# SCADA v7.20-v7.30 WebClient Quick Start Guide

May 2012 / Technical Paper Rev2 - Updated in October 2013

by Raj Singh / Vincent Thomas

Make the most of your energy



# **Table of Contents**

I.	SCADA WebClient Architecture 4 -		
II.	Server Side Configuration7	-	
1	- 7 Software Requirements	-	
	1.1 IIS Setup on Windows 7	-	
0	1.2 IIS setup on windows Server 2008	-	
2	2 1 Create User Groups - 17	-	
	2.2 Create Users	-	
3	Set up security of the web server 23	-	
4	. Set up security for web deployment 28	-	
5	Prepare SCADA Project for Deployment 30	-	
III.	Client Side Configuration 33	-	
1	Create SCADA Project Deployment	-	
2	Connecting 36	-	
3	Licensing 37	-	
IV.	Connecting WAN Web Clients to SCADA servers and Web Server	-	
1	. Configuring Ports Forwarding in the router-firewall 41	-	
2	Creating a SCADA Web Deployment, with 'Address Forwarding' 43	-	
3	. FAQ 46	-	
IV.	Troubleshooting 47	-	
1	. Internet Explorer and Windows Security settings 47	-	
2	. Software Protection Failure on a Web Client 48	-	
3	Page display and update issues 51	-	
4	. Slow Web Client start-up 54	-	
VI.	IIS Issues 55	-	
1	. IIS v6.0 issues 55	-	
2	. Security (Not applicable for IIS v7 and above) 57	-	
3	- 58 ASP.NET	-	
4	CAB File Download and Installation 59	-	
VII.	References 60	-	
1	. Knowledge base articles: 60	-	
2	User manuals: 60	-	



# Introduction

To display a live Citect project in an Internet browser, you need to combine the content of the project pages and the current data these pages present using standard, Web-based communication protocols. To understand the communication architecture for the Vijeo Citect Web Client, it's easiest to consider the role each of the following components play in achieving this outcome:

- **Citect Web Server** Performs the server-side functionality of the system. It operates by accepting requests from the client, and providing a response to the client when the client's details are authenticated. It then directs a client to the graphical and functional content of a Vijeo Citect project and the location of the runtime servers. This information is stored on the Web Server when a Vijeo Citect project is configured as a "deployment". A Vijeo Citect Web Server can contain multiple deployments.
- Citect Runtime Servers (including the I/O Server, Alarm Server, Trends Server and Reports Server) Monitor the physical production facility and contain the live variable tag data, alarms and trends that the Web Client will display.
- Web Client provides the platform to merge a deployed project's pages and content with the raw data drawn from the runtime servers. Again, standard Web technologies are necessary, so the client uses Microsoft Internet Explorer.

# Audience

The contents of this document are targeted towards SCADA engineers, systems integrators and individuals with intermediate to advanced level knowledge of CitectSCADA/Vijeo Citect, and looking to setup and/or diagnose a SCADA WebClient system.



# I. SCADA WebClient Architecture

The CitectSCADA Web Client allows the remote viewing and control of a live running CitectSCADA project through internet explorer. The three components required are:

- Web server (CitectSCADA web server + Microsoft IIS)
- Run time servers (IO and RAT servers)
- Web client (Internet Explorer)



Figure 1: CitectSCADA Communication Architecture

As we can see from the diagram, the WebServer acts as a Fileserver for project files, however the actual data is still received directly from the SCADA Servers, as per a normal Display Client.



In the following example, the WebServer and SCADA Servers are on the same PC, but this does not always have to be the case.

Hence, in this example only two PCs will be required:



Figure 2: Communication structure of example web client project

- Server
  - Hosts the WebServer
  - Hosts SCADA Runtime Servers
- Client
  - o A 'Display Client' viewed via Internet Explorer
    - Retrieves Project files from WebServer
    - Receives Comms from SCADA Runtime Servers



# Important

User performing steps mentioned in this guide must be logged in with local administrative privileges. If you are not logged in as a local administrator to your Windows PC, please do so before continuing further.

Internet Explorer 10 will only be supported by SCADA WebClient v7.30 Spk1 onwards. See KB article <u>Q6473</u> for further details.



# II. Server Side Configuration

The main benefit of Citect SCADA WebClient is that the majority of the configuration is 'Server-Side'.

In most cases the Client PC does not require any configuration, as Internet Explorer will download the required program files when the WebClient is first run.

However, in some corporate environments, some security settings are required to be modified on the client. All 'Client-Side' settings are covered in a later section.

This section deals with the 'Server-Side' configuration.

### 1. Software Requirements

There are only a few software requirements for installing and functioning of the Web Server component on a PC. It is required to setup Internet Information Sevices (IIS) on the machine designated to be used as a web server

This section covers IIS setup for

- Windows 7
- Windows Server 2008

### 1.1 IIS Setup on Windows 7

The Windows IIS World Wide Web service needs to be installed. Select:

Control Panel >> Program and Features





• Turn Windows Features on or off option on the left of the window.



• Expand Internet Information Services section and select required IIS settings as shown in following screen shots (Table below each screen shots provide a short description on selected options)

Internet Information Services-> Web Management Tools-> IIS 6 Management Compatibility

💽 Windows Features		
Turn Windows features on or off		
To turn a feature on, select its check box. To turn a feature of feature is turned on.	off, clear its check box. A filled box n	
Internet Information Services		
🖃 🔳 🖟 Web Management Tools		
🖃 🔳 🖟 IS 6 Management Compatibility		
IS 6 Management Console		
IS 6 Scripting Tools		
IS 6 WMI Compatibility		
IS Metabase and IS 6 configuration co	ompatibility	
🔽 🍌 IIS Management Console		
IS Management Scripts and Tools		
IS Management Service		

IIS 6 Management Compatibility	Allows you to use existing IIS 6.0 APIs and scripts to manage this IIS 7.0 Web server.
IIS 6 Management Console	Installs the IIS 6.0 Management Console. Provides support for administration of remote IIS 6.0 servers from this computer
Management Service	Allows this Web server to be managed remotely from another computer via the Web server Management Console.



Internet Information Services-> World Wide Web Services-> Application Development Features

🔂 Windows Features		
Turn Windows features on or off		
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled feature is turned on.		
🖃 🔲 🖟 Internet Information Services		
FTP Server		
🕀 🔳 🔒 Web Management Tools		
🖃 🔲 🔒 World Wide Web Services		
Application Development Features		
.NET Extensibility		
ASP		
ASP.NET		
CGI		
ISAPI Extensions		
ISAPI Filters		
Server-Side Includes		

.NET Extensibility	Enables your web server to host .NET framework managed module extensions
ASP	Enables your web server to host classic ASP applications
ASP.NET	Enables your web server to host ASP.NET applications
ISAPI Extensions	Allows ISAPI extensions to handle client requests
ISAPI Filters	Allows ISAPI filters to modify web server behavoiur



Internet Information Services-> World Wide Web Services-> Common HTTP Features

Default Document	Allows you to specify a default file to be loaded when users do not specify a file in a request URL
Directory Browse	Allow clients to see the contents of a directory on your web server
HTTP errors	Installs HTTP error files. Allows you to customize the error messages returned to clients
HTTP redirection	Provides support to redirect client requests to a specific destination
Static Content	Server .htm, .html and image files from a web site
WebDAV Publishing	Web based Distributer Authorising and Versioning. A protocol used for publishing and managing contents to we servers



Internet Information Services-> World Wide Web Services-> Security

Ě	👿 Windows Features		
L	Turn Windows features on or off		
	To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled be feature is turned on.		
l	<ul> <li>□ □ ↓ Internet Information Services</li> <li>         ⊕ □ ↓ FTP Server     </li> </ul>		
L	Application Development Features      Opmon HTTP Features		
L			
L			
L	Basic Authentication		
L			
L	IIS Client Certificate Mapping Authentication		
L	Request Filtering		
	URL Authorization		
	<ul> <li>Health and Diagnostics</li> <li>Performance Features</li> <li>Security</li> <li>Basic Authentication</li> <li>Client Certificate Mapping Authentication</li> <li>Digest Authentication</li> <li>IIS Client Certificate Mapping Authentication</li> <li>IP Security</li> <li>Request Filtering</li> <li>URL Authorization</li> <li>Windows Authentication</li> </ul>		

Basic Authentication	Requires a valid windows user name and password for connection
Request Filtering	Configures rules to block selected clients
Windows Authentication	Authenticates Clients by using NTLM (NT LAN Manager) or Kerberos



### Once all settings are done, IIS setup options should look similar to this:





### 1.2 IIS setup on Windows Server 2008

To enable the required IIS 7 components under *Windows Server 2008*, you need to do the following:

- Click Start, click Administrative Tools, and then click Server Manager.
- In the navigation pane, right-click **Roles**, and then click **Add Roles**.
- Step through the Add Roles Wizard as shown below:

Add Roles Wizard		X
Select Server Ro	les	
Before You Begin Server Roles Web Server (IIS) Role Services Confirmation Progress Results	Select one or more roles to install on this server.         Roles:         Active Directory Certificate Services         Active Directory Domain Services         Active Directory Federation Services         Active Directory Lightweight Directory Services         Active Directory Rights Management Services         Active Directory Rights Management Services         Application Server         DHCP Server         Bile Services         Hyper-V         Network Policy and Access Services         Print and Document Services         Windows Deployment Services         Windows Server (US)         Windows Server Update Services         Windows Server roles	Description:         Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.         application infrastructure.















