CitectSCADA

v7.20

Installation and Configuration Guide

October 2010

Legal Notice

DISCLAIMER

Schneider Electric (Australia Pty. Ltd.) 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 (Australia Pty. Ltd.) reserves the right to revise this publication at any time without incurring an obligation to notify any person of the revision.

COPYRIGHT

TRADEMARKS

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

Citect, CitectHMI, and CitectSCADA are registered trademarks of Schneider Electric (Australia Pty. Ltd.)

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 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 NOTICE

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

October 2010 edition for Schneider Electric (Australia Pty. Ltd.)

Manual Revision Version 7.20.

For further information contact Schneider Electric (Australia) Pty. Ltd. at www.Citect.com/scada

Contents

Chapter 1: Introduction 5

About This Guide 5

Purpose 5

Maintaining System Currency 5

Audience 5

Chapter 2: Migration 7

Changes in Functionality 7

Network Support 7

New Features 8

Introduced in Version 7.0 8

Introduced in Version 7.10: 10

Cicode Functions From Version 7.0 13

Introduced in Version 7.20: 13

The Migration Process 17

Low Impact Changes 17

Changes Impacting Migration 18

Migration Aids 18

Upgrading a Runtime-only Installation 19

Chapter 3: Installation Description 21

Task Selection Dialogs 21

Installation Profiles 21

Documentation Installation 22

Add-ons Installation 22

Communication Drivers 23

Chapter 4: Installation Requirements 25

All Core Components 25

System Hardware 25

System Software 26

System Software 28

Runtime Only Server or Client 29

Hardware Requirements 29

System Software 30

Software Licensing 30

Updating Your Hardware Key 30

CitectSCADA License Point Count 31

Demo Mode....32

Chapter 5: Installation 33

The Installation Process 33

Preliminary Installation 33

Installation Profiles 36

Completing the Installation 40

Installing Additional Communication Drivers 45

Installing Service Packs....46

Modify, Repair, or Remove Components 46

Uninstall a Service Pack....47

Chapter 6: Configuration.... 49

Local Area Network Configuration 49

Network Communications Overview....49

Configuring Communications Over a WAN 50

Web Server Configuration 51

The IIS Virtual Directory 51

Setting Up Security....52

Web Client user account types....52

Configuring Security Using IIS....52

Testing the Web Server Security Settings....56

Logging on to the Web Server....56

Index.... 59

Safety Information

Hazard categories and special symbols

The following symbols and special messages may appear in this manual or on the product to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

A lightning bolt or ANSI man symbol in a “Danger” or “Warning” safety label on the product indicates an electrical hazard which, as indicated below, can or will result in personal injury if the instructions are not followed.

The exclamation point symbol in a safety message in a manual indicates potential personal injury hazards. Obey all safety messages introduced by this symbol to avoid possible injury or death.

Symbol	Name
	Lightning Bolt
	ANSI man
	Exclamation Point

⚠ 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** property 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

Before You Begin

CitectSCADA is a Supervisory Control and Data Acquisition (SCADA) solution. It facilitates the creation of software to manage and monitor industrial systems and processes. Due to CitectSCADA's central role in controlling systems and processes, you must appropriately design, commission, and test your CitectSCADA project before implementing it in an operational setting. Observe the following:

⚠ WARNING
UNINTENDED EQUIPMENT OPERATION Do not use CitectSCADA or other SCADA software as a replacement for PLC-based control programs. SCADA software is not designed for direct, high-speed system control. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

⚠ WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.[a]
- Each implementation of a control system created using CitectSCADA must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[a] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control".

Chapter 1: Introduction

About This Guide

Purpose

This document is a guide for installing CitectSCADA. It describes the installation process and optional components which can be installed in each environment.

The configuration section provides an overview of using CitectSCADA in a Local Area Network (LAN), a Wide Area Network (WAN), and as a Web Server.

It includes information on the following aspects of installing CitectSCADA:

- Migration
- Installation Description
- Installation Requirements
- Installation
- Configuration

Maintaining System Currency

After you have completed the installation and configuration of CitectSCADA and deployed it as your production system, it is very important that you keep your software up to date. Schneider Electric (Australia Pty. Ltd.) will periodically publish updates in the form of Service Packs, Hot Fixes or Advisories relating to safety, security and functionality of CitectSCADA. These updates are available from the Knowledge Base page of the “MyCitect” web site. We especially recommend that you nominate a person in your organisation to refer, and subscribe, to the RSS feeds for Safety and Security, as well as the latest articles on the web site.

Audience

This document is primarily for those who install CitectSCADA, either on a single workstation or on a network. It is also useful for system administrators and new users of CitectSCADA.

Chapter 2: Migration

This chapter describes changes in functionality and new features introduced in CitectSCADA Version 7.0, 7.10 and 7.20 and how it may effect your installation and migration from a previous version. Migration information in this chapter covers only migration from Version 6.x to Version 7.20. If you are running a version earlier than 6.0 it is recommended that you upgrade to Version 6.0 before migrating to Version 7.20.

Changes in Functionality

Network Support

In order to incorporate the many benefits provided with the introduction of the New Communications Architecture in CitectSCADA Version 7.0, it was necessary to remove the support for NetBIOS network communications. Version 7.10 and later only supports TCP/IP networking.

If you are currently using TCP/IP as your network protocol you may ignore this section. However, if you currently implement NetBIOS, change your network communication over in your current version of CitectSCADA to TCP/IP before installing CitectSCADA Version 7.20.

Converting from NetBIOS to TCP/IP

This conversion is a two part operation. The first part is to convert each of your servers (Alarms, Reports, Trends). For the transition time that you are performing the conversion of your entire system you need to maintain network communication between your servers and your clients, this requires that your servers support both NetBIOS and TCP/IP for a brief period. Do this by directly editing the appropriate parameter in the LAN section of the Citect.ini file on each server. This can be done by using the Computer Setup Editor.

In order to support both NetBIOS and TCP/IP set the TCP/IP parameter to 1 in the Citect.ini file as shown below.

```
[LAN]
NetBIOS =1
TCPIP =1
```

Also set the server parameters in the DNS section as described in the Version 6 online help under the topic "Using TCP/IP for network communications " under the topic "Using CitectSCADA on a Network".

Once you have configured your servers to use TCP/IP (and maintain NetBIOS) edit the Citect.ini file on each of your client machines, set TCPIP=1 and NetBIOS=0 for each of those clients. You do not need to maintain NetBIOS on the clients as they are now communicating with the servers using TCP/IP.

Note:

- It is essential to set up your servers to use TCP/IP before you set up your client machines.
- Once you have finished the conversion on all client machines, return to the Citect.ini file of each server and set the NetBIOS parameter to 0, so disabling NetBIOS on each server as this is now redundant.

On completion of the conversion described above to your existing system to use TCP/IP, you can then continue with the remainder of the The Migration Process and installation procedure to Version 7.20.

New Features

CitectSCADA Version 7.20 includes the following new features or changes in functionality. In many cases these new features will not impact the installation or initial configuration. However, some of them may impact your project configuration and functionality. Once you have installed this version, refer to the online help for information on how to reconfigure your projects to take advantage of the new features and improved functionality.

Introduced in Version 7.0

CitectSCADA Version 7.0 incorporates the following new features

Improved Support for Clustering

The concept of "clustering" was introduced in an earlier version of CitectSCADA. The original concept allowed the "grouping" of duplicated elements, and gave you the ability to cluster Alarms, Reports and Trends servers. However, there were limitations.

The concept of clustering has since evolved and has the advantage of greater flexibility and improved performance. Each of the servers (IO, Alarm, Trend and Report) has a unique name and is part of a Cluster. Each Cluster has a unique name and clients can refer to clusters by it.

A CitectSCADA project can now include separate clusters allowing for geographical or logical divisions to be implemented in a single project.

Configure CitectSCADA's clustering as a direct reflection of the system that is to be deployed, and in particular:

- The requirements for the system
- The physical layout of the facility
- The strategy for maintenance and deployment of the system

Online Changes for Clients

Server decoupling allows changes to be implemented at runtime on clients without a shutdown of the client being required. Regardless of whether a server requires a restart for an online change, the client does not require a restart.

Clients currently contain a copy of Trend, Alarm and Variable Tags which has to match the server copy. In Version 7.0, the need for the variable tag configuration to be loaded by the clients has been removed. The client retrieves the configuration from the server when required and is notified by the server when changes occur.

The following list describes the online changes that can be made without the client machine having to be restarted:

- Adding Trends, Alarms, Alarm categories and Address based Variable Tags

- Modifying a subset of properties of Trends, Alarms and Alarm categories
- Modifying Address based Variable Tag properties
- Deleting Address based Variable Tags
- Adding and deleting pages and PAV files (except the current one)
- Modifying pages and PAV files (except the current one)
- Adding, deleting or modifying user profiles

New Communications Architecture

A new publish-subscribe architecture removes much of the need for polling. It is an enabling technology and a step towards improved performance, project deployment, server side online changes, and discovery services.

Local Variables

Memory I/O devices have been removed from CitectSCADA Version 7.0 and a new tag has been introduced called Local Variable to replace the "Memory PLC" based variable tag. A Local Variables allows you to store data in memory when you start your runtime system. Local variables are created each time your runtime system starts, and therefore do not retain their values when you shut down your system. They can be of any data type supported by CitectSCADA.

Each process has its own copy of each local variable configured in the project, the values in a local variable are available only to the process that wrote them.

Publish Alarm Property

Alarm devices were defined as devices with their Protocol field set to "Alarm". The function of these devices are now configured on an Alarm Server by setting the "Publish Alarm Properties" property to True.

Memory Mode for Devices

Devices can now be run in simulation mode. When configuring an I/O device, you have the option to set memory mode. This means that the I/O device will be created in memory and its values stored in memory at runtime.

This is useful when you are configuring a system for the first time, as you can design and test your system before using a physical I/O device in the system.

As with local variables, the values of an I/O device in memory mode are not retained when you shut down.

Persist Mode for Devices

When configuring an I/O device, you have the option to set persist mode. This means that the value of each variable in the I/O device is stored on the computer's hard disk. Since the values are saved to disk, when you restart your system after a system becomes inoperative or a shutdown, the latest values are immediately available.

Persist mode is useful for status information or predefined data that is required as soon as the system restarts.

Improved Hardware Alarms

The limitation in previous releases of CitectSCADA of only a single alarm from multiple alarm situations being displayed has been lifted. All and any alarms are now displayed simultaneously, allowing for immediate response to multiple situations.

Event Driven Cicode

Cicode can now be triggered by the change of a specific tag. This improves the efficiency of the CitectSCADA system by removing the need to poll for changing tag values.

Publisher-Subscriber Model

CitectSCADA now uses a Publisher-Subscriber data acquisition model. Client computers subscribe to configured tags and receive notification when the tag values change. Cicode functions can also be triggered by the change of a tag, removing the need to poll, and improving the efficiency of the system.

Dual Network Support

Previous CitectSCADA versions have been able to support redundant networks via NetBIOS. From Version 7.0, users can specify multiple IP addresses for each server using only TCP/IP, providing native support for network redundancy.

Project-Based Network Configuration

From Version 7.0, the project topology is embedded in the project, and network configuration can be performed from within the Project Editor. Servers and their IP addresses are set up in the Network Addresses dialog in the Project Editor.

This means that physical computers in the system can easily be changed. As long as the IP address or computer name of the new machine is the same as the one being replaced, the new computer will be able to immediately take the same role.

Introduced in Version 7.10:

CitectSCADA 7.10 incorporates the following new features

New Location for Configuration and User Files

To improve the security of your SCADA system and provide compatibility with Windows Vista, CitectSCADA Version 7.10 can now be run under a standard user account (i.e. one without administrator privileges). To achieve this, some modifications to the location of files installed by CitectSCADA have been made. These changes apply to all supported operating systems. Specifically, it is no longer possible for standard users to write to the Program Files or System directories, which means the citect.ini file cannot live in the Bin or Windows directory, and the User folder cannot live under Program Files. It is advisable that you accept the default installation path when installing , or that your chosen User/Data folder is writable by standard users.

File type	Platform	Install Path
Configuration files such as the citect.ini file	Pre- Vista	Documents and Settings/All Users/Application Data/Citect/CitectSCADA 7.10/Config
	Vista	ProgramData/Citect/CitectSCADA 7.10/Config
User directory	Pre- Vista	Documents and Settings/All Users/Application Data/Citect/CitectSCADA 7.10/User
	Vista	ProgramData/Citect/CitectSCADA 7.10/User
Data directory	Pre- Vista	Documents and Settings/All Users/Application Data/Citect/CitectSCADA 7.10/Data
	Vista	ProgramData/Citect/CitectSCADA 7.10/Data
Log files All log files produced by drivers are written to a sub-folder called ‘Drivers’.	Pre- Vista	Documents and Settings/All Users/Application Data/Citect/CitectSCADA 7.10/Logs
	Vista	ProgramData/Citect/CitectSCADA 7.10/Logs

Windows® Integrated Security

In CitectSCADA Version 7.10 you have the ability to incorporate CitectSCADA users and security options with the standard Windows security system. Of course you can still use the CitectSCADA native security if you prefer to define users in the project and logon to CitectSCADA runtime.

Using the integrated Windows security feature, the Windows user can logon to CitectSCADA runtime with runtime privileges configured within the project.

Multi-Signature Support

CitectSCADA 7.10 provides the facility for up to four users to approve an action or tag write operation using the new Cicode functions MultiSignatureForm and MultiSignatureTagWrite.

Two further Cicode functions, VerifyPrivilegeForm and VerifyPrivilegeTagWrite, enable you to restrict access to a specific action or tag write for a user with a specific set of privileges.

Edit .dbf Files in Microsoft Excel

CitectSCADA allows you to edit and save .dbf files (tables) used inCitectSCADA by opening them in Microsoft® Office Excel®.

