

Web Client Guide Vijeo Citect 2015

July 2015 – Whitepaper

Warwick Black
Validation Specialist

Make the most of your energy



SCADA Expert Vijeo Citect 2015 – Web Client Guide

The Vijeo Citect Web Client is a browser-based SCADA client. The client software and requisite SCADA project files are downloaded on demand from an IIS-based Web Server; The Web Client then obtains real-time data directly from the relevant SCADA servers, as per a standard SCADA client.

Because the runtime environment is an ActiveX control, it is only supported by Internet Explorer. For cross-platform solutions, we recommend reading the whitepaper on [Remote Desktop Services](#).

Benefits

- No need to pre-install Vijeo Citect (VJC) software on the Client
- Multiple versions (v6.0 – v7.50/2015) of the Web Client ActiveX can be installed side-by-side
- Central repository for Project files, integrated version control
 - o Project files are downloaded and cached locally on demand
 - o Project files are automatically updated when a newer version is available

Limitations

- ActiveX technology is only supported in Windows, and only via Internet Explorer
- No access to the 'Kernel' window and some Cicode functions
- Web Clients need direct network access to the SCADA Servers.
 - o **SCADA Servers should never be exposed directly to the Internet!**
 - For secure remote access, refer to the Remote Desktop Services whitepaper or use a VPN in conjunction with Web Client.
 - If required, the 'Port-Forwarding / Address Forwarding' section shows how to expose the SCADA network to another internal network.

Licencing

As of version 7.30, the Web Client leverages the same 'Control' and 'View-Only' licences as a standard client.

Web Client licences can only be obtained via the standard floating-licence mechanism, where the Client polls all connected IO Servers to obtain a licence.

Tested Web Server Configurations

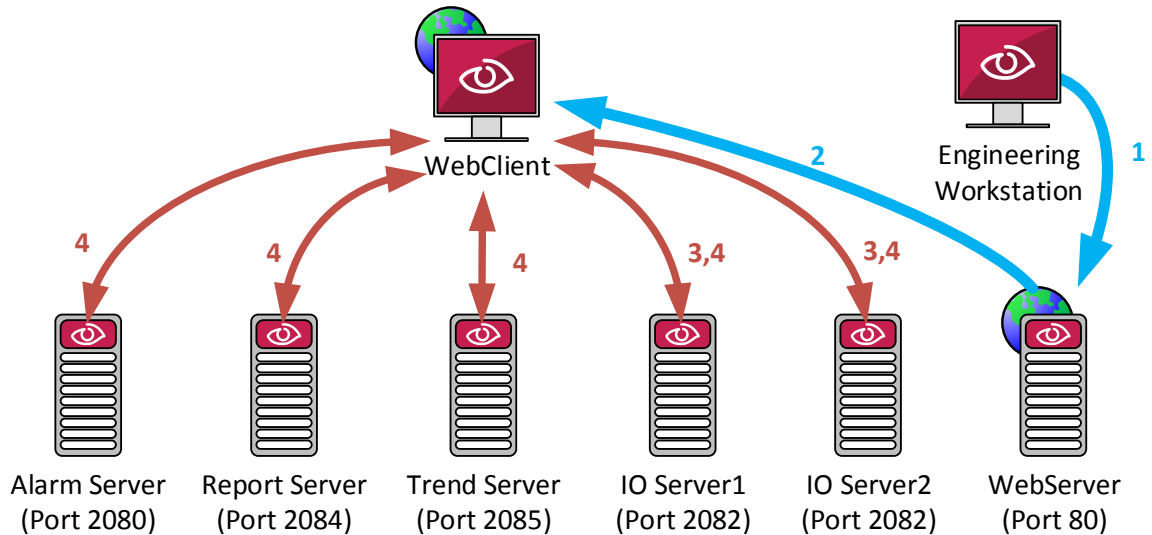
We have installed and tested the Web Server on the following configurations:

- Windows 7:
 - o Internet Explorer (IE): **8, 11.0.9600**
 - o Internet Information Services (IIS): **7.5.7600**
- Windows 8.1:
 - o Internet Explorer (IE): **11.0.9600**
 - o Internet Information Services (IIS): **8.5.9600**
- Windows Server 2008:
 - o IE: **8.0.7601, 11.0.9600**
 - o IIS: **7.5.7600**
- Windows Server 2012
 - o Internet Explorer (IE): **11.0.9600**
 - o Internet Information Services (IIS): **8.5.9600**

Architecture

Although all components could exist on the same machine, the diagram below shows each component on a separate PC to demonstrate the communication paths.

1. The Engineering Workstation 'Prepares the Deployment' and pushes files to the IIS server
2. The Web Client downloads an ActiveX control, and the Project Files from the Web Server
3. The Web Client obtains a floating licence from a connected IO Server
4. The Web Client obtains real-time data from all the SCADA servers, as per a normal client



Installation Overview

The basic process will be:

- Install Internet Information Services (IIS) on your Web Server PC
- Install the Vijeo Citect Web Server components on the Web Server PC
- Configure user security on the Web Server PC
- Prepare a Deployment and upload to Web Server
- Open a Web Client Session, install the Client ActiveX

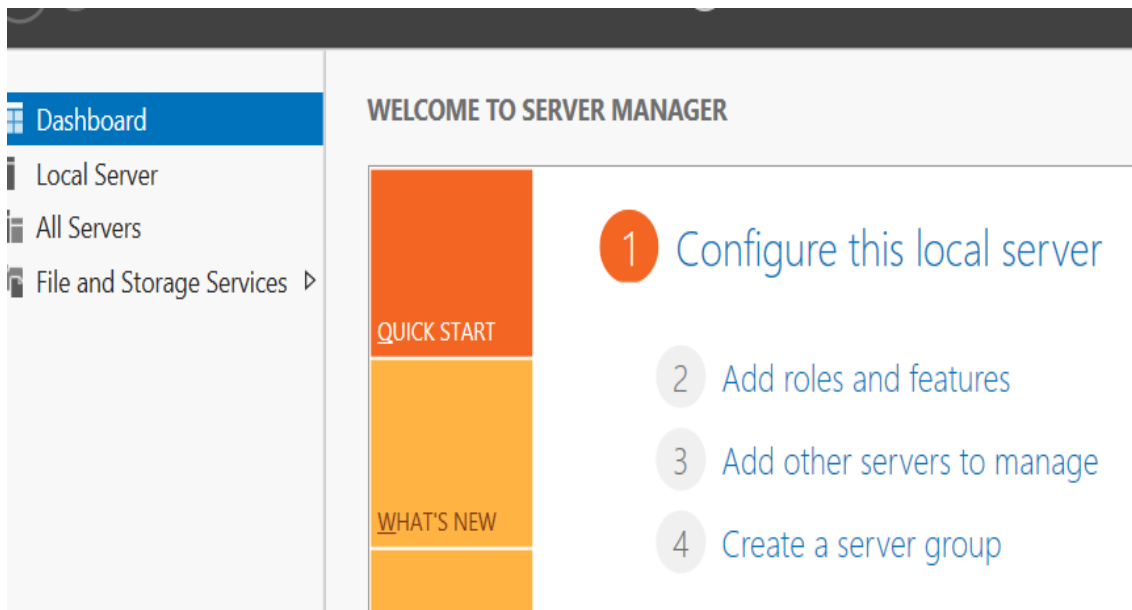
Contents

SCADA Expert Vijeo Citect 2015 – Web Client Guide	2
Benefits	2
Limitations	2
Licencing.....	2
Tested Web Server Configurations	2
Architecture	3
Installation Overview	3
Installing IIS	5
Web Server Installation - Windows Server 2012	5
Web Server Installation - Windows Server 2008 R2	10
Web Server Installation - Windows 7/8.....	13
Windows Firewall Settings.....	15
Installing Vijeo Citect Web Server Components	16
How are privileges determined?.....	18
Configuring Groups	19
Preparing and Uploading a Deployment.....	23
Manually uploading a deployment (OPTIONAL / ALTERNATE METHOD):	26
Client-side configuration:.....	27
Preventing 'Integrated' Security	29
Running Web Client	30
Port-Forwarding / Address Forwarding	31
Troubleshooting:.....	33
Quick Tips:.....	33
KB Articles:	33

Installing IIS

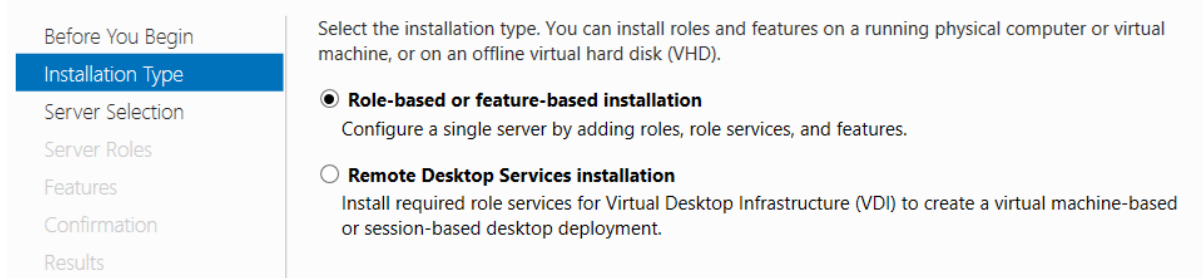
Web Server Installation - Windows Server 2012

- From the 'Server Manager', select 'Add Roles and Features'



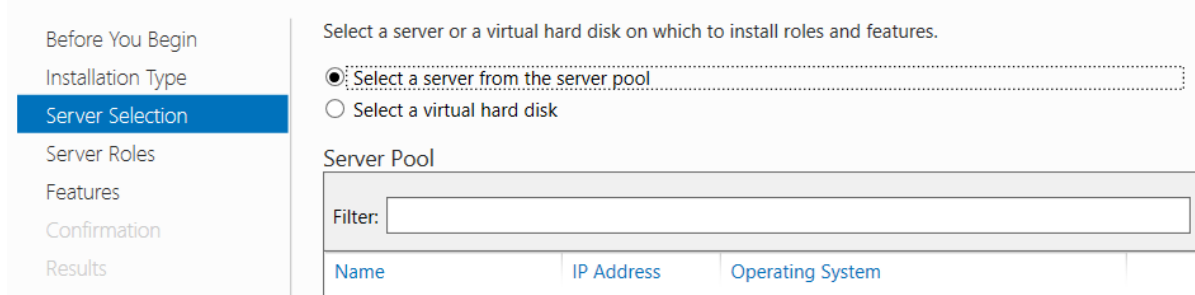
- Select 'Role-based or Feature-based Installation'

Select installation type



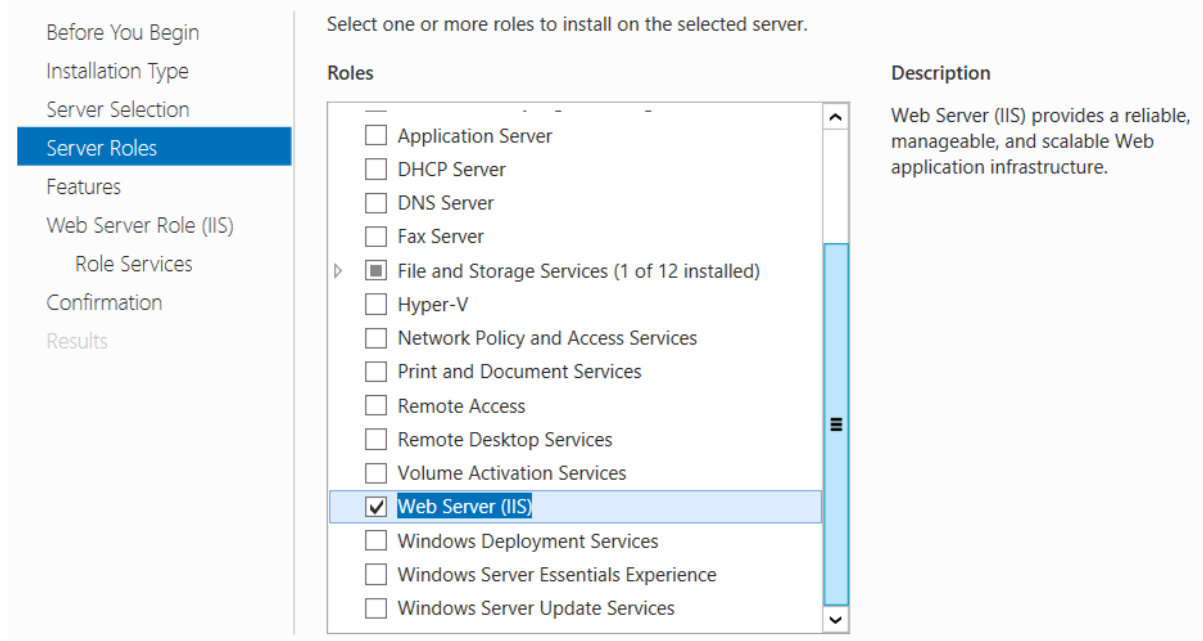
- Select your target PC from the 'Select a Server from the Server Pool' option.

