

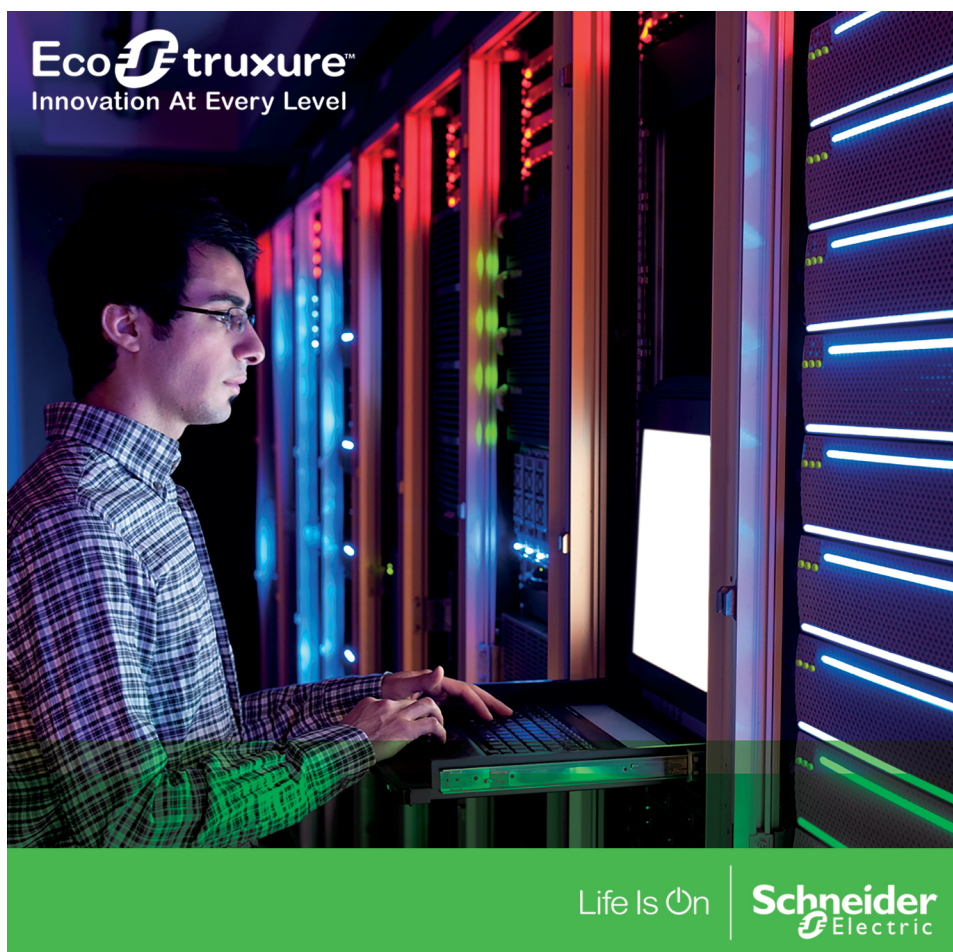
EcoStruxure™

Power Operation 2021 with Advanced Reporting and Dashboards

IT Guide

7EN02-0465-00

07/2021



Schneider
Electric

Legal Information

The Schneider Electric brand and any registered trademarks of Schneider Electric Industries SAS referred to in this guide are the sole property of Schneider Electric SA and its subsidiaries. They may not be used for any purpose without the owner's permission, given in writing. This guide and its content are protected, within the meaning of the French intellectual property code (Code de la propriété intellectuelle français, referred to hereafter as "the Code"), under the laws of copyright covering texts, drawings and models, as well as by trademark law. You agree not to reproduce, other than for your own personal, noncommercial use as defined in the Code, all or part of this guide on any medium whatsoever without Schneider Electric's permission, given in writing. You also agree not to establish any hypertext links to this guide or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the guide or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

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

As standards, specifications and designs change from time to time, please ask for confirmation of the information given in this publication.

Safety Information

Important Information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service or maintain it. The following special messages may appear throughout this bulletin or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



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 potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

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

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

Contents

Contents	4
Safety Precautions	6
Support and version information	7
Version Information	8
Computer requirements	9
Server CPU and RAM requirements	9
Client CPU, RAM, and disc requirements	11
Server disk storage	11
Network requirements	12
Supported operating systems	12
Supported SQL Server versions	13
Virtualization	13
Installing	16
Before installing	16
Pre-installation checks	16
Supported environments	17
Preparing servers	17
Component selection	17
Core components selection	18
Add-ons selection	18
System software order of installation	19
Installing the software	21
Installing the ETL Administration Tool	22
Install Power SCADA Anywhere Server	23
Installing CAE	24
After installing the software	25
Maintaining system currency	25
Getting started with Power Operation	25
Uninstall and reinstall Power Operation	25
Cybersecurity	27
IEC 62443	28
Product defense-in-depth	28
Cybersecurity capabilities	28
Protected environment assumptions	30
Potential risks and compensating controls	31
Hardening	32
Configuring cybersecurity	32
Default security settings	34
Viewing security settings	34
Default port numbers	35

Windows Active Directory	37
Whitelisting	38
Configuring third-party certificates	39
Encryption, locking USB ports, and hardening servers	42
Configuring two-factor authentication	45
Configuring projects for network segmentation	53
Threat Intelligence	53
Using the Security Viewer Filter	55
Using Cybersecurity Admin Expert (CAE) for cybersecurity	56
Default CAE security settings	58
Configuring CAE cybersecurity	60
Working with CAE projects	65
Threat intelligence and CAE	67
Windows Updates	68
User accounts and passwords	69
User account roles and privileges	69
Managing user accounts, role names, and mapping	72
Managing user account lockouts and timeouts	75
Passwords	75
Using single sign-on and passwords	75
Two-factor authentication	75
Using CAE for user accounts and passwords	76
Managing CAE user accounts	76
Managing user account lockouts and timeouts	77
Managing CAE passwords	77
Managing CAE user account lockouts and timeouts	79
Managing CAE models	80
Managing CAE user roles	82

Safety Precautions

During installation or use of this software, pay attention to all safety messages that occur in the software and that are included in the documentation. The following safety messages apply to this software in its entirety.

WARNING

UNINTENDED EQUIPMENT OPERATION

- Do not use the software or devices for critical control or protection applications where human or equipment safety relies on the operation of the control action.
- Do not use the software to control time-critical functions.
- Do not use the software to control remote equipment without proper access control and status feedback.

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

WARNING

INACCURATE DATA RESULTS

- Do not incorrectly configure the software or the devices.
- Do not base your maintenance or service actions solely on messages and information displayed by the software.
- Do not rely solely on software messages and reports to determine if the system is functioning correctly or meeting all applicable standards and requirements.
- Consider the implications of unanticipated transmission delays or failures of communications links.

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

WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices to help prevent unauthorized access to the software.

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

Work with facility IT System Administrators to ensure that the system adheres to the site-specific cybersecurity policies.

Support and version information

Documentation

Go to www.se.com, search for Power Operation, and select the **Catalogs & User Guides** checkbox. In the search results, you will find the most current versions of:

- *EcoStruxure Power Operation Release Notes* – PDF
- *EcoStruxure Power Operation System Guide* – PDF
- *EcoStruxure Power Operation IT Guide* – PDF
- *EcoStruxure Power Operation eBrochure* – PDF (What's New)
- *Power Monitoring Expert – IT Guide* – PDF (Advanced Reporting Module)

Documentation for previous versions can be found on se.com by searching for the version of Power Operation you have and refining the search results.

Version information

See [Version information](#) for steps on identifying the version of Power Operation installed.

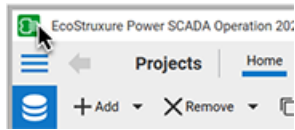
Other support

- Schneider Electric Exchange:
 - [Design & Quote](#) tools, including:
 - PO Software Assurance Calculator.
 - PO Disk Sizing Calculator.
 - PO Commissioning Time Tool.
 - Power SCADA Anywhere documents.
- Documentation for Legacy Graphics Builder can be found in previous versions of Power Operation Help online.
- Go to the [AVEVA Knowledge & Support Center website](#) for information on PLANT SCADA or to generate upgrade authorization codes using the online license generator.
- Go to [Schneider Electric Cybersecurity Support Portal](#) for the latest cybersecurity news. Includes security notifications, and where you can report a vulnerability, or a security or data privacy event.
- [Schneider Electric FAQs](#).
- [Schneider Privacy Policy](#).
- If your license is out of support, contact your Schneider Electric account manager or email orders.software@se.com with your license and site ID details.

Version Information

To identify the version of Power Operation installed:

1. Open **Power Operation > Power Operation Studio**.
2. Click the program icon on the top left:



3. Select **About EcoStruxure Power Operation > Technical Info** tab.

Power Operation version	Plant SCADA file version
PO 2021 R1	8.3
PSO 2020 R2	8.21
PSO 2020	8.2
PSO 9.0	8.10.0.2086
PSE 8.2	8.0.0.2065
PSE 8.1	7.50.0.4150
PSE 8.0 SR1	7.50.0.4107
PSE 8.0	7.40.1.239
PSE 7.40 SR1	7.40.1.239
PSE 7.40	7.40.1.239
PSE 7.30 SR1	7.30.0.601, 7.30.1.94
PSE 7.20 SR1	7.20.4.38
PSE 7.20	7.20.1.33

Computer requirements

This section provides information on the hardware and software requirements for a Power Operation with Advanced Reporting and Dashboards system.

Server CPU and RAM requirements

Power Management software needs to be installed on dedicated machines, so that other non-Power Management software applications do not consume machine resources.

When selecting server hardware, carefully review the 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 a web browser. This will return the CPU's calculated performance as compared to other similar well-known processors.

CPU and RAM recommendations for various system architectures

- The requirements listed in this topic are minimum requirements; we recommend that you consider doubling the RAM requirements listed.
- Power SCADA Anywhere server must have a CPU with SSE2 instruction set support.

Power Operation server (medium and large systems)

The following table lists the number of CPU cores and RAM required for a Power Operation system.

NOTE: Use the tag or device number that is higher of the two numbers. For example, if you have a system using 120,000 tags with 300 devices, use six CPU cores and 16 GB of RAM.

NOTE: These are minimum requirements. We recommend that you consider doubling the RAM requirements listed.

Use the larger figure below	CPU PassMark Score	# CPU Cores	RAM (GB)
1,500 tags or 50 devices	2,000	2	8
15,000 tags or 100 devices	4,500	4	16
50,000 tags or 200 devices	8,000	6	16
100,000 tags or 400 devices	8,000	6	16
150,000 tags or 600 devices	8,000	8	32

Use the larger figure below	CPU PassMark Score	# CPU Cores	RAM (GB)
200,000 tags or 800 devices	10,000	8	48
250,000 tags or 1,000 devices	10,000	12	48
300,000 tags or 1,200 devices	10,000	16	64
350,000 tags or 1,400 devices	10,000	12	16
400,000 tags or 1,600 devices	10,000	24	96
450,000 tags or 1,800 devices	10,000	24	96
500,000 tags or 2,000 devices	10,000	30	96

Power Operation and Power Monitoring Expert on the Same Machine

The following table lists the number of CPU cores and RAM required for a Power Operation and Power Monitoring Expert system on the same machine.

NOTE: Use the tag or device number that is higher of the 2 numbers. For example, if you have a system using 120,000 tags with 300 devices, use 10 CPU cores and 28 GB of RAM.

NOTE: These requirements are based on product testing at the factory. They are intended as recommendations on system sizing. However, some customers may find that based on their system's design or usage they require more or less resources than what is recommended by this guide.

Use the larger figure below	CPU PassMark Score	# CPU Cores	RAM (GB)
50,000 tags or 200 devices	8,000	14	40
100,000 tags or 400 devices	8,000	16	48
150,000 tags or 600 devices	8,000	18	64

For systems greater than 150,000 tags or 600 devices, we recommend a distributed architecture with separate physical machines for Power Operation and Power Monitoring Expert.

Power Operation and Power Monitoring Expert on separate machines

Refer to the *Power Monitoring Expert 2021 – System Guide* for specific CPU and RAM requirements when installing Power Operation and Power Monitoring Expert on separate machines.

Client CPU, RAM, and disc requirements

Power Operation Clients used as Windows desktop thick clients have the following minimum requirements:

- CPU PassMark: 2000
- CPU: 2 Cores
- RAM: 4 GB
- Disk storage: 10 GB
- Screen resolution: 1920 x 1080

Monitoring CPU for running systems

Optimal performance is achieved when all computers in your Power Operation network use approximately 40% or lower CPU in normal state. If you have any concerns about system responsiveness or its ability to handle abnormal situations, consider adding resources to lower overall CPU utilization.

Power Operation Graphics Adapter

Minimum requirements:

- DirectX 9 or later with WDDM 1.0 Driver
- 128 MB of dedicated VRAM (for systems of any size)

Server disk storage

The main consumers of historical data in PO are:

1. Advanced Reporting and Dashboards Module (PME) historical data for display in reports and dashboards.
2. PO historical data stored for PO alarm viewer, trend viewer, and built-in basic reports.

Advanced Reporting and Dashboards data is stored in Microsoft SQL databases. PO data is stored in file system flat files (no SQL required).

Required disk space without Advanced Reporting

When planning a Power Operation system without Advanced Reporting (Power Monitoring Expert), you can fine tune your disk storage requirements based on how Power Operation stores data.

Power Operation has two major consumers of disk storage space:

1. Alarm information which is stored in a propriety database that may grow over time to a size of 1-2 GB.
2. Historical data stored in trend files (flat files on the disk) used by PO built-in reports and trend viewer. The size and number of these trend files depend on number of tags in system, logging interval, and number of years to store data.

Trend files are pre-allocated (reserved) on the hard disk the first time that Power Operation is started. Hard disk space does not "grow" over time by acquiring trend data. In other words, if the hard drive is not big enough for the number of years of trending that you plan for, the system will tell you.

Calculating disk storage

To calculate disk storage size for your system, use the Power Operation Disk Sizing Calculator. Go to the [Schneider Electric Exchange](#) for more information.

NOTE: These values include a 2 GB alarm database size and assume that you configure trends to be stored in separate files each week.

Network requirements

Use Ethernet whenever possible. For best system performance with devices, we recommend minimum 1 Gigabit Ethernet communication.

If you are using serial communication, use a minimum baud rate of 19.2K.

Supported operating systems

The following table lists the compatible operating systems for Power Operation, ENM, and Advanced Reporting. Columns for version 2021, 2020, 9.0, and 8.2 represent super-set of all PO components including Servers, Clients, and Advanced Reporting and Dashboards (PME).

