

PowerSCADA Anywhere

Server Installation and Configuration Guide

Legal Information

DISCLAIMER

Schneider Electric makes no representations or warranties with respect to this manual and, to the maximum extent permitted by law, expressly limits its liability for breach of any warranty that may be implied to the replacement of this manual with another. Further, Schneider Electric reserves the right to revise this publication at any time without incurring an obligation to notify any person of the revision.

Schneider Electric gives no express warranties, guarantees or conditions and to the extent permitted under applicable laws, Schneider Electric disclaims all implied warranties, including any implied warranties of merchantability, fitness for a particular purpose or non-infringement of third parties' intellectual property rights.

Schneider Electric shall not be liable for any direct, indirect or consequential damages or costs of any type arising out of any action taken by you or others related to the Example Projects.

COPYRIGHT

© Copyright 2015 Schneider Electric All rights reserved.

TRADEMARKS

Schneider Electric has made every effort to supply trademark information about company names, products and services mentioned in this manual.

Citect, CitectHMI, Vijeo Citect, Vijeo Citect Lite, PowerSCADA Expert and CitectSCADA are either registered trademarks or trademarks of Schneider Electric.

Pelco, Spectra, Sarix, Endura, are registered trademarks of Pelco, Inc.

IBM, IBM PC and IBM PC AT are registered trademarks of International Business Machines Corporation.

MS-DOS, Windows, Windows NT, Microsoft, and Excel are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

DigiBoard, PC/Xi and Com/Xi are trademarks of Digi International Inc.

Novell, Netware and Netware Lite are either registered trademarks or trademarks of Novell, Inc. in the United States and other countries.

dBASE is a trademark of dataBased Intelligence, Inc.

All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

GENERAL INFORMATION

Some product names used in this manual are used for identification purposes only and may be trademarks of their respective companies.

09/01/2015 edition for Schneider Electric Citect Anywhere Version 1.0.0.

Manual Revision Version 1.0.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. © 2015 Schneider Electric. All Rights Reserved.

Validity Note

The present documentation is intended for qualified technical personnel responsible for the implementation, operation and maintenance of the products described. It contains information necessary for the proper use of the products. However, those who wish to make a more "advanced" use of our products may find it necessary to consult our nearest distributor in order to obtain additional information.

The contents of this documentation are not contractual and in no way constitute an extension to, or restriction of, the contractual warranty clauses.

Contact Schneider Electric today at www.schneider-electric.com

Contents

Contents	4
Safety Information	8
Chapter 1: Welcome	10
Chapter 2: Overview	12
Architecture	12
RDP Compression and Acceleration	14
Licensing	14
Chapter 3: Before You Install	16
Prerequisites	16
Configuring Firewalls	17
Binding Service to All Network Interfaces	20
Verifying the Current Network Interface Configuration	20
Chapter 4: Installation	22

Installing PowerSCADA Anywhere Server	22
Repairing an Installation	28
Uninstalling PowerSCADA Anywhere	30
Citect Anywhere Web Component	34
Installing the Web Component	34
Secure Connections	35
Secured WebSocket Communication to Remote Desktops	35
Secured WebSocket connections via Citect Anywhere Secure Gateway	36
Benefit of Using a Trusted Certificate	36
 Chapter 5: Configuring Citect Anywhere Server	38
Configuring Remote Desktop Services	38
Configuring User Access	39
Activating a Vijeo Citect License	42
Configuring Flexera License Server	43
Configuring the License Server Manager Port	44
The Configuration Console	45
General Tab	46
Performance Tab	47
Communication Tab	48

Acceleration Tab	48
Security	49
Logging Tab	50
Advanced	50
Chapter 6: Configuring Mobile Devices	52
Supported Browsers	52
Browsers Tested with Citect Anywhere	52
Logging On to Citect Anywhere	53
Configuring Advanced Settings	54
Changing the Display Language	55
Automatic Display Resize	56
Using Gestures on Client Portable Devices	57
Google Chromebooks	57
Chrome Keyboard	57
Tablet and Smartphones	58
HTTPS Mode	59
Chapter 7: Advanced Configuration	62
Static Configuration of Config.js	62
Settings Table	63

Defining Configuration Groups	66
Settings Precedence	67
Passing Credentials using Form POST	68
Embedding Citect Anywhere in an iframe	68
 Chapter 8: SSL VPN Configuration	70
Web Proxy with 7.4	70
Web Proxy with Older Juniper Versions	71
Single Sign On(SSO) Using Cookies	71
Network Connect	72
JSAM and WSAM	72
Auto-starting JSAM or WSAM upon Login	73

Safety Information

Read these instructions carefully, and familiarize yourself with PowerSCADA Anywhere before trying to install, operate, or maintain your system. The following special messages may appear throughout this documentation or on the PowerSCADA Anywhere application to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.



The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.



DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in death or serious injury**.



WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in death or serious injury**.



CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in minor or moderate injury**.

CAUTION
CAUTION , used without the safety alert symbol, indicates a potentially hazardous situation which, if not avoided, can result in equipment damage .

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and the installation, and has received safety training to recognize and avoid the hazards involved.

Chapter 1: Welcome

NOTE: The Secure Gateway product is not supported in PowerSCADA Expert 8.1.

Use Schneider Electric PowerSCADA Anywhere(also referred to as Citect Anywhere) to access Vijeo Citect clients hosted on Terminal Servers with HTML5 compatible web browsers. Follow the instructions in this guide to begin using PowerSCADA Anywhere.

This guide assumes knowledge of the following:

- Vijeo Citect
- Enabling and configuring RDP on Windows operating systems
- Firewall configuration
- Web server administration

Important terminology used in this guide includes the following:

- **RDP** - Remote Desktop Protocol. A remote desktop protocol developed by Microsoft. RDP is a standard component of Microsoft Windows.
- **RDP Host** - a Windows system that can be remotely accessed using Microsoft RDP, such as a Terminal Server (RDS Session Host) with remote access enabled.
- **HTML5** - a new update to the HTML specification. Extends HTML with new features and functionality for communication, display, etc.
- **WebSocket** - a bi-directional, full-duplex communication mechanism introduced in the HTML5 specification.

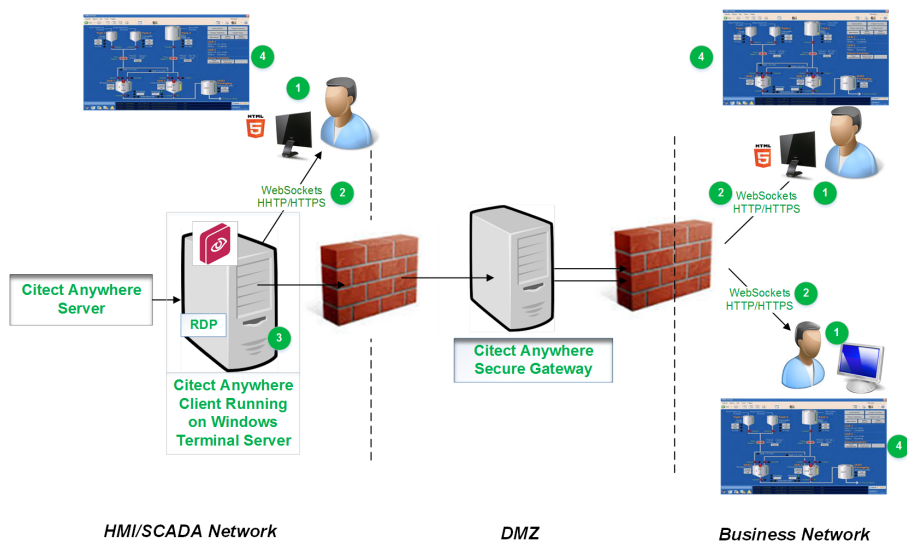
- **SSL** - Secure Sockets Layer. A cryptographic protocol that provides communications security over the Internet.

Chapter 2: Overview

PowerSCADA Anywhere provides remote access to Vijeo Citect clients using any HTML5 web browser running on a desktop computer or a mobile device. Any browser that supports HTML5 canvas can be used as the client to view Vijeo Citect. HTML5 WebSockets are typically required for PowerSCADA Anywhere.

Architecture

The following diagram illustrates how the different components of PowerSCADA Anywhere work together:



REFERENCE	DESCRIPTION
1	Initiate a connection from the client device by directing the browser to the PowerSCADA Anywhere start page hosted on the web server (<i>https://<computer name>:8080/</i>). The <i>Start.html</i> page is displayed in the web browser using HTTP/HTTPS.

REFERENCE	DESCRIPTION
2	The browser opens a WebSocket connection to the PowerSCADA Anywhere Server, which is running on the RDP host itself. If the optional PowerSCADA Anywhere Secure Gateway is installed, a PowerSCADA Anywhere browser session will connect through it.
3	The PowerSCADA Anywhere Server translates the WebSocket communication to and from RDP, thus establishing a connection from the browser to the RDP host itself.
4	The browser then displays the content of the remote client.

Note: If the optional PowerSCADA Anywhere Secure Gateway is installed, a PowerSCADA Anywhere Server browser session will connect through it.

Important: Using the Secure Gateway to connect to your SCADA system from an external network may expose your SCADA system to unauthorized access. It is recommended that you use the Secure Gateway in conjunction with other security measures to improve the overall security of your system.

This is the recommended architecture to remotely access clients running on an HMI/SCADA network from an untrusted business network.

- The PowerSCADA Anywhere Server (WebSocket Server) is installed on a separate server from either PowerSCADA Anywhere or the Advanced Reports server. This installation requires a Citect Floating License to be activated on the same computer. The Citect Anywhere server must be installed on one of the following operating systems:
Windows Server 2006 R2
Windows Server 2012
- The PowerSCADA Anywhere Secure Gateway is an optional server installed separately on a computer in a DMZ to access PowerSCADA Expert protected by a firewall.

RDP Compression and Acceleration

PowerSCADA Anywhere provides RDP compression and acceleration technology to improve remote client performance over a network and Internet. There are three main features of RDP technology:

- Image compression

Images are compressed before they are transmitted to a browser for rendering. A higher compression value results in lower image quality, less impact to the network and faster update.

- Packet shaping

Packet shaping is a computer network traffic management technique that delays some or all datagrams to reduce latency and increase usable network bandwidth.

- Whole frame rendering

Whole frame rendering updates the display as a whole rather than in blocks, as performed by standard RDP. The benefit of whole frame rendering is especially noticeable when watching video over slow network connections. Coupled with the other optimization features, whole frame rendering results in a smoother video display on a browser.

Licensing

PowerSCADA Anywhere is licensed for use with Vijeo Citect versions v7.20 (SP5a), v7.40 (SP1 and SP2) and v7.50 only.

In order to run PowerSCADA Anywhere, licenses are required for the following:

1. Microsoft Remote Desktop Service (RDS): Every remote desktop session opened with a browser using PowerSCADA Anywhere consumes an RDS license. Confirm that the required number of RDS licenses is available to users.
2. Vijeo Citect License(s) - Availability of a Vijeo Citect license is verified every time a user attempts to connect to a Vijeo Citect Client using PowerSCADA Anywhere.

3. PowerSCADA Anywhere License(s) - PowerSCADA Anywhere licenses are available as a bundle of 5, with one license being used per active connection. When connection is established with a Vijeo Citect client, a license is used up. The license becomes available for use again when the session is terminated.

The availability of a license is checked at 5-minute intervals. If the license check does not detect a license three times in a row, an error message is displayed and the Vijeo Citect client is shut down.

Chapter 3: Before You Install

Prior to installing PowerSCADA Anywhere, confirm that:

- The computer that will host the PowerSCADA Anywhere Server is running an operating system supported by Vijeo Citect.
- The PowerSCADA Anywhere Server and the Secure Gateway need to be installed on separate computers.
- Remote Desktop Services is configured on the host computer.

Important: PowerSCADA Anywhere leverages RDP and translates RDP to WebSockets. RDP access must be enabled on the computer hosting PowerSCADA Anywhere. For more information, see the [Remote Desktop Services with Vijeo Citect 2015](#) whitepaper. Note that you need to register with the site before you can access the document.

- The host computer's firewall is configured to permit inbound and outbound network traffic on port 8080.

Prerequisites

The PowerSCADA Anywhere Server has been tested with Microsoft Windows Server versions 2008 and 2012. PowerSCADA Anywhere Server must be installed on the RDP server where Vijeo Citect resides. The PowerSCADA Anywhere Server is highly efficient, and will have minimum impact on the RDP host's performance and scalability.

Important: Microsoft Windows Server should not be configured as a Domain Controller.

The PowerSCADA Anywhere Server itself includes a built-in web server. This includes a copy of the PowerSCADA Anywhere web components.

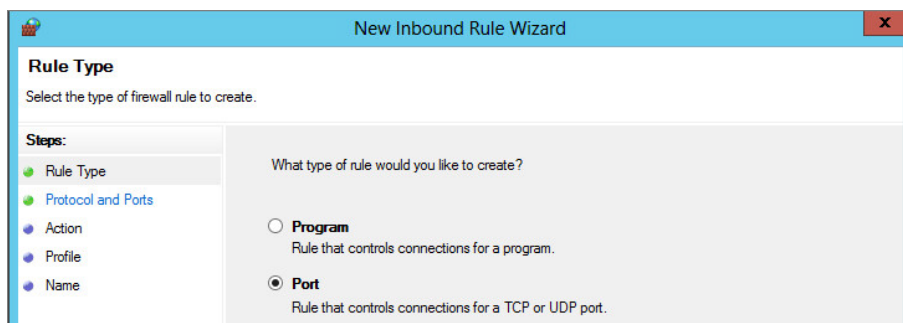
Configuring Firewalls

By default, a client (browser) connects to a PowerSCADA Anywhere Server using port 8080 for both encrypted and unencrypted WebSocket communication. This port number can be changed using the PowerSCADA Anywhere Server Configuration utility.

