CitectSCADA

Version 7.0

Installation and Configuration Guide

July 2007

July 2007 edition for CitectSCADA Version 7.0

Manual Revision Version 7.0.

Contact Citect today at www.citect.com
OCEANIA +61 2 9496 7300, NORTH AMERICA +1770 521 7511, LATIN AMERICA +1770 521 7511, AFRICA +27 11 699 6600,
EUROPE +31 71 576 1550, MIDDLE EAST +31 71 576 1550, GREATER CHINA +86 21 6886 3799, NORTH ASIA +65 6866 3712,
SOUTH EAST ASIA +65 6866 3712, INDIA +65 6866 3712.

Contents

Chapter 1: Introduction

About This Guide

Purpose

This document is a guide for installing CitectSCADA for an Integrated or Stand Alone environment. 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

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 and how it may effect your installation and migration from a previous version. Migration information in this chapter covers only migration from CitectSCADA version 6.x to version 7.0. If you are running a version earlier than 6.1 it is recommended that you upgrade to version 6.x before migrating to version 7.0.

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 7.0 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 you must change your network communication over in your current version of CitectSCADA to TCP/IP before installing CitectSCADA Version 7.0.

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

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

Once you have configured all of your servers to use TCP/IP (and maintain NetBIOS) you should then 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:

1. It is essential to set up your servers to use TCP/IP before you set up your client machines.
2. Once you have completed 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 7.0.

New Features

CitectSCADA version 7.0 includes the following new features or changes in functionality. In most cases these new features will not impact the installation or initial configuration. However, many of them may impact your project configuration and functionality. Once you have installed this version you should refer to the on line help for information on how to reconfigure your projects to take full advantage of the new features and improved functionality.

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.

How CitectSCADA's clustering is best configured will always be 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 otherwise problems occur. In v7.0, the tag configurations only exist on the server. The client retrieves the configuration from the server when required and is notified by the server when changes occur.

The following list describes the on line 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 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 failure or 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 all alarm states.

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.

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

In 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.

Cicode Functions in Version 7.0

Changes have been made Cicode functions in CitectSCADA Version 7. 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 Version 7.0" topic of the CitectSCADA on line help.

The Migration Process

There are a number of considerations that you must make before migrating your projects to CitectSCADA version 7. 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 not impact on your existing CitectSCADA V6.x projects when they are migrated to this version. These changes can optionally be incorporated into your existing projects during later development, or may safely be ignored if they are of no benefit to the way that CitectSCADA is used in your organization.

Safe 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

Note: It is optional for you to utilize the full capability of clustering, however after you have installed CitectSCADA V7 you must create a minimum of one

cluster. For details on creating a cluster refer to the “Upgrading Procedure” topic in the CitectSCADA on line 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.

- Network Support
- Local Variables
- Publish Alarm Property
- Dual Network Support
- Project-Based Network Configuration
- Cicode Functions in Version 7.0

In order to understand any implication these changes in functionality may have on your existing projects, refer to the “Upgrading to CitectSCADA Version 7.0” topic in the CitectSCADA on line 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. 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 required in version 7. 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 should 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 the critical changes in project functionality which are incorporated in version 7.

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

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, you must refer to Chapter 4, Installation Requirements, to ensure 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

Install Integrated Environment

The first option that you may select is under the category **Install** CitectSCADA **Integrated Environment**.

The options are:

- Server
- Display / Manager Client

The **Server** option will install a fully functional CitectSCADA server system. Such an installation will include the CitectSCADA development environment, runtime infrastructure files, I/O Server, Alarm Server, Trend Server and Reports Server. It also includes by default a “Display Client” installation.

You should 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.

This option will also allow you to install additional server components including Web Server Client, TimeScheduler etc.

The **Display / Manager Client** option will install a fully functional CitectSCADA server system and the client components which communicate with a server system. A “Display” client has full control of an existing system, whereas a “Manager” client can only receive information on an existing system. Once a “Display / Manager Client” has been installed, its state as a client is determined when you run the Computer Setup Wizard.

This option will also allow you to install additional client components such as Batch Client and TimeScheduler Client.

Install Standalone Environment

The second option, under **Install Standalone Environment,** allows you to install an additional standalone component of CitectSCADA. If you wish to install more than one option, you must run a new instance of the setup procedure for each additional selection.