Select destination server



- Select **'Web Server (IIS)'** and click **'Next'**.

Select server roles



Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
 Role Services
Confirmation
Results

Select one or more roles to install on the selected server.

Roles

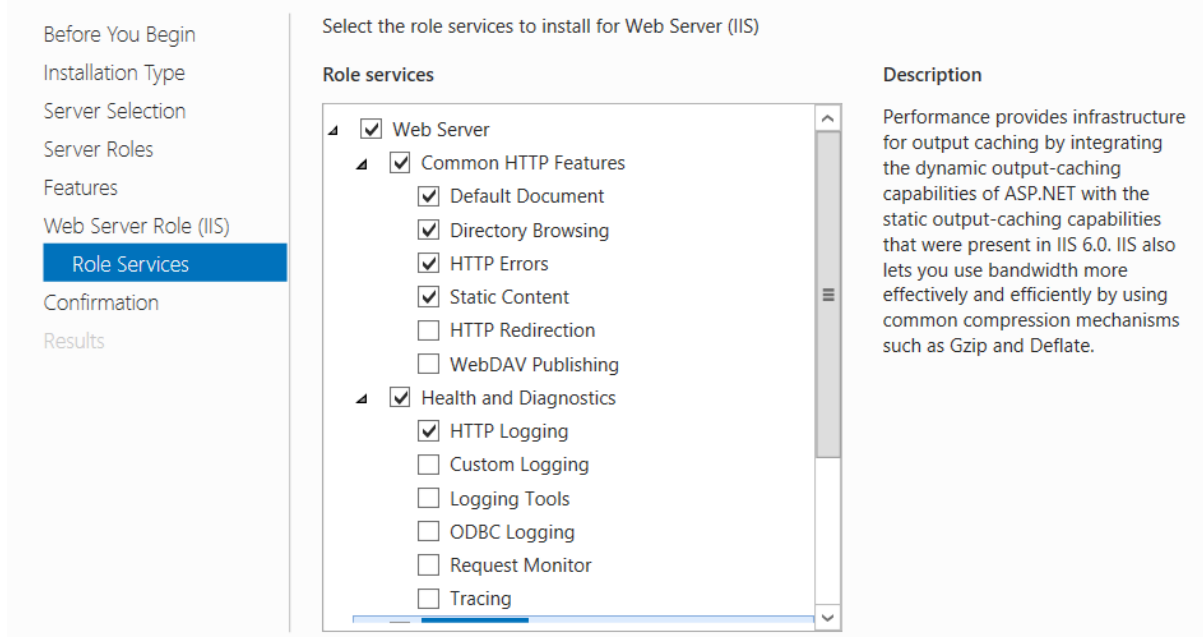
- Application Server
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)**
- Windows Deployment Services
- Windows Server Essentials Experience
- Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

- Select **'Next'** till you get to the **'Select Role Services'**
- After Selecting **'Web Server'**, it will pre-fill several options
 - For **'Common HTTP Features'** leave the default settings
 - For **'Health and Diagnostics'** leave the default settings

Select role services



Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services

- Web Server
 - Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - WebDAV Publishing
 - Health and Diagnostics
 - HTTP Logging
 - Custom Logging
 - Logging Tools
 - ODBC Logging
 - Request Monitor
 - Tracing

Description

Performance provides infrastructure for output caching by integrating the dynamic output-caching capabilities of ASP.NET with the static output-caching capabilities that were present in IIS 6.0. IIS also lets you use bandwidth more effectively and efficiently by using common compression mechanisms such as Gzip and Deflate.

- For 'Performance' leave the default settings
- For 'Security', add:
 - Windows Authentication

Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

Select the role services to install for Web Server (IIS)

Role services

- Performance
 - Static Content Compression
 - Dynamic Content Compression
- Security
 - Request Filtering
 - Basic Authentication
 - Centralized SSL Certificate Support
 - Client Certificate Mapping Authentication
 - Digest Authentication
 - IIS Client Certificate Mapping Authentication
 - IP and Domain Restrictions
 - URL Authorization
 - Windows Authentication
- Application Development

Description

Windows authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access your Web site from behind firewalls and proxy servers.

- For 'Application Development', add the following:
 - ASP
 - ISAPI Extensions

Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

Select the role services to install for Web Server (IIS)

Role services

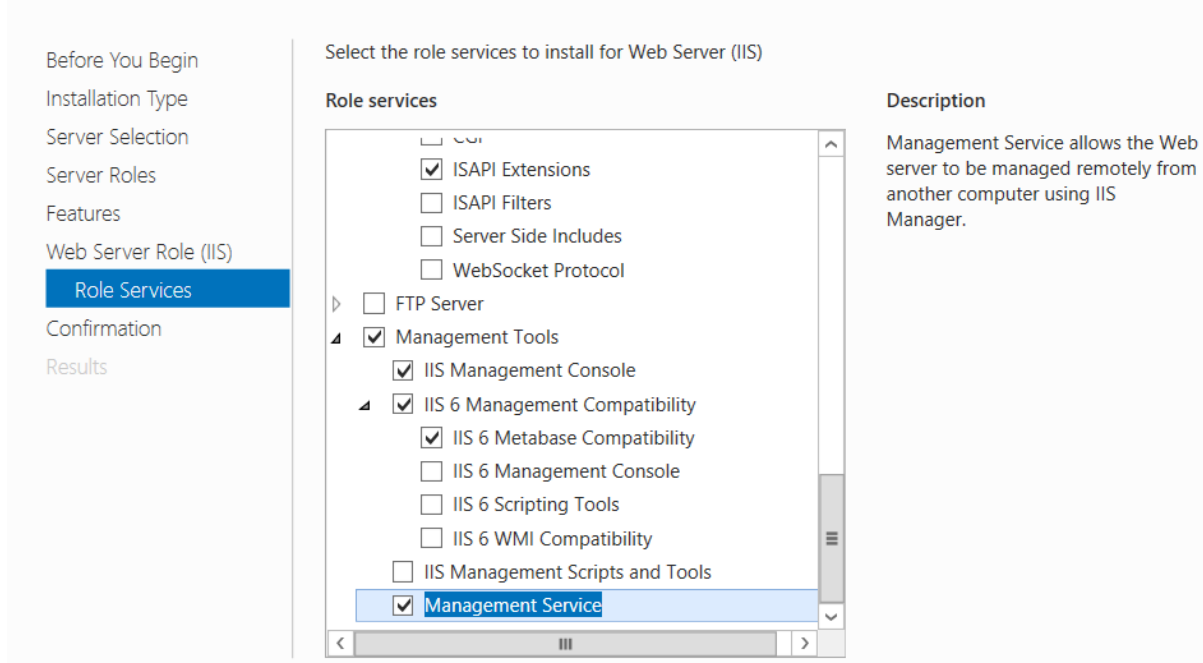
- Windows Authentication
- Application Development
 - .NET Extensibility 3.5
 - .NET Extensibility 4.5
 - Application Initialization
 - ASP
 - ASP.NET 3.5
 - ASP.NET 4.5
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
 - WebSocket Protocol
- FTP Server

Description

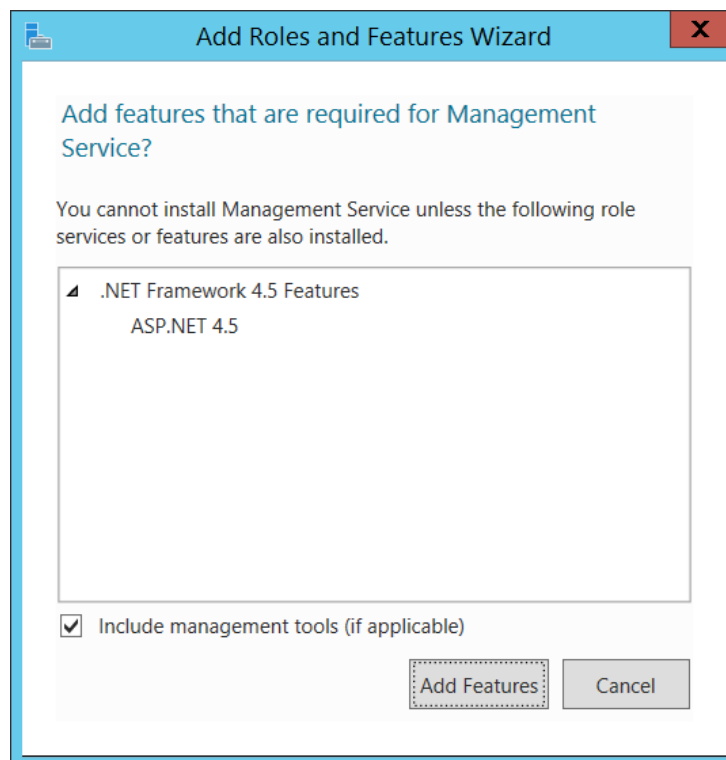
Active Server Pages (ASP) provides a server side scripting environment for building Web sites and Web applications. Offering improved performance over CGI scripts, ASP provides IIS with native support for both VBScript and JScript. Use ASP if you have existing applications that require ASP support. For new development, consider using ASP.NET.

- For 'Management Tools', add the following:
 - IIS Management Compatibility
 - IIS 6 Metabase Compatibility
 - Management Services

Select role services



At various times, you may receive notification of other dependant components that are required, select 'Add Feature' when prompted:



- Confirm the installation options:

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- .NET Framework 4.5 Features
 - ASP.NET 4.5
- Web Server (IIS)
 - Management Tools
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS Management Console
 - Management Service

... Features
Web Server Role (IIS)
Role Services
Confirmation
Results

- Web Server
 - Application Development
 - ASP
 - ISAPI Extensions
 - Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content

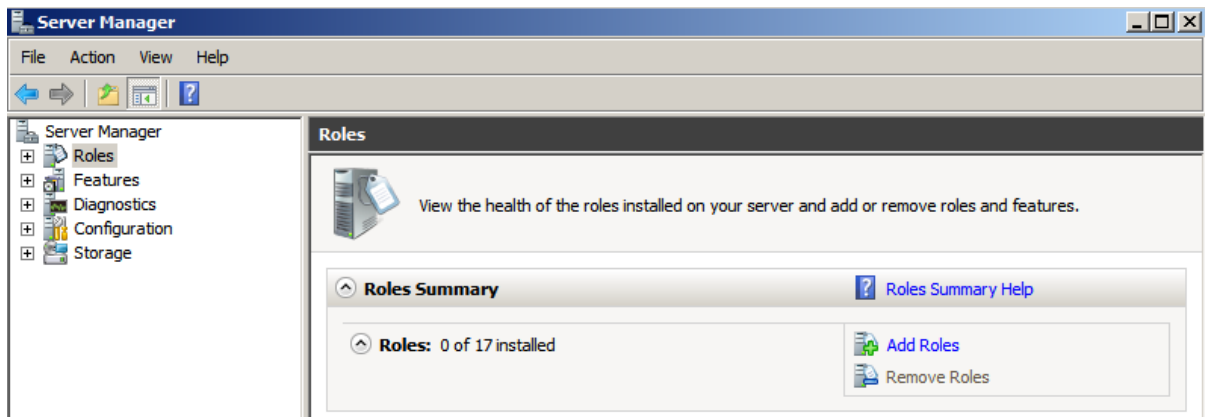
... Role Services
Confirmation
Results

- Static Content
- Health and Diagnostics
 - HTTP Logging
- Performance
 - Static Content Compression
- Security
 - Request Filtering
 - Windows Authentication

