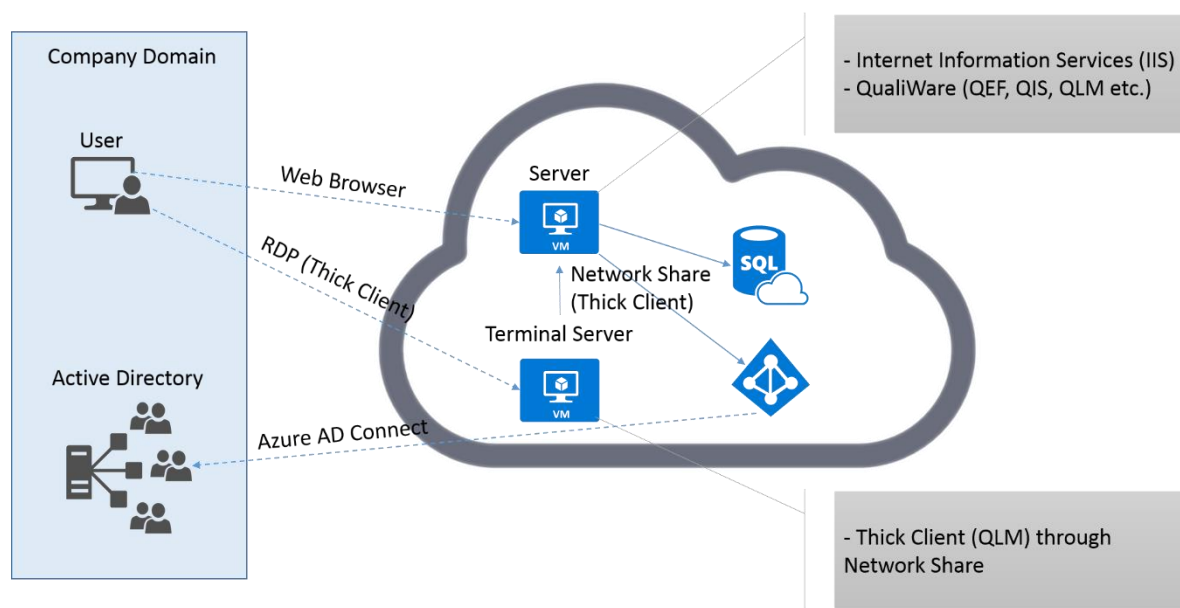


Figure 2 QualiWare in Azure environment.

### 3 Prerequisites

Before you can access Azure, you need to have a valid subscription.

All the prerequisites are installed in Azure. Azure Portal is a Web application used to install, configure and manage all the prerequisites. Address to Azure Portal:

<https://portal.azure.com>

Address to classic Azure Portal:

<https://manage.windowsazure.com>

#### 3.1 MS SQL Server and Database

Before QualiWare can be installed, MS SQL Server and database must be created. For this go to Azure Portal, SQL databases page. On this page use action buttons to create MS SQL server and database. A step-by-step documentation on how to create MS SQL server and database can be found at the following address:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-get-started>

For more information about MS SQL database, please refer to the official documentation and tutorials by Microsoft:

<https://docs.microsoft.com/en-us/azure/sql-database>

Please note that you will be charged for each server and database that is created. Prices can be found at the following address:

<https://azure.microsoft.com/en-us/pricing/details/sql-database>

For this reason it is advised to create as few servers and databases as possible, if the other is not required. QualiWare software can be configured to use only one database. So the minimum requirements is one server and one database.

## 3.2 Virtual Machines

QualiWare software is installed on a virtual machine. Before it can be installed, a virtual machine must be created. For this go to Azure Portal, Virtual machines (Classic) page. On this page use action buttons to create Windows Server virtual machine. A step-by-step documentation on how to create virtual machine can be found at the following address:

<https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-hero-tutorial>

For more information about virtual machines, please refer to the official documentation and tutorials by Microsoft:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows>

Please note that you will be charged for virtual machine that is created. Prices can be found at the following address:

<https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows>

For this reason it is advised to create as few virtual machines as possible, if the other is not required. QualiWare software can be configured to use only one virtual machine. Often one more virtual machine may be required. This virtual machine is used as terminal server to run thick client. So the minimum requirements is from one to two virtual machines.