Before proceeding further check that IIS is setup correctly and you can browse to the IIS home page. To do this type <u>http://<IP</u> Address of the Web Server machine> and press Enter

If IIS is installed correctly and running, you should see a page similar to the one below





# 2. User Account Setup

### 2.1 Create User Groups

Security on the CitectSCADA web server is handled by Windows. Three Windows User Groups must be created on the Server PC:

- 1. WebAdmins user in this group are permitted to remotely view, add, update and delete deployments
- 2. WebControlClients user can view project pages and make adjustments to writable values
- **3.** WebViewOnlyClients user can only view the project pages

To define access privileges on the Server PC:

- Log in to Windows with Local Administrator privileges.
- Go to Control Panel >> Administrative Tools >> Computer Management Tool
- Find "Local Users and Groups" in the directory tree.
- Right select the "Groups" folder and select *New Group*.

	<ul> <li>✓ ✓</li> <li>Search Control Panel</li> </ul>	٩
Adjust your computer's settings	View by: Large icons 🔻	
Action Center Administrativ	re Tools	E
🔾 🖓 🕫 « All Control Panel Items 🕨 Administrative Tools	<ul> <li>✓</li> <li>✓</li> <li>Search Administrative Tools</li> </ul>	,
Organize 🔻 🔳 Open Burn	:≕ ▼	
A Name	Date modified Type	
Desktop	14/07/2009 2:57 PM Shortcut	
Downloads 🛛 🕞 Computer Management	14/07/2009 2:54 PM Shortcut	
🗐 Recent Places 🛛 🔊 Data Sources (ODBC)	14/07/2009 2:53 PM Shortcut	
🔚 Computer Management		
File Action View Help		
B Computer Management (Local Name		
▲ 🎁 System Tools		
Figure 1 Viewer		
Shared Folder	New Group	
Local Users and Groups	Refresh	
Users	Help	

• Right select the "Groups" folder and select *New Group*.



- To create the 'WebAdmins' Group:
  - In the *Group Name* type "WebAdmins" and in the
  - o **Description** type "CitectSCADA Web Client Admin".
  - Select the *Create* button.

New Group	? 💌
Group name:	WebAdmins
Description:	CitectSCADA Web Client Admins
Members:	
Add	Remove
Help	Create Close

- To create the 'WebControlClients' Group:
  - o In the *Group Name* type "WebControlClients" and in the
  - **Description** type CitectSCADA Web Control Clients".
  - Select the *Create* button.
- To create the 'WebViewOnlyClients' Group:
  - o In the Group Name type "WebViewOnlyClients" and in the
  - o Description type "CitectSCADA Web View Only Clients".
  - Select the *Create* button.
- Select the **Close** button.



You will now see these three groups in the list of groups presented in the Computer Management console.

🎥 Computer Management		
File Action View Help		
🗢 🄿 🖄 🖬 🔀	? 🗊	
Ecomputer Management (Lc	Name	Description
<ul> <li>System Tools</li> <li>Task Scheduler</li> <li>Event Viewer</li> <li>Shared Folders</li> <li>Shared Folders</li> <li>Local Users and Grou</li> <li>Users</li> <li>Groups</li> </ul>	SQLServerMSSQLServ SQLServerMSSQLUser SQLServerReportServe SQLServerSQLAgentU WebAdmins WebControlClients	Members in the group have the re Members in the group have the re Members in the group have the re Members in the group have the re
4 III >	wmware	VMware User Group

### 2.2 Create Users

• Create example user of each group in the Computer Management console

Control Panel >> Administrative Tools >> Computer Management

• Find the Local Users and Groups tree sub-item.



• Right-select the Users folder and select New User.



• Enter each of the following three accounts and press **Create** for each:

New User	? 💌	New User	? 🗙
User name: WebAdminUser Full name: Description:		User name: WebControlUser Full name: Description:	
Password: Confirm password: User must change password at next User cannot change password Password never expires Account is disabled	logon	Password:       ••••••••         Confirm password:       ••••••••         User must change password at next logon         User cannot change password         Password never expires         Account is disabled	
Help	Create Close New User User name: Web ViewOnlyU Full name: Description:	Help Create	Close
	Password: Confirm password: User must change password at a User cannot change password at a Ver cannot change password at a Account is disabled Help	next logon	

- Set the password for all three accounts to be something easy to remember, for e.g. **Citect**.
- When done press **Close**.



 Once the users are created, assign these users to the groups created in the previous step. To do this. For each user right select and select **Properties**.
 Computer Management

in comparer management				
File Action View Help				
🗢 🔿 🖄 📰 🔀 📄	? 🗊			
<ul> <li>Computer Management (Local</li> <li>System Tools</li> <li>Task Scheduler</li> <li>Event Viewer</li> <li>Shared Folders</li> <li>Local Users and Groups</li> </ul>	Name vmware_u Administrator ASPNET Guest RajSingh	Full Name	_user Machine Acco	Description VMware Us Built-in acc Account us Built-in acc
Users Groups ▷ (◎) Performance ⓓ Device Manager ⓓ Storage ⓓ Disk Management ▷ █ Services and Applications	WebAdmin	WebAd WebCc WebVit	Set Password All Tasks Delete Rename Properties Help	···

• Select the Member Of tab and press Add.

WebAdminUser Properties	? 🗙
General Member Of Profile	
Member of:	
A Users	
Changes to a user's group men	nbership
Add Remove are not effective until the next t user logs on.	time the
OK Cancel Apply	Help



- Make sure the "locations.." field displays the workstation name.
- Enter the group for each user in the bottom field and press **Ok**.

Select Groups	<u>لا م</u>
Select this object type:	
Groups	Object Types
From this location:	
WIN-K54MP822KNF	Locations
Enter the object names to select ( <u>examples</u> ): WIN-K54MP822KNF\WebAdmins	Check Names
, Advanced	OK Cancel

• Once done for each, the group will be in the **Member of** list for the specific use.

WebAdminUser Properties
General Member Of Profile
Member of: WebAdmins
Add Remove Changes to a user's group membership are not effective until the next time the user logs on.
OK Cancel Apply Help

Note:

Above example is for adding "WebAdminUser" to "WebAdmin" group. Repeat this process to add "WebControlUser" to "WebControlClients" group and "WebViewUser" to "WebViewClients" Group.



### 3. Set up security of the web server

- You need to adjust the security settings for the Web Server folder.
- Locate and right-select the Web Server folder, located in the installation directory.
- By default this will be C:\inetpub\wwwroot\Citect
- Select Properties.





• From the Properties dialog select the **Security** tab and click on the **Edit** button

📙 Citect Properties 🧮	3
General Sharing Security Previous Versions Customize	
Object name: C:\inetpub\wwwroot\Citect	
Group or user names:	
& SYSTEM	
Administrators (W7AU0611299QC7L\Administrators)	
02 11eare (M/7A1106112990) TI \11eare)	
To change permissions, click Edit.	
Permissions for CREATOR	
OWNER Allow Deny	
Full control	
Modify	
Read & execute	
List folder contents	
Read	
Write T	
For special permissions or advanced settings, Advanced Advanced.	
Learn about access control and permissions	
OK Cancel Apply	

• From "**Permissions for Citect**" pop up select the **Add** button to add the three new groups we have created in the previous steps

👃 Permissions for Citect		×
Security		
Object name: C:\inetpub\www.rd	oot\Citect	
Group or user names:		
& CREATOR OWNER		
& SYSTEM		
Administrators (W7AU061129	9QC7L\Administrate	ors)
& Users (W7AU0611299QC7LV	Users)	
8 IIS_IUSRS (W7AU0611299Q	C7L\IIS_IUSRS)	
X IrustedInstaller		
	Add	Remove
Permissions for CREATOR		
OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		-
Learn about access control and pe		
Lean about access control and pe	missions	



You need to be logged into Windows with a user that has Administrator privileges to edit security permissions on the Citect folder.