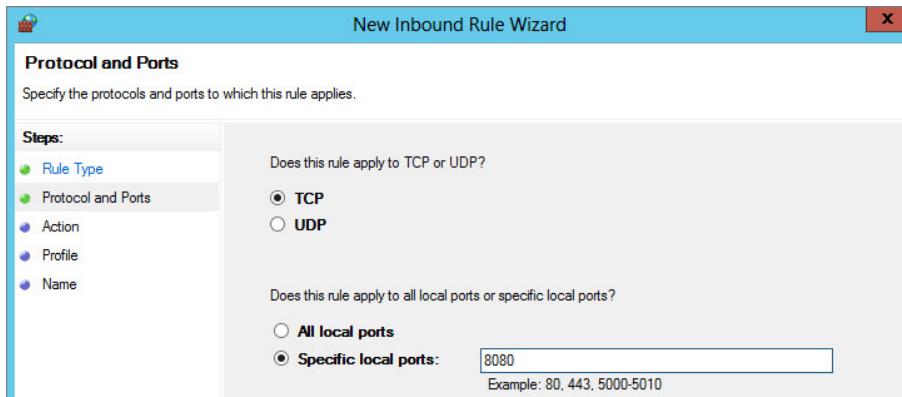
To enable direct connection from the client to the PowerSCADA Anywhere Server (without using the Secure Gateway), the server must be directly accessible from the client using port 8080.

If the Windows firewall is enabled on the same computer where the PowerSCADA Anywhere Server is installed, configure it to enable the PowerSCADA Anywhere client connection.

1. Open the **Windows Control Panel** and then **Windows Firewall**
2. Select **Advanced Settings** and select **Inbound Rules**.
3. Click **New Rule**.

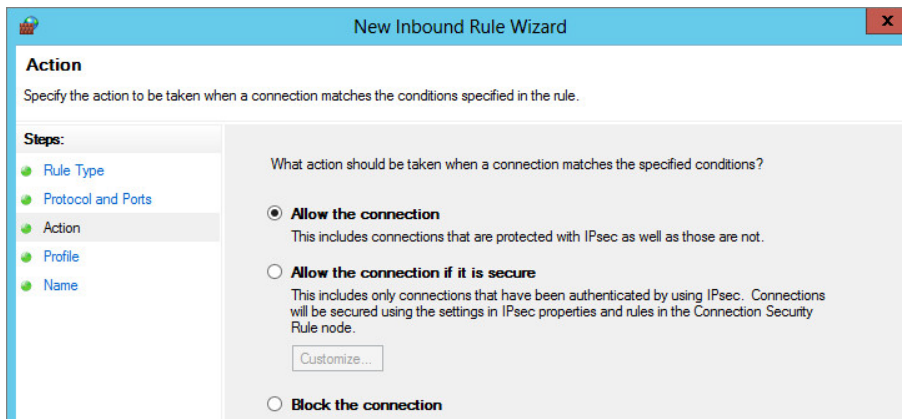


4. Select **Port** and click **Next**.
5. Enter the specific port: 8080.



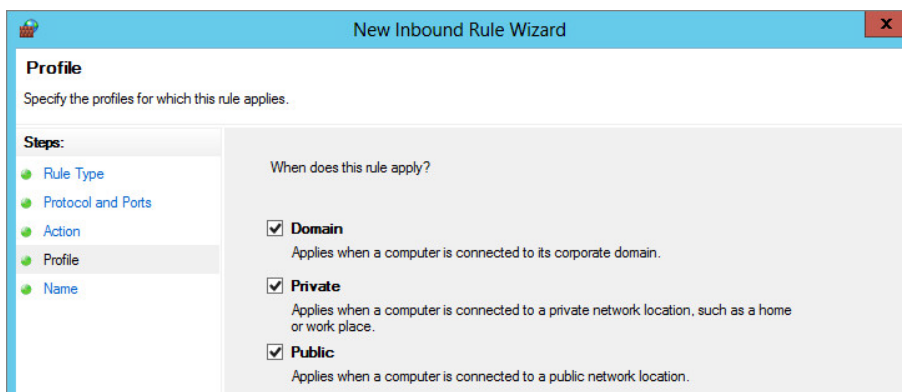
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'. The second question is 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports' (selected). Below the second question is a text input field containing '8080' and an example text 'Example: 80, 443, 5000-5010'.

6. Click **Next** and select **Allow the connection**.



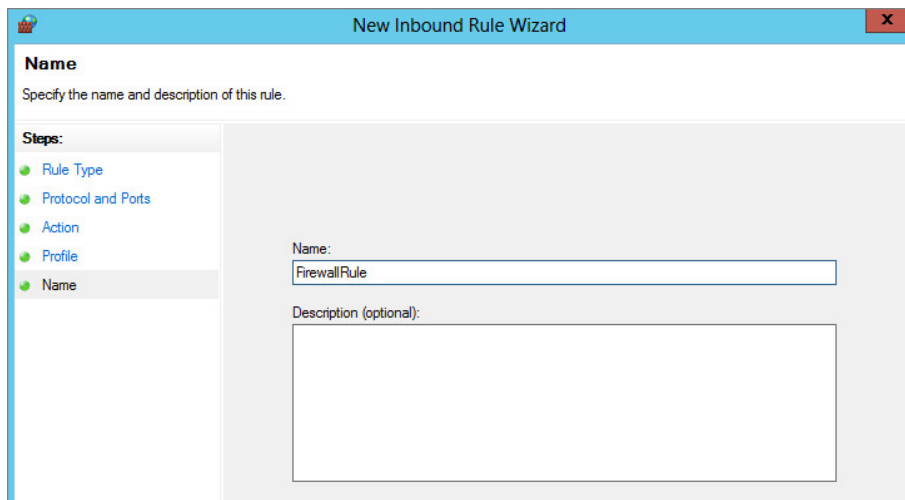
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button. The 'Block the connection' option is currently unselected.

7. Click **Next** and select to apply the rule on the **Domain**, **Private** and **Public** networks.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile (selected), and Name. The main area contains the question 'When does this rule apply?'. There are three checked radio button options: 'Domain', 'Private', and 'Public'. The 'Domain' option has a description: 'Applies when a computer is connected to its corporate domain.' The 'Private' option has a description: 'Applies when a computer is connected to a private network location, such as a home or work place.' The 'Public' option has a description: 'Applies when a computer is connected to a public network location.'

8. Click **Next**, assign a name for the rule.



The image shows a 'New Inbound Rule Wizard' dialog box. The title bar is blue with a small icon on the left and a close button (X) on the right. The main area is white. At the top, it says 'Name' and 'Specify the name and description of this rule.' Below this, there is a 'Steps:' section on the left with a list of steps: 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Name' step is currently selected and highlighted. To the right of the steps, there is a large text input area. The 'Name:' label is above a text box containing 'FirewallRule'. Below that, the 'Description (optional):' label is above a larger, empty text box.

New Inbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:
FirewallRule

Description (optional):

9. Click **Finish**.

Binding Service to All Network Interfaces

In a virtual network environment, PowerSCADA Anywhere Server should use all virtual network interfaces, rather than just one virtual Network Interface Controller (NIC). Network interfaces used by PowerSCADA Anywhere Server must be accessible to the target group of users.

Verifying the Current Network Interface Configuration

As a quick test of your current network configuration, run PowerShell 3.0 and enter the following command:

```
RESOLVE-DNSNAME dnsname
```

Example:

```
PS C:\Users\user1> resolve-dnsname itaatest
```

Note: PowerShell 3.0 is included with Microsoft Windows Server 2012. You will need to install it if you are running earlier versions of Windows Server.

Chapter 4: Installation

PowerSCADA Anywhere Server is the server-side service that translates RDP into WebSocket communication. The PowerSCADA Anywhere Server is installed on the RDP host.

The PowerSCADA Anywhere client interface, running in the browser, connects to this service using WebSockets directly or through the Secure Gateway.

For more information about the Secure Gateway, refer to the PowerSCADA Anywhere Secure Gateway Installation and Configuration Guide.

Installing PowerSCADA Anywhere Server

The PowerSCADA Anywhere installer allows you to install the PowerSCADA Anywhere Server and the Secure Gateway. Note that these two components **cannot** be installed on the same computer.

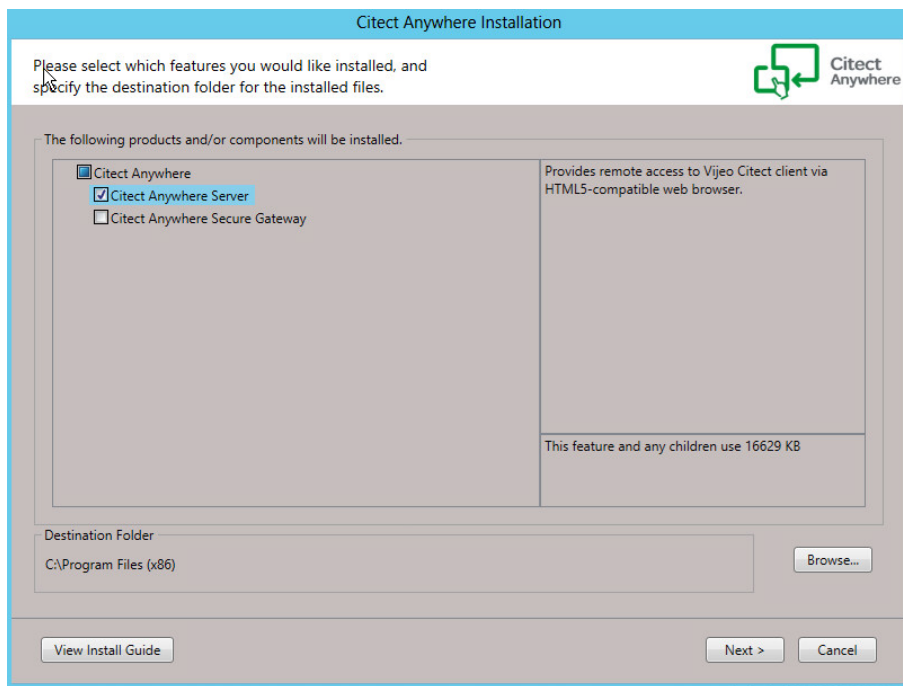
To install PowerSCADA Anywhere Server:

1. Insert the CD into your CD-ROM drive, and run the *Setup.exe* file. The PowerSCADA Anywhere splash screen appears.

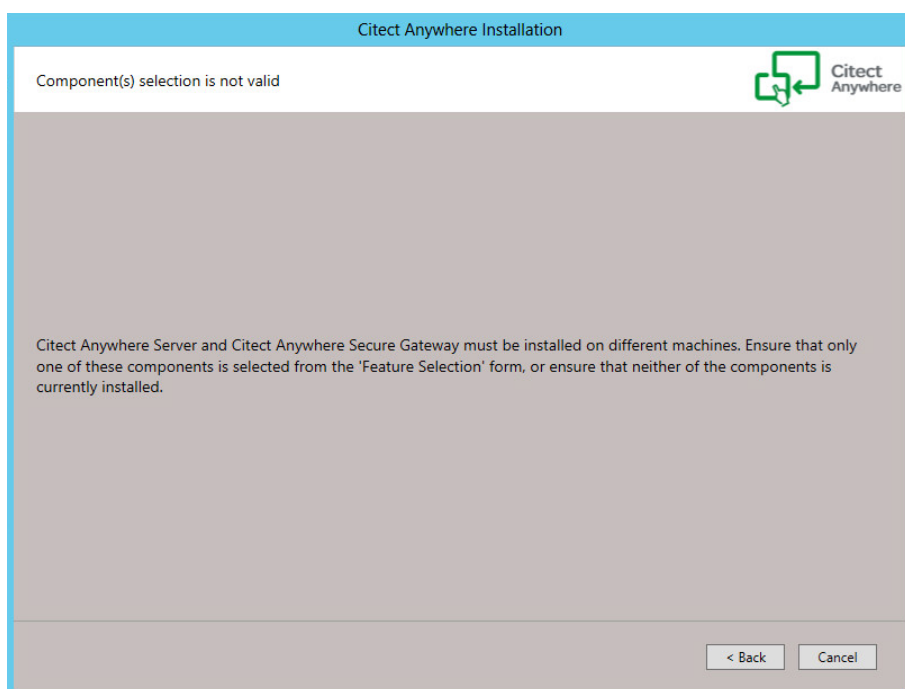


The message *"Please wait for configuration to complete"* appears as the installer prepares to start the installation.