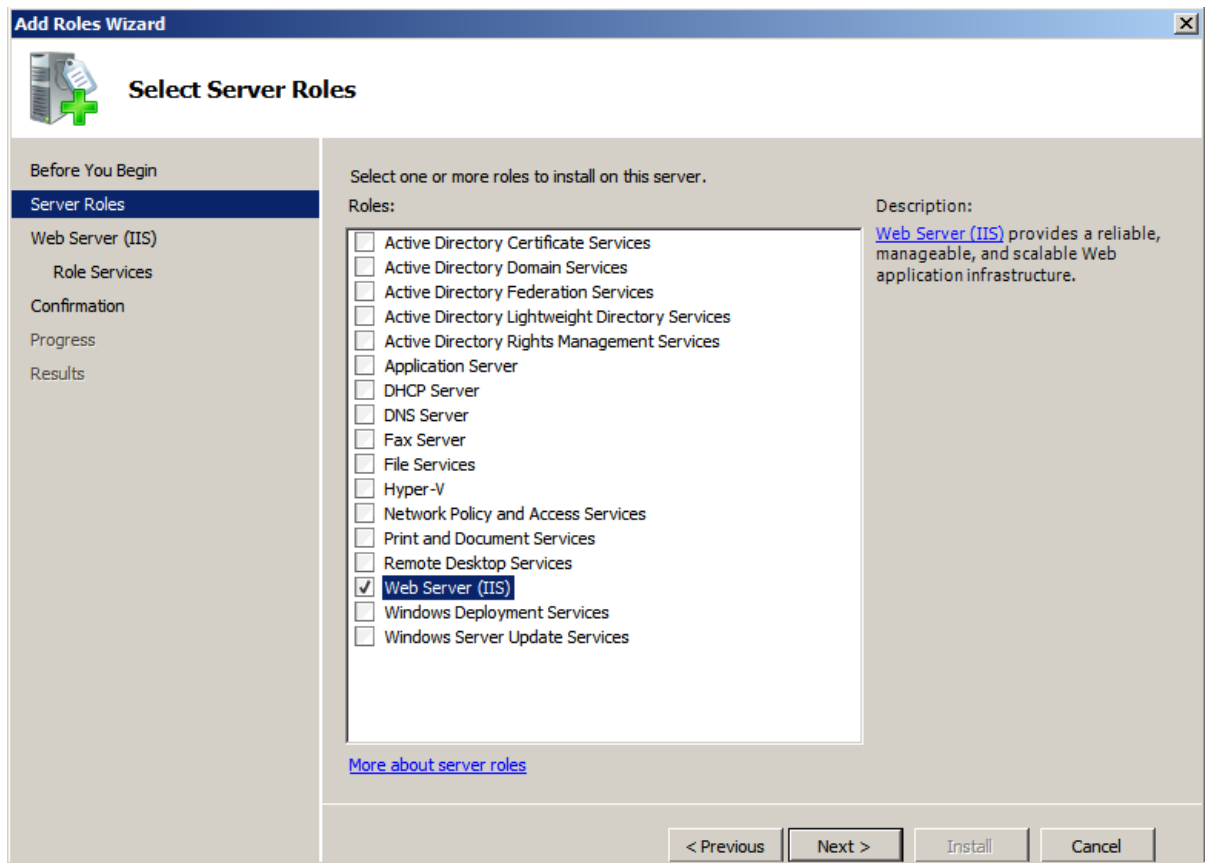
- Click **'Install'** to complete the IIS installation

Web Server Installation - Windows Server 2008 R2

- Open **'Server Manager'** and select **'Add Roles'**



- Select the **'Web Server (IIS)'** role



- In addition to the default settings, add the following non-standard options:

Add Roles Wizard

Select Role Services

Before You Begin
Server Roles
Web Server (IIS)
Role Services
Confirmation
Progress
Results

Select the role services to install for Web Server (IIS):

Role services:

- Common HTTP Features
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - HTTP Redirection
 - WebDAV Publishing
- Application Development
 - ASP.NET
 - .NET Extensibility
 - ASP
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
- Health and Diagnostics
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing

Description:
[IIS 6 Metabase Compatibility](#) provides infrastructure to query and configure the metabase so that you can run applications and scripts migrated from earlier versions of IIS that use Admin Base Object (ABO) or Active Directory Service Interface (ADSI) APIs.

...
Web Server (IIS)
Role Services
Confirmation
Progress
Results

- Custom Logging
- ODBC Logging
- Security
 - Basic Authentication
 - Windows Authentication
 - Digest Authentication
 - Client Certificate Mapping Authentication
 - IIS Client Certificate Mapping Authentication
 - URL Authorization
 - Request Filtering
 - IP and Domain Restrictions
- Performance
 - Static Content Compression
 - Dynamic Content Compression
- Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility

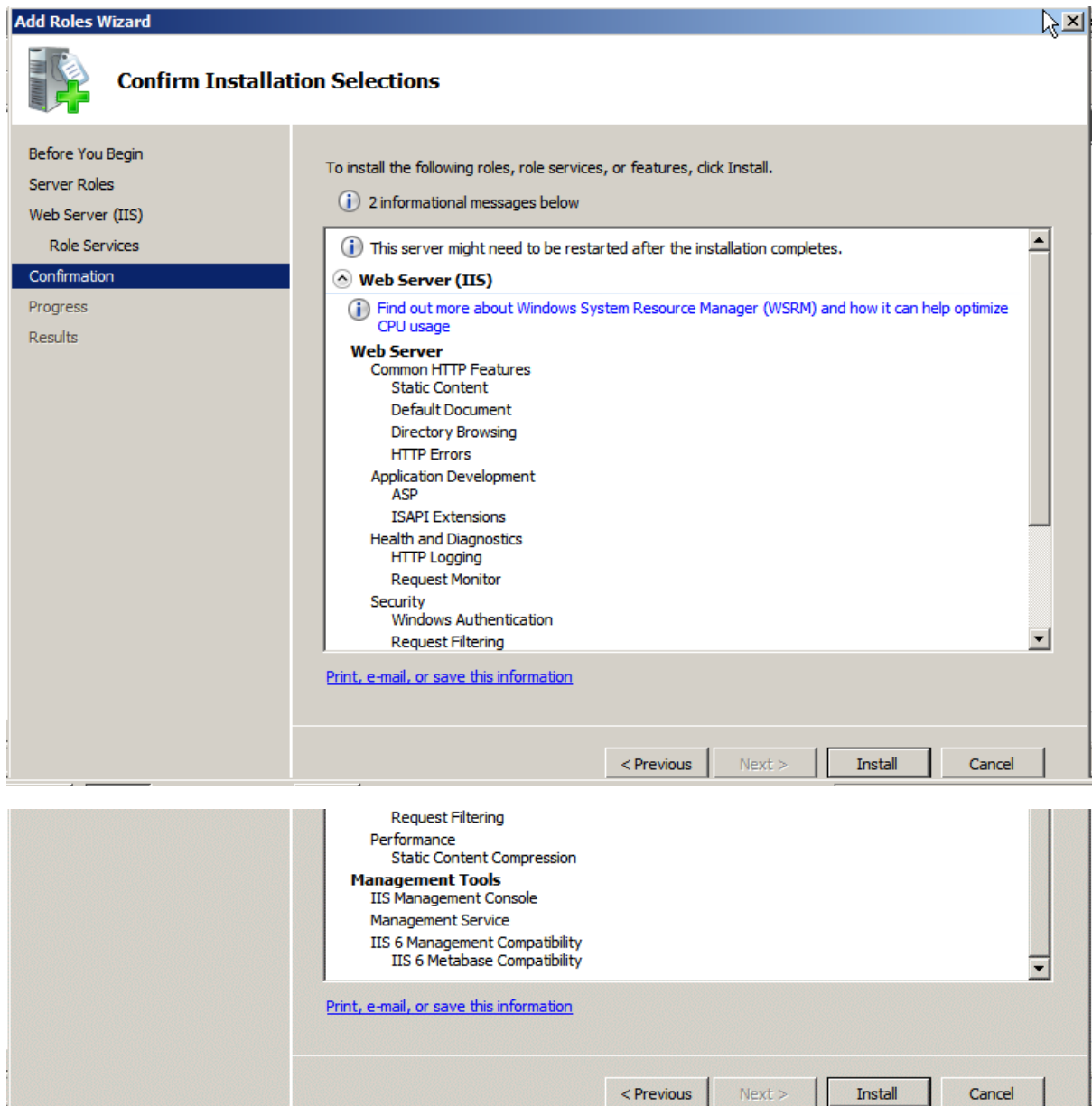
Description:
[IIS 6 Management Compatibility](#) provides forward compatibility for your applications and scripts that use the two IIS APIs, Admin Base Object (ABO) and Active Directory Service Interface (ADSI). You can use existing IIS 6 scripts to manage the IIS 7 Web server.

...
 IIS 6 Scripting Tools
 IIS 6 Management Console
 FTP Server
 IIS Hostable Web Core

[More about role services](#)

< Previous Next > Install Cancel

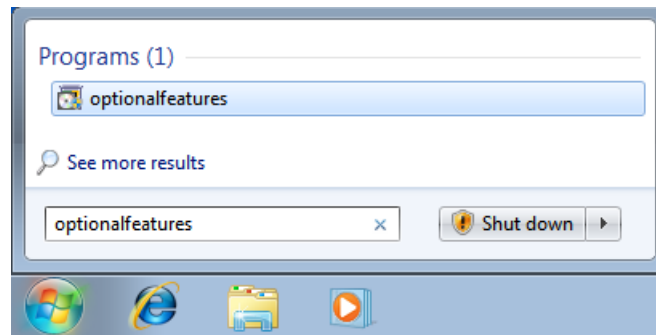
- Confirm the installation options:



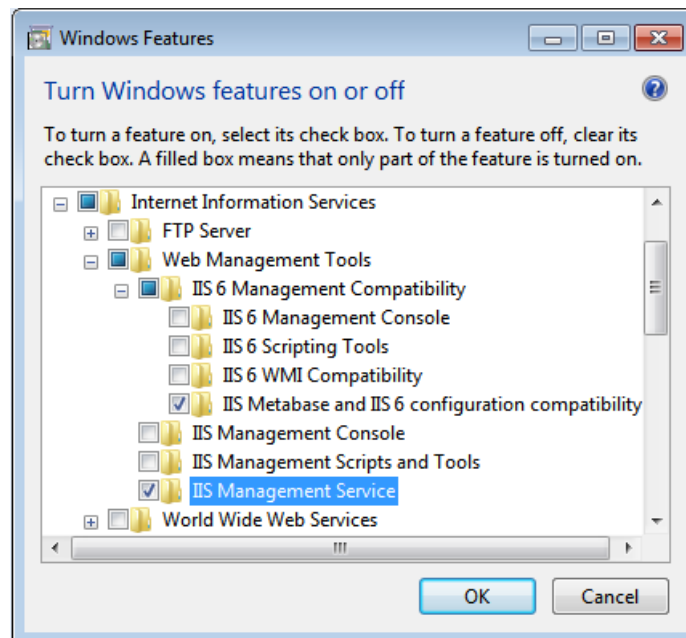
- Select 'Install'

Web Server Installation - Windows 7/8

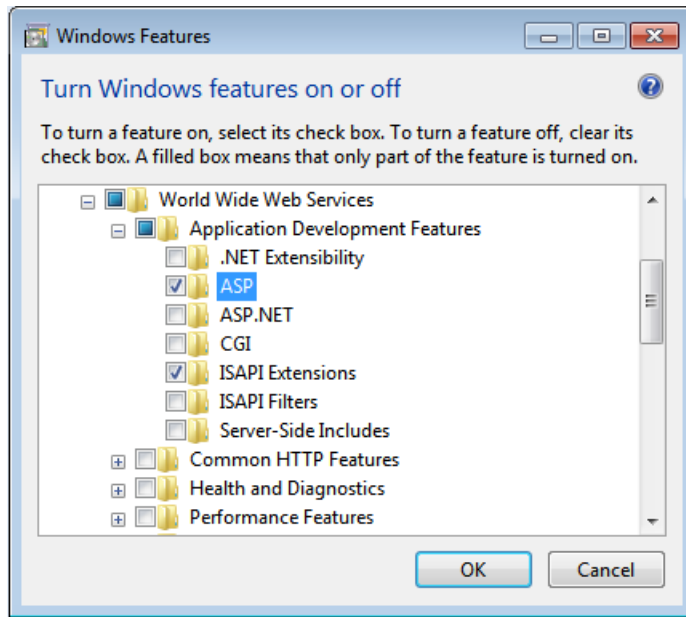
- Start > Run > **'optionalfeatures'**
 - Or navigate there via **'Add /Remove Programs'**, **'Turn Windows Features on or off'**