NOTE: 64-bit operating systems are recommended for best performance.

Operating System	Power Operation Version				
	2021	2020	9.0	8.2	8.1
Windows Server 2019	✓	✓	–	–	–
Windows Server 2016	✓	✓	✓	✓	–
Windows 10	✓ ³	✓ ²	✓	✓	✓ ¹

Operating System	Power Operation Version				
	2021	2020	9.0	8.2	8.1
Windows Server 2012 R2	✓	✓	✓	✓	✓
Windows 8.1	–	–	–	✓	✓
Windows Server 2012	–	–	✓	✓	✓
Windows Server 2008 R2	–	–	–	✓	✓
Windows 7	–	–	✓	✓	✓

¹: Available with 8.1 update 6 or later

²: Requires Windows 10 version LTSC 1607 and later (64-bit only)

³: Requires Windows 10 version LTSC 1607 and later (64-bit only) or Windows 10 1803 and later (64-bit only)

Supported SQL Server versions

Power Operation with Advanced Reporting and Dashboards requires a Microsoft SQL Server database. Power Operation with Advanced Reporting and Dashboards supports the following SQL Server versions:

- SQL Server 2019 Express/Standard/Enterprise/Business Intelligence
- SQL Server 2017 Express/Standard/Enterprise/Business Intelligence
- SQL Server 2016 Express/Standard/Enterprise/Business Intelligence
- SQL Server 2014 Express/Standard/Enterprise/Business Intelligence
- SQL Server 2012 Express/Standard/Enterprise/Business Intelligence, SP2

NOTE: Power Operation 2021 **without** Advanced Reporting and Dashboards does NOT require a SQL Server database.

Power Operation with Advanced Reporting and Dashboards installation media includes SQL Server 2019 Express that can be used with Advanced Reporting.

Virtualization

The following table lists the virtualization support for installation and operation of Power Operation with Advanced Reporting and Dashboards:

	Microsoft Hyper-V	VMWare vSphere
Power Operation Server (including web server host)	Yes	Yes
Power Operation Client Access (this refers to Windows Desktop clients)	Yes	Yes
Mobile Notifications (Event Notification Module)	Yes	Yes
Advanced Reporting and Dashboards (Power Monitoring Expert)	Yes	Yes

NOTE: Power Monitoring Expert is validated with additional virtualization systems, see the *Power Monitoring Expert 2021 – System Guide* for additional details.

Virtualization planning notes:

- Set all resource allocation (CPU, memory, and disk) to fixed; dynamic is not supported.
 - Do not share resources between virtual machines via over-allocation. The total of all individual VM resources should not exceed that which is available from the host.

NOTICE

UNINTENDED DATA LOSS OR LOSS OF SOFTWARE FUNCTION

Do not exceed device limits.

Failure to follow these instructions can result in irreversible damage to software and databases.

- If you are using shared drive storage, use Fiber SAN storage. If you are not using Fiber SAN storage, use a direct attached, dedicated hard drive used by Power Operation only.
- You must have a fixed-size disk virtual machine.
- Set host (for example: ESX host) power management to “High Performance”.
- Adjust Quality of Service (QoS) to allow precedence to Power Operation over less time-critical applications.
- Create your Power Operation virtual machine on a host without other time-critical applications.

Additional virtual machine configuration guidelines vary by hypervisor.

When running virtual machines, licenses remain trusted during the following scenarios:

- Changes to the NIC card MAC address of the physical host or virtual machine.
- Changes to the physical host or virtual machine RAM
- Changes to physical host hard disk or virtual machine disk
- Changes to the OS clock (within +/- 2 hours)
- The physical host or virtual machine is rebooted.
- The virtual machine is paused or resumed.

- The virtual machine is restored from a snapshot.
- The virtual machine is live migrated/moved (eg. VMotion) for common migration scenarios.

Virtual machine live migration/move scenarios that may cause licenses to go untrusted include:

- VMWare moving from one vCenter to another (cross-vCenter migration).
- Microsoft Hyper-V moving from one System Center Virtual Machine Manager to another.

Installing

You can install Power Operation with Advanced Reporting and Dashboards as a new product only.

Power Operation does not support different versions running side-by-side. If you are upgrading from an earlier version of Power Operation, back up your existing project files. These files include LiveView templates; reporting configurations (such as email addresses); and Profile Editor custom tags, device types, profiles, and units (in the Program Data folder).

Uninstall prior versions before installing v2021.

Remove existing Power Operation License Configuration Tool installations before installing the new version.

Before proceeding with the installation of Power Operation with Advanced Reporting and Dashboards and optional components, refer to ["Before installing" on page 16](#) for detailed installation prerequisite information.

Before installing

This section describes the requirements for hardware, operating system software, and system configuration prior to installing Power Operation with Advanced Reporting and Dashboards and any of its components.

These requirements vary based on the components of Power Operation with Advanced Reporting and Dashboards that you install on any computer. This section identifies the basic system software requirements, as well as requirements specific to each component. Refer to ["Core components selection" on page 18](#) to determine the components that you want to install.

WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Apply all Windows security updates on machines running Power Operation and Power Monitoring Expert.

Failure to follow these instructions can result in death, serious injury, equipment damage, and permanent loss of data.

Before you begin to install Power Operation with Advanced Reporting and Dashboards, install the latest updates from Microsoft for your operating system and system software. See ["Preparing servers" on page 17](#) for more information. Also see the Operating System Matrix that shows the operating systems that are compatible with various versions of Power Operation.

Pre-installation checks

Depending on your operating system version, your SQL Server edition, and the setup type (server or client) that you select for installation, the installer performs some or all of the following tasks prior to the installation of the software:

- Check for .NET Framework 4.7 and automatically installs it if required.
- Uninstall previous versions. If a previous version of the software is installed, installation will

stop.

- Verify that the SQL Server Agent is installed. If not found, the installer will install SQL Server Express. (Advanced Reporting and Dashboards only.)
- Validate that a supported SQL Server edition and service pack level are installed (Advanced Reporting and Dashboards only).
- Check the database location. The database must be local for some installation types and remote for others. (Advanced Reporting and Dashboards only.)
- Check for 32-bit SQL Server edition (Advanced Reporting and Dashboards only).
- Check for the presence of ASP.NET.
- Verify that the appropriate account permissions are defined, for example, that the SQL Server system administrator (sa) account is set with Administrator as the user (Advanced Reporting and Dashboards only).
- Verify that the Windows account that the SQL Server service runs under has the proper folder permissions to proceed (Advanced Reporting and Dashboards only).

Supported environments

Review the "[Computer requirements](#)" on [page 9](#) section to ensure that your hardware and system software meet the requirements for your selected installation.

Preparing servers

The software Installer performs several of the setup and configuration tasks during installation to ensure that the prerequisites for your Power Operation with Advanced Reporting and Dashboards system are met. Complete the following before proceeding with the installation.

Updating the operating system

WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Apply the latest updates and hotfixes to your Operating System and software.

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

Run the Windows Update service to install the latest security patches and hotfixes from Microsoft.

Component selection

Decide which Power Operation with Advanced Reporting and Dashboards components and add-ons you want to install.

Core components selection

The installer provides a list of options to help you select the appropriate components during installation. The options are described here.

Runtime Environment

Selects Runtime, Sentinel Driver, and Communications Drivers for installation. It is an installation that installs the runtime components for both a Server and Client. This installation includes runtime infrastructure files, Client and I/O Server, Alarm Server, Trend Server, and Reports Server.

Select this option if this is an installation of Power Operation that will act as a server to service many client installations.

Configuration and Development Environment

Installs the design-time configuration environment. Users who have sufficient security privileges can set up graphics pages, create reports, and the like. The configuration tools include: Power Operation Studio, Application Configuration Utility, IO Device Manager, Project Setup, Project Backup/Restore, and the Power Operation Runtime.

Deployment Client

Installs the Deployment Client component, which allows projects to be deployed to this machine remotely.

Deployment Server

Installs the Deployment Server component, which allows projects to be administered, versioned, and deployed to other remote Deployment Client machines from this machine. The server can roll out project changes to the various computers in your project.

Add-ons selection

After you select the core components that you want to install, select any add-ons that you want to include in your installed system. The options are described here:

Project DBF Add-in for Excel

Installs an Add-In for Microsoft Excel. When this Add-In is loaded into Excel, it allows you to browse, open, edit and save Power Operation .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.

Power Operation Web Server for IIS

Installs 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 Power Operation project, and the location of the runtime servers. This information is stored on the Web Server when a Power Operation project is deployed. A Web Server can contain multiple deployments.

NOTE: If the Web Server and Power Operation 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 Power Operation Server that is hosting the web deployment files.

If a trust relationship is established between the Web Server and the Power Operation server, they can be on different domains if the Web Server has read access to the project folder on the Power Operation Server.

Power Operation Reporting

Installs the Power Operation basic reports.

The Power Operation Profile Editor

Installs the Profile Editor. Profile Editor lets you create tags, device types, devices, and projects outside of the Power Operation Studio environment.

The Power Operation LiveView

Installs LiveView. LiveView lets you create table templates for real-time system readings.

System software order of installation

This section provides an overview of the general steps required to install:

- Power Operation
- Advanced Reporting and Dashboards Module files: Advanced Reporting and Dashboards
- Extract, Transform, and Load (ETL): Use this module to extract historical data from Power Operation and transform it into a format that can be used in the Advanced Reporting and Dashboards Module.
- Power SCADA Anywhere

Before you begin, you need the following items:

- Installation medium for Power Operation with Advanced Reporting and Dashboards and Power Operation 2021 Installation Guide.
- Installation medium for ETL and Power SCADA Anywhere (included on the Power Operation with Advanced Reporting and Dashboards ISO).
- Installation medium for .NET Framework 4.7.2, downloaded from Microsoft.
- Installation for Microsoft SQL Server.

NOTE: SQL Express is included on the Power Operation with Advanced Reporting and Dashboards ISO. Microsoft SQL Server must be obtained from Microsoft.

On the Power Operation Server Computers

The following table lists software that you will install on each of the servers and clients in your project.

Power Operation Primary Server	Power Operation Secondary Server	Power SCADA Anywhere	Advanced Reporting and Dashboards Server
Power Operation 2021	Power Operation 2021	Power Operation 2021 client access only	SQL Server
		Power SCADA Anywhere	Advanced Reporting and Dashboards (from the Power Operation ISO)
		Windows Terminal Services must be enabled.	ETL

Power Operation Server Computers

Install all operating system updates before you install Power Operation.

On the server that you will use for Power Operation, install software in the following order:

- Verify that you have the correct Internet Explorer version for your operating system.
- Install .NET 4.7.2
- If you want to have Matrikon Explorer on the computer, install Matrikon before you install Power Operation.
- Install Power Operation.

On the Advanced Reporting and Dashboards Computer

On the server that you will use for the Advanced Reporting and Dashboards Module, install the software in the following order:

- Microsoft SQL Server: You must install SQL Server on the Advanced Reporting and Dashboards server. Refer to the *Power Monitoring Expert 2021 – System Guide* for information.
- Advanced Reporting and Dashboards Module: Use the Power Operation with Advanced Reporting and Dashboards installation medium and installation guide.
- On the Advanced Reporting and Dashboards Module server only, install ETL. See "[Installing the ETL Administration Tool](#)" on page 22 for details.

NOTE: The installation medium is located on the same DVD or .ISO as the Power Operation installation, in the Advanced Reporting and Dashboards Module folder.

On the Power SCADA Anywhere Server Computers








You need to install Power SCADA Anywhere on a remote client computer.

Installing the software

When you begin the installation, if any required system software is not detected, you must install it before you can begin the Power Operation with Advanced Reporting and Dashboards installation. For example, if you have not yet installed .NET Framework 4.7.2, you will be prompted to install it first.

Required for this procedure:

- Do not have Windows Update running when you install.
 - Microsoft .NET Framework 4.7.2 installed.
1. Go to www.se.com and download the software ISO file. To find the most recent software ISO file, search for Power Operation and refine your search results by selecting the Software/Firmware check box.
 2. Extract the ISO files.
 3. Open `MainSetup.exe`: The Power Operation installer opens.

Name	Date modified	Type	Size
 Documentation	4/23/2021 5:40 PM	File folder	
 OFS v3.62	4/23/2021 5:40 PM	File folder	
 OPC UA Client	4/23/2021 5:40 PM	File folder	
 Prerequisites	4/23/2021 5:40 PM	File folder	
 setup	4/23/2021 5:40 PM	File folder	
 autorun	4/23/2021 5:40 PM	Setup Information	
 MainSetup	4/23/2021 5:32 PM	Application	1,4

4. Select the Core Components you want > click **Next**. See "[Core components selection](#)" on [page 18](#) for a description of each component.
5. Select the Add-ons you want > click **Next**. See "[Add-ons selection](#)" on [page 18](#) for a description of each add-on component.

NOTE: Project DBF Add-in for Excel can only be selected if Microsoft Excel 2003, 2006, 2010, or 2013 is installed on the computer.

6. Select Destination Folders for the files > click **Next**.
7. Enter a password for the Database Engine > click **Next**.
8. Enter a password for the Power Operation Database > click **Next**. The Check System screen opens.

If the installation is unsuccessful:

- a. Click **Open Log** to review where the installation stopped.
- b. Note the files that need to be corrected, and correct them in the order they are presented.
- c. After you make the corrections, click **try again** to re-install PO.
- d. Repeat this step, as necessary, until all problems are solved.

9. When **System Verified** is displayed on the Check System screen, click **Next**. The Ready to Configure screen opens.
10. Review the component list > click **Install**.
11. Click **Close** when the installation is complete.

Depending on your system architecture, complete the installation of the Power Operation with Advanced Reporting and Dashboards system components.

Refer to [Plant SCADA help](#) for information about configuring a system management server, deployment server, and TLS certificate management.

Installing the ETL Administration Tool

The ETL tool extracts historical data from and transforms it into a format that loads it into Power Monitoring Expert. Install ETL on the machine hosting Advanced Reporting and Dashboards.

Go to the [Schneider Electric Exchange](#) and download the ETL Administration tool.

Install ETL on the machine hosting Advanced Reporting and Dashboards. Install the ETL Administration Tool on the Power Monitoring Expert server using a Windows Administrator account.

To install ETL for PO:

1. In Windows Explorer, navigate to \Power Operation with Advanced Reports ETL.
2. Copy the PO to PME ETL EXE to the PME server.
3. Double-click `SegApps_ETL_PowerSCADA-xxx.exe`.
(Where xxx is the build number.)
4. **Application Language:** Select your preferred application language from the drop-down list and click **Next**.

NOTE: The ETL Administration Tool supports English only.