2. Select the **PowerSCADA Anywhere Server** option.

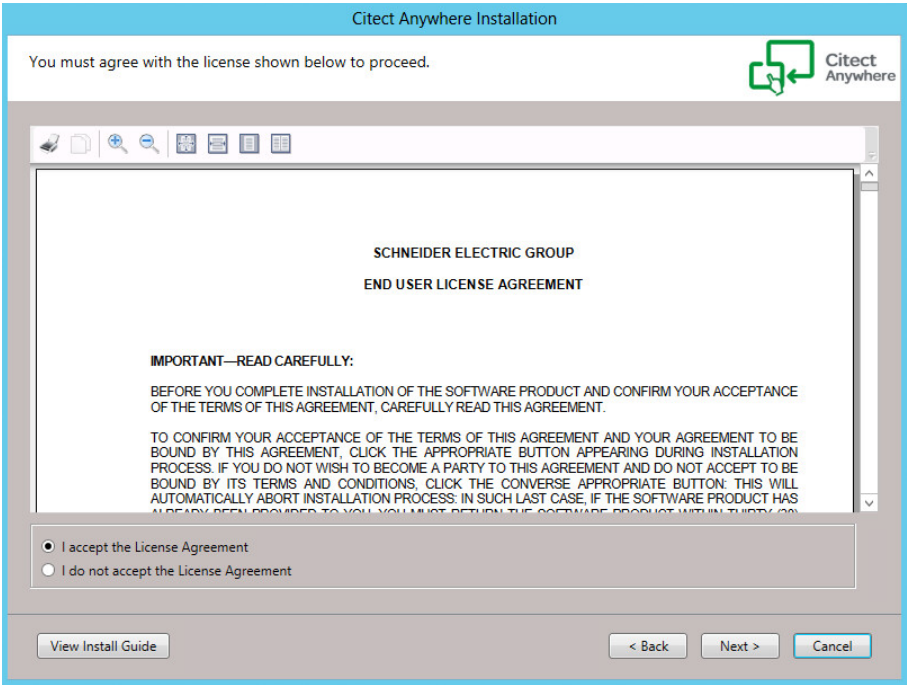


If you select both options, the installer will prevent you from proceeding with the installation. The following message appears.



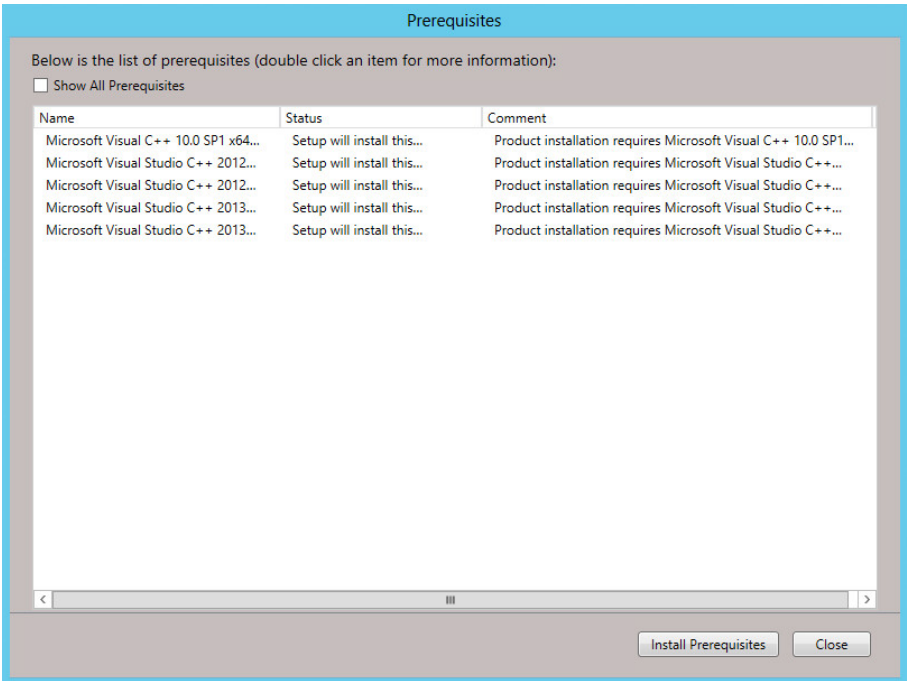
Click **Back** to return to the Component Selection screen.

3. Click **Next**. The License Agreement screen appears. Read the license agreement carefully, and select the **I accept the License Agreement** option to continue. Selecting **I do not accept the License Agreement** will prevent you from proceeding with the installation.

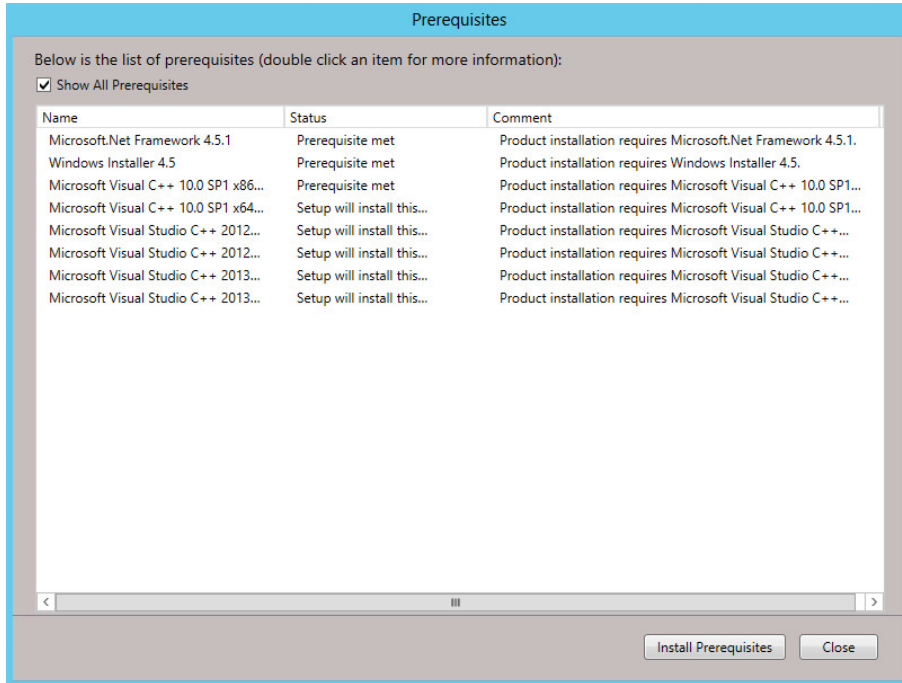


4. Click **Next**. The Installation Prerequisites screen appears.

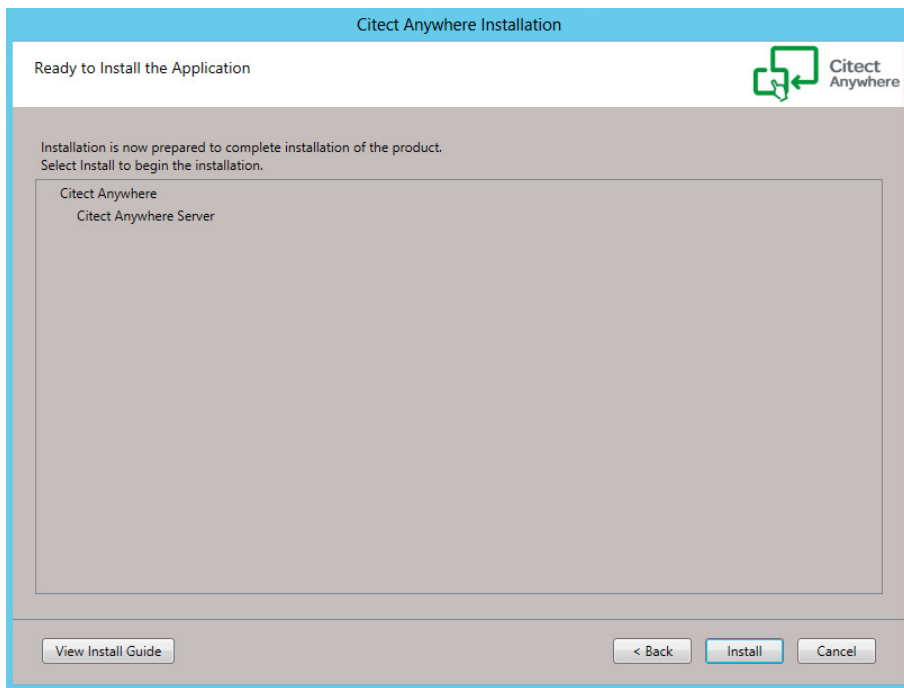
The installation program checks whether the installation prerequisites are met, and shows the missing prerequisites.



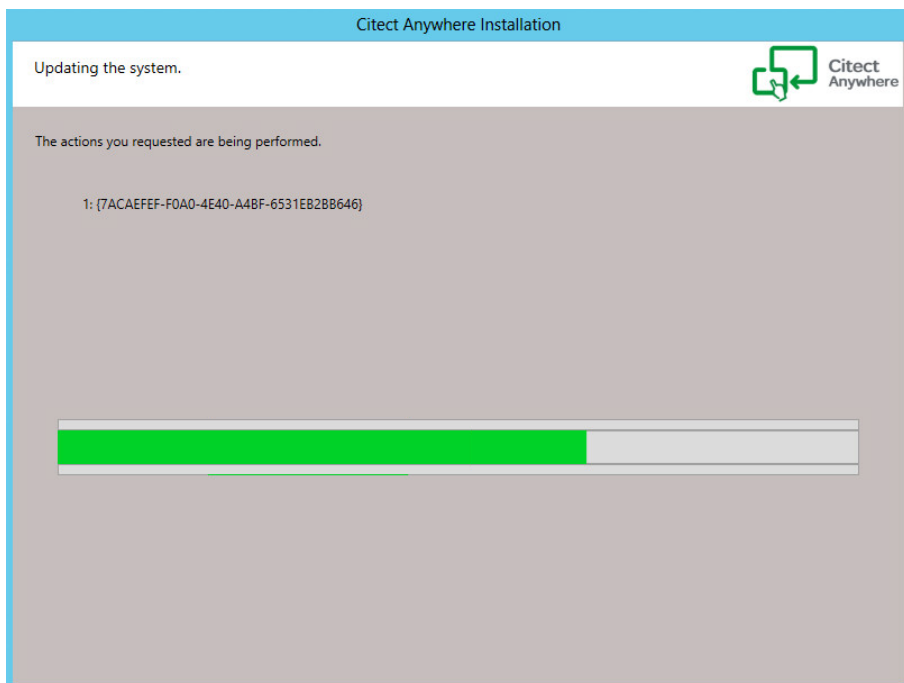
5. To view a list of all prerequisites, select the **Show All Prerequisites** option.



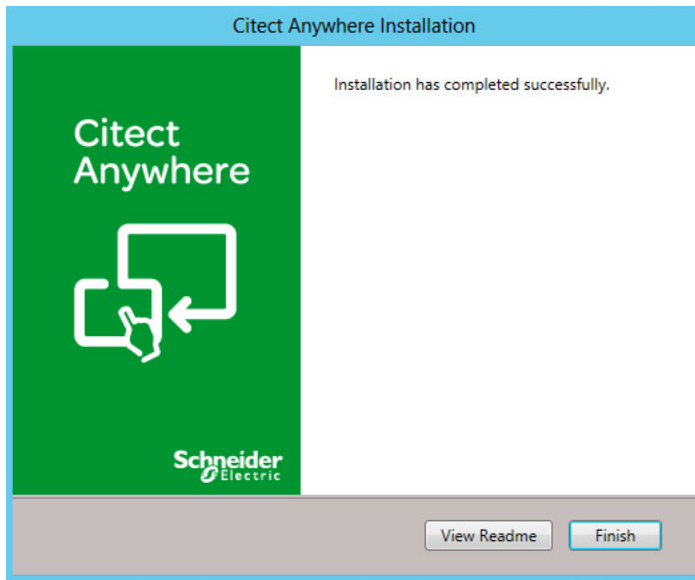
6. Click **Install Prerequisites** to install the missing prerequisites.
7. Click **Next**. The list of components selected for installation is displayed.



8. Click **Install**. The progress bar appears.



9. After the installation is complete, the Installation Complete dialog box appears. Click **View Readme** to open the *Readme.html* file, which contains details about PowerSCADA Anywhere features, or click **Finish**.



The PowerSCADA Anywhere Server service is configured to run automatically on system startup. If the service is stopped or is unable to listen on its default port (8080), clients will not be able to connect to that host. Configure firewalls and proxies between the end-point devices and the server-side component to allow communication using port 8080, or use the PowerSCADA Anywhere Secure Gateway.

Note: PowerSCADA Anywhere Server cannot be installed on systems where the host name contains non-English characters.

PowerSCADA Anywhere Server and PowerSCADA Anywhere Secure Gateway cannot be installed on the same machine.

