Citect SCADA 2018 R2

Installation and Configuration Guide

July 2019

Legal Information

DISCLAIMER

AVEVA Group Plc 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, AVEVA Group Plc reserves the right to revise this publication at any time without incurring an obligation to notify any person of the revision.

COPYRIGHT

The Example Project is provided to you for the purpose of illustrating how the SCADA software 2018 R2 could be used in an operational environment ("the Purpose"). AVEVA grants you a royalty free, non exclusive, non transferable license to use the example project installed with your SCADA software version 2018 R2 (“the Example Project”) for the Purpose only.

The Example Project is provided by AVEVA as part of the SCADA software version 2018 R2 on an "as is" basis and AVEVA does not guarantee the reliability, serviceability or function of the Example Project.

Should you modify the Example Project, you bear the risk of any use of such modified Example Project.

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

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

Publication date: July 2019
AVEVA Group plc
High Cross Madingley Road
Cambridge CB3 OHB. UK
https://www.aveva.com/

GENERAL INFORMATION

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

July 2019 edition for Citect SCADA Version 2018 R2.

Manual Revision Version 2018 R2.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by AVEVA Group Plc for any consequences arising out of the use of this material. © July 2019 AVEVA Group Plc. All Rights Reserved.

Validity Note

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

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

For information on how to contact sales, customer training, and technical support see https://sw.aveva.com/contact.

Contents

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.

Symbol	Description
⚡ or ⚡	The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.
⚠	This is the safety alert symbol. It is used to alert you to personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ 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.

NOTICE

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

Please Note

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

Before You Begin

Citect SCADA 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 Citect SCADA's central role in controlling systems and processes, you must appropriately design, commission, and test your Citect SCADA project before implementing it in an operational setting. Observe the following:

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not use Citect SCADA 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, power outage and restart.
- 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.
- Observe all accident prevention regulations and local safety guidelines. [1]
- Each implementation of a control system created using Citect SCADA 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.

1. For additional information, refer to NEMA ICS 1.1 (latest edition) "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control", and to NEMA ICS 7.1 (latest edition) "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

Chapter 1: Introduction

About This Guide

This document provides instructions for installing Citect SCADA. It describes the installation process and optional components which can be installed in each environment, either on a single workstation or on a network (online upgrade).

The configuration section provides an overview of using Citect SCADA 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 Citect SCADA:

- Upgrading
- Installation Description
- Installation Requirements
- Installation
- Configuration

Maintaining System Currency

After you have completed the installation and configuration of Citect SCADA and deployed it as your production system, it is recommended that you keep your software up to date.

AVEVA will periodically publish software updates for Citect SCADA and advisories relating to safety, security and functionality. These are available from the **Product Hub** page of the AVEVA Knowledge & Support Center website at https://softwaresupport.aveva.com. We especially recommend that you nominate a person in your organization to refer, and subscribe, to the RSS feeds for Safety and Security, as well as the latest articles on the web site.

Chapter 2: Upgrading to Citect SCADA 2018 R2

This chapter describes upgrading the product, and new features introduced in Citect SCADA 2018 R2.

> **Note**: Cross version compatibility is not available for alarms version v7.20 onwards.

When updating the computer with a new product version, backup the existing projects and uninstall the existing installation. Install the new version and restore projects into the new version.

> **Note**: The new version you are installing may have updates available. The update may have a fix for the automatic upgrade and may be required to be installed before restoring the project. Please refer to the **Product Hub** page of the AVEVA Knowledge & Support Center website at https://softwaresupport.aveva.com.

Before you review this information, check that you have the necessary hardware and software required to run this version.

When upgrading to Citect SCADA 2018 R2 you need to consider the following:

- Upgrade Method: Depending on whether your system can afford downtime and loss of data, choose an upgrade method: Offline or Online.
- Upgrade Path: Upgrade path refers to the number of versions to which you need to upgrade to get from your current version to Citect SCADA 2018 R2. For upgrading to intermediate versions specified in the upgrade path (for example, v2015 or v2016), refer to the documentation for those versions.

> **Note:** For instructions related to previous versions of Citect SCADA, such as backing up a or restoring a project, consult the documentation for that version.

New Features Introduced in 2018 R2

Citect SCADA2018 R2 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.

The following list of new features introduced in this release is only a brief description. For more details, and links to using the features in your projects, refer to the "What's New in Citect SCADA" page in the main Citect SCADA help.

Graphics Browsing

Enhancements have been made to graphics browsing providing you with a List View as well as a Thumbnails view of graphics objects to easily view their attributes. You can perform the following operations in these views:

- Browse, search and filter across graphic types
- Filter across projects and libraries to identify duplicate graphic objects
- Perform bulk operations directly from Citect Studio including delete, update pages and pack libraries
- Create new graphic objects or open existing objects in Graphics Builder directly from Citect Studio

Managing and editing graphics has also been simplified by allowing you to manually enter the size and position of a selected object. It is also possible to move or nudge an object using the keyboard.

Encrypted Connections

Citect SCADA2018 R2 allows for encrypted communications between Citect SCADA servers, clients and other processes. Security certificates are centrally configured for all nodes including secure deployment of configuration to remote clients.

Citect SCADA provides enhanced protection against external security threats by providing secure connectivity for remote CtAPI clients.

Publish Citect SCADA Data to Cloud

A new interface is now available to AVEVA Insight, which allows you to publish your Citect SCADA data to the cloud easily and securely. You can

- Access your data from browsers and mobile devices, anywhere, any time
- Create and share customized content for your process/plan easily
- Automatically detect anomalous patterns in your historical data and display these via the AVEVA Insight "newsfeed"

For more information, refer to the AVEVA Insight documentation.

Upgrade Method

Before you plan to upgrade to Citect SCADA 2018 R2, consider whether your SCADA system can afford downtime and whether your historical information needs to be available. The upgrade method you choose will depend upon this.

Upgrade methods are of the following types:

- **Offline**: This method requires your system to be shut down for the duration of the upgrade. If your system can afford downtime and depending on whether historical information needs to be available, this method is suitable for you. This is the basic upgrade process that will be required even if you use the online upgrade method.
- **Online**: If you need your system to be available, this method is suitable for you. To be able to conduct an online upgrade, you need to have at least one pair of redundant servers (for details and other pre-requisites, see *Pre-requisites for an Online Upgrade* in the Citect SCADA documentation.)

Upgrade Path

Upgrade path refers to the number of versions to which you need to upgrade to get from your current version to Citect SCADA 2018 R2. Historically, some versions of Citect SCADA have included substantial changes to the product, which required incremental upgrades involving several intermediate steps between very distant versions (for example, 5.21 to 7.20). We have improved the upgrade code so that fewer steps are necessary to go from version 5.21 to 2018 R2. The number of necessary steps will depend on whether you do an offline or online upgrade.

If you plan to perform an offline upgrade, you can upgrade your project from v5.21 directly to Citect SCADA 2018 R2.

If you plan to perform an online upgrade, you need to follow an upgrade path that will depend on your starting version:

- v2015 - If this is your starting version, you need to restore your project to either SP1 or to the latest patch depending upon your requirements. Compile and run the project in order to restore your data.
- v2016 - If this is your starting version, you need to restore your project to either the RTM version or to the latest patch depending upon your requirements. Compile and run the project in order to restore your data.
- v2018 - If this is your starting version, you need to restore your project to either the RTM version or to the latest patch depending upon your requirements. Compile and run the project in order to restore your data.

Note: When you perform an online upgrade to version 2018 R2, the **Accept encrypted and non-encrypted connections (mixed mode)** setting on the **Configurator**, **Encryption** page is selected by default. You can clear this option prior to performing the upgrade if you want to use unencrypted communications. Alternatively, you can configure your system to use encryption after the upgrade process is complete. Information about configuring security and encryption is provided in the *Configuration* chapter in this Install Guide.

Offline Upgrade

Note: This is the basic upgrade process and you will need to perform these steps even if you choose to use the Online Upgrade method.

An Offline Upgrade to Citect SCADA 2018 R2 comprises the following steps:

1. **Backup your current project and relevant files.**

Perform a backup of your project and other relevant files. For the upgrade to complete smoothly, you need to back up a number of files/folders from your system other than your project files. The number of files you need to back up depends on your system configuration. For more information about performing a backup, refer to the Backing Up a Project section in the online help of your current version.

The following files need to be backed up:

File	Description
Project backup (.ctz file)	This is the main file to back up. For information about backing up a project, refer to your current version's online help. You need to have the **Save sub-directories** and **Save configuration files** options selected in the Backup dialog.
Citect.ini	This file is located in the config folder.
Deployment configuration files	If you have deployment configured, back up the following files: • SE.Asb.Deployment.Server.WindowsService.exe.config • SE.Asb.Deployment.Node.WindowsService.exe.config. These are located in the path [CtEdit]Config.
Data directory	This file is found on the path [CtEdit]Data.
Deployment database	This is located in the Deployment directory. For example: **C:\ProgramData\AVEVA\Citect SCADA 2018 R2\Deployment**.
Alarm Database (for v2015)	The Alarm Database is located in the Data directory: **[Data]\<Project Name>\<ClusterName.AlarmServerName>**. For each alarm server you have in your system, a corresponding Alarm Database will exist. You need to backup all alarm databases.

File	Description
Trend files: *.HST and *.00X	The path and names of these files are defined on the trend tag itself and created in the Data directory defined in [CtEdit]Data. The files will be named after the trend name and number of files. For example, if the trend name is CPU, file names will be CPU.HST, CPU.001, CPU.002 and so on.
Report Files	These files contain the code that is executed on your reports. They are located in the [CtEdit]User\<Project Name> folder.
Custom ActiveX Controls (.OCX)	Citect SCADA includes some ActiveX controls, which will be available with the 2018 R2 installation. However, you need to take a backup of your custom ActiveX controls. Check your ActiveX.dbf file in the [CtEdit]User\<Project Name> folder. This file contains a list of the ActiveX controls in your project and their GUID. Using the GUID, find the path of an ActiveX control using the Windows Registry key: KEY_LOCAL_ MACHINE\SOFTWARE\Classes\CLSID\"GUID"\InProcServer32\. The default value for this key is a path to the .DLL or .OCX file you need to back up.
Process Analyst files	Backup the main <Project Folder>\Analyst Views and <Project Folder>\Dictionary folders.
Device logs	These files contain any logging (alarm logs, report logs) you have configured in your project. You will find their location in the Devices dialog. Refer to your online help for more information.
Additional Files	Check your Citect.ini file or use the **Setup Editor, Paths** section as it could contain runtime files used by custom code in the project.
Driver Hotfixes	If you are aware of any driver hotfix in your system, backup this driver DLL which is located in the Bin directory where Citect SCADA is installed. **Note:** The fixes contained in this hotfix may have been included in the drivers which ship with Citect SCADA 2018 R2.

2. **Upgrade your licenses**

In order to do this, you will either need to have a valid support agreement or you will need to purchase a license upgrade. You can upgrade your key or soft license on the **License Activation** page of the AVEVA Knowledge and Support Center. You can also check the support status.

If your license is out of support, contact your local authorized AVEVA distributor. If you don't know who your local distributor is, send an email to scada.orders@aveva.com with your license and site ID details. For more information about licensing in Citect SCADA2018 R2, refer to the *Licensing* section of the Citect SCADA documentation.

3. Install Citect SCADA

Uninstall the current version of Citect SCADA completely and install version 2018 R2. For instructions on installing Citect SCADA 2018 R2, see The Installation Process.

4. Configure the Server Password

Configure the Server Password using the Configurator's **Computer Setup** page. For more information, see *Set Up a Runtime Computer* in the Citect SCADA documentation.

5. Configure the System Management Server

Configure the System Management Server in the Configurator, System Management Server page. For more information, see *Configure a System Management Server* in the Citect SCADA documentation.

6. Restore your project

Restore your project. For instructions on restoring your project, refer to the online documentation.

7. Upgrade your project

As a default, when you restore your project from a previous version, Citect SCADA will force an update, and you will get a warning message. Click **Yes** to proceed with project upgrade.

If this message is not displayed, you can force an update of all projects by setting the **[CtEdit]Upgrade** INI parameter to 1. Close and re-open Citect Studio. Once you re-open Citect Studio, you will get a warning message. After clicking **Yes** all projects will be upgraded.

8. Migrate your project

The automatic project upgrade does not fully upgrade your projects and needs to be followed by the Migration Tool. The Migration Tool is a separate application that runs automatically after the project upgrade has been executed. It adds computers from the existing topology. You may need to run the Migration Tool separately for other components. Refer to the Citect SCADA documentation for more information about running the Migration Tool.

9. Merge your INI file

If you have defined any project-specific parameters in your Citect.INI file, merge them into the new version's INI file.

Merge any driver parameters from you old INI file as they will most likely be necessary to interface with your I/O network. For a list of changes to .INI parameters, refer to the topic *Citect.INI Parameters in Version 2018 R2* in the Citect SCADA documentation.

10. Compile your project

After upgrading your project and running the Migration tool, compile your project to ascertain that runtime functionality works as expected. It is very likely that you may encounter errors when you compile your project. One of the common sources of errors when upgrading is Cicode functions. This is because functions may have changed, deprecated or simply because the compiler code has been updated to prevent runtime errors. You can find a list of updates to Cicode functions in the *What's New* section of the Citect SCADA documentation.

Refer to the Citect SCADA documentation for instructions on compiling your project.

11. Run the Setup Wizard

Before running your project, run the Setup Wizard to configure the Runtime Manager and other settings that are relevant to the runtime process. The Setup Wizard will automatically determine the role of your computer based on the network addresses defined in your project. After finishing the Setup Wizard, restore your historic data and other files, and run your project.

12. Restore runtime files

After compiling your project, place the files necessary for runtime in the correct directories. Refer to point 1 in this topic for the list of files you need to place in the corresponding directories as defined in your Citect.INI file and project configuration.

13. Restore historical data files

Restore the historical data files before running your upgraded projects.

Alarms (v2015 and later)

Convert your Alarm Database in the Data directory with the following steps:

1. Check that you have placed your backed-up Alarm Database in the directory defined by the [CtEdit]Data parameter.
2. Before starting runtime, confirm that the directory [Alarm]SavePrimary does NOT contain ANY ALMSAV.DAT nor ALMINDEXSAVE.DAT files.

Trends

Follow these steps to convert the files:

1. Create the same file hierarchy on the new system.
2. Place the files in the same folders.
3. If you want to change the folder location or you cannot replicate the same file hierarchy, edit the trend tag definitions to match the new file paths.

> **Note**: If you are changing the trend tag name, use the trend renaming tool available on the **Product Hub** page of the AVEVA Knowledge and Support Center.

14. **Run your project**

Run your project to check that the functionality works as intended:

- Check any Cicode that you needed to modify in order to compile your project.
- Test communications to your I/O devices, alarm triggering and trend capture.

Migrate to Production

Review the following information to complete your Offline Upgrade process and apply the changes to your production system.

Testing Considerations

After the upgrade and configuration changes to the project are complete, it is recommended to perform system testing of the new project version. This is to check that functionally and operation behaves as expected before applying the new project to the production environment.

Licensing

When changing to use a newer product version, the hardware/software key may need to be updated. The hardware key is a physical key that plugs into either the parallel port or USB port of your computer. To upgrade the key, a new authorization code is required which can be created by using the AuthCode Generator. To prepare the system, it is recommended to update the production machine keys before the project is updated on the production machines as the updated key will still license the previous version. You can update the hardware/software key in the Licensing activity in Citect Studio.

Prepare Configuration [INI] Files

Before beginning any changes to the production computers, it is recommended that you back up the configuration [INI] files for each machine as they may be required for reference.

The current configuration file can be used with the new product version after the path parameters have been updated to the new version file locations. Refer to the setup of the development environment section of the specific version for further parameter information.

The Setup Editor and Setup Wizard can be used to finalize the configuration of the computer setup.

Server Addresses

During a migration with an existing system, it may be useful to use a new set of IP addresses and computer names for the new version. This is typically done when there is a need to provide isolation between the system project versions to allow the two systems to individually co-exist on the network for a period of time. When isolated, the systems will be independent and not cross communicate or synchronize between the existing and new versions. This type of upgrade would have the new version start with a snapshot of the historical data from the previous system and then run in parallel.

Communication Drivers

The project may be using specialty drivers. If so, it is recommended that you back up the driver files located in the product ‘bin’ directory. Existing specialty drivers that are used may be required for the new version. The Connectivity Hub on the AVEVA Knowledge & Support Center can be checked for driver availability and compatibility at https://softwaresupport.aveva.com.

Specialty Software

The project may be using specialty software to provide certain system functionality. These applications may be required to be updated or re-installed during the upgrade process and considered in the context of the upgrade.

Format File

The project may be using custom configuration forms in the product. This configuration is located in the FRM file which may be required in the new installation. For further information, check the Tech Note "Upgrading with a modified CITECT.FRM file" (TN3795) on the AVEVA Knowledge & Support Center.

Trend and Alarm Data

A project upgrade may also require the trend and alarm data to be updated based on the new product features. It is recommended to keep a backup of the existing production trend data files and the alarm save data file from the original

Once the data files have been upgraded, the updated data files may not be compatible with the previous version.

It is not recommended to change the directory path of the trend data files during the project upgrade as this may affect the trend operation. The default data directory may be changed between product versions and may need to be considered in the context of the install and upgrade with regards to the trend file location.

Troubleshooting Offline Upgrade

This section lists common issues you might encounter during your Offline Upgrade, which may be compiling errors or any other pre-runtime issues.

Not able to upgrade license key

1. Check that you have correctly installed the latest versions of **CiUSafe** and the **Sentinel Driver** via the **License Activation** page of the AVEVA Knowledge and Support Center.
2. Check that the Authorization code matches the Key you are trying to upgrade. If you still cannot upgrade your license, please check the Tech Note "CIUSafe Error Return Codes" (TN5882) on the **Tech Notes, FAQ** page of the AVEVA Knowledge and Support Center.

Compiler errors and warnings not related to deprecated functions

As Citect SCADA evolves, the compiler feature becomes stricter in order to maintain project quality and runtime success. The fact that you are getting compiling errors that were not appearing before is because of stricter compilation, which will result in more predictable and stable runtime. Refer to the error code in the error message to resolve any errors and warnings. You can search the online help using the error code for more information about a specific error code.

Online Upgrade

An online upgrade takes advantage of Citect SCADA's native server redundancy to avoid loss of data and minimize downtime on a production system. There are two ways to perform an online upgrade:

1. Upgrade one by one - firstly primary servers, then clients and then standby servers.
2. Upgrade side by side - where a new set of server and clients runs in parallel.

Similar to the offline upgrade, you will need to follow the upgrade path, and repeat the process as many times as the number of steps in your upgrade path.

Refer to the relevant section depending upon your current version of Citect SCADA.

- Upgrading from v2015
- Upgrading from v2016
- Upgrading from v2018

Pre-requisites for Online Upgrade

As mentioned earlier, an online upgrade will allow you to avoid downtime and loss of data. It is important that you take into consideration the complexity and size of your project when planning for this upgrade. It is recommended that you review the following pre-requisites before you start an online upgrade:

1. **At least one pair of redundant servers**: This is to upgrade one server at the time while the redundant server assumes primary operation, avoiding downtime and loss of data.
2. **Upgraded project**: Check that your project runs and works properly on Citect SCADA 2018 R2 before migrating to production and starting the online upgrade. If your project is complex, it is recommended that you have a test environment as the offline upgrade could be complex and could involve a long server downtime if done on your production system.
3. **Restore runtime files**: Check that you have restored the necessary files for runtime onto the appropriate directories to avoid any disturbances on the upgraded live system.
4. **Capture data files**: To allow historic data to be restored into the new version, you need to assess and move data files to the required location during the upgrade process. This is described in detail in the online upgrade steps in the relevant sections.
5. **Configure your running system for Online upgrade**: To allow this process to be as smooth as possible, we recommend leveraging of your current redundant system and adding the following Citect.INI parameters before the online upgrade:
    - **[LAN] EarliestLegacyVersion**: Use 7500 for upgrade from v2015, 8000 for v2016 and 8100 for v2018. This will allow your upgraded servers to accept connections from the older version
    - **[Alarm]EnableStateLogging**: Set this parameter to 1 to allow logging the alarm synchronization messages into the syslog.
    - **[Debug] Kernel = 1** (optional): Enable this to allow for monitoring the kernel during the upgrade.

Upgrading from v2015

To upgrade from v2015:

1. Check that you have SP1 or the latest patch (depending on your requirements) installed. For instructions on upgrading to this version, refer to the v2015 documentation.
2. Check that you have added the following parameters in the .INI file to all your server nodes before you start the online upgrade.