Select Users or Groups	? 💌
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
W7AU0611299QC7L	Locations
Enter the object names to select ( <u>examples</u> ):	
W7AU0611299QC7L\WebAdmin	Check Names
1	
Advanced	OK Cancel

- Make sure the "**locations..**" field displays the workstation name. Type in "WebAdmin" for web administrators group and click on the Check Names button to make sure this group names resolves correctly to the group we have created in section 3.1. Once done click OK.
- Repeat this process to add "WebControlClients" and "WebViewOnlyClients". Once you
  have all three groups added, Security section in "Permissions for Citect" should look as
  below

Permissions for Citect		
Security		
Object name: C:\inetpub\w	www.root\Citect	
Group of upor pomos:		
Restedinstaller	2330071113_10313)	<u> </u>
& WebAdmin (W7AU0611)	299QC7L\WebAdmin)	-
& WebControlClients (W7A	U0611299QC7L\Web	ControlClien 🗉
& WebViewOnlyClients (W	7AU0611299QC7L\W	ebViewOnly 👻
•	111	+
•	Mdd	Remove
Permissions for WebViewOnlyClients	Add	Remove
Permissions for WebViewOnlyClients Full control	Add Allow	Remove Deny
Permissions for WebViewOnlyClients Full control Modify	Add Allow	Remove Deny
Permissions for WebViewOnlyClients Full control Modify Read & execute	Add Allow	Remove Deny
Permissions for WebViewOnlyClients Full control Modify Read & execute List folder contents	Add Allow	Remove Deny
Permissions for WebViewOnlyClients Full control Modify Read & execute List folder contents Read	Add Allow	Remove Deny
Permissions for WebViewOnlyClients Full control Modify Read & execute List folder contents Read	Add Allow	Remove Deny
Permissions for WebViewOnlyClients Full control Modify Read & execute List folder contents Read Leam about access control ar	Add Allow Allow	Remove Deny

Make sure all three groups have "Read & Execute", "List Folder Contents" and "Read" permissions



• Click OK on the Permissions for Citect pop up and go back to the Citect Folder properties - > Security Tab. This should now list the three groups we have added

1. Citect Properties
General Sharing Security Previous Versions Customize
Object name: C:\inetpub\wwwroot\Citect
Group or user names:
🞎 WebAdmin (W7AU0611299QC7L\WebAdmin)
& WebControlClients (W7AU0611299QC7L\WebControlClien
WebViewOnlyClients (W7AU0611299QC7L\WebViewOnly  Administrators (W/7AU0611299QC7L\Administrators)
4 m
To change permissions, click Edit.
Permissions for WebAdmin Allow Deny
Full control
Modify
Read & execute 🗸 🗉
List folder contents 🗸
Read 🗸
Write
For special permissions or advanced settings, Advanced
Learn about access control and permissions
OK Cancel Apply

Press the Advanced button to bring up "Advanced Security Settings for Citect" and Click on the "Change Permissions" Button

-	entries:			
Туре	Name	Permission	Inherited From	Apply To
Allow	CREATOR OWNER	Special	<not inherited=""></not>	Subfolders and files only
Allow	SYSTEM	Full control	<not inherited=""></not>	This folder, subfolders and
Allow	Administrators (W7AU061	Full control	<not inherited=""></not>	This folder, subfolders and 🗮
Allow	Users (W7AU0611299QC	Read & execute	<not inherited=""></not>	This folder, subfolders and
Allow	IIS_IUSRS (W7AU06112	Read & execute	<not inherited=""></not>	This folder, subfolders and
Allow	TrustedInstaller	Full control	<not inherited=""></not>	This folder, subfolders and
Allow	WebAdmin (W7AU06112	Read & execute	<not inherited=""></not>	This folder, subfolders and
	M-LC	D 0 111	And a sub-case dis-	Tu:: /
Chang Include	ge Permissions] e inheritable permissions from this permission entries	object's parent		



• Select Replace permission entries on all child objects...,

🗼 Advance	d Security Settings for Citect				×
Permissions					
To view or Object nar	r edit details for a permission en me: C: \inetpub \www.root\C	try, select the entry a itect	and then click Edit.		
Permission	entries:				
Type	Name	Permission	Inherited From	Apply To	5
Allow	CREATOR OWNER	Special	<not inherited=""></not>	Subfolders and files only	
Allow	SYSTEM	Full control	<not inherited=""></not>	This folder, subfolders a	
Allow	Administrators (W7AU06	Full control	<not inherited=""></not>	This folder, subfolders a	Ĩ
Allow	Users (W7AU0611299Q	Read & execute	<not inherited=""></not>	This folder, subfolders a	
Allow	IIS_IUSRS (W7AU06112	Read & execute	<not inherited=""></not>	This folder, subfolders a 🖕	.
•				•	
	Edit	Remove			
Replac	e all child object permissions wit	h inheritable permissio	ons from this object		
Managing	permission entries				
			ОК	Cancel Apply	

• Once selected, press Ok. A security dialog will appear, press Yes.





### 4. Set up security for web deployment

• We need to set up user group specific access rights. Locate the Deploy subdirectory in the Web Server folder



• Right select "deploy" folder and select properties. Select **Edit** button and highlight "WebAdmin" group in the new "Permissions for deploy" pop-up and give **Full Control** to this group

👗 deploy Properties 🛛 🔀	🖡 Permissions for deploy 💽
General Sharing Security Previous Versions Customize	Security
Object name: C:\inetpub\wwwroot\Citect\deploy	Object name: C:\inetpub\wwwroot\Citect\deploy
Group or user names:	Group or user names:
Image: System     Image: System       Image: System     Image: System       Image: System     Image: System	& CREATOR OWNER
WebContmlCliente (W7ALIDG112990C7) WebContmlClien     To change permissions, click Edit.	WebAdmin (W/AU0611299QC7L\WebAdmin)  WebControlClients (W7AU0611299QC7L\WebControlClien  WebViewOnlyClients (W7AU0611299QC7L\WebViewOnly
Permissions for WebAdmin Allow Deny	Add Remove
Full control Modify	Permissions for WebAdmin Allow Deny
Read & execute	Full control
Read	Modify
Write	Read & execute
For special permissions or advanced settings.	List folder contents
click Advanced.	Read 🗸 📃 👻
Learn about access control and permissions	Leam about access control and permissions
OK Cancel Apply	OK Cancel Apply



• Locate the **deploy\#displayClient** subdirectory and set **Deny Full Control** for the "WebViewOnlyClients" Group

🗼 #displayclient Properties 🛛 🔀	der
General Sharing Security Previous Versions Customize	🐌 Permissions for #displayclient 💽
Object name: C:\inetpub\wwwroot\Citect\deploy\#displayclient	Security
Group or user names:	Object name: C:\inetpub\wwwroot\Citect\deploy\#displayclient
& WebControlClients (W7AU0611299QC7L\WebControlClien 🔺	
& WebViewOnlyClients (W7AU0611299QC7L\WebViewOnly	Group or user names:
& Administrators (W7AU0611299QC7L\Administrators)	& CREATOR OWNER
1 Leare ΛΛ/7ΔΙΙΩ611299∩C7I\\Leare\	& SYSTEM
4 m	🎎 WebAdmin (W7AU0611299QC7L\WebAdmin)
To change permissions, click Edit.	& WebControlClients (W7AU0611299QC7L\WebControlClien
Permissions for	🎎 Web ViewOnlyClients (W7AU0611299QC7L\Web ViewOnly 👻
WebViewOnlyClients Allow Deny	4
Full control	
Modify	Add Remove
Read & execute	Permissions for Web View OphyCliepts Allow Depy
Pead Paid	Full control
Wa.	Modify 🖉 🚽
vvnte	Read & execute 🗸 🗸 👘
For special permissions or advanced settings, Advanced	List folder contents
click Advanced.	Read 🗸 🗸 🗸
Leam about access control and permissions	Learn about access control and permissions
OK Cancel Apply	OK Cancel Apply

• A security prompt will appear, press Yes to accept changes





# 5. Prepare SCADA Project for Deployment

We will be using the Example project in CitectSCADA 7.20 for demonstration of the web client.. Make it the active project in Citect Explorer and then Compile the project (File >> Compile in the Project Editor). Then, from either the Project Editor or Citect Explorer, run *Tools* >> *Computer Setup Wizard*.

• Use the following settings:







- If the content of the project incorporates any user created files, such as DBF, HTML or CSV files, you will need to manually place these into a special zip file called Misc.zip and store inside the Citect\User\<Project Name> directory.
- Similarly, if a project contains any ActiveX objects, these will also need to be included in a zip file called **ActiveX.zip**. The example project comes with this already done.
- The example project already comes compiled with CitectSCADA V7.20, so there is no need to compile the project unless you have made changes to it. Otherwise, if you are using a different project a fresh compile is required before the next step.



Next run *Tools* >> *Web Deployment Preparation* [or the button] in Citect Explorer.

	Citect Explorer
Web deployment preparation	
Copying file tanks_con_pipe.ctl	Successfully created deployment
Abort	ОК

A progress bar and completion message will appear, as shown above. Confirm that a webdeploy folder exists in the Example project folder.

Name kample_old include system tab_style_include

Once this is complete, run the example project in Citect.



# **III.** Client Side Configuration

Internet Explorer 6.0 or later is required to use the Web Client.

Please note that Microsoft Internet Explorer is the only supported web browser at present. Please also note that Internet Explorer 10 is only supported from SCADA version v7.30 Spk1.

# 1. Create SCADA Project Deployment

- Open up Internet Explorer and enter this url: <u>http://<server>/Citect</u>.
- <server> is either the: server PC name, server PC IP address, or *localhost* if the web client is running on the server PC.
- A login screen will appear, for each user created, enter the login details. The screen that is supposed to appear is shown below.