Microsoft Office Excel 2007 does not allow you to save files in .dbf format though you may open and edit them using the File > Open command. In order to overcome this limitation CitectSCADA now includes an Add-In for Microsoft Excel called ProjectDBFAddIn. When this Add-In is loaded into Excel, it allows you to browse, open, edit and save .dbf files in the correct format.

Enhanced Driver Installation

The installation of CitectSCADA prior to Version 7.10 installed all the available communication drivers automatically with the installation of the product. From Version 7.10 the installation of these drivers is performed at the final stage of the product installation using a separate installation process. This installation process allows you to select individual drivers that you want to install, specific to your system and its I/O Devices.

Note: There are certain drivers that the product installation will install that are required for CitectSCADA to function correctly. These will be installed automatically as in previous releases.

New Font Selection for Graphics Button

In previous releases of CitectSCADA, you were not able to change the properties of text such as font, size, style on buttons in the Graphics Editor. This inability to configure the button text properties led to graphics with text from different source objects having different font settings on the same page, which appears aesthetically untidy and inconsistent on the runtime displays.

From Version 7.10 the text displayed on a button object can be configured in the same manner as other CitectSCADA text objects within the Graphics Editor and the automation interface. This will allow you to present a more polished and consistent user interface to meet individual project runtime presentation requirements.

When migrating from a previous release, button object text properties are preserved and converted to the new button object text properties with the appropriate default property values automatically placed in the new configuration such as Font=Arial, Size=12, Alignment=centre, style=regular, etc.

Microsoft® Windows Vista® Support

CitectSCADA Version 7.10 and later has achieved the Microsoft "Works with Windows Vista" certification. However, merely meeting the requirements of this certification was not sufficient to make CitectSCADA functional on Vista. A number of other changes were required to achieve satisfactory functionality on the Vista operating system.

Version 7.10 satisfies many of the requirements of the "Certified for Windows Vista" certification, and by having this level of qualification we are confident that you will find minimal differences when running the product on the Vista operating system compared to previous operating systems.

New Alarm Field Enhancements

There are two enhancements to alarm fields:

- Runtime writes to custom alarm fields
- Alarm summary field changes
- Alarm display field changes
- Alarm paging

Runtime Writes to Custom Alarm Fields

It is now possible to write to the eight custom alarm fields during runtime. In previous releases these fields could really only be used for alarm filtering.

Alarm Summary Field Changes

Alarm Summary Fields can now be used to format an alarm display or alarm log device. In addition any Alarm Display Field can be used in your alarm summary, apart from State.

New Alarm Summary Fields

Field Name	Description
{SumType,n}	Type of alarm summary (similar to alarm display "Type").

Alarm Display Field Changes

Now any alarm display field can be used for any type of alarm. Where not applicable for a particular alarm type, zero or an empty string will be displayed.

Alarm Paging

The CitectSCADA alarm facility constantly monitors equipment data and alerts operators of any equipment errors (sometimes called "faults"), or alarm condition. When an alarm is triggered it is displayed on the standard alarm display page. The operator has to be continuously sitting in front of an HMI monitoring the system. CitectSCADA Version 7.10 provides the facility to link alarms with a remote paging system for operators.

Two Alarm Properties have been added to enable CitectSCADA to interface with any third-party paging system. The Paging property is a flag to indicate that the alarm is going to be paged, the PagingGroup property is a freeform text field indicating the sequence of people to notify in the event the alarm occurred.

See your third-party paging system documentation for information on how to interface with CitectSCADA.

New Time Synchronization Service

In order to maintain time synchronization CitectSCADA Version 7.10 installs a Windows service called TimeSyncService, which runs under the built-in LocalSystem account. This replaces the existing time synchronization server which is not compatible with Windows Vista. This purpose of this service is to maintain the time on the local computer against one or more time sources.

A Time synchronization utility is provided by CitectSCADA to assist you to configure time synchronization, and control the service as part of your administration environment. This utility requires administrator rights as it configures and controls a windows service. When run on Windows Vista with User Access Control (UAC) on, you will be prompted to elevate to an administrator. When run on earlier operating systems, the utility will exit after displaying a message if the current user is not an administrator on the local machine.

Cicode Functions From Version 7.0

Changes have been made to Cicode functions from CitectSCADA Version 7.0 onwards. These changes incorporated functions that have been added, modified or made redundant. For a detailed explanation of these changes refer to the “What's New in CitectSCADA” topic of the CitectSCADA online help.

Introduced in Version 7.20:

Improved Installation process

The installation process of CitectSCADA has been improved to simplify the operation and guide the user through the installation by use of Installation Profiles and the creation of default component selections. Whilst still allowing for complete flexibility for the experienced user, the complexity and multiple installation paths and options have been greatly reduced. The installer has been enhanced to allow the installation of a runtime-only version of the product. This allows the runtime environment to be installed without the project tools of the CitectSCADA Integrated Environment. The Runtime Only installation provides not only a smaller installation footprint but also the ability to set up workstations which do not allow project configuration. This automatically improves the security of the system configuration.

Control SCADA Client Connections

Two Citect.ini parameters determine how a client will behave should it be unable to maintain a connection with a primary Alarms, Reports or Trends server. Each server type has access to these parameters:

[Type.<ClusterName>.<ServerName>]Priority
and
[Type.<ClusterName>.<ServerName>]DisableConnection

where Type is the relevant server type (Report, Trend or Alarm).

Dynamically Optimized Writes

Following the move to the new Publish-Subscribe infrastructure with Version 7.0, a number of customers were adversely affected by a change in the way the product behaves in respect to combining multiple writes together. This change is generic across ALL drivers and specific issues have been raised with in regard to HITACHI, MODBUS and OPC.

In Version 7.20 changes have been made to the way that writes are performed at the I/O Server in order to restore the pre-version 7.0 behavior.

These changes result in a similar level of blocking as occurred in previous versions. It does not guarantee that writes will be blocked, but it is more than likely that they will be if they are initiated close enough together.

This will also allow use of the re-instated Citect.ini parameter [IOServer]BlockWrites in order to choose whether to use the Block Writes functionality.

Graphics Enhancements

Enhancements have been made to how you can configure graphic pages and the objects you place on the page. These enhancements can be used in the creation and implementation of Genies and Super Genies.

Improved Security

Security enhancements have been implemented in this release to address known security issues from previous versions and to reduce the potential risk of malicious attack. These security enhancements include, improved inter-operability through the introduction of new INI parameters, trusted network authentication, and the addition of assigning roles to runtime users, as you currently do for Windows users.

New Example Project

The Example Project has been updated to demonstrate the new tab menu templates that are available with Version 7.20.

The project includes a "What's New?" menu to introduce some of the new features offered. This menu links to pages that demonstrate:

- the use of tag extensions and tag properties on graphics pages
- server monitoring and the ability to implement online changes for alarm and trend servers
- multi-monitor support
- Instant Trending using the Process Analyst

The new content complements pages drawn in from the existing Example Project and CSV_Example Project, which are now superseded.

To view the new Example Project, select and run it from Citect Explorer. For more information, use the help button included in the project on the main navigation panel.

OFSOPC Driver

The release of CitectSCADA coincides with the availability of the OFSOPC Driver for Schneider Electric's OPC Factory Server (OFS).

OFS is a foundation component for communication with certain Schneider Electric PLCs. The OFSOPC Driver allows CitectSCADA to tightly integrate with OFS, minimizing the amount of configuration required for an end-to-end Schneider Electric system.

You can install the OFSOPC Driver and its supporting documentation via the Driver Selection page of the CitectSCADA installer.

Pelco Camera Support

This feature adds two buttons to the Graphics Builder toolbox, which will allow two of the Pelco Camera ActiveX controls to be easily added to a graphics page. This control provides an ActiveX component that will connect to Pelco IP cameras with configurable bandwidth usage for slow network connections and auto-resizes video to fit the ActiveX control size.

The two ActiveX controls supported are:

Video Streaming - Fully Resizable, multiple bandwidth levels, MPEG4 Video, returns the camera name and model.

Camera Control PTZ (Pan, Tilt and Zoom) - Communicates with DVRs and IP cameras. Featuring pan zoom and tilt, iris, focus, presets, patterns and adjustable speed.

Performance Improvements

The architecture of Version 7Version 7.20 includes a new threading model that offers significant performance improvements. The new Platform Task Framework (PTF) defines an explicit threading environment for each subsystem, providing a standard protocol for work to be created and passed between them.

The performance improvements have been implemented in a way that retains all existing functionality.There is no changes to the configuration or operation of a system, just performance benefits and improved stability.

Persisted I/O Memory Mode

Many customers use DiskPLC I/O devices to provide system-wide global variable tags that are managed by I/O Servers and are persisted to disk to maintain their latest values. DiskPLC I/O devices take advantage of the standard I/O system redundancy features, such that, if one I/O server is unavailable, another can provide client(s) with tag values. They also perform a level of synchronisation by using features such as standby write and by providing redundant paths to the persisted binary data files, so that, at startup of an I/O server, the latest value can be read into the system from the most recently modified data file.

However, there is no synchronisation when network connections are inoperative and regained, resulting in several scenarios in which redundant DiskPLC I/O devices can end up with different values for the same tag.

With Version 7.20, the new feature of persistence when applied to I/O Devices in memory mode, provides an improved alternative to a DiskPLC device, as there is full synchronisation in scenarios involving one of the servers becoming unavailable for a period of time. Persistence is enabled using the Persist field in the extended section of the I/O Devices Properties dialog.

Post Compile Commands

After a project has compiled successfully you can execute an optional command, script or batch file. This offers useful functionality if you have tasks that could be automated after a successful compile. This provides an expansion point for you to add your own script or command to perform additional tasks. You can also launch an optional command, script or batch file to execute after an unsuccessful compile.

Server Side Online Changes

To improve the ability to change configurations on a live system without having to restart the servers, CitectSCADA now provides the facility to reload server configurations during runtime either programmatically or using the Runtime Manager.

Microsoft® Windows 7 Support

CitectSCADA also supports the Microsoft Windows 7 and Microsoft Windows Server® 2008 R2 operating systems. The changes to CitectSCADA undertaken in the 7.10 release to support Windows Vista significantly reduced the changes that were required to support Windows 7 and Windows Server 2008 R2. Previous Vista users will experience no functional differences when migrating to Windows 7. However if you migrate to Windows 7 from Widows XP there are functional differences with CitectSCADA between XP and Vista, as described in “New Locations for Configuration and Project Files” in the CitectSCADA online help.

Supportability Enhancements

Supportability Enhancements have been added to provide easier access to the diagnostics functionality of the product. Although the enhancements were primarily introduced to assist Technical Support personnel with system analysis, they have resulted in many benefits to the end user. These include:

- Timestamp harmonization across all log files.
- Additional [Debug] parameters to support category and severity filtering (see Citect.ini Parameters in Version 7.20).
- Support for online logging adjustments using the new SetLogging() and GetLogging() Cicode functions.
- A set of parameters that can be modified while online due to periodic or an on-demand read of the citect.ini file during runtime.

Additionally, the home page of the Computer Setup Editor now includes a link to the Logging Parameters page, which provides comprehensive instructions for the configuration of logging.

New Tab Menu Templates

To improve the user interface of projects and integrate the look and feel with the latest Windows® systems, CitectSCADA now features new templates with a tab style menu system. Main menu items can be represented as tabs along a menu bar, below which subsidiary items are displayed in a ribbon. New projects have the new Tab_Style_Include templates already available to them.

Tag Extensions

With the addition of Tag Extensions in Version 7.20, the variable tag can now represent data as a collection of elements, and each of these elements can contain a collection of items. For example, the tag variable data received from the PLC can be represented as the “Field”or "Valid" element, which contains the following items within the "VQT Tag Element":

v - the value of the tag.

vt - the timestamp of when the value last changed.

q - the quality of the value , GOOD, UNCERTAIN or BAD. The Quality variable can be further identified using Cicode QUALITY functions.

qt - the timestamp of when the quality last changed.

t - the timestamp of when the element was last updated.

The Migration Process

⚠ WARNING

UPGRADE ALTERS COMMUNICATIONS CONFIGURATIONS
After upgrading, confirm and adjust the configuration of all I/O devices in your project.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

There are a number of considerations for you to make before migrating your projects to CitectSCADA Version 7.20 from Version 6.x. These considerations relate primarily to the introduction of new features, or changes to existing functionality, as described earlier.

The following list identifies the changes which will have low impact on your existing CitectSCADA Version 6.x projects when they are migrated to this version. These changes can optionally be incorporated into your existing projects during later development, or may be ignored if they are of no benefit to the way that CitectSCADA is used in your organization.

Low Impact Changes

- Improved Support for Clustering
- Online Changes for Clients
- New Communications Architecture
- Memory Mode for Devices
- Persist Mode for Devices
- Improved Hardware Alarms
- Event Driven Cicode
- Windows® Integrated Security
- Multi-Signature Support
- Edit .dbf Files in Microsoft Excel
- New Font Selection for Graphics Button
- New Alarm Field Enhancements
- Runtime Writes to Custom AlarmFields
- Alarm Summary Field Changes
- Alarm Display Field Changes
- New Time Synchronization Service
- Improved Installation process
- Control SCADA Client Connections
- Dynamically Optimized Writes
- Graphics Enhancements
- New Example Project
- OPC Factory Server (OFSOPC) Driver
- Pelco Camera Support
- Performance Improvements
- Persisted I/O Memory Mode
- Post Compile Commands
- Server Side Online Changes
- Supportability Enhancements

- Tab Menu Templates
- Tag Extensions

Note: It is optional for you to utilize the extensive capability of clustering, however, after you have installed CitectSCADA Version 7.20 you need to create a minimum of one cluster. For details on creating a cluster refer to the “Upgrading Procedure” topic in the CitectSCADA online help after you have installed the product.

Changes Impacting Migration

The following list identifies functionality changes that may impact migration of your existing projects to CitectSCADA Version 7.20.