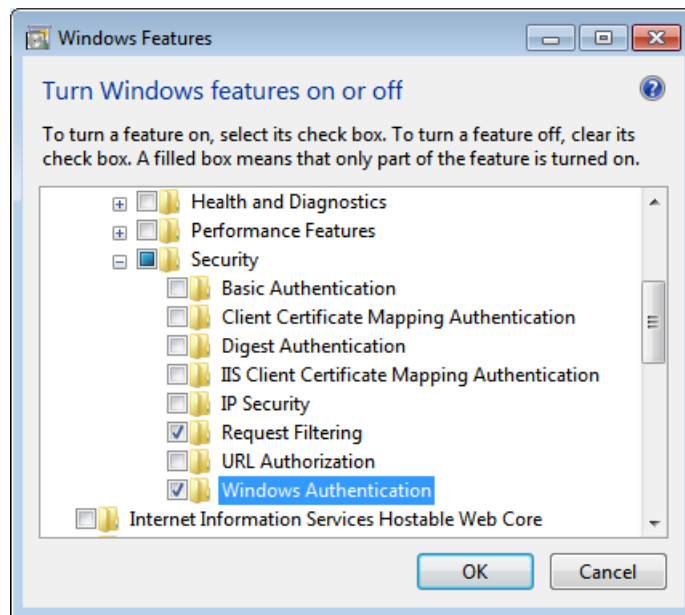
- Select and expand **'Internet Information Services'**, and add the following:
 - IIS 6 Management Compatibility
 - IIS Metabase and IIS Configuration compatibility
 - IIS Management Service



- Expand World Wide Web Services, Application Development Features
 - Select ASP and ISAPI Extensions



- Expand Security
 - Select Windows Authentication

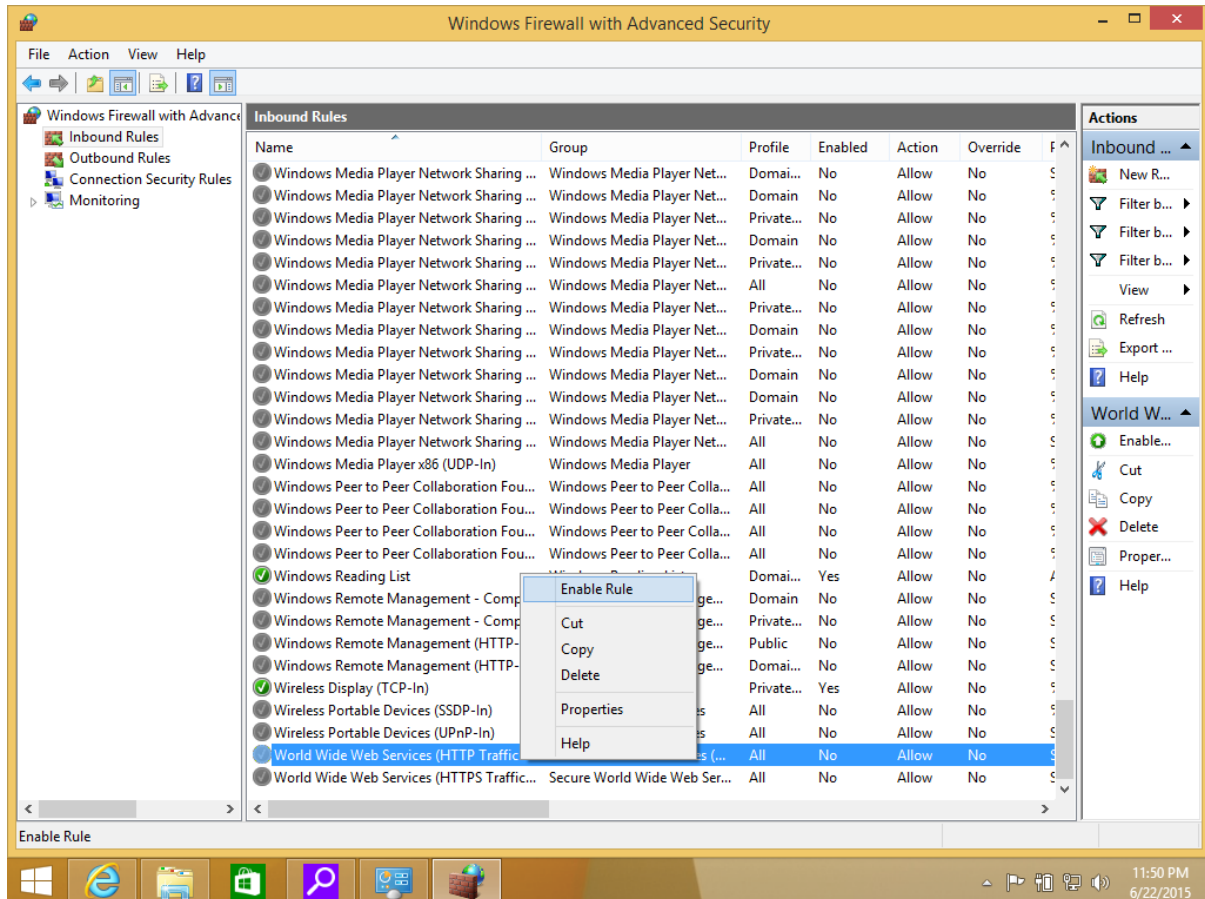


- Click 'Install' to complete the IIS installation

Windows Firewall Settings

In order to allow remote access to the Web Server, you must enable the **'World Wide Web Services (HTTP)'** exception rule in the Windows Firewall.

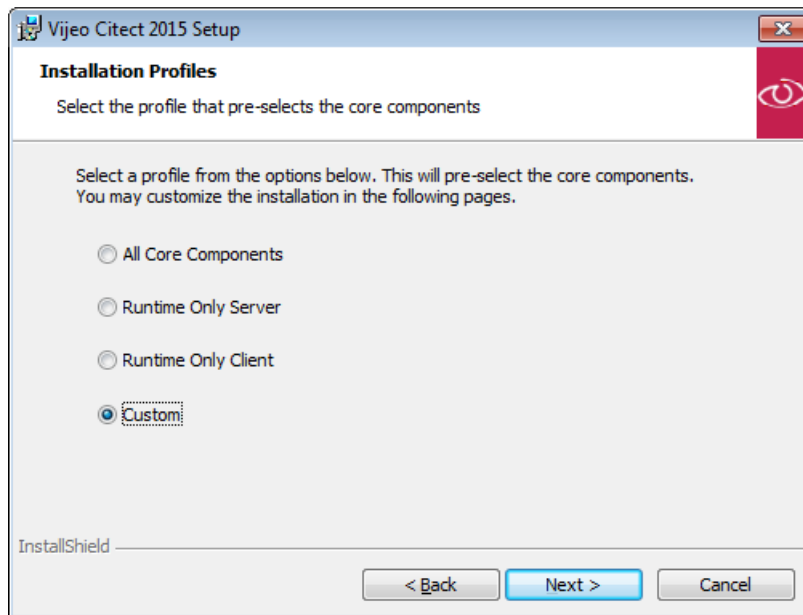
- Start > Run **'wf.msc'**
- Select **'InBound Rules'** and scroll to find the **'World Wide Web Services (HTTP)'**
- Right Click the rule, and select, **'Enable Rule'**



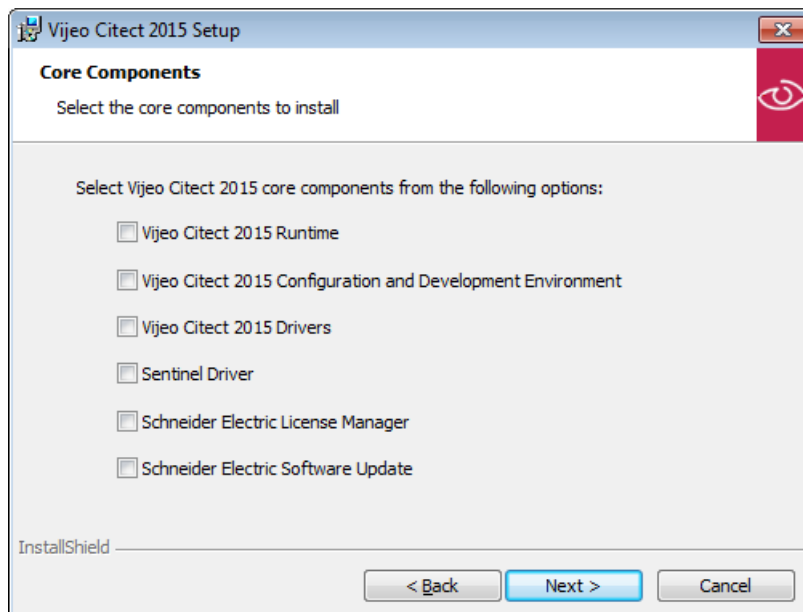
Installing Vijeo Citect Web Server Components

The minimum installation of Vijeo Citect components on our Web Server machine, is shown below:

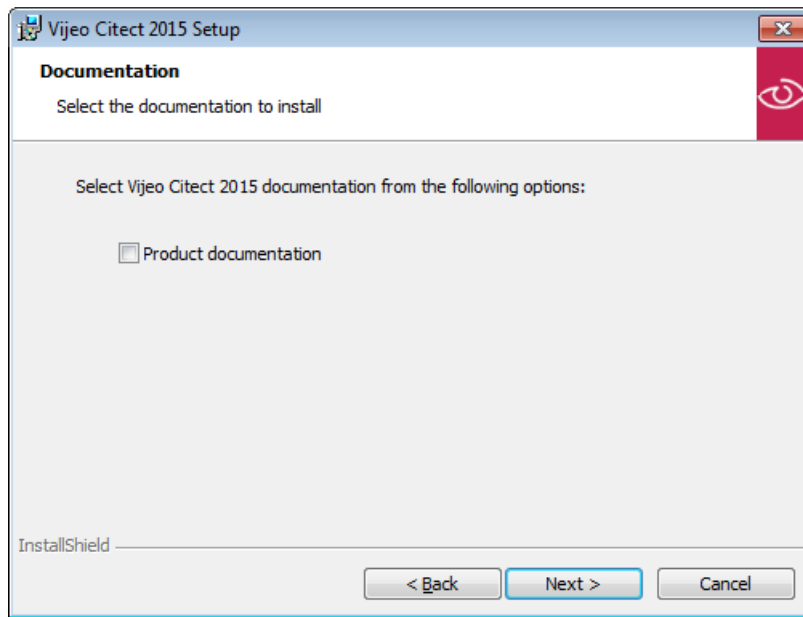
- Select **'Custom'**



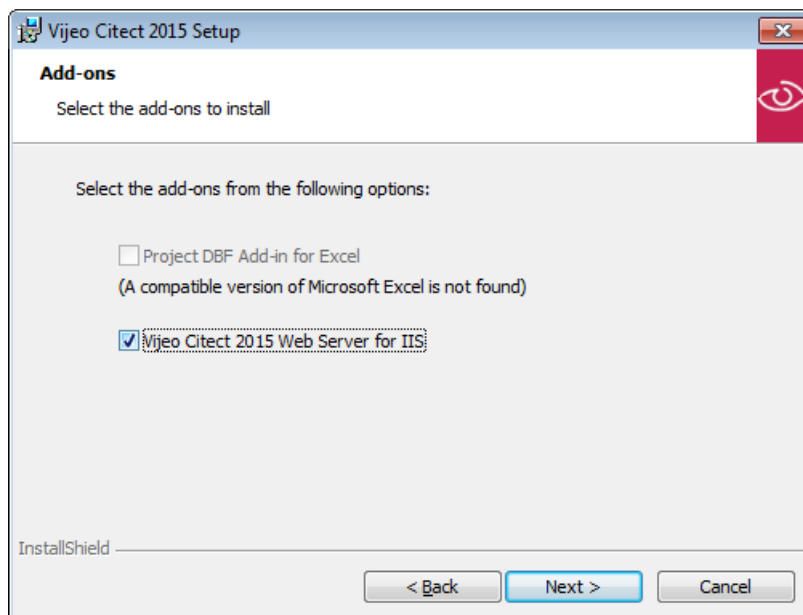
- It is not necessary to select any of the 'Core Components' on the Web Server.



- It is not necessary to install any documentation



- On the 'Add-on' page, we can select the 'Vijeo Citect 2015 Web Server for IIS' option

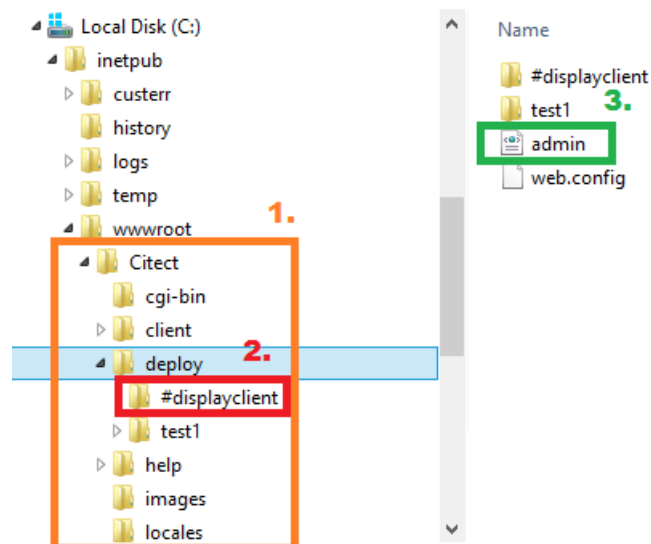


The remainder of the installer is self-explanatory, or the **'Installation Guide'** shipped with the installer can be referred to for more information.