    [LAN]EarliestLegacyVersion = 7500.

Restart the servers after adding the parameter for the changes to take effect.

3. Shutdown SCADA runtime on the primary server
4. Upgrade Citect SCADA on this server according to the offline upgrade procedure.
5. Set up the Server Password in the Configurator, Computer Setup page.
6. Configure your System Management Server and encryption settings based on your requirements.

> **Note:** Version 2018 R2 should not have encryption enabled with **Accept encrypted and non-encrypted** not selected, otherwise the servers will not be able to communicate. **Mixed Mode** should be used, or encryption should be disabled.

7. Place the backed-up Alarm database in the [CtEdit]Data directory. This will allow a quicker synchronization of alarm servers.
8. Restart the primary server, which is now upgraded.
9. Citect SCADA 2018 R2 server will synchronize its alarm database with the running v2015 server. You need to wait for the synchronization process to finish, and this will depend on the size of your alarm database. The synchronization information is available from the main kernel window of the Alarm Process as well as the syslog.
10. Upgrade your client nodes one by one.
11. Configure your System Management Server and encryption settings based on your requirements.
12. Shutdown runtime on the standby server.
13. When the newly upgraded v2018 R2 server assumes the primary server role it will migrate the entire alarm database to the new format.
14. Upgrade Citect SCADA on this server according to the offline upgrade procedure.
15. Set up the Server Password in the Configurator, Computer Setup page.
16. Configure your System Management Server and encryption settings based on your requirements.
17. Restart the standby server, which is now upgraded.
18. Check functionality of the system as a whole.
19. Test redundancy by switching off the primary server and checking that the standby takes over and Clients switch over.

Special Considerations

Alarm Save Files

When doing an online upgrade from v7.50 to v2018 R2 check that any pre-7.20 Alarm Save files are removed from the v2018 R2 project folders (e.g. <project_cluster>_ALMSAVE.DAT and <project_cluster>_ALMINDEXSAVE.DAT).

Upgrading from v2016

To upgrade from v2016:

1. Check that you have the RTM version or the latest patch (depending on your requirements) installed. For instructions on upgrading to this version, refer to the v2016 documentation.
2. Check that you have added the following parameters in the .INI file to all your server nodes before you start the online upgrade.

   [LAN]EarliestLegacyVersion = 8000.

   Restart the servers after adding the parameter for the changes to take effect.
3. Shutdown SCADA runtime on the primary server
4. Upgrade Citect SCADA on this server according to the offline upgrade procedure.
5. Set up the Server Password in the Configurator, Computer Setup page.
6. Configure your System Management Server and encryption settings based on your requirements.

   > **Note:** Version 2018 R2 should not have encryption enabled with **Accept encrypted and non-encrypted** not selected, otherwise the servers will not be able to communicate. **Mixed Mode** should be used, or encryption should be disabled.

7. Place the backed-up Alarm database in the [CtEdit]Data directory. This will allow a quicker synchronization of alarm servers.
8. Restart the primary server, which is now upgraded.
9. Citect SCADA v2018 R2 server will synchronize its alarm database with the running v2016 server. You need to wait for the synchronization process to finish, and this will depend on the size of your alarm database. The synchronization information is available from the main kernel window of the Alarm Process as well as the syslog.
10. Upgrade your client nodes one by one.
11. Configure your System Management Server and encryption settings based on your requirements.
12. Shutdown runtime on the standby server.
13. When the newly upgraded v2018 R2 server assumes the primary server role it will migrate the entire alarm database to the new format, and you should now be able to see Alarm Summary data on all migrated Clients.
14. Upgrade Citect SCADA on this server according to the offline upgrade procedure.
15. Set up the Server Password in the Configurator, Computer Setup page.
16. Configure your System Management Server and encryption settings based on your requirements.
17. Restart the standby server, which is now upgraded.
18. Check functionality of the system as a whole.

19. Test redundancy by switching off the primary server and checking that the standby takes over and Clients switch over.

Upgrading from v2018

To upgrade from v2018:

1. Check that you have the RTM version installed. For instructions on upgrading to this version, refer to the version 2018 documentation.
2. Check that you have added the following parameters in the .INI file to all your server nodes before you start the online upgrade.

   [LAN]EarliestLegacyVersion = 8100.

   Restart the servers after adding the parameter for the changes to take effect.
3. Shutdown SCADA runtime on the primary server
4. Upgrade Citect SCADA on this server according to the offline upgrade procedure.
5. Set up the Server Password in the Configurator, Computer Setup page.
6. Configure your System Management Server and encryption settings based on your requirements.

   Note: Version 2018 R2 should not have encryption enabled with **Accept encrypted and non-encrypted** not selected, otherwise the servers will not be able to communicate. **Mixed Mode** should be used, or encryption should be disabled.

7. Place the backed-up Alarm database in the [CtEdit]Data directory. This will allow a quicker synchronization of alarm servers.
8. Restart the primary server, which is now upgraded.
9. Citect SCADA v2018 R2 server will synchronize its alarm database with the running v2018 server. You need to wait for the synchronization process to finish, and this will depend on the size of your alarm database. The synchronization information is available from the main kernel window of the Alarm Process as well as the syslog.
10. Upgrade your client nodes one by one.
11. Configure your System Management Server and encryption settings based on your requirements.
12. Shutdown runtime on the standby server.
13. When the newly upgraded version 2018 R2 server assumes the primary server role it will migrate the entire alarm database to the new format, and you should now be able to see Alarm Summary data on all migrated clients.
14. Upgrade Citect SCADA on this server according to the offline upgrade procedure.
15. Set up the Server Password in the Configurator, Computer Setup page.
16. Configure your System Management Server and encryption settings based on your requirements.
17. Restart the standby server, which is now upgraded.
18. Check functionality of the system as a whole.

19. Test redundancy by switching off the primary server and checking that the standby takes over and clients switch over.

Troubleshooting Online Upgrade

This section lists common issues you might encounter during your Online Upgrade, which may be related to runtime issues and redundancy connectivity.

Redundant servers do not communicate

I cannot make my redundant servers communicate and I keep getting the hardware alarm "Redundant Server not found".

1. Check that you have set your [LAN]EarliestLegacyVersion parameter correctly.

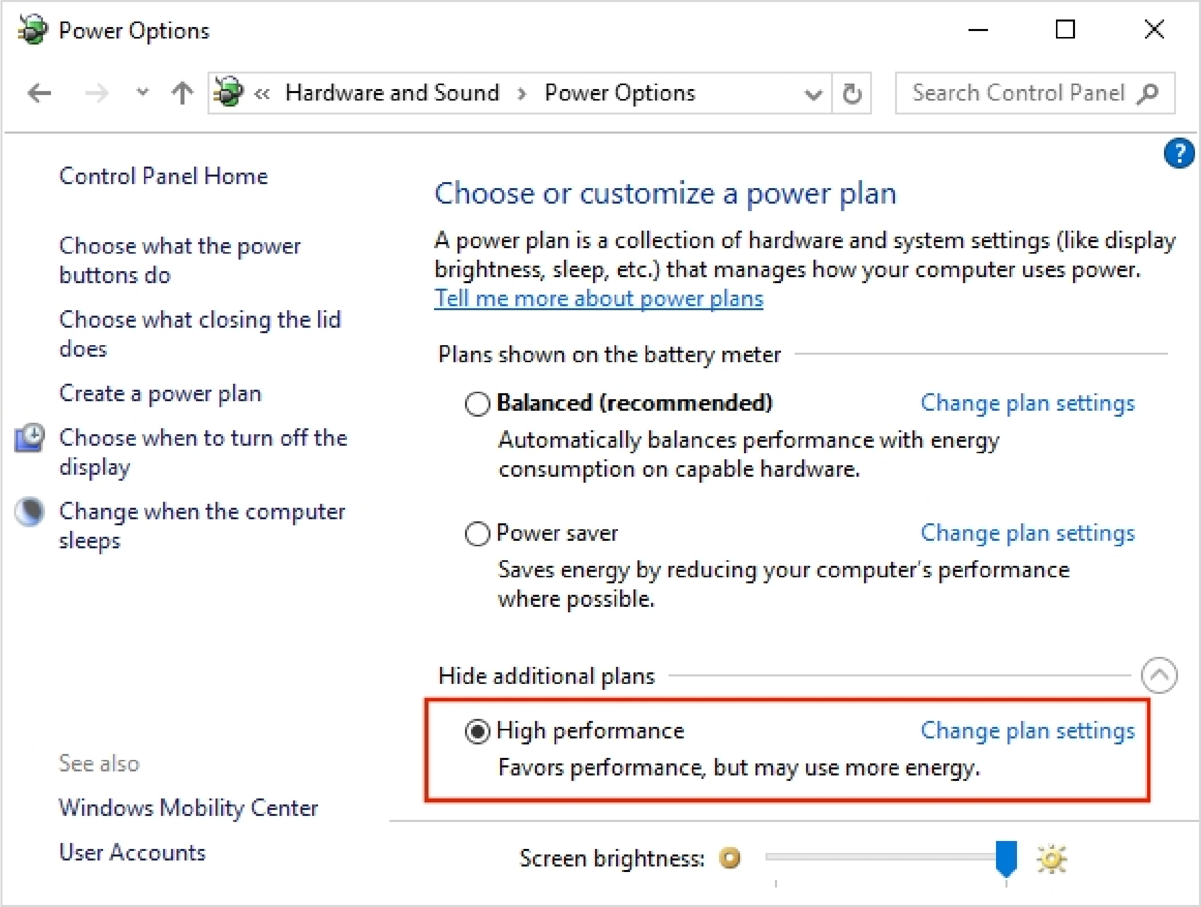
- If upgrading v2015 use [LAN]EarliestLegacyVersion=7500.
- If upgrading v2016 use [LAN]EarliestLegacyVersion=8000.
- If upgrading v2018 use [LAN]EarliestLegacyVersion=8100.
- Check that you have run the Setup Wizard and set both servers to Networked mode.

2. Set the same server password on both servers in the Setup Wizard.
3. If security is enabled, check that Citect Runtime Manager is running as a Windows service.
4. Check that the **Accept encrypted and non-encrypted connections (mixed mode)** option is selected in the Configurator, Encryption page.

> **Note:** Version 2018 R2 should not have encryption enabled with **Accept encrypted and non-encrypted** not selected, otherwise the servers will not be able to communicate. **Mixed Mode** should be used, or encryption should be disabled.

My system is performing slowly even though Hardware and software requirements are met

Check your system's power options: **Control Panel**, **Power Options**.



Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power.
Tell me more about power plans

Plans shown on the battery meter

○ **Balanced (recommended)**
Automatically balances performance with energy consumption on capable hardware.

○ Power saver
Saves energy by reducing your computer's performance where possible.

Hide additional plans

● High performance
Favors performance, but may use more energy.

Remove Upgrade related parameters

After finalizing the upgrade process and confirming that runtime is fully functional, we recommend removing or updating the following .INI parameters. You will need to restart the servers after changing the parameters for the changes to take effect.

- **[Debug]Kernel = 0**: this is to enhance security and keep operators out of the kernel.
- **[LAN]EarliestLegacyVersion**: remove this parameter.

Migration Tool

The automatic update that occurs when you initially launch Citect SCADA 2018 R2 does not fully upgrade your projects, and needs to be followed by the use of the Migration Tool (if migrating from v7.x this is particularly noteworthy). The automatic update is a passive action which updates the database field definition for any database that has been changed between the two versions and copies new files that are necessary in 2018 R2.

The Migration Tool is a separate application which has to be run manually after the automatic upgrade has been executed. It can be initiated after you have prepared the project for final migration. This tool will accommodate the changes in project functionality that are incorporated in 7.x and subsequent versions.

Note: Some of the features introduced in 2018 R2 of Citect SCADA require changes in the project data from version 6.x.

⚠ **WARNING**

UPGRADE ALTERS COMMUNICATIONS CONFIGURATIONS

After upgrading, confirm and adjust the configuration of I/O devices in your project.

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

Using the Migration Tool

Note: Before you use the Migration Tool, is recommended that you familiarize yourself with the process that it performs, and the preparatory steps that you need to carry out with your existing projects.

To run the Migration Tool:

1. Backup the projects that you need to migrate.
2. Navigate to the Project activity in Citect Studio, select **Home**, **Migration Tool** to display the Migration Tool dialog.
3. Either accept the project displayed in the edit box, or browse for the project that you wish to upgrade.

4. Specify the changes you would like to implement during the migration process by selecting from the options described in the following table.

Option	Description
Remove obsolete Memory and Alarm devices	Select this check box if you wish to delete these types of devices after successful migration (see Remove Obsolete Memory and Alarm Devices). **Note:** Do not select this check box when you run the tool for the first time on a project that contains any included projects which are shared with more than one master project. If you want to delete obsolete devices under these circumstances, you can run the tool a second time using this option if the migration is successful after it is run the first time.
Append to existing log file	Use this option to append information about the migration process to the existing Migration Tool log file (located in Citect SCADA's User directory). If this option is not selected, a new log file will be created when migration is complete.
Create roles from User security information	Select this option if you wish to migrate the users database from an existing project (see Creation of Roles).
Copy XP_Style menu into Tab_Style menu	Select this option to convert legacy menu entries to the format necessary for the new menu configuration system. By default, this option is unchecked to avoid potential compile errors that may occur if the legacy menu.dbf contains functions which have been removed.
Migrate included projects	Select this option to migrate the included projects associated with the selected project (see Migrate Included Projects).
Migrate equipment database	Select this option if you have an existing database that you want to migrate into this version. When upgrading from an earlier version, and the "PARENT" field of the equipment table was used, you should select this check box. Otherwise existing data from the PARENT field will be ignored. If runtime browsing is used, the PARENT field will return the equipment parent (the substring of the equipment name without the last '.' and anything after that). To retrieve information that was stored in the previous "PARENT" field the "COMPOSITE" field should be used.
Migrate ABCLX to OPCLX	Select this option if you want to migrate devices that currently use the ABCLX driver to the OPCLX driver. Select the **Configure** button to indicate which I/O devices you would like to migrate. **Note:** You should confirm that the OPCLX driver is installed before you use this option.
Migrate Trend/SPC storage method	If you select this option, the storage method will be set to scaled (2-byte samples) for all trends that have no storage method defined. Use this option to stop the compiler error message "The Storage Method is

Option	Description
	not defined". In previous versions, a blank storage method would default to scaled. However, this is no longer supported, resulting in the compile error message.
Create computers from Network Addresses	If you select this option, computers will be created from the servers and network addresses that you have configured for a project and its include projects. This option distinguishes whether a computer has multiple IP addresses.

> **Note:** If 'Copy XP Style menu into Tab_Style Menu' and 'Migrate Included Projects' are both selected when the migration tool runs, the following message will be displayed: "Copying menus of included projects may lead to conflicts. Any conflicts will need to be manually corrected". To avoid this from occurring, it is recommended you run the migration tool twice. In the first instance just select the option 'Copy XP_Style menu into Tab_Style Menu', and in the second instance just select the option 'Migrate Included Projects'.

5. Click **Migrate** to begin the migration process.

   A progress dialog will display indicating the stage of the conversion and the name of the project being migrated. If you wish to cancel the migration at this point click the **Abort** button.

   > **Note:** Aborting a migration will stop the migration process, and any changes already completed will not be rolled back. You will have to restore your project from the backup created in the first step.

   When the migration process is concluded, a confirmation dialog box will display indicating the number of variables converted and the number of I/O devices deleted (if device deletion was selected at the start of migration).
6. Click the **Close** button to close the dialog.

Remove Obsolete Memory and Alarm Devices

When you use Citect SCADA's Migration Tool, the **Remove obsolete Memory and Alarm devices** option adjusts the following:

Memory tags to local variables: tags that are on an I/O device that are configured to use a 'memory' port.

Note: If there are real I/O devices in your project that have been set to use a 'memory' port during testing, these can be changed before running the migration tool to avoid those tags getting adjusted.

Alarm devices: can remove I/O devices that have a protocol set to 'Alarm', which was needed in earlier versions to enable alarm properties as tags. In version 7.x, the alarm properties are enabled via a setting on the alarm server configuration form.

Memory Devices

In previous versions of Citect SCADA an I/O Device could be defined as a memory device by setting the port value to "Memory". This was generally done for one of the following purposes:

- To provide for future devices that were not currently connected to the system, but their points needed to be configured at this stage of project.
- For virtual devices where there was no corresponding physical I/O Device and you needed data storage with the entire functionality normally associated with I/O variables such as alarms.
- To act as a variable which was local to the process being used in place of Cicode global variables.

You can still use I/O Devices for future or virtual devices in version 7.0, but manually set the Port parameter to an unused value other than Memory, and set the Memory property of the device to True to indicate that it is an offline in-memory device before running the Migration Tool.

You need to review your project to identify which memory I/O Devices are local variable holders and which ones need to be changed to non-memory so that the Migration tool does not convert their variables.

The Migration Tool will set any I/O Device's port which is identified as a Memory device to the new Local Variable, and the original device record will be deleted.

Alarm Devices

In previous versions of Citect SCADA Alarm devices were defined as devices with their Protocol property set to "Alarm". In version 7.0 the function of configuring such a device is now replaced by setting the Publish Alarm Properties property to True on the Alarm Server.

Alarm devices with their Protocol property set to "Alarm" will be deleted from I/O Devices table by the Migration Tool.

The Migration tool can delete memory and alarm device records. If you want to delete the devices at a later time, deselect the "Remove obsolete Memory and Alarm Devices" option.

> **Note:** Alarm devices with their Protocol property set to "Alarm" are no longer used and will be removed by the Migration Tool. The Alarm Servers will now publish Alarm Properties.

Converting Memory Variables

A memory variable is a variable with its I/O Device Port property set to either "Memory" or "MEM_PLC".

If there are multiple I/O Devices with the same name, possibly on different I/O Servers, the device would not be considered as a memory device regardless of its port value. In other words, the Migration tool will not process the variables for memory devices with duplicate names.

Inserting New Local Variables

When the Migration Tool runs, a local variable record will be inserted for each identified memory variable, and the variable data will be copied into the new local variable.

Local variables have fewer fields than variables; the following table shows the mapping from variable to local variable when copying their data.

Variable Tag Parameter or Constant Value	Local Variable Parameter
Variable Tag name	Name
Data Type	Date Type
(Empty)	Array Size
Eng. Zero Scale	Zero Scale
Eng. Full Scale	Full Scale
Comment	Comment

With the exception of the Array Size, which has been introduced in version 7.0 exclusively for local variables, every field receives its value from the same or similar field.

Deleting Variable Tags

Once the Migration Tool has created the local variable records it will insert those variable tag records that have been converted in the previous step, and delete the original variable tag.

If an error is detected during the insertion of the local variables, the deletion of the variable tags will not be performed. If this occurs it is possible to have two records with same name and data, one in the local variable (the newly inserted record) and one in the variable tags (the original record that has not been deleted). You need to delete either of the variables manually, or restore the backed up project after removing the cause of the error then run the Migration Tool again.

Deleting Obsolete I/O Devices

Deleting obsolete I/O Devices is an optional step in the Migration Tool and will be performed after the memory variables are converted. If the delete option is chosen, obsolete Memory devices and Alarm devices will be deleted as the final step of the Migration Tool operation.

Creation of Roles for Existing Users

When upgrading an existing project using the migration tool, a new role will be created (if needed) for every existing user. The new role will have the same security settings that were defined for that user and be given a generic name such as Role_1, Role_2 etc. During the upgrade process, if a role exists with the same security settings as the user, then the existing role will be assigned to the user being upgraded. For example; If Role_1 exists and matches the security settings of the upgraded user then that user will be assigned Role_1 also.

If you do not want to migrate users from an existing project, clear the option **Create Roles from User security information** from the migration tool dialog before running it.

Migrate Included Projects

Each project may contain multiple included projects. Additionally, any included project may contain its own included project so creating a cascading project.

The Migration Tool needs to process the original project and included projects in a single step. The reason for this is that variables can be defined in one project that refer to I/O Devices defined in another included project.

The Migration Tool performs this procedure sequentially on the "master" project then each included project.

In the case where two master projects share the same project as an included project, you should not select the "Remove obsolete Memory and Alarm devices" check box when you process a project that contains shared included projects. This is because the removal is performed at the conclusion of the migration process on each master and included projects sequentially. This could cause the deletion of an I/O Device in the first master project which is referenced by a tag in a shared included project which is processed in a later step.

If two separate "master" projects contain the same included project, run the Migration Tool on each "master" project without selecting to delete obsolete devices.

⚠ 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.

To remove obsolete devices, it is recommended that once the Migration Tool has completed successfully (without the check box being selected), run it a second time with the check box selected. This will remove the devices since every tag conversion were completed in the first pass of the Migration Tool.