## 3.3 Azure Active Directory

To integrate company Active Directory with Azure Active Directory (Azure AD) and enable single sign on, it is required to use Azure AD Connect. Azure AD Connect will integrate on-premises directories with Azure AD. This allows to provide a common identity for users for Office 365, Azure, and QualiWare applications integrated with Azure AD.

### 3.3.1 Install Azure Active Directory Connect

TODO: To be completed by Brian.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>

### 3.3.2 Enable Single Sign On

TODO: To be completed by Brian.

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-ss0>

## 4 Installing QualiWare Software

QualiWare software is installed on a virtual machine. Installation and configuration process is very close to the process in on-premises environment. For a step-by-step documentation on how to install QualiWare software, please refer to “Server Installation.docx”.

### 4.1 Synchronize with Azure Active Directory

There are two options to configure synchronization with Azure AD.

#### 4.1.1 Active Directory Connection

Before QualiWare software can be synchronized with Azure AD using standard Active Directory connection, Azure AD must have Domain Services enabled. A step-by-step documentation on how to enable Azure AD Domain Services can be found at the following address:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started-enableaadds>

After Azure AD Domain Services is enabled follow standard configuration described in “One Time Configurations Inside QEF - Active Directory Synchronization.docx” to synchronize QualiWare with Azure AD using Active Directory connection.

#### 4.1.2 Azure Active Directory Connection

Below are the steps to create Azure Active Directory connection:

1. Go to **Admin Console**.
2. Go to **Active Directory Synchronization**.
3. Click **Create Azure AD Connection**.
4. Enter the following fields:

**Tenant Name** – The name of a tenant in Azure AD to synchronize with. Optional.

**Tenant Id** – The identifier (GUID) of a tenant in Azure AD to synchronize with. Required.

To obtain tenant name and ID:

- a. Go to **Azure Portal**.
- b. Go to **Azure Active Directory**.
- c. Go to **Properties**.
- d. **Name** contains tenant name and **Directory ID** contains tenant ID.

Alternatively:

- a. Go to **Azure Portal**.
- b. Click **Help + support** icon in the top right corner.

- c. Click **Show diagnostics**.
- d. Search for **tenants**.
- e. **displayName** contains tenant name and **id** contains tenant ID.

**Client Id** – The identifier (GUID) of QEF registered as client application in Azure AD. Required.

**Client Secret** – Secret key string issued by Azure AD if QEF is registered as web application.

Optional.

To obtain client name and client secret:

- a. Go to **Azure Portal**.
- b. Go to **Azure Active Directory**.
- c. Go to **App registrations**.
- d. **Name**: QEFNative
- e. **Application Type**: Native
- f. <https://{DNS server name}/qef/instance/signin>
- g. **Object ID** contains client id.
- h. Client secret is not applicable to native application.

Alternatively:

- e. Go to **Azure Portal**.
- f. Go to **Azure Active Directory**.
- g. Go to **App registrations**.
- h. **Name**: QEFWeb
- i. **Application Type**: Web App / API
- j. <https://{DNS server name}/qef65/instance/signin>
- k. **Object ID** contains client id.
- l. Go to **Keys**.
- m. Generate and save client secret.

**Polling interval (auto)** – Defines an interval for Auto mode to poll Azure AD with (differential queries).

**Login as** – Whether to use explicit user-defined credentials to connect to Azure AD with. Used if QEF is registered as native application in Azure AD.

**Login** – Explicit user-defined credentials to connect to Azure AD with. Only login in full UPN format is valid.

**Authority base URL** – URL of Azure AD services provider. Gets filled with Microsoft cloud default.

**Graph API URL** – URL of graph API RESTful service in Azure AD. Gets filled with Microsoft cloud default.

**Enabled** - enable or disable synchronization with Active Directory server.

**Status** - Synchronization status when it is started.

## 4.2 Enable HTTPS

Before HTTPS can be enabled, a certificate must be created.