How are privileges determined?

Privilege are determined by NTFS access levels for the logged in user.

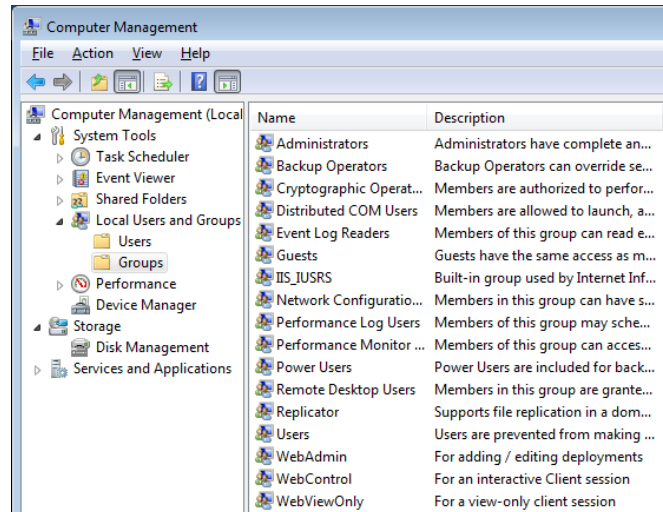
- **No Access:**
 - **Can't** read/execute any of the files in **wwwroot\Citect (1)**
- **Administrator:**
 - **Can** read/execute the code in **wwwroot\Citect (1)**
 - **Can** open and save the 'admin.xml' file in the 'deploy' folder (3)
- **View Only:**
 - **Can** read/execute the code in **wwwroot\Citect (1)**
 - **Can't** open and save the 'admin.xml' file in the 'deploy' folder (3)
 - **Fails** to get the directory listing of **#displayclient (2)**
- **Control Client:**
 - **Can** read/execute the code in **wwwroot\Citect (1)**
 - **Can't** open and save the 'admin.xml' file in the 'deploy' folder (3)
 - **Succeeds** in getting the directory listing of **#displayclient (2)**



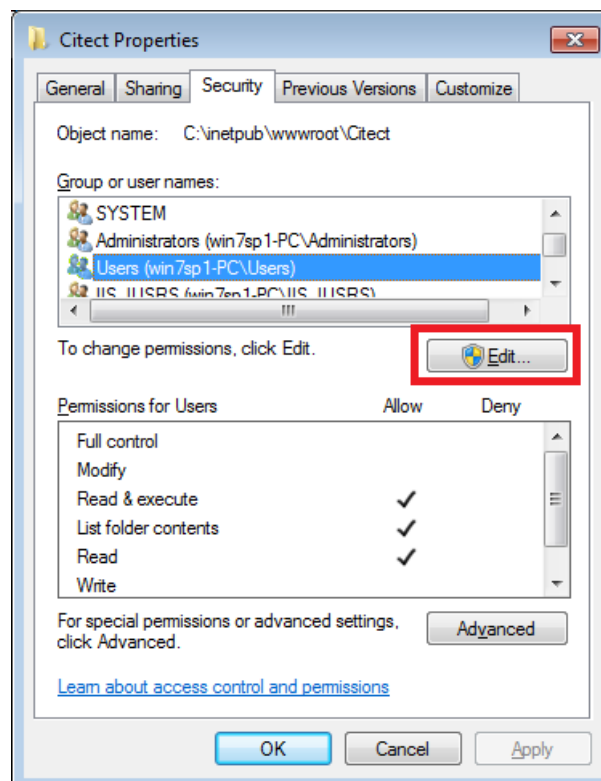
Configuring Groups

One method of configuring these privileges is to use local groups, then add the required users to those groups. If part of a Domain, this may need to be done by your Domain Administrator.

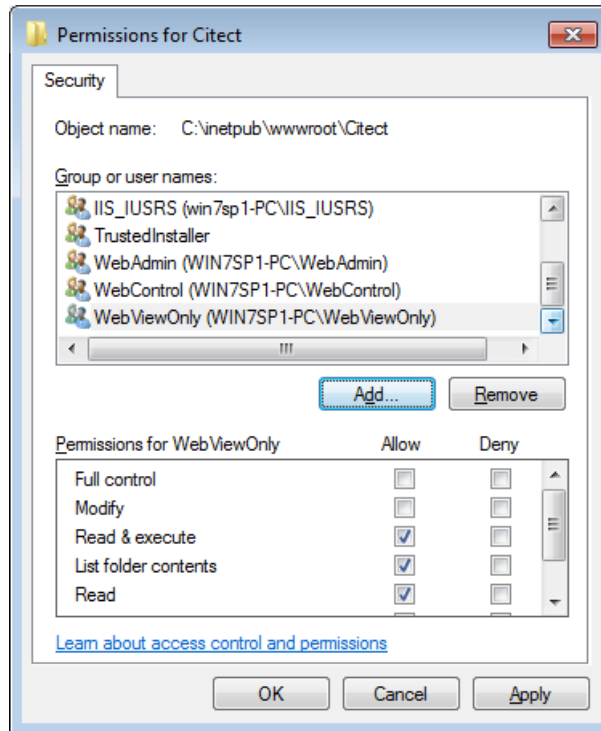
- Start > Run > **'Lusrmgr.msc'**
 - Create 3 new Groups, **WebAdmin, WebControl, WebViewOnly**



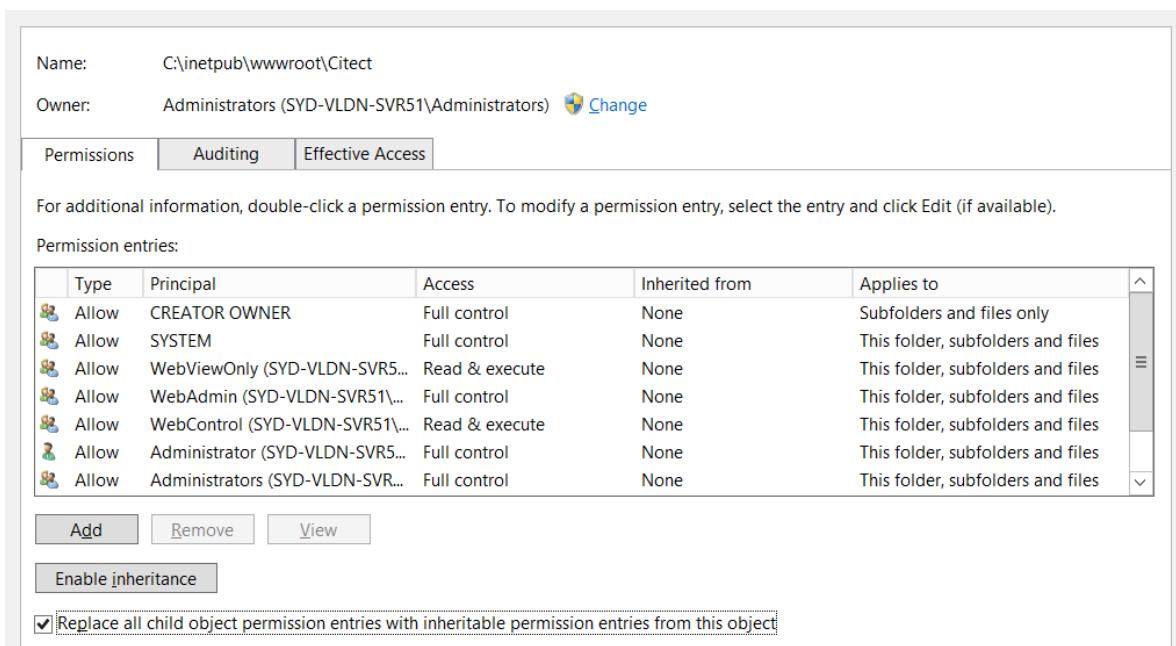
- Close 'Computer Management'
- Open File Explorer and navigate to **c:\inetpub\wwwroot**
 - Right Click the **'Citect'** folder, select **'Properties'**, then the **'Security'** tab
 - Click **'Edit'**



- **'Remove'** any overly inclusive groups, such as **'User'**
 - Just **'Remove'** the account from the list, don't **'Deny Full Control'**.
 - Most accounts also belong to the **'User'** group, so a **'Deny'** rule here would override any other **'Allow'** roles.
- Give our 3 new groups read & execute permissions:
 - **WebAdmin, WebControl & WebViewOnly:**

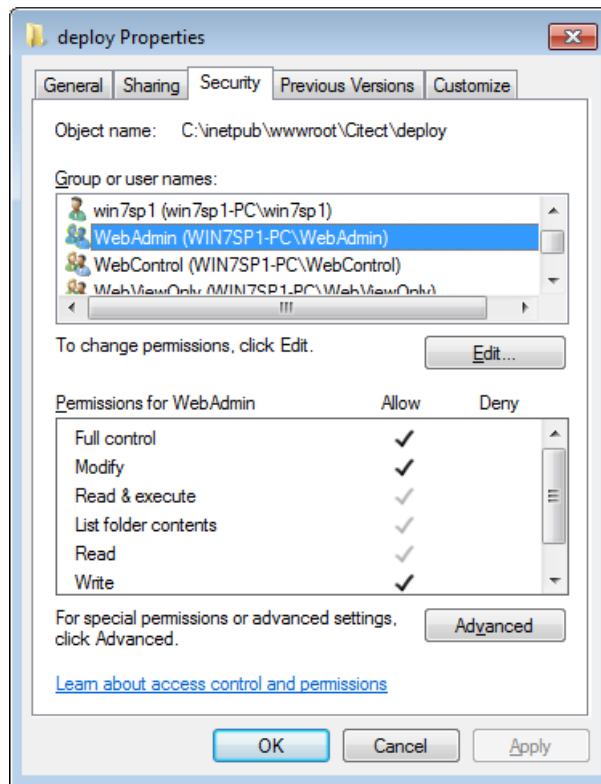


- Click OK
- Click Advanced

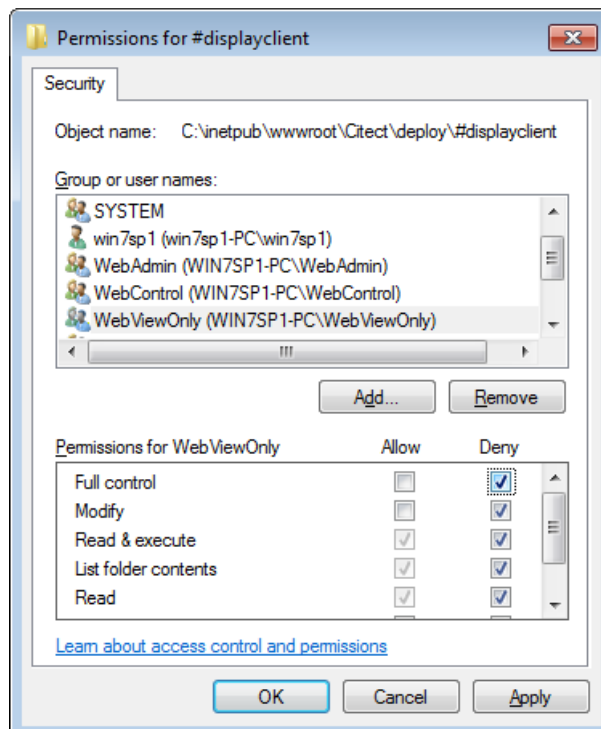


- Check the box **'Replace all child object permission entries with inheritable permission entries from this object'** and press OK.

- Navigate to **c:\inetpub\wwwroot\Citect**
 - Right Click the **'deploy'** folder, select **'Properties'**, then the **'Security'** tab
 - Click **'Edit'** and give **'Full Control'** to the **WebAdmin** account.