The options are:

- CitectSCADA WebServer
- CitectSCADA Batch
- CitectSCADA Pocket

The CitectSCADA **WebServer** option will install a Web Server running on Microsoft Internet Information Service (IIS) or Apache Tomcat.

The Web Server performs the server-side functionality of a Web Service to a 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 configured as a "deployment". A CitectSCADA Web Server can contain multiple deployments.

Note: If the CitectSCADA 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 must 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 **CitectSCADA Batch** option will install the CitectSCADA Batch application. This is a flexible, modular batch management system for the automatic administration, control and documentation of batch-oriented manufacturing processes.

It links production to planning levels, and the individual production plants to integrated production lines, ensuring efficient process cycles. It allows you to monitor and control all automated actions and manual operation in the plant.

Note: A CitectSCADA Server installation must exist on the target machine before you can install CitectSCADA Batch.

The **CitectSCADA Pocket** option will install CitectSCADA Pocket, which takes advantage of the latest Microsoft technologies, including the Pocket PC and WindowsMobile Operating System. Connection to the XML Web Service is provided through HTTP, allowing you to use any available wireless media that your Pocket PC supports, such as WLAN, Bluetooth, GPRS or 3G.

CitectSCADA Pocket has been designed for ease of use and configuration, and contains pre-defined displays for Trends, Variable Tags and Alarms. Once CitectSCADA Pocket is installed, simply connect to your CitectSCADA system, download the Tags and it is ready to use. No changes to your CitectSCADA configuration are required.

Server Components

If you selected to install the CitectSCADA Server from the **Install** CitectSCADA **Integrated Environment** option dialog, you will be presented with the CitectSCADA Server Components dialog. This allows you to chose one or more additional components to install with the server.

The options are:

- CitectSCADA Web Server
- CitectSCADA TimeScheduler
- CitectSCADA Batch
- CitectSCADA Pocket Server
- CitectSCADA Knowledge Base
- CitectSCADA Driver Update Tool

The CitectSCADA **Web Server** option will install a Web Server, as described earlier in his chapter. However, when you select it as an additional option to install with the CitectSCADA Server, it will automatically install the IIS version of the Web Server. If you wish to install the Apache Tomcat version of the web server you must install the Web Service from the Standalone options in Install Standalone Environment as described earlier in this chapter.

The **CitectSCADA TimeScheduler** option will install CitectSCADA TimeScheduler, an integrated tool that can automatically control equipment based on calendar events. Also, with configured “special days”, the scheduler can automatically control certain parts of your plant or building during holidays or other irregular events.

Note: For full Event scheduling you can use the Events functionality in CitectSCADA.

The **CitectSCADA Batch** option will install the CitectSCADA Batch application, as described earlier in his chapter

The **CitectSCADA Pocket Server** option will install the CitectSCADA Pocket Server for CitectSCADA Pocket, as described earlier in his chapter.

The CitectSCADA **Knowledge Base** option will install the CitectSCADA Knowledge Base. This is a is a steadily 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.

The Knowledge Base provides detailed technical support information about CitectSCADA, and is a supplement to the CitectSCADA Online Help and printed manuals. Originally intended for developers of complex systems, the Knowledge Base is now a useful tool for all users. The Knowledge Base is updated on a regular basis, and if you have a valid Citect Membership, you can obtain the latest articles directly through the Internet.

The **Driver Update Tool** option will install the CitectSCADA Driver Update Tool.

CitectSCADA communicates with any 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 device driver. It is important that these drivers are the latest version. The CitectSCADA Driver Update Tool is 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 update.

Client Components

If you selected to install the CitectSCADA Display / Manager Client from the **Install CitectSCADA Integrated Environment** option dialog, the **CitectSCADA Client Components** dialog will be displayed.

This allows you to chose one or more additional components to install with the client.

The options are:

- CitectSCADA TimeScheduler Client
- CitectSCADA Batch Client

The **CitectSCADA TimeScheduler Client** option will install CitectSCADA TimeScheduler Client for the CitectSCADA TimeScheduler application, as described earlier in this chapter.

The **CitectSCADA Batch Client** option will install the CitectSCADA Batch client for the CitectSCADA Batch application, as described earlier in his chapter.