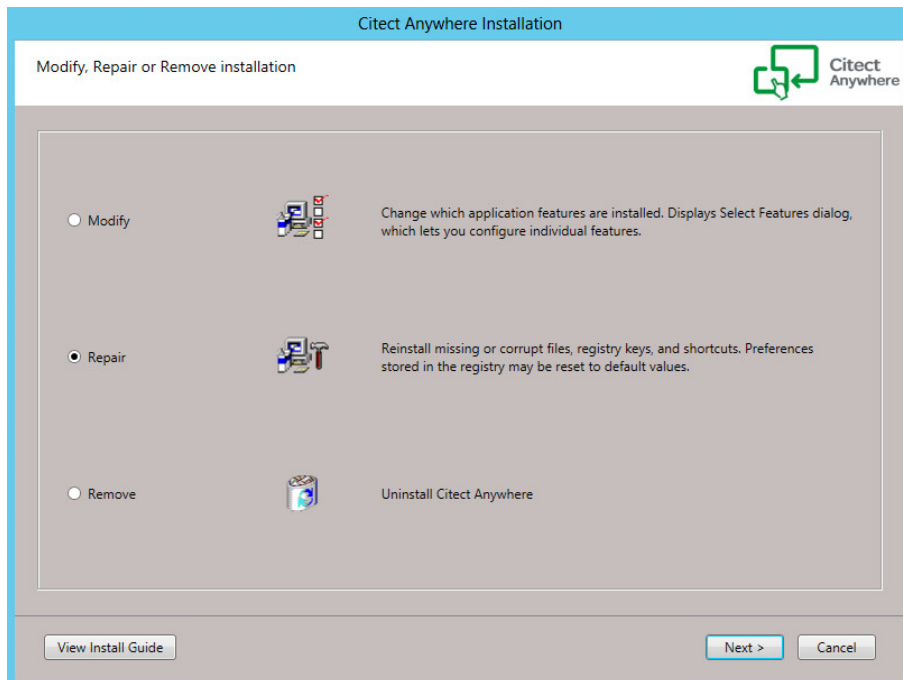
Repairing an Installation

You can use the installation program to repair corrupt files of installed PowerSCADA Anywhere components.

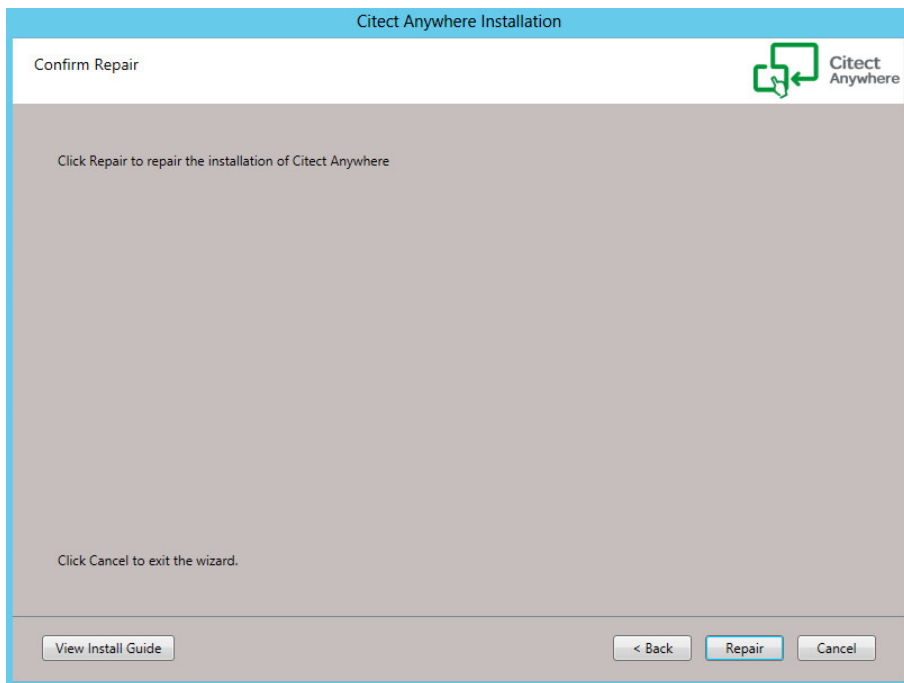
Note: You need to have the installation CD inserted in the CD-ROM drive before you can repair an installation, or have access to other media where the installation files are located.

To repair an installation:

1. From the **Windows Start** menu, select **Control Panel > Programs > Programs and Features > Uninstall a Program**. All programs installed on your computer are listed.
2. Select the PowerSCADA Anywhere component you wish to repair. Click **Uninstall/Change**. The installer program appears.
3. Select **Repair**, and then click **Next**.



4. Click **Repair**.



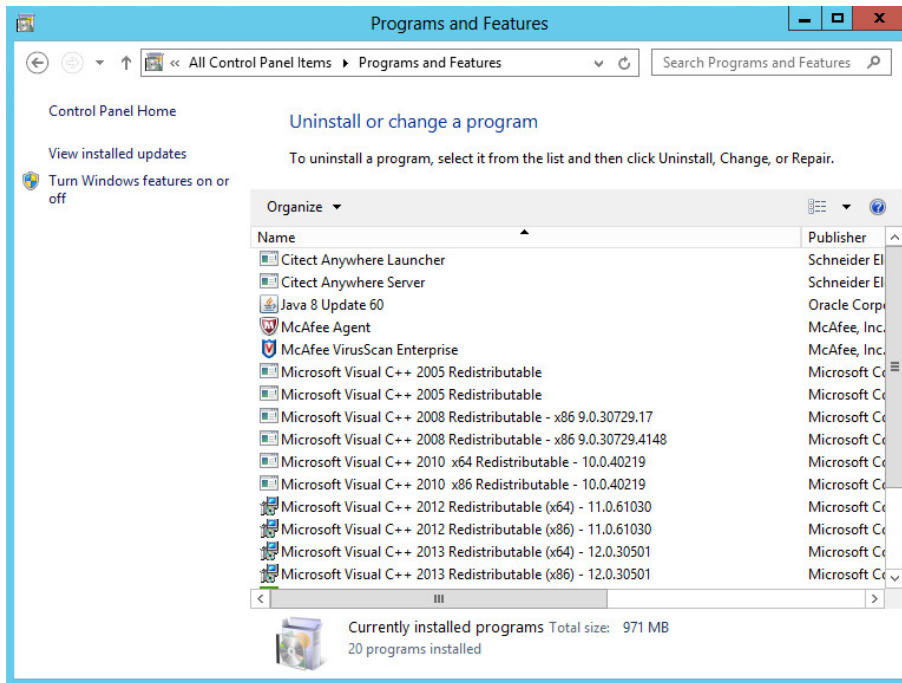
5. Installed PowerSCADA Anywhere components are repaired, and a message confirming successful repair appears.
6. Click **Finish** to close the dialog box.

Uninstalling PowerSCADA Anywhere

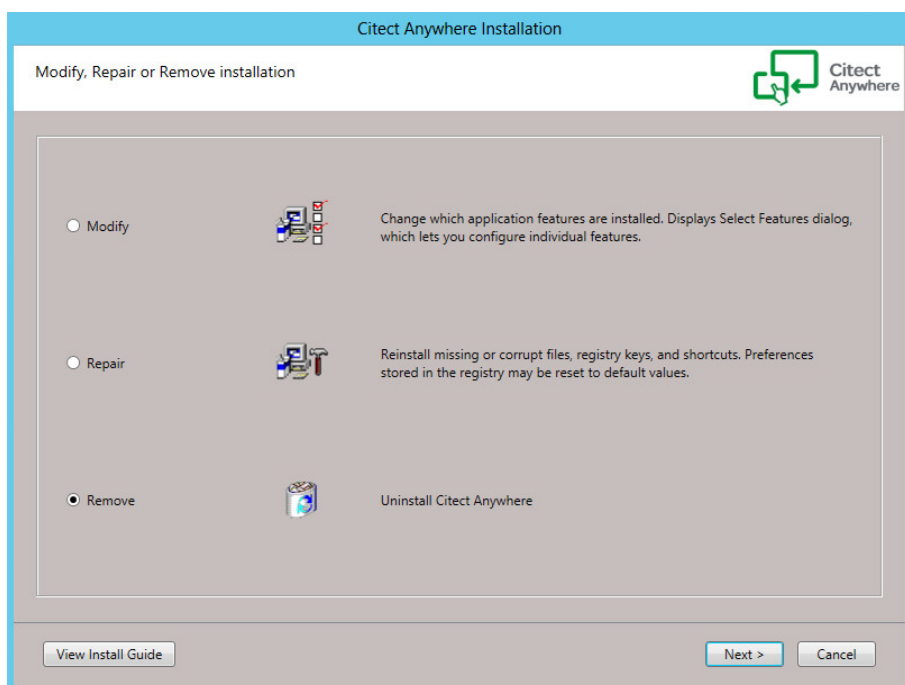
You may wish to remove PowerSCADA Anywhere components. This section provides instructions for uninstalling PowerSCADA Anywhere components.

To uninstall PowerSCADA Anywhere components:

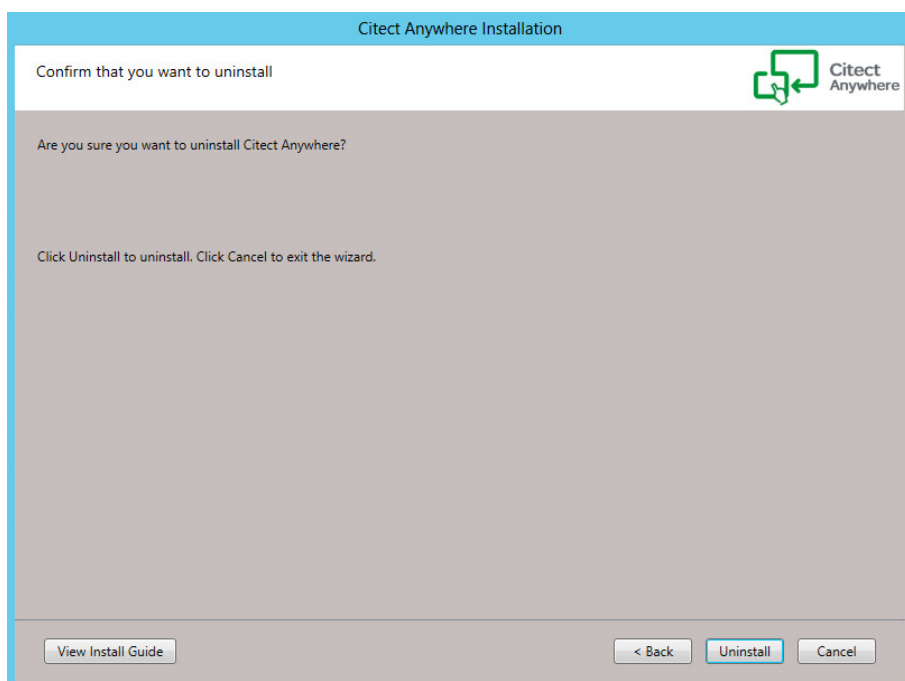
1. From the Windows Start menu, select **Control Panel > Programs > Programs and Features > Uninstall a Program**. All programs installed on your computer are listed.
2. Locate the PowerSCADA Anywhere Server component to uninstall, and click to select the component.



3. Click **Uninstall/Change**. The Modify, Repair or Remove Installation dialog box appears.
4. Select **Remove**.



5. Click **Uninstall** and then click **Next**. A screen confirming the uninstallation appears.



Note: This will remove only the selected component. To remove all components installed with the PowerSCADA Anywhere Secure Gateway (the PowerSCADA Anywhere Secure Gateway Client Components), run *setup.exe* again and perform a complete uninstall. Some files may still exist in the installation folders after the uninstallation.

Citect Anywhere Web Component

The web component contains the resources that are used by the web browser to display an interface for users to use to connect to their remote application or desktop. These resources include HTML pages, JavaScript and CSS files and graphic images. Review the chapter on [Advanced Configuration](#) to modify the appearance and behavior of the web component interface.

Installing the Web Component

The Citect Anywhere web component is automatically installed along with the Citect Anywhere Server. The web component may be found in the Citect Anywhere Server folder:

```
<drive letter>\Program Files (x86)\Schneider Electric\Citect Anywhere\  
Server\WebServer\CitectAnywhere
```

Secure Connections

This section describes secure connection communication between WebSockets to both remote desktops and to the Citect Anywhere Secure Gateway.

Secured WebSocket Communication to Remote Desktops

The Citect Anywhere Server installation includes a self-signed certificate for SSL connections. Some browsers, such as Google Chrome, allow self-signed certificates for SSL- encrypted WebSocket connections.

Chrome and Safari 5.x do not allow SSL connections using self-signed certificate.

In order to provide connectivity from these browsers, a trusted certificate must be imported into the Citect Anywhere Server or into the Citect Anywhere Secure Gateway if it is being used as a proxy for Citect Anywhere Server. A trusted certificate must be purchased from a trusted certificate authority (i.e. VeriSign).

Note: The DNS address of the Citect Anywhere Server or Secure Gateway server needs to match the certificate name. If a wildcard certificate is being used, the domain needs to match. For example, if the certificate is for **.acme.com* the server name must end with *acme.com*.

To import a trusted certificate into the Citect Anywhere Server, perform the following steps using the Microsoft Certificate Manager:

1. Show the Windows Command Prompt running as an Administrator.
2. Type `certmgr.msc` to show the Certificate Manager.
3. Import the trusted certificate to the Computer (**Personal | Certificates**) store.
4. Mark the certificate as exportable during the import.
5. Go to the Certificate's Details tab and highlight the Thumbprint.
6. Copy the thumbprint (CTRL+c).
7. Stop the Citect Anywhere Server service.