Certificate Error: Navigation Blocked - Windows Internet Explorer
G ⊂ ▼ Image: A https://localhost/Citect/
🚖 Favorites 🛛 🚔 🌄 Suggested Sites 👻 🔊 Web Slice Gallery 💌
Certificate Error: Navigation Blocked
Windows Security
The server localhost at localhost requires a username and password.
webadminuser
Remember my credentials
OK Cancel



Depending on which user is being logged in, a web client home page similar to one of the below will be disaplyed



Username: WebAdminUser Password: citect

Username: WebControlUser

Password: citect

Web Deployments Overview - Windows	Internet Explorer			
G 🕞 🗢 🙋 http://localhost/Citect/			🕶 💀 🐓 🗙 🖸 Bing	+ م
🚖 Favorites 🛛 🚔 🌄 Suggested Sites 🕶	🥭 Web Slice Gallery 🕶			
A Web Deployments Overview			🏠 🔻 🔝 👻 🖶 🗮 👻 Page 🕶	Safety ▼ Tools ▼ 🕢 ▼
				*
Vijeo Citect		< <<	System Messages	>> >
a socollaborative software		LOGINDC	Control Client webcontrolclientuser logge	d in.
Web Client Deployment				
Deployment	Description			Action 🕜
Example_project				

#### Username: WebViewOnlyUser

Password: citect

( Web Deployments Overview - Windows In	nternet Explorer	-		
G 🕞 🗢 🖉 http://localhost/Citect/			🕶 💀 🐓 🗙 📴 Bing	+ م
🖕 Favorites 🛛 🚔 🌄 Suggested Sites 🔻	💋 Web Slice Gallery 🔻			
See Web Deployments Overview			🏠 🔻 🔝 🔻 🖃 🖶 👻 Page 🕶 Sa	afety ▼ Tools ▼ 🕢 ▼
				^
Vijeo Citect		< <<	System Messages	>> >
a socoliaborative software		LOGINMC	View-only Client webviewonlyuser logged in.	
Web Client Deployment				
Deployment	Description			Action 🕜
Example_project				<b>3</b>

If you do not get these windows for each user, the setting up of user access rights from Section 3.3 has not been done correctly.

<u>Note:</u> If you have Windows authentication enabled, you may be logged in automatically to the web server without being prompted for a username or password, please follow KB Q5957 for details on fixing this.



To create the project deployment, login as the web client admin user ("WebClientAdminUser" in

this example). Then select the Add New Deployment icon

In the Deployment field enter the name to identify the deployment, in this case "TestExample". Enter the project path of the Example project on the CitectSCADA server PC, and select the Client control from the list [there should be one available].

🏉 Web Deployment C	onfiguration - Windows In	ternet Explorer	r man	and the second second				
🕞 🔾 🔻 🙋 http	o://localhost/Citect/addedi	itdeploy.htm?D	eployDir=Exa	mple_project⟨:	en-us	🗕 🔀 🗲 🗙 🔁 Bing		۹ م
🖕 Favorites 🛛 👍	🤉 Suggested Sites 👻 🙋	Web Slice Galle	ery 🔻					
🥖 🖉 Web Deployment	Configuration					🛐 🔻 🖾 👻 🚍 🖛 Page 🗸 Si	afety 🔻 Too	ls 🕶 🔞 🕶 🤅
Vijeo C	Citect orative software				< <<	System Messages		>> >
Web Client	Deployment							
Deployment				Description			Action	?
Example_projec	t						V	
Server	IP Address	Port	2	File Paths		284 / 23 MB		
			Èr 🦻	Project Path:		C:\ProgramData\Schneider Electric\Vijeo 7.20\User\Example	Citect	A T
				Client Control:		720/CitectSCADAWebClient_7_20_0_598.cab -		

Select the **Apply Changes** button **I**. A progress bar will be displayed as the project deployment files are copied from the User\Example\webdeploy folder to the \inetpub\wwwroot\Citect\deploy\Example\_Project.

🥫 Web Deployn	nent Progress Webpage Dialog
59% CO5317~1	.CLZ
DEPWAIT	Copying Deployment Examp, please wait

**Note:** When a project is deployed the project path and client control settings are first taken from the citect.ini file. If they cannot be found they are taken from the settings entered at this stage.

Select the Go to Deployment List button

If it is the first time you start the client, the required software is automatically downloaded and will prompt the user to install. When the windows security dialog appears click on **Yes**.



# 2. Connecting

You can display the list of connected clients on the Citect server at any time. Type "page table tran" in the main window of the kernel. Screenshot below shows how this would appear in kernel window.

Citect Kernel - [Table]	-	_				-	-	-	-	_		
嶺 Options View Tools	Window Help						_					_ 8 ×
Table Tran Handle 29 Tength	64 Offeet 0	0					Web C	lient loc	ated on	i local ma	chine conn	ecting to this server
Name	Node	Туре	Mode	Hnd	Cnt	Send	Rec	Wait	Stack	Service	State	Access
IOServerCluster1	WIN-K54MP822KNF	Client	InProc	0	1	7	56	0	0	IO	Online	Trusted
DRI:Cluster1Alarm	WIN-K54MP822KNF	Client	InProc	1	1	7	289	0	0	Alarm	Online	Trusted
DRI:Cluster1Trend	WIN-K54MP822KNF	Client	InProc	2	1	8	55	0	0	Trend	Online	Trusted
Cluster1Alarm	WIN-K54MP822KNF	Client	InProc	3	1	581	491	0	0	Alarm	Online	Trusted
AlarmServer1Cluster1	WIN-K54MP822KNF	Client	InProc	4	1	7	289	0	0	Alarm	Online	Trusted
AlarmServer1Cluster1	WIN-K54MP822KNF	Server	InProc	5	1	489	582	0	0	Alarm	Online	Trusted
AlarmServer1Cluster1	WIN-K54MP822KNF	Server	InProc	6	1	287	8	0	0	Alarm	Online	Trusted
AlarmServer1Cluster1	WIN-K54MP822KNF	Server	InProc	7	1	287	8	0	0	Alarm	Online	Trusted
Cluster1Trend	WIN-K54MP822KNF	Client	InProc	8	1	53	101	0	0	Trend	Online	Trusted
TrendServer1Cluster1	WIN-K54MP822KNF	Server	InProc	9	1	99	54	0	0	Trend	Online	Trusted
Cluster1Report	WIN-K54MP822KNF	Client	InProc	10	1	7	55	0	0	Report	Online	Trusted
ReportServer1Cluster	WIN-K54MP822KNF	Server	InProc	11	1	53	8	0	0	Report	Online	Trusted
TrendServer1Cluster1	WIN-K54MP822KNF	Server	InProc	12	1	53	9	0	0	Trend	Online	Trusted
IOServerCluster1	WIN-K54MP822KNF	Server	InProc	13	1	54	8	0	0	IO	Online	Trusted
IOServerCluster1	WIN-K54MP822KNF	Server	OutPro	14	1	56	12	0	0	IO	Online	Authenticat
AlarmServer1Cluster1	WIN-K54MP822KNF	Server	OutPro	15	1	480	487	0	0	Alarm	Online	Authenticat
AlarmServer1Cluster1	WIN-K54MP822KNF	Server	OutPro	16	1	277	9	0	0	Alarm	Online	Authenticat
TrendServer1Cluster1	WIN-K54MP822KNF	Server	OutPro	17	1	54	10	0	0	Trend	Online	Authenticat
ReportServer1Cluster	WIN-K54MP822KNF	Server	Out.Pro	18	1	53	9	0	Ω	Report	Online	Authenticat
IOServerCluster1	W7AU0611299QC7L	Server	Remote	19	1	9	10	0	0	IO	Online	Authenticat
AlarmServer1Cluster1	W7AU0611299QC7L	Server	Remote	20	1	22	19	0	0	Alarm	Online	Authenticat
AlarmServer1Cluster1	W7AU0611299QC7L	Server	Remote	21	1	14	10	0	0	Alarm	Online	Authenticat
TrendServer1Cluster1	W7AU0611299QC7L	Server	Remote	22	1	8	9	0	0	Trend	Online	Authenticat
ReportServer1Cluster	W7AU0611299QC7L	Server	Remote	23	1	7	8	0	0	Report	Online	Authenticat
				Web	Client	located	on a diff	erent m	achine (	connectir	g to this se	rver



# 3. Licensing

Web control client and Web view only clients are licensed using the "Web/ Internet Control Clients" and "Web/ Internet View-only Clients" license respectively. You can check for availability of these licenses using CiUsafe or Kernel->View->General window.

Product: Vijeo Citect		Visit <u>http://www.citect.com/authcode</u> to get an update authorization code for your Citect key.
Serial No: 0479 - 81846		Enter your authorization code and press 'Update Key'
,  :	Mahar	Authorization Code:
SCADA Version SCADA Point Count Full Licenses Control Clients View-only Clients Web/Internet Control Clients Web/Internet View-only Clients	7.3x Unlimited 1 1 1 1	Update Key
Connectivity/OPC Servers OLEDB Connectors	10 10 10	Key ID: HZASHSHNDBEDENEREBDH
Site ID	21607	Retum Code: KEY FOUND SUCCESSFULLY



💐 General	- • ×
General Statistics Version 7.20	
Node Name: WIN-K54MP822KNF Time: Fri May 11 2012 10:04:04 AM Timer Resolution: 1 ms Running since last Startup : 0 Days 0 Hours 2 min 20 sec Running since last Stat Reset: 0 Days 0 Hours 2 min 20 sec Memory Total 1,808,308 KB Physical 376,100 KB Resources 100 %	
Read Requests:00Write Requests:00Physical Reads:00Physical Writes:00Blocked Reads:0Blocked Writes:00Digital Reads:0Register Reads:00Digital Reads Per Sec:0Register Reads Per Sec:0	
Cache Reads:0Cache Reads:0 %Cache RD Ahead:0Cache RD Ahead:0 %	
Cache Buffers:         0         Cache Flush:         0           Average         Minimum         Maximum         Count           Response Times:         0.000         0.000         0           KerMain Cycle:         0.002         0.000         4294937.94         0.000         65,162	
Scheduler Cycles:     779     Tasks Per Second:     6028       CPU Usage:     14 % Lost Errors:     0       Paint Count     New Full:     1     Current Full:     1	
Max: Huge Max V/O: 1 Current V/O: 0 Peak V/O: 0 Current: 0 Max Ctrl: 1 Current Ctrl: 0 Peak Ctrl: 0	
Max Inet V/O:1Current Inet V/O:0Peak Inet V/O:0Max Inet Ctrl:1Current Inet Ctrl:1Peak Inet Ctrl:1Max API:10Current API:0Peak API:0Max OLEDB:10Current OLEDB:0Peak OLEDB:0	
Web Control / View-Only client Licenses currently	used
Available Web Control / View-Only client Licenses	

When a web client tries to connect to a server that does not have any Web/ Internet Control or View-only licenses left the following prompt windows will appear.