5. **Welcome:** Review the steps and click **Next**.
6. **License Agreement:** Read the End User License Agreement and if you accept the terms of the agreement, click **I Agree** to proceed.
7. **Setup Type:** ETL: Power Operation 2021 can only be installed with the **Standalone Server** option. Click **Next**.
8. **File Destination:** Click **Next** to install the ETL tool to the default location. To select a different location, click the ellipsis button and then select a new location. Click **OK**.
9. **Check System:** The installer checks the operating system. If a condition affecting installation is detected, the installer notifies you to correct it. When verification is successful, click **Next**.
10. **Ready to Configure:** A summary of your configuration choices for the installation. Ensure that all items are correct before proceeding.
11. Click **Install** to continue or click **Back** to move back through the installer and change any items.

The **Copy Files** screen appears and the ETL files are copied to the system.

12. **Configure System:** The selected configuration settings are applied.
13. Click **Next**.
14. **Complete:** The Complete page appears after the install is successful. Click **Installation Log** to view details recorded for the installation process.
15. Click **Close** to finish.

After installing the ETL (PO to PME) you will need to allow the ETL to remotely access the Power Operation Server.

Install Power SCADA Anywhere Server

Power SCADA Anywhere allows a remote desktop session using a Web browser to the Power Operation Server. It is accessible only in the Power Operation Runtime.

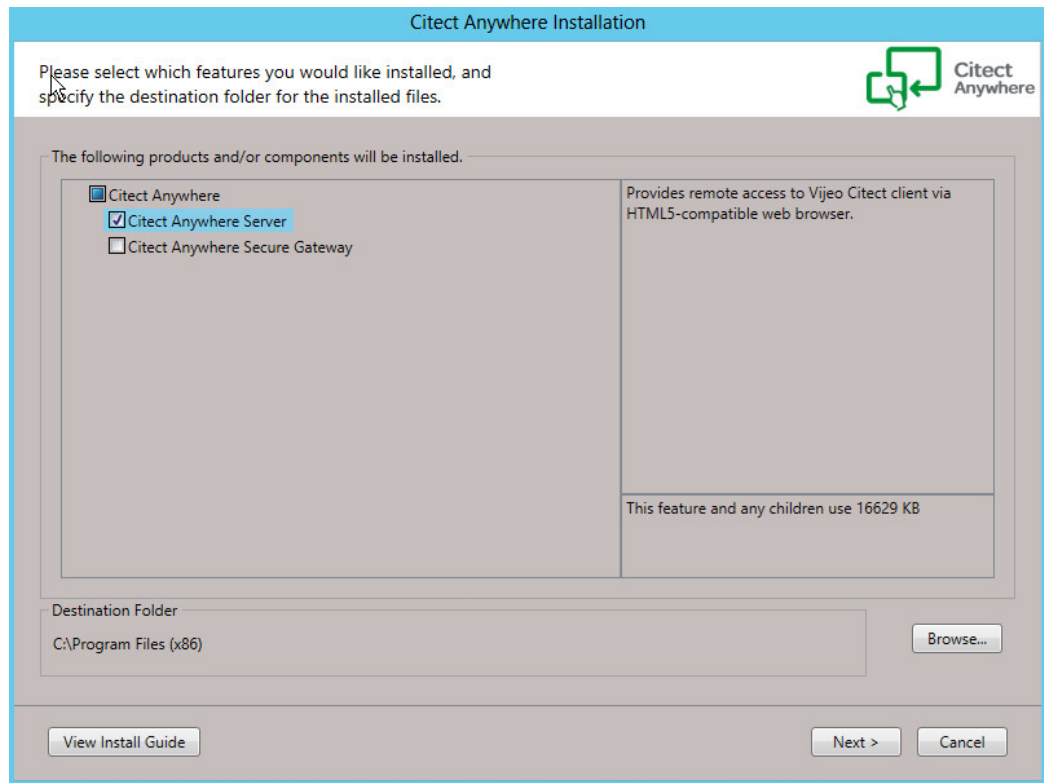
Power SCADA Anywhere is a rebranded name for Citect Anywhere. The term Power SCADA Anywhere will appear only in the end user-facing Web browser, at the login screen and the launch screen. Everything that is not end user-facing will be referred to as Citect Anywhere, including the installer, the configuration tool, and various file paths. Power SCADA Anywhere is available for download on the [Schneider Electric Exchange](#).

Prerequisites

- Before installing Power SCADA Anywhere, you must first install the Power SCADA Anywhere Server.
- Install a Power Operation Client Access. For the Power Operation Client Access, run the Power Operation install and select the client access-only installation. This installation requires a floating license. It must be on one of the following operating systems: Windows Server 2008 R2 SP1 Standard, Enterprise (64-bit)
 - Windows Server 2012 Standard
 - Windows Server 2016
 - Windows Server 2019

To install Power SCADA Anywhere:

1. On the machine where the Power SCADA Anywhere server is installed, launch the installer from the Power SCADA Anywhere installation folder: double-click setup.exe.
2. Click **Citect Anywhere Server**:



3. Accept the license agreement and click **Next** on each screen of the installation. If a prerequisite is missing, it will be installed for you.
4. When installation is complete, you see a confirmation screen. Click **Finish** to close the install.

For detailed instructions on installing and using the Power SCADA Anywhere Server, see the following documents:

- Power SCADA Anywhere Quick Start Guide.pdf
- Power SCADA Anywhere Installation and Configuration Guide.pdf

These documents in the Power SCADA Anywhere Installer folder.

Installing CAE

Cybersecurity Admin Expert (CAE) software tool installation requirements:

- Windows® 10 Pro 32-bit or 64-bit.
- Windows Server 2019, Windows Server 2016 64-bit, or Windows Server 2008 R2 64-bit
- Cybersecurity Admin Expert ZIP file.
 - ZIP file x86 for Windows 10 Pro 32-bit.
 - ZIP file x64 for Windows 10 Pro 64-bit.
- Other software components automatically installed in order to properly run CAE.
- Windows administrator username and password sign-in credentials.

1. Right-click the Cybersecurity Admin Expert ZIP file and select **Extract All... > Extract**.
2. Double-click the EXE file. The Cybersecurity Admin Expert wizard opens.
3. Select language > **OK**.
4. Click **Install**.
5. Click **Next** to go through the screens and select the options you want.
6. Click **Install**.
7. Click **Finish**. Cybersecurity Admin Expert icon is created on the desktop.

See [Configuring CAE cybersecurity](#) for detailed steps on configuring CAE.

After installing the software

Maintaining system currency

After you install and configure Power Operation 2021 with Advanced Reporting and Dashboards and deploy it as your production system, it is very important that you keep your software up to date. Schneider Electric will periodically publish updates in the form of service releases, hot fixes, or advisories relating to safety, security, and functionality of Power Operation.

Getting started with Power Operation

Power Operation is a suite of tools that lets you develop, design, and deploy SCADA systems. Built on the Plant SCADA platform, Power Operation Studio is the main SCADA development portal. Use Power Operation Studio to:

- Create, manage, and customize SCADA projects
- Create and manage I/O devices
- Design Power Operation Runtime elements
- Manage user access
- Open other SCADA productivity tools.

Power Operation is shipped with a project that has example page configuration.

To launch Power Operation Studio:

- Click Start > Schneider Electric > Power Operation Studio
- OR
- From the desktop, open the Power Operation folder and then open Power Operation Studio.

Uninstall and reinstall Power Operation

Use Add/Remove Programs in the Windows Control Panel to uninstall these programs:

- Power Operation v2021 (if you uninstall this, you also uninstall the Profile Editor)
- Power Operation Profile Editor
- Any additional Power Operation programs, such as the WebServer, that you installed

If you uninstall programs after you have already created projects, the project data will not be deleted. It is in `[Project Drive]\ProgramData\Schneider Electric\Power Operation\v2021\User`. The first time you launch the application after you re-install it, it will locate the project data and re-link it.

Uninstall does not remove all files from the system. Decommissioning removes Power Operation files from your system to prevent potential disclosure of sensitive, confidential, and proprietary data and software from your Power Operation system. You risk disclosing your power system data, system configuration, user information, and passwords if you don't decommission. We strongly recommend you decommission your system at the end of its' life.

Cybersecurity

This section contains up-to-date information about Power Operation cybersecurity. Network administrators, system integrators, and personnel that commission, maintain or dispose of a device should:

- Apply and maintain Power Operation security capabilities. See [Cybersecurity capabilities](#) for details.
- Review assumptions about protected environments. See [Protected environment assumptions](#) for details.
- Address potential risks and mitigation strategies. See [Potential Risks and compensating controls](#) for details.
- Follow recommendations to optimize cybersecurity.
- Implement cybersecurity configuration procedures. See [Configuring cybersecurity](#) for detailed configuration information.
- Regularly check for new releases of Power Operation. There may be additions or updates related to cybersecurity.

Power Operation has security capabilities that:

- Allow it to be part of a NERC CIP compliant facility. Go to the [North American Electric Reliability Corporation](#) website for information on NERC Reliability Standards.
- Align with cybersecurity standards in the IEC 62443 international standard for business IT systems and Industrial Automation and Control Systems (IACS) products. Go to the [International Electrotechnical Commission](#) website for information about the IEC62443 international standard. See [IEC 62443](#) for more information.

To communicate a security topic affecting a Schneider Electric product or solution, go to <https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp>.

WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords to help prevent unauthorized access to settings and information.
- Use Windows Active Directory for user account management and access to network resources.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.
- Follow cybersecurity tasks as described by your organization or contact your network administrator.

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

IEC 62443

IEC 62443 is an international cybersecurity Operational Technology (OT) standard with various levels of robustness against cyber threats.

Power Operation is SL2 certified to comply with IEC 62443 standard at the component level:

- IEC 62443-4.1: Assess a supplier's product development lifecycle for Industrial Automation and Control Systems (IACS).
- IEC 62443-4.2: Defines the security requirements for components of an IACS.

Product defense-in-depth

Use a layered network approach with multiple security and defense controls in your IT and control system to minimize data protection gaps, reduce single-points-of-failure and create a strong cybersecurity posture. The more layers of security in your network, the harder it is to breach defenses, take digital assets, or cause disruption.

Cybersecurity capabilities

This section describes the security capabilities available with Power Operation and capabilities when configured using Windows Active Directory and authentication.

Information confidentiality

- Secure protocols that employ cryptographic algorithms, key sizes and mechanisms used to help prevent unauthorized users from reading information in transit and information at rest.

- Support for McAfee Application Control or similar software to help protect against zero day attacks.
- Passwords and sensitive or confidential data on disk are encrypted while at rest.
- Certificates in compliance with recognized international standards are used to encrypt TLS data in transit:
 - Certificates for gRPC and the web are generated during installation and are unique for every installation. Each having its own issuing authority which is also generated during installation.
 - The Citect comms certificate is created during configuration and secures Citect communication.

Configuration

These security capabilities support the analysis of security events, help protect the software from unauthorized alteration and records configuration changes and user account events:

- Internal time synchronization.
- Time source integrity protection and configuration event logging.
- Timestamps, including date and time.
- Settings can be saved as a configuration file using Plant SCADA.
- Offload information to syslog or a protected storage or retention location.

User accounts and privileges

These security capabilities help enforce authorizations assigned to users, segregation of duties and least privilege:

- Windows Active Directory integration, role-based access control, and two-factor authentication using YubiKey.
- Power Operation Runtime user partitioning, eight levels of user privilege, and user event monitoring, including, log in, log out, shutdown, control.
- Identify and authenticate software processes managing accounts using Windows Active Directory.
- Least privilege and whitelisting configurable in multiple dimensions: read; control; time sync; alarm acknowledgement; application access; notification, security and communications configuration.
- User account lockouts configurable with number of unsuccessful login attempts using Windows Active Directory.
- Use control is used to restrict allowed actions to the authorized use of the control system.
- Supervisors can override user authorizations by deleting their account.
- Password strength feedback using Windows Active Directory.

Hardening

These security capabilities help prohibit and restrict the use of unnecessary functions, ports, protocols and/or services:

- Least functionality can be applied to prohibit and restrict the use of unnecessary functions, ports, protocols and/or services.
- Port numbers can be changed from default values to lower the predictability of port use.
- Session lock is used to require sign in after a configurable time-period of inactivity using Windows Active Directory.
- Session termination is used to terminate a session automatically after inactivity or manually by the user who initiated the session.

System upgrades and backups

This security capability helps protect the authenticity of the software and facilitates protected file transfer: digitally signed software is used to help protect the authenticity of the software and only allows software generated and signed by the manufacturer.

Threat intelligence

These security capabilities help provide a method to generate security-related reports and manage event log storage:

- Machine and human-readable reporting options for current security settings.
- Audit event logs to identify:
 - Software configuration changes.
 - Energy management system events.
- Audit storage using event logs by default and alternate methods for log management using Windows Active Directory.

Protected environment assumptions

- Cybersecurity governance – available and up-to-date guidance on governing the use of information and technology assets in your company.
- Perimeter security – installed devices, and devices that are not in service, are in an access-controlled or monitored location.
- Emergency power – the control system provides the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.
- Software and firmware upgrades – software and device upgrades are implemented consistently to the current version.
- Controls against malware – detection, prevention and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.
- Physical network segmentation – the control system provides the capability to:
 - Physically segment control system networks from non-control system networks.
 - Physically segment critical control system networks from non-critical control system networks.
- Logical isolation of critical networks – the control system provides the capability to logically and

physically isolate critical control system networks from non-critical control system networks. For example, using VLANs.

- Independence from non-control system networks – the control system provides network services to control system networks, critical or non-critical, without a connection to non-control system networks.
- Encrypt protocol transmissions over all external connections using a Virtual Private Network (VPN) or a similar solution.
- Zone boundary protection – the control system provides the capability to:
 - Manage connections through managed interfaces consisting of appropriate boundary protection devices, such as: proxies, gateways, routers, firewalls and encrypted tunnels.
 - Use an effective architecture, for example, firewalls protecting application gateways residing in a DMZ.
 - Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site, for example, data centers.
- No public internet connectivity – access from the control system to the internet is not recommended. If a remote site connection is needed, for example, encrypt protocol transmissions.
- Resource availability and redundancy – ability to break the connections between different network segments or use duplicate devices in response to an incident.
- Manage communication loads – the control system provides the capability to manage communication loads to mitigate the effects of information flooding types of DoS (Denial of Service) events.
- Control system backup – available and up-to-date backups for recovery from a control system failure.