8. Using the Command Prompt (cmd.exe) go to the folder that contains *AccessServer64.exe*.
9. Run: *AccessServer64.exe /genbincert <thumbprint of cert to export enclosed in quotation marks>*
10. After importing the thumbprint, a notification appears confirming the BIN certificate has been successfully created.
11. Start the Citect Anywhere Server service and it will be ready for use.

Secured WebSocket connections via Citect Anywhere Secure Gateway

When using the Citect Anywhere Secure Gateway, the connection between the Citect Anywhere Server browser client and the Citect Anywhere Secure Gateway can be secured. The Secure Gateway is installed with a self-signed certificate by default, but supports trusted certificates as well. Refer to the Citect Anywhere Secure Gateway Administrator's Manual for full instructions on how to install and configure it for use with Citect Anywhere.

Benefit of Using a Trusted Certificate

Certain browsers require that HTTPS or SSL connections be made only when a trusted certificate is present. Install a trusted certificate in the Citect Anywhere Secure Gateway or Citect Anywhere Server to confirm secure and reliable connections from a wide range of web browsers. A trusted certificate must be purchased from a trusted certificate authority (i.e. VeriSign).

Chapter 5: Configuring Citect Anywhere Server

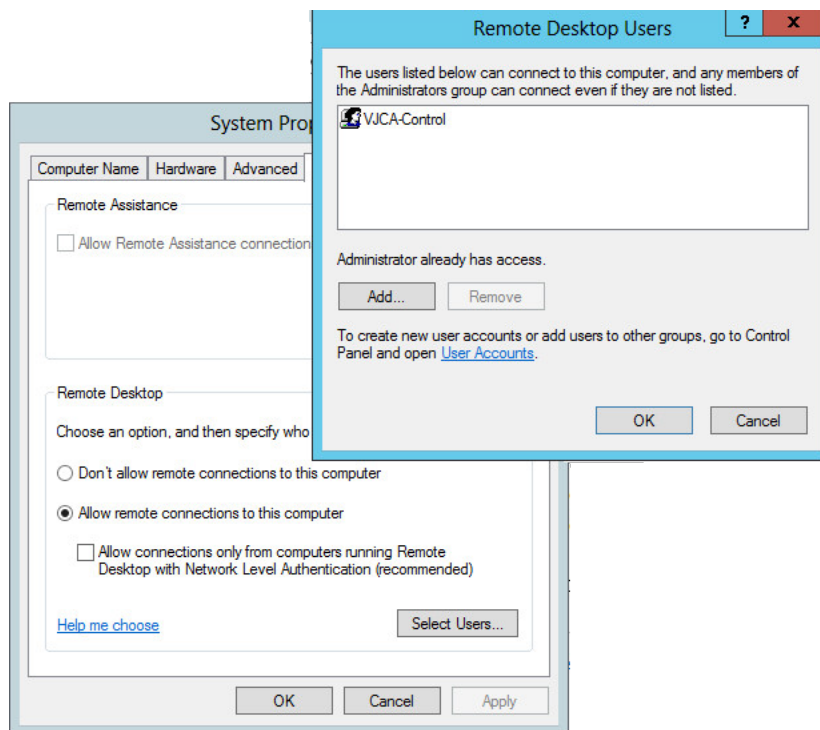
This chapter provides detailed information about configuring your PowerSCADA Anywhere Server. Configuration of the PowerSCADA Anywhere Server involves the following tasks:

- Configure settings for the PowerSCADA Anywhere Server service in the [Configuration Console](#)
- [Configuring user access](#) for Vijeo Citect

Configuring Remote Desktop Services

To sign in remotely, users or groups to which users belong need to be added to the Remote Desktop Users group. Complete these steps on the computer on which the PowerSCADA Anywhere Server is installed:

1. Navigate to the Control Panel. Select **System and Security > System**.
2. Select the **Advanced system settings** option on the left. The System Properties dialog is displayed.
3. Click the **Remote** tab.
4. Select the **Allow remote connections to this computer** option.



5. Click **Select Users**. The Remote Desktop Users dialog is displayed.
6. Add the required users and click **OK**.

Note: For more details about configuring RDS, see the [Remote Desktop Services with Vijeo Citect 2015](#) whitepaper. You need to register with the site before you can access the document.

Configuring User Access

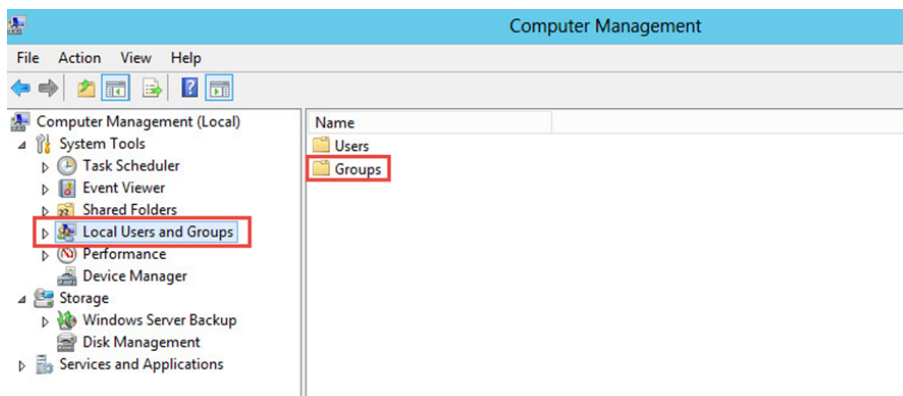
Depending upon their access, users can launch a Vijeo Citect View-only client or a Control client.

A View-only client is a computer configured with view-only access to the Vijeo Citect runtime system. No control of the system is possible, but full access to data monitoring is performed.

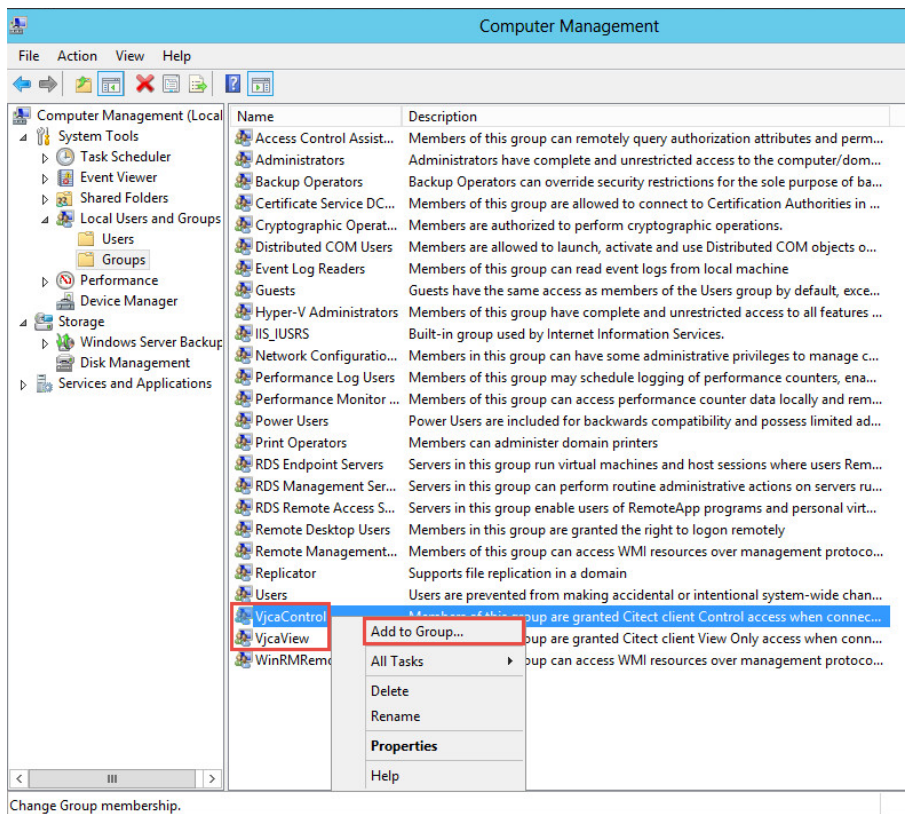
A Control client is the interface between the Vijeo Citect runtime system and an operator. If you are using Vijeo Citect on a network, all Vijeo Citect computers (on the network) are control clients.

Access to the client type is granted through two special Windows user groups created by the installer on the computer where the PowerSCADA Anywhere Server is installed. Users need to be added to the required group manually. To do this:

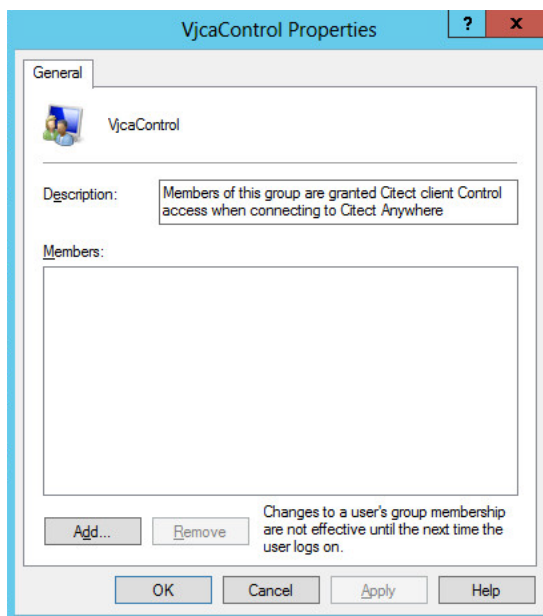
1. Navigate to the Control Panel. Select **Administrative Tools > Computer Management**.
2. In the left pane, navigate to **System Tools | Local Users and Groups**.



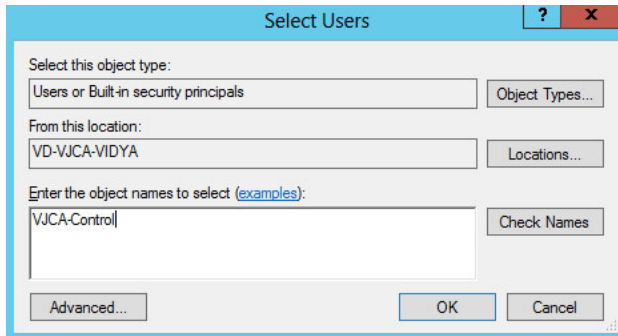
3. In the right pane, double-click on **Groups** to expand the node.
4. Locate the PowerSCADA Anywhere groups, and right-click on the group to which you want to add a user.



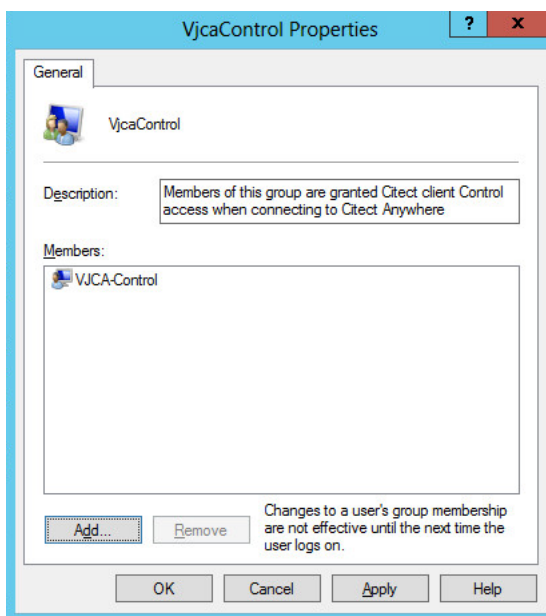
5. Select **Add to Group** from the context menu. The group properties dialog box appears.



- Click **Add**. The Select User dialog box appears.



- In the **Enter the object name to select** box, type the name of the user you want to add.
- Click **Check Names**. Once the user name is verified, click **OK**.group properties dialog box appears.



- Click **Apply**. The user is added to the selected group.

Activating a Vijeo Citect License

To connect to a Vijeo Citect client using Citect Anywhere, you need a Vijeo Citect floating license. Connection is possible only after the floating license is activated.

Obtain a Vijeo Citect floating license, and activate it using the Schneider Electric Floating License Manager. For instructions on activation, refer to the Activation Methods section in the Floating License Manager online help.