#### **4.2.1 Request an Internet Server Certificate**

The first step in creating of a valid certificate is to create and send request to public certification authorities (CA). A step-by-step documentation on how to request an Internet server certificate can be found at the following address:

[https://technet.microsoft.com/en-us/library/cc732906\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx)

#### **4.2.2 Install an Internet Server Certificate**

When you receive a response from a public certification authority (CA) to whom you sent a certificate request, you must complete the process by installing the server certificate on your Web server. A step-by-step documentation on how to install an Internet server certificate can be found at the following address:

[https://technet.microsoft.com/en-us/library/cc771816\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771816(v=ws.10).aspx)

#### **4.2.3 Configure an HTTPS Binding**

After installing certificate, an HTTPS binding must be configured to use the certificate. A step-by-step documentation on how to configure an HTTPS binding can be found at the following address:

[https://technet.microsoft.com/en-us/library/hh467896\(v=sc.12\).aspx](https://technet.microsoft.com/en-us/library/hh467896(v=sc.12).aspx)

### **4.3 Configure redirection**

After QualiWare is installed and QEP solution is published, the address to access it is rather long and may hint that the solution is installed in Azure. To use a more concise address, a new DNS name must be registered and HTTP redirection set up.

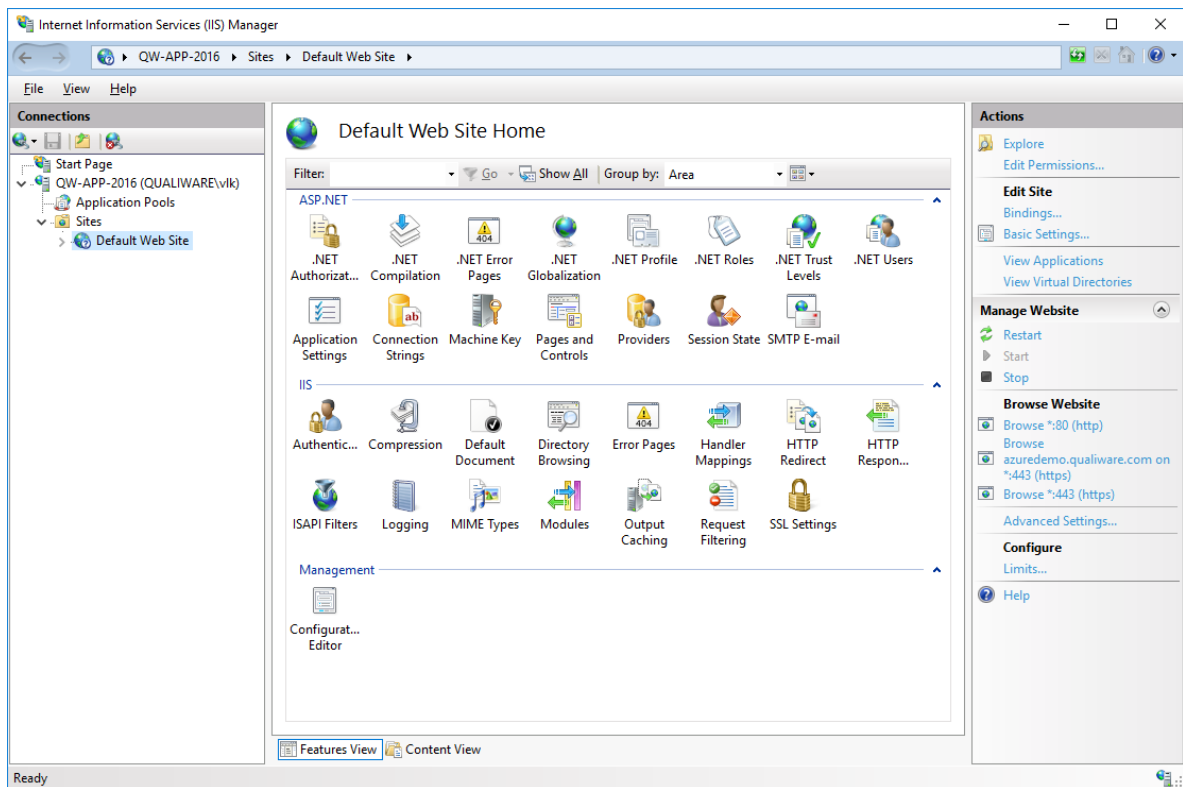
#### **4.3.1 Register DNS Name**

TODO: To be completed by Brian.

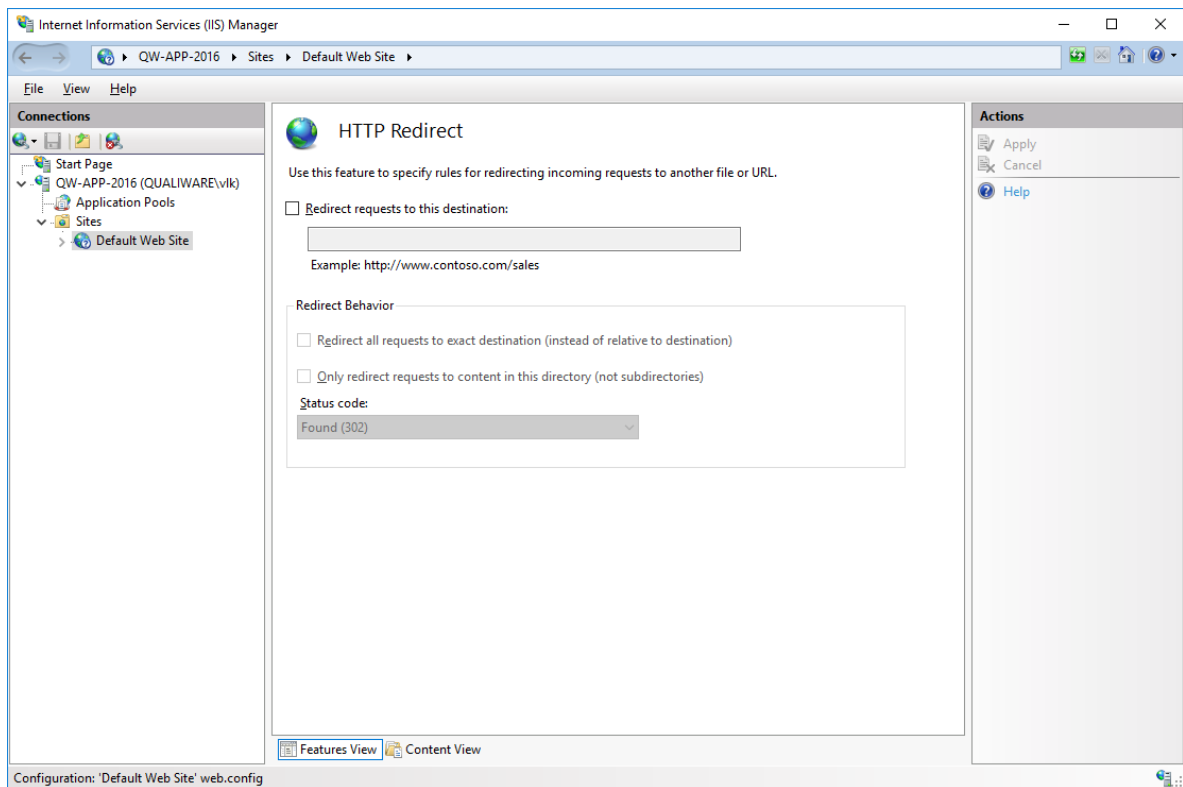
#### **4.3.2 Configure redirection**

Below are the steps to configure redirection:

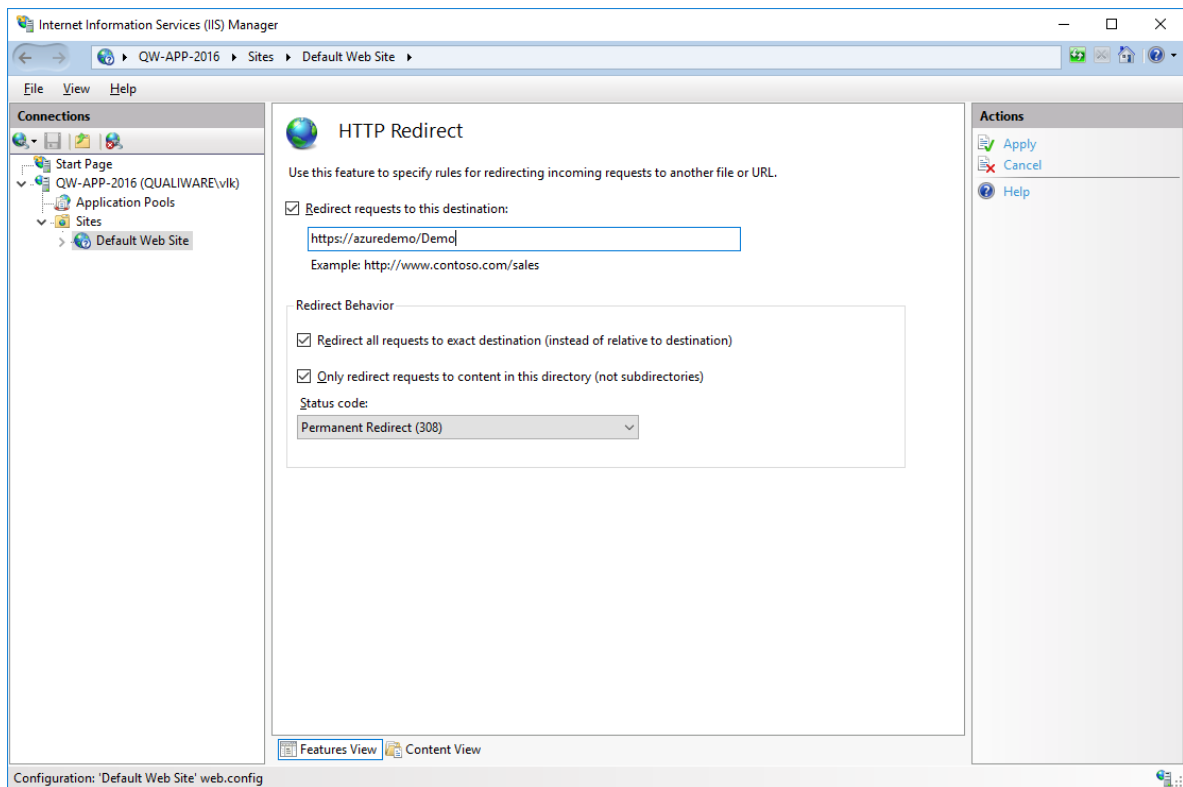
1. Start **Internet Information Services (IIS) Manager**.
2. Select **Default Web Site**.



3. Double-click HTTP Redirection.



4. Check **Redirect requests to this destination**.
5. Enter path to published QEP solution using public DNS name (see previous chapter).
6. Check **Redirect all requests to exact destination (instead of relative to destination)**.
7. Check **Only redirect requests to content in this directory (not subdirectories)**.
8. In **Status code** select **Permanent Redirect (308)**.



9. Click Apply.

## 4.4 Create Web Application

QualiWare integrates with Azure AD and provides secure sign in and authorization. To integrate an application or service with Azure AD, it is required to first register the details about application with Azure AD. A step-by-step documentation on how to register application with Azure AD can be found at the following addresses:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-integrating-applications#adding-an-application>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal#create-an-active-directory-application>

When registering application use the following address as **Sign-on URL**:

<https://{DNS server name}/{QEF instance name}/Instance/signin>