Potential risks and compensating controls

Address potential risks using these compensating controls:

Area	Issue	Risk	Compensating control
Secure protocols	ION, Modbus, DNP, IEC 61850 and some IT protocols are unsecure. Power Operation does not have the capability to transmit data encrypted using these protocols.	If a malicious user gained access to your network, they could intercept communications.	For transmitting data over an internal network, physically or logically segment the network.
			For transmitting data over an external network, encrypt protocol transmissions over all external connections using a Virtual Private Network (VPN) or a similar solution.
			See Protected environment assumptions for information on compensating controls.

⚠ WARNING

DATA IN TRANSIT IS POTENTIALLY UNENCRYPTED AND COULD BE ALTERED

When transmitting data using ION, Modbus, DNP, IEC 61850 and some IT protocols:

- Physically or logically segment the network.
- Encrypt protocol transmissions over all external connections using a Virtual Private Network (VPN) or a similar solution.

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

Hardening

Recommendations to optimize cybersecurity in a protected environment:

- Harden environments according to your company's policies and standards.
- Apply least functionality to prohibit and restrict the use of unnecessary functions, ports, protocols and/or services.
- Implement cybersecurity configuration procedures. See [Configuring cybersecurity](#) for detailed configuration information.

Configuring cybersecurity

Recommendations to optimize cybersecurity in a protected environment:

- Use Access Control for objects in Windows Active Directory and authentication.
- Use Plant SCADA to store configuration files.
- Follow recommendations and implement cybersecurity configuration using the [Cybersecurity configuration checklist](#).

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices to help prevent unauthorized access to the software.

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

Cybersecurity configuration checklist

Action	Link
Address potential risks using compensating controls.	Potential risks and compensating controls

Action	Link
Set-up user access and apply least privilege.	Default security settings Using single sign-on Configuring two-factor authentication Windows Active Directory
Harden environments, change port numbers from default values, and configure server and firewalls to restrict and control traffic between IT, OT, and Internet network zones.	Default port numbers Encryption, locking USB ports, and hardening servers
Follow whitelisting design considerations and use application whitelisting and McAfee to prevent unauthorized applications from running on your systems.	Whitelisting
Configure the Service Layer, set permissions on the certificate, and update the registry configuring third-party certificates.	Configuring third-party certificates
Configure a one-time password for two-factor authentication using a YubiKey USB key device.	Configuring two-factor authentication
Configure to communicate with multiple network adapters in a segmented architecture.	Configuring projects for network segmentation

See [Using Cybersecurity Admin Expert \(CAE\) for cybersecurity](#) for information on configuring cybersecurity using the CAE tool.

Personal information confidentiality

Power Operation does not proactively collect personal information. Some personal information is collected and stored related to settings and functionality.

Ensure live data and backups are protected.

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords to help prevent unauthorized access to settings and information.
- Use Windows Active Directory for user account management and access to network resources.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.
- Follow cybersecurity tasks as described by your organization or contact your network administrator.

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

See:


- [Product defense-in-depth](#) for details about defense controls in your IT and control system to maximize data protection.
- [Cybersecurity capabilities](#) for more details about information confidentiality.

Default security settings

Area	Default setting
Firewall ports	Enabled.
User access to application resources	Disabled.
User account roles and privileges	See User account roles and privileges for details.

Viewing security settings

Area	View settings
Ports	Use the built-in Windows command line netstat to view enabled ports. Follow hardening tasks as described by your organization or contact your network administrator.

Area	View settings
User access to application resources	<ol style="list-style-type: none"> 1. Click Start  on the taskbar. 2. Select AVEVA > Configurator. The Configurator opens. 3. Select Power Operation > Security Roles.
User account roles and privileges	Open the configuration file <code>configuration.xml</code> located in <code>C:\Program Files (x86)\Schneider Electric\Power Operation\v2021\Applications\AppServices\bin\</code> . See User account roles and privileges for more information.

Default port numbers

Each server component has a unique default port assigned to it. This default port may only be used with that type of server. However, application engineers may choose ports other than the defaults, depending on the design of the project. Non-default ports need to also be added to the firewall exceptions.

Which ports are required for a specific installation depends on the Power Monitoring Expert system configuration and the monitoring devices used.

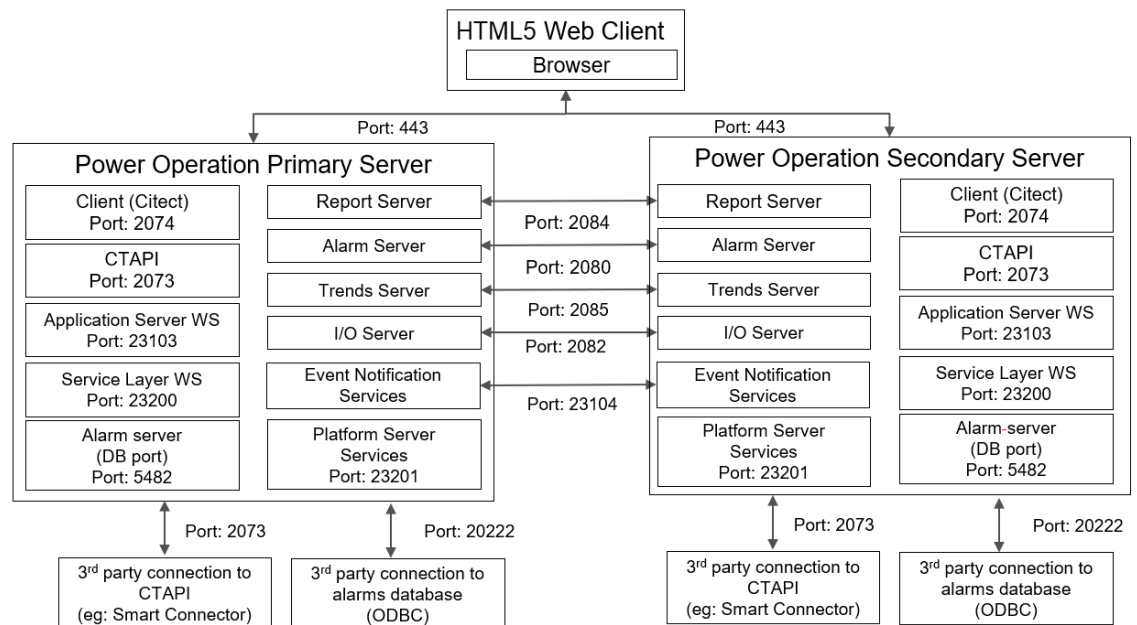
If Power Operation alarm, trend, report and I/O servers are created using non-default ports, create those ports exceptions.

Service	Default port	Description
Alarm Server (Citect)	5482	Database port for alarms.
Alarm Server (Citect)	2080	Synchronization between redundant Citect alarm server components.
Application Server	23103	Web services used by Basic Reports and Live View.
Client (Citect)	2074	Cicode (custom script) debugging.
Client access and/or ActiveX web client	5500-5509	Ports used for thick control client and ActiveX web client to communicate to server.
CTAPI (Citect)	2073	Used by Power Operation components to interact with Citect server processes.
Database	5432	Used to connect to PostgreSQL Database Engine.
Event Notification	23104	Synchronization between redundant Power Operation notification servers.
FTP, IDC	21	Page downloads for IDC, Internet Display Server/Client communications.
I/O Server (Citect)	2082	Publish and subscribe I/O server communications.
ODBC	20222	Open Database Connectivity server.
OPC UA	48031	OPC Unified Architecture communication
Report Server (Citect)	2084	Report server communications.

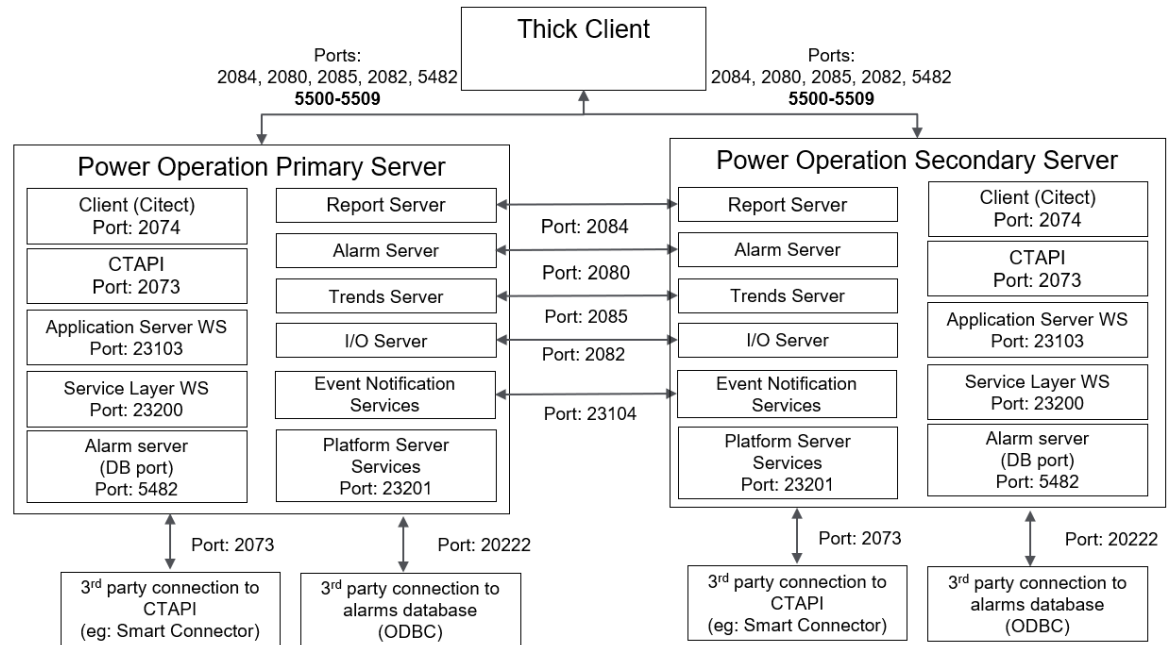
Service	Default port	Description
Platform Server	23201	Services for communications with the Service Layer Platform Server.
Trends Server (Citect)	2085	Synchronization between redundant Citect trend server communications.
Web Server	443	Web HMI application. Access to page and document content, diagrams, and all system data.
Service Layer	23200	Services for communications with the Service Layer Pso Web Service.

Default port numbers and associated server types

HTML5 Web Client



Thick Client



For information about the ports for Advanced Reporting and Dashboards, see Ports in the *Power Monitoring Expert – IT Guide*.

Windows Active Directory

It is recommended to use Windows Active Directory exclusively for user account management and access to network resources. Power SCADA Anywhere users should only be managed using Windows Active Directory.

Power Operation supports Windows Active Directory integration, including enforcement of minimal password complexity, password expiration, role based access control and other password management strategies.

For cybersecurity purposes, we recommend that you use Windows Active Directory with a strong password policy.

If you don't use Windows Active Directory:

- Unintentional access could occur, for example assumed inactive accounts could actually be active.
- The ability to configure some settings may not be available, for example automated password complexity and expiry.

There are eight levels of user privileges (HMI user partitioning) and HMI user event monitoring (login/logout, shut down, control).

Power Operation components including Servers, Client Access, and View-only Clients support both user management using Windows Active Directory groups and local users.

NOTE: Power SCADA Anywhere must be installed on a machine that is part of a Windows domain.

Whitelisting

Whitelisting design considerations:

- Power Operation Servers, Client Access, View-only Clients, and Advanced Reporting have been validated using McAfee Application Control.
- McAfee Whitelisting product documentation can be found on the [McAfee website](#).

Application whitelisting

Zero Day cybersecurity attacks take place before a software vendor is aware of a cybersecurity exploit. This means that neither software nor anti-virus programs have been created or updated to protect against the zero-day threat or attack.

Application whitelisting is recommended to protect against Zero Day attacks. Application whitelisting proactively blocks unauthorized executable files on the PO Server than are not part of the whitelist, such as executable files, java apps, Active X controls, and scripts.

Power Operation has been validated with the McAfee Application Control whitelisting application.

NOTE: Allow the install to add a desktop shortcut; you need it for all interactions with Application Control. Also, before you run Application Control, make sure that you have installed all other software that you want on the computer.

Using Application Control

Right-click the desktop icon and select the Run As Administrator option.

First, you need to create and confirm the whitelist. To do this:

1. Invoke the *sadmin* command line as an administrator and type the command `sadmin solidify`.

This process can take some time to complete. When it is complete, you see a line telling you total files scanned and the number that are "solidified."

2. Verify the whitelist with the command `sadmin status`.

Verify that the whitelist status of drives or volumes is *solidified*.

3. When this is complete, you need to enable the enforcement of the whitelist: type the command `sadmin enable`.

4. Add updaters: Updaters are components for which you provide permission to update the system. Any program or script that will be able to update the system must be configured as an updater. To add an updater, enter on the command line:

```
sadmin updaters add <xxx>
```

where xxx is the name of the component

For a complete discussion of updaters, see "Using Updaters" in the McAfee Product Guide (on the Power Operation installation disk, see McAfee Embedded Control > Documents > Product-Guide-v6.2.0)

When running in Enabled mode, Application Control can prevent a legitimate application from executing if the required rules are not defined. Application Control tracks all unsuccessful attempts made by authorized applications to modify protected files or run other executable files.

Review information for unsuccessful attempts

Do this to identify updater rules and allow legitimate applications to run successfully.

1. Enter the command `sadmin dia`.
2. To add the suggested updaters to the authorized list, use the command `sadmin diag fix`.

When you deploy Application Control, it scans the system and creates a whitelist of all executable binaries and scripts present on the system. The whitelist also includes hidden files and folders.

The whitelist lists all authorized files and determines trusted or known files. In Enabled mode, only files that are present in the whitelist can execute. All files in the whitelist are protected; you cannot change or delete them. An executable binary or script that is not in the whitelist is said to be "unauthorized," and it is prevented from running.

You can also use Application Control to help write-protect files, directories, drives or registry entries. Additionally, you can use it to read-protect files, directories, or drives. For more information about these applications, see the Product Guide.

Configuring third-party certificates

To configure third-party certificates for use with Power Operation, you must configure the service layer, edit the certificate, and then update the registry.

NOTE: The third-party certificate you want to use must be in the Personal Information Exchange (PFX) file format.

Configuring the Service Layer

1. Navigate to and double-click the PFX file you want to import. The Certificate Import Wizard appears.
2. Select **Local Machine** and click **Next**.
3. In the File name field, verify the name of the file you are importing, then click **Next**.
4. If a password exists for the private key, enter it in the **Password** field.
5. Select the **Mark this key as exportable. This will allow you to back up or transport your keys at a later time.** and **Include all extended properties.** check boxes.

Type the password for the private key.

Password:

.....