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 depending on the components of CitectSCADA that you intend 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 recommended that you ensure that you have the latest updates installed from Microsoft® for your operating system, and system software.

Integrated Environment

Server

The following tables indicate the computer hardware requirements for the CitectSCADA Server installation and all optional server 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 if running a Web Server (2GB if running both Windows Server 2003 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 that screen resolution should be set at 1024 by 768 pixels or higher.

System Software

The following table indicates the system software that is required on any computer onto which you intend to install the CitectSCADA Server and its optional components.

CitectSCADA Component	Minimum System Software
CitectSCADA Server	Operating System Windows 2000 with Service Pack 4 or Windows XP Professional with Service Pack 2 or Windows 2003 Standard Edition with Service Pack 1 and Microsoft .NET Framework 2.0 (installed with CitectSCADA if required). Internet Explorer Version 6.0 A Local Area Network (LAN) if you intent to have multiple clients access the server.
CitectSCADA WebServer	As for CitectSCADA Server, with the addition of: A New Technology File System (NTFS). A LAN running TCP/IP and Microsoft Internet Information Services (IIS) Version 5.0 or Apache Tomcat 5.5. Tomcat Administration Tool.
CitectSCADA Time Scheduler	As for CitectSCADA Server.
CitectSCADA Batch	As for CitectSCADA Server.
CitectSCADA Pocket Server	As for CitectSCADA Server, with the addition of: Microsoft .NET Framework 1.0. and Microsoft Internet Information Services (IIS) Version 5.0.
CitectSCADA Knowledge Base	As for CitectSCADA Server.
CitectSCADA DriverUpdate Tool	As for CitectSCADA Server.

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

Display / Manager Client

The following tables indicate the computer hardware requirements for the CitectSCADA Display / Manager Client installation, and all optional server components.

Description	Minimum Specification
Processor	Intel Pentium 3
Processor Speed	500MHz

Description	Minimum Specification
Random Access memory (RAM)	128MB
Available Disk Space	40GB
Graphics Adapter	With 64MB of VRAM if using Process Analyst.

CitectSCADA

Description	Recommended Specification or Higher
Processor	Intel Pentium 3.
Processor Speed	1GHz
Random Access memory (RAM)	512MB
Available Disk Space	60GB
Graphics Adapter	With 128MB of VRAM if using Process Analyst.

CitectSCADA

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

System Software

The following table indicates the system software that is required on any computer onto which you intend to install the CitectSCADA Display / Manager Client and its optional components.

CitectSCADA Component	Minimum System Software
CitectSCADA Display / Manager Client	Operating System: Windows 2000 with Service Pack 4 or Windows XP Professional with Service Pack 2 or Windows 2003 Standard Edition with Service Pack 1 Microsoft .NET Framework 2.0 (installed with CitectSCADA if required). Internet Explorer Version 6.0
CitectSCADA Time Scheduler Client	As for CitectSCADA Display / Manager Client.
CitectSCADA Batch Client	As for CitectSCADA Display / Manager Client.

Standalone Environment

The following standalone components of CitectSCADA can be installed independently of the CitectSCADA Integrated Environment, Server and Display / Manager Client installations:

- CitectSCADA WebServer
- CitectSCADA Batch
- CitectSCADA Pocket

For information on the minimum hardware and system software requirements for standalone components, refer to the preceding tables under Integrated Environment in the section Server.

If you choose to install CitectSCADA WebServer from the Standalone installation option, you will be requested to select the Microsoft Internet Information Services version, or the Apache Tomcat version.

If you select the Apache Tomcat version you will be directed to review other documentation to accomplish the installation. This installation process cannot install the Apache Tomcat Web Server. For instructions on how to install the Apache Tomcat version, refer to Installing the WebServer on Apache Tomcat in Chapter 5, "Installation." Prior to proceeding with the Apache Tomcat version, you will need the additional system software Apache Tomcat Version 5.x installed.

Note: To install CitectSCADA Pocket there is the additional system software requirement of Microsoft ActiveSync, if you choose to install the Pocket Client option.

Software Licensing

CitectSCADA uses a hardware key to safeguard against license infringement. 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, which is found in the Help menu of Citect Explorer.