Configuring Flexera License Server

Flexera License Server is a prerequisite for installing PowerSCADA Anywhere Server. Typically the Flexera License Server is installed on the computer where the PowerSCADA Anywhere Server is installed. However, if you install the Flexera License Server on a different computer, you need to explicitly point to this computer from the computer where the PowerSCADA Anywhere Server is installed. To do this:

1. After you install the PowerSCADA Anywhere Server, navigate to the folder `\\Program Files (x86)\\Schneider Electric\\Citect Anywhere\\Launcher`.
2. Locate the file `SE.Scada.AnywhereLauncher.exe.config`.
3. Update the following lines:

```
<setting name="LicenseServer" serializeAs="String">  
  
<value>localhost</value>  
  
</setting>
```

Change "localhost" to the name or IP address of the computer on which the License Server is installed. For example:

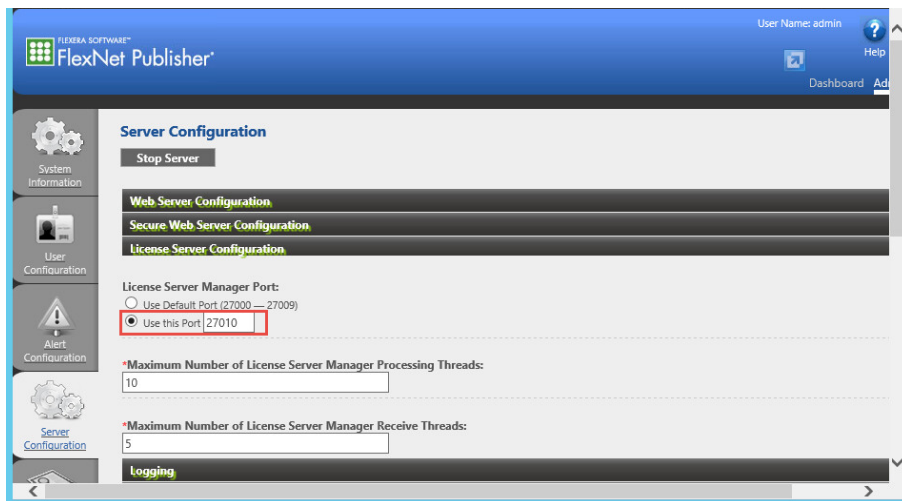
```
<setting name="LicenseServer" serializeAs="String">  
  
<value>10.175.10.158</value>  
  
</setting>
```

4. Save the file.
5. Restart the Citect Anywhere service for the change to take effect.

Configuring the License Server Manager Port

When PowerSCADA Anywhere Server is installed, the Flexera License Server Manager is upgraded to the latest version. The new version uses port 27010 to communicate with Vijeo Citect. Previous versions of Flexera used port 27000 as the default. The default will however remain the same when Flexera is upgraded. You will need to change the default port. To do so, follow these steps:

1. Open the FlexNet License Administrator.
2. Click the **Server Configuration** tab on the left. The Server Configuration page is displayed.
3. Click the **License Server Configuration** tab.
4. Select the **Use this Port** option, and specify the port to be used.



5. Click **Save**.
6. Restart the following services:
 - Flexnet Licensing service
 - ImadminSchneider service

Ensure that the PowerSCADA Anywhere Server is communicating on the same port. To do this:

1. Navigate to the folder `\\Program Files (x86)\\Schneider Electric\\Citect Anywhere\\Launcher`.
2. Locate the file `SE.Scada.AnywhereLauncher.exe.config`.

3. Update the following lines:

```
<setting name="LicenseServerPort" serializeAs="String">  
  
<value>27000</value>  
  
</setting>
```

Change "27010" to the new port number. For example:

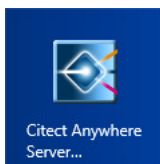
```
<setting name="LicenseServerPort" serializeAs="String">  
  
<value>27010</value>  
  
</setting>
```

4. Save the file.
5. Restart the Citect Anywhere service for the change to take effect.

The Configuration Console

The Server Configuration console presents a series of tabs that enable an administrator to configure various settings for the server service.

Double-click *ServerConfiguration.hta* file, located in the <drive letter>\Program Files (x86) \Schneider Electric\Citect Anywhere\Server folder. Alternatively, click the PowerSCADA Anywhere Server Configuration icon on your Desktop.



The Configuration Console appears. The Configuration Console only works on systems with Microsoft Internet Explorer 7 or later.

In general, changing Citect Anywhere Server configuration is not required. It is recommended to use the default settings.

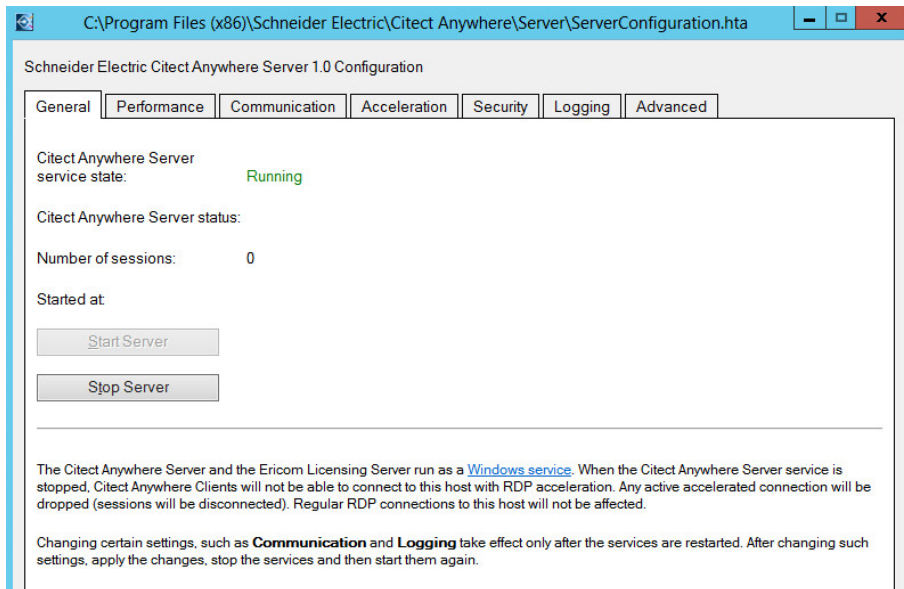
IMPORTANT: It is recommended that end users are not given access to the computer on which the PowerSCADA Anywhere Server is installed.

The following sections describe the different configuration tabs of the Citect Anywhere Server.

- [General](#)
- [Performance](#)
- [Communication](#)
- [Acceleration](#)
- [Security](#)
- [Logging](#)
- [Advanced](#) (for Administrator User Only)

General Tab

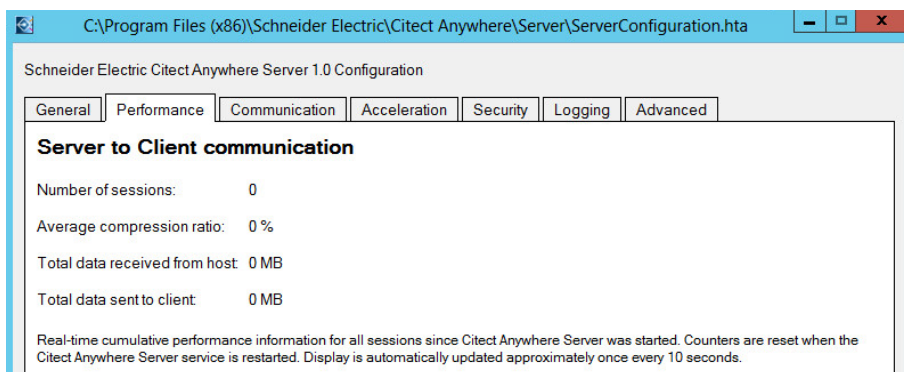
This page provides functions to start and stop the Citect Anywhere Server service. For certain configuration changes, a service restart is required. This page also displays the number of active Citect Anywhere Server client sessions connected to this computer.



Whenever the PowerSCADA Anywhere Server service is restarted, all sessions on the server will be disconnected.

Performance Tab

The Performance tab displays current performance statistics related to Citect Anywhere connections.



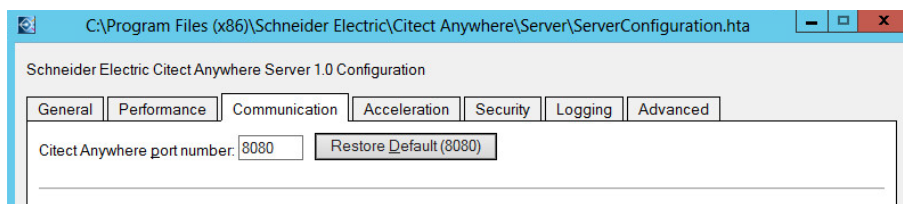
Communication Tab

This tab provides options to change the Citect Anywhere Server port and the address of the host computer running RDP.

When using a Citect Anywhere Server listening port other than the default (8080), the port number needs to be explicitly specified in the client address field (i.e., `http://<computer name>:5678/`).

When running Citect Anywhere Server on a computer with multiple network cards, change the RDP host address from localhost to the IP or DNS address of the network card that has RDP access to the system.

A change to either setting requires a service restart. This can be done via the General tab or using the Windows Service Manager.

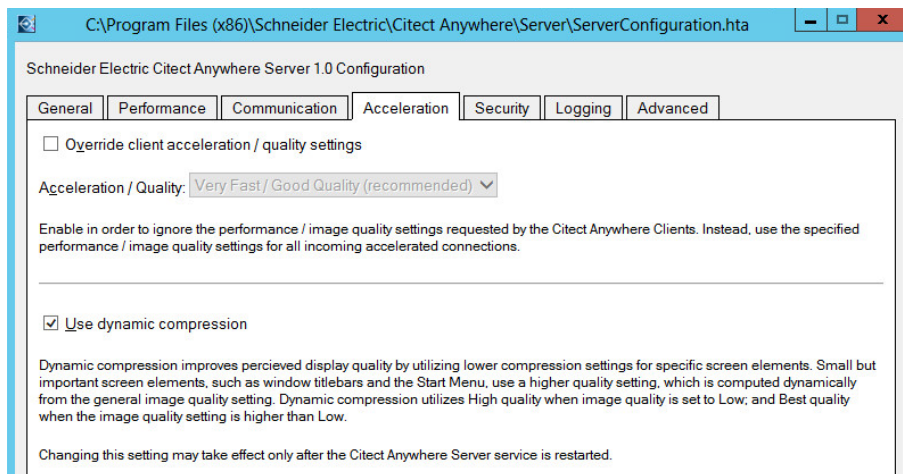


Acceleration Tab

This tab provides options to change the Acceleration/Quality level and disable dynamic compression. When the **Override client acceleration / quality settings** option is selected, all sessions use the configured setting, and all client settings are ignored. When selecting or clearing this setting, the service must be restarted for the change to take effect. When the setting is enabled, changing the acceleration level does not require a service restart, but active users must reconnect to use the new setting.

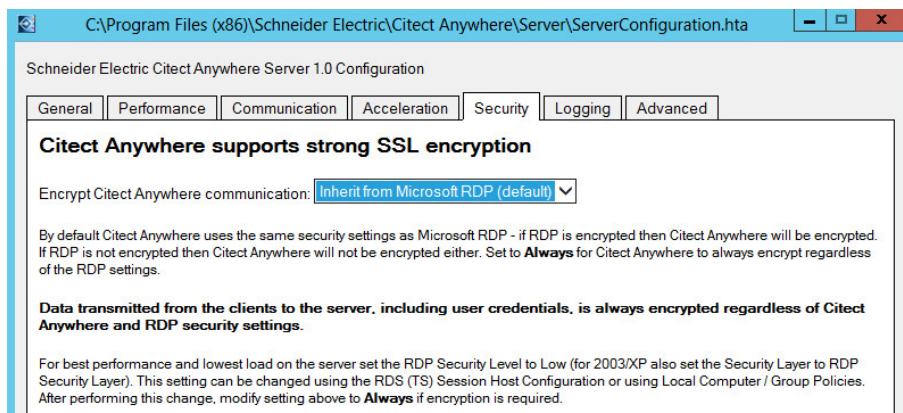
Dynamic Compression identifies small graphical objects on the screen (such as toolbar icons, task bar icons, Start Menu icons, etc.) and compresses them. Setting the image quality to low will result in maximum compression, minimizing the impact on the network. All other graphical objects are compressed at the selected quality. This provides the visual impression of a high quality remote desktop session.

By default, this feature is enabled. To disable, clear the **Use dynamic compression** box.



Security

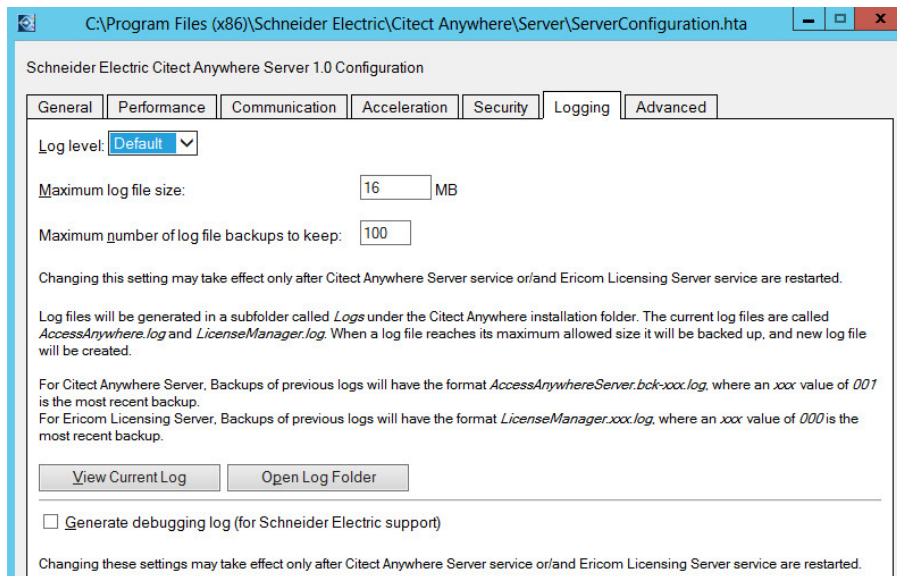
This page configures the Citect Anywhere Server security settings.