- Network Support
- Local Variables
- Publish Alarm Property
- Dual Network Support
- Project-Based Network Configuration
- Parameters and Cicode Functions
- New Location for Configuration and User Files
- Enhanced Driver Installation
- Windows Vista® Support
- Microsoft® Windows 7 Support
- Improved Security

In order to understand any implication these changes in functionality may have on your existing projects, refer to the “Upgrading to CitectSCADA Version 7.20” topic in the CitectSCADA online help after you have installed the product.

Migration Aids

In order to assist in the migration of your existing projects CitectSCADA provides two migration aids. One aid is an automatic update of the project database, the other is a manually invoked Migration Tool.

Automatic Update

The automatic update is carried out when you initially launch CitectSCADA Version 7.20. This update is a passive action which typically updates the database field definition for any database that has been changed between the two versions and copies new files that are needed in Version 7.20. Prior to the automatic upgrade proceeding you are given the option of cancelling the upgrade. The upgrade can be invoked at a later time by adjusting the Update parameter in the Citect.ini file.

Migration Tool

The Migration Tool is a separate application which needs to be manually run after the automatic upgrade has been executed, and initiated by you after you have prepared the project for final migration. This tool will accommodate many of the changes in project functionality which are incorporated in Version 7.20.

It is necessary for you to prepare your existing projects for a successful upgrade using this tool. For details on the Migration Tool, and the preparatory steps for you to make prior to its use, refer to the “Migration Tool” topic in the CitectSCADA online help after you have installed the application.

Upgrading a Runtime-only Installation

You can upgrade a runtime-only installation of CitectSCADA to a full installation that incorporates the configuration environment by simply running the installer again and selecting the **All Core Components** option from the Installation Profiles page.

However, if a project has been restored and operated under the runtime-only environment, it will not automatically appear in Citect Explorer following the upgrade to a full installation.

If you would like to add a missing project to Citect Explorer, you can use the **Add Project Link** feature, accessible via the **File** menu. You can select the required project from the Add Project Directory dialog when it appears.

Chapter 3: Installation Description

Before you begin the installation of CitectSCADA, you need to first decide which components you want to install. This is determined by the functionality you want the installation to support.

After you have decided on the CitectSCADA environment, and any additional stand alone components that you want to install, refer to Chapter 4, Installation Requirements, so that your hardware and system software meet the requirements for your selected installation.

Once you have progressed through the preliminary dialogs of the installation interface, you will be requested to begin selecting the components that you want to install. The options that the installation interface will present to you are described below.

Task Selection Dialogs

Installation Profiles

The installer provides a set of profiles to help you select the appropriate components for installation. Depending on the profile that you choose, the next dialog will have default selections recommended for installation. You may accept the default components, or select the ones of your choice on the components selection screen which is displayed after you click Next on the Installation Profiles dialog.

The options are:

- All Core Components
- Runtime Only Server
- Runtime Only Client
- Custom

The **All Core Components** option will select the .Net Framework 3.5 SP1 (if not installed), Configuration Environment, Runtime, Drivers and Sentinel Driver for installation. It is a “Complete” installation which will install a fully functional CitectSCADA development and server/client system. Such an installation will include the CitectSCADA development environment, runtime infrastructure files, Client, I/O Server, Alarm Server, Trend Server and Reports Server. Select this option if this is an initial installation of CitectSCADA which will run as a single system, or act as a server to service a number of client installations.

The **Runtime Only Server** option will select Runtime, Sentinel Driver and Communications Drivers for installation. It is an installation which will install the runtime components for both a Server and Client. Such an installation will include runtime infrastructure files, Client andI/O Server, Alarm Server, Trend Server and Reports Server.

Select this option if this is an installation of CitectSCADA which will act as a server to service a number of client installations.

The **Runtime Only Client** option will only select the Runtime system for installation. It is an installation which will install the runtime components and a Client. Such an installation will include runtime infrastructure files, but will exclude drivers.

Select this option if this is an installation of Vijeo Citect which will be used as a client.

If you wish to upgrade either of the Runtime installations to a full installation, including the Development and Configuration environment, insert the original installation media and select “All Core Components” or “Custom” from the Installation Profiles dialog.

Note: You can also install the CitectSCADA Runtime Only Client from a single installation file. This file is named CitectSCADA 7.20.exe and located in the <discmedia>\CitectSCADA 7.20\Extras\Runtime Installer folder of the installation DVD. This allows installation of the software to computers which only need the runtime. The file can be copied to a network location for remote installation

The single-file installation does not include Communication Drivers, the Sentinel Driver, or the Microsoft® .NET Framework which is a prerequisite of the runtime. If the .NET Framework is not already installed on the target computer, you cannot use the single-file installation. In this case, you may use the full package installer to automatically install the .NET Framework during the installation of CitectSCADA. Alternatively you can install .NET Framework from another source, then carry out the single file runtime installation.

The **Custom** option will not select any components for installation; it will allow you to select the core components that you specifically need, or allow you to install Add-ons or documentation only.

Documentation Installation

The Product Documentation option will install a comprehensive library of user guides and references in Adobe Portable Document Format (PDF). These can be accessed from a master contents HTML page.

It is highly recommended that you install the product documentation for future reference.

The Knowledge Base option will install the CitectSCADA Knowledge Base. This is a progressively growing library of technical articles written to support CitectSCADA users. It contains the latest information about CitectSCADA, including answers to questions raised by users, solutions to problems, and general discussions.

Add-ons Installation

Once you have selected the components that you want to install, the next dialog allows you to select any Add-ons that you wish to use in your installed system..

The options are:

- Project DBF Add-in for Excel™
- Web Server for IIS
- Driver Update Tool

The **Project DBF Add-in for Excel** option will install an Add-In for Microsoft Excel. When this Add-In is loaded into Excel, it allows you to browse, open, edit and save CitectSCADA .dbf files in the correct format. This is only available for selection if Microsoft Excel 2003 or above is installed on the computer. Otherwise, it is visible but is deselected and disabled.

The **Web Server** option will install a Web Server running on Microsoft Internet Information Service (IIS). The Web Server performs the server-side functionality of a Web Service to the Web Client. As well as facilitating communication, it directs a client to the graphical and functional content of a CitectSCADA project and the location of the runtime servers. This information is stored on the Web Server when a CitectSCADA project is deployed. A Web Server can contain multiple deployments.

Note: If the Web Server and CitectSCADA runtime server are set up on different machines, and it is not possible to establish a trust relationship between them, the two machines need to be on the same domain so that the Web server can access the directory on the CitectSCADA server that's hosting the web deployment files. If, conversely, a trust relationship can be established between the Web Server and the CitectSCADA server, they can be on different domains as long as the Web server has read access to the project folder on the CitectSCADA server.

The **Driver Update Tool** option will install the CitectSCADA Driver Update Tool, an on line system which scans the computer on which it is run, identifies the drivers in use and contacts the Citect DriverWeb to find updated versions that are available. You can then choose which drivers you want to up¬date.

Communication Drivers

CitectSCADA communicates with many control or monitoring I/O Device that has a communication port or data highway - including PLCs (Programmable Logic Controllers), loop controllers, bar code readers, scientific analysers, remote terminal units (RTUs), and distributed control systems (DCS). This communication takes place with each device through the implementation of a communications driver. It is important that these drivers are the latest version. Use the CitectSCADA Driver Update Tool to maintain your drivers at the latest release level.

The installation of CitectSCADA prior to Version 7.10 installed all the available communication drivers automatically with the installation of the product. From Version 7.10 the installation of these drivers is performed at the final stage of the product installation using a separate installation process. This installation process allows you to select individual drivers that you want to install, specific to your system and its I/O devices. There are certain drivers that the product installation will install that are necessary for CitectSCADA to function correctly. These will be installed automatically as in previous releases.

Only install drivers which are identified as being compatible with the computers operating system. If you select any driver that is not yet identified as being compatible, or is specifically identified as not compatible, the installation process will provide an alert to that effect, and will allow you to deselect the driver prior to continuing with the installation.

⚠ WARNING

INCOMPATIBLE DRIVERS

Do not ignore alerts during driver installation. If you choose to ignore such alerts, the driver will be installed but may operate incorrectly.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The communication driver installation can also be invoked individually at any time after the product installation to install additional drivers.

Chapter 4: Installation Requirements

This chapter describes the requirements for hardware, operating system software and system configuration prior to installing CitectSCADA and any of its components.

These requirements will vary subject to the components of CitectSCADA that you want to install on any computer. Refer to Chapter 3, Installation Description, to determine the components that you want to install. This chapter identifies the basic hardware and system software requirements, as well as requirements specific to each particular component.

Before you begin to install CitectSCADA it is important that you install the latest updates from Microsoft® for your operating system and system software.

All Core Components

System Hardware

The following tables indicate the computer hardware requirements for the CitectSCADA “All Core Components” installation and all optional components.

Description	Minimum Specification
Processor	Intel Pentium 3
Processor Speed	1 GHz
Random Access Memory (RAM)	500MB or 1GB if running Windows Server 2003 or 2008, or if running a Web Server (2GB if running both Windows Server and a Web Server)
Available Disk Space	80GB, or 160GB if running a Web Server
Graphics Adapter (see note below)	With 64MB of VRAM if using Process Analyst

Description	Recommended Specification or Higher
Processor	Intel Pentium 4
Processor Speed	3.2GHz
Random Access memory (RAM)	2GB for all supported operating systems, or 3GB if running a Web Server
Available Disk Space	160GB, or 250GB if running a Web Server
Graphics Adapter (see note below)	With 128 MB of VRAM if using Process Analyst

Note: Due to limitations in the Computer Setup Editor, Project Editor and several input forms in CitectSCADA it is a requirement to set the screen resolution at 1024 by 768 pixels or higher.

System Software

The following table indicates the system software that is needed on any computer onto which you want to install the CitectSCADA "All Core Components" installation and all optional components..

CitectSCADA Component	Minimum System Software
All Core Components	Operating System Windows 2000 with Service Pack 4 or Windows XP Professional with Service Pack 2 or Service Pack 3 - (32 Bit and 64 Bit) or Windows Server 2003 Standard Edition with Service Pack 1- (32 Bit and 64 Bit) or Windows Server 2008 Standard Edition with Service Pack 2- (32 Bit and 64 Bit) or Windows Vista with Service Pack 2 (32 Bit and 64 Bit) or Windows 7 (32 Bit and 64 Bit) and Microsoft .NET Framework 3.5 with Service Pack 1(installed with CitectSCADA if not already installed). Internet Explorer Version 6.0 or greater. A Local Area Network (LAN) if you want to have the client access a remote server. If running under virtualization with VMWare, the minimum system requirement is VMWorkstation 6.03 and later. **Note:** Due to compatibility issues between VMWare Workstation and the SafeNet Sentinel hardware protection key, CitectSCADA cannot run in a virtualized 64 bit environment.
CitectSCADA WebServer	As for CitectSCADA All Core Components with the addition of: A LAN running TCP/IP and Microsoft Internet Information Services (IIS) See Microsoft IIS Compatibility for information.
CitectSCADA Knowledge Base	As for All Core Components.
Product Documentation	As for All Core Components.
CitectSCADA Driver Update Tool	As for All Core Components.
Project DBF Add-in for Excel	As for All Core Components, and Microsoft Excel 2003 or 2007.
CitectSCADA Driver Update Tool	As for CitectSCADA Server.

Note: Use an NTFS file system on the target drive for the Web Server software, otherwise you won't have effective access to the necessary Windows security settings (that is, the Folder Properties dialog will not have a Security tab). If you are currently using a FAT/FAT32 system, convert the drive to NTFS before installing the Web Server software.

Microsoft IIS Compatibility

For correct operation of the WebServer, install the appropriate Microsoft Internet Information Services (IIS) feature for your operating system:

- For Windows XP install IIS v5.0
- For Windows Server 2003 or 2008 install IIS v6.0
- For Windows Vista and Windows 7 install IIS v7.0 and follow the Microsoft documentation for IIS7 to install the following components:

Component	Install?
- FTP Publishing services	no to all
- Web Management Tools	yes
- IIS6 Management Compatibility	yes
- IIS6 management console	no
- IIS6 Scripting tools	no
- IIS6 WMI Compatibility	no
- IIS6 Metabase and IIS6 Configuration compatibility	yes
- IIS Management Console	yes
- IIS Management scripts and tools	no
- IIS Management Service	yes
- World Wide Web services	yes
- Application Development Features	yes
- .NET Extensibility	yes
- ASP	yes
- ASP.NET	yes
- CGI	no
- ISAPI Extensions	yes
- ISAPI Filters	yes
- Server-Side Includes	no
- Common Http features	yes to all
- Health and Diagnostics	no to all
- Performance features	no to all
- Security	yes
- Basic Authentication	no
- Client Certificate Mapping authentication	no
- Digest Authentication	no
- IIS Client Certificate Mapping authentication	no
- IP Security	no
- Request filtering	yes
- URL Authorization	no
- Windows Authentication	yes

Note: In the above table, 'yes' means the feature is essential or recommended for the WebServer installation and 'no' means the feature is optional or not relevant to the WebServer.

System Software

The following table indicates the system software that is needed on any computer onto which you want to install the CitectSCADA Control/ View-only Clients and its optional components.

CitectSCADA Component	Minimum System Software
CitectSCADA Control / View-only Client	Operating System: Windows 2000 with Service Pack 4 or Windows XP Professional with Service Pack 2 and Service Pack 3 (RC2) - (32 Bit and 64 Bit) or Windows 2003 Standard Edition with Service Pack 1 or Windows Server 2008 Standard Edition with Service Pack 1 or Windows Vista with Service Pack 2 (32 Bit and 64 Bit) or Windows 7 (32 Bit and 64 Bit) and Microsoft .NET Framework 3.5 with Service Pack 1 (installed with CitectSCADA if not already installed). Internet Explorer Version 6.0 If running under virtualization with VMWare, the minimum system requirement is VMWorkstation 6.03 and later. **Note:** Due to compatibility issues between VMWare Workstation and the SafeNet Sentinel hardware protection key, CitectSCADA cannot run in a virtualized 64 bit environment.