Note: If you have CitectSCADA v5.21 or 5.20, you must run ciusafe.exe from the Citect bin directory. You can also download the latest version of the upgrade program from the Key Upgrade section of the Citect website at www.citect.com.

When you launch the CitectSCADA Key Update, the program displays a Key ID. The serial number of the hardware key is also displayed if it has been written to the key. If not, read the number from the printed label on the hardware key. To perform the update, visit the Citect web site and enter the serial number. Provided that your Customer Service agreement and license details are valid, an authorization code appears, which you enter in the CiUSAFE dialog.

To update the hardware key:

1. In Citect Explorer choose **Help | Citect Key Update**. If you have CitectSCADA 5.21 or 5.20, run ciusafe.exe from the Citect bin directory.

   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 displayed. However, 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.

Citect 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 read or write using DDE, ODBC, or the CTAPI.

It does not count any points statically at compile time.

Notes:

- Dynamic and static points are counted only once, regardless of how many times they are used.
- At runtime, the static and dynamic point counts are available through the Kernel and the CitectInfo() Cicode function.
- The decision as to whether a resolved tag is counted is based on the existence of a license property associated with the tag. The server adds this property to the tag when it is resolved, so that it is counted. For example, a DISK_PLC tag would not get this property but an I/O tag would.
- Existing MEMORY_PLC tags in this version are converted to the new "local variables" during migration. Local variables are stored on the client and resolved on the client. Since the client does not add the licensed property to a tag, it only checks its existence, they are not included in the point count.
- When you plan your system you should 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 immediately shutdown.

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.

This is a new feature and it means that when the actual point count gets close to the limit a warning is displayed. Two thresholds can be set in the Citect.ini file a maximum of 2 warnings might be displayed before the system stops - in the terms of % of the maximum point count. The default thresholds are 95% and 98%. For details of the settings in the Citect.ini file, refer to the on line help under the Citect.ini topics.

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 runtime and I/O.

Note: If you configure CitectSCADA to run as multiple processes on one CPU or multiple CPUs, you cannot use CitectSCADA in demo mode. If you run CitectSCADA as one process, you can use demo mode as with previous versions of CitectSCADA.

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, you must 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, you must configure a real variable tag, with an accompanying PLC or I/O device. The tag must be used by a page or in Cicode. If you do not have a real I/O device connected, CitectSCADA gives a hardware error, which you can disable using the IODeviceControl function.
- 8 hours with a maximum of 42,000 real I/O. This is only available through special CitectSCADA Integration Partners (CIP) keys.

Chapter 5: Installation

The Installation Process

Before proceeding with the installation of CitectSCADA and optional components refer to Chapter 4, Installation Requirements, and ensure that you have the required hardware and system software on the target computer to support the installation.

Note: Ensure that you uninstall version 6.x before installing version 7.0, as CitectSCADA does not support different versions running side-by-side.

Additionally, to use the version 7.0 Example and CSV_Example projects, it is recommended that you delete the existing Example and CSV_Example projects using Citect Explorer before starting the installation.

Once you have decided which components of CitectSCADA you want to install you can perform the installation process by following the steps below.

Preliminary Installation

1. To begin the installation, place the CitectSCADA Compact Disk in the CD 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 CD and click Setup.exe to display the initial CitectSCADA **Setup** dialog.
2. When this dialog is displayed, click **Next** to begin the installation process and display the **Welcome to** CitectSCADA dialog.
3. Click **Next** to display the **License Agreement dialog.** Read the license agreement, and if you accept the terms of the agreement, select the appropriate radio button, then click **Next** to display the **Environment Selection** dialog.

Environment Selection

1. In the **Environment Selection** dialog choose one of the options in either environment that you want to install by selecting the appropriate radio button. The options are:

   Install CitectSCADA **Integrated Environment**

   - Server
   - Display /Manager Client

   Install CitectSCADA **Standalone Environment**

   - CitectSCADA Web Server
   - CitectSCADA Batch
   - CitectSCADA Pocket

2 Click **Next** to display the subsequent dialog in the installation sequence. The subsequent dialog will depend on the option that you select in this **Environment Selection** dialog.