Default Scale

The Scale properties in both variable tags and local variables are optional. If a Scale value is not specified, the default value is indicated by a parameter in the Citect.ini file. The parameter name is "DefaultSliderScale" under the [General] section in the Citect.ini file. The default values for Scale is 0-32000, unless the default slider scale is true in which case the default value depends on the type, for example, Integer, String, or so on.

The Migration Tool will read this parameter and if it is not set, or set to false, then it will explicitly set any empty Scale property to a value in to the range of 0 to 32000. This will be done even if either of the Zero Scale or Full Scale parameters has a value, in which case the empty Scale parameter will receive the default value.

If the DefaultSliderScale in the Citect.ini file set to True, the Scale parameters will not be populated with a default value if they are empty, rather they will be interpreted at runtime.

Chapter 3: Installation Description

Before you begin the installation of Citect SCADA, 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 Citect SCADA environment, and any additional standalone 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 as follows:

Option	Description
All Core Components	This option will select Runtime, the Configuration and Development Environment, Drivers, Sentinel Driver and the Floating License Manager for installation. It is a "complete" installation which will install a fully functional Citect SCADA development and server/client system. Such an installation will include the Citect SCADA development environment, runtime infrastructure files, client, I/O Server, Alarm Server, Trend Server and Reports Server. This option also allows you to select the Deployment Server and Deployment Client components for installation. You can use a deployment server to distribute a project's runtime files to the computers within a Citect SCADA system that have been configured as a deployment client. Select this option if this is an initial installation of Citect SCADA which will run as a single

Option	Description
	system, or act as a server to service a number of client installations. If the .NET Framework 4.7.2 installation does not complete, you can install it manually from the installation file in the Extras folder of the Citect SCADA installation disk, then install Citect SCADA.
Runtime Only Server	This 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 and I/O Server, Alarm Server, Trend Server and Reports Server. Select this option if this is an installation of Citect SCADA which will act as a server to service a number of client installations.
Runtime Only Client	This 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 Citect SCADA 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 Citect SCADA Runtime Only Client from a single installation file. This file is named Citect SCADA 2018 R2.exe and located in the <product installation files folder>\Citect SCADA 2018 R2\Extras\Runtime Installer folder of the installation media. This allows installation of the software to computers which only require 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 Citect SCADA. Alternatively you can install .NET Framework from another source, then carry out the single file runtime installation.
Custom	This 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.

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

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 Citect SCADA .dbf files in the correct format. This is only available for selection if Microsoft Excel 2007 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 Citect SCADA project and the location of the runtime servers. This information is stored on the Web Server when a Citect SCADA project is deployed. A Web Server can contain multiple deployments.

Note: If the Web Server and Citect SCADA 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 Citect SCADA server that's hosting the web deployment files. If, conversely, a trust relationship can be established between the Web Server and the Citect SCADA server, they can be on different domains as long as the Web server has read access to the project folder on the Citect SCADA server.

Communication Drivers

Citect SCADA communicates with control or monitoring I/O Devices that have a communication port or data highway - including PLCs (Programmable Logic Controllers), loop controllers, bar code readers, scientific analyzers, 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 recommended that these drivers are the latest version.

The 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 Citect SCADA to function correctly. These will be installed automatically.

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 section describes the requirements for hardware, operating system software and system configuration prior to installing Citect SCADA and any of its components.

These requirements will vary subject to the components of Citect SCADA that you attempt 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 Citect SCADA, it is recommended that you install the latest updates from Microsoft® for your operating system and system software.

Hardware Requirements

Selecting hardware is dependent upon a number of factors such as:

- The role of the hardware in your SCADA system
- The amount of I/O, alarms, trends and the frequency of change
- Number of clients (for servers)
- Server clustering
- Complexity of the user interface
- Degree of customization.

The requirements below have been tested using a simulated SCADA system with 10 clients connected maintaining a server CPU load of less than 25% and should be used as a guideline only due to the impact of the factors listed above.

The SCADA system may require more or less powerful hardware.

Hard Disk Drive (HDD) indicates an estimate of the required amount of space to install the software, store projects and runtime data.

Computer Performance

General PC performance will be affected by the major elements of CPU, RAM, Bus and HDD speed.

It is recommended to look for two things when selecting client and server hardware – PassMark score and CPU Clock Speed. The required processor is defined according to an average CPU mark given by PassMark® Software. To check CPU performance, for example a Core i3 CPU, type "PassMark Core i3" in the search engine of an internet browser. This will return the CPU's calculated performance as compared to other similar well-known processors.

In general, the more intense an application, the higher the clock speed to be selected. This is especially true for clients operating graphically intense or heavily scripted applications.

In general, it is recommended that computers in the SCADA network should target between ~25%-%50 CPU in normal state. This allows the system to be responsive to abnormal situations.

Client Recommendation

CPU PassMark®	Cores *1	RAM	HDD *2	Graphics	Screen Resolution *3	Network
2000	2	4 GB	10 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM	1920 x 1080	100 Mb

1. The complexity of your pages such as the number of graphical animations and Cicode running in the background will impact your client CPU choice. It is recommended to use a higher performing PC with high clock speed when building complex user interfaces. As a guidance, the following will require high clock speed to maintain a Client CPU load of less than 25% on a single core:
   a. HD user interface with 50 complex genies
   b. UHD4K user interface with 100 complex genies
2. If the Deployment feature is being used, the HDD needs to have the required space for the number of configured version +2 of the project.
3. Citect SCADA supports lower and higher resolutions including 4K UHD Resolution (3840 x 2160). A 4K UHD will require a high clock speed CPU.
4. A multi-monitor client will typically require a higher clock speed CPU and more memory.

Server Recommendation

I/O per Server *1	**CPU PassMark-®**	**Cores**	**RAM**	**HDD *2 *3**	**Graphics**	**Screen Resolution**	**Network**
Compact (<1,500 pts)	1800	1	4 GB	10 GB	DirectX 9 or later with WDDM 1.0 Driver, 64 MB of dedicated VRAM	1920 x 1080	100 Mb
Small (<15,000 pts)	4500	4	8 GB	20 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM	1920 x 1080	100 Mb
Medium (<50,000 pts)	8000	4	8 GB	100 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM	1920 x 1080	100 Mb
Large (<200,000 pts)	10000	8	16 GB	500 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM	1920 x 1080	1 Gb

1. This is a recommendation for a single server only running I/O, alarms, trends and reports. For larger systems, services can be distributed to their own PC and/or clustering can be used to add additional servers. System resources of CPU and Memory should be increased when:
   - Using clustering
   - There is high rate of change of data (I/O or Alarms)
2. If the Deployment feature is being used, the HDD needs to have the required space for the number of configured versions+ 2 of your project.
3. Disk space is an estimate only and includes:
   - Runtime components
   - Compiled project
   - 20% of the I/O trending with a change on average every 10 seconds, 24 x 7 for 3 months.
   - Alarm changes equal to the number of I/O changing per day.

Engineering Workstation Recommendation

Total System Size	CPU PassMark®	Cores	RAM	HDD *1 *2 *3	Graphics	Screen Resolution *4	Network
Compact (<1,500 pts)	2000	2	8 GB	10 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM	1920 x 1080	100 Mb
Small (<15,000 pts)	2000	2	8 GB	20 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM.	1920 x 1080	100 Mb
Medium (<50,000 pts)	4250	4	8 GB	50 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM.	1920 x 1080	100 Mb
Large (<500,000 pts)	4250	4	8 GB	50 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM.	1920 x 1080	100 Mb
Huge (>500,000 pts)	8000	4	8 GB	100 GB	DirectX 9 or later with WDDM 1.0 Driver, 128 MB of dedicated VRAM.	1920 x 1080	100 Mb *5

1. SSD is recommended for engineering machines for a smoother and faster experience. If a non-SSD is used, select a minimum RPM of 7200.
2. If the engineering machine is being used as a Deployment Server, the size of the HDD will determine how many versions of the system you can retain.
3. Disk space is an estimate only and includes:
   - Full Citect SCADA installation including optional components and documentation
   - Project assets for the specified system size.
4. Citect Studio is designed for a minimum desktop resolution of 1920 x 1080.
5. If the engineering machine is being used as a Deployment Server, a 1Gb network connection is recommended.

HMI Recommendation

System Size*[1]	CPU PassMark-®	Cores	RAM	HDD	Graphics	Screen Resolution	Network
Compact (<1,200 pts)	1400	1	8 GB	10 GB	DirectX 9 or later with WDDM 1.0 Driver, 64 MB of dedicated VRAM	1920 x 1080	n/a

1. HMI Client/Server combination.

System Software

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

Citect SCADA Component	Minimum System Software
All Core Components	**Operating Systems**: Windows® 7 SP1 (64 bit only) Windows® 8.1 (64 bit only) Windows® 10 version 1607 and later (64 bit only) Windows® 10 LTSC version 1607 and later (64 bit only) Windows® Server 2008 R2 SP1 Windows® Server 2012 Windows® Server 2012 R2 Windows® Server 2016 Windows® Server 2019 Microsoft .NET Framework 4.7.2 (installed with Citect SCADA if not already installed). Microsoft .NET Framework 2.0 (x64) is required by "Schneider Electric Software Update" if using Windows Server 2012.

Citect SCADA Component	Minimum System Software
	Internet Explorer Version 9.0 or greater. **Note**: If installation is unsuccessful check if an earlier version of ArchestrA Data Store is installed on your machine. If an earlier version is installed, uninstall it. Restart your machine before installing Citect SCADA. A Local Area Network (LAN) if you want to have multiple clients access a remote server.
Virtualization Host Support	The following virtualization environments are supported: • Microsoft Hyper-V: based on the version of Windows • VMware Workstation • VMWare vSphere For further information on virtualization, please refer to the Citect SCADA Tech Notes page of the AVEVA Knowledge & Support Center website at https://softwaresupport.aveva.com.
Citect SCADA Web Server	As for Citect SCADA, all Core Components with the addition of: A LAN running TCP/IP and Microsoft Internet Information Services (IIS) See Microsoft IIS Compatibility for information. **Note:** Use an NTFS file system on the target drive for the Web Server software, otherwise you will not have 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.
Project DBF Add-in for Excel	As for All Core Components, and Microsoft Excel 2007 or later (32 bit only) .

Note: Citect SCADA's configuration environment can be affected by different DPI settings. It is recommended when running Citect SCADA that you set the Windows® Display setting **Scale and Layout** to "100%". After changing the Scale and Layout setting for a computer, you should restart it.

Microsoft IIS Compatibility

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

Operating System	IIS version
Windows Server 2019	10.0 (version 1809)
Windows Server 2016	10.0 (version 1607)
Windows 10	10.0
Windows 8.1	8.5
Windows Server 2012 R2	8.5
Windows 8	8.0
Windows Server 2012	8.0
Windows 7	7.5
Windows Server 2008 R2	7.5

Components recommended for Web Server Installation	
Web Management Tools	IIS6 Management Compatibility IIS6 Metabase and IIS6 Configuration compatibility IIS Management Console IIS Management Services
Application Development Features	ASP ISAPI Extensions
Common HTTP Features	Default Document Directory Browsing HTTP Errors HTTP Redirection Static Content WebDAV Publishing
Health and Diagnostics	HTTP Logging
Performance Features	Static Content Compression
Security	Basic Authentication Request Filtering Windows Authentication

Runtime Only Server or Client System Software

An installation of a Citect SCADA Runtime Only Server or Client has the same hardware and system software requirements as the Core.

Virtualization Host Support

You can run components of your Citect SCADA system in a virtual environment.

The following virtualization environments are supported:

- Microsoft Hyper-V: based on the version of Windows
- VMware Workstation: basic virtualization without High Availability and Disaster Recovery
- VMware vSphere.

For further information on virtualization, please refer to the Citect SCADA Tech Notes page of the AVEVA Knowledge & Support Center website at https://softwaresupport.aveva.com.

Anti-virus Software Setup

⚠ WARNING

SYSTEM PERFORMANCE DEGREDATION

The "on access" scan in anti-virus products can lock files used by Citect SCADA, usually having the effect of slowing Citect SCADA down whilst it waits for the scan of that file to finish.

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

⚠ CAUTION

INOPERABLE SYSTEM OR LOSS OF DATA

In some extreme cases, anti-virus software may (incorrectly) detect certain patterns within data files as being viruses. Depending on the anti-virus configuration, this may result in files being relocated or deleted, resulting in data being lost or the system being inoperable.

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

It is recommended that the following directories are excluded from scanning by any antivirus products:

- Program Files installation directory (including files and sub directories)
- Data and Logs directories
- Any alarm server archive paths

The above exclusions are recommended for "on access" or "real time" scans that run continuously and scan each file that is read from or written to.

Software Protection

Citect SCADA supports two different software licensing models:

- **Sentinel Licensing** (using USB keys)

  Sentinel Licensing is a legacy licensing solution for Citect SCADA. It uses physical USB keys that plug in to each computer in your Citect SCADA system. The USB key contains details of your user license, such as its type and I/O point count.

  When you upgrade to a new version of Citect SCADA, you are required to update your Sentinel keys. To do this, you need to retrieve an authorization code from AVEVA's online License Generator (see Updating Your Hardware Key).
- **FLEXERA Softkey Licensing**

  The FLEXERA softkey solution stores license information on a FlexNet Enterprise License Server. The Citect SCADA client process will retrieve licenses from this server as required by the Citect SCADA system. To activate and administer licenses, you use the **Floating License Manager** (see Floating Point License Manager).

In both cases, Citect SCADA uses a Dynamic Point Count Licensing to determine if your system is operating within the limitations of your license agreement. This process tallies the number of I/O device addresses being used by the runtime system.

A point limit is allocated to each type of license included in your license agreement. These license types include:

- Full Server Licenses
- Control Client Licenses
- View-only Licenses.

A Server License is required if you want to run a computer as a dedicated OPC server. For more information, contact Technical Support.

Note:

- There is no distinction between a Control Client and an Internet Control Client.
- There is no distinction between a View-Only Client and an Internet View-Only Client.

See Also

Demo Mode

Updating Your Hardware Key

When you upgrade to a new version of Citect SCADA, you need to update any existing Sentinel USB hardware keys to enable the system to run.

To update a Sentinel USB key with CiUSAFE:

1. Plug the key you would like to update in a local USB port.
2. Open Citect Studio.
3. On the Activity Bar, select **Licensing** from the menu.

   OR

   Click the **Licensing** icon.
4. On the **Sentinel Key Update** panel, click **Launch**.

   The CiUSAFE dialog box will appear.
5. Retrieve the **Serial Number** for the key from CiUSAFE.
6. Visit the **License Activation** page of the AVEVA Knowledge & Support Center website at https://softwaresupport.aveva.com.
7. Click **Submit**.

   If the key is validated, an authorization code will be generated.
8. In CiUSAFE, enter the generated code in the **Authorization Code** field.
9. Click **Update**.

   CiUSAFE will display a **Return Code** to confirm if the update was successful. See the table below for an explanation of the return code values.

0	The key was updated successfully.
1,3	Either the KeyID or the Authorization code you entered is invalid.
2	Either the KeyID or the Authorization code you entered has been corrupted.
4,16	Either the KeyID or the Authorization code you entered is invalid.
9	No hardware key could be found.

Note: Each time you run the Sentinel Key Update, a different Key ID is generated which is normal. 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.

Floating Point License Manager

If your Citect SCADA system uses FLEXERA Softkey Licensing, you need to activate your licenses to allocate the computers in your system. To do this, you use the AVEVA Floating License Manager.

> **Note:** If you have purchased softkey licenses for your Citect SCADA system, the required activation codes will be emailed to you.

To activate a license using Floating License Manager:

1. Obtain the required license activation code from the purchase confirmation email.
2. Open Citect Studio.
3. On the Activity Bar, select **Licensing** from the menu.

   OR

   Click the **Licensing** icon.
4. On the **License Manager** panel, click **Launch**.

   The AVEVA Floating License Manger will appear. It will include a list of the floating licenses that are already available on the FlexNet Enterprise License Server.
5. Click **Activate**.
6. On the dialog that appears, select an **Activation Method**, then click **Next**.
7. Enter the **Activation ID** that was emailed to you, then click **Next**.

   The following steps will be determined by activation method you selected. If you require assistance, click the **Help** button for instructions.
8. To finalize the activation process, you will be prompted to restart the FlexNet License Administrator. Click **Yes**.

   The license you have activated will now appear in the list displayed in the Floating License Manager.

There are several other tasks you can perform with Floating License Manager. For more information on its supported functionality, see the documentation that is available from the **Help** menu.

Dynamic Point Count Licensing

Citect SCADA counts I/O device addresses dynamically at runtime.

The client process keeps track of the dynamic point count. This includes variable tags used by the following:

- Alarms
- Trends
- Reports
- Events
- OPC DA Server
- EWS Server
- Pages and Super Genies
- Cicode functions (TagRead, TagWrite, TagSubscribe, TagGetProperty and TagResolve)
- Any tag referenced by Cicode
- Reads or writes using DDE, ODBC, CTAPI or external OPC DA clients.

A particular variable tag is only counted towards your point count the first time it is requested. Even if you have configured a certain tag on a particular page in your project, the variable tag will not be counted towards your point count unless you navigate to that page and request the data.

You should also be aware of the following:

- A dynamic point count is tag based, not address based. For example, two tags that use the same PLC address will be counted twice.
- For the multi-process mode, each server component will accumulate its own point count which will add to the total of the client dynamic point count.

  If two trend tags use the same variable tag, it will be counted once. If two server components use the same tag(s) (say alarm and trend), the tags will not be counted twice when the point count gets totaled in the client process.
- For the multi-process mode, the client component will also accumulate its own point count, which will include all the variable tags that are used by the process.
- For the multi-process mode, the machine point count will be the point count of the client component, or the point count added up from each server component, depending on whichever is bigger. If the server point count is greater than 500, the client component point count is disregarded.
- Reading properties of a tag with TagGetProperty() or TagSubscribe() will cause that tag to be included in the point count, even if the value is not read.
- Persisted I/O (memory devices), local variables and disk I/O variable tags will not count towards the dynamic point count, unless they are written to by an external source (via OPC, DDE, ODBC, or CTAPI). For example, if you use an OPC client to write to a local variable, each local variable will be counted once the first time it is used.

Note: You can use the CitectInfo() Cicode function or the General page in the Kernel to determine the point count status of a client process. See the Licensing Statistics for the Page General Kernel command in the Citect SCADA documentation.

Demo Mode

You can run Citect SCADA without the hardware key in demonstration (demo) mode. Demo mode lets you use every Citect SCADA feature normally, but with runtime and I/O restrictions.

In demo mode, you can run multiple processes (with the networking model selected as "stand alone"), or in single process mode.

The following demonstration modes are available:

- 15 minutes with a maximum of 50,000 real I/O.
- 10 hours with a maximum of one dynamic real I/O. This is useful for demonstrations using memory and disk I/Os. Citect SCADA starts in this mode if no hardware key is available. If the system detects that you are using more than one real I/O point at runtime, then it will swap to the 15 minutes demo mode.

Note: Writing to any tag through DDE, CTAPI, or ODBC will cause that tag to contribute to the dynamic point count even if it is a memory or disk I/O point. So if you write to more than one point through these interfaces, it will swap to the 15 minute demo mode.

Chapter 5: Installation

The Installation Process

Note: Backup your existing projects then uninstall prior versions before installing 2018 R2, as Citect SCADA does not support different versions running side-by-side.

Note: If you have an existing installation of OFS (OPC Factory Server), you will need to uninstall it before proceeding with the installation of Citect SCADA. To uninstall OFS select OPC Factory Server from the list displayed in the Windows Add or Remove Programs dialog, then follow the on screen instructions.