Runtime Only Server or Client

Hardware Requirements

The following tables indicate the computer hardware requirements for the CitectSCADA Runtime Only Server or Client installation.

Description	Minimum Specification
Processor	Intel Pentium 3
Processor Speed	1 GHz
Random Access Memory (RAM)	500MB or 1GB if running Windows Server 2003 or 2008, or if running a Web Server (2GB if running both Windows Server and a Web Server)
Available Disk Space	80GB, or 160GB if running a Web Server
Graphics Adapter (see note below)	With 64MB of VRAM if using Process Analyst

Description	Recommended Specification or Higher
Processor	Intel Pentium 4
Processor Speed	3.2GHz
Random Access memory (RAM)	2GB for all supported operating systems, or 3GB if running a Web Server
Available Disk Space	160GB, or 250GB if running a Web Server
Graphics Adapter (see note below)	With 128 MB of VRAM if using Process Analyst

System Software

The following table indicates the system software that is needed on any computer onto which you want to install the CitectSCADA Runtime Only Server or Client.

CitectSCADA Component	Minimum System Software
All Core Components	Operating System Windows 2000 with Service Pack 4 or Windows XP Professional with Service Pack 2 or Service Pack 3 - (32 Bit and 64 Bit) or Windows Server 2003 Standard Edition with Service Pack 1- (32 Bit and 64 Bit) or Windows Server 2008 Standard Edition with Service Pack 2- (32 Bit and 64 Bit) or Windows Vista with Service Pack 2 (32 Bit and 64 Bit) or Windows 7 (32 Bit and 64 Bit) and Microsoft .NET Framework 3.5 with Service Pack 1(installed with CitectSCADA if not already installed). Internet Explorer Version 7.0 or greater. A Local Area Network (LAN) if you want to have the client access a remote server. If running under virtualization with VMWare, the minimum system requirement is VMWorkstation 6.03 and later. **Note:** Due to compatibility issues between VMWare Workstation and the SafeNet Sentinel hardware protection key, CitectSCADA cannot run in a virtualized 64 bit environment.
CitectSCADA WebServer	As for CitectSCADA All Core Components with the addition of: A LAN running TCP/IP and Microsoft Internet Information Services (IIS) See Microsoft IIS Compatibility for information.

Software Licensing

CitectSCADA uses a hardware key to help manage the software licensing. The hardware key is a physical key that plugs into either the parallel port or USB port of your computer. The hardware key contains details of your user license, such as type and I/O point limit.

Updating Your Hardware Key

When you upgrade to a new version of CitectSCADA, you might need to update your hardware key to enable the system to run. See the CitectSCADA Readme file to confirm whether you need to perform an update.

Updating the hardware key involves running the CitectSCADA Key Update command, which is found in the Help menu of Citect Explorer.

Note: If you have CitectSCADA Version 5.21 or 5.20, run ciusafe.exe from the Citect bin directory. You can also download the latest version of the upgrade program from the AuthCode Generator section of the CitectSCADA website at http://scadasupport.citect.com/.

To update the hardware key:

1. In Citect Explorer choose **Help** | **Citect Key Update**.

   A Key ID is displayed. The hardware key's serial number might also appear. If not, read the serial number from the label on the key.
2. Visit http://www.citect.com/ and enter the serial number as prompted. You might also be asked for the Key ID and your web login name and password.
3. The authorization code is displayed. Type the code (or copy and paste it from the web site) into the **Authorization Code** field in CiUSAFE. Do not use any spaces when entering the characters.
4. Click **Update**.

   The **Return Code** field indicates whether the hardware key was updated successfully. For a detailed explanation of the fields in the **CiUSAFE** dialog, click the **Help** button on the dialog.

Note: Each time you run the CitectSCADA Key Update, a different Key ID is generated, which is normal. If you obtain an authorization code but do not immediately update the hardware key, you can enter the same authorization code the next time you run the update.

CitectSCADA License Point Count

The point limit is the maximum number of I/O device addresses (variable tags) that can be read, and is specified by your CitectSCADA license. CitectSCADA counts all I/O device addresses dynamically at runtime.

This includes all tags used by alarms, trends, reports, events, pages, in Super Genies, use of the TagRead() and TagWrite() Cicode functions, or internal values written to using DDE, ODBC, or the CTAPI.

It does not count any points statically at compile time.

- Dynamic points are counted only once, regardless of how many times they are used.
- At runtime, the dynamic point counts are available through the Kernel and the CitectInfo() Cicode function.
- Existing MEMORY_PLC tags from before Version 7.0 are converted to the new "local variables" during migration. Local variables are stored on the client and resolved on the client and they are not included in the point count.
- When you plan your system you be aware of your point count so that you do not exceed your point limit. This is particularly important, as at runtime, you can incrementally add to your point count by using tags that have not yet been included in the total count.

When you run CitectSCADA at runtime, the dynamic point count is continuously checked against your hardware key. When the total number of dynamic points (at runtime) pushes the total point count above the point license limit, CitectSCADA will refuse to get values for the additional points..

CitectSCADA has two preconfigured 'watermark' messages that will display to the user when the dynamic point count reaches 95% and 98% of their point license limit. You can configure these percentages in the Citect.ini file.

Demo Mode

You can run CitectSCADA without the hardware key in demonstration (Demo) mode. Demonstration mode lets you use all CitectSCADA features normally, but with restricted time and I/O.

The following demonstration modes are available:

- 15 minutes with a maximum of 50,000 real I/O.
- 10 hours with no static points and a maximum of one dynamic real I/O. This is useful for demonstrations using memory and disk I/O. CitectSCADA starts in this mode if no static points are configured.
  If you want to demonstrate DDE, CTAPI, or ODBC writes to CitectSCADA in this mode, you can only write one point. To write to more than one point, force CitectSCADA to start in 15 minute-50,000 I/O demo mode by creating at least one static I/O point.
- For this to work, configure a real variable tag, with an accompanying PLC or I/O device. Use the tag by a page or in Cicode. If you do not have a real I/O device connected, CitectSCADA gives a hardware alarm, which you can disable using the IODeviceControl function.

Chapter 5: Installation

The Installation Process

Before proceeding with the installation of CitectSCADA and optional components refer to Chapter 4, Installation Requirements, so that you have the necessary hardware and system software on the target computer to support the installation. Also refer to Chapter 3, "Installation Description.", which explains the installation process and the options tot make to correctly install the system that you want. Once you have decided which components of CitectSCADA you want to install you can perform the installation process by following the steps below.

Note: Backup your existing projects then uninstall prior versions before installing Version 7.20, as CitectSCADA does not support different versions running side-by-side.

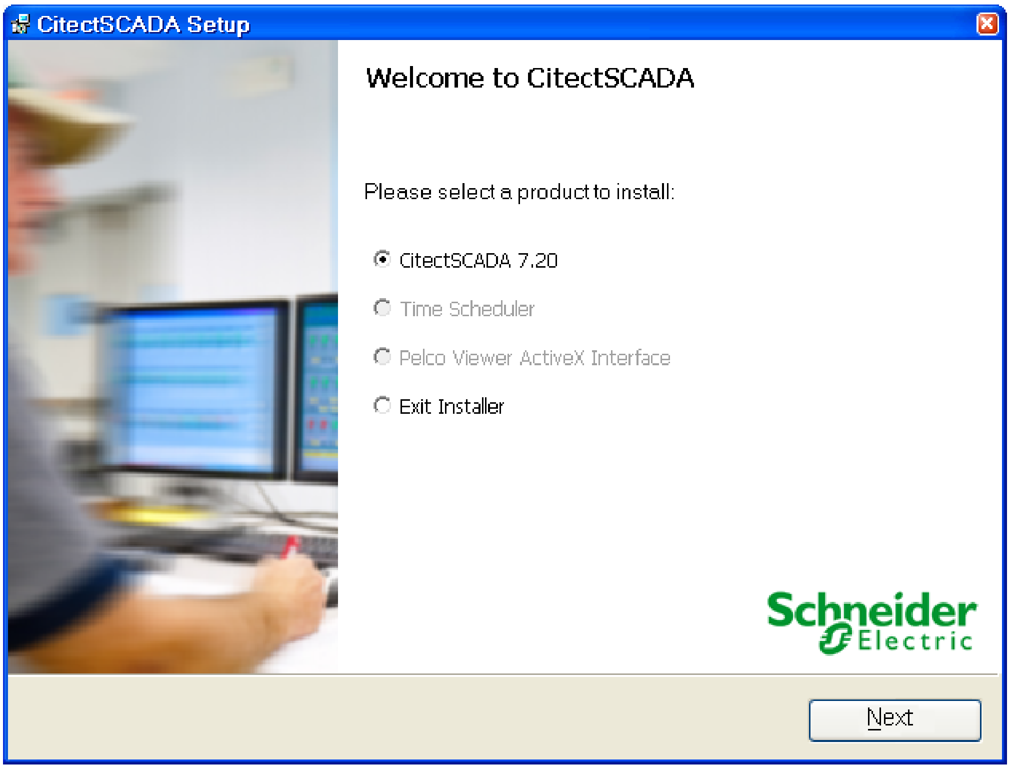
Preliminary Installation

Do not have Windows Update running when attempting to install CitectSCADA.

When you begin the installatiion any additional system software that is necessary will be installed prior to the initial **CitectSCADA Setup** dialog being displayed.

1 To begin the installation, place the CitectSCADA DVD in the DVD drive of your computer. If you have autorun enabled the initial **CitectSCADA Setup** dialog will display. If this does not occur, use Windows Explorer to navigate to the root directory of the

DVD and click Launch.exe to display the initial **CitectSCADA Setup** dialog.



Welcome to CitectSCADA

Please select a product to install:

● CitectSCADA 7.20

○ Time Scheduler

○ Pelco Viewer ActiveX Interface

○ Exit Installer

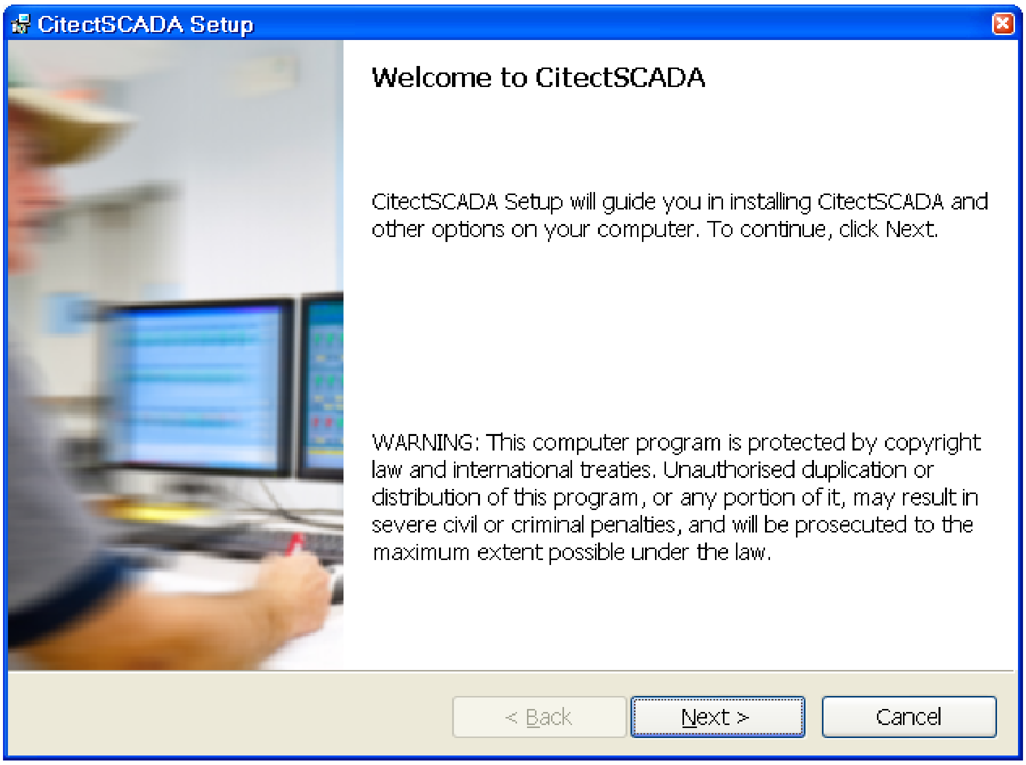
When the **CitectSCADA Setup** dialog is displayed choose which application you wish to install.

The **Pelco ActiveX interface** adds a button to the Graphics Builder toolbox in **CitectSCADA**, which will allow two of the Pelco Camera ActiveX controls to be easily added to a graphics page. If you choose the Pelco ActiveX interface follow the on screen instruction. Full details on the installation for the Pelco ActiveX interface can be found in the Pelco Camera documenation located on the installation DVD.

The **Time Scheduler** is a calendar based programming tool that allows you to manipulate tag values within a CitectSCADA project. It can be used to create a sequence of automatically executed commands, delivering a valuable scheduling tool for applications. If you choose the Time Scheduler follow the on screen instruction. Full details on the installation for the Time Scheduler can be found in the Time Scheduler documenation located on the installation DVD

If you choose the **CitectSCADA** installation, click **Next** to display the **Welcome to CitectSCADA** dialog.

2 When this dialog is displayed, click **Next** to begin the installation process and display the **Welcome to CitectSCADA** dialog.