Display Password

Import options:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Protect private key using virtualized-based security(Non-exportable)

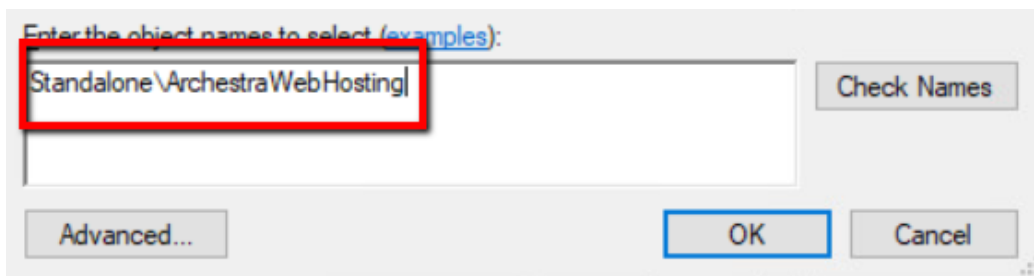
Include all extended properties.

Next Cancel

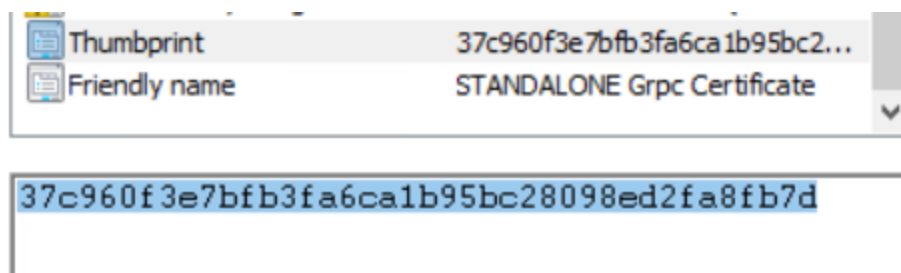
6. Click **Next**.
7. On the Certificate Store page, choose the default option (**Automatically select the certificate store based on the type of certificate**), then click **Next**.
8. Click **Finish**.
9. Click **OK**.

Setting permissions on the certificate

1. Press **Window + R** to open the Run window.
2. In the Open field, type **mmc** and click **OK**.
3. In the Console window, select **File > Add/remove snap-in**.
4. In the left pane, select **Certificates**, then click **Add**.
5. In the Certificates snap-in window, select **Computer account**, then click **Next**.
6. Select **Local computer**, then click **Finish**.
7. Click **OK** to close the Add or Remove Snap-ins window.
8. In the Console Root pane, expand **Certificates > Personal > Certificates**. The installed certificate appears in the right pane.
9. Right-Click the certificate and select **All Tasks > Manage Private Keys...**
10. Click **Add** and type **<ComputerName\ArchestraWebHosting>** then click **OK**.



11. Verify that Full Control and Read permissions are allotted to the OrchestraWebHosting group.
12. Click **OK**.
13. Double-Click the certificate to view it. Select the **Details** tab, then locate and click the Thumbprint field in the list.
14. Highlight the value, then press **Ctrl + C** to copy the value and press **Ctrl + V** to paste it to notepad or another text editor. You will need this value to update the registry.



NOTE: Some operating systems may store the Thumbprint with spaces, you may have to delete the spaces prior to updating the registry.

Updating the Registry

NOTICE

IRREVERSIBLE OPERATING SYSTEM DAMAGE OR DATA CORRUPTION

Before making any changes, back up your Windows Registry to a network folder or other remote location.

Failure to follow these instructions can result in permanent loss of Failure to follow these instructions can result in irreparable damage to your computer's operating system and all existing data.

NOTE: Registry edits must be performed only by qualified and experienced personnel.

1. Start a Windows command-prompt in Administrator mode.
2. Copy and paste the following command to create a backup of the registry key:
Reg copy "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Schneider Electric\Power Operation\WebApplications\Default" "HKEY_LOCAL_

```
MACHINE\SOFTWARE\WOW6432Node\Schneider Electric\Power Opeation\We-  
bApplications\Default_orig" /s /f
```

3. Copy and paste the following command to update the registry value:
Reg Add "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Schneider Elec-
tric\Power Operation\WebApplications\Default" /t REG_SZ /v SslThumbprint /d "<PASTE
THE THUMBPRINT HERE>" /f
4. Run the following commands for the changes to take effect in the services:

```
%windir%\System32\inetsrv\Appcmd stop apppool /apppool.name:PsoWebServiceAppPool  
%windir%\System32\inetsrv\Appcmd start apppool /apppool.name:PsoWebServiceAppPool  
%windir%\System32\inetsrv\Appcmd stop apppool /apppool.name:PlatformServerAppPool  
%windir%\System32\inetsrv\Appcmd start apppool /apppool.name:PlatformServerAppPool
```
5. Close the command prompt.

Encryption, locking USB ports, and hardening servers

Encryption

Configure the system to use the latest version of Transport Layer Security (TLS), at least version 1.2.

PO supports the ability to encrypt communication between PO components via latest Transport Layer Security (TLS) version. Communication is encrypted between:

- Server(s) and client(s)
- Server to server.

Locking-down USB ports on server computers

Power Operation supports electronic software keys to allow IT departments to lock-down USB ports on server computers.

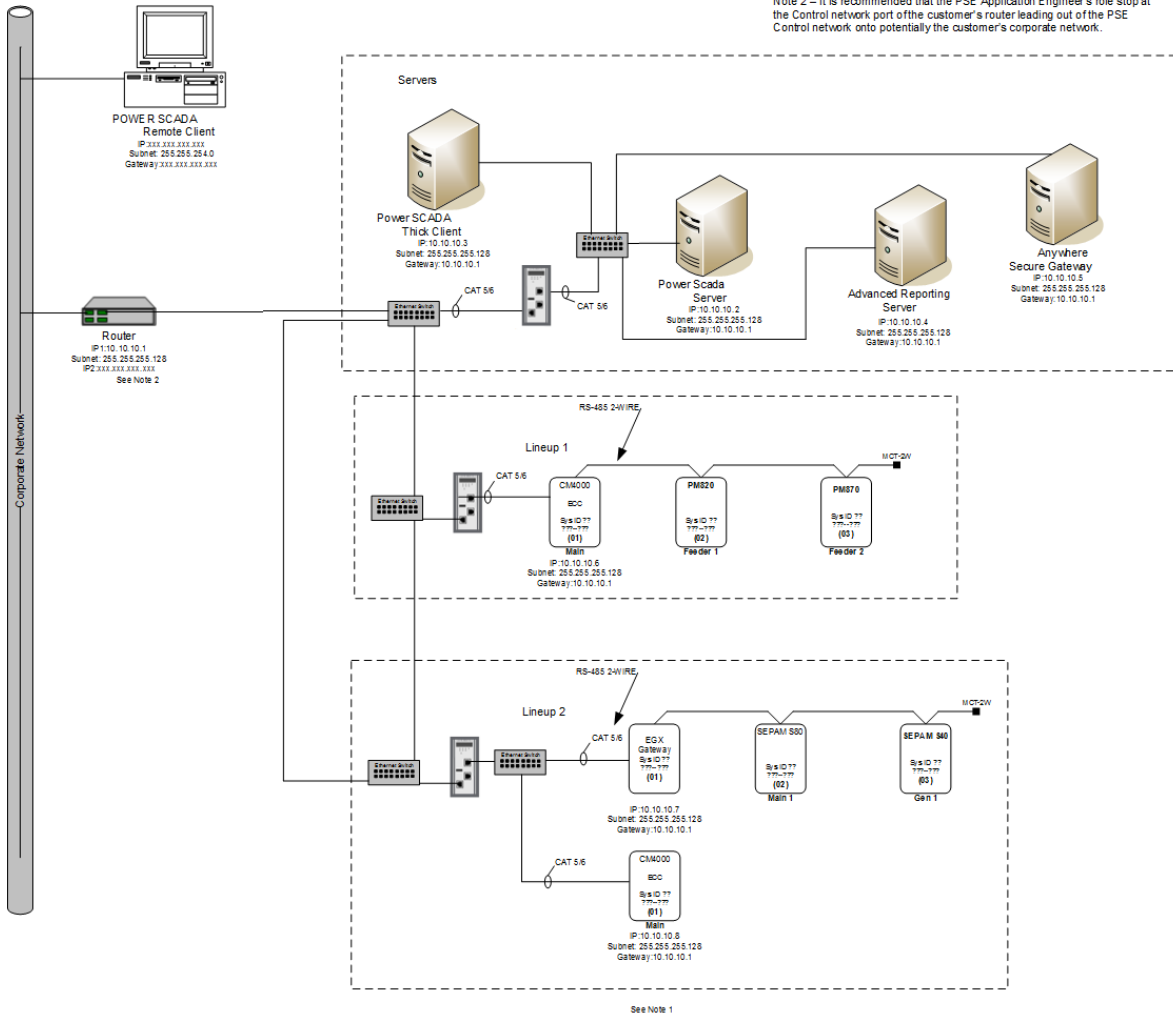
The configuration setup steps are:

1. Create a project.
2. Add all the devices on the network.
3. Configure the rules for the network that define the traffic that can pass through which firewall.

We recommend that you begin with the firewalls in test mode so you can see what would be blocked and then adjust accordingly. The firewall configurations should be then loaded onto a USB flash drive that is used to upload the configuration to each firewall.

The following is an example architecture that can serve as reference for how one of the networks might be constructed. It is a small network that can be scaled out to fit a much larger system.

Note 1 – Two lineups are shown, but this architecture is scalable to include many more lineups or operational areas.
 Note 2 – It is recommended that the PSE Application Engineer's role stop at the Control network part of the customer's router leading out of the PSE Control network onto potentially the customer's corporate network.



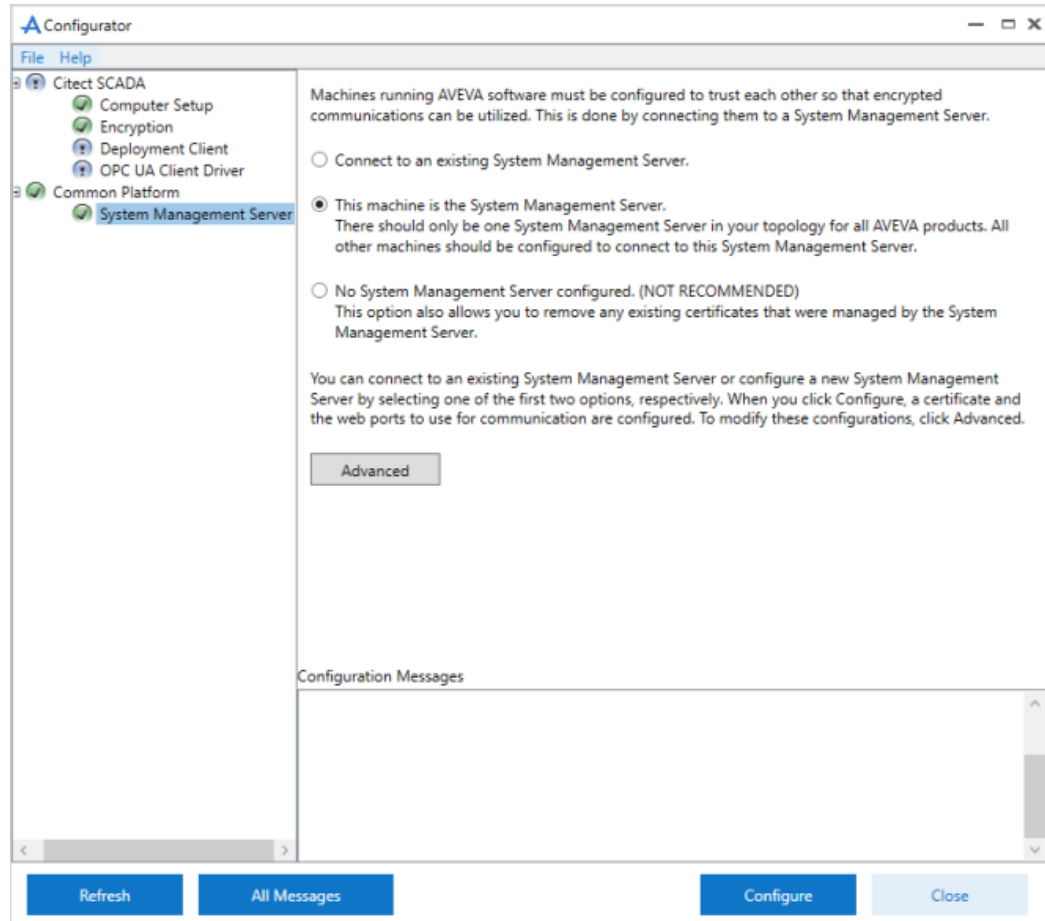
Configuring a System Management Server

Power Operation needs post-installation configuration to use encrypted communications. Only one of the machines in the network can be identified and configured as the System Management Server. Use the Configurator to establish a trust relationship between one or more machines running Power Operation. 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.

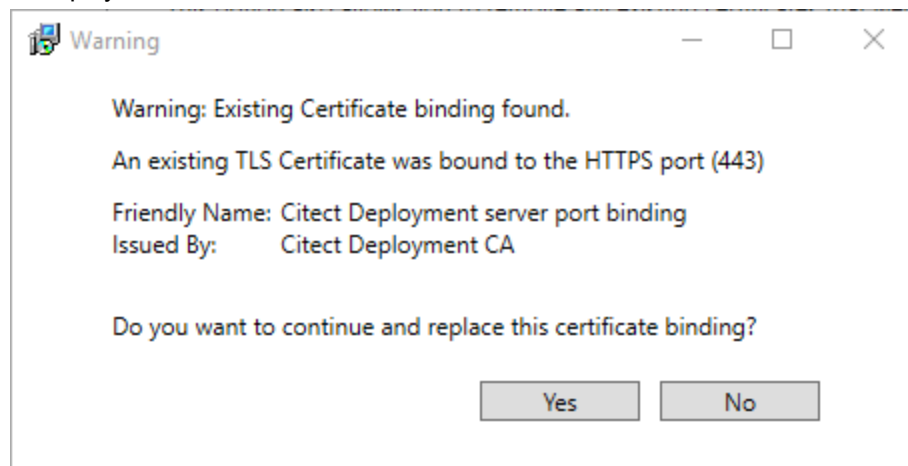
To connect to the System Management Server, you need to be a member of either the “aaAdministrators” or the “Administrators” group on the machine where the System Management Server is installed.