If you selected the **Server** option in the previous step, the next dialog will be the **Install** CitectSCADA **Server Components** dialog. This allows you to install additional components along with the CitectSCADA Server installation. You can select multiple options from the following list:

- CitectSCADA WebServer
- CitectSCADA TimeScheduler
- CitectSCADA Batch
- CitectSCADA Pocket Server
- CitectSCADA Knowledge Base
- CitectSCADA Driver Update Tool.

If you selected the **Server** option, proceed to Install Integrated Components below.

If you selected the **Display / Manager Client** option in the previous step, the next dialog will be the **Install CitectSCADA Client Components** dialog. This allows you to install additional components along with the CitectSCADA Client installation. You can select multiple options from the following list:

- CitectSCADA TimeScheduler Client
- CitectSCADA Batch Client

If you selected the **Display / Manager Client** option, proceed to Install Integrated Components below.

If you selected any one of the options in the **Install Standalone Environment** category in the previous step, the next dialog will be the dialog appropriate to the standalone option selected. proceed to Install Standalone Environment below.

Install Integrated Components

Once you have selected the additional components that you want to install from either the **Server** installation or the **Display / Manager** installation click **Next** to display the **Destination Folder** dialog.

Go to Completing the Installation.

Install Standalone Environment

The Standalone Environment allows you to select any one of the following CitectSCADA components:

- CitectSCADA WebServer
- CitectSCADA Batch
- CitectSCADA Pocket

The following steps will guide you through the installation dialogs that will display for each selection.

CitectSCADA **WebServer**

1 Select CitectSCADA **WebServer** to install a stand alone Web Server, this will display the **Installing** CitectSCADA **Web Server** dialog.

2 In the **Installing** CitectSCADA **Web Server** dialog, select either **Web Server on IIS (Internet Information Services)**, or **Web Server on Apache Tomcat**, then click **Next** to display the **Destination Folder** dialog.

If you select Web Server for IIS from the installation options panel, 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.If this is not the case, the following error message will appear:

Note: Though there is an option on this dialog to install the Web Server on Apache Tomcat, the installation program is unable to install it on Apache Tomcat automatically. It must be installed and deployed manually. For instructions on how to perform a manual installation, refer to Uninstall the Web Server on Apache Tomcat

3 Proceed to Completing the Installation.

CitectSCADA Batch

1 Select **CitectSCADA Batch** to install the stand alone Batch application, then click **Next** to display the **Destination Folder** dialog.

2 Proceed to Completing the Installation

CitectSCADA Pocket

1 Select **CitectSCADA Pocket** to install a stand alone Pocket server and/or client, this will display the **Installing CitectSCADA Pocket** dialog.

2 In the **Installing CitectSCADA Pocket** dialog select either the **CitectSCADA Pocket Server** or **CitectSCADA Pocket Client**, or select both. Click Next to display the **Ready to Install the Program** dialog**.**

Note: In order to install the Pocket Client you need to have your Pocket PC device connected to the computer via its docking station.

3 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. If you are installing either one of the Integrated Environments and you change the default location, you can click the **Reset** button to return the folder selections to the original default locations.

When you are satisfied with the folder selections, click **Next.**

2 If you are installing either of the Integrated Environments *and* you have selected additional components the **Base Folder** dialog will be displayed. 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.

Note:

If you are installing either of the Integrated Environments and you have *not* selected additional components, or you are only installing certain options for the Standalone Environment, the Base Folder will not be displayed, and the **Ready to Install the Program** dialog will be displayed.

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

3 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.

When the installation is complete the **Setup Completed** dialog is displayed which lists a summary of the programs that have been installed. Select the checkbox if you wish to be connected to the Citect online registration web site, otherwise click **Finish** to complete the installation.

Installing the WebServer on Apache Tomcat

Before proceeding with this part of the installation, ensure that all required system software is correctly installed. For details of the requirement refer to Chapter 4, Installation Requirements,

To install CitectSCADA runtime on the Tomcat Web Server, you must initially deploy it as recognized application. This requires a ".war" file to be copied to the Tomcat server.

1 Call up the Tomcat Web Application Manager. To do this, direct your browser to the Tomcat launch page (http://localhost:8080/), then follow the **Tomcat Manager** link.

2 Locate the **Deploy** panel.

3 In the **WAR file to deploy** section, use the **Browse** button to locate the required CitectSCADA**.war** file. You can upload this file directly from the CitectSCADA installation DVD/CD.