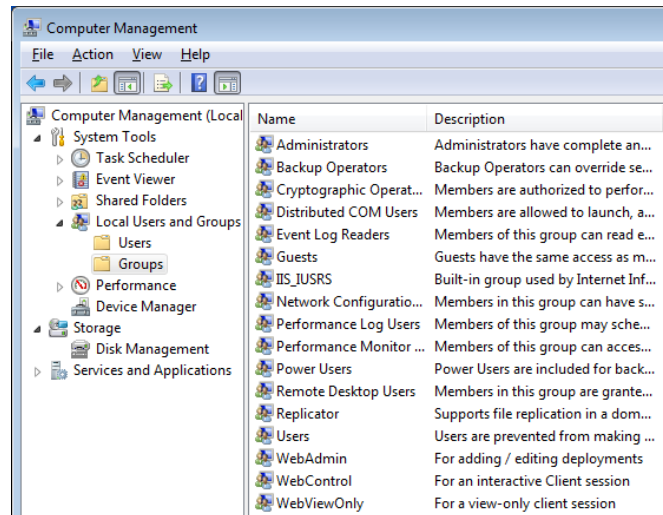


- Navigate to **c:\inetpub\wwwroot\Citect\deploy**
 - Right Click the **'#displayClient'** folder, select **'Properties'**, then the **'Security'** tab
 - Click **'Edit'** and **'Deny Full Control'** to the **WebViewOnly** account.



You can now add the relevant users to the correct Windows Group to give them access.

- Start > Run > **'Lusrmgr.msc'**
 - Add your existing users to the desired groups **WebAdmin**, **WebControl**, **WebViewOnly** or create new Users for this purpose.



- Close 'Computer Management'

Preparing and Uploading a Deployment

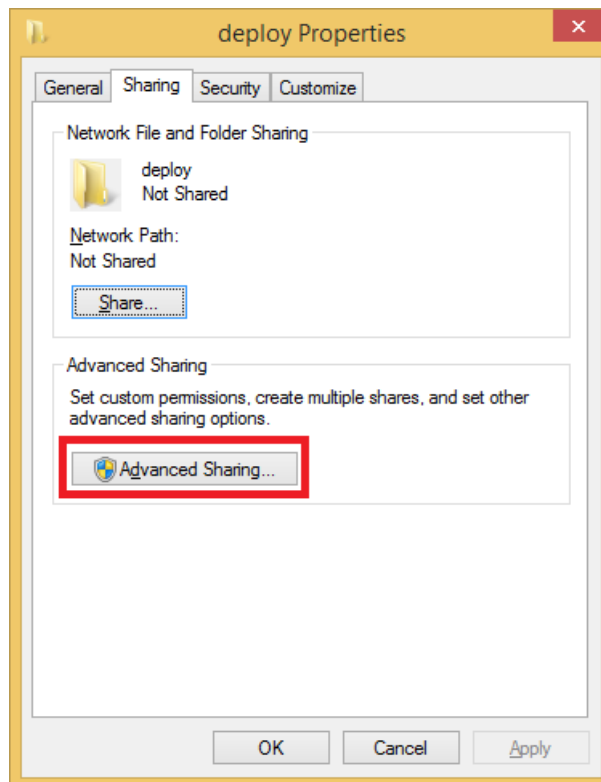
Now that the Vijeo Citect Web Server is installed, we need to prepare and upload our project files from the Engineering Workstation, to the IIS machine.

Files can be manually transferred to the Web Server, then an entry can be created through the Web Client web interface.

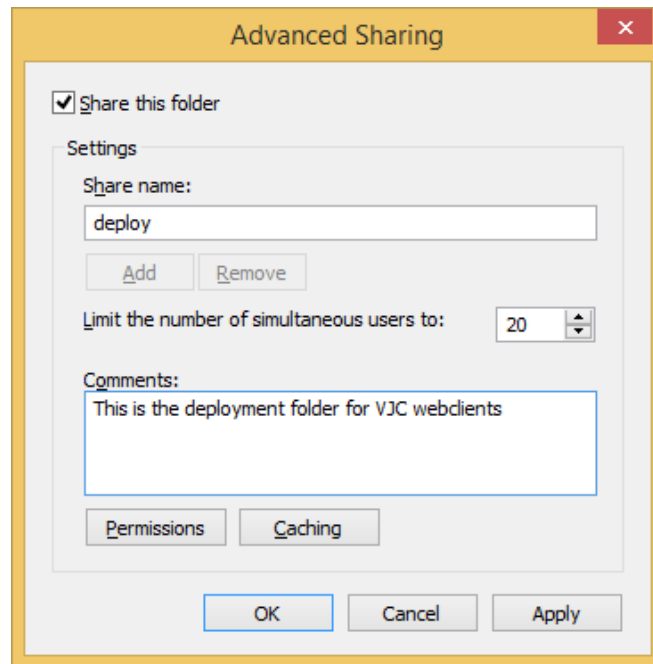
Alternatively we can configure Vijeo Explorer to push the files to the IIS Web Server in one-step. We recommend the one-step process and will cover this first.

On the IIS Web Server:

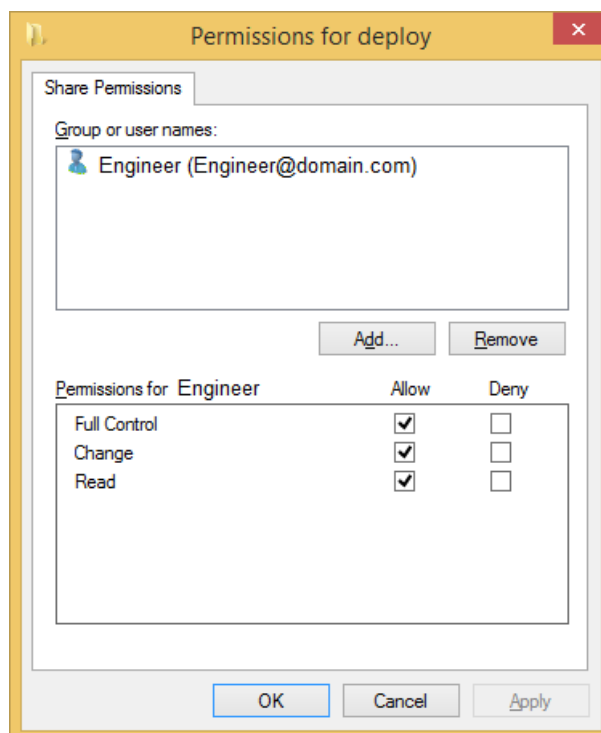
- Navigate to **c:\inetpub\wwwroot\Citect**
 - Right Click the **'deploy'** folder, select **'Properties'**, then the **'Sharing'** tab



- Tick **'Share this folder'**, enter a comment, then select **'Permissions'**

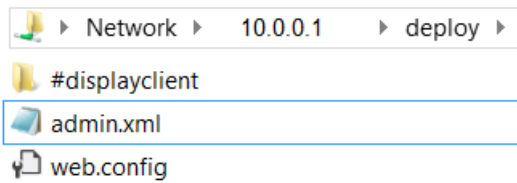


- Select **only** the specific **user**, or **domain group** that will be allowed to edit and deploy VJC Projects.
 - You could add the **'WebAdmin'** group, but only if this group was made as a **'Domain Group'** in earlier steps.
 - Select **'Full Control'**

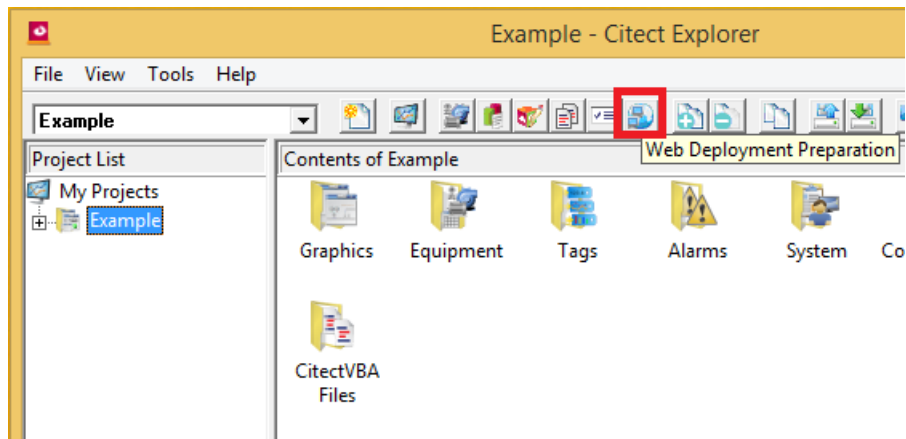


From your Engineering / Development PC:

- In Explorer, check access to the share folder we just created
 - For this example, the Web Server IP address is 10.0.0.1



- Edit the local INI file, adding the following parameters:
 - [WEBSERVER]
 - DeployRoot = \\10.0.0.1\deploy
 - WebClientCab = 750/CitectSCADAWebClient_7_50_0_4107.cab
- Open **Vijeo Citect Explorer**
- Selected your project on the left hand tree, then select **'Web Deployment Preparation'**



- This will perform the following actions:
 - Prepare the project files ready for deployment
 - Upload the files to the [WEBSERVER]'DeployRoot' folder, defined above.
 - Creates the entry on the Webpage to show the deployment
- Now, browse to the website, and you will see your deployment is there, ready to launch:

Web Client Deployment

Deployment	Description	Action
example		

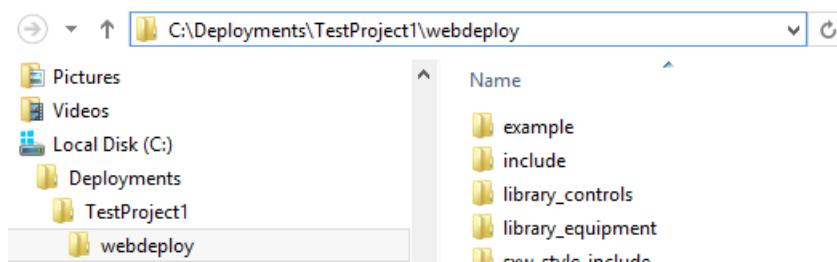
- If we edit the deployment we see several fields greyed-out, but we can still edit the **'Server', 'IP Address', 'Port' fields**, discussed in a later section


Web Client Deployment

Deployment	Description	Action
LocalDeployment	This is being created from a local WebClient	
Server	IP Address	Port
<input type="text"/>	<input type="text"/>	<input type="text"/>
File Paths 350 / 34 MB		
Project Path: C:\ProgramData\Schneider Electric\Vijeo Citect 7.50\User\Example		
Client Control: 750/CitectSCADAWebClient_7_50_0_4107.cab		



Manually uploading a deployment (OPTIONAL / ALTERNATE METHOD):

- Manually copy the **'WebDeploy'** files to a local folder on the IIS machine, such as:
 - **C:\Deployments\ProjectName\WebDeploy**



- Navigate to the site via Internet Explorer (i.e <http://10.0.0.1/Citect>)
 - Log in as a member of **WebAdmin**.
- Select the button to the right of **'Action'** 
- This will open the **'Create a New Deployment'** page.