CitectSCADAWeb - Microsoft Internet Explorer		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
🗢 Back 🔹 🔿 🗸 🔯 🖓 Search 📾 Favorites 💔 Media 🧭 🖏 🚽 🎒		
Address 💩 http://192.168.0.253/CitectScada/scada.htm?DeployDir=TestExample&ProjectName=example&ClientCAB=600/CitectS	∂Go	Links »
Citest Web Client queter shorted. Disease relead page to restart		<u> </u>
Chect web chent system aborted. Please reload page to restart		



# IV. Connecting WAN Web Clients to SCADA servers and Web Server

**Note:** It can be considered a security risk to open your SCADA Network to the Internet, or even the Corporate Network. In such environments, it is <u>our advice to use third-party VPN software to allow</u> <u>external clients to securely and temporarily connect to the SCADA Network</u>, then run the Web Client as a local LAN user, with default settings.



A Web Client can be located outside of the Local Area Network (LAN) to which both the Citect SCADA and Web servers are located. The setup shown above consists of redundant I/O, Report, Alarm and Trend Servers in a single 'Cluster'.

Allowing Web Clients on the WAN to communicate to the SCADA Servers on the LAN, is a twostep procedure:

- Configure '**Port Forwarding**' in the Router, so that requests to the ports of 125.0.0.1 are redirected to the appropriate Web / SCADA Servers.
- Configure 'Address Forwarding' so that the Web Clients knows to use these new addresses, instead of those configured in the project.



The following table defines the default ports for SCADA v7.20, and those required for a Web Client to communicate with the SCADA and Web Servers, are highlighted in **RED**:

Default Port	Server Type	Server Role
21	FTP Server	Page downloads for IDC
80	Web Server	Project files for Web Client
2073	СТАРІ	CTAPI Communications
2074	Client	Cicode Debugging
2084	Report Server	Report Server communications
2080	Alarm Server	Alarm Server communications
2085	Trend Server	Trend Server communications
2078	I/O Server	Legacy I/O communications
2079	IDC	Internet Display Server/Client communications
2080	Alarm Server	Alarm Properties Connector
2088	Time Server	Time Server communications
2082	I/O Server	Publish Subscribe I/O Server communications
20222	ODBC	ODBC Server

The following table defines the default ports for SCADA v7.30, and those required for a Web Client to communicate with the SCADA and Web Servers, are highlighted in **RED**:

Default Port	Server Type	Server Role
21	FTP Server	Page downloads for IDC
80	Web Server	Project files for Web Client
2073	CTAPI	CTAPI Communications
2074	Client	Cicode Debugging
2084	Report Server	Report Server communications
2080	Alarm Server	Alarm Server communications
2085	Trend Server	Trend Server communications
2078	I/O Server	Legacy I/O communications
2079	IDC	Internet Display Server/Client communications
2080	Alarm Server	Alarm Properties Connector
2088	Time Server	Time Server communications
2082	I/O Server	Publish Subscribe I/O Server communications
20222	ODBC	ODBC Server
5482	Alarm Server	Database Port

<u>Note</u>: From SCADA version 7.30, a 'server advise' connection is needed between SCADA web client and Alarm server. This connection is an OPC A&E connection, and it is used by the Alarm server to send Alarm notifications to the SCADA clients. By default, the ports range for that Alarm 'server advise' connection is 5500 to 5509. This means that the Alarm server needs to be able to create TCP connections to the SCADA WebClient ports 5500 to 5509. Therefore, the router on the SCADA server side needs to be configured to allow outbound connections on ports 5500-5509 to any web client machines. Moreover, the router on the Web Client side needs to be configured to allow inbound connection on port 5500 to 5509 from the

SCADA Alarm server machines.



# 1. Configuring Ports Forwarding in the router-firewall

If your router has an inbuilt firewall blocking incoming communication, you must make sure that you define the above port numbers on the exclusion list to allow communication between SCADA clients and servers.

For our example, you will then need to configure 'Port Forwarding' in your Router as follows:

Incoming IP:Port	Outgoing IP:Port	Server Type
125.0.0.1: <b>80</b>	192.168.0. <b>2</b> :80	Web Server
125.0.0.1: <b>2084</b>	192.168.0. <b>3</b> :2084	Report Server 1
125.0.0.1: <b>2080</b>	192.168.0. <b>3</b> :2080	Alarm Server 1
125.0.0.1: <b>2080</b>	192.168.0. <b>3</b> :2080	Alarm server 1 Properties
		connector
125.0.0.1: <b>2085</b>	192.168.0. <b>3</b> :2085	Trend Server 1
125.0.0.1: <b>2078</b>	192.168.0. <b>3</b> :2078	I/O Server 1 Peer Port
125.0.0.1: <b>2082</b>	192.168.0. <b>3</b> :2082	I/O Server 1
125.0.0.1: <b>3084</b>	192.168.0. <b>4</b> :2084	Report Server 2
125.0.0.1: <b>3080</b>	192.168.0. <b>4</b> :2080	Alarm Server 2
125.0.0.1: <b>3080</b>	192.168.0. <b>4</b> :2080	Alarm server 2 Properties
		connector
125.0.0.1: <b>3085</b>	192.168.0. <b>4</b> :2085	Trend Server 2
125.0.0.1: <b>3078</b>	192.168.0. <b>4</b> :2078	I/O Server 2 Peer Port
125.0.0.1: <b>3082</b>	192.168.0. <b>4</b> :2082	I/O Server 2

### Ports forwarding table for a SCADA v7.20 system:

**Note:** For the Second I/O RAT Server, we cannot use the ports 125.0.0.1:2078-->2085, as they have already been mapped to Server1. Hence, we must then use a different range of external ports, but we can still map them to the standard ports on the Servers, since the Servers are at different IP addresses.

i.e 125.0.0.1:3082 is mapped to 192.168.0.4:2082

Not having to change the ports on the Servers allows us not to disturb any configuration of existing Display Clients on the SCADA Network.



Incoming	Outgoing	Server Type
IP:Port	IP:Port	
125.0.0.1: <b>80</b>	192.168.0. <b>2</b> :80	Web Server
125.0.0.1: <b>2084</b>	192.168.0. <b>3</b> :2084	Report Server 1
125.0.0.1: <b>2080</b>	192.168.0. <b>3</b> :2080	Alarm Server 1
125.0.0.1: <b>5482</b>	192.168.0. <b>3</b> :5482	Alarm 1 Database Port
125.0.0.1: <b>2085</b>	192.168.0. <b>3</b> :2085	Trend Server 1
125.0.0.1: <b>2078</b>	192.168.0. <b>3</b> :2078	I/O Server 1 Peer Port
125.0.0.1: <b>2082</b>	192.168.0. <b>3</b> :2082	I/O Server 1
125.0.0.1: <b>3084</b>	192.168.0. <b>4</b> :2084	Report Server 2
125.0.0.1: <b>3080</b>	192.168.0. <b>4</b> :2080	Alarm Server 2
125.0.0.1: <b>6482</b>	192.168.0. <b>4</b> :5482	Alarm 2 Database Port
125.0.0.1: <b>3085</b>	192.168.0. <b>4</b> :2085	Trend Server 2
125.0.0.1: <b>3078</b>	192.168.0. <b>4</b> :2078	I/O Server 2 Peer Port
125.0.0.1: <b>3082</b>	192.168.0. <b>4</b> :2082	I/O Server 2

### Ports forwarding table for a SCADA v7.30 system:

### Notes:

**1-** For the Second I/O RAT Server, we cannot use the ports 125.0.0.1:2078-->2085 and port 5482, as they have already been mapped to Server1. Hence, we must then use a different range of external ports, but we can still map them to the standard ports on the Servers, since the Servers are at different IP addresses.

i.e 125.0.0.1:6482 is mapped to 192.168.0.4:5482

**2-** As mentioned previously, from SCADA v7.30 an Alarm 'server Advise' connection needs to be created by the Alarm server to TCP ports 5500-5509 of the SCADA WebClient. This means that the firewall-router needs to be able to dynamically forward outgoing connections to ports 5500-5509 of any WebClient machines.