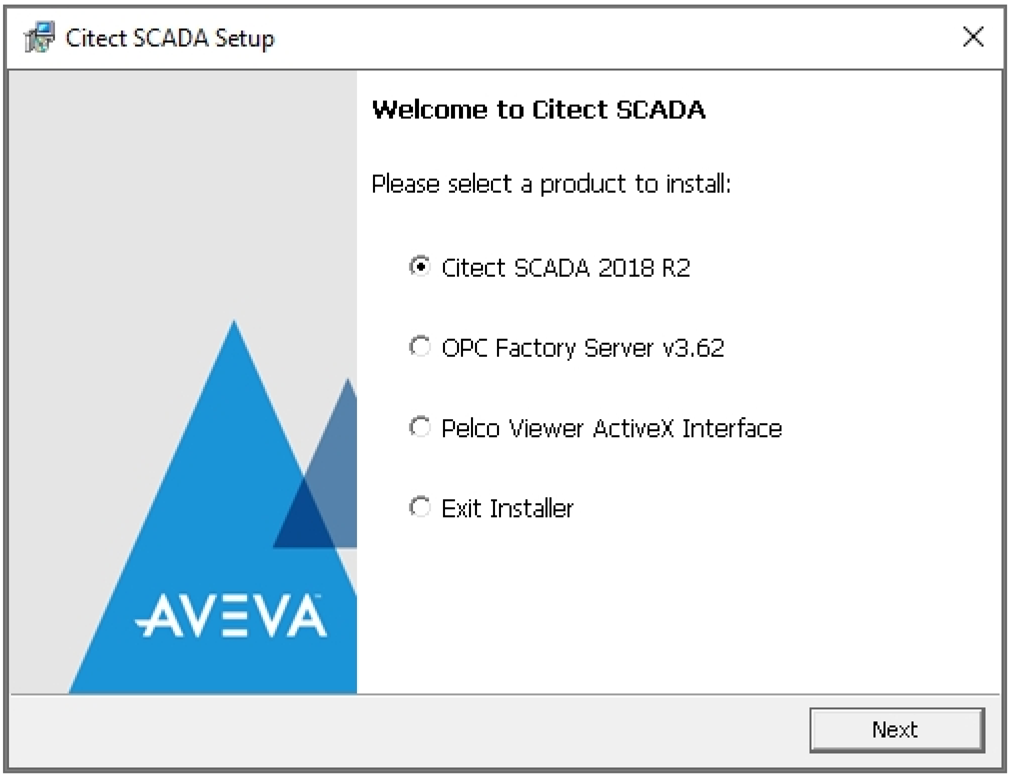
Note: Remove existing Floating License Managers installations before installing the new version.

Preliminary Installation

Make sure Windows Update is not running when you attempt to install Citect SCADA.

When you begin the installation any additional system software that is necessary will be installed prior to the initial Citect SCADA Setup dialog being displayed.

1. To begin the installation, locate and run Launch.exe on your installation media to display the initial **Citect SCADA Setup** dialog.



Citect SCADA Setup

Welcome to Citect SCADA

Please select a product to install:

● Citect SCADA 2018 R2

○ OPC Factory Server v3.62

○ Pelco Viewer ActiveX Interface

○ Exit Installer

When the Citect SCADA Setup dialog is displayed choose which application you wish to install.

NOTICE

You must install Citect SCADA before you install the OPC Factory Server to have the OFS Server licensed using the Citect SCADA license key. This will allow the correct Part and Serial number combination to be registered during the OFS Server installation.

The **OPC Factory Server**, based on the OPC protocol, software enables Windows client applications to communicate with PLCs of the TSX Compact, micro, TSX Momentum, TSX/PCX Premium, Quantum, M340, TSX Series 7 and TSX S1000 families in order to supply the OPC clients with data.

If you choose the OPC Factory Server follow the on screen instruction. Complete details on the installation options for OPC Factory Server can be found in the OPC Factory Server User Manual located in OFS v3.62\Documentation on the installation media.

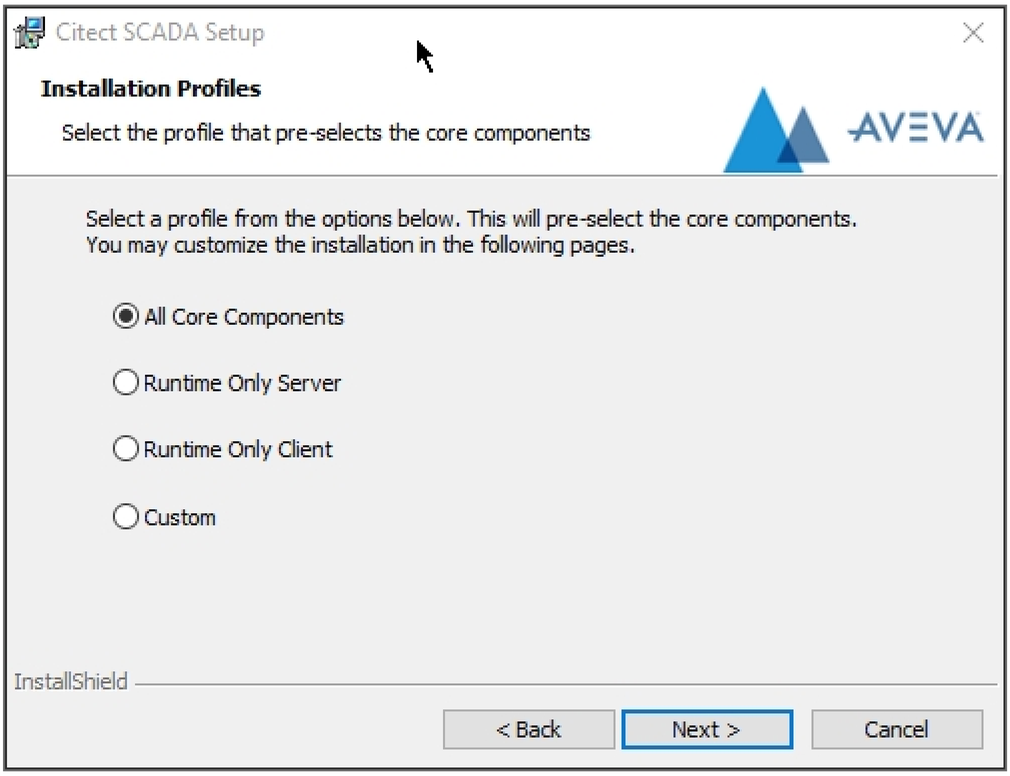
If you choose the Citect SCADA installation, click **Next** to display the Welcome to Citect SCADA dialog.

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

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 recommended that you read them.
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 radio 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 require. For information on the profiles and their application components refer to Chapter 3, "Installation Description".



Citect SCADA Setup

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

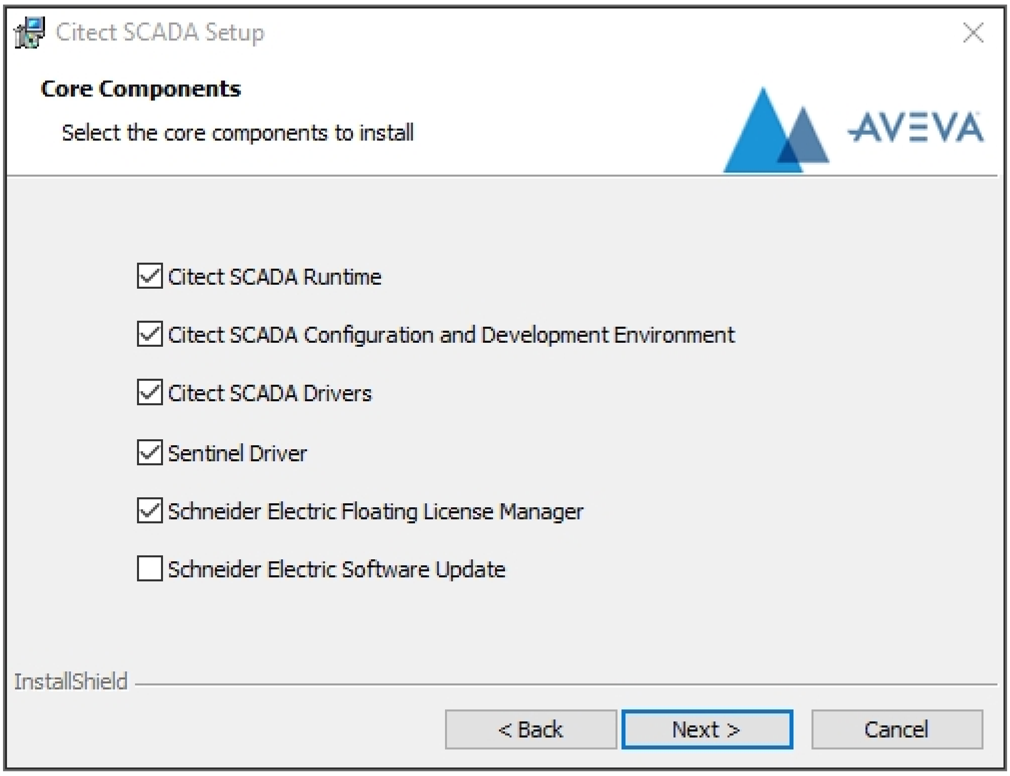
○ Runtime Only Server

○ 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.



Core Components

Select the core components to install

☑ Citect SCADA Runtime

☑ Citect SCADA Configuration and Development Environment

☑ Citect SCADA Drivers

☑ Sentinel Driver

☑ Schneider Electric Floating License Manager

□ Schneider Electric Software Update

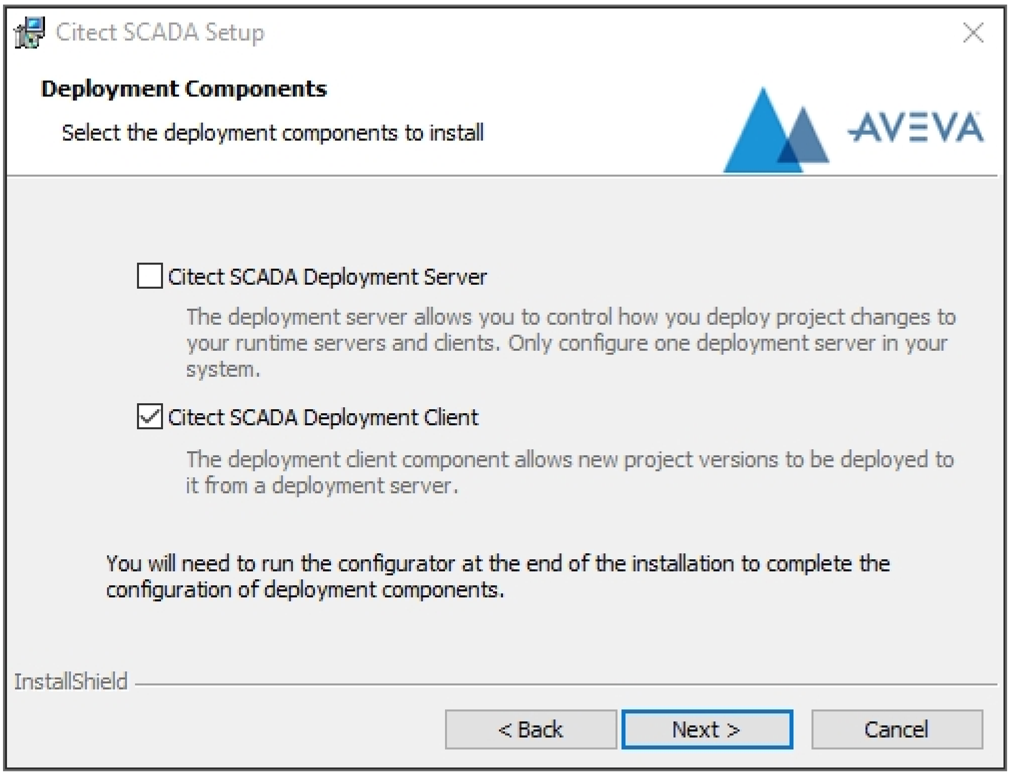
This dialog allows you to change the selected components if you wish to have a different installation configuration from the default provided by the profile which you chose in the previous step.

Note: For the Deployment Client to be installed, the Citect SCADA2018 R2 Runtime option needs to be selected.

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 installation to a full Configuration and Development Environment, you will need to select the Sentinel Driver option so that the hardware protection key will be recognized.

Note: Remove existing Floating License Manager installations before installing the new version.

3. Click **Next** to display the **Deployment Components** dialog.



Citect SCADA Setup

Deployment Components

Select the deployment components to install

□ Citect SCADA Deployment Server

The deployment server allows you to control how you deploy project changes to your runtime servers and clients. Only configure one deployment server in your system.

☑ Citect SCADA Deployment Client

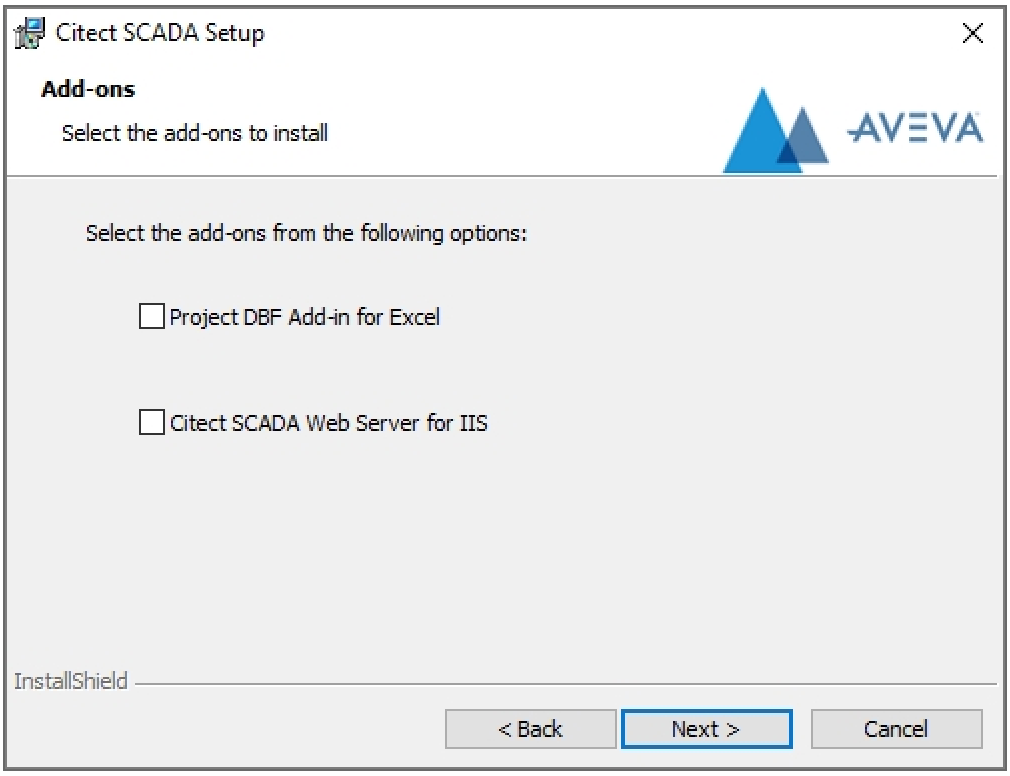
The deployment client component allows new project versions to be deployed to it from a deployment server.

You will need to run the configurator at the end of the installation to complete the configuration of deployment components.

By default, the **Deployment Server** option is not selected. If you plan to use the computer as a deployment server, select this option. You will be able to launch the deployment server configuration tool when installation is complete.

The **Deployment Client** option is selected by default and allows new project versions to be deployed to the current computer from a deployment server.

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



Citect SCADA Setup

Add-ons

Select the add-ons to install

Select the add-ons from the following options:

□ Project DBF Add-in for Excel

□ Citect SCADA Web Server for IIS

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

The options are:

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

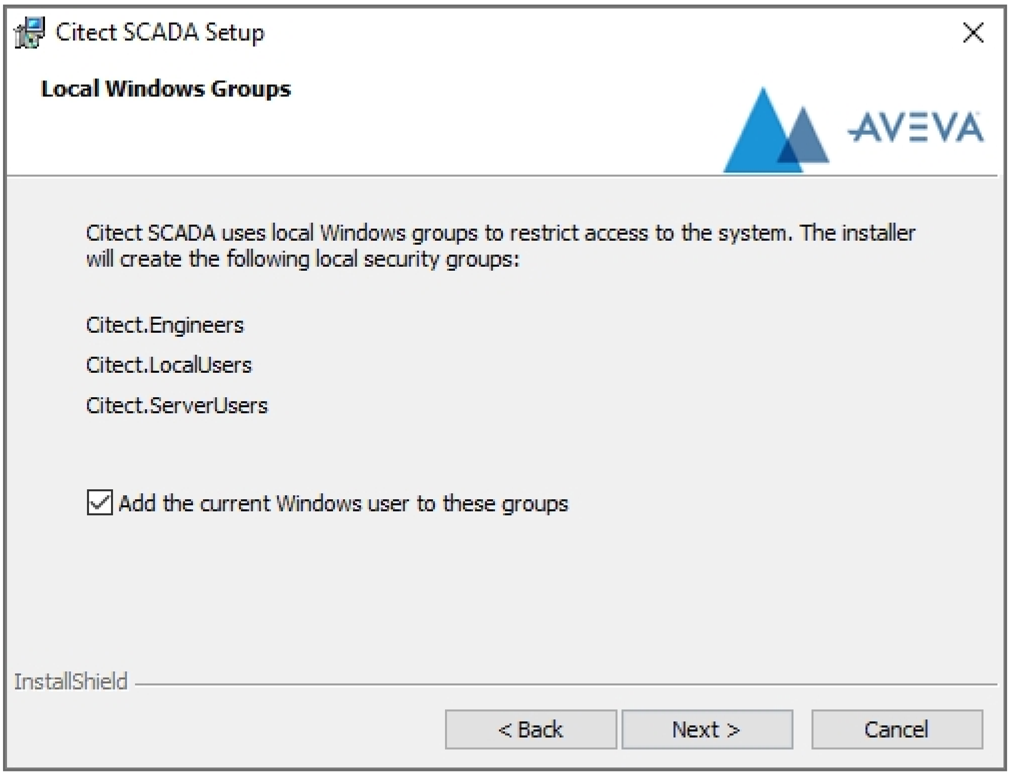
Refer to "Installation Description", for a description of these optional Add-on components.

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. Click **Next** to display the **Local Windows Groups** dialog.



Citect SCADA uses local Windows groups to restrict access to the system. The installer will create the following local security groups:

Citect.Engineers

Citect.LocalUsers

Citect.ServerUsers

☑ Add the current Windows user to these groups

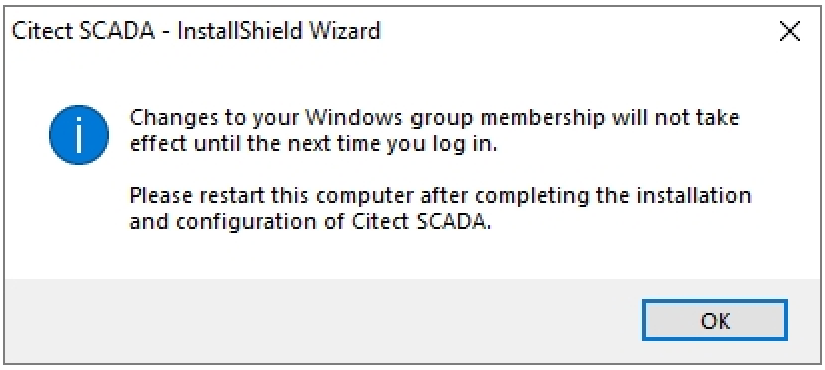
The Local Windows Groups dialog allows you to add the user that is currently logged on to the following Windows groups: Citect.Engineers, Citect.LocalUsers and Citect.ServerUsers. To add the current user to these groups, select **Add the current Windows user to these groups**.

Adding the user to these groups will give them access to certain security-related operations within the engineering and runtime environments. Details of these groups and their purpose are outlined below.

Windows User Group Name	Description
Citect.Engineer	Users in this group can read and write the server to server password. This user corresponds to a user who would run the Setup Wizard activities (either in Citect Studio or the Configurator). Users in the group have all privileges available to users in the other two groups.
Citect.Server-Users	Controls which users can run Citect SCADA as a server process. This group is used to limit access to the server password which is used in server to server communications. If you are not running Citect SCADA as a service, any Windows user who needs to run a Citect SCADA server (including a display client with [CtAPI]Remote enabled needs to be added to this group.

Windows User Group Name	Description
	Note: If you are running Citect SCADA as a service, it is recommended that you do not add users to this group.
Citect.LocalUsers	Users in this group have access to the local CtAPI interface exposed by Citect SCADA client processes. This group can be used to restrict CtAPI access to pre-determined users or services.

Click **Next**. The following message is displayed.

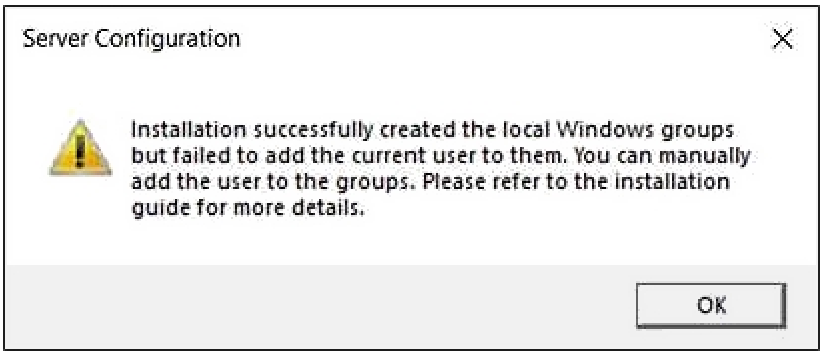


Citect SCADA - InstallShield Wizard

Changes to your Windows group membership will not take effect until the next time you log in.