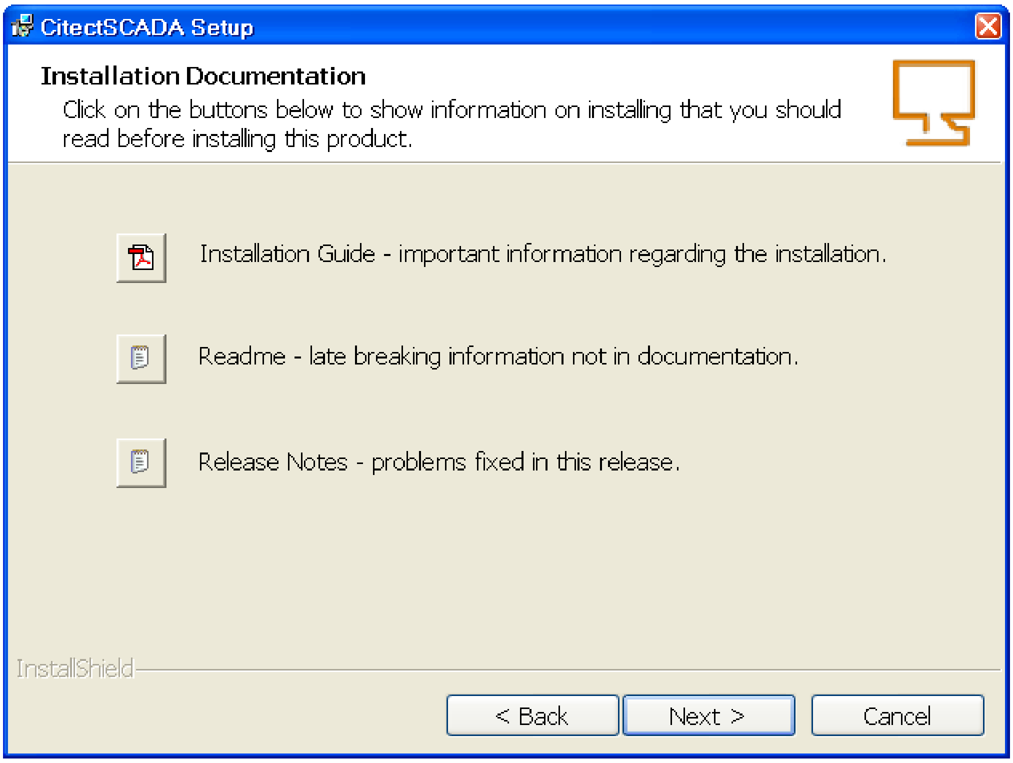


Welcome to CitectSCADA

CitectSCADA Setup will guide you in installing CitectSCADA and other options on your computer. To continue, click Next.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorised duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3 Click **Next** to display the **Installation Documentation** dialog**.** This allows you to read the Installation Guide (this document), the readme file and Release Notes prior to continuing the installation. It is recomended that you read them.



CitectSCADA Setup

Installation Documentation

Click on the buttons below to show information on installing that you should read before installing this product.

Installation Guide - important information regarding the installation.

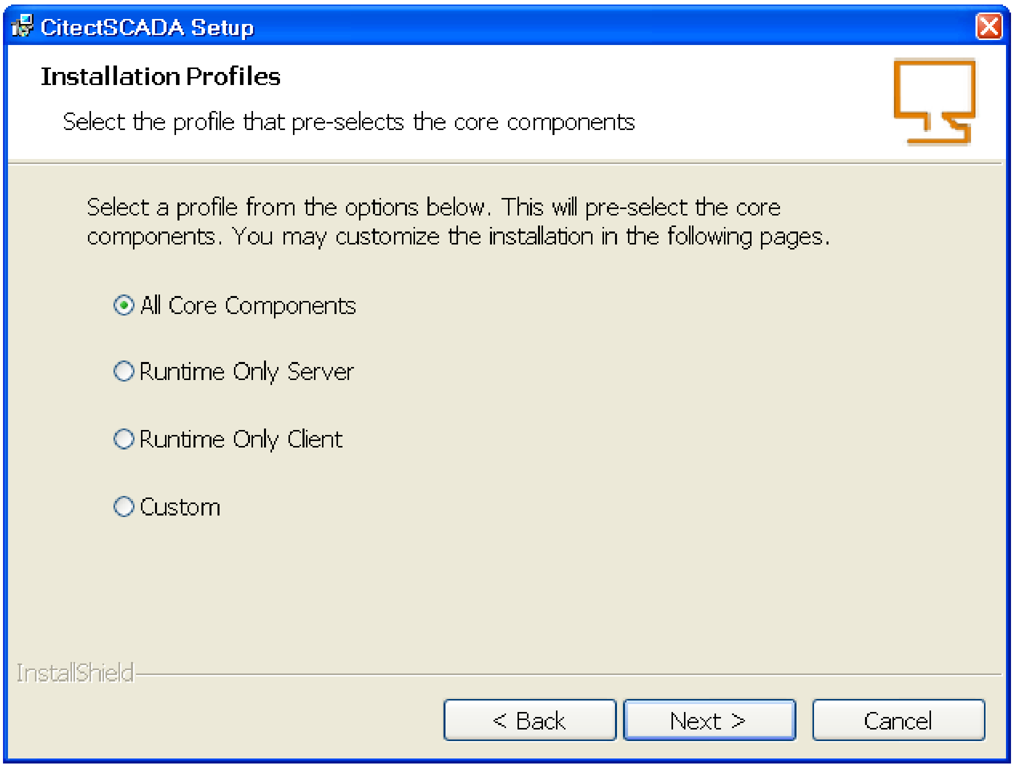
Readme - late breaking information not in documentation.

Release Notes - problems fixed in this release.

4 Click **Next** to display the **License Agreement dialog.** Read the license agreement, and if you accept the terms of the agreement, select the appropriate button, then click **Next** to display the **Installation Profiles** dialog.

Installation Profiles

1 In the **Installation Profiles** dialog select the profile that represents the type of installation that you need. For information on the profiles and their application components refer to Chapter 3, "Installation Description.".



Installation Profiles

Select the profile that pre-selects the core components

Select a profile from the options below. This will pre-select the core components. You may customize the installation in the following pages.

● All Core Components

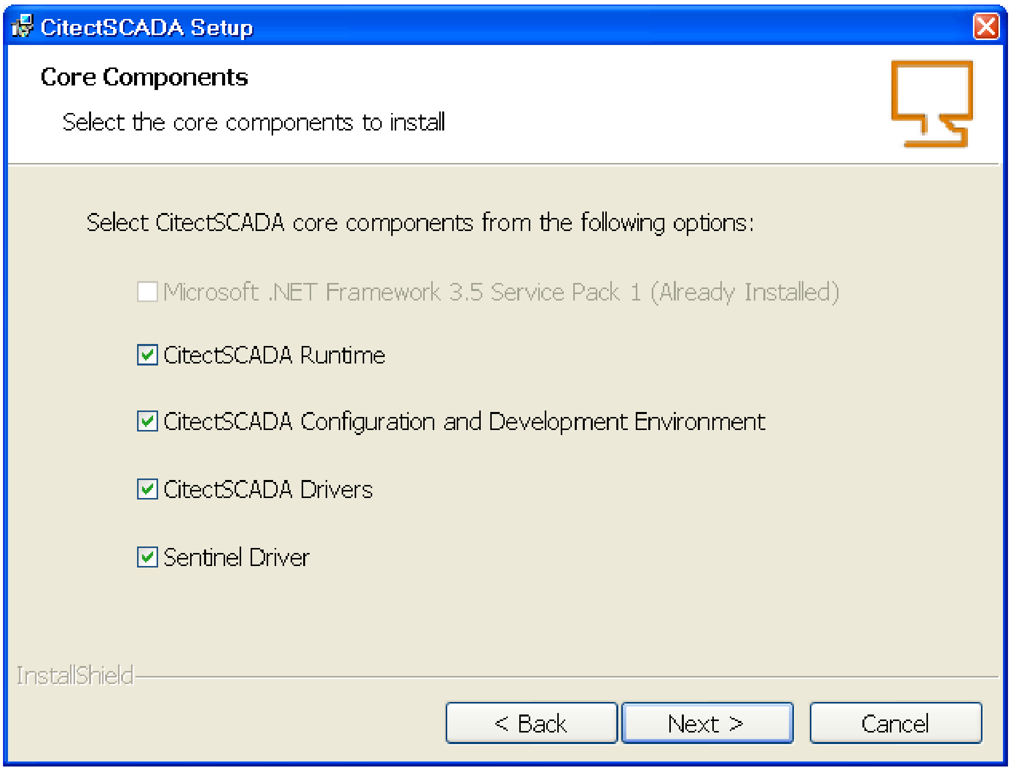
○ Runtime Only Server

○ Runtime Only Client

○ Custom

2 Click **Next** to display the subsequent dialog in the installation sequence. The optional components selected by default in the subsequent dialog will vary subject to the option that you select in this **Installation Profiles** dialog.

As an example, if you selected the **All Core Components** option in the previous step, when you click **Next** the **Core Components** dialog will be displayed and will have all the components selected by default. If you had selected another profile in the previous step, only some of the components will be selected.



CitectSCADA Setup

Core Components

Select the core components to install

Select CitectSCADA core components from the following options:

□ Microsoft .NET Framework 3.5 Service Pack 1 (Already Installed)

☑ CitectSCADA Runtime

☑ CitectSCADA Configuration and Development Environment

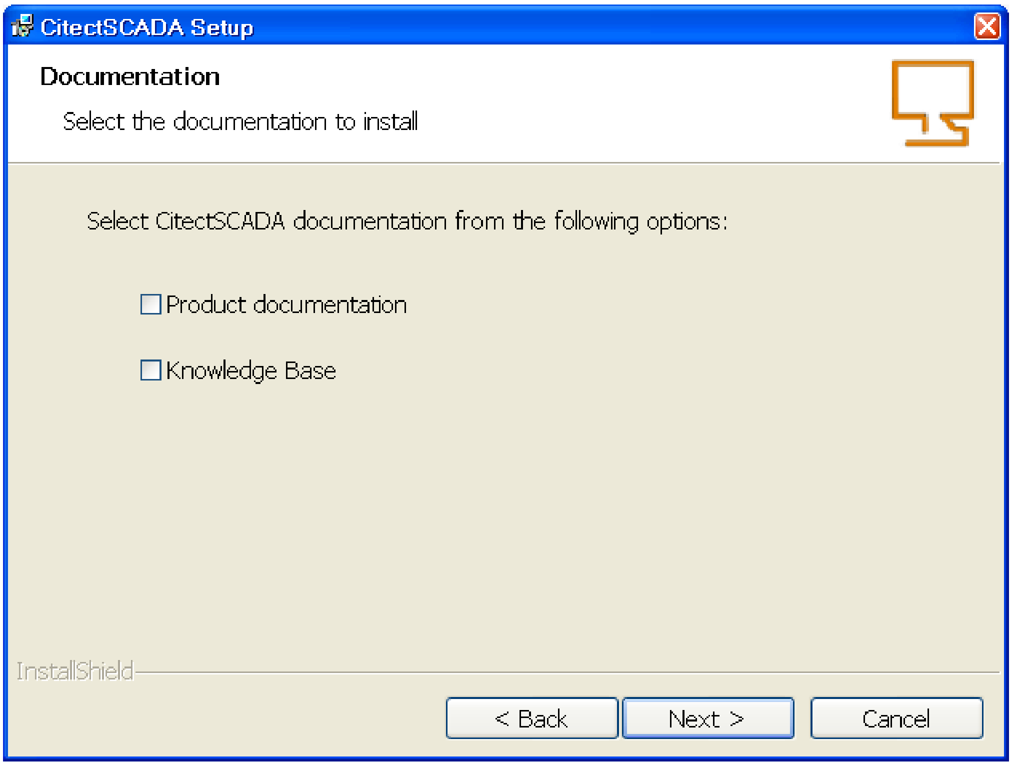
☑ CitectSCADA Drivers

☑ Sentinel Driver

This dialog allows you to change the selected components if you wish to have a different installation configuration from the default provided by the profile which you chose in the previous step. Microsoft® .Net Framework is needed. If this component option is disabled then it is already installed on your system. If it is enabled, select it to continue the installation.

Note: The Sentinel Driver is not necessary on a client that gets a floating license from a server. However if you upgrade from a Runtime installtion to a Configuration and Development Environment you need to select the Sentinel Driver so that the hardware protection key wil be recognized.

3 When you are satisfied with the components that are selected click **Next** to display the **Documentation** dialog



CitectSCADA Setup

Documentation

Select the documentation to install

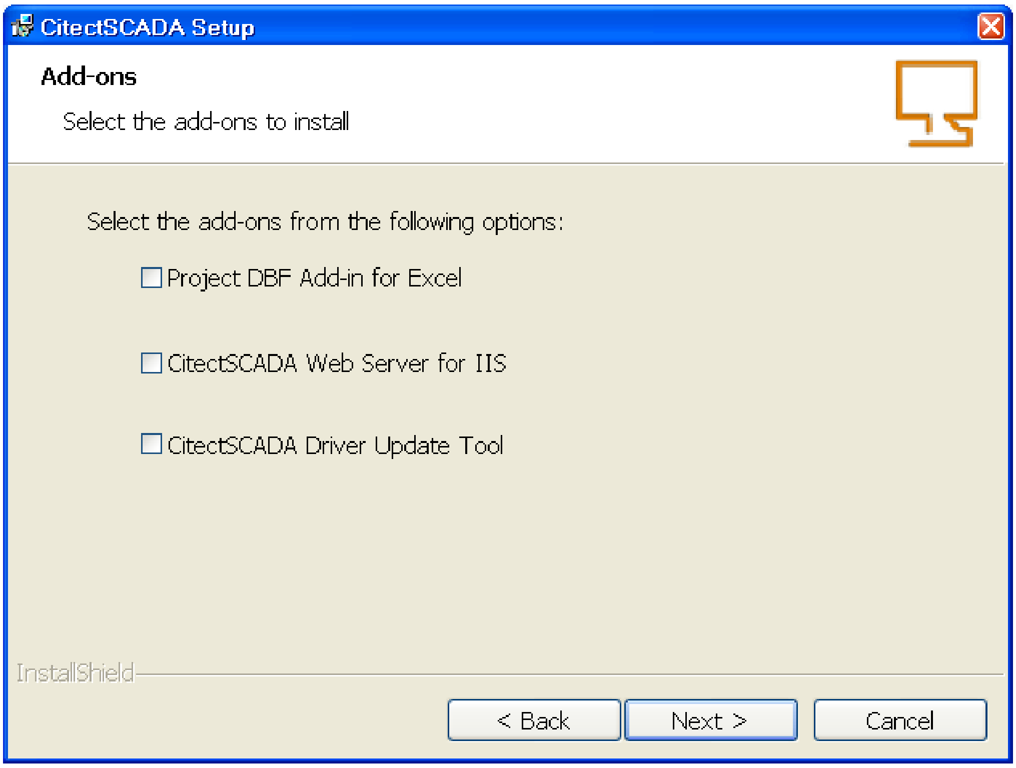
Select CitectSCADA documentation from the following options:

□ Product documentation

□ Knowledge Base

The Documentation dialog allows you to install the Product Documentation and/ or the Knowledge Base.