1. Start the Configurator.

- In the left pane, click **Common Platform > System Management Server**. The following is displayed:

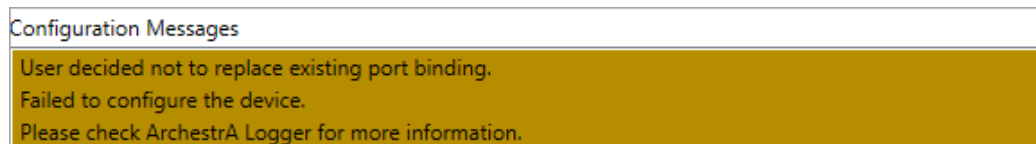


- Select **This machine is the System Management Server**. Review the notes on the screen before you start the configuration.
- Click **Configure**. If an existing binding is found for the specified ports, the following message is displayed:

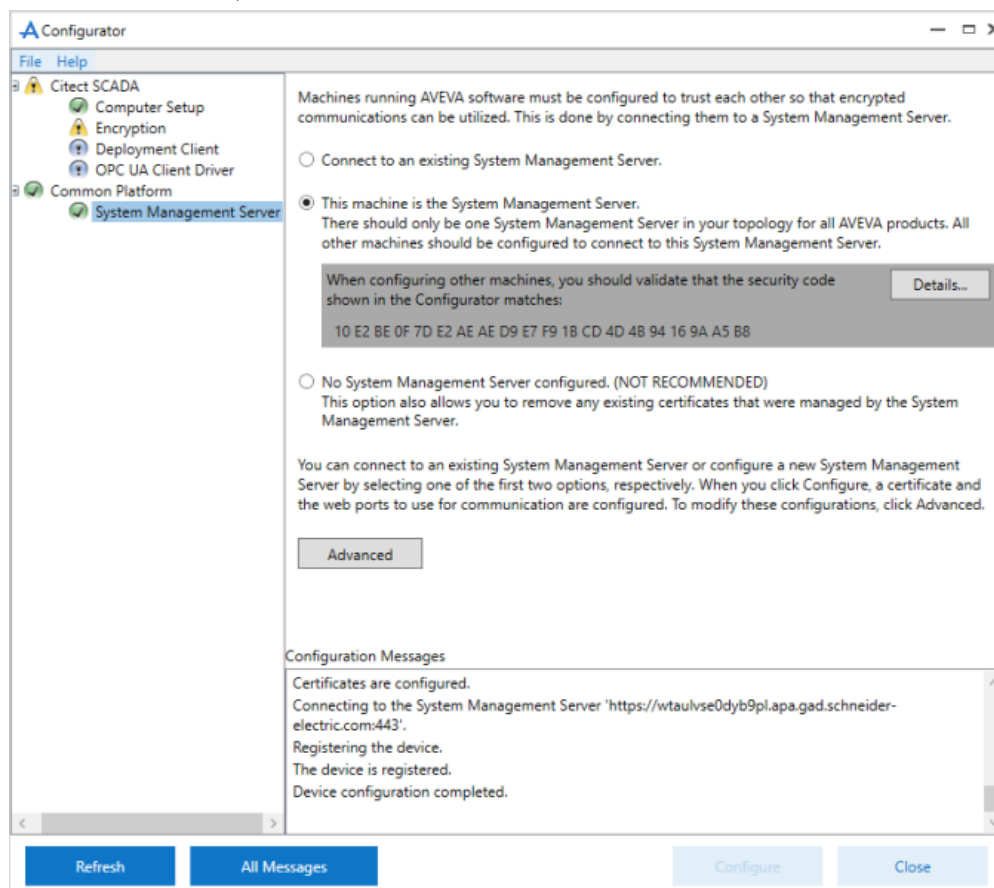


- Click **Yes** if you wish to replace the binding. The Configurator will start configuring the System Management Server.

If you click **No**, the following message will be displayed in the Configuration Messages area:



- 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**.



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

Configuring two-factor authentication

NOTE: For cybersecurity purposes, it is strongly recommended that you configure two-factor authentication in your projects; especially in deployments with control functionality.

Power Operation uses a one-time password (OTP) to accomplish two-factor authentication. OTP is implemented in Power Operation using a USB key device called a YubiKey. The YubiKey is designed to fit on a key ring or attached to a badge. It must be plugged into the client machine when the user authenticates.

NOTE: You can export one-time password settings to other servers.

Ordering YubiKeys

Keep in mind these points when you are ordering or using a YubiKey:


- You must set "Allow RPC" to TRUE for all roles that are using YubiKey.
- YubiKey is compatible with all thick clients.
- YubiKey requires access to a USB port at each client.
- Each Power Operation I/O Server must have Application Services (Core Service Host) running.
- Multiple I/O servers may reside on a physical machine. In this case, only one instance of Application Services resides on the machine.
- YubiKey must be configured and synchronized across all I/O servers (this includes redundant pairs and distributed systems).
- YubiKey is enabled on each client independently. If YubiKey is enabled on a client, all users on that client must authenticate via YubiKey.
- It is possible to configure YubiKey on one machine, export the configuration for all users, and import the configuration to all remaining machines.
- It is not necessary to re-program YubiKey when changing passwords. The YubiKey changes the OTP every time so it is not susceptible to replay attacks.
- YubiKey is authenticated against all servers that contain at least one I/O Server. All servers must successfully authenticate the OTP for success. If a single server does not authenticate (due to misconfiguration, etc.), the user will not be able to log in.
- If a machine (with an I/O Server) is not available, it is not included in the authentication scheme. This means that if a primary server is down, the secondary can still successfully authenticate the OTP.
- If no servers (with I/O servers) are available, the user will not be able to log in on clients that have YubiKey enabled.

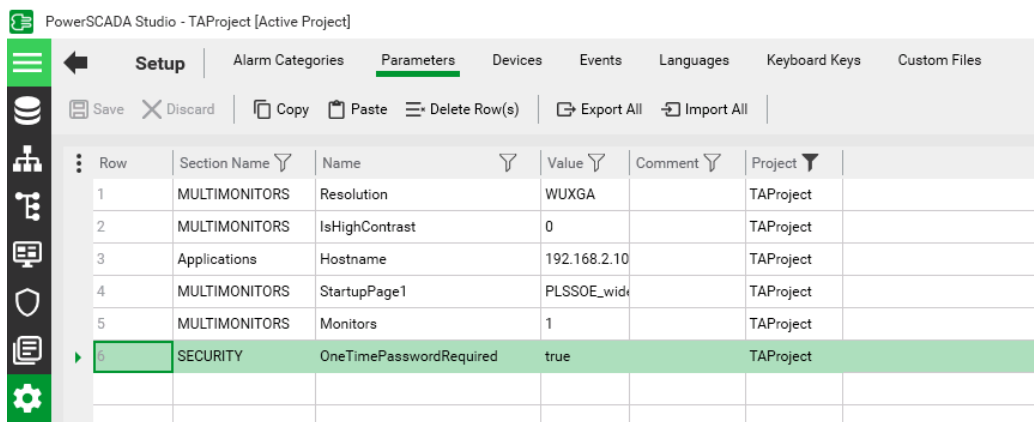
Add the Citect parameter

You need to add the parameter that allows Power Operation to communicate with the YubiKey. You can do this before or after you configure the YubiKey.

NOTE: Before you add the parameter, make sure the correct project is active.

To add the parameter:

1. From Power Operation Studio, click **Setup**  > **Parameters**.
2. Enter the following:
 - Section Name: Security
 - Name: OneTimePasswordRequired
 - Value: true




Row	Section Name	Name	Value	Comment	Project
1	MULTIMONITORS	Resolution	WUXGA		TAPProject
2	MULTIMONITORS	IsHighContrast	0		TAPProject
3	Applications	Hostname	192.168.2.10		TAPProject
4	MULTIMONITORS	StartupPage1	PLSSOE_wid		TAPProject
5	MULTIMONITORS	Monitors	1		TAPProject
6	SECURITY	OneTimePasswordRequired	true		TAPProject

3. Compile the project.

Set Allow RPC to TRUE for all YubiKey-user roles

To use YubiKey in Power Operation, you must set Allow RPC to TRUE for all roles that include users with assigned YubiKeys. The default for Power Operation 2021 is FALSE.

To change Allow RPC to TRUE:

1. In Power Operation Studio, click **Security**  > **Roles**.
2. For each YubiKey-user role, change **Allow RPC** to **TRUE**.

YubiKey configuration

You can autoconfigure a YubiKey or program it manually.

In most cases, you can autoconfigure the YubiKey, thus avoiding the lengthier process of programming it. Autoconfiguration may not work with all YubiKey models; however, all OTP-compliant keys can be manually programmed.

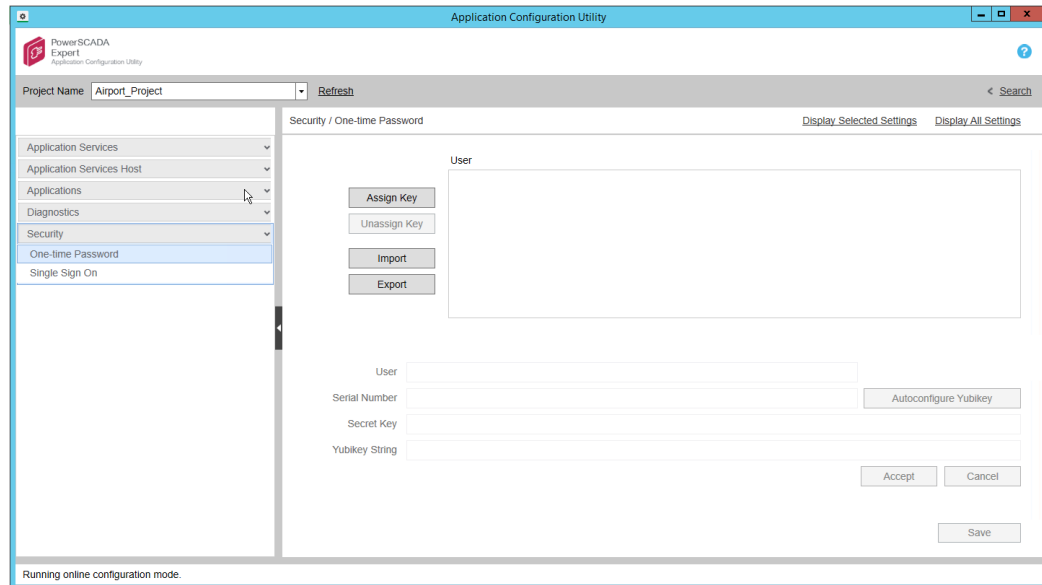
NOTES:

- Autoconfigure requires that you have a USB port available on your computer.
- If you do not have a USB port available on the server – because it is in a virtual machine or you do not have physical access– program the key on a remote machine (see ["Manually configure the YubiKey" on page 49](#), below), and then transfer the configuration to the server .
- Autoconfigure will not work on virtual machines.
- You can only have one YubiKey inserted at a time.
- If autoconfigure will not work, you must manually program the YubiKey. See ["Manually configure the YubiKey" on page 49](#) for instructions.

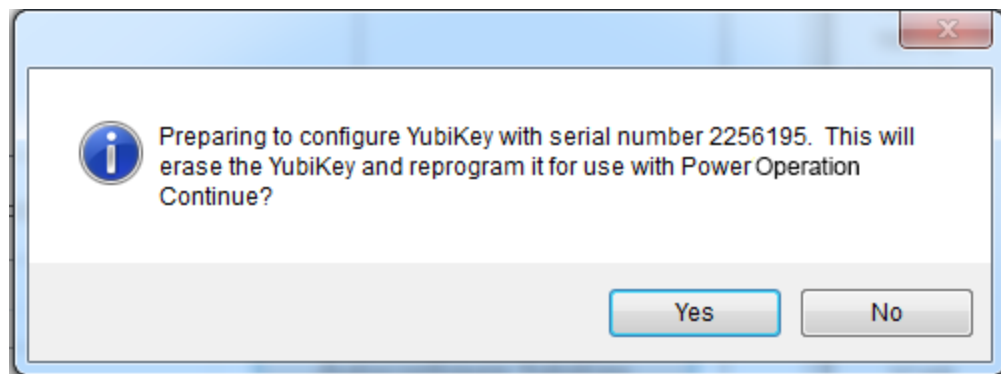
Auto-configuring the YubiKey

To auto-configure the YubiKey:

1. Insert the YubiKey into the USB port of the computer.
2. In the Application Configuration Utility, click **Security > One-Time Password**.



3. Click **Assign Key**.
The grayed-out fields are enabled.
4. In the **User** field, type the Power Operation username (or user name from Active Directory) to which you want to assign the YubiKey.
5. Click **Autoconfigure YubiKey**. The following message appears:



This message tells you that all settings on the key will be erased, including any key assignments.

6. To continue, click **Yes**. The key will receive a new secret key.
7. Click **Accept**.

Manually configure the YubiKey

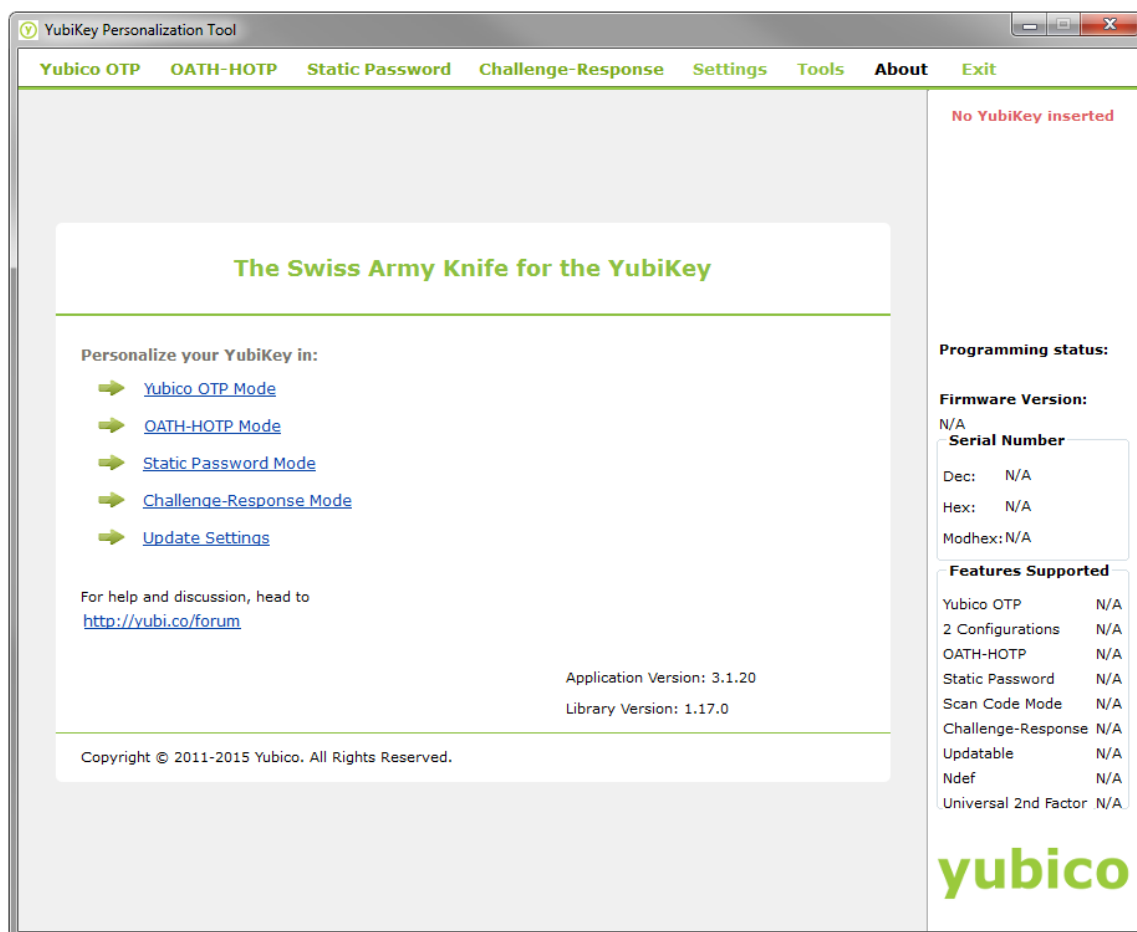
If you cannot auto-configure the YubiKey, program and configure it manually.