Note: Citect Anywhere provides integrated 128-bit SSL encryption. For best performance, set the host's RDP Security Encryption level to Low and change the **Encrypt Citect Anywhere communication** to *Always*. Using this configuration, Citect Anywhere SSL encryption will be used instead of the RDP encryption. Do not set this if users will be connecting directly to RDP regularly, as those sessions will end up using Low encryption.

Logging Tab

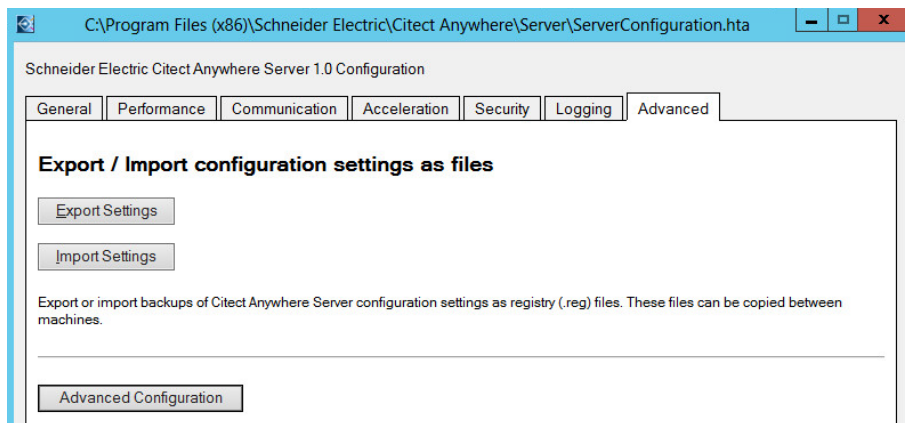
This tab provides options to enable/disable certain logging features. Technical Support may request a debugging log for diagnostic purposes. The debugging log is enabled here.



Advanced

This page provides access to advanced Server settings that are stored in the system's Registry.

- **Export Settings:** Exports the Citect Anywhere Server Registry key to the user's home folder (i.e., My Documents).
- **Import Settings:** Imports previously saved Citect Anywhere Server Registry settings.
- **Advanced Configuration:** Adds all configurable Registry key settings to the Registry. By default, only settings that are changed from the default value are saved into the Registry.



Chapter 6: Configuring Mobile Devices

This chapter contains information about using PowerSCADA Anywhere on mobile devices. The following information is covered here:

- [Supported Browsers](#)
- [Logging On](#) to PowerSCADA Anywhere
- [Automatic Display Resize](#)

Supported Browsers

With Citect Anywhere, users can access remote Vijeo Citect from HTML5 compatible web browsers on any device including smartphones, tablets, and laptop computers. To start a session, navigate to the *start.html* file that is installed on the Citect Anywhere Server. To do this, point a browser to the Citect Anywhere Server URL:

http://machineaddress:8080

Browsers Tested with Citect Anywhere

- Internet Explorer 10 and 11
- Microsoft Edge
- Google Chrome 33
- Safari 8 on Apple iOS

Multiple PowerSCADA Anywhere sessions can be opened in different tabs within the web browser, or in different browser windows. When a session is not in use (its tab or window is not displayed) it will reduce its CPU and memory utilization.

Logging On to Citect Anywhere

To log on to the Citect Anywhere Connection Web Page, follow these steps:

Note: If you have any trouble remotely connecting to the Citect Anywhere environment, see [Checking Connectivity](#) on page 1 for help.

1. Navigate to `http://<VJCA Server Node Name>:8080/`. The logon form appears.

2. Enter the connection parameters.

Note: When using a Secure Gateway, the **User Name** and **Password** fields are mandatory, otherwise they are optional.

CONNECTION PARAMETERS	DESCRIPTION
User Name	Credentials to log on to the RDP host. It can optionally contain domain specification, for example, domain\user. If it is not specified, you will be prompted for credentials by the RDP host. The user needs to be a Windows user, be a member of the VjcView or

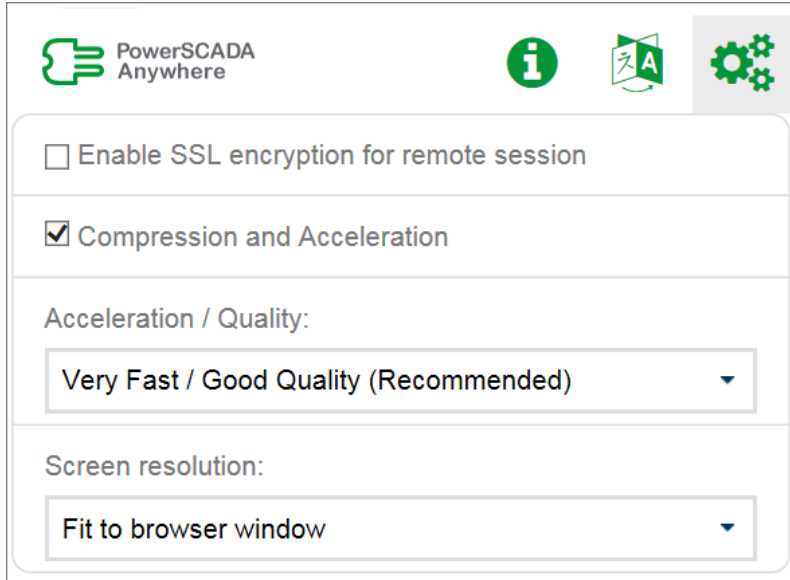
CONNECTION PARAMETERS	DESCRIPTION
	VjcControl group and must be a valid Vijeo Citect user.
Password	Corresponding password for the user name. For security reasons, this value should not be saved for future connections. If it is not specified, you will be prompted for credentials by the RDP host.
Remember Password	Select this option to save the specified password for the next session. This option can be hidden from the web page.

3. Tap or click **Connect** to initiate the connection. The following progress indicator is displayed before connection is established.

Configuring Advanced Settings

To configure advanced settings:

1. Click . The options appear as shown below:



2. Complete the following options:

OPTIONS	DESCRIPTION
Enable SSL encryption for	This option is selected as a default. It enables the client to use Secure Socket Layer (SSL) encrypted WebSocket communication to the Citect Anywhere Server.

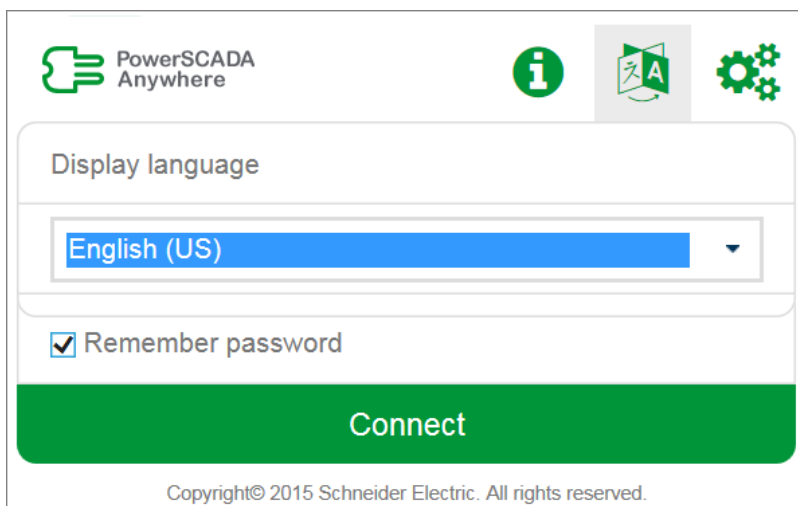
OPTIONS	DESCRIPTION
remote session	
Compression and Acceleration	Select this option to enable lossy image compression for the session. The acceleration, or degree of quality loss, can be specified by selecting options from a drop down list.
Acceleration Quality	Controls the degree of acceleration that is enabled in the session. Faster acceleration will result in lower quality images.
Screen Resolution	Sets the resolution size of the Citect Anywhere session. Select a value from the drop down list of values. For example: "800 x 600". This should be configured to match the Vijeo Citect project.

3. Click anywhere to return to the connection details.
4. Tap or click **Connect** to initiate the connection.

Changing the Display Language

To change the language in which the form is displayed:

1. Click .
2. From the **Display language** list, select the required language.



Note: For details about the version of Citect Anywhere you are running, click



Automatic Display Resize

Citect Anywhere supports automatic display re-size. Whenever a browser window is re-sized, the Citect Anywhere session automatically adjusts itself to the new dimensions. To re-size a browser window, drag any corner of the browser window and release it when the desired dimensions are reached. If a browser is placed into full screen mode, the Citect Anywhere session will automatically expand to the full screen.

Using Gestures on Client Portable Devices

Google Chromebooks

Citect Anywhere operates on Google Chromebook and Chromebox just like it does with a Google Chrome browser. Here are some tips to keep in mind when using Citect Anywhere with a Chromebook or Chromebox.

FUNCTION	DESCRIPTION
Mouse Left-click	Click the Chromebook trackpad with one finger.
Mouse Right-click	Click the Chromebook trackpad with two fingers
Scrolling a document or website	Drag two fingers on the Chromebook trackpad up or down to scroll
Configure Chromebook	In the address field: <i>chrome://settings</i>

Chrome Keyboard

The Chromebook keyboard lacks several keys that are used by Windows. ChromeOS provides standard mappings that use existing keys with the ALT button to represent certain missing keys. Citect Anywhere supports these key combinations:

COMMAND	KEY COMBINATION
Delete (DEL)	ALT+Backspace
Page Up	ALT+Up
Page Down	ALT+Down
Home	CTRL+ALT+Up
End	CTRL+ALT+Down

In addition, Citect Anywhere provides special non-standard mappings for additional key combinations on ChromeOS.

COMMAND	KEY COMBINATION
F1	CTRL+1
F2, ...	CTRL+2, ...

COMMAND	KEY COMBINATION
ALT+TAB	ALT+`
ALT+SHIFT+TAB	ALT+SHIFT+`
CTRL+Home	CTRL+ATL+Left
CTRL+End	CTRL+ALT+Right

Tablet and Smartphones

Citect Anywhere can operate on tablets or smartphones with an HTML5 compliant browser (see list of browsers in Citect Anywhere Readme). Browser versions that have been tested and their specific behaviors are detailed in the Citect Anywhere User Guide.

When you design Vijeo Citect clients for use with Citect Anywhere, remember that touch devices have different interface requirements and capabilities than a keyboard and mouse. For example, input animations should not invoke a Vijeo Citect or Windows keyboard, as mobile devices have their own.

With existing Vijeo Citect clients that make use of mouse events and keys or key combinations without a supported equivalent, you may want to modify your application to use alternate application events.

The following list provides gestures available when using Citect Anywhere from a tablet or smartphone device where a physical keyboard and mouse is not available. Functionality will vary across different devices and certain commands may not be available.

- Single Tap performs a left click.
- Single long Tap performs a right-click.
- Tap + Hold + Drag performs a select then drag/scroll function.
- Double Tap, or tapping once with two fingers, performs double-click.
- Tap with three fingers sends Back command to a remote browser.
- Swipe down with three fingers is Page Up.

- Swipe up with three fingers is Page Down.
- Drag left or right with three fingers performs a left arrow and right arrow respectively.
- Tap the keyboard icon (upper right-hand corner of window) to open/close the virtual keyboard.
- Swipe and pinch gestures will apply to the Citect Anywhere session (i.e. zoom in with pinch in).
- (iOS only) When saving a Citect Anywhere icon to the iOS desktop, the shortcut will open the Citect Anywhere session full-screen mode. The browser's toolbar will be hidden and there will be more remote desktop area available.

HTTPS Mode

For environments where WebSockets support is not available, Citect Anywhere can work in HTTPS mode such that all communication will be sent via HTTPS only. HTTPS mode will only be used if WebSockets is not available. WebSockets will be used when available as it will provide better performance. HTTPS mode is required when using Microsoft Internet Explorer 9 or with SSL VPNs that only proxy HTTPS traffic.

To enable HTTPS Mode, the Citect Anywhere Secure Gateway is required. The Citect Anywhere Server web pages need to be delivered using the web server built into the Citect Anywhere Secure Gateway (files are located under the Webserver/Citect Anywhere folder). Carry out the following steps to enable Citect Anywhere for HTTPS support.

1. Install Citect Anywhere Server on the desired RDP Host.
2. Install the Secure Gateway in a separate machine located in a DMZ. The Secure Gateway must be installed on a server that is accessible by the target end-user group(s).
3. To connect to the Citect Anywhere Server using HTTPS - enter the Citect Anywhere URL of the Secure Gateway (the Secure Gateway includes the Citect Anywhere web component)
`https://<securegatewayaddress>/Citect Anywhere/start.html`
4. Enter the parameters for the target Citect Anywhere Server in the start.html page.
5. Upon connection, if HTTPS mode is active a '-' symbol will then be shown as a prefix to the address in the browser tab.

Note: HTTPS mode requires a browser that supports Canvas. Older browsers, such as Microsoft Internet Explorer 8 (or earlier) do not support Canvas.

Chapter 7: Advanced Configuration

Citect Anywhere also easily integrates with other web pages and portals. The application can accept configuration settings from other pages or directly from a web server. These settings can also be displayed in the Citect Anywhere start page for the user to view and modify, or trigger an automatic connection.

Static Configuration of *Config.js*

An administrator can modify configuration settings for Citect Anywhere by editing the *config.js* file that is installed as part of the Citect Anywhere web component. This is a JavaScript file that can be modified using any text editor.