When connecting, the Web Client will use the WAN IP Address of the Router, 125.0.0.1. Internet Explorer uses port 80 as the default, so the port can be omitted. i.e: <u>http://125.0.0.1/Citect</u>

This communication is automatically '**Port Forwarded**' to 192.168.0.2:80, where it will connect to the WebServer, and you will be presented with the screen below:





System Messages

# 2. Creating a SCADA Web Deployment, with 'Address Forwarding'

From Citect v7.0, the 'Network Addresses' of each Server are hard-coded within the project, i.e 192.168.0.3. However, the Web Client will not be able to connect directly to these IP addresses. Hence, we need a mechanism of telling the Web Client to use a different IP address to reach the SCADA server(s). This is where the INI section **[AddressForwarding]** comes in.

In order to manage this remapping, the easiest way to configure this is on the 'Edit Deployment' page of the Web Server interface.

Under 'Server', 'IP Address', and 'Port' we need to fill out an entry for each SCADA server that we want the Web Client to talk to. These should be in the following format:

|< <<

# **CitectSCADA**

Web Client Deployment

Server: <Cluster\_Name>.<Server\_Name>

Deployment				Description		Action 🥝
examplev720		_				📝 🔮
Server K	IP Address	Port	1	File Paths	291 / 33 MB	
Cluster1.ReportS1	125.0.0.1	2084	È 💈	Project Path:	C:\ProgramData\Citect\CitectSCADA 7.20	4
Cluster1.AlarmS1	125.0.0.1	2080	Ē 🦻	Client Control:	720/CitectSCADAWebClient 7 20 3 280.cab	
Cluster1.TrendS1	125.0.0.1	2085	È 💈			
OServer1_PeerPort	125.0.0.1	2078	È 💈			
Cluster1.IOserver1	125.0.0.1	2082	È 💈			
Cluster1.ReportS2	125.0.0.1	3084	le 🦻			
Cluster1.AlarmS2	125.0.0.1	3080	Er 🦻			
Cluster1.TrendS2	125.0.0.1	3085	Èr 🦻			
OServer2_PeerPort	125.0.0.1	3078	È 7			
Cluster1.IOserver2	125.0.0.1	3082	Èp 🦻			
Cluster1.AlarmS1_A	125.0.0.1	2080	Êp 🦻			
Cluster1.AlarmS2_A	125.0.0.1	3080	Êp 🦻			

After Applying changes, and expanding the deployment entry:

examplev720			
Server	IP Address	Port	File Paths Project Path: C:\ProgramData\Citect\CitectSCADA7.20\User\Example
Cluster1.ReportS1	125.0.0.1	2084	Client Control: 720/CitectSCADAWebClient_7_20_3_280.cab
Cluster1.Alarm S1	125.0.0.1	2080	
Cluster1.TrendS1	125.0.0.1	2085	
Cluster1.IOServer1_PeerPort	125.0.0.1	2078	
Cluster1.IOserver1	125.0.0.1	2082	
Cluster1.ReportS2	125.0.0.1	3084	
Cluster1.Alarm \$2	125.0.0.1	3080	
Cluster1.TrendS2	125.0.0.1	3085	
Cluster1.IOServer2_PeerPort	125.0.0.1	3078	
Cluster1.IOserver2	125.0.0.1	3082	
Cluster1.AlarmS1_AlarmProps	125.0.0.1	2080	
Cluster1.Alarm S2_AlarmProps	125.0.0.1	3080	



**Note:** For more information on the special ports, '<I/O Server Name>\_PeerPort' and '<Alarm Server Name>\_AlarmProps', please consult the <u>SCADA Help file</u>.

#### [AddressForwarding]

Cluster1.ReportServer1	=	125.0.0.1:2075
Cluster1.AlarmServer1	=	125.0.0.1:2076
Cluster1.TrendServer1	=	125.0.0.1:2077
Cluster1.IOServer1_PeerPort	=	125.0.0.1:2078
Cluster1.AlarmServer1_AlarmProps	=	125.0.0.1:2080
Cluster1.IOServer1	=	125.0.0.1:2082
Cluster1.ReportServer2	=	125.0.0.1:3075
Cluster1.AlarmServer2	=	125.0.0.1:3076
Cluster1.TrendServer2	=	125.0.0.1:3077
Cluster1.IOServer2_PeerPort	=	125.0.0.1:3078
Cluster1.AlarmServer2_AlarmProps	=	125.0.0.1:3080
Cluster1.IOServer2	=	125.0.0.1:3082

The Web method is by far the best and easiest to maintain, however, we could add these to the Web Client's INI file manually.

Since we only want these settings on the Web Client, and not on the Server's INI, we would need to make the changes to the INIs at either of the following two stages:

- On the Server, in the C:\<User>\<Project Name>\WebDeploy\Citect.ini file, *after* 'Preparing the deployment' but *before* Creating / Editing the deployment.
  - This will ensure that the modified file does not get over written during the 'Preparation' process, which copies the Server's INI to the 'WebDeploy' folder.
  - This will also ensure that once the file has been modified, it is then copied to the Web Server during the 'Deployment' stage.
  - This will need to be done every time the project is changed, and a new deployment created.

### <u>OR:</u>

• After preparing and deploying the project to the Web Server, Edit the Citect.ini file on the Web Server itself, before the Web Clients connect.

### Note regarding Citect v7.30 'Address Forwarding':

Although the address forwarding parameters are documented in the <u>7.30 help</u>, they have not been implemented in the new alarm server in 7.30. I/O data, reports, and trends work OK with address forwarding but no alarms will be displayed. This problem is currently being investigated.

See KB article <u>Q6449</u> for further details.



# <u>Checklist</u>





# 3. FAQ

• How do I set up my network so that both LAN and WAN PC's can access my CitectSCADA and CitectWeb Servers?

Please refer to the Document "Running both LAN and WAN Citect Web Clients".

#### • Where are the downloaded project files located on the Web Client?

The project files are downloaded to the location specified by the following Windows Environment Variable:

%TMP%\Citect\<Project Name>

By default, on XP, %TMP% is equal to:

Document and Local Settings \ <Current user logon> \ Local Settings \ Temp

By default, on Windows 7, %TMP% is equal to:

#### C:\Users\<Current user logon> \AppData\Local\Temp

To get a fresh copy from the server simply delete this folder including its subfolders and contents. When you restart the web client, it will automatically re-download the project.

#### • Can I connect through web client to a Citect server running in demo mode?

No, on the web client side the project pages can be viewed but the tag values will display #COMS. You will also get the following prompts, and IE will be unresponsive for several minutes, as the WebClient quits:



If you deploy whilst in demo mode this copies a copy of citect.ini file to the deployment folder on the server with the network settings disabled. If you then obtain a license dongle, you will need to re-run Citect Explorer computer setup and redeploy on the server PC.

#### • What are the software requirements?

Web Server	Web Client		
<ol> <li>Windows XP Pro SP2 or SP3, Windows Server 2003 SP1, Windows Server 2008 SP2, Vista SP2, Windows 7</li> </ol>	1. Windows XP Pro SP2 or SP3, Windows Server 2003 SP1, Windows Server 2008 SP2, Vista SP2, Windows 7		
(32 bit or 64 bit supported for all mentioned OS)	(32 bit or 64 bit supported for all mentioned OS)		
2. Microsoft Internet Information Services (IIS) (Version 5 or later)	2. Microsoft Internet Explorer (Version 6.0 or later)		
3. Microsoft Internet Explorer (Version 6.0 or later)			
4. NTFS file system			

<u>Note</u>: The target drive for the Web Server software must use an NTFS file system, otherwise you won't have full access to the required Windows security settings - Folder Properties dialog will not have a Security tab. If you are currently using FAT32 system, ensure you convert the drive to NTFS before installation of the Web software.



# IV. Troubleshooting

The following trouble shooting issues are taken from the FAQ section of the Web Client user manual. This document contains only a subset of this but also include screenshots.

### 1. Internet Explorer and Windows Security settings

If the security settings are high within Internet Explorer on the client side PC you will need to add http://<webserver>/Citect as a trusted web site. Open Internet Explorer then select the *Tools* >> *Internet Options* menu item. Select the **Security** tab.

Internet Options	×
General Security Privacy Content Connections Programs Advance	ed
Select a Web content zone to specify its security settings.	
Internet Local intranet Trusted sites Restricted sites	
Trusted sites This zone contains Web sites that you trust not to damage your computer or data.	
Security level for this zone	
<b>Custom</b> Custom settings. - To change the settings, click Custom Level. - To use the recommended settings, click Default Level.	
<u>C</u> ustom Level <u>D</u> efault Level	
OK Cancel Apply	

- Click on the **Sites...** button.
  - Enter the http://<webserver>/Citect address
  - Deselect the "Require server verification" checkbox.
  - Select the Add button.

Trusted sites	Trusted sites
You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.	You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.
Add this Web site to the zone:	Add this Web site to the zone:
http://192.168.0.253/Citect <u>A</u> dd	Add
Web sites:	<u>W</u> eb sites:
<u>R</u> emove:	http://192.168.0.253/Citect
$\hfill\square$ Require server verification (https:) for all sites in this zone	Require server verification (https:) for all sites in this zone
OK Cancel	OK Cancel

• Press Ok button.

Knowledgebase article Q3943 discusses the implication of Windows XP service pack 2 in terms of network security. Of particular importance are the firewall settings.



If your operating system includes a firewall, you must configure it to allow connections on the SCADA communication ports.