4 Click on the **Deploy** button to add CitectSCADA to the list of applications.

Note: If you click the CitectSCADA link in the Application table, a login dialog opens. Do not attempt to log in until you have defined the required users and roles for the application. For details, see Chapter 6, Configuring Security Using Apache Tomcat,.

This completes installation of the required components for CitectSCADA Web Server on Apache Tomcat.

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 should I install a Service Pack?

A Release Note document is distributed when the Citect Support Programmers release a Service Pack. You should read the Release Note and see if it states that a problem you are experiencing has been fixed. If so, then you should apply the Service Pack. However, Service Packs should not be applied on the premise that they 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 C, for instance, you get all fixes and enhancements for Service Pack A and Service Pack B. The Release Note 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 required Service Pack, and the associated Release Notes document from the Citect support web site.
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** application available from the Start, Settings, Control Panel menu item.

Note: The CitectSCADA 7 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.

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 CitectSCADA component 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). To uninstall this application use the same procedure as for uninstalling CitectSCADA, but select Sentinel Protection Installer from the list displayed in the Add or Remove Programs dialog, then follow the on screen instructions.

Uninstall the Web Server on Apache Tomcat

To uninstall CitectSCADA runtime on the Tomcat Web Server, you must "undeploy" it as recognized application.

1 Call up the **Tomcat Web Application Manager**. To do this, direct your browser to the Tomcat launch page (http://localhost:8080/), then follow the Tomcat Manager link.

2 Display the **Applications** panel.

3 Identify the CitectSCADA application under the **Path** column and click **Undeploy** under the **Commands** column.

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 be required to operate over a Local Area Network (LAN) or a Wide Area Network (WAN).

For large applications, you can add a LAN to the CitectSCADA system, or use an existing LAN supported by CitectSCADA.

You can use NetBEUI, IPX/SPX, TCP/IP, and other network protocols 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 must be made 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 must have successfully installed all (non-CitectSCADA) network hardware and software in strict accordance with the instructions provided by the manufacturer, and you should also be familiar with the basic operation of the network.

You must install the CitectSCADA software on every PC you want to use as a CitectSCADA design-time development machine, runtime CitectSCADA Display Client, CitectSCADA I/O server, and CitectSCADA Alarm, Report, or Trend server.

You must 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 must have 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

Using TCP/IP for network communications

In version 7.0 CitectSCADA uses TCP/IP to facilitate communications across a network.

To set your system to TCP/IP-based communications, a number of parameters must 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 on line help.

You then need to map the name for each server to a TCP/IP address. This is done by setting the server’s network address in the Networking Addresses dialog under the Servers menu in the CitectSCADA 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

You will also have to determine the IP address for each machine and add them using the Network Addresses dialog. You can use the DOS command “ipconfig” to obtain this information.

Configuring Communications Over a WAN

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

There are several Citect.INI parameters that work together to achieve the three types of configuration as described below.

LAN parameter settings to allow the use of TCPIP over the WAN.

INTERNET parameter settings to make the computer an FTP server.

LAN parameter settings to allow the use of TCPIP over a WAN

A typical arrangement of parameters and settings is shown below. The critical setting is 'Tcpip=1' to enable the use of Windows Sockets by CitectSCADA. TCPIP does not have the maximum sessions limit that NETBIOS has (maximum of 255 sessions), and so permits more CitectSCADA communication sessions than NETBIOS allows.

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 the Citect.ini File Parameters in the on line help.

```
[LAN]
Node=TEST_PC
LanA=-1
Tcpip=1
```

You will need to run the Computer Setup Wizard for each I/O server on which you want to enable TCP/IP over the WAN.

Internet parameter settings to enable FTP on an Internet Server

Typical settings to do this are shown in the following example:

```
[INTERNET]
Server=1
display=patrick (any text password for a display license)
manager=jimmeh (any text password for a manager license)
RunFTP=1
ZipFiles=0
LogFile=D:\
```

You should not make the manager and display passwords the same.

Web Server Configuration

To display a live CitectSCADA project in an Internet browser, you must combine the content of the project pages and the current data these pages present using standard, Web-based communication protocols.