Note: Always create a backup of the original *config.js* file before making any changes. This will ensure easy rollback to the original configuration.

Most settings in the file have the following format:

name: value

A value can be a number, a flag (true or false), or text enclosed in quotes. Some settings are prefixed by a double slash // which means they are disabled. Remove the double slash in order to set a value for the setting. Javascript rules apply in this file, certain characters need to be escaped (i.e. backslash). Once the settings are configured, save the file and the next user will have the new settings applied.

Refer to the [Settings Table](#) for a description of each setting.

Settings Table

The *config.js* file contains the following configuration settings. Setting names are case sensitive. When settings are specified using cookies, their name are prefixed by *EAN_*.

SETTING NAME	DESCRIPTION
overrideSaved	False (default), settings that the user changes are preserved between sessions and override values set in <i>config.js</i> . Change to True for <i>config.js</i> to override preserved settings.
onlyHTTPS By	By default, Citect Anywhere first attempts to connect using WebSockets. If the Secure Gateway is used with Citect Anywhere, the connection will fall back to HTTPS when WebSockets is not available. If this setting is true, HTTPS is used immediately.
noHTTPS	By default, Citect Anywhere first attempts to connect using WebSockets. If the Secure Gateway is used with Citect Anywhere, the connection will fall back to HTTPS when WebSockets is not available. If this setting is true, only WebSockets will be used and HTTPS fallback will be disabled.
hidden	A comma- or space-separated list of field names as they appear in <i>config.js</i> . For example "username, password, domain". The listed fields will be hidden so that the user will not be able to modify them. To hide a button, such as the Advanced button, prefix the button text with the word show. For example, "showAdvanced, showAbout" hides both the Advanced and About buttons. All hidden variables ignore previously saved settings.
settings (URL parameter only)	Name of a Configuration Group to be used.
wsport	The default WebSocket port that will be used by the client. The value specified in the file (8080 by default) will be used for both encrypted and unencrypted WebSocket communication. The user can override this value by explicitly specifying a port address in the client UI. For backward compatibility with older versions of Citect Anywhere Server, this behavior can be modified. If singlePort is set to false then the port value specified is only for encrypted communication. The value specified in the file plus one (8081 by default) will be used for unencrypted WebSocket communication.

SETTING NAME	DESCRIPTION
gwport	The default gateway port that will be used if it is not explicitly specified in the address field.
dialogTimeoutMinutes	Timeout period, in minutes, after which an inactive dialog is automatically closed and the session is logged off. This is only relevant for dialogs that have a logoff button.
sessionTimeoutMinutes	Timeout period, in minutes, after which an inactive session is disconnected. This timeout is reset whenever user clicks on the keyboard or a mouse button. The default value is 0, which disables this feature.
specialkeys	Enables support for special RDP key combination commands, such as CTRL+ALT+END which starts the Windows NT Security dialog box (similar to local CTRL+ALT+DEL). See http://support.microsoft.com/kb/186624 for the list of key combinations.
chromeKeys	true (default) support special ChromeOS keys combinations
showDownload	true displays a link in the connection dialog to download the Citect Anywhere Server installer.
clipboardSupport	true (default) enables clipboard functionality; false disables it.
clipboardTimeoutSeconds	The delay duration before the clipboard image automatically fades out.
clipboardUseFlash	true (default) uses Flash when available for one-click copy into local clipboard.
clipboardKey	Key to open clipboard paste dialog, set to false to disable.
console	false (default) set true to enable RDP console mode.
settingsURL	false (default) set true to enable RDP console mode.
endURL	URL to open to after the Citect Anywhere session has ended (# value closes window). If there is a prefix with the symbol ^ then this sets the value of window.location instead of top.location. This is useful when the Citect Anywhere session is embedded in a frame.
address	Address of Citect Anywhere Server. Always blank for the standard configuration.
fulladdress	Address of RDP host. Always blank for the standard configuration.
username	Username to pass into the Citect Anywhere session.

SETTING NAME	DESCRIPTION
password	Password to pass into the Citect Anywhere session (entered as clear text in <i>config.js</i> file)
domain	Domain to pass into the Citect Anywhere session.
remember	False (default) determines whether the user's password will be saved in the Citect Anywhere page for future use. Set to true to enable password saving (not recommended for kiosk usage).
encryption	False determines if encryption will be enabled from the Citect Anywhere client to the server
blaze_acceleration	True determines if RDP acceleration will be used
blaze_image_quality	Sets the quality level using a numeric For example: 40 (fair quality), 75, 95 (best).
resolution	Sets the resolution size of the Citect Anywhere session. The value set must be a valid option under the Citect Anywhere screen resolution setting. For example: "1024,768" For Full Screen, use: screen.
use_gateway	False (default), set to true to use a Secure Gateway for remote access.
gateway_address	Defines the address and port of the Secure Gateway For example: secure.acme.com:4343
useScancodes	No longer in use, see <i>convert_unicode_to_scancode</i> .
convert_unicode_to_scancode	False (default), set to True when using certain applications that send characters as scancodes (i.e. VMware vSphere Client, any application where you may have issues typing text). This setting will generate scancodes based on the selected locale.
leaveMessage	The message displayed to the user after they navigate away from an active session.
audiomode	0, enables audio redirection (default) 1, play audio on remote computer 2, disables audio redirection
name	Defines a custom string for the connection name. By default, the RDP Host address is used.
minSendInterval	Specifies the minimum duration between mouse position messages sent from the client when the mouse button is pressed. Units is milliseconds.

Note: In some cases, the local browser must be closed and reopened before changes take effect. The local browser cache may also need to be cleared.

Defining Configuration Groups

All users share the configuration settings defined in the *config.js* configuration file. It is possible to specify special settings that will override the global settings for certain groups of users. Multiple configuration groups are defined in the configuration file.

For example, if the Marketing group will have clipboard redirection and printing enabled, change *config.js* as follows:

```
var defaults = { //this already exists in the file

...

    "Marketing":{ //Bold text are new additions

remember:false,

audiomode:0

    },

};
```

Note: The double quotes surrounding Marketing must be identical. It may be necessary to delete them and re-type them if the text was copied from another source.

Also, the last setting of the configuration group should not have a ‘,’ at the end. This comma will be placed after the closing bracket ‘}’.

In the URL to be used by the Marketing group, add the **settings** parameter:

http://<computer name>:8080/Citect Anywhere/start.html? **settings=Marketing**

Settings Precedence

When a Citect Anywhere client starts, it reads configuration information from a variety of sources. If two or more sources contain different values for the same setting, the value that Citect Anywhere will use is determined by the following precedence order:

Highest precedence to Lowest precedence

- URL parameters
- Cookies
- Saved settings from previous session
- *config.js*

For example, if the gateway_address is specified to be "server1" in config.js but "server2" in a cookie (EAN_gateway_address), then the value "server2" will be used.

If the setting override Saved is set to true in *config.js*, then any settings predefined in the config.js file will override previously used settings, and the precedence order will change slightly:

Highest Precedence to Lowest Precedence

- URL parameters
- Cookies
- Saved settings from previous session
- config.js

These settings become effective only after the user starts a new session. In some cases, the local browser must be closed and reopened before changes become effective. The local browser cache may also need to be cleared.

Passing Credentials using Form POST

User credentials may be passed to Citect Anywhere using the form POST method. This functionality is used to provide SSO (single sign-on) from an outside source that has already authenticated the user (such as an SSL VPN.)

The Citect Anywhere Secure Gateway is required in order to use form POST with Citect Anywhere. Refer to the Citect Anywhere Secure Gateway manual for detailed instructions.

Embedding Citect Anywhere in an iframe

To embed Citect Anywhere within a third-party web page using the iframe mechanism, simply place an iframe tag within the containing page, and have the iframe's SRC attribute reference the Citect Anywhere URL.

For example:

```
<body>
```

```
    <h1>Embedded Citect Anywhere</h1>
```

```
    <iframe src="http://127.0.0.1:8080/CitectAnywhere/start.html"
        style="width:1024px; height:768px"></iframe>
```

```
</body>
```

When a Citect Anywhere session ends, it can be configured to send the browser to a specified URL using the endURL setting.

- Specify a simple URL to redirect the iframe.
- Prefix the URL with ^ to redirect the iframe's parent (container).
- Prefix the URL with \$ to redirect the top-most container.
- Specify # and the URL will close the browser tab.

Chapter 8: SSL VPN Configuration

Citect Anywhere is compatible with most SSL VPNs. An SSL VPN that does not support WebSockets will require the Secure Gateway (SG) as well. Juniper IVE version 7.4 supports WebSockets, so the Secure Gateway is not required.

Citect Anywhere has been tested with Juniper's SA SSL VPNs and the documentation in this section will be based off Juniper's administration pages. Configuration with other third-party SSL VPN appliances will be similar to the procedures described here (difference are mostly in terminology).

Web Proxy with 7.4

Juniper version 7.4 supports WebSockets. Citect Anywhere links are published in the Juniper's web interface as web applications. To publish a new Citect Anywhere connection, go to the Juniper Admin page and do the following:

1. Go to **Resource Profiles | Web | New Web Application Resource Profile**.
2. Enter the **Name** of the Citect Anywhere connection that the users should see.
3. Enter the Citect Anywhere URL in the **Base URL** box.
4. Click **Save and Continue**.
5. In the Roles dialog add all roles that should have access to the Citect Anywhere link and click **Save Changes**.
6. In the Bookmarks tab, enter the desired label for the connection.
7. When you log into Juniper, a Citect Anywhere link will be displayed under the Web bookmarks section (i.e. Citect Anywhere). Click on the link to connect to a Vijeo Citect client published with Citect Anywhere.

Web Proxy with Older Juniper Versions

Juniper versions prior to 7.4, and most other SSL VPNs do not support native WebSockets. Such SSL VPNs require HTTPS Mode (see HTTPS Mode chapter in this guide) to run Citect Anywhere. HTTPS mode is enabled by installing the Secure Gateway (SG).

To use Citect Anywhere and the Secure Gateway:

1. Go to **Resource Profiles | Web | New Web Application Resource Profile**.
2. Enter the **Name** of the Citect Anywhere connection that the users should see.
3. Enter the Gateway's Citect Anywhere URL address as the Base URL. Click **Save**.
4. Go to **Autopolicy: Web Access Control**.
5. Edit the automatically entered address and delete the subfolder "Citect Anywhere ".
Instead of `https://GWaddress.com:443/Citect Anywhere /*` the correct resource is `https://GWaddress.com:443/*`
6. Click **Save and Continue**
7. In the Roles dialog, add all roles that should have access to the Citect Anywhere link and click **Save Changes**.
8. When you log into Juniper - the Citect Anywhere link will be displayed under the Web bookmarks section (i.e. Citect Anywhere Connection to RDP Host). Simply click on the link to connect to an application or desktop published with Citect Anywhere.

Note: If the link is not translating properly, make sure that there is not a Passthrough Proxy policy defined for the Gateway Server (where the web component is hosted).

Single Sign On(SSO) Using Cookies

In the Single Sign-on Config, set **Remote SSO**.

Set **Send the following data as request headers** to the Citect Anywhere URL. Set the desired cookies, for example:

- EAN_username=<USER> (this passes the username)
- EAN_password=<PASSWORD> (this passes the password)
- EAN_autostart=true (this auto starts the connection, “bypassing” the start page)
- Other Citect Anywhere parameters may also be passed as cookies

Network Connect

Juniper’s Network Connect mode opens a VPN tunnel to the private network. When using Network Connect, simply enter the Citect Anywhere parameters as if they were on the private network.

JSAM and WSAM

The Java and Windows Secure Access Manager provide additional security by limiting the end user’s access on the private network to only assigned resources. The Citect Anywhere parameters will be masked by Juniper and will not be directly accessible by the end user. To configure Citect Anywhere for JSAM, go to the Juniper Admin page and do the following (WSAM configuration is similar to the JSAM procedure below):

1. Publish a JSAM Client Application Profile by going to **Resource Profiles | SAM | Client Applications**
2. Click **New Profile** and enter the following parameters:
 - a. Type: *JSAM*
 - b. Application: *Custom*
 - c. Name: <enter desired label here>
 - d. Server Name: <enter address of Citect Anywhere Server>
 - e. Server Port: <enter Citect Anywhere port # (default is 8080)>
 - f. Client Loopback IP: Juniper’s aliased address for the Citect Anywhere Server (Important note: this address must be entered as the Citect Anywhere address for Juniper users).
 - g. Client Port: Juniper’s aliased port for the Citect Anywhere Server (Important note: this port must be entered as the Citect Anywhere port for Juniper users). The default port 8080 may be used here if it does not create a port conflict.
 - h. Click **Save and Continue**

- i. Select the Roles that will have access to this JSAM application.
- j. Click **Save Changes**, and now this application is ready for use.

Auto-starting JSAM or WSAM upon Login

Users may have to manually start a Client Application Session upon login.

To have the JSAM or WSAM applet launch on login to Juniper, go to the Juniper Admin page and do the following:

1. Click on **User Roles | <select desired Role> | General**.
2. Verify that the **Secure Application Manager** is checked and click on **Options**.
3. Check the **Auto-launch Secure Access Manager** option.
4. Click **Save Changes** and the next time you log in the SAM will automatically start.