4 When you have made your selection, click **Next** to display the **Add-on selection** dialog.



CitectSCADA Setup

Add-ons

Select the add-ons to install

Select the add-ons from the following options:

□ Project DBF Add-in for Excel

□ CitectSCADA Web Server for IIS

□ CitectSCADA Driver Update Tool

The Add-on dialog allows you to select specific additional components for your installation.

The options are:

- Project DBF Add-in for Excel™ (Only selectedable if Microsoft Excel 2003 or 2007 is installed on the computer.)
- Web Server for IIS

Refer to Chapter 3, “Installation Description.”, for a description of these optional Add-on components.

The **Web Server on IIS (Internet Information Services)** option will use IIS as a platform for your server.

If you proceed with the Web Server for IIS installation, the installer automatically determines if IIS is installed. An error message is displayed if IIS is not installed. Install IIS before you continue with the Web Server for IIS installation.

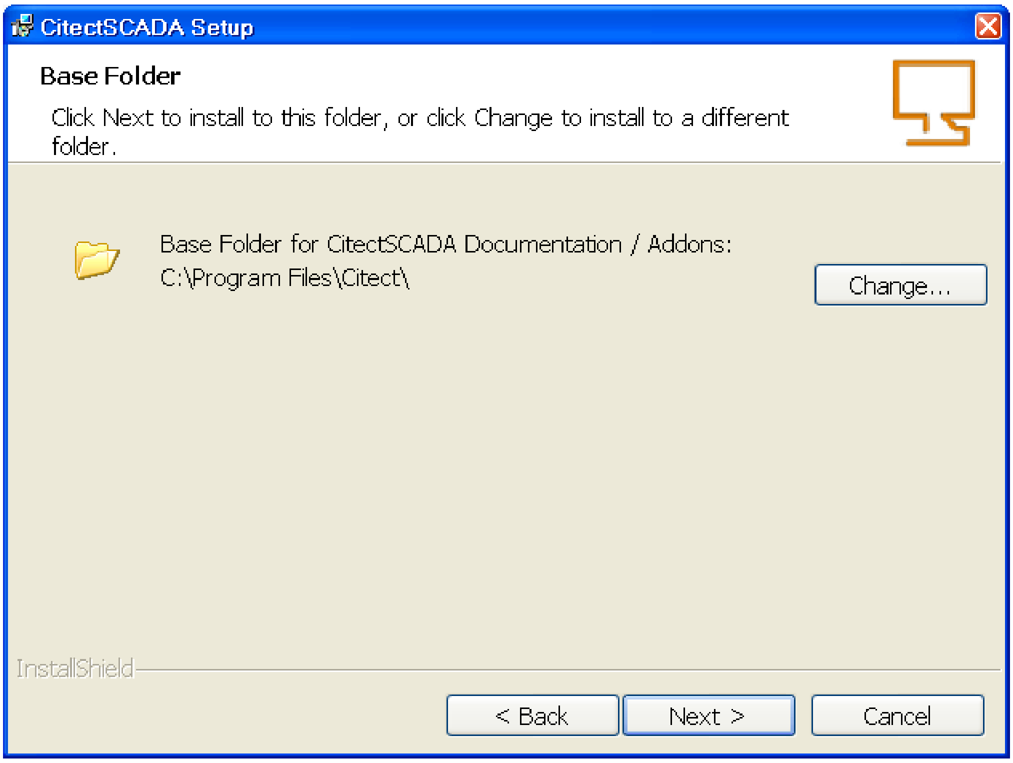
5 Proceed to Completing the Installation.

Completing the Installation

1 The **Destination Folder** dialog identifies the folders into which the CitectSCADA program files you have selected will be installed.

You may change the folder locations by clicking the **Change** buttons and selecting alternative locations.

2 When you are satisfied with the folder selections, click **Next** to display the **Base Folder** dialog.



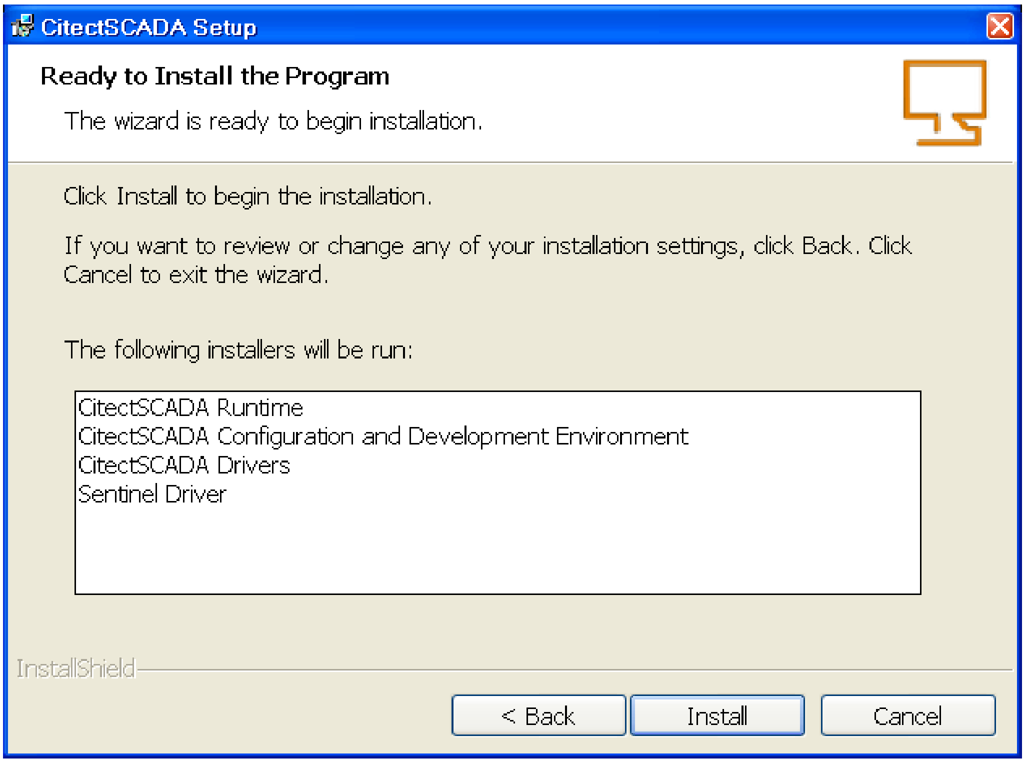
CitectSCADA Setup

Base Folder

Click Next to install to this folder, or click Change to install to a different folder.

Base Folder for CitectSCADA Documentation / Addons:
C:\Program Files\Citect\

The Base Folder dialog identifies the base folder into which the additional or optional components of CitectSCADA that you have selected will be installed. You may change the folder location by clicking the **Change** buttons and selecting an alternative location. If you are satisfied with the folder selection, click **Next** to display the **Ready to Install the Program** dialog.



CitectSCADA Setup

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

The following installers will be run:

CitectSCADA Runtime
CitectSCADA Configuration and Development Environment
CitectSCADA Drivers
Sentinel Driver

The **Ready to Install the Program** dialog lists the CitectSCADA programs that will be installed.

1 Review the list and if you wish to change the selections click the **Back** button through the previous dialog until you reach the selection that you want to change. Click **Install** to install the programs in the list and display the **Installing CitectSCADA** dialog.

2 The **Installing CitectSCADA** dialog displays a progress bar and identifies the status of the installation. You can click **Cancel** if you want to terminate the installation.

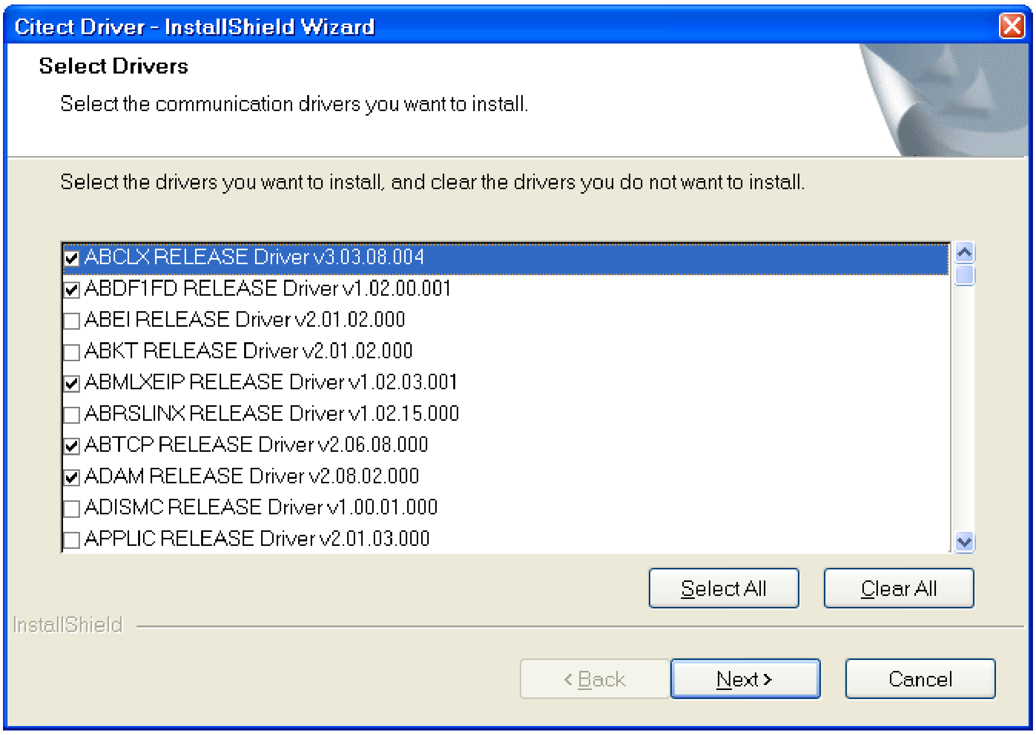
During the course of the final installation you may be asked to confirm certain actions, depending on the additional components that you have selected to install. In such cases follow the prompts on the dialogs.

Communication Drivers

If Vijeo Citect Drivers was selected, the communication driver installation will commence towards the end of the main product installation.

You can also run the communications driver separately at a later time from the user interface or the command line if you want to install additional drivers. For details see Installing Additional Communication Drivers.

Installation of the drivers commences with the drivers being extracted to a temporary folder. The **Driver Selection** dialog will then be displayed**.**



Select Drivers

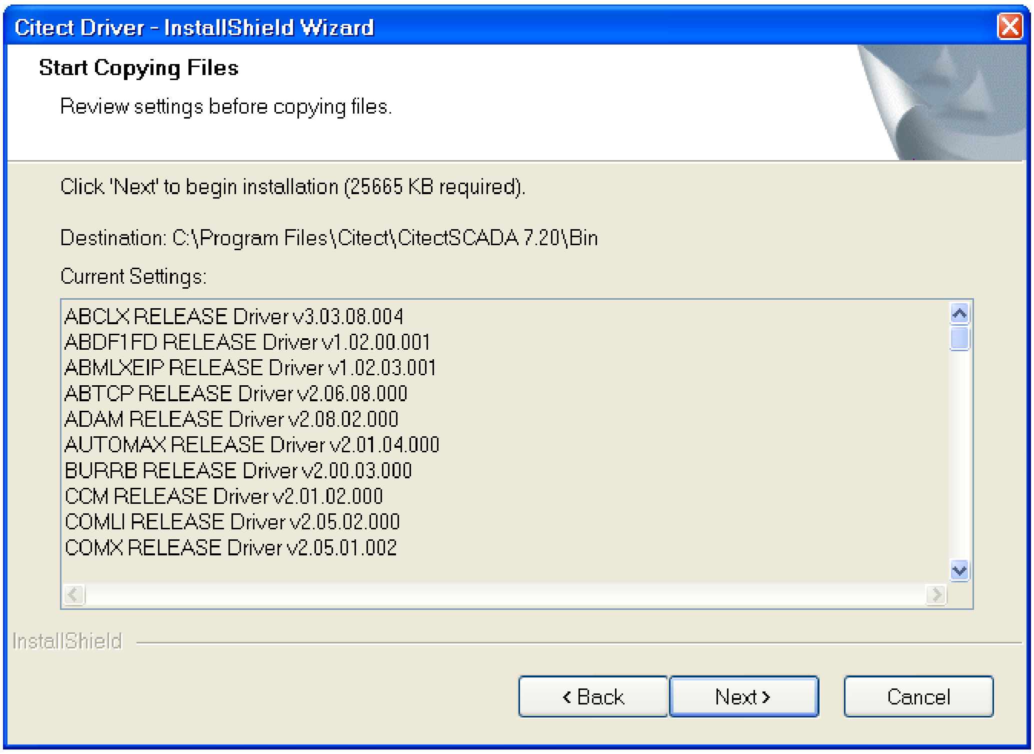
Select the communication drivers you want to install.

Select the drivers you want to install, and clear the drivers you do not want to install.