# 2. Software Protection Failure on a Web Client

One of the most common issues encountered on a web client is "Software Protection Failure". There can be more than one cause for this error on a web client machine. Here are few known issue that may cause this problem

License Availability: Web client license is available as a *Web/ Internet Control Client* and *Web/ Internet View Only client* license. A control client or a View Only client license will not work with a web client. So the first thing to check is the availability of a suitable license on your license dongle. This can be done by checking the key details via CiUsafe

License     Value       SCADA Version     7.3x       SCADA Point Count     Unlimited       Full Licenses     1       Control Clients     1       View-only Clients     1       Web/Internet Control Clients     1       Web/Internet View-only Clients     1       Networking Allowed     Yes       Connectivity/OPC Servers     10	
Connectivity/OPC Servers 10 Key ID:	Update Key
FastLinx     Yes       Site ID     21607	DCPITGEEBDH

A web client license (Control client or View Only client) must exist on the license dongle present at the IO server this client is connecting to. IO Server is responsible for providing a license to the web client, so it is not possible to to have a web client license on the client machine or the web server machine (if it is different to the IOserver machine).

**Networking issues**: Once we have confirmed that a web client license is available at the server, next step in fixing this issue is to check if we are able to connect with the IO server on the server port. To check our connectivity to the lo server port, we can use "Telnet" and open a connection to the server.



With Windows 7, Telnet client is disabled. To enable Telnet client, Go to control Panel→ Programs and Features → Turn Windows features on or off and check "Telnet Client" option as shown below

CO V 🗟 « All Control Par	nel I > Programs and Features - 47 Search Programs and Features	Q
Control Panel Home View installed updates Turn Windows features on or off	Uninstall or change a program To uninstall a program, select it from the list and then click Uninstall, Char Repair.	nge, or
Install a program from the network	Windows Features	• 🗙
	Turn Windows features on or off	0
	To turn a feature on, select its check box. To turn a feature off, clear its check bo box means that only part of the feature is turned on.	x. A filled
	<ul> <li>Simple TCPIP services (i.e. echo, daytime etc)</li> <li>Subsystem for UNIX-based Applications</li> </ul>	*
	Tablet PC Components	
	Telnet Server	=
	Windows Gadget Platform	
	Windows Process Activation Service      Windows Concele	-
	ОК	Cancel

Once done bring up the command prompt and open a Telnel session to the IO server by using the command syntax as

### Telnet <IO Server IP Address> <IO Server port>

For eg. If we are using the default server port and server is present at IP 10.176.17.78, this should look like "*Telnet* 10.176.17.78 *2082*"





If we are unable to initiate a telnet session to the IO server port an error similar to the one below is shown in the command prompt window



**Project Configuration**: On many occasions when a new project configuration is started, the Network Address field is set to Loop-Back adaptor (127.0.0.1). When this project is later on deployed on the web server and a web client is strated, it is then looking for an IO Server on server port 2082 at IP 127.0.0.1, which is the loop back address for the client machine. To fix this make sure that Network Address field reflects the IP address of the PC where the server would be running.



### Further Reading:

KB article Q4235 Software protection failure on a web client



# 3. Page display and update issues

First step in fixing this issue would be to check if Fast Runtime Display in enabled. If Fast Runtime Display is disabled the graphics builder will not create .CTF files and the web preparation tool will not create graphics files for the project pages.

Fast runtime display option can be enabled via :

Citect Graphics builder  $\rightarrow$  Tools $\rightarrow$  Options



This is further complicated if Fast Runtime Display is disabled after development of a page has begun (and the page saved). In this case a .CTF files exists but are not updated with the recent changes. The result in web clients displaying an older version of the graphics page. Here the problem is not with web client but web server not having the latest version of .CTF file.



This is the process flow of generating and propagating a .CTF file to web server and then web Client. This example is with the assumption that Fast Runtime display is enabled.

On saving a page .CTG and .CTF files are generated in the project folder. An .RDB file for the page is then generated and saved in project folder at compile time. Keep note of the date/ time stamp on .CTF and .RDB files as it moves from Project Folder to Deploy folder.

		Project Folder	line 1	
🖌 « Schneider Ele	ctric )	→ Vijeo Citect 7.20 → User → Example →	✓ Search E	ixample
Open	Burn	New folder .RDB ge	enerated at com	oile time 🚛
es	*	Name	Date modified	Туре
5		ProcessAnalyst.RDB	5/17/2012 11:11 AM	RDB File
		ProcessLine.ctF	5/17/2012 11:08 AM	CTF File
ter		ProcessLine.ctg	5/17/2012 11:08 AM	CTG File
Disk (C:)	Ξ	ProcessLine.RDB	5/17/2012 11:11 AM	RDB File
		ProcessLine_Simulation.ci	9/29/2010 8:56 PM	CI File
k	+ 4	.CTG and .CTF genera	ated on saving a	page

On running the Web Deployment Prepration tool the .CTF and .RBD files are compressed and saved as .CGZ web deploy folder

Deploy Folder					
Citect 🕨	deploy + Example	e_project 🕨 example 🕨		rch example	
Organize 🔻 🗋 Open Burn New folder					
Pictures	<ul> <li>Name</li> </ul>		Date modified	Туре	
📑 Videos	processa	nalyst.cgz	5/17/2012 11:17 AM	CGZ File	
	processli	ne.cgz	5/17/2012 11:17 AM	CGZ File	
🖳 Computer	securityp	w.cgz	5/17/2012 11:17 AM	CGZ File	
🚢 Local Disk (C:)	😑 📄 securityu	iv.cgz	5/17/2012 11:17 AM	CGZ File	
	🔲 📄 singlepa.	cgz	5/17/2012 11:17 AM	CGZ File	
📬 Network	<b>▼</b> ₹				
CGZ Conte	nts	:≕ ▼ □			
Name	Туре	Date modified			
ProcessLine.ctF	CTF File	5/17/2012 11:08 AM			
ProcessLine.RDB	RDB File	5/17/2012 11:11 AM			



When we run the web client and browse to the page ("ProcessLine" in this example), only at that time this page (as a .CTF file) is downloaded to the web client. To view contents of the Citect temporary folder, type in %tmp% in the run prompt hit Enter, browse to Citect folder and then to the project folder in there.



Local 🕨 Ten	np 🕨	Citect + Example_project + example +	← ← Search	example																
📄 Open	Shar	e with 🔻 🛛 Burn 🛛 New folder	Web Client Temp	Folder 💷 🔹																
	*	Name	Date modified	Туре																
		Polish.dbf	9/29/2010 9:56 PM	DBF File																
(0)		ProcessLine.ctF	5/17/2012 11:08 AM	CTF File																
(C:) E	II		_	_			_	_	_	_								ProcessLine.RDB	5/17/2012 11:11 AM	RDB File
		projectversion.xml	5/17/2012 11:21 AM	XML Document																
		RUSSIAN.DBF	9/29/2010 9:56 PM	DBF File																
	▼ 4																			

### **Further Reading:**

**KB article** <u>Q1762</u> Fast Runtime Display – CTF file (information on what is a .CTF file and why are these needed in the first place)

KB article <u>Q6041</u> Web Client Error "Cannot Display Page"

**KB** article **Q4621** Pages not updated on Web Client after web deployment



## 4. Slow Web Client start-up

This issue could be related to the operating system checking for certificates against the Certificate revocation list with certifying Authority. To fix this, go to *Internet Options* and select the *Advanced tab* and uncheck the "Check for publisher's certificate revocation" option as shown below

Internet Options	S		
General Security Privacy Content Connections Programs Advance	<b>1</b>		
Settings			
<ul> <li>Do not submit unknown addresses to your auto-search pro</li> <li>Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is involution of the signature is involution.</li> <li>Check for publisher's certificate revocation</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is dc</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> </ul>			
*Takes effect after you restart Internet Explorer			
Reset Internet Explorer settings Resets Internet Explorer's settings to their default condition. You should only use this if your browser is in an unusable state.			
OK Cancel Apply			

### Why is CRL check needed in the first place ?

Windows OS later than Win XP (VISTA, Windows 7 and above) requires .NET DLLs to be signed. This signing normally means that at start-up, .NET checks to see if the Certificate has been revoked. This requires Internet access or access to the domain group CRL files. After 2 minutes the system continues running if the check cannot be done. Once the check is done, the default rechecks time is every 20 days. The reason why this problem is showing up is because your network settings are not allowing Windows to access the CRL.

<u>Note:</u> This issue usually occurs on machines that do not have internet access, so it is more likely to happen on SCADA Web Client that are located on a corporate network with no Internet access (and/or access to domain group CRL files)



# VI. IIS Issues

### 1. IIS v6.0 issues

The following note applies if you are running IIS v6.x (included with Windows 2003 Server). If you start the Web Client and get the message "Starting Citect Web Client failed: Can not initialise Citect system", and then the Web Client fails it is due to a MIME configuration problem. The initialisation files are not being recognised in Windows 2003 as registered file extensions. To correct this, you must add the correct MIME extension by doing the following:

- Run the IIS manager (Control Panel >> Administrative Tools >> Internet Information Services)
- Go to Web Sites | Default Web Site | CitectSCADA | deploy | <deployed directory>

Services			_ 🗆 🗵
File Action View Help			
	2 💂 🕨 🗉 🛛		
Internet Information Services     SyD-DTEST-2G-3 (local computer     SyD-DTEST-2G-3 (local computer     SyD-DTEST-2G-3 (local computer     SyD-Edault Web Site     SyD-Ed	Name  Casample  System  CitectSCADA.xml  st	Path	Status
Opens property sheet for the Properti	es		

- Choose properties from the folder's right-click menu
- Go to HTTP Headers | Mime Map and press the File Types button

TestExample Properties	? ×
Directory Documents Directory Security HTTP Headers	Custom Errors
Content Expiration	
C Expire Immediately	
C Expire on Saturday , December 11, 2004 💌	at 12:00:00 AM
Custom HTTP Headers	
	A <u>d</u> d
	E diţ
	<u>R</u> emove
Content Rating	
Ratings help identify to your users what type of content your site provides.	Edit Rati <u>n</u> gs
МІМЕ Мар	
To configure additional MIME types the Web Service sends to browsers in the HTTP Header, click File Types.	Eile Types
OK Cancel	Apply Help



• On the File Types form press the **New Type** button.