After you obtain the YubiKey from a third-party vendor, (such as Amazon), download the YubiKey Personalization Tool from the Yubico web site: www.yubico.com; click Products > Services & Software > Personalization Tools > Download YubiKey Configuration Tools.

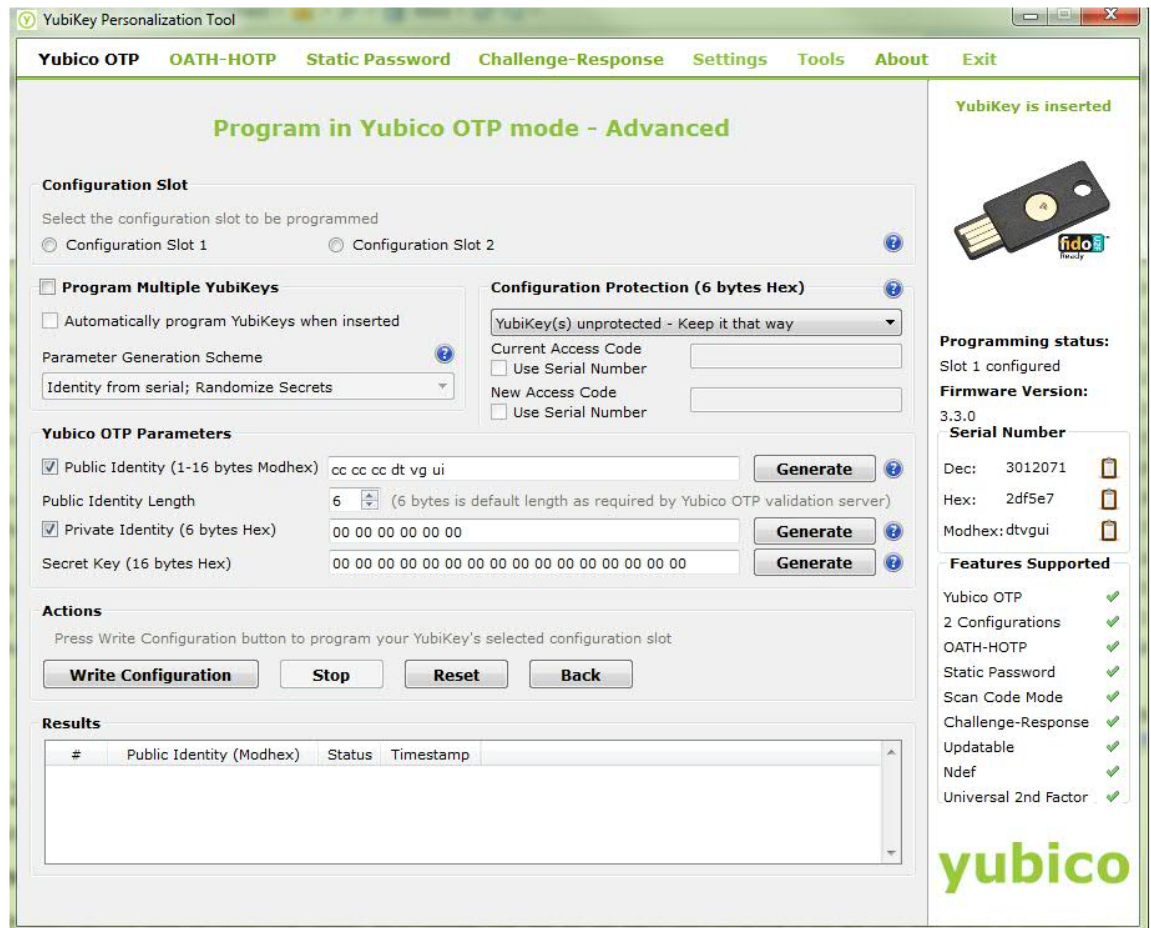
NOTE: This procedure outlines how to configure a single slot. If you want to use both of the key's configuration slots, download the YubiKey documentation, located under the Support tab of the Yubico website.

To manually configure the key:

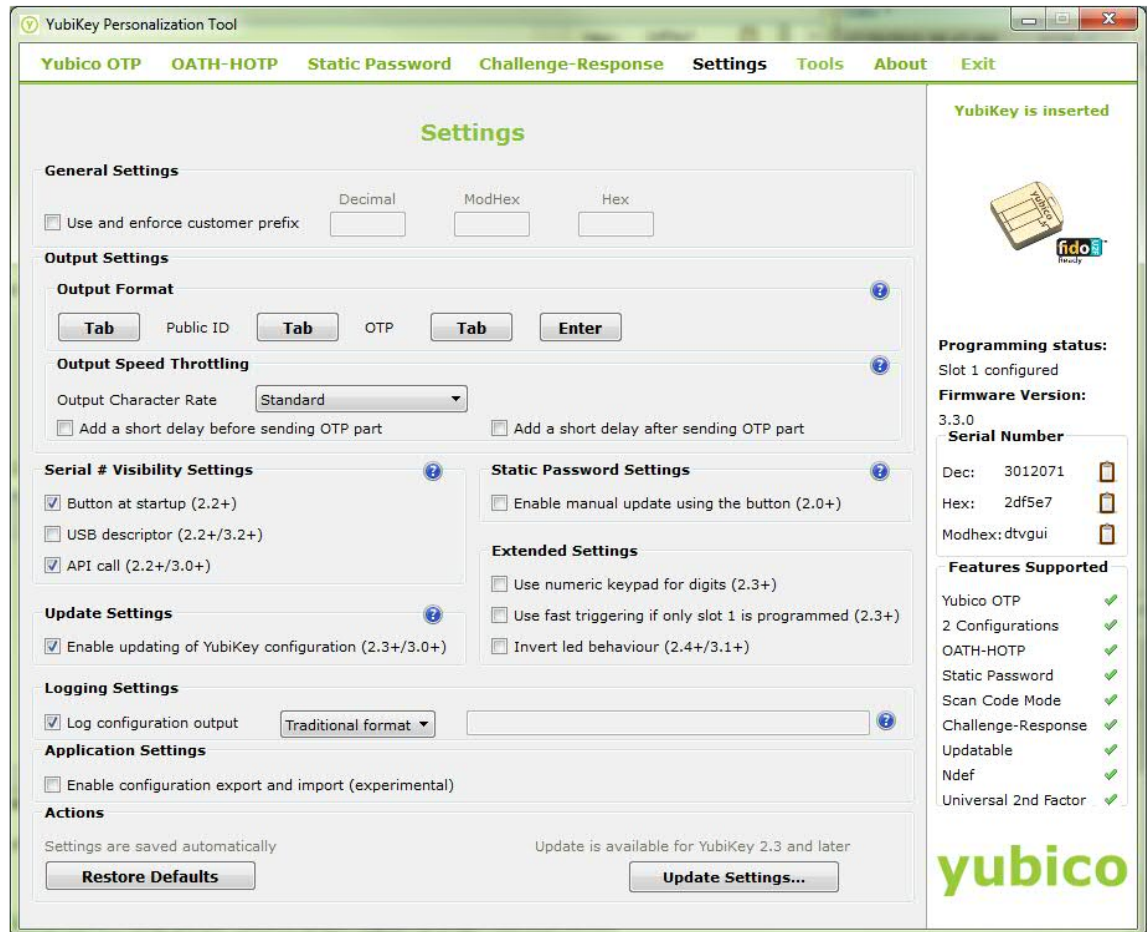
1. Launch the YubiKey Personalization Tool. The following screen appears:



2. Insert the YubiKey into a USB port of your computer. Click the Yubico OTP Mode link. At the next screen, click **Advanced**. The following screen appears:



3. In the **Configuration Slot** section, select the slot you want to configure.
4. In the **Yubico OTP Parameters** section:
 - a. Click **Public Identity**, and then click **Generate**.
 - b. Do not edit the default **Public Identity Length**.
 - c. Click **Private Identity** and then click **Generate**.
 - d. Beside **Secret Key**, click **Generate**.
 - e. Make note of the secret key that displays, including all characters and spaces. You will need it when you add the key to the Application Configuration Tool.
5. In the **Actions** section, click **Write Configuration**.
6. Click the **Settings** tab. This following screen appears:



7. Enter the following information:
 - a. Under **Output Settings**, click **Enter** to enable it; when enabled the button turns blue. Do not enable any of the **Tab** buttons.

This causes a return and an "OK" to automatically occur when you press the Yubikey as part of login in Power Operation.
 - b. Ignore the remaining settings. Click **Update Settings** at the bottom right of the screen.

The key is programmed.
8. Next, configure the key on the Power Operation computer:
 - a. In the Application Configuration Utility, click **Security > One-Time Password**.
 - b. Click **Assign Key**.
 - c. The fields on the lower half of the screen are enabled.
 - d. For **User**, type the user name that you are adding. This should be a Power Operation Studio user.
 - e. For **Serial Number**, type the number that is printed on the underside of the key.
 - f. For **Secret Key**, enter the Secret Key from the YubiKey Personalization Tool (created above). Enter the secret key exactly as it was created, including all spaces. After you enter it, the key will be encrypted and will display as bullets (••••) in the future.

- g. Press the button on the top of the YubiKey.
 - h. **YubiKey String:** This field is populated when you press the button in step 6.
 - i. Click **Accept**.
9. Repeat step 8 for any additional keys.

NOTE: Repeat steps 1 to 8 on each server computer in a redundant or distributed system.

Logging in with a programmed YubiKey and One-Time Password

After the key is programmed and associated with a user in Power Operation, and you have enabled YubiKey usage, the user will use the key to log in to the system.

To log in:


1. Insert the programmed YubiKey into a USB port of the Power Operation server.
2. Launch Power Operation Runtime, or access runtime via a remote web client.
3. Run the project you want to view.
4. In the upper right corner of the Startup screen, click **Login**.
5. Enter your name and password and then click **OK**. The One-time Password screen appears.
6. Press the button on the YubiKey.

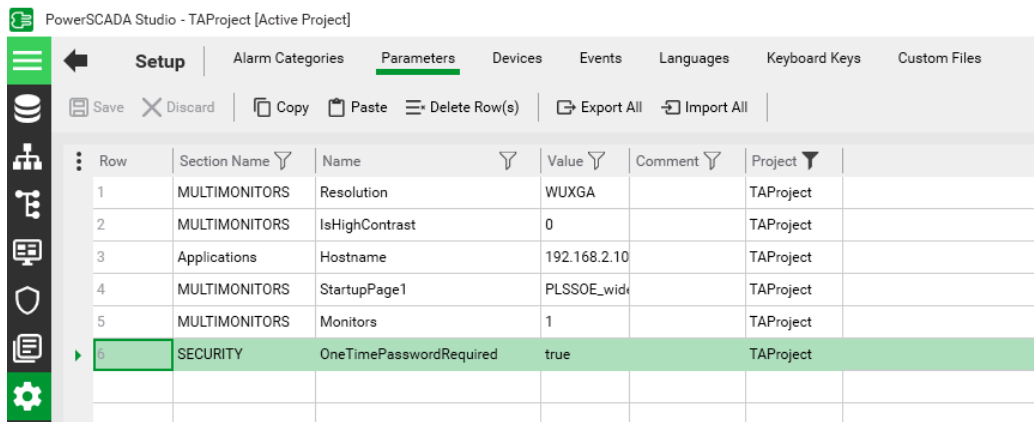
The one-time password is generated. The key and software communicate behind the scenes to verify the uniqueness of the one-time password and to click OK.

You can start using runtime screens.

Disabling YubiKeys

To disable a YubiKey:

1. In Power Operation Studio, click **Setup**  > **Parameters**, locate the parameter for the YubiKey.
2. Change the **Value** from true to false, and then compile the project.



Row	Section Name	Name	Value	Comment	Project
1	MULTIMONITORS	Resolution	WUXGA		TAPProject
2	MULTIMONITORS	IsHighContrast	0		TAPProject
3	Applications	Hostname	192.168.2.10		TAPProject
4	MULTIMONITORS	StartupPage1	PLSSOE_wid		TAPProject
5	MULTIMONITORS	Monitors	1		TAPProject
6	SECURITY	OneTimePasswordRequired	true		TAPProject

Configuring projects for network segmentation

Power Operation can be configured to communicate with multiple network adapters in a network segmentation architecture. For security reasons, consider network segmentation for the following scenarios:

- Multiple Power Operation servers or clients are configured to run over a WAN or the Internet.
 - Confirm that appropriate security precautions (such as a VPN) are used when connecting networks over a potentially public link (such as the Internet).
- An untrusted corporate network is connected to the control system network.

To configure a Power Operation project for network segmentation, follow these guidelines:

1. Go to the [AVEVA Knowledge & Support Center website](#) for information on adding network addresses.
2. Vijeo Citect 2015 Web Client Guide: Port-Forwarding / Address Forwarding (see Power Operation 2021Installation disc)
3. [Default port numbers](#)

Threat Intelligence

Event logs can assist with monitoring suspicious activity and identifying the cause of cybersecurity breaches that could lead to a cybersecurity incident. The Security Viewer lets you view user activity within your system. This screen lists all user actions that are captured in the Event Log.