☑ ABCLX RELEASE Driver v3.03.08.004
☑ ABDF1FD RELEASE Driver v1.02.00.001
□ ABEI RELEASE Driver v2.01.02.000
□ ABKT RELEASE Driver v2.01.02.000
☑ ABMLXEIP RELEASE Driver v1.02.03.001
□ ABRSLINX RELEASE Driver v1.02.15.000
☑ ABTCP RELEASE Driver v2.06.08.000
☑ ADAM RELEASE Driver v2.08.02.000
□ ADISMC RELEASE Driver v1.00.01.000
□ APPLIC RELEASE Driver v2.01.03.000

The **Driver Selection** dialog lists all the drivers that are available for installation. There are certain drivers that the product installation will install that are necessary for CitectSCADA to function correctly. These are not displayed in the list and will be installed automatically as in previous releases. For convenience, the most commonly used drivers are selected by default. In addition it will advise you of any drivers that are time limited or not supported by your operating system. If you see that any of the drivers in the list are subject to limitations, click the Back button and deselect them from the previous dialog.

Select the check box against the drivers that you wish to install, or deselect any that you do not wish to install. You may select all the drivers by clicking the **Select All** button.Then click the **Next** button to display the **Driver Information** dialog.



Start Copying Files

Review settings before copying files.

Click 'Next' to begin installation (25665 KB required).

Destination: C:\Program Files\Citect\CitectSCADA 7.20\Bin

Current Settings:

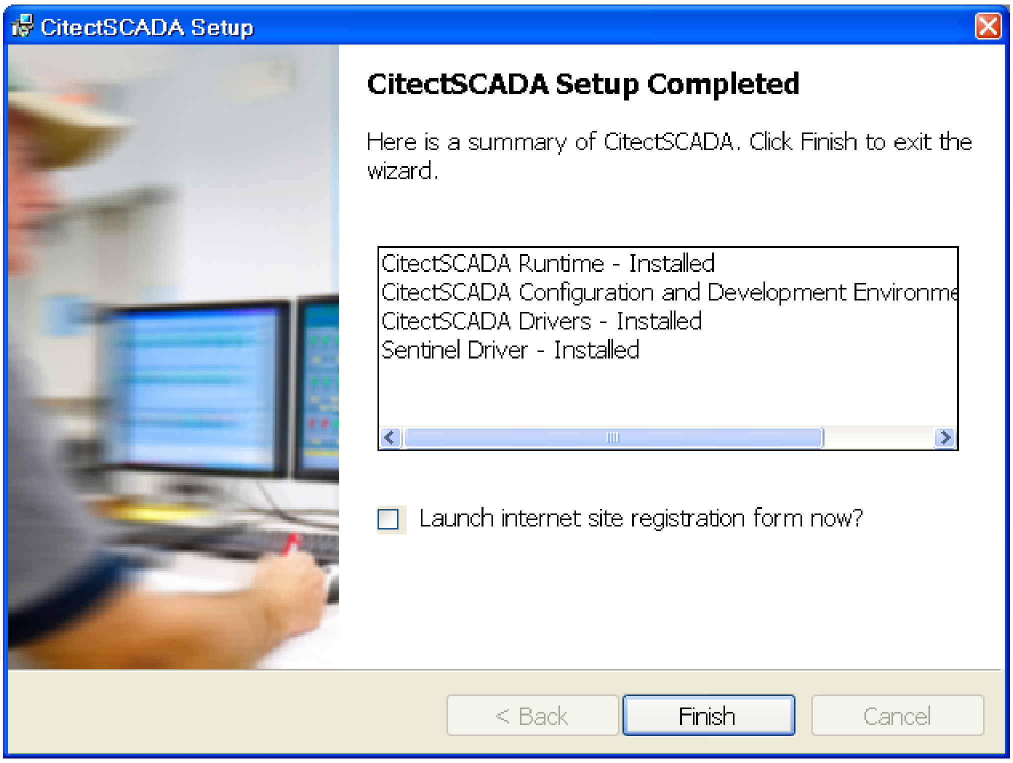
```
ABCLX RELEASE Driver v3.03.08.004
ABDF1FD RELEASE Driver v1.02.00.001
ABMLXEIP RELEASE Driver v1.02.03.001
ABTCP RELEASE Driver v2.06.08.000
ADAM RELEASE Driver v2.08.02.000
AUTOMAX RELEASE Driver v2.01.04.000
BURRB RELEASE Driver v2.00.03.000
CCM RELEASE Driver v2.01.02.000
COMLI RELEASE Driver v2.05.02.000
COMX RELEASE Driver v2.05.01.002
```

The **Driver Information** dialog displays a confirmation list of the drivers that will be installed.

In addition it will advise you of any drivers that are time limited or not supported by your operating system. This operating system support limitation is particularly for the Microsoft® Windows Vista™ or Windows 7 operating system on which some drivers have not yet been confirmed to operate correctly, or have been confirmed specifically to not operate correctly. If you see that any of the drivers in the list are subject to limitations, click the **Back** button and deselect them from the previous dialog, then click **Next** to return to the **Driver Information** dialog. When you are satisfied that the correct drivers will be installed click the **Next** button to install the selected drivers.

3 When the driver installation is finished, any Add Ons that you selected to install earlier will be installed, followed by the main product installation **Setup Completed** dialog. This lists a summary of the programs that have been installed. If you wish to be connected to the Citect on line registration web site select the chek box. Click **Finish** to close the installation

dialog.



CitectSCADA Setup Completed

Here is a summary of CitectSCADA. Click Finish to exit the wizard.

CitectSCADA Runtime - Installed
CitectSCADA Configuration and Development Environme
CitectSCADA Drivers - Installed
Sentinel Driver - Installed

□ Launch internet site registration form now?

The **Setup Completed** dialog lists a summary of the programs that have been installed. If you wish to be connected to the Citect on line registration web site select the chek box. Click **Finish** to close the installation dialog.

Installing Additional Communication Drivers

You can install additional communications drivers at any time after you have installed the main CitectSCADA product.

To install additional drivers:

1 From the Installation DVD, locate the CitectDriverInstaller.exe file in the CitectSCADA Version 7.20\Citect directory.

Note: If you are using the Windows Vista® or above, operating system and have User Account Control (UAC) switched on the UAC dialog will display when you open the file. You will need to supply administrator credentials if you are not an administrator of the computer.

2 Open the file to display the Welcome dialog and follow the steps above in Communication Drivers noting the following additional step.

3 After you have accepted the license agreement an additional **Choose Destination** dialog will display. This will identify the default folder in which to install the drivers. You can accept the default location or change to another folder using the **Browse** button. The installation folder has to contain the citect32.exe file otherwise a warning

message will be generated. In other words the location needs to have an existing CitectSCADA product installed in that location.

4 Click the **Next** button to display the **Driver Selection** dialog and continue with the installation as described in Communication Drivers.

Installing Service Packs

Citect distributes upgrades for current versions of CitectSCADA via Service Packs. A Service Pack is a minor version upgrade of CitectSCADA executable and/or database files. These files are upgraded to provide bug fixes and necessary enhancements. Enhancements are included only when they will aid in more enhanced debugging of CitectSCADA Runtime.

When to install a Service Pack?

A Release Notes document is distributed when Technical Support for this product release a Service Pack. Read the Release Notes and see if it states that a problem you are experiencing has been fixed. If so, then apply the Service Pack. However, do not be apply Service Packs on the premise that they will fix a problem not stated in the readme.

Service Packs include the fixes or enhancements of all previous Service Packs. So, if you are running a released version, and you install Service Pack 3, for instance, you get all fixes and enhancements for Service Pack 1 and Service Pack 2. The Release Notes document for each Service Pack also identifies the fixes or enhancements of the previous Service Packs.

How to install a Service Pack:

1 Download the necessary Service Pack, and the associated Release Notes document from http://scadasupport.citect.com/service-packs.html.

2 Close all CitectSCADA applications. Ideally, close all Windows applications.

3 Follow the installation instructions in the Release Notes document specific to that Service Pack, and to the CitectSCADA components that are installed on your machine.

Modify, Repair, or Remove Components

You can modify, repair or remove installed CitectSCADA components by using the **Windows Add/Remove Programs** (or "Programs and Features" icon in Microsoft Vista).

Note: The CitectSCADA Version 7.20 installation, and the CitectSCADA Knowledge Base can only be removed using this operation. You cannot Modify or Repair these installations. In order to Modify or Repair those particular installations you need to re-install them from the main CitectSCADA installation interface.

To perform a Modify, Repair, or Remove follow these steps.

1 From the **Start** menu select **Settings**, **Control Panel** to display the Control Panel window.

2 Select **Add or Remove Programs** to display the Add or Remove Programs dialog box.

3 Locate the CitectSCADA program on which you want to carry out the operation from the list.

4 If the **Change** button is present, you can modify or repair the installation. If only the Remove button is available you can only remove the installation, to do so click **Remove** and follow the prompts on the dialog.

5 If you click the **Change** button, the CitectSCADA Installation Wizard will display. Click **Next** to display the **Program Maintenance** dialog.

6 On the **Program Maintenance** dialog, click the radio button for the operation that you wish to undertake and follow the prompts on the dialog.

Note: When uninstalling on a computer running the Microsoft Vista operating system and you have User Access Control switched on, the UAC dialog will be displayed before the uninstaller is launched. Select allow and proceed with the uninstallation. This is a limitation imposed by the User Access Control and cannot be avoided.

The available maintenance operations are shown below.

- **Modify** allows you to add CitectSCADA components that were not installed during the original installation, or remove selected components via the Custom Setup dialog. If you select the Modify operation, when you click the Next button the Custom Setup dialog will be displayed.
- **Repair** the existing CitectSCADAcomponent installation by reinstalling all non-customizable files in the same location as the previous installation. If any of the files were accidentally deleted or modified, then this option will restore the software back to its original state.
- **Remove** CitectSCADA component files and remove all the registry entries. This will restore the computer to the state prior to installation of the CitectSCADA component. If you select the Remove operation, when you click the Next button a message box will display requesting that you confirm or cancel the operation. If you confirm the operation, the CitectSCADA component will be uninstalled.

Note: The uninstallation of CitectSCADA does not uninstall the Sentinel Protection Software (used by the hardware protection key), Web Server, or the Project DB Add-in. To uninstall these applications use the same procedure as for uninstalling CitectSCADA, but select the appropriate installer from the list displayed in the Add or Remove Programs dialog, then follow the on screen instructions.

Uninstall a Service Pack

When a Service Pack is installed, a backup directory is created. This backup directory structure mirrors the CitectSCADA directory including all subdirectories. Files that were replaced during the Service Pack installation will be backed up in these directories.

To uninstall a Service Pack:

1 Close all CitectSCADA for Windows applications. Ideally, close all Windows applications.

2 Follow the un-installation instructions in the Release Notes document specific to that Service Pack, and to the CitectSCADA components, that are installed on your machine.

3 Recompile all your CitectSCADA projects.

After following this procedure, you will be running the CitectSCADA version and Service Pack level you were running before installing the latest Service Pack.

Chapter 6: Configuration

In all but the smallest system, CitectSCADA will need to operate over a Local Area Network (LAN) or a Wide Area Network (WAN).

You can use TCP/IP with CitectSCADA. CitectSCADA supports scalable architecture, which lets you initially implement CitectSCADA on a single computer, or over a small network, and then expand the system later without changing your existing hardware, software, or system configuration.

Using CitectSCADA on a LAN adds more flexibility to the system, and coordination within large plants can be more easily achieved. You can control and monitor autonomous areas within the plant separately, and interrogate the whole plant using any CitectSCADA computer on the network if you want.

In any of these scenarios there are basic configurations that you have to make for the successful operation of your CitectSCADA system. The configuration steps are described in this chapter.

Local Area Network Configuration

To set up a local area network (LAN) for CitectSCADA, you need to have successfully installed all network hardware and software in strict accordance with the instructions provided by the manufacturer, and also be familiar with the basic operation of the network.

Install the CitectSCADA software on every PC you want to use as a CitectSCADA design-time development machine, CitectSCADA Runtime OnlyClient, CitectSCADA I/O server, CitectSCADA Alarm, Report, or Trend server.

Also, set up CitectSCADA for your network, using the Computer Setup Wizard on every one of the machines. To access the Computer Setup Wizard, Open Citect Explorer. In the project list area, select My Projects and double-click the Computer Setup Wizard icon, or choose Tools, Computer Setup.

Note: You need a compiled project to select in order to run the Computer Setup Wizard.

For a detailed explanation on the Computer Setup Wizard, and its options refer to “Running the Computer Setup Wizard” in the online help.

Network Communications Overview

Networking and Microsoft Windows 7

Microsoft Windows 7 distinguishes between Public, Home and Work networks. Each network has its own firewall profile, which allows you to configure different firewall rules depending on the security requirements of your location. The CitectSCADA installers automatically modify the windows firewall settings for the current active network profile during installation. If you later change network settings, you will need to manually modify the firewall settings within Windows.

Note: CitectSCADA networking and redundancy needs the options "CitectSCADA FTP server" and "CitectSCADA Runtime" to communicate through a Windows firewall. You will need to manually add an application to the Windows 7 firewall exception list for a particular network profile.

Using TCP/IP for network communications

CitectSCADA uses TCP/IP to facilitate communications across a network.

To set your system to TCP/IP-based communications, a number of parameters need to be set in the citect.ini file. These parameters will be set automatically when you run the Computer Setup Wizard and select TCP/IP, after you have completed the installation of CitectSCADA. For details of these parameters, and all others, refer to “Citect.ini File Parameters” in the online help.

The Computer Setup Wizard will recognize the computers IP address and match it to the IP address configured in the project for the various servers in the Networking Addresses dialog under the Servers menu in the Vijeo Citect Project Editor.

For example, if you had the following servers in your system:

Citect_IO_1

Citect_IO_2

Citect.PrimaryAlarm

Citect.StandbyAlarm

Citect.PrimaryTrend

Citect.StandbyTrend

Citect.PrimaryReport

Citect.StandbyReport

If the role you need for your PC is not available, you will also have to determine the IP address and update the project accordingly. You can use the DOS command “ipconfig” to obtain this information. Alternatively, you can change the PCs IP address to match that defined in the project.

Configuring Communications Over a WAN

You can configure your system for use with wide area networks (WANs).