Note: To use the web server you must switch your system over to TCP/IP-based communications. Refer to Network Communications Overview for details of how to do this.

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 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 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 required, so the client uses Microsoft Internet Explorer.

Once you've installed CitectSCADA Web Server for IIS, you will find the following directories under the CitectSCADA destination folder.

- The **WebServer** directory primarily hosts the administrative pages that are displayed by a Web Server.
- The **cgi-bin** and **images** directories contain the content required 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 7.00).
- 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 required to support different languages for the client interface. See also Implementing Multiple Language Support.

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 Citect virtual directory should appear 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 requires experience with IIS and an understanding of the implications of adjusting its settings.

Setting Up Security

If you intend 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 required is that of security on the server. The method of setting security differs depending on whether the web server is running on Microsoft Internet Information Services (IIS) or Apache Tomcat.

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. With an Apache Tomcat Web Server, the access rights for each user type is defined through the creation of "roles".

For information on setting security on each of these, refer to Configuring Security Using IIS or Configuring Security Using Apache Tomcat.

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.
Display Client	User can view project pages and make adjustments to writable values.
Manager 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 protection of 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.

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	DISPLAY	MANAGER
WebServer	read	read	read
WebServer \ cgi-bin	read	read	read
WebServer \ client	read	read	read
WebServer \ deploy	full control	read	read
WebServer \ deploy \ #displayclient	read	read	access denied
WebServer \ 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 manager client must be denied access to the #displayclient folder to prevent the ability to write back to a CitectSCADA project.

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

To implement the Web Server's security strategy successfully, you should follow the procedure below to protect your system, and simplify managing client accounts.

The ongoing management of your Web Server security should then involve adding and removing individual accounts as required.

Notes:

- The installation and initial configuration of the Web Server must be performed by a Windows user with local administrator permissions; that is, they must be able to add and edit Windows User accounts, and modify file/folder protection. This capability is required 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 must 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 should appear in the list of groups presented in the Computer Management console.

Repeat the steps above to create Display Client and Manager Client user groups.

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

Preparing the Web Server folder

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

To prepare the WebServer folder:

1. Log on to the Web Server computer as a Windows Administrator.
2. Launch Windows Explorer and browse to the WebServer folder.

   The WebServer folder is located in the installation directory. By default, this is C:\ProgramFiles\Citect\WebServer on the web server computer.
3. Right-click the WebServer 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. You should give this group the following access to the WebServer folder; allow **Read & Execute, List Folders Contents,** and **Read** permissions. This provides local users on the Web Server machine with the equivalent of Display Client permissions.

   If there are other groups defined for the Web Server 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 WebServer folder.
6. Confirm the security settings for the three newly created groups. Each should have the same access as the Everyone group: **Read & Execute, List Folders Contents,** and **Read** permissions.
7. Ensure all the subdirectories inherit the permissions set for the WebServer 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 ensures consistent security settings across all the installed directories. A Security dialog might appear warning 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, require specific security settings for the Administrator Client and Manager Client types. An Administrator needs write access to the Deploy subdirectory, and the Manager needs to be denied access to the #displayclient subdirectory.

To configure security setting for the **Administrator Client** group:

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

1. Locate the Deploy subdirectory in the Web Server folder. By default, this is C:\ProgramFiles\Citect\WebServer\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 **Manager Client** group:

The Manager Client must be denied access to the #displayclient subdirectory to prevent write changes being made to a deployed CitectSCADA project.

1. Locate the #displayclient subdirectory in the Web Server folder. By default, this is C:\ProgramFiles\Citect\WebServer\Deploy\#displayclient.
2. Right-click the folder and select **Properties** to display the folder properties.
3. Click the **Security** tab and locate the Web Client Manager group you created in the list of users and groups.
4. Edit the permissions set for the group, which you should change to **Deny Full Control**.
5. A Security dialog appears warning “Deny entries take priority over all Allow entries”. Click **Yes** to continue.

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

It is critical that security permissions are set 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 Web Server folder.

However, if security is a concern, you should deny the user access to the Web Server folder before you delete them. This avoids a known problem 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 securely delete a user account

1. Add the user as an individual to the Web Server folder.

2 Set their access rights to **Deny Full Control.**

3 Remove the user from the groups that have permissions set for the Web Server 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 should read "LOGINADMIN Admin (UserName) logged in".