Please restart this computer after completing the installation and configuration of Citect SCADA.

If the currently logged in user does not have permissions to read/update Windows group membership, the following message will be displayed:

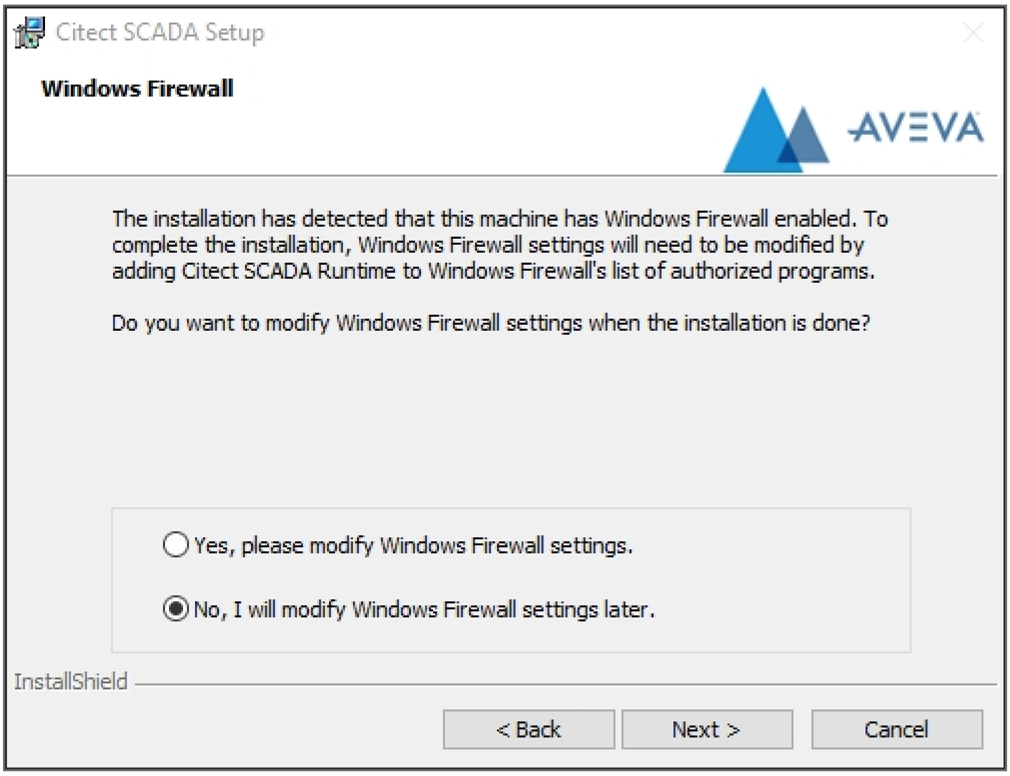


Server Configuration

Installation successfully created the local Windows groups but failed to add the current user to them. You can manually add the user to the groups. Please refer to the installation guide for more details.

Click **OK**, and then manually add the user to the required groups after the installation is complete.

6. Click **OK** to continue. If the installer detects that the computer has Windows™ Firewall enabled, you will be asked if you would like the installer to modify your Windows Firewall settings.



Citect SCADA Setup

Windows Firewall

The installation has detected that this machine has Windows Firewall enabled. To complete the installation, Windows Firewall settings will need to be modified by adding Citect SCADA Runtime to Windows Firewall's list of authorized programs.

Do you want to modify Windows Firewall settings when the installation is done?

○ Yes, please modify Windows Firewall settings.

● No, I will modify Windows Firewall settings later.

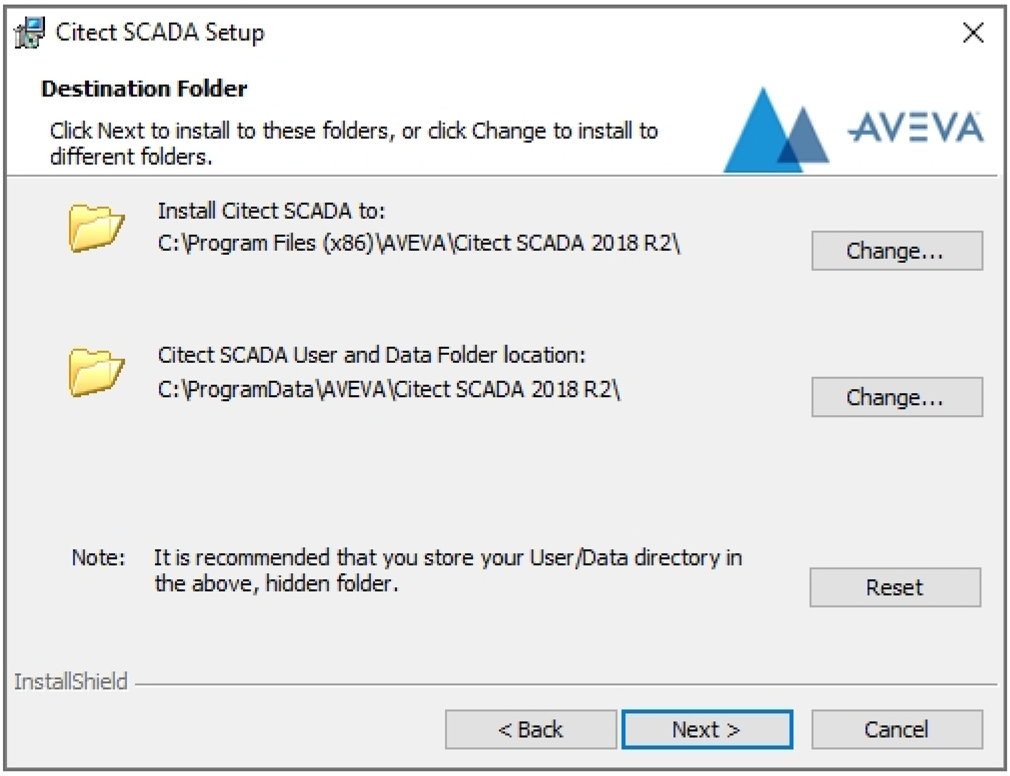
If you select **Yes**, this will add Citect SCADA Runtime to the list of authorized programs.

When you have made your selection, click **Next**.

7. Proceed to Completing the Installation.

Completing the Installation

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



Citect SCADA Setup

Destination Folder

Click Next to install to these folders, or click Change to install to different folders.

Install Citect SCADA to:
C:\Program Files (x86)\AVEVA\Citect SCADA 2018 R2\

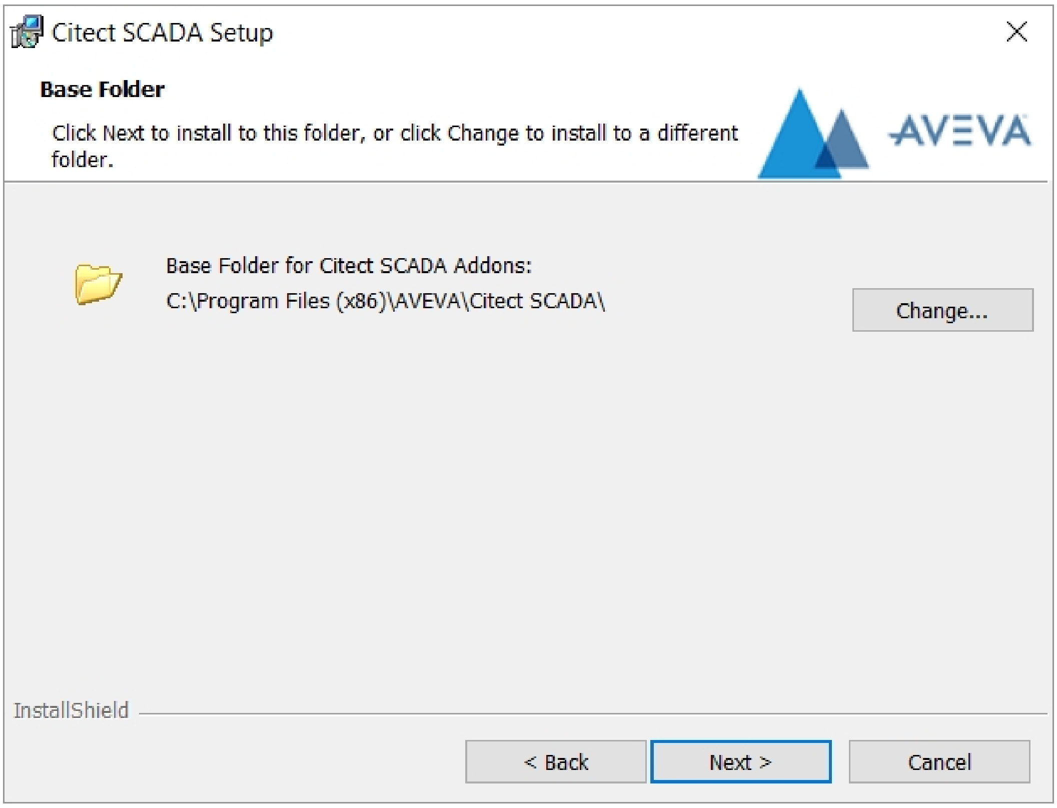
Citect SCADA User and Data Folder location:
C:\ProgramData\AVEVA\Citect SCADA 2018 R2\

Note: It is recommended that you store your User/Data directory in the above, hidden folder.

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.

The **Base Folder** dialog identifies the base folder into which the additional or optional components of Citect SCADA that you have selected will be installed. You may change the folder location by clicking the **Change** buttons and selecting an alternative location.



Citect SCADA Setup

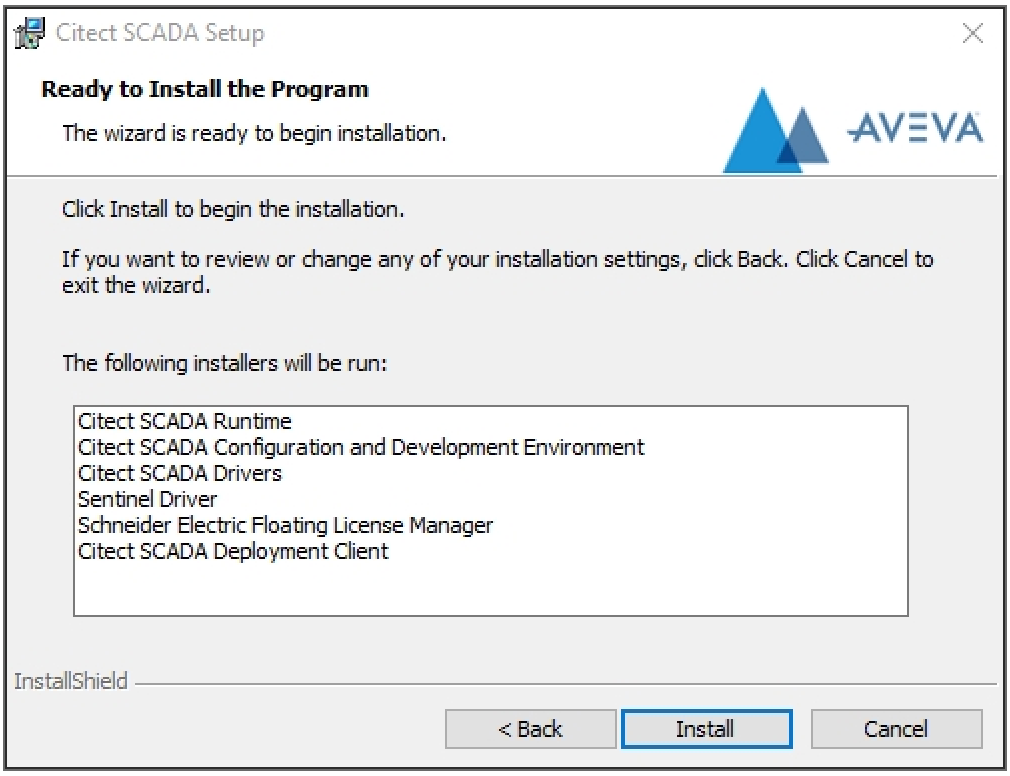
Base Folder

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

Base Folder for Citect SCADA Addons:
C:\Program Files (x86)\AVEVA\Citect SCADA\

If you are satisfied with the folder selection, click **Next** to display the **Ready to Install the Program** dialog.

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



Citect SCADA Setup

Ready to Install the Program

The wizard is ready to begin installation.

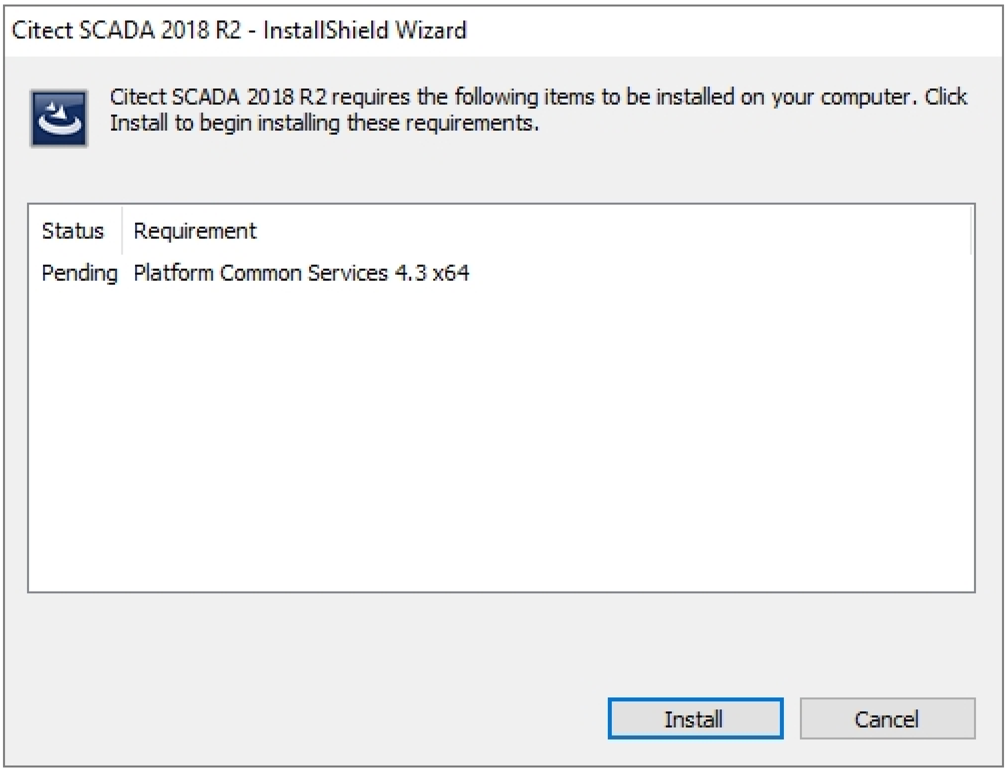
Click Install to begin the installation.

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:

Citect SCADA Runtime
Citect SCADA Configuration and Development Environment
Citect SCADA Drivers
Sentinel Driver
Schneider Electric Floating License Manager
Citect SCADA Deployment Client

3. 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.
4. Click **Install** to install the programs in the list. The installer prompts you to install Platform Common Services. This is required for configuring the System Management Server for encrypted communications.



Citect SCADA 2018 R2 - InstallShield Wizard

Citect SCADA 2018 R2 requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	Platform Common Services 4.3 x64

5. Click **Install**. A progress bar is displayed for Platform Common Services installation.
6. Then, the Installing **Citect SCADA** 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.

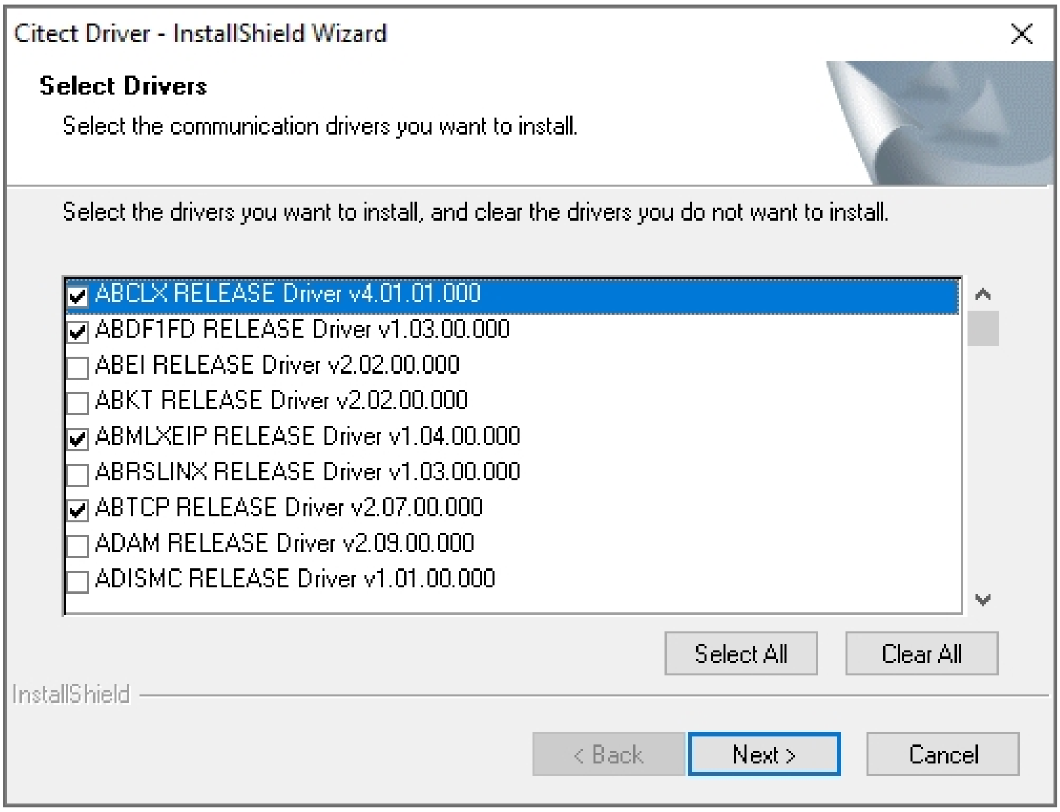
> **Note**: If you selected the **Add the current Windows user to these groups** on the Local Windows Groups dialog, restart your computer and log on as the current user to be added to these groups.

Communication Drivers

If Citect SCADA 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.



Citect Driver - InstallShield Wizard

Select Drivers

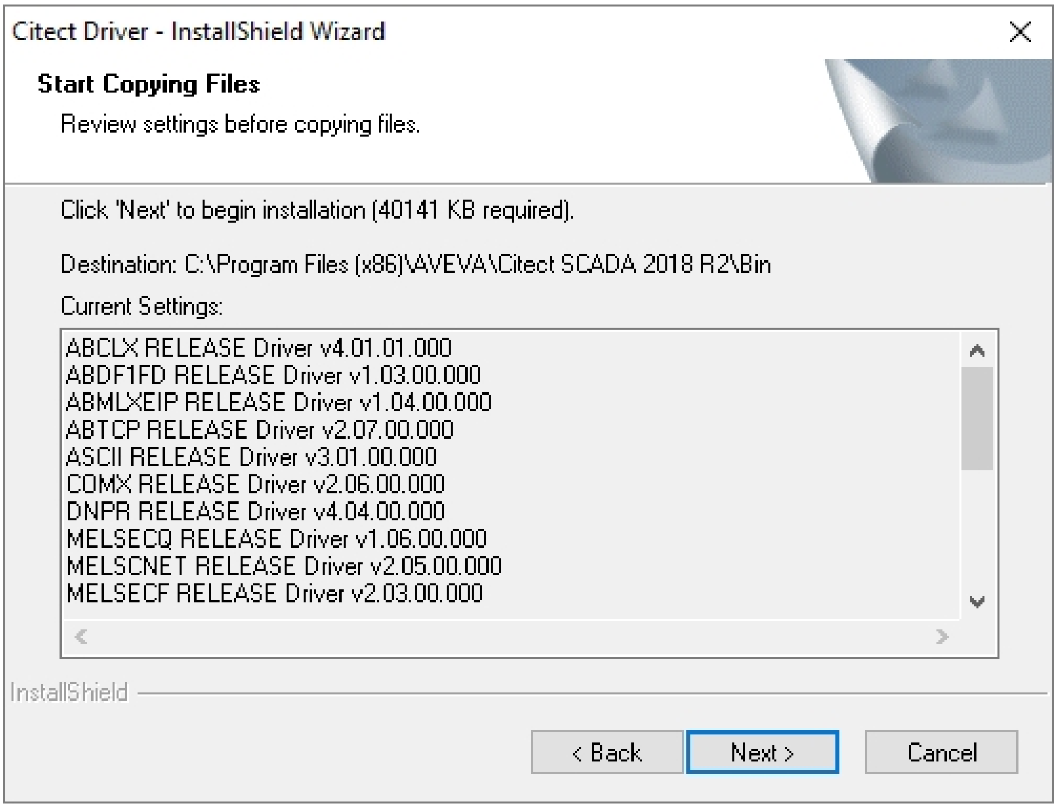
Select the communication drivers you want to install.