Web Client Deployment

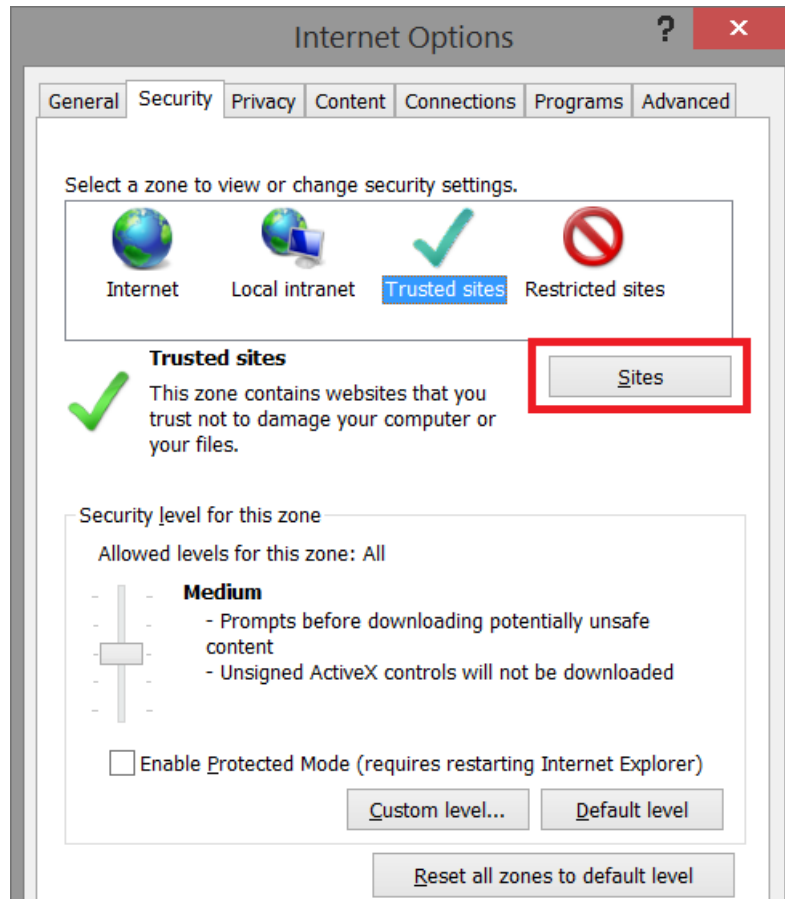
Deployment			Description		Action ?
<input type="text"/>			<input type="text"/>		 
Server	IP Address	Port	File Paths		
<input type="text"/>	<input type="text"/>	<input type="text"/>	Project Path: <input type="text"/>		
			Client Control: <input type="text"/>		

- Fill in the **'Deployment'** and **'Description'** with a value of your choosing.
- The **'Server'**, **'IP Address'**, **'Port'** fields can be left blank for now, and are discussed later.
- For **'Project Path'**:
 - The code automatically appends **'webdeploy'** to the **'Project Path'**, so we remove it when we enter the path, i.e: **'C:\Deployments\ProjectName'**.
 - Regardless if your Web Client session is local or remote to the IIS Server, enter the file location, relative to the IIS Server.
 - This is because we aren't uploading the files, instead, the Server-Side code impersonates the privileges of the logged in Web Client and copies from the 'Project Path' to the IIS folders.
 - Hence the 'Project Path' must be readable by the logged in User, or **'WebAdmin'** group that it belongs to.
 - **Known Issue:** Access to the Parent Folder is also required. In our example above, this would mean that the **'WebAdmin'** group would also need read access to 'Deployment'.
- For **'Client Control'**, select the correct version of the ActiveX Client to use for this project.
 - By default there is only the current version Client, however you may have added others through Service Packs, Hotfixes or manually adding older versions.

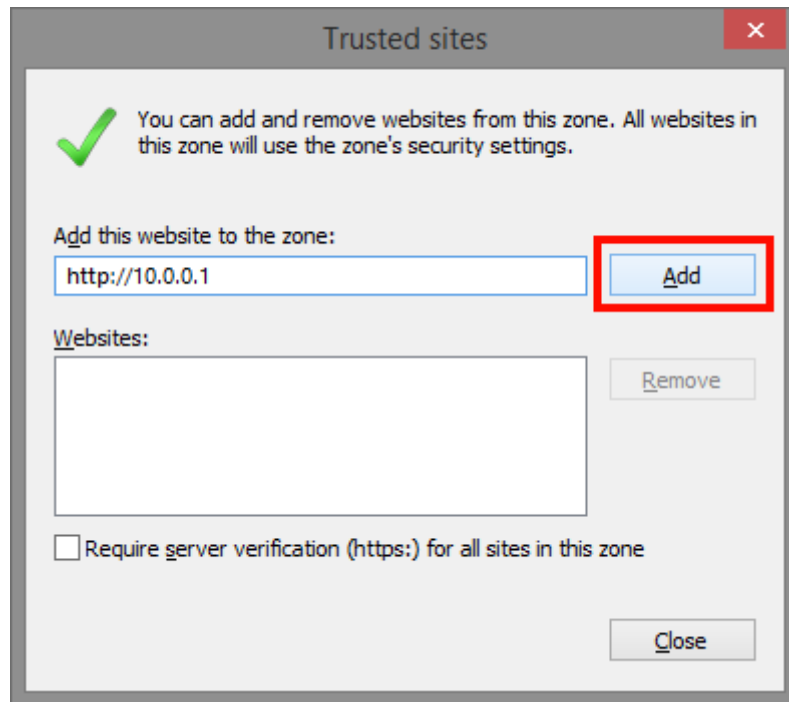
Client-side configuration:

On the Client-side, we recommend adding your Web Server as a Trusted Site:

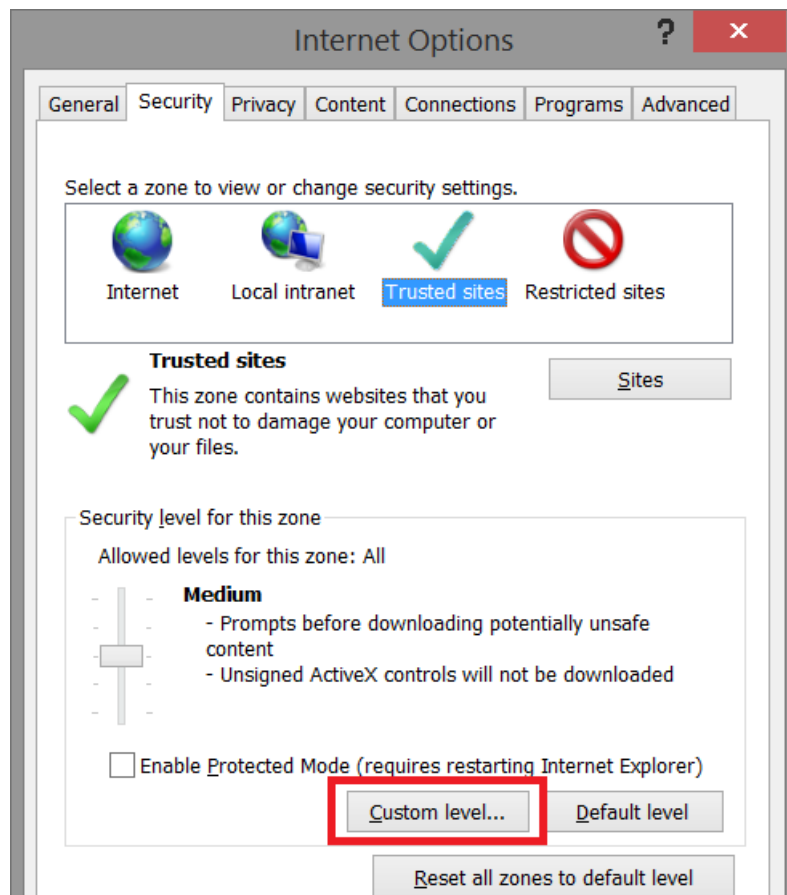
- In Internet Explorer, open **'Internet Options'**
- Select the **'Security'** Tab, and Highlight **'Trusted Sites'**
- Click the **'Sites'** button

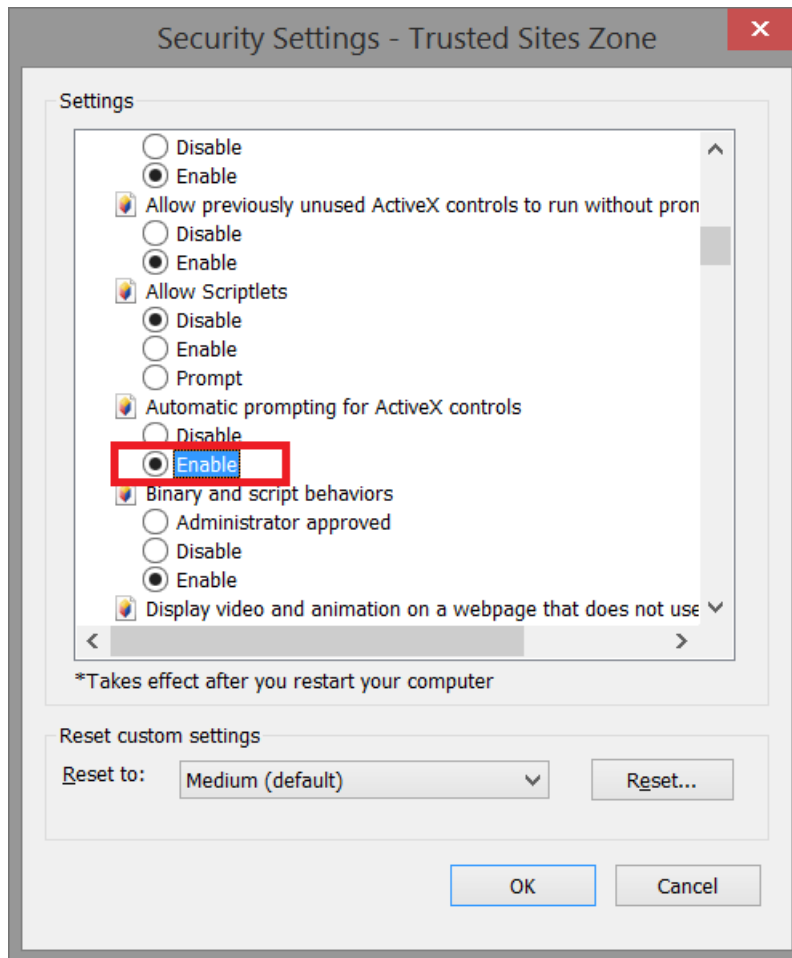


- Enter the external IP address, or name, of your VJC Web Server, click **'Add'**, then **'Close'**



- We also recommend enabling **'Automatic Prompting for ActiveX Controls'** via the **'Custom Level'** menu.

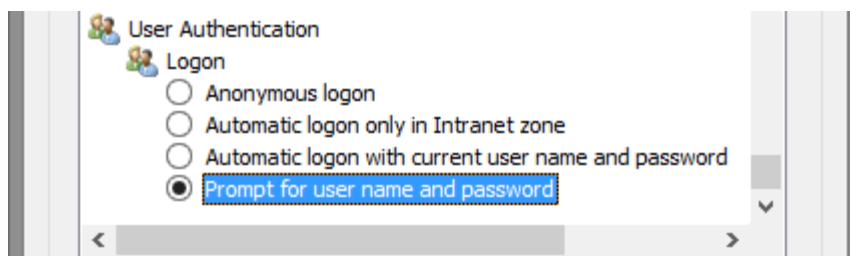




- Enabling this option prevents a looping scenario where a popup: 'Failed to Download CAB file' prevents you from agreeing to install the ActiveX, and closing the popup returns you to the deployment page.

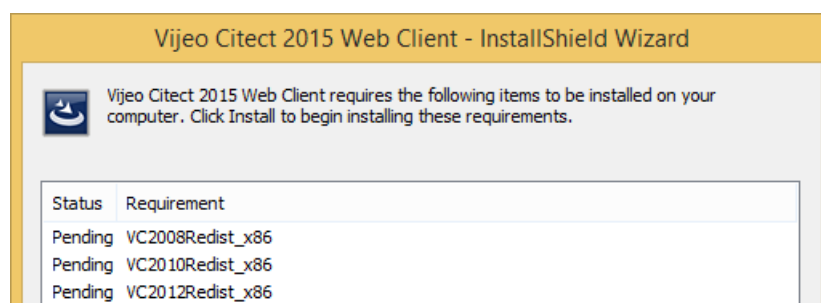
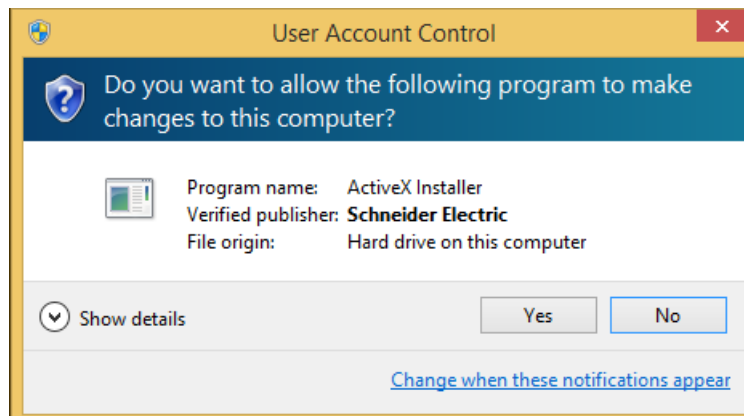
Preventing 'Integrated' Security

- Sometimes you may wish to use a different login to your current Windows user, in this case you could try selecting the following option in the 'Custom Level' settings for your 'Trusted Sites':

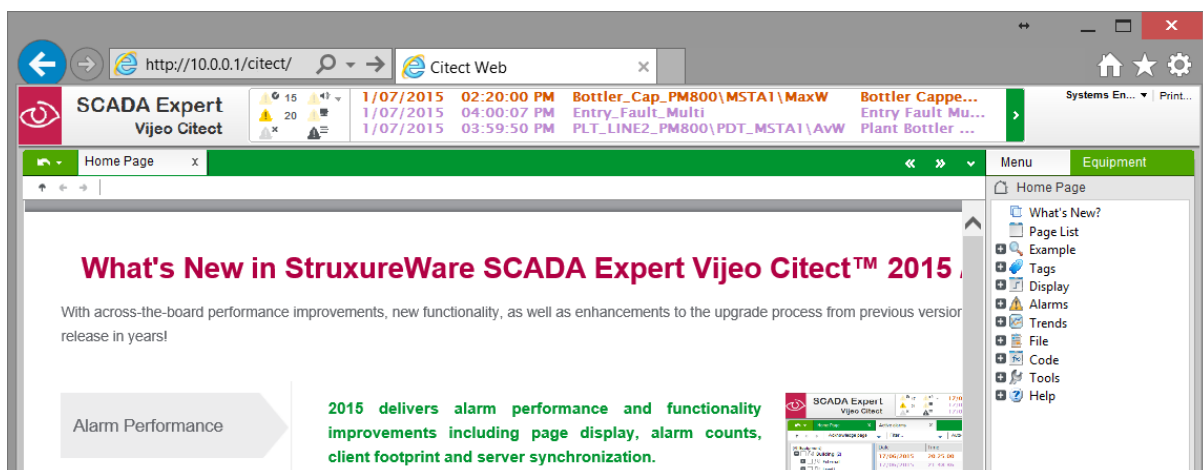


Running Web Client

- Navigate to your Web Server <http://webserver/citect>
- Login with a user from the **WebAdmin**, **WebControl** or **WebViewOnly** groups.
- Select the deployment you wish to run, and whether you wish to use a **ViewOnly** licence, or a **Control Client** Licence.
- You may receive several prompts when running the Client for the first time, such as those below:



- After installing any pre-requisites the Web Client should then load.
- If the Client installs and SCADA pages open, typically the Web Server configuration is correct.
 - Any **#COM**, or **'Software Protection Failure'** events are to do with the connection between the Web Client and the relevant SCADA Server.
 - If you are accessing Web Client from a different network to the SCADA Servers, you will need to use a VPN or configure 'Port Forwarding' as discussed in the next section.