If the message starts with LOGINDC (for Display Client) or LOGINMC (for Manager 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 ensure an error hasn't been made.

4 Repeat this process with a Display Client and Manager 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, you must provide them with the details.

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

Configuring Security Using Apache Tomcat

The Web Client user accounts types are defined on a Tomcat Web Server through the creation of "roles". Each user is assigned a role when they are configured in the Tomcat Administration Tool, providing a level access appropriate to their associated Web Client account type.

The roles that need to be defined on the Tomcat Web Server are as follows.

Role	Web Client account type	Description
citectadmin	Administrator	User can remotely view, add, update, and delete deployments.
citectdisplayclient	Display Client	User can view project pages and adjust writable values.
citectmanagerclient	Manager Client	User can only view project pages.

To configure users and roles using the Tomcat Administrator

1 On the Tomcat Server, call up a browser and direct it to the installed Apache Tomcat Home page, using one of the following addresses:

`http://127.0.0.1:8080`

or

`http://localhost:8080/`

2 Click the **Tomcat Administration** link to display the Tomcat Web Server Administration Tool login page (`http://127.0.0.1:8080/admin`).

3 Type in the **User Name** (for example, **admin**) and **Password** you provided during the installation of Tomcat, and click **Login**.

4 On the Administration Tool page, select **Roles** from the **User Definition** section of the contents tree. This displays a list of all existing roles on the Tomcat Server.

5 Choose **Create New Role** from the list of available **Role Actions** to display the **Create New Role Properties** form.

6 Type in the role name **citectadmin** and a description if required, then click **Save**.

7 Repeat the previous step, to create the roles **citectdisplayclient** and **citectmanagerclient**. When complete select **Commit Changes**.

You are now ready to add the three Tomcat users that correspond to the Web Client account types.

8 Select **Users** from the **User Definition** section of the contents tree to display a list of all existing users on the Tomcat Server.

9 Select **Create New User** from the list of available **User Actions** to display the **Create New User Properties** page.

10 Type the user name **citectwebadmin** and a password, then select the checkboxes next to the following roles:

- **citectadmin**
- **citectdisplayclient**

- **citectmanagerclient**

11 Repeat the previous step to create the user **citectwebdc**. Associate the following roles:

- **citectdisplayclient**
- **citectmanagerclient**

12 Repeat the step again, this time creating the user **citectwebmc**. Associate the role:

- **citectmanagerclient**

Note: The role names must be identical to "citectadmin", "citectdisplayclient" and "citectmanagerclient", and are case-sensitive.

13 Once you have created the three users, Click **Commit Changes**.

Note:

- You can define your own user names; however, any user you create must have at least the "citectmanagerclient" role associated with them.
- If you wish, you can create "Groups" to control several users.

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

1 Launch Internet Explorer on the Web Server machine.

2 Call up the Web Client home page by entering the following address:

```
http://localhost:8080/Citect
```

Note: "8080" represents the port defined for your Tomcat Server; 8080 is the default.

3 Log in with the administrator user profile you have created; for example, "citectwebadmin".

If successful, the CitectSCADA Web Client Deployment page appears. The System Messages dialog should read "LOGINADMIN Admin citectwebadmin logged in".

4 Repeat this process with the Display Client and Manager Client profile, "citectwebdc" and "citectwebmc".

Once confirming that security is correctly set up on the Web Server, you are ready to distribute login information to your client users.

Logging on to the Tomcat Web Server

Once you have set 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 they will have to enter into their Web browser to gain access to the CitectSCADA Web Server.

  If they are doing this remotely, the address is:

  ```
  http://<machine name>:8080/Citect
  ```

or

`http://<machine IP address>:8080/Citect`

Note: "8080" represents the port defined for your Tomcat Server; 8080 is the default.

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

`http://localhost:8080/Citect`

- **User name** and **password**

  Once the browser has connected to the Web Server, the user will be asked for a user name and password.

  Typically, you will just need to provide them with the user name that offers the appropriate level of access; for example, "citectwebadmin" if they require full access, or "citectwebmc" if they only require read-only access.

  If you created a specific user profile for a particular person, you will have to provide them with the details.

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

Index