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

☑ ABCLX RELEASE Driver v4.01.01.000
☑ ABDF1FD RELEASE Driver v1.03.00.000
□ ABEI RELEASE Driver v2.02.00.000
□ ABKT RELEASE Driver v2.02.00.000
☑ ABMLXEIP RELEASE Driver v1.04.00.000
□ ABRSLINX RELEASE Driver v1.03.00.000
☑ ABTCP RELEASE Driver v2.07.00.000
□ ADAM RELEASE Driver v2.09.00.000
□ ADISMC RELEASE Driver v1.01.00.000

The **Driver Selection** dialog lists the drivers that are available for installation. There are certain drivers that the product installation will install that are necessary for Citect SCADA to function correctly. These are not displayed in the list and will be installed automatically as in previous releases. For convenience, 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 drivers that you wish to install. You can select every driver by clicking the **Select All** button. Then click the **Next** button to display the **Driver Information** dialog.



Citect Driver - InstallShield Wizard

Start Copying Files

Review settings before copying files.

Click 'Next' to begin installation (40141 KB required).

Destination: C:\Program Files (x86)\AVEVA\Citect SCADA 2018 R2\Bin

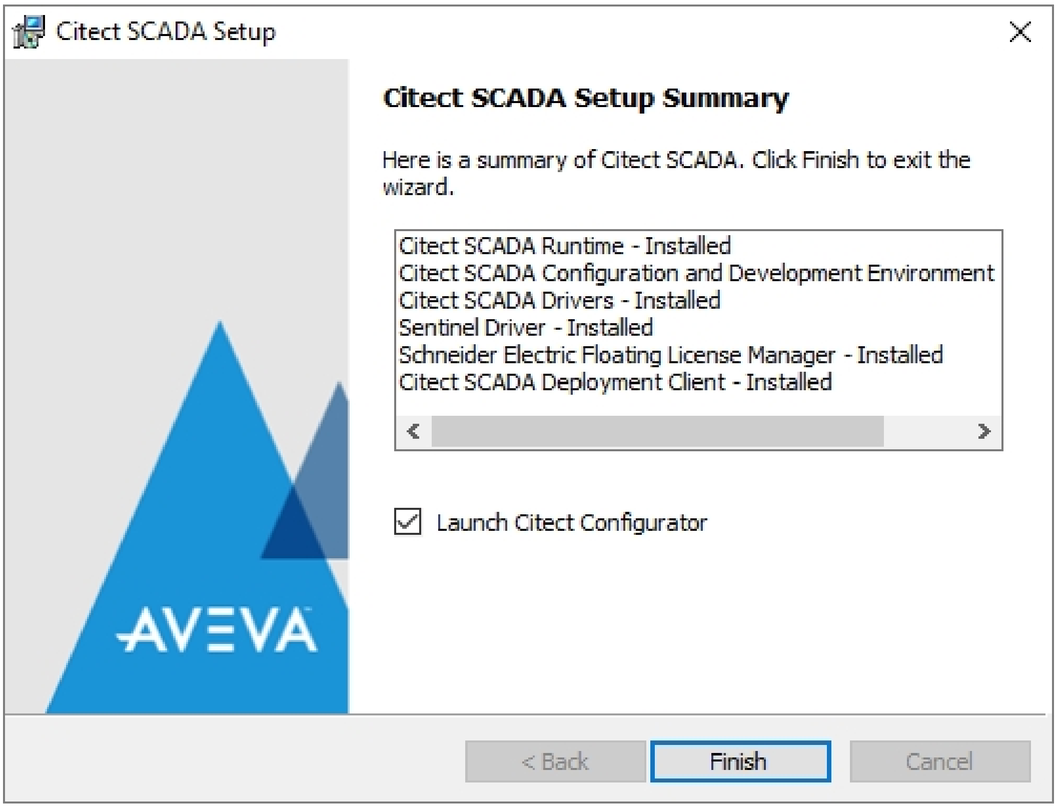
Current Settings:

```
ABCLX RELEASE Driver v4.01.01.000
ABDF1FD RELEASE Driver v1.03.00.000
ABMLXEIP RELEASE Driver v1.04.00.000
ABTCP RELEASE Driver v2.07.00.000
ASCII RELEASE Driver v3.01.00.000
COMX RELEASE Driver v2.06.00.000
DNPR RELEASE Driver v4.04.00.000
MELSECQ RELEASE Driver v1.06.00.000
MELSCNET RELEASE Driver v2.05.00.000
MELSECF RELEASE Driver v2.03.00.000
```

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. In particular, some drivers may have not yet been confirmed to operate correctly, or have been confirmed specifically to not operate correctly with the supported 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, 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.

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.



Citect SCADA Setup

Citect SCADA Setup Summary

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

Citect SCADA Runtime - Installed
Citect SCADA Configuration and Development Environment
Citect SCADA Drivers - Installed
Sentinel Driver - Installed
Schneider Electric Floating License Manager - Installed
Citect SCADA Deployment Client - Installed

☑ Launch Citect Configurator

If you wish to configure your deployment server now, select **Launch Citect Configurator**. Clear the selection and click **Finish** to close the installation dialog. You can configure your Deployment Server at a later stage by launching the Citect Configurator from **Start Programs**, **AVEVA**, **Common**, **Configurator**.

Installing Additional Communication Drivers

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

To install additional drivers:

1. From the Installation media, locate the CitectDriverInstaller.exe file located in the root directory.

> **Note:** If you are using the Microsoft® Windows operating system and have User Account Control (UAC) switched on the UAC dialog will display when you open the file. You will be required 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 an alert message will be generated. In other words, the location needs to have an existing Citect SCADA 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.

Modify, Repair, or Remove Components

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

> **Note:** The Citect SCADA 2018 R2 installation can only be removed using this operation. You cannot Modify or Repair this installation. In order to Modify or Repair this installation you need to re-install it from the main Citect SCADA 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 Citect SCADA program on which you want to carry out the operation from the list.

The available maintenance operations are shown below.

- **Modify** allows you to add Citect SCADA 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 Citect SCADA 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** Citect SCADA component files and remove all the registry entries. This will restore the computer to the state prior to installation of the Citect SCADA 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 Citect SCADA component will be uninstalled.

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

In addition, you will need to separately uninstall OFS (OPC Factory Server) and the OFS Configuration Tool. To uninstall these applications, use the same procedure as for uninstalling Citect SCADA, but select OPC Factory Server from the list displayed in the Add or Remove Programs dialog, then follow the on screen instructions. After OPC Factory Server has been uninstalled, select OFS Configuration Tool from the list displayed in the Add or Remove Programs dialog, then follow the on screen instructions.

Chapter 6: Configuration

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

You can use TCP/IP with Citect SCADA. Citect SCADA supports scalable architecture, which lets you initially implement Citect SCADA 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 Citect SCADA 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 Citect SCADA 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 Citect SCADA system. The configuration steps are described in this chapter.

Configure a System Management Server

Citect SCADA needs post-installation configuration in order to use encrypted communications. Configure a **System Management Server** using the **Configurator** dialog once you have installed Citect SCADA.

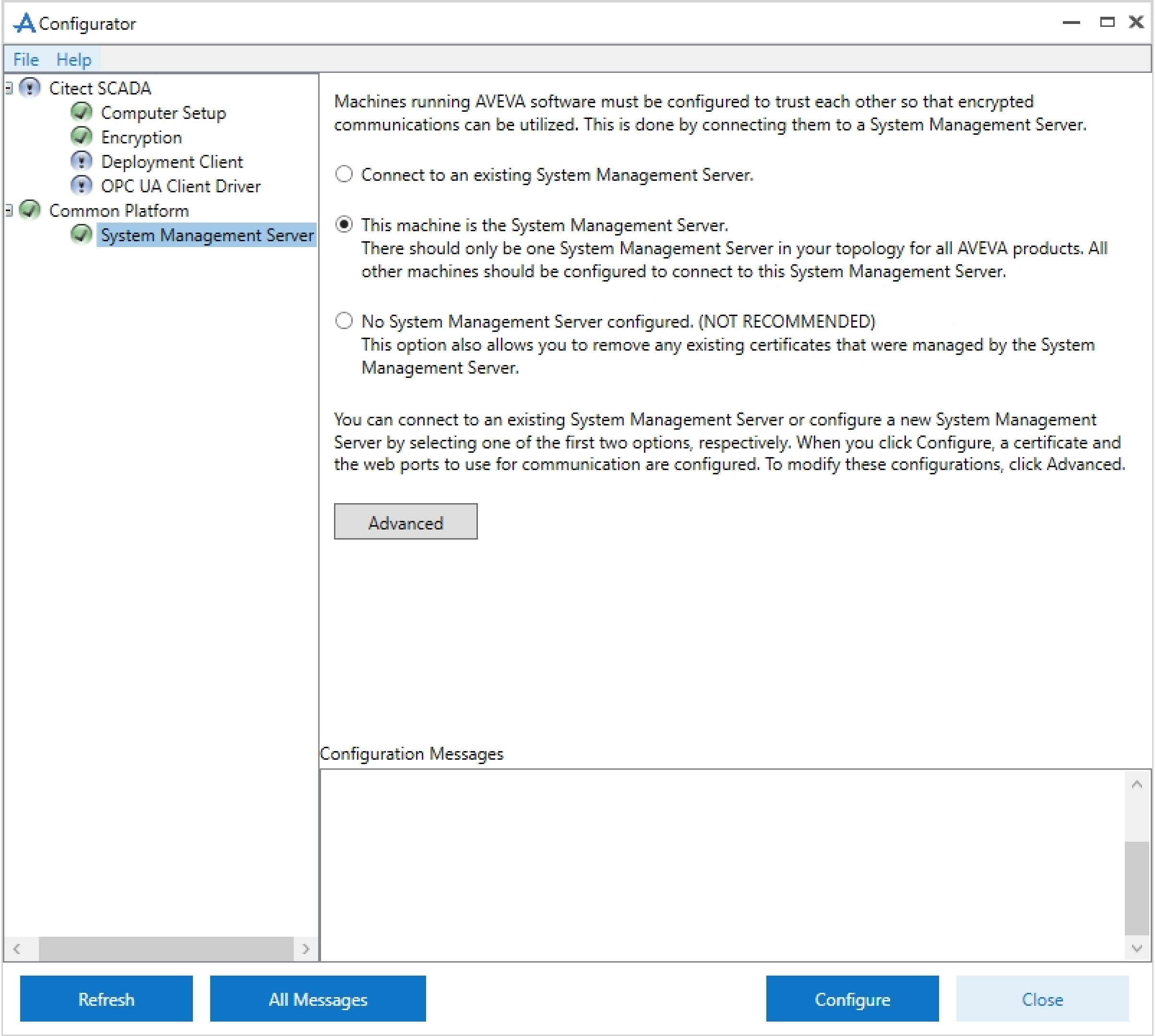
This section provides information about configuring the **System Management Server**. Only one of the machines in the network can be identified and configured as the **System Management Server**.

Use the **Configurator** to establish a trusted relationship between one or more machines running Citect SCADA. This configuration allows for encrypted communication between these machines, which is achieved through a common **System Management Server** on which a certificate is created and used to encrypt communications. Certificates may be generated automatically on the System Management Server or provided by the IT department.

> **Note**: To connect to the System Management Server, you need to be a member of either the “aaAdministrators” or the “Administrators” group on the machine where the System Management Server is installed.

To configure the System Management Server

1. Start the **Configurator**.
2. In the left pane, click **Common Platform**, **System Management Server**. The following is displayed:



Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.

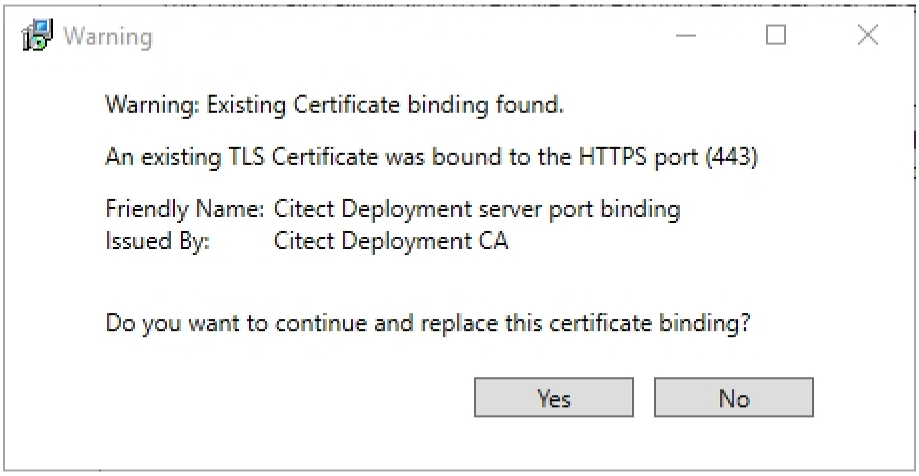
○ Connect to an existing System Management Server.

● This machine is the System Management Server.
There should only be one System Management Server in your topology for all AVEVA products. All other machines should be configured to connect to this System Management Server.

○ No System Management Server configured. (NOT RECOMMENDED)
This option also allows you to remove any existing certificates that were managed by the System Management Server.

You can connect to an existing System Management Server or configure a new System Management Server by selecting one of the first two options, respectively. When you click Configure, a certificate and the web ports to use for communication are configured. To modify these configurations, click Advanced.

3. Select **This machine is the System Management Server**. Review the notes on the screen before you start the configuration.
4. Click **Configure**. If an existing binding is found for the specified ports, the following message is displayed.



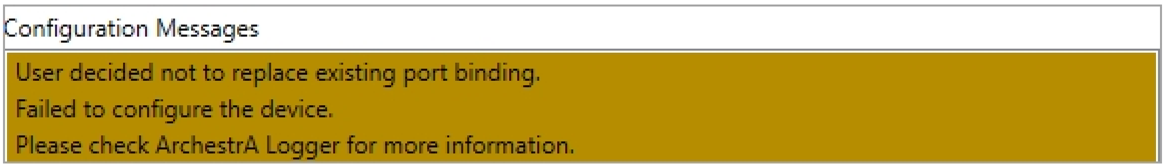
Warning: Existing Certificate binding found.

An existing TLS Certificate was bound to the HTTPS port (443)

Friendly Name: Citect Deployment server port binding
Issued By: Citect Deployment CA

Do you want to continue and replace this certificate binding?

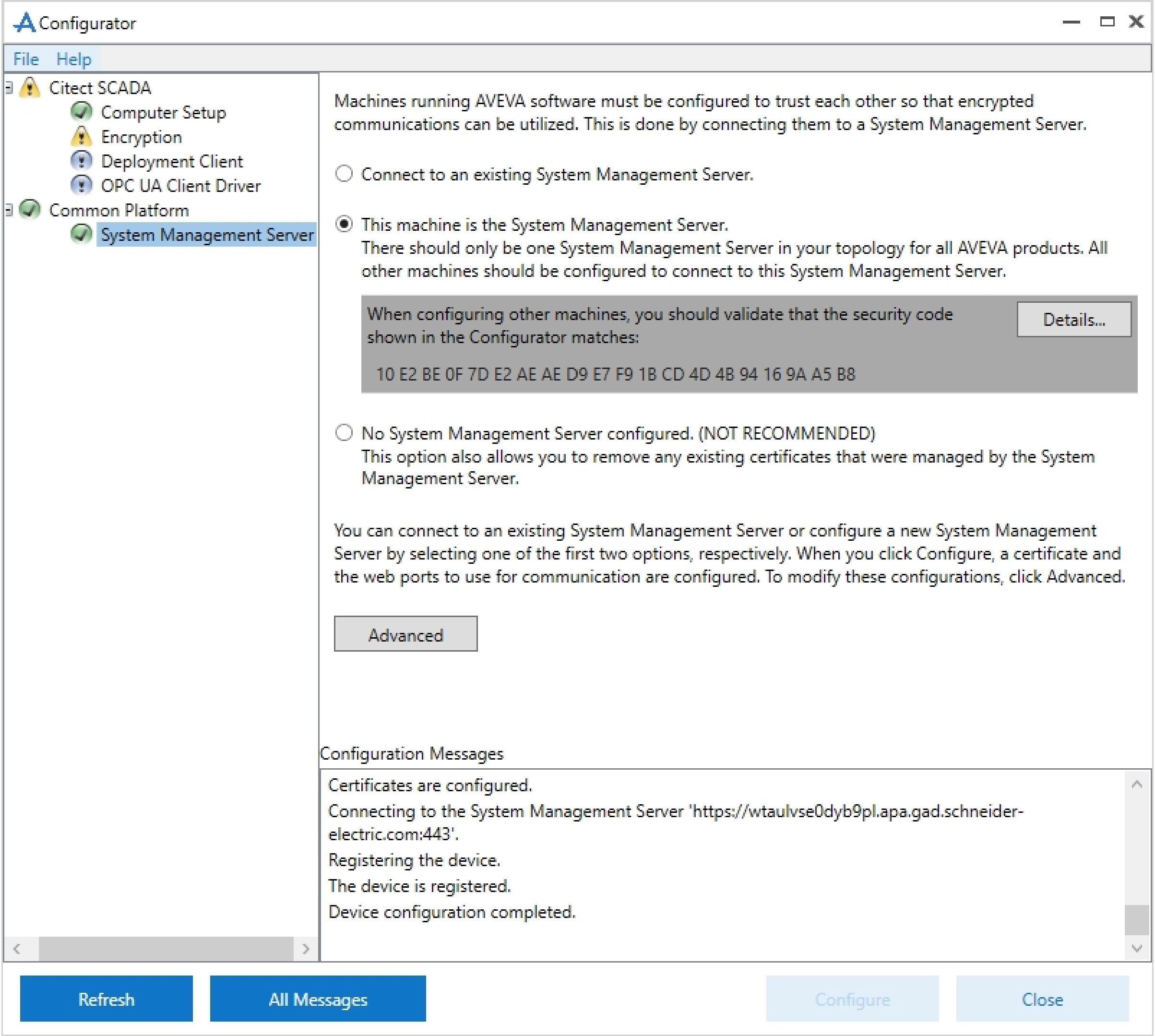
5. Click **No** if you do not want to replace the existing binding. The following message will be displayed in the Configuration Messages area. If you wish to configure the System Management Server on a different port, click **Advanced**. For more information, see the *Advanced Configuration* section.



Configuration Messages

User decided not to replace existing port binding.
Failed to configure the device.
Please check ArchestrA Logger for more information.

6. Click **Yes** if you wish to replace the binding. The **Configurator** will start configuring the System Management Server.
7. On successful configuration, the message "Device configuration completed" is displayed. The security code is displayed in the **Configurator** as shown below. To view more information about the certificate, click **Details**.



Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.

○ Connect to an existing System Management Server.

● This machine is the System Management Server.
There should only be one System Management Server in your topology for all AVEVA products. All other machines should be configured to connect to this System Management Server.

When configuring other machines, you should validate that the security code shown in the Configurator matches:

10 E2 BE 0F 7D E2 AE AE D9 E7 F9 1B CD 4D 4B 94 16 9A A5 B8

○ No System Management Server configured. (NOT RECOMMENDED)
This option also allows you to remove any existing certificates that were managed by the System Management Server.

You can connect to an existing System Management Server or configure a new System Management Server by selecting one of the first two options, respectively. When you click Configure, a certificate and the web ports to use for communication are configured. To modify these configurations, click Advanced.

Configuration Messages

```
Certificates are configured.
Connecting to the System Management Server 'https://wtaulvse0dyb9pl.apa.gad.schneider-electric.com:443'.
Registering the device.
The device is registered.
Device configuration completed.
```

If the configuration is unsuccessful, check the ArchestrA Logger, located at:

C:\Program Files (x86)\Common Files\ArchestrA\aalogviewer.exe

Alternatively, you can view details in the System Management Console. For more details, refer to the ArchestrA documentation.