Using a Wide Area Network (WAN) is configured in much the same way as using a LAN, with several additional considerations:

1. That the PCs on the WAN can see each other.
2. That appropriate security precautions (eg: VPN) are used when connecting networks over a potentially public link (eg: the Internet).
3. Performance of the connections is appropriate to the data being transferred.
4. Reliability of the connection is appropriate to the requirement for access.

Web Server Configuration

To display a live CitectSCADA project in an Internet browser, you need to publish the project configuration by merging the content of the project pages and the current data these pages present using standard, Web-based communication protocols.

For the web server to function you need to create an exception in the Windows firewall or any other third party firewall to allow TCP traffic to flow on port 80. Specifically, if the machine hosting the web server is running the Windows Vista or Windows 7 operating system, you must enable the World Wide Web Services (HTTP) option in the Windows Vista inbound firewall.

To understand the communication architecture for the CitectSCADA Web Client, it's easiest to consider the role each of the following components play in achieving this outcome:

- CitectSCADA Web Server - Performs the server-side functionality of the system. As well as providing communication, it directs a client to the graphical and functional content of a CitectSCADA project and the location of the runtime servers. This information is stored on the Web Server when a CitectSCADA project is configured as a "deployment". A CitectSCADA Web Server can contain multiple deployments.
- CitectSCADA Runtime Servers (including the I/O Server, Alarms Server, Trends Server and Report 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 needed, so the client uses Microsoft Internet Explorer.

Once you've installed CitectSCADA Web Server for IIS, you will find the following directories under the \Inetpub\wwwroot\Citect folder.

- The **base** directory primarily hosts the administrative pages that are displayed by a Web Server.
- The **cgi-bin** and **images** directories contain the content necessary to display these pages.
- The **client** folder contains the client components (.cab files) that are delivered to a remote computer to run a deployment. Any subdirectories includes the components associated with a particular release (in this case, Version 7.20).
- The **deploy** folder includes the files associated with any deployments (CitectSCADA projects) configured on the Web Server.
- The **#displayclient** folder (located in the Deploy folder) plays a key role in the Web Server security, as the permissions defined for this folder determine the access rights for each user.
- The **locales** folder contains the files needed to support different languages for the client interface. See "Implementing Multiple Language Support" in the Web Client topic of the CitectSCADA online help.

The IIS Virtual Directory

The installation process also adds a virtual directory called Citect to Windows IIS (Internet Information Services). This virtual directory establishes the Web Server as a valid destination for client applications. However, it also plays an important role in managing which users have access to the site.

You can view evidence of this virtual directory in the IIS management console, which is launched by selecting Internet Information Services (or Internet Services Manager on Windows 2000) from Windows' Administration Tools menu. The CitectSCADA virtual directory is shown under the list of default web sites.

You can view the properties for the directory by selecting Properties from the right-click menu.

The Virtual Directory inherits all security settings from the computer's default web site, with the following exceptions:

- Directory Browsing is enabled
- Script Source Access is disabled
- The default document is set to default.htm only
- Anonymous access is disabled
- Integrated Authentication is disabled
- Basic Authentication is enabled

These security settings, including integrated authentication, anonymous access and SSL Encryption, can be customized by the local administrator. However, proper configuration needs experience with IIS and an understanding of the implications of adjusting its settings.

Setting Up Security

If you want to use a Web Server/Client for communications in your CitectSCADA system there are configuration requirements for both the server and the client. The major configuration needed is that of security on the server.

Security on the Web Server is based on the implementation of user accounts. In the case of an IIS-based Web server, security is tightly integrated with Windows user authentication. For information on setting security on each of these, refer to Configuring Security Using IIS.

Web Client user account types

Both systems support the same three user account types on a Web Client.

Client type	Description
Administrator	User is permitted to remotely view, add, update and delete deployments.
Control Client	User can view project pages and make adjustments to writable values.
View-only Client	User can only view the project pages.

The Web Server tests the access rights for each user when they log in and then displays or hides the appropriate buttons on the home page accordingly.

Note: Although the Web Client security architecture controls access to your projects on the Web Server, the CitectSCADA system security (privilege/area settings) still manages the control system, maintaining a primary level of security.

Configuring Security Using IIS

Setting up security on an IIS-based Web Server primarily involves creating three Windows user groups, each representing one of the Web Client user account types. Individual users can then be assigned to the relevant user group, and automatically inherit appropriate access rights based on the Windows security settings defined for the group.

Note: To avoid security access issues for operating systems Windows Vista® and above, creation of these Windows user groups is mandatory.

Client Type Access Rights

The following table defines the access rights that each type of user has to the Web Server's installed directories, as defined by the properties for each.

In the table, **read** means Read & Execute, List Folder Contents and Read user permissions are allowed; **read and write** means Full Control is allowed, and **access denied** means Full Control is denied.

Installed directory	ADMINISTRATOR	CONTROL	VIEW-ONLY
Citect	read	read	read
Citect \ cgi-bin	read	read	read
Citect \ client	read	read	read
Citect \ deploy	read and write	read	read
Citect \ deploy \ #displayclient	read	read	access denied
Citect \ images	read	read	read

For example, an administrator client needs to be able to read all the installed folders to fully access the components of the home page. Additionally, they need write access to the Deploy subdirectory to create new deployments.

By comparison, a View-only Client needs to be denied access to the #displayclient folder to deny the ability to write back to a CitectSCADA project.

Therefore, when setting up security on the Web Server, your user accounts need to align appropriately with the permissions outlined in the table above.

To implement the Web Server’s security strategy successfully, follow the procedure below to configure your system, and simplify managing client accounts.

The ongoing management of your Web Server security then involves adding and removing individual accounts as needed.

Note:

- The installation and initial configuration of the Web Server needs to be performed by a Windows user with local administrator permissions; that is, they are able to add and edit Windows User accounts, and modify files and folders. This capability is needed to set up Web Client user accounts and manage security settings.
- It is important to understand the distinction between the role of the Windows Local Administrator, and the Web Client’s Administrator users:
  - **Windows Administrator** - configures security on the Web Server and sets up client accounts.
  - **Web Client Administrator** - an end user capable of modifying and managing projects deployed on the Web Server.

  The two roles parallel a CitectSCADA configuration engineer and a runtime operator.

Configuring Client Account User Groups

Creating a user group associated with each type of Web Client account on your Web Server allows you to manage security without having to deal with individual users. Users are then added to a group and inherit the security status set for the group.

To create a User Group on the Web Server computer, you log in to Windows with Local Administrator permissions.

To create the client account user groups:

1 From the Computer Management tool, locate Local Users and Groups in the directory tree. This is where the users and groups for the local machine are configured and managed.

2 Right-click the Groups folder and select New Group. This displays the New Group dialog.

3 In the Group Name, type Web Client Administrator (or something appropriate), and describe the group's purpose.

4 Click Create.

The group you have just created will appear in the list of groups presented in the Computer Management console.

Repeat the steps above to create Control Client and View-only Client user groups.

To test your security settings, add at least one user to each group.

Preparing the Citect folder

You need to set the security settings for the Citect folder and its sub-directories, as this will determine the access granted to each type of client account.

To prepare the Citect folder:

1 Log on to the Web Server computer as a Windows Administrator.

2 Launch Windows Explorer and browse to the Citect folder.By default, this is **Inetpub\wwwroot\Citect** on the web server computer.

3 Right-click the Citect folder and select **Properties**.

4 From the **Properties** dialog, select the **Security** tab to display the users currently configured for the folder.

There will probably be several groups already defined in this folder. The two you need to pay attention to are the **Administrators** group and the **Everyone** group.

- The Administrators group represents all the Windows users recognized by the Web Server computer with Local Administrator rights. This group has **Full Control** permissions on the folder, facilitating the ability to adjust the Web Server security settings. If this is the case, there should be no reason to modify this group.
- The Everyone group represents all other users recognized by the local machine. Give this group the following access to the Citect folder; allow **Read & Execute, List Folders Contents,** and **Read** permissions. This provides local users on the Web Server machine with the equivalent of Control Client permissions.

If there are other groups defined for the Citect folder, you might want to remove these groups to simplify managing your Web Client accounts.

5 Add the three groups that you created in Configuring Client Account User Groups to the Citect folder.

6 Confirm the security settings for the three newly created groups.Each group has to have the same access as the Everyone group: **Read & Execute, List Folders Contents,** and **Read** permissions.

7 All the subdirectories have to inherit the permissions set for the Citect folder. To do this click the **Advanced** button on the **Security** tab of the properties dialog, and select **Replace permission entries on all child objects,** then click **OK**.

This provides consistent security settings across all the installed directories. A Security dialog might appear to alert you that this will “remove or reset explicitly defined permissions on child objects”. Click **Yes** to continue.

Setting Access Rights for Client Accounts

The three client account types supported by the Web Client are defined by the security settings for each within the installed directories on the Web Server machine.

The differences, outlined in the table in Client Type Access Rights, need specific security settings for the Administrator Client and View-only Client types. An Administrator needs write access to the Deploy subdirectory, and the View-only Client needs to be denied access to the #displayclient subdirectory.

To configure security setting for the Administrator Client group:

The Administrator Client needs full access to the Deploy subdirectory to enable the creation and modification of deployments.

1 Locate the Deploy subdirectory in the Deploy folder. By default, this is Inetpub\wwwroot\Citect\Deploy

2 Right-click the folder and select **Properties** to display the Deploy folder properties.

3 Click the **Security** tab and locate the Web Client Administrator group you created in the list of users and groups.

4 Edit the permissions set for the group to **Allow Full Control**.

To configure the security settings for the View-only Client group:

The View-only Client needs to be denied access to the #displayclient subdirectory to deny write changes being made to a deployed CitectSCADA project.

1 Locate the #displayclient subdirectory in the Citect folder. By default, this is Inetpub\wwwroot\Citect\Deploy\#displayclient.

2 Right-click the folder and select **Properties** to display the folder properties.

3 Click the **Security** tab and locate the View-only Client group you created in the list of users and groups.

4 Edit the permissions set for the group, and change to **Deny Full Control**.

5 A Security dialog appears “Deny entries take priority over all Allow entries”. Click **Yes** to continue.

Note: The Control Client group needs no additional configuration, as it uses the settings outlined in Preparing the Citect folder.

Set security permissions accurately in order for the web server to operate correctly. If you experience any problem with communicating from the web client check that the security settings are correct for your installation.

Deleting a User Account

You can deny a user access to the Web Server by removing them from the groups that have permissions set for the Citect folder.

However, if security is a concern, then deny the user access to the Citect folder before you delete the user. This avoids the situation where the operating system doesn't immediately acknowledge that a user account has been deleted, creating a short period where a deleted user can still log on.

To absolutely delete a user account

1. Add the user as an individual to the Citect folder.
2. Set their access rights to **Deny Full Control.**
3. Remove the user from the groups that have permissions set for the Citect folder.

With all access denied, they cannot do anything even if they gain access.

Testing the Web Server Security Settings

To test the security settings for your Web Server client groups:

1. Launch Internet Explorer on the Web Server machine.
2. Call up the Web Client home page by typing in the following address:

   ```
   http://localhost/Citect
   ```
3. Log in to the home page using a user name and password that's been added to the Administrator Client group.

   If successful, the System Messages dialog will read “LOGINADMIN Admin (UserName) logged in”.

   If the message starts with LOGINDC (for Control Client) or LOGINMC (for View-only Client), there is a problem with your configuration. Confirm that you are using the correct user name for the group you are testing. If the problem still occurs, revisit the process in Setting up security using IIS to check that an error hasn't been made.
4. Repeat this process with a Control Client and View-only Client user.

Once you have confirmed that security is correctly set up on the Web Server, you can now prepare your CitectSCADA project for deployment. For more information see Configuring a deployment in the online help.

Logging on to the Web Server

After setting up your client accounts, you must provide the following details to each end user so they can log on to the Web Server:

- Address of the Web Server

  This is the address users have to type into their Web browser to gain access to the CitectSCADA Web Server.

If they are doing this remotely, the address is:

```
http://<machine name>/Citect or http://<machine IP address>/Citect
```

If they are logging on to the Web Server computer, the address is:

```
http://localhost/Citect
```

- User name and password

  Once the browser has arrived at the Web Server, the end user is asked to provide a user name and password. Typically, you just need to tell them that their Windows user name and password will provide appropriate access. If you had to create a new user profile for someone, provide them with the details.

Note: In some operating systems users may be logged in automatically. To modify this behavior so the user is prompted to login, go to User Authentication in Internet Explorer | Tools | Internet Options | Security Settings.

Once you have finalized the security setup on the Web Server, you are ready to prepare your CitectSCADA projects for deployment.

Index

A
additional drivers, 45
architecture, 9

B
Base Folder dialog, 40

C
Citect.ini parameters, 50
clustering, 8
communications drivers, 42
configuration, 49

D
demo mode, 32
description
  Integrated Environment, 21
  TimeScheduler, 23
drivers, 42, 45

H
hardware alarms, 9
hardware key, 30

I
IIS components, 27
Installation, 21
installation
  Environment Selection, 37
installation modify, repair or remove, 46
Installation Requirements, 25
Installing dialog, 42
installing drivers, 42
Installing Web Server, 40
IPX/SPX, 49

L
LAN, 49
License Agreement dialog, 36
license points
  dynamic, 31
  static, 31
local variable, 10, 18

M
memory mode, 9
migration, 7
Modify, 47
Modify, Repair, or Remove, 46

N
NetBEUI, 49
Network Support, 7
new features, 7
new functionality, 7

O
online changes, 8

P
persist mode, 9, 17
preliminary installation, 33
Program Maintenance dialog, 47

R
Ready to Install the Program dialog, 41
Remove, 47
Repair, 47
Requirements
  hardware, 25
  IIS, 26, 27, 30
  LAN, 26, 30
  NET Framework, 26, 30

operating system, 26, 30
Processor, 25, 29
RAM, 25
System Software, 25, 26, 30

S

Server Components dialog., 37
service pack
installing, 46
uninstalling, 47
Setup dialog, 34

T

TCP/IP, 7, 49
TCP/IP setup, 49

W

WAN, 49
Web Server
on IIS, 40