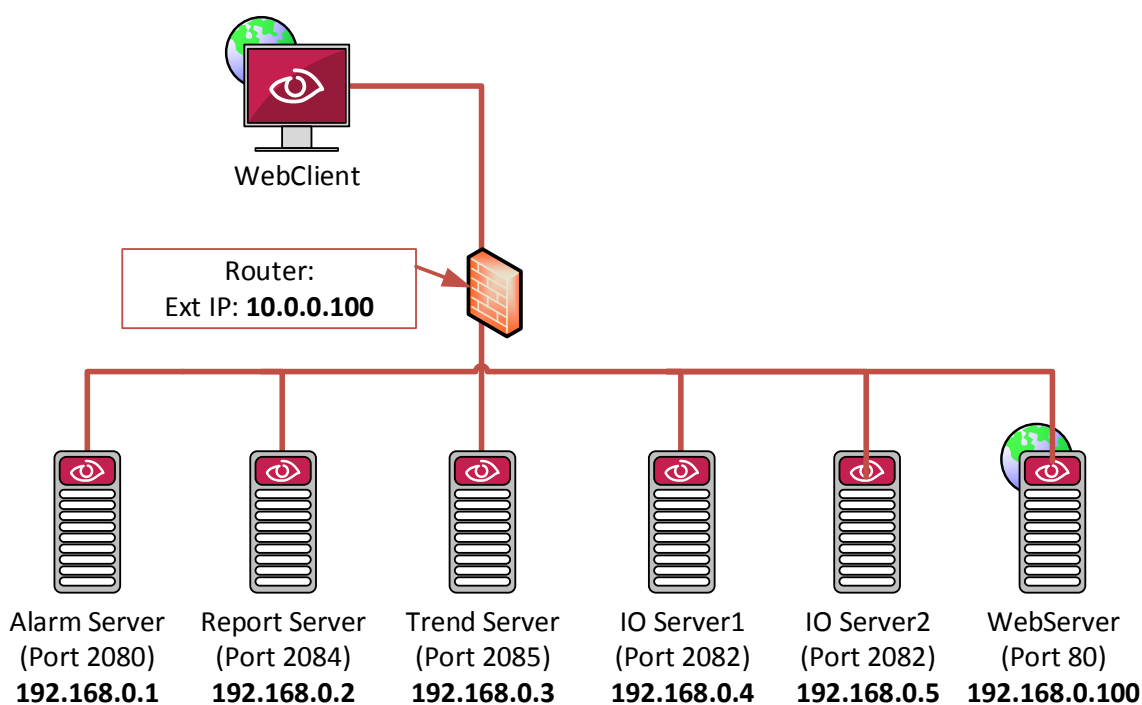


Port-Forwarding / Address Forwarding

As mentioned earlier, it is not appropriate to expose production SCADA servers to the Internet. We strongly recommend a Defence in Depth approach to Control System networking, and recommend following the ISA/IEC 62443 standards as a guide. We suggest the use of Remote Desktop Services (formerly Terminal Services) and/or a VPN to provide secure remote access.

However, if you need to expose your Web Server and SCADA Servers to another network, you will need to establish some form of port forwarding in your perimeter firewall, and then modify your Web Deployment so that your Web Clients are referring to the externally accessible IP addresses.

Example Architecture:



In this scenario, the **Web Client** can access the router's external IP address of **10.0.0.100**, but not the servers directly.

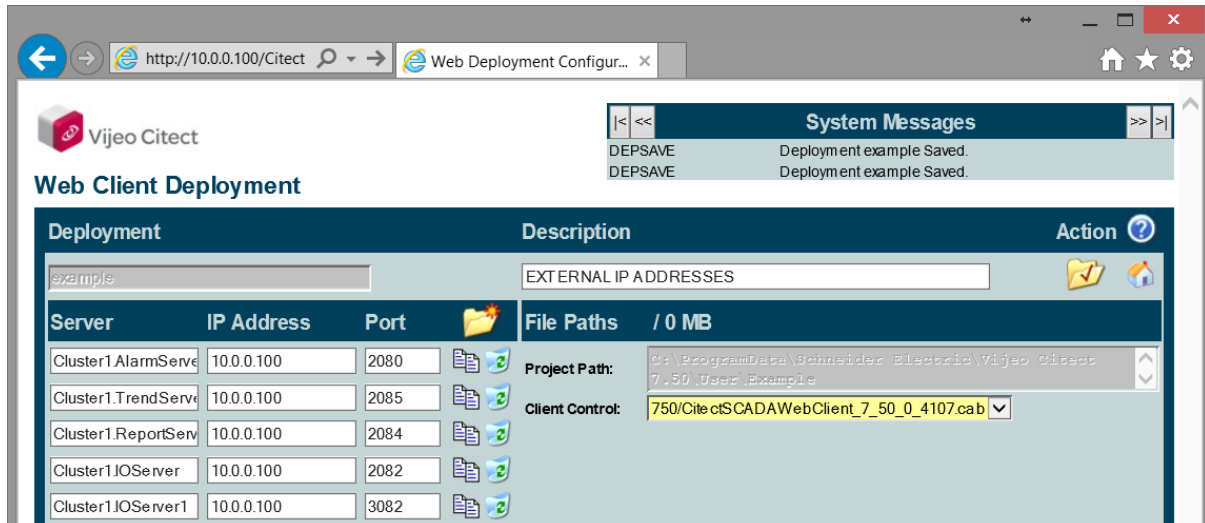
External IP	External Port	Internal IP	Internal Port	Target :
10.0.0.100	80	192.168.0.100	80	Web Server
10.0.0.100	2080	192.168.0.1	2080	Alarm Server
10.0.0.100	2084	192.168.0.2	2084	Report Server
10.0.0.100	2085	192.168.0.3	2085	Trend Server
10.0.0.100	2082	192.168.0.4	2082	IO Server1
10.0.0.100	3082	192.168.0.5	2082	IO Server2

NOTE:

- We picked an arbitrary external port (3082) for 'IO Server2', as 2082 was already in use by 'IO Server1'.
- The 'Internal Ports' above are their default (blank) value, however these should match the values defined for 'Port' in the 'Citect Project Editor' > 'Servers' configuration.

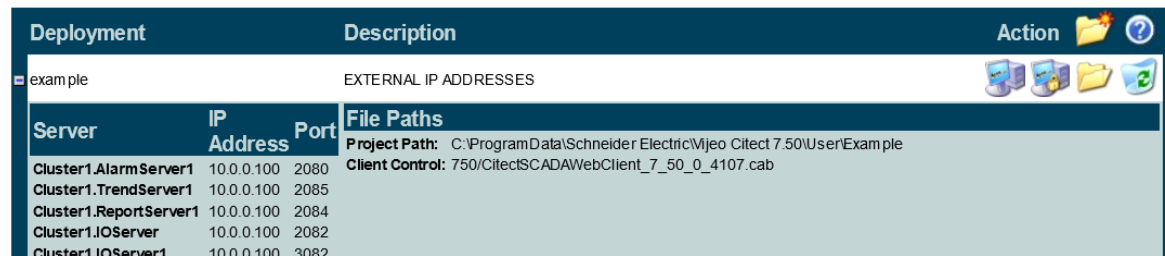
After configuring this port-forwarding in your router, your external Web Clients will need to modify the web deployment so the Web Clients will use the external IP addresses. This is done via the web interface, 'Edit Deployments'.

We can now fill out the 'Server', 'IP Address' and 'Port' settings for the deployment. If you have Web Clients inside and outside the network, you are best of creating two deployments, one with a blank 'Server', 'IP Address' and 'Ports' section to use the default IP address configuration.



Once applied, these settings can be viewed on the main page by clicking the '+' to the left of the Deployment name.

Web Client Deployment



Note: Unfortunately, at the time of publishing, these IP Address settings seem to be lost every time a new Deployment is pushed to this directory from Vijeo Citect Explorer. As a workaround you could manually backup & restore the configuration XML before/after pushing an updated deployment to the Web Server (C:\inetpub\wwwroot\Citect\deploy\ProjectName\citectscada.xml).

Troubleshooting:

Quick Tips:

- Remember, the Web Server **only** serves the ActiveX control and project files
 - Any other **#COM, License Protection Failure** or other standard SCADA-type error is generally to do with the connection between the Web Client, and the SCADA Servers. Ensure that the SCADA Client can ping the SCADA Servers.
- If you are having issues creating a deployment remotely:
 - We strongly recommend using the [WEBSERVER] INI parameters and network shares to push files to the Web Server.
 - If creating the deployment manually, try configuring the deployment via a local Web Client instance directly on the Web Server.
 - Ensure the NTFS permissions are set correctly for the destination IIS folders
 - Ensure there are no extra groups the user belongs to, where 'deny' rules have been set
 - In order to upload a deployment, only the contents of the **'webdeploy'** folder is needed, however, the code is still expecting the folder structure: 'User\ProjectName\webdeploy'.
 - The names of the folders 'User' and 'ProjectName' do not matter.
 - The **'webdeploy'** folder must remain named **'webdeploy'**
 - When manually entering the path to the web deployment, only enter the path to the 'ProjectName' folder.
 - The code then automatically looks for a 'webdeploy' subfolder.
 - Ensure that the **'WebAdmin'** group has permissions to read the 'User' folder and all subfolders, otherwise the deployment will fail.

KB Articles:

Some notable Web Client KB articles are listed below:

<http://www.citect.schneider-electric.com/scada/vijeo-citect/find-answers/knowledge-base>

Q4503 WebClient not supported in FireFox / Mozilla

Q6268 SCADA Web Client Quick Start Guide v7.20, v7.30, v7.40

Q6261 IIS setup for web clients to connect to the web server over HTTPS using SSL

Q4281 Web client Full-screen and as a shell

Q4586 Auto Delete WebClient Cache- Toolbox "ActiveX component can't create object: 'Wscript.Shell'"

Q4467 Installing / Running Web Client without admin rights

Q6041 WebClient Error "Cannot Display Page"

Q6480 WebClient files not copied over correctly from IIS web server

Q6473 Internet Explorer 10 and SCADA webclient – **This workaround is integrated into v7.50 / 2015**

Q4020 XP Style Navigation Menu Is Not Updated Correctly in the WebClient

Q6478 Debugging WebClient - IIS Communication

Q4843 'Loading' screen for Web Client

Q6358 WebClient not functioning properly (CAB file) on IE 64-bit

Q6041 WebClient error "Cannot Display Page"

Q4946 Web Client across LAN / WAN

Q6199 Cannot edit deployment: "DEPERR: error saving deployment permission denied"

Q5649 Error when creating a deployment on a remote Web server

Q4067 How is a Citect.ini file + Settings on a Development/Deployment Machine Propagated to a Web Client?

Q4621 Pages not updated on web client after web deployment