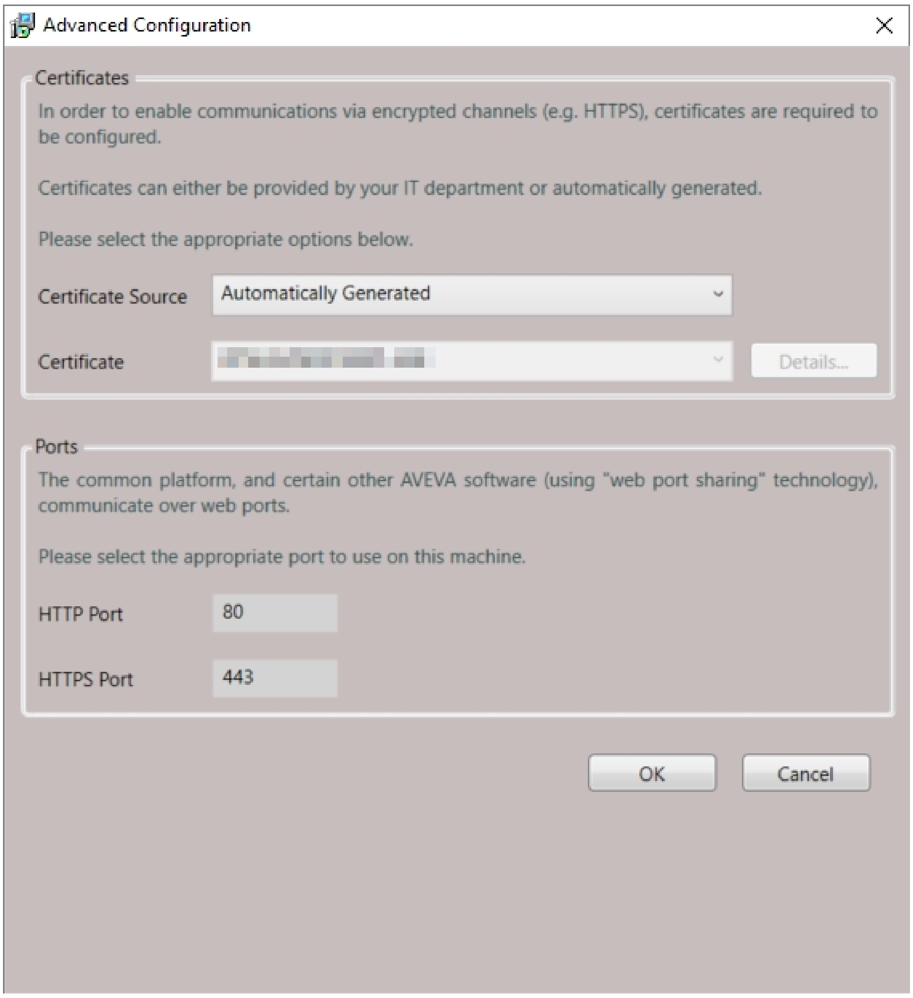
8. Click **Close** to exit the **Configurator**.

Advanced Configuration

If you have already configured a **System Management Server** or have selected a **System Management Server** to connect to, the configuration may be modified if it is required.

To modify an existing configuration:

1. Click **Advanced**. The **Advanced Configuration** dialog is displayed.



Certificates

In order to enable communications via encrypted channels (e.g. HTTPS), certificates are required to be configured.

Certificates can either be provided by your IT department or automatically generated.

Please select the appropriate options below.

Certificate Source: Automatically Generated

Certificate: [redacted]

Ports

The common platform, and certain other AVEVA software (using "web port sharing" technology), communicate over web ports.

Please select the appropriate port to use on this machine.

HTTP Port: 80

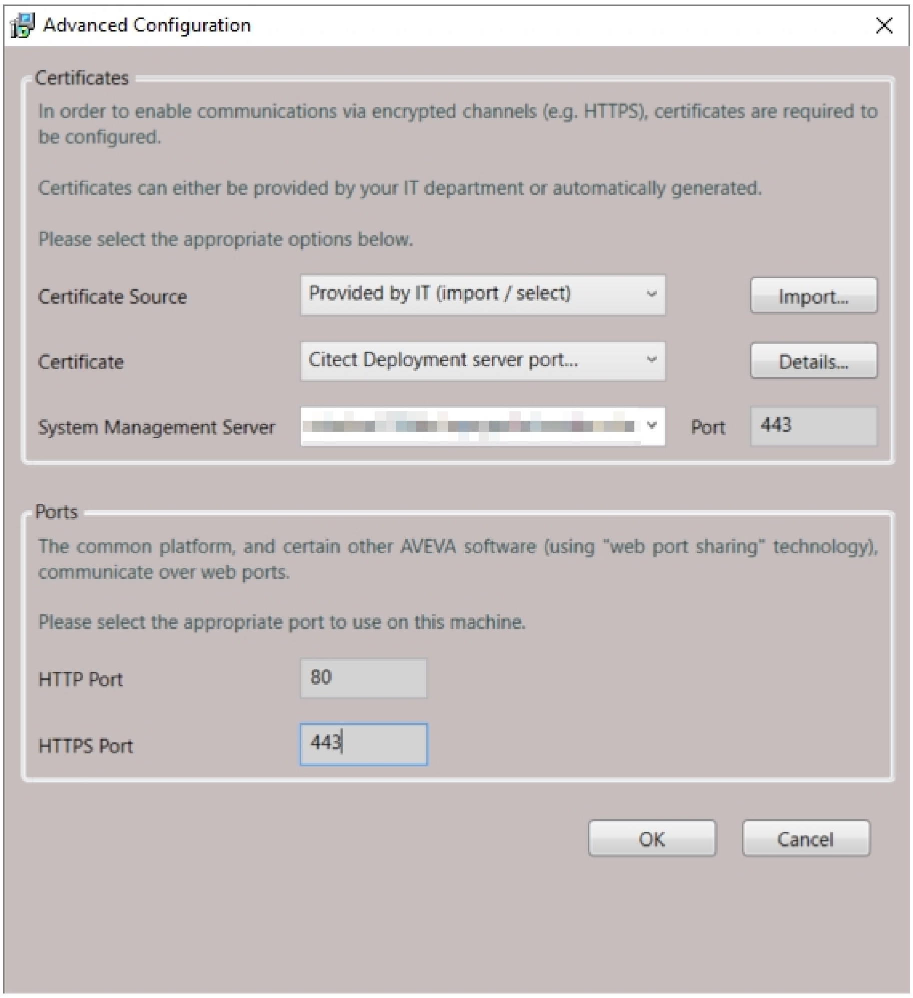
HTTPS Port: 443

2. If you want the Configurator to generate a certificate, select **Automatically Generated** from the **Certificate Source** list. This is the default (shown above).

   The Certificate field is disabled if this option is selected, or if certificates generated earlier have been deleted. To view more information about the certificate, click **Details**.

> **Note**: Automatically generated certificates are renewed automatically.

3. If you want to use a certificate generated by your IT Department, select Provided by IT (import/select) from the Certificate Source list.



Advanced Configuration

Certificates

In order to enable communications via encrypted channels (e.g. HTTPS), certificates are required to be configured.

Certificates can either be provided by your IT department or automatically generated.

Please select the appropriate options below.

Certificate Source: Provided by IT (import / select)

Certificate: Citect Deployment server port...

System Management Server: Port 443

Ports

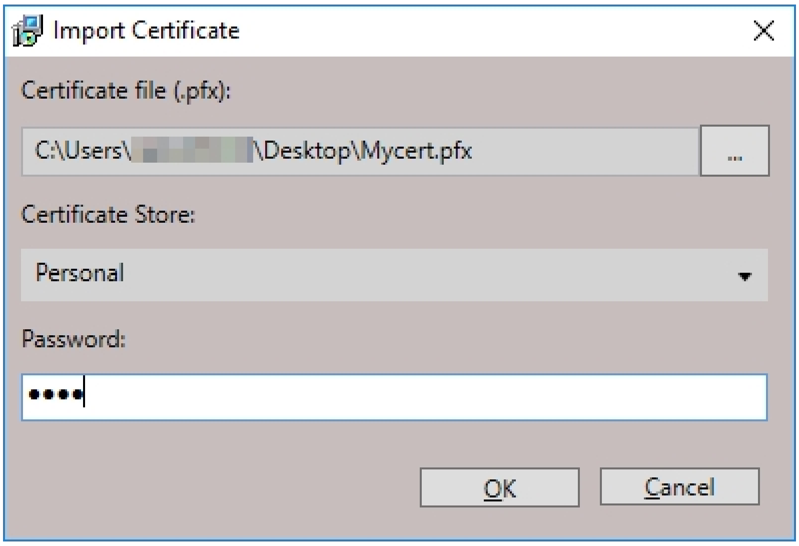
The common platform, and certain other AVEVA software (using "web port sharing" technology), communicate over web ports.

Please select the appropriate port to use on this machine.

HTTP Port: 80

HTTPS Port: 443

4. From the **Certificate** list, select the certificate you want to use.
5. To use a certificate not listed in the **Certificate** list, click **Import**. The **Import Certificate** dialog is displayed.



Import Certificate

Certificate file (.pfx): C:\Users\[redacted]\Desktop\Mycert.pfx

Certificate Store: Personal

Password: ••••

a. In the **Certificate file** field, click to select a certificate.
b. From the **Certificate Store** list, select the type of certificate to create – Root, Intermediate or Personal. Depending upon the type selected here, the certificate will be stored in the **Certificate Store** identified by the certificate type.
c. In the **Password** field, type the password for the selected **Certificate Store**.
d. Click **OK** to save the details and close the **Import Certificate** dialog.

> **Note**: The IT Department needs to renew certificates they generate as and when required.

6. To view the details of the certificate, click **Details** next to the **Certificate** field.
7. The **System Management Server** field is displayed only if you have selected the Connect to an existing System Management Server option in the previous screen. You can use this field to change to a different System Management Server. From the System Management Server list, select the machine on which you want the certificate to be generated.

> **Note**: You can only specify a computer name or a fully-qualified domain name for the System Management Server. Specifying the name in a different format, for example an IP address, may result in errors.

8. In the **Port** field, type the port number to be used. This is the port number on which the System Management Server is configured, and is automatically populated. It is recommended that you also check the port number manually.
9. In the Ports area, select the HTTP Port and HTTPS Port. The defaults are 80 and 443, respectively. These ports are local ports on the current machine, which are used by web services and clients connecting to this machine.

> **Note**: HTTP and HTTPS ports range from 0 to 65535. Within this range, you can choose any port that has not been blocked or is currently in use. Otherwise, you will get the "Port number conflict" error.

10. Click **OK** to save your settings. The Configurator's main screen is displayed.
11. Click **Configure**. The Configuration Messages area displays the steps in the configuration process and the progress. On successful configuration, the Certificate is generated on the selected **System Management Server** and its name is displayed in the Certificate field on the Advanced Configuration dialog.
12. If the configuration is unsuccessful, view details of the errors in the System Management Console. For details, refer to your Aveva product documentation.
13. Click **Close** to exit the **Configurator**.

Connect a Computer to a System Management Server

Computers running Citect SCADA need to connect to the **System Management Server** to use encrypted communication via a configured certificate.

> **Note**: If you do not have a System Management Server configured, refer to the section *Configure a System Management Server* for instructions. All AVEVA applications need to be configured to trust each other so that encrypted communications can be utilized.

To connect a machine to the System Management Server, you use the System Management Server plug-in via the **Configurator**.

> **Note**: The machine on which you want to install the System Management Server needs to be configured to have a static IP address.

The **Configurator** can be launched at the completion of the installation procedure, or from the Windows™ **Start** menu.

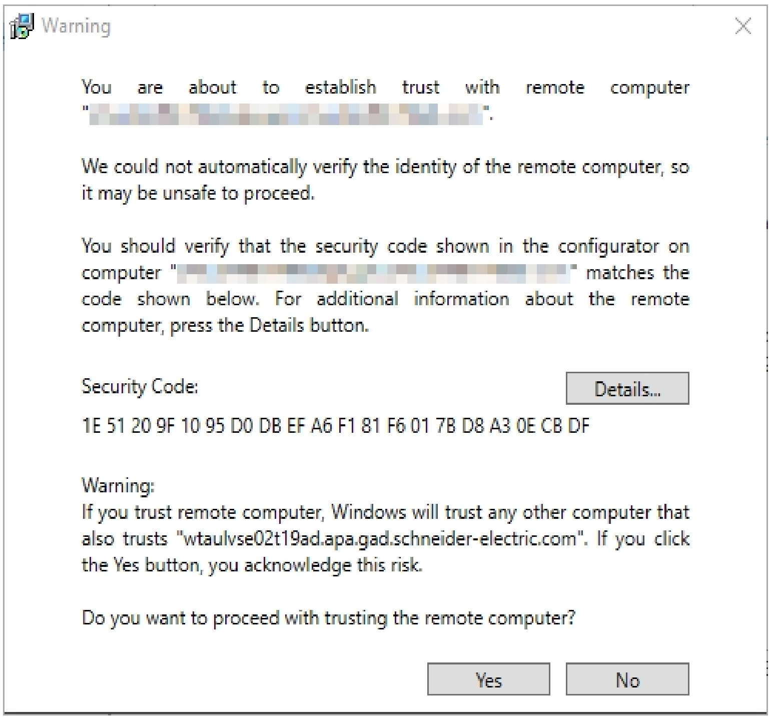
To connect your machine to the System Management Server:

> **Note**: To connect to the System Management Server, you need to be a member of either the "aaAdministrators" or the "Administrators" group on the machine where the System Management Server is installed.

1. In the panel on the left side of the **Configurator** select **Common Platform**, **System Management Server**.
2. Select the following option:

- **Connect to an existing System Management Server**: Select the name of the Management Server from the drop-down list. If the name does not appear in the list, type the Windows computer name of the machine on which the System Management Server is installed.

3. Click **Configure**. The root certificate is downloaded, and the following message is displayed.



You are about to establish trust with remote computer "[redacted]".

We could not automatically verify the identity of the remote computer, so it may be unsafe to proceed.

You should verify that the security code shown in the configurator on computer "[redacted]" matches the code shown below. For additional information about the remote computer, press the Details button.

Security Code:

1E 51 20 9F 10 95 D0 DB EF A6 F1 81 F6 01 7B D8 A3 0E CB DF

Warning:
If you trust remote computer, Windows will trust any other computer that also trusts "wtaulvse02t19ad.apa.gad.schneider-electric.com". If you click the Yes button, you acknowledge this risk.

Do you want to proceed with trusting the remote computer?

4. Review the message carefully before you click **Yes**. Clicking **No** will cancel the configuration process. A dialog box prompting you to log on to the Management Server is displayed.
5. Enter the credentials required to connect the machine to the Management Server and click **OK**.
6. The Configuration Messages area displays the steps in the configuration process and the progress.
7. If the configuration is unsuccessful, check the ArchestrA Logger. You can access this by typing \Program files (x86)\common files\archestra\aaLogviewer.exe at the Windows command prompt. Alternatively, view details of the errors in the System Management Console. For more details, refer to the ArchestrA documentation.
8. Click **Close** to exit the **Configurator**.

If you have already selected a Management Server to connect to, you can modify the configuration settings by selecting **Advanced**. Refer to the topic *Advanced Configuration* section for more information.

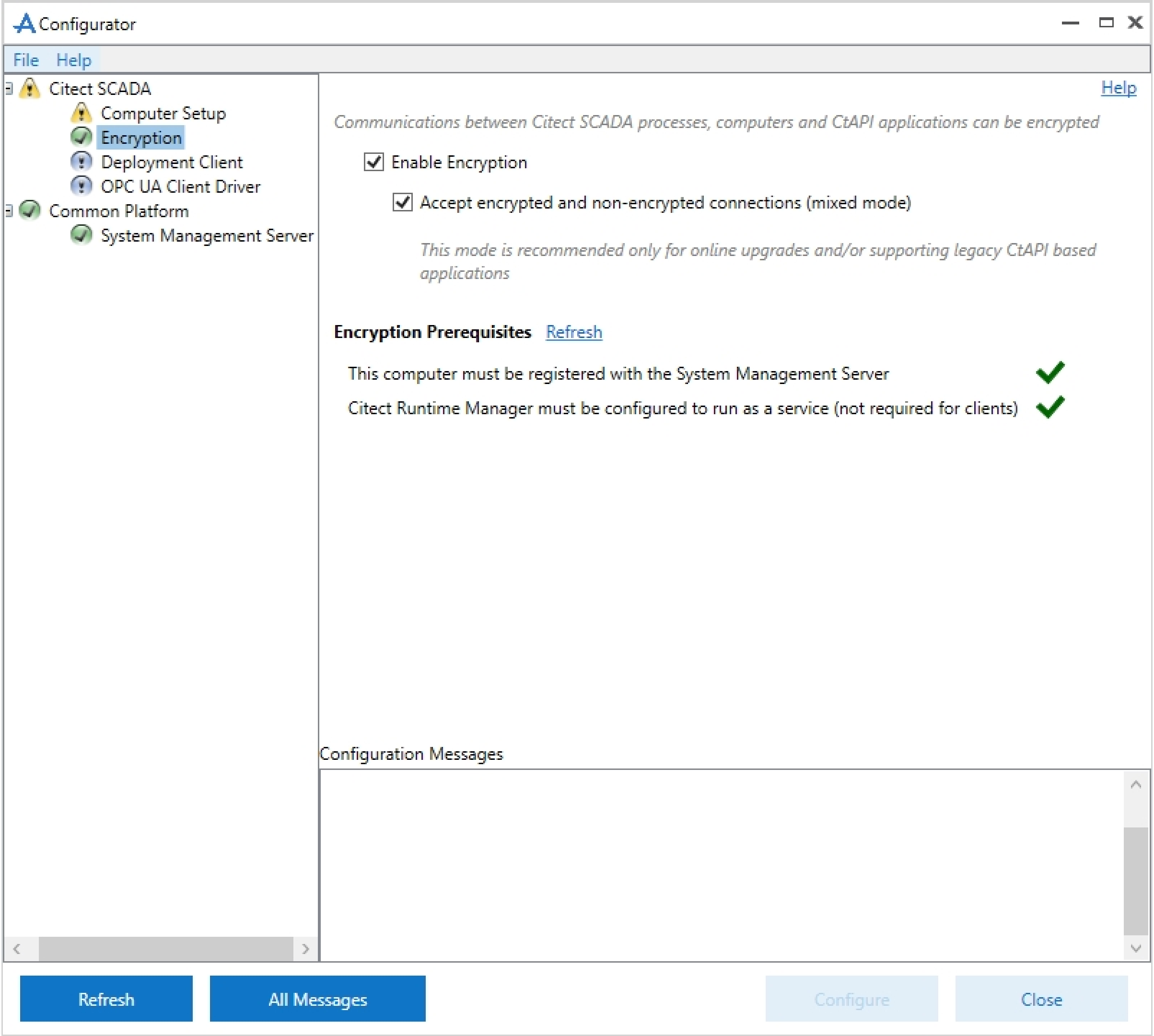
Enable Encryption

Communications between Citect SCADA processes, computers and CtAPI can be encrypted in Citect SCADA 2018 R2.

To use encrypted communications, you need to have a System Management Server configured. In addition, the Runtime Manager should be running as a service. If these prerequisites are not met, warning messages will be displayed.

To enable encryption:

1. Launch the **Configurator** after the installation, or from the Windows™ **Start** menu.
2. In the left pane, select **Encryption**.
3. Select **Enable Encryption**.
4. If you are performing an online upgrade to version 2018 R2 or running an older version of Citect SCADA, select **Accept encrypted and non-encrypted connections (mixed mode)**. Note that you can clear this option and configure your system to use encryption after the upgrade process is complete.
5. Click **Configure**. A message is displayed when encryption setup is completed.



Communications between Citect SCADA processes, computers and CtAPI applications can be encrypted

☑ Enable Encryption

☑ Accept encrypted and non-encrypted connections (mixed mode)

This mode is recommended only for online upgrades and/or supporting legacy CtAPI based applications

Encryption Prerequisites

This computer must be registered with the System Management Server ✓

Citect Runtime Manager must be configured to run as a service (not required for clients) ✓

> **Note**: If you do not select **Enable Encryption** before you click **Configure**, the following message is displayed: "Encryption is currently disabled. It is recommended that you enable encryption.".

Set Up a Runtime Computer

When you set up a computer to operate as a deployment client, you can use the **Configurator** to adjust the following runtime environment settings:

- **Server Authentication** — specifies the password the Citect SCADA server processes use to communicate with each other.