File Types		×
Registered file types:		
		<u>N</u> ew Type
		<u>R</u> emove
		<u>E</u> dit
File type details		
Extension:		
Content Type (MIME):		
	OK	Cancel

• Add the MIME type (File extension) .\* and enter the Content type (MIME) as application/octect-stream.

File Type		×
Associated extension:	.* application/octet-stream	
	OK Cancel	

• Select Ok

	Nocice stream	<u>N</u> ew Type
		<u>R</u> emove
		-
File type details		
	×	
Extension:	·	

• Select Ok and restart your web server and client.



# 2. Security (Not applicable for IIS v7 and above)

Enter http://<server address>/Citect into the URL of an Internet Explorer screen. If you get "Page error 404 or 405" the application protection settings of IIS need to be changed. Open the IIS management console:

Services			
<u>File Action View H</u> elp			
	😫   👂 🔳 🗉		
Internet Information Services SYD-DIEST-2G-3 (local computer Web Sites Default Web Site ISHelp CitectSCADA	Name IISHelp CitectSCADA help.gif iisstart.asp localstart.asp mmc.gif pagerror.gif print.gif Thumbs.db warning.gif web.gif winxp.gif	Path c:\windows\help\iishelp C:\Program Files\Citect\CitectSCAD	Status
T	•		F

Right select the CitectSCADA virtual directory and select Properties. In the CitectSCADA virtual directory properties in screen below set the Application Protection to **Low (IIS Process)**.

itectSCADA Properties	<u>? ×</u>
Virtual Directory Documents Directory Security HTTP Headers	Custom Errors
When connecting to this resource, the content should come from:	:
A directory located on this computer	
C A share located on another computer	
O A redirection to a <u>U</u> RL	
Logal Path: C:\Program Files\Citect\CitectSCADAv6\	Browse
□ Script source access     ▼ Log visits       ▼ Bead     ▼ Index this resource       □ Write	
Directory browsing	
Application Settings	
Application name: CitectSCADA	R <u>e</u> move
Starting point: <default\citectscada< td=""><td></td></default\citectscada<>	
Execute Permissions: Scripts only	Configuration
Application Protection: Low (IIS Process)	Unjoad
OK Cancel <u>App</u> l	y Help



### 3. ASP.NET

*The following is a Windows 2003 Server related issue.* The Web Client deployment page may display incorrectly and the icons for Start Display Client, Delete Deployment and Edit Deployment are also missing. There are two problems that could be occurring here:

- On Windows 2003 Server, the default setting is to have all web locations except localhost as an untrusted site.
  - a. Update the Trusted Sites settings as detailed in Chapter 9
- Enable ASP for IIS6 on Windows 2003 Server. Follow these steps:
  - a. Choose Control Panel >> Add Remove Programs >> Components
  - b. In the Windows Components Wizard dialog box, select Application Server and select **Details**.

To add or remove a compo part of the component will b Details.	nent, click the checkbox. A shaded box means that only e installed. To see what's included in a component, click	
Components:	Application Server	
E-mail Services     As Fax Services     Description: Includes ASF     Application S	Subgomponents or Application Server:	0.0 ME 0.0 ME 0.0 MI
	Enable network DTC access      Main and the services (IIS)	0.0 ME 18.0 MF
Total disk space required: Space available on disk:	Message Queuing	6.5 ME

- Make sure that ASP.NET is selected.
- Also, open Control Panel >> Administrator Services >> Internet Information Services (IIS) Manager
- On the local machine traverse to **Web Sites | Web Service Extensions** and make sure that *All Unknown ISAPI Extensions, Active Server Pages* and *ASP.NET v1.1.4322* items have the status of Allowed.

Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow	v <u>H</u> elp		_ 8 ×
⇔ →   🖻 💽   🖗 🛱	2 里 ▶ ■ Ⅱ		
Internet Information Services	📁 Web Service Extens	sions	
🗄 📁 Application Pools		A Web Service Extension	Status
E 🥥 Web Sites		All Unknown ISAPI Extensions	Allowed
🖃 👹 Default Web Site (S	Allow	All Unknown CGI Extensions	Prohibite
	Fleshibit	Active Server Pages	Allowed
	Promot	ASP.NET v1.1.4322>	Allowed
msadc	Properties	Internet Data Connector	Prohibite
F Plant2NET	8 <b>.</b>	Server Side Includes	Prohibite
viewer	Tasks	WebDAV	Prohibite
Web Service Extension	<ul> <li>Add a new Web service e</li> <li>Allow all Web service extra specific application</li> <li>Prohibit all Web service e:</li> <li>Open Help</li> </ul>	xtension ensions for a xtensions	
		•	



# 4. CAB File Download and Installation

After configuring the Citect web server as per Web Client quick start guide, during project deployment, errors are experienced downloading cab file. The address of the webserver is added as a trusted site however the problem still persists. The Server and Clients both use Internet Explorer 6 and all Internet Explorer security levels have been set to the lowest level. Windows firewall is also disabled. What can be the problem?

### Solution:

Usually when this occurs, Citect is looking for Microsoft Installer that has been corrupted due to previous Windows update. In order to remedy this problem you can get the latest update from Microsoft.

The problem of corrupted Microsoft Installer can be verified further by using Citect version 7.20. In Citect v7.20, you can install this CAB file manually to the client machine by double clicking the CAB file. If when installing the CAB file, Windows Installer error 1723 appears, you would then need to install the latest Microsoft Installer (iiscript.msi).

This installer can be downloaded from the Microsoft website or can be obtained from your IT staff.



# VII. References

# 1. Knowledge base articles:

Q6480 Webclient files not copied over correctly from IIS web server

Q6473 Internet Explorer 10 and SCADA webclient

Q6478 Debugging WebClient - IIS Communication

Q6358 Webclient not functioining properly (CAB file) on IE 64-bit

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

Q6041 Webclient error "Cannot Display Page"

<u>Q5816</u> How to configure IIS 7 on Windows Vista, Windows 7 and Windows Server 2008 for Citect Web Server 7.10 installation

<u>Q5957</u> I am being logged in automatically to the web server without being prompted for a username or password

Q4946 Web Client across LAN / WAN

Q4941 V7.xx Citect Display Client / Web Client through Router - No more DNS Section, have to use AddressForwarding

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

Q4467 Installing / Running Web Client without admin rights

Q4621 Pages not updated on web client after web deployment

Q4281 Web client Full-screen and as a shell

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

Q5649 Error when creating a deployment on a remote Web server

Q3943 Implications for Citect and Microsoft Windows XP Service Pack 2

Q3010 Setting up a combined FTP Server/Proxi Server for a WAN

Q3912 How can I use a Proxy I/O server in CitectHMI/SCADA?

### 2. User manuals:

CitectSCADA Web Client User Guide CitectSCADA User Guide



### Disclaimer

By using the information contained within this document, you agree to the following:

#### **Disclaimer of All Warranties**

SCHNEIDER ELECTRIC (AUSTRALIA) PTY LTD DISCLAIMS ANY AND ALL WARRANTIES WITH RESPECT TO SCHNEIDER ELECTRIC (AUSTRALIA) PTY LTD PRODUCTS AND THE RELATED DOCUMENTATION, WHETHER EXPRESS OR IMPLIED, INCLUDING SPECIFICALLY THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A GENERAL OR PARTICULAR PURPOSE.

CITECTSCADA/ VIJEO CITECT AND THE RELATED DOCUMENTATION ARE PROVIDED "AS IS," AND YOUR COMPANY UNDERSTANDS THAT IT ASSUMES ALL RISKS OF THEIR USE, QUALITY, AND PERFORMANCE.

#### **Disclaimer of Liability**

YOUR COMPANY AGREES AND ACKNOWLEDGES THAT SCHNEIDER ELECTRIC (AUSTRALIA) PTY LTD SHALL HAVE NO LIABILITY WHATSOEVER TO YOUR COMPANY FOR ANY PROBLEMS IN OR CAUSED BY SCHNEIDER ELECTRIC (AUSTRALIA) PTY LTD PRODUCTS OR THE RELATED DOCUMENTATION, WHETHER DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL (INCLUDING LOSS OF PROFITS).



#### Schneider Electric (Australia) Pty Ltd

78 Waterloo Road Macquarie Park, NSW 2113 Phone: + 61 (2) 9125 8500 Fax: + 61 (2) 9888 2941 http://www.schneider-electric.com