- **Project Run Path** — instructs Runtime Manager to run the project currently selected in Citect Studio, or the deployed project from the specified directory.
- **Runtime Manager Configuration** — allows you to run Runtime Manager as a service.

The **Configurator** can be launched at the completion of the installation procedure, or from the Windows™ **Start** menu.

To set up a runtime computer:

1. In the panel on the left side of the Configurator, select **Computer Setup**.
2. If the computer will be used to host a Citect SCADA server process, you will need to specify a password for server authentication. To do this, go to the **Server Authentication** section of the dialog.
3. Select the **Configure Server Password** check box.
4. Enter the required password and confirm it in the fields provided.

   The password you enter needs to match the password configured for the other server processes included in your Citect SCADA system. This password can be set on each computer using the Configurator or the Setup Wizard. Note that the Configurator should be run either as an administrator or by a member of the Citect.Engineers group.

   > **Note:** If the **Password** and **Confirm Password** fields already contain an entry, it means a server password has already been configured on the local computer. If required, you can enter a new password.

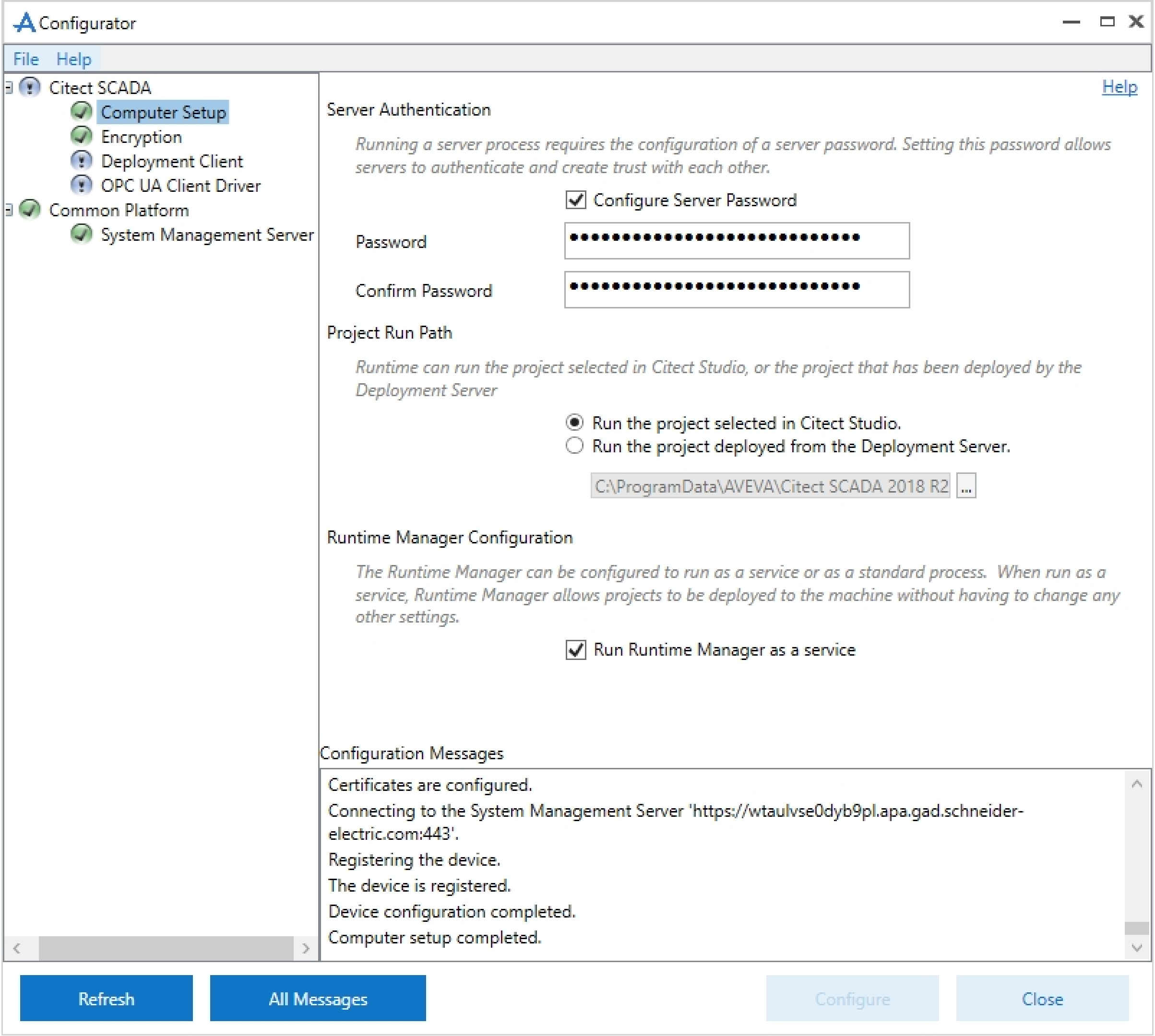
5. In the **Project Run Path** section of the dialog, select one of the following options to determine which project will be launched by Runtime Manager:
   - **Run the project currently selected in Citect Studio** - This is selected by default and will run the project from Citect Studio.
   - **Run the project deployed from the Deployment Server**- Select this option only if you need to set up Deployment.
     This option allows you to specify the directory location from which the deployed project will run. If the specified folder does not exist, it will be created during the deployment process. The default location is: C:\ProgramData\AVEVA\Citect SCADA 2018 R2\Deployment\Client\Project

     > **Note**: If Citect Runtime is running as a service and the **Project Run Path** option in the Configurator is changed to **Run the project deployed from the Deployment Server**, you need to restart the Runtime Manager service for deployment to function correctly.

6. Go to the **Runtime Manager Configuration** section of the dialog.
7. Select **Run Runtime Manager as a Service**.

> **Note**: If you are using Deployment to run a project and do not select the **Run Runtime Manager as a Service** option, you will need to manually start the Citect Runtime Manager before deploying the project.

8. To apply your settings, click the **Configure** button.



Server Authentication

Running a server process requires the configuration of a server password. Setting this password allows servers to authenticate and create trust with each other.

☑ Configure Server Password

Password ••••••••••••••••••••••••••••

Confirm Password ••••••••••••••••••••••••••••

Project Run Path

Runtime can run the project selected in Citect Studio, or the project that has been deployed by the Deployment Server

● Run the project selected in Citect Studio.
○ Run the project deployed from the Deployment Server.

C:\ProgramData\AVEVA\Citect SCADA 2018 R2

Runtime Manager Configuration

The Runtime Manager can be configured to run as a service or as a standard process. When run as a service, Runtime Manager allows projects to be deployed to the machine without having to change any other settings.

☑ Run Runtime Manager as a service

Configuration Messages

```
Certificates are configured.
Connecting to the System Management Server 'https://wtaulvse0dyb9pl.apa.gad.schneider-electric.com:443'.
Registering the device.
The device is registered.
Device configuration completed.
Computer setup completed.
```

Deployment Configuration

A deployment server allows you to send runtime files to specific computers in a Citect SCADA system. This simplifies the process of distributing project changes across multiple computers.

When installation is complete, you will be able to run the Configurator and connect to an existing System Management Server for encrypted communications. Check that you have already configured your System Management Server. If you are upgrading from v2016 or v2018, you can use deployment with or without encrypted communications.

A project's runtime files can be stored on the deployment server as a "version". From here, they can be distributed across an encrypted connection to those computers that have been set up as a deployment client. Any computer in a Citect SCADA system can be a deployment client, including system servers and/or display clients.

To set up a deployment server for your system, you initially need to install the deployment server components on the host computer. This option is available on the **Deployment Components** installation profile.

You will also need to install the Citect SCADA runtime components on each deployment client.

You can also use the Configurator to adjust some runtime environment settings for a deployment client. These settings include:

- **Server Authentication** — specifies the password the computer will use to communicate with other Citect SCADA server processes.
- **Project Run Path** — instructs Runtime Manager to run the deployed project, or the project currently selected in Citect Studio.
- **Runtime Manager Configuration** — allows you to run Runtime Manager as a service.

To configure the deployment server (on a local computer):

1. In the panel on the left side of the **Configurator**, select **Deployment Server**. The [**START**] page will display.
2. You can choose one of the following options:

- **Configure the Deployment Server** - this option is available when no deployment server has been configured.
- **Update the configuration of the current Deployment Server** - this option is available once a deployment server has been configured. If selected, you can update the database password and transfer speed for a deployment server; however you are unable to update the port number.

- **Import configuration file from previous version of the Deployment Server** - If you have an earlier version of the deployment server configured, you can import the settings. In the field provided browse for the following Configurator file:

  "SE.Asb.Deployment.Server.WindowsService.exe.config".

> **Note**: The default location is "C:\ProgramData\AVEVA\Citect SCADA 2018 R2\Config"

Once imported you will be able to continue using the deployment database and file repository created previously in the current or earlier versions of Citect SCADA.

3. Click the [**Next**] button. The **ROLES** page will display.

   This page lists the Windows user groups the deployment server creates to control access to some of its functionality. These groups include:
   - [local]\Asb.Deployment.AdminRole - users can add and remove computers and groups
   - [local]\Asb.Deployment.UploadRole - users can add and remove project versions
   - [local]\Asb.Deployment.DeployRole - users can deploy projects to runtime computers
   - [local]\Asb.Deployment.ReadRole - users can browse project versions and computers.

   When the configuration process is complete, the current user account will be added to these groups. If required, you can manually add additional users to these groups in the Windows configuration environment.
4. Click the **Next** button. The **SETTINGS** page will display.

   This page allows you to set the password used by the deployment database. It also allows you to set the transfer rate to limit the network bandwidth used when deploying a project.
5. Enter the **Password** for the database. Confirm the password.

> **Note**: To change an existing database password you need to reconfigure the deployment server.

6. In the **Transfer Speed (KB/s)** field, enter a value between 0 and 2147483647 (0 being unrestricted). The default is 10000 (KB/s). By limiting the transfer speed, you allow other processes to use the remaining network bandwidth. This value may affect the overall duration of a deployment operation. For example, if your project is 20MB with a limit set to 1000 KB/s, the project will take approximately 20 seconds to transfer.

> **Note:** Settings may vary according to your network infrastructure.

7. Click the **Next** button. The **FINISH** page will display.

   If required, you can use the **Previous** button to make any changes to your settings before you complete the configuration process.
8. Click the **Configure** button. The Configuration Messages panel will indicate if the deployment server configuration was successful.

To configure a deployment client (on a local computer):

1. In the panel on the left side of the Configurator, select **Deployment Client**.The [**START**] page will display.
2. You can choose one of the following options:
   - **Configure the Deployment Client** - this option is available when no deployment client has been configured.
   - **Update the configuration of the current Deployment Client** - this option is available if a deployment client has been configured. The Deployment Client configuration needs to be updated whenever there is change in the System Management Server configuration.
   - **Import configuration file from previous version of the Deployment Client** - if you have an earlier version of the deployment client configured (from Citect SCADA 2016 or 2018), you can import the client settings. In the field provided, browse for the following Configurator file:

   "SE.Asb.Deployment.Node.WindowsService.exe.config".

   The default location is “C:\ProgramData\AVEVA\Citect SCADA<version>\Config”

   Click the **Next** button. The **CONNECT** page will display.
3. In the **Server** field, select the deployment server to which you would like to connect. If the name does not appear in the list, type the Windows computer name of the machine on which the System Management Server is installed.

   To change the deployment server to which a deployment client is connected, repeat the steps needed to configure a deployment client.

   If the deployment client is also configured as a deployment server, the deployment client should only connect to the local deployment server.
4. Click the **Next** button. The **AUTHORIZE** page will display.

   Enter the **User Name** and **Password** for the Windows user account that will be used to register the client computer with the deployment server. The user account you enter needs to be part of the "Deployment Admin Role" Windows user group that is configured locally on the deployment server.
5. Click the **Next** button. The **SETTINGS** page will display.

On the **SETTINGS** page you can set the Unpack Rate. In the **Unpack rate (KB/s)** field, enter a value between 0 and 2147483647 (0 being unrestricted). If you limit the unpack rate, your system will still be able to run other processes. This value may affect the overall duration of a deployment operation.

6. Click the **Next** button. The **FINISH** page will display.

   This page informs you that the **Configurator** is ready to send a request to the deployment server for registration.

   If required, you can use the **Previous** button to make any changes to your settings before you initiate the registration process.
7. Click the **Configure** button.

   If registration is successful, the configured client information will be stored on the computer and a connection will be established. If registration is not successful, you will be notified via the Configuration Messages panel.

To set up a runtime computer:

1. In the panel on the left side of the Configurator, select **Computer Setup**.
2. If the computer will be used to host a Citect SCADA server process, you will need to specify a password for server authentication. To do this, go to the **Server Authentication** section of the dialog.
3. Select the **Configure Server Password** check box.
4. Enter the required password and confirm it in the fields provided.

   The password you enter needs to match the password configured for the other server processes included in your Citect SCADA system. This password can be set on each computer using the Configurator or the Setup Wizard. Note that the Configurator should be run either as an administrator or by a member of the Citect.Engineers group.

   > **Note:** If the **Password** and **Confirm Password** fields already contain an entry, it means a server password has already been configured on the local computer. If required, you can enter a new password.

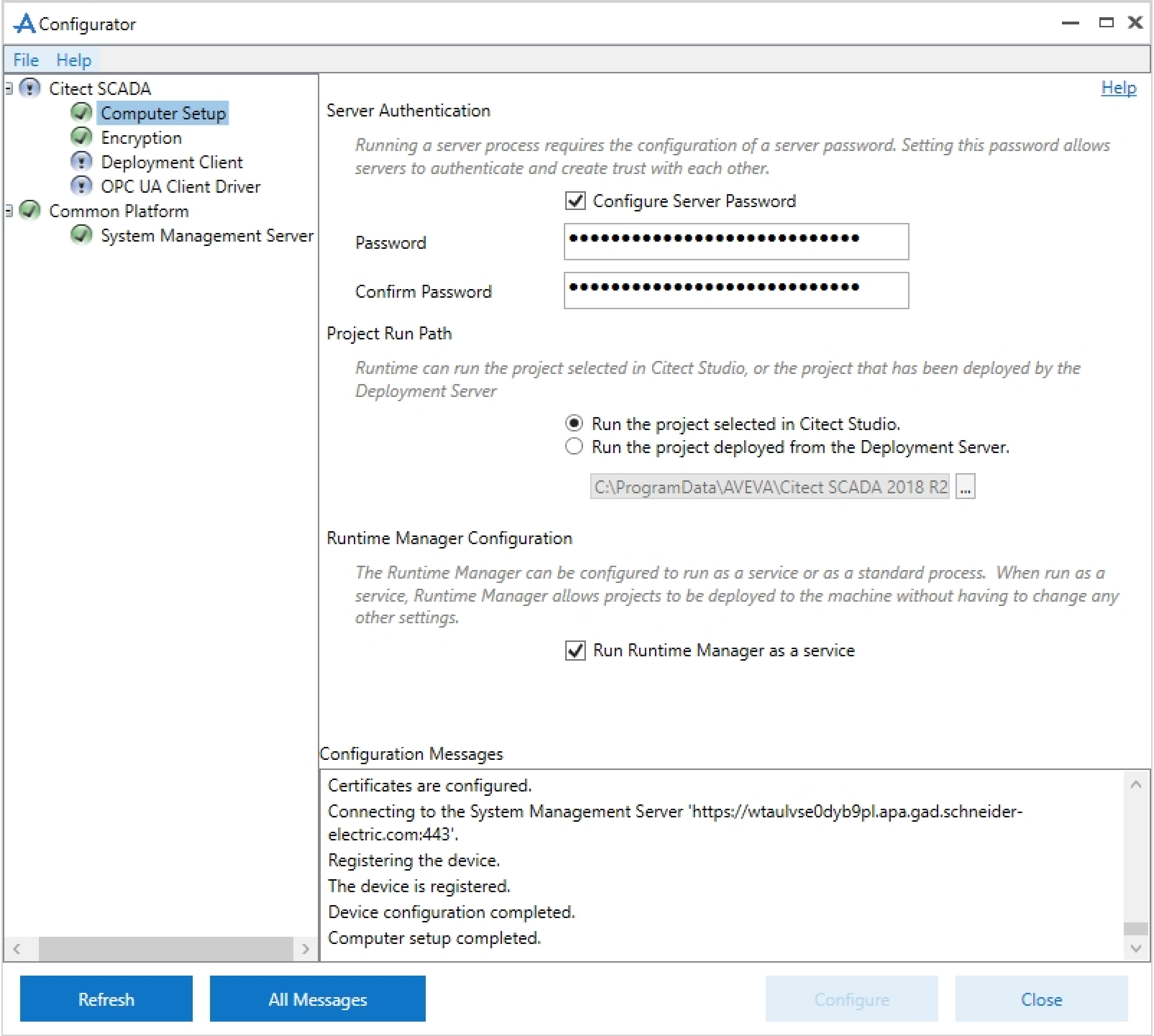
5. In the **Project Run Path** section of the dialog, select one of the following options to determine which project will be launched by Runtime Manager:
   - **Run the project currently selected in Citect Studio** - This is selected by default and will run the project from Citect Studio.
   - **Run the project deployed from the Deployment Server**- Select this option only if you need to set up Deployment.
     This option allows you to specify the directory location from which the deployed project will run. If the specified folder does not exist, it will be created during the deployment process. The default location is: C:\ProgramData\AVEVA\Citect SCADA 2018 R2\Deployment\Client\Project

> **Note**: If Citect Runtime is running as a service and the **Project Run Path** option in the Configurator is changed to **Run the project deployed from the Deployment Server**, you need to restart the Runtime Manager service for deployment to function correctly.

6. Go to the **Runtime Manager Configuration** section of the dialog.
7. Select **Run Runtime Manager as a Service**.

> **Note**: If you are using Deployment to run a project and do not select the **Run Runtime Manager as a Service** option, you will need to manually start the Citect Runtime Manager before deploying the project.

8. To apply your settings, click the **Configure** button.



Server Authentication

Running a server process requires the configuration of a server password. Setting this password allows servers to authenticate and create trust with each other.

☑ Configure Server Password

Password ••••••••••••••••••••••••••••

Confirm Password ••••••••••••••••••••••••••••

Project Run Path

Runtime can run the project selected in Citect Studio, or the project that has been deployed by the Deployment Server

● Run the project selected in Citect Studio.
○ Run the project deployed from the Deployment Server.

C:\ProgramData\AVEVA\Citect SCADA 2018 R2

Runtime Manager Configuration

The Runtime Manager can be configured to run as a service or as a standard process. When run as a service, Runtime Manager allows projects to be deployed to the machine without having to change any other settings.

☑ Run Runtime Manager as a service

Configuration Messages

```
Certificates are configured.
Connecting to the System Management Server 'https://wtaulvse0dyb9pl.apa.gad.schneider-
electric.com:443'.
Registering the device.
The device is registered.
Device configuration completed.
Computer setup completed.
```

Network Communications Overview

Networking and Microsoft® Windows®

Microsoft Windows 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 Citect SCADA 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:Citect SCADA networking and redundancy needs the option "Citect SCADA Runtime" to communicate through a Windows firewall. You will need to manually add an application to the Windows firewall exception list for a particular network profile.

Web Server/Client Configuration

To display a live Citect SCADA project in an Internet browser, you need to publish 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 Microsoft® Windows® operating system, enable the World Wide Web Services (HTTP) option in the Windows inbound firewall.

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

- Citect SCADA 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 Citect SCADA project and the location of the runtime servers. This information is stored on the Web Server when a Citect SCADA project is configured using the Citect Studio, Projects activity, **Prepare Web Deployment** option. A Citect SCADA Web Server can contain multiple web deployments.
- Citect SCADA 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 web-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 Citect SCADA 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 web deployment. Any subdirectories include the components associated with a particular release (in this case, v2018 R2).
- The **deploy** folder includes the files associated with any web deployments (Citect SCADA projects) configured on the Web Server.

- The #**displayclientfolder** (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 necessary to support different languages for the client interface. See “Implementing Multiple Language Support” in the Web Client topic of the Citect SCADA 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 a key role in managing which users have access to the site.

You can view evidence of this virtual directory in Windows' Internet Information Services (IIS) Manager. The Citect SCADA 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 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 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 Citect SCADA 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 Citect SCADA 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

Installed directory	ADMINISTRATOR	CONTROL	VIEW-ONLY
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 Citect SCADA 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 need to be 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 Citect SCADA configuration engineer and a runtime operator

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. The Citect folder is located in the installation directory. 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.

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 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 Citect 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 Citect SCADA 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, deny the user access to the Citect folder before you delete the user. This avoids a 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 Citect SCADA 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 need to 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 Citect SCADA 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 Citect SCADA projects for Web deployment.