By default, event logs are not shared with unauthorized users. Events are read only and cannot be changed.

Viewing event logs in the Security Viewer

- In the Power Operation Runtime, click the **Alarms/Events** tab, and then click **Security Viewer**.

The screenshot shows the 'Security Viewer' window with a table of alarm events. The table has the following columns: Date, Time, Operator, Classification, Message, and UserLocation. The first row shows an event at 02:52:32.947 PM with the message 'PLS AdvOL_LogEng_Fail_Primary - Alarm raised'. The interface also includes navigation tabs like HOME, ONE-LINE, ALARMS/EVENTS, ANALYSIS, SYSTEM SUPERVISION, REPORTS, APPLICATIONS, and ELEVATIONS. There are also filter and reset filter buttons above the table.

The screen displays a table with the following default columns:

Date	The date that the activity was logged.
Operator	User name from the Citect users.
Time	The time that the activity was logged.
Classification	The class of the event.
Message	From the Message field in the Alarm Log.
UserLocation	URL of the computer at which the activity occurred.

For more information on these fields, see **Alarm SOE fields** in the Plant SCADA help. Go to the [AVEVA Knowledge & Support Center website](#) for information on PLANT SCADA.

To change the view of the log, you can use any of the sort or filter features that are available in the Event Log.

Filtering information:

- To the left of the log, check one or more of the devices in the system. This filters information to include data only for those devices. When nothing is checked, all devices are included.
- You can insert and remove columns.

To add a column:

- Right-click in the header area of the log, then choose **Insert Column**. From the list that appears, check an additional column title. The new column displays to the left of the

column you clicked.

To remove a column:

- Right-click on the header of the column you want to delete and then click **Remove Column**.
- You can filter that data that is included. To do this, use the Security Viewer filter. For instructions on filtering the columns in the log, see ["Using the Security Viewer Filter" on page 55](#).

Using the Security Viewer Filter

To filter for the information that displays in the security viewer log, click **Filter** (in the upper left corner of the screen). The Security View Filter screen displays.

The following table describes the Security View Filter settings:

Filter option	Description: Display alarms for:
Basic Filter box:	
Start Date/End Date	<p>Choosing only a start date displays alarms from that date to the current date.</p> <p>Choosing only an end date displays alarms for the past year up to that date.</p> <p>For example, to display alarms only for today's date, enter only a start date.</p>
Start Time/End Time	<p>Choosing only a beginning time displays alarms from that time through the end of the day (23:59:59 or 11:59:59 p.m.).</p> <p>Choosing only an ending time from the start of the day (00:00:00 or 12:00:00 a.m.) through the time selected.</p>

Filter option	Description: Display alarms for:
Cluster	This is a single cluster, which was added when setting up the project (listed in Project Editor > Servers > Clusters)
Area	Area (Between 0 and 255). See Alarm SOE fields in the Plant SCADA help file (... \Program Files (x86) \Schneider Electric \Power Operation \v2021 \bin \Help \SCADA Help).
Classification	The class of the event. See Alarm SOE fields in the Plant SCADA help file (... \Program Files (x86) \Schneider Electric \Power Operation \v2021 \bin \Help \SCADA Help).
Operator	The user ID of the person who has logged on Power Operation.
Message	This comes from the Message field in the Alarm Log.
Custom Filter	There are eight custom filters, which can be assigned by the customer in each alarm. A group of alarms in a specific location could have the same name in CUSTOM8 so that custom filtering can be easily applied. Custom8 has a default assignment of "Equipment." To change custom filter assignments, use the AlarmFormat parameter (Project Editor > System > Parameters). This is the only means available for filtering on a custom field. When viewing the log, you can use the new custom filter by typing it into the Custom Filter field.

Using Cybersecurity Admin Expert (CAE) for cybersecurity

Cybersecurity Admin Expert (CAE) is a software tool used to configure and apply security settings to a device in a network of industrial control systems. Devices can include switches, firewalls, PCs, and IED/Protection relays.

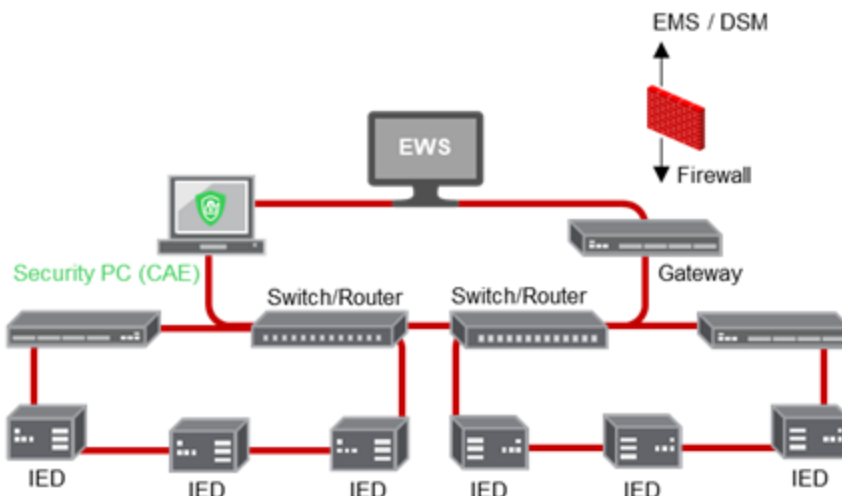
Devices must be CTI023 compliant or have a Digital Power CS brick, a cybersecurity brick embedded inside that enables it to communicate with CAE.

Using CAE with EcoStruxurePower Operation is optional. See [Installing CAE](#) for information about installing the tool.

CAE has security capabilities that help:

- Protect the confidentiality of information.
- Align with NERC CIP reliability standards and IEC 62443 international standards.
- Protect the device from unauthorized configuration security changes.
- Enforce authorizations assigned to users, segregation of duties, and least privilege.
- Prohibit and restrict the use of unnecessary functions, ports, protocols, and/or services.

CAE Architecture



Encryption

CAE manages the encryption of data exchanged through some of the communication channels. CAE helps protect configuration and process data from any corruption, malice, or attack.

Hardening

Recommendations to optimize cybersecurity in a protected environment:

- Harden devices according to your company's policies and standards.
- Apply and maintain the CAE security capabilities.
- Use an antivirus software and implement updates for the operating system and Microsoft .NET Framework on the machine dedicated to CAE tool.
- Follow user account management tasks as described by your organization or contact your network administrator.

WARNING

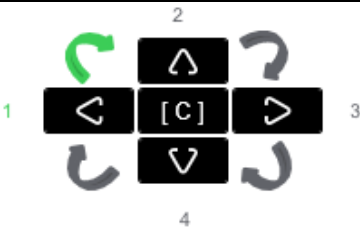
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords to help prevent unauthorized access to settings and information.
- Use Windows Active Directory for user account management and access to network resources.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.
- Follow cybersecurity tasks as described by your organization or contact your network administrator.

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

Default CAE security settings

Area	Setting	Default
------	---------	---------

User accounts	Security administrator username and password (access to CAE)	Username: SecurityAdmin Password: AAAAAAAA
	Security auditor username and password (access to CAE)	Username: DefaultSecAud Password: AAAAAAAA
	Default arrow password for all default user accounts	 <p>Enter this password twice, starting from the left arrow and go clockwise:</p> <ol style="list-style-type: none"> 1. Left 2. Up 3. Right 4. Down
	Preconfigured user accounts (no access to CAE)	DefaultEngineer, DefaultInstaller, DefaultOperator DefaultRbacMnt, DefaultSecAud, DefaultViewer, SecurityAdmin
Models	Models	Disabled
Security Settings > User Accounts	Minimum activity period (min)	15 mins.
	Password complexity	None
	Number of previous passwords which cannot be reused	3
	Activate 'Local Default Access'	Yes. VIEWER by default.
	Allow user account locking	15 mins.
	Maximum login attempts	Yes
	Password attempts timer (min.)	5
	Automatic user account locking	Enabled
Logs	Log and monitoring standard	BDEW
	Server port	601
	SYSLOG parameters server port	601
Security Banners	Banner on device front panel displays	None

Authentication Configuration	Authentication mode	Local
	Default role for centralized authentication	Viewer
	Centralized authentication timeout duration (s)	5 seconds
	Centralized authentication protocol	None

Configuring CAE cybersecurity

Cybersecurity Admin Expert can be configured online or offline. CAE must be online to send and apply configuration to devices and view user accounts and devices in the network in real-time view.

Only user accounts assigned SECADM or SECAUD roles can access CAE. By default, the security administrator (SecurityAdmin) and Default Security Auditor (DefaultSecAud) user accounts have access.

See [Installing CAE](#) for information about installation, system requirements, and licensing.

Configuration checklist:

- **Record activities:** Document actions according to your company's policies and standards to keep a record of activities, usernames, and passwords.
- **Open Cybersecurity Admin Expert:** Use the default security administrator (SecurityAdmin) username and password for first login. CAE automatically forces the default password to be changed. See [Managing CAE passwords](#), for information about default passwords and user accounts.
- **[Add devices and certificates:](#)**
 - Devices using Device Profiles for Web Services (DPWS) communications protocol are automatically discovered.
 - Add devices manually when they do not use UDP (User Datagram Protocol) communications or when substation network firewalls and routers do not allow UDP.
 - Device certificates must be added and accepted to the CAE Certificate Whitelist.
- **[Define Authentication Configuration security settings](#)**
- **Add projects, user accounts, roles, and models:**
 - See [Working with CAE projects](#), for information about default passwords and user accounts.
 - See [Managing CAE user accounts](#), for information about default passwords and user accounts.
 - See [Managing CAE user roles](#), for information about default passwords and user accounts.
 - See [Managing CAE models](#), for information about default passwords and user accounts.
- **["Adding Security Banners to device displays \(optional\)" on page 63](#)** (optional)
- **["Importing a PFX key container file from a device" on page 64](#)** (optional)

- ["Sending and applying configuration to a device" on page 63](#)
- ["Viewing Configuration History" on page 65](#)

Required for these procedures:

- Security administrator (SecurityAdmin) log-in credentials.

Adding devices and certificates


Device certificates must use encrypted communication between devices in system networks.

Use this procedure to add devices and certificates one at a time.

To add multiple devices at a time, import a CSV file containing a list of devices from the SYSTEM EDITOR tab. The spreadsheet must contain one device per row, with the following information in cells: device name, device type as known by the system, firmware version, IP address, Ethernet port number for getting metadata (if blank, default is 9867).


1. Open Cybersecurity Admin Expert.
2. Select **SYSTEM EDITOR** tab > **Add Device** button. The Add a new device dialog opens.
3. Enter values for the device and click **Save**:







NOTE: Right-click on a device to edit or delete it.

4. **MANAGEMENT OF SYSTEM** tab > click refresh icon . The New certificate(s) detected window opens if new device certificates are detected.
5. Verify device certificates are valid > select certificates > click **Accept**.

NOTE: You can also add a certificate in the SECURITY SETTINGS tab.

6. Click **Yes** to accept addition to CAE Certificate Whitelist.
7. Click **OK** to push certificates to CAE Certificate Whitelist.
8. Confirm that all devices and certificates have been successfully discovered or found if added manually:

Indicator	Description	Action
Status 	Device successfully discovered.	None

Status 	Device has been discovered, but its information is different from the local device discovered.	Go to System Editor and re-enter the correct device information.
Status 	Device discovered in the network, but not declared in System Editor.	Go to System Editor to add the device manually.
Status 	Device has not been discovered over the network, but was added in System Editor.	Review device IP Address and port. Ensure device is on. Restart may be required.
Security version – Connection denied	Device password refused or device user account is locked out.	Right-click on device and select Log on. Enter specific device password or common password.
Name 	Device certificate is in the CAE whitelist.	None
Name 	Device certificate is not in the CAE whitelist.	Right-click on a device to get, send, or remove certificate.
Name 	No certificate information found for device.	Click the Refresh icon and accept certificate.

- Click **Send Security Configuration**. CAE stores accepted certificates in CAE Whitelist and displays them in Security Settings tab.

You can get, send, or remove certificates by right-clicking on a device in the MANAGEMENT OF SYSTEM tab.

You can edit, delete, or export accepted certificates by right-clicking on a device under Certificate Whitelist in the SECURITY SETTINGS tab.

Defining Authentication Configuration security settings

Authentication is the mechanism used to verify the identity of users. Use Authentication Configuration in CAE to define the authentication mode, for example, local or local then centralized, and other authentication security settings.

- Open Cybersecurity Admin Expert.
- Select **SECURITY SETTINGS** tab > **Authentication Configuration**.
- Select the options you want.

Radius server authentication protocol options:

Radius Details	Description
Mode	RADIUS client mode of connection.
IP address	The IP address of the RADIUS Server.
Port	Port number used by RADIUS Server for communication with the Radius client.
Shared secret	Text string password between the RADIUS client and the RADIUS server.
Backup server IP address	IP address of second RADIUS Server (optional).

Backup server port	Port number used by second RADIUS Server for communication with the Radius client.
Backup server shared secret	Text string password between the RADIUS client and the RADIUS server.
Role attribute name	Attribute name in the Radius protocol accepted answer where the role assignment is stored.
AoR attribute name	Attribute name in the Radius protocol accepted answer where the AoR assignment is stored.
Date attribute name	Attribute name in the Radius protocol accepted answer where the date assignment is stored.
Attribute separator	Character that splits the attributes if several attributes returned.
Dictionary	String storing contents of RADIUS dictionary.
Parsing debug	Enable or disable parsing debug.

LDAP client-server protocol authentication protocol options:

LDAP Details	Description
Domain	Domain name of the LDAP server, e.g. DC=MyDomain, DC=com.
IP address	IP address of the LDAP server.
Port	Port number used by LDAP server for communication with the LDAP client.
Group(s)	Name of LDAP Group(s).

4. Click **Save**.

Adding Security Banners to device displays (optional)

1. Open Cybersecurity Admin Expert.
2. Select **SECURITY SETTINGS** tab > **Security Banners**.
3. Enter text for security banners.
4. Click **Save**.

Sending and applying configuration to a device

Use this procedure to send and apply security configuration settings from CAE to a device.

At the end of this procedure, CAE will:

- Create four XML files and sends them to each device: user account file, role file, user file, and a security policy settings file. Sometimes, a Device Specific Settings file is created and sent.
 - Create a devices report CSV file.
 - Display the newest security configuration version number and name for Devices in the MANAGEMENT OF SYSTEM tab.
1. Open Cybersecurity Admin Expert.
 2. Select **MANAGEMENT OF SYSTEM** tab.

3. Click the **Send security Configuration** button. The Push Security Configuration dialog box opens.
4. Click **Yes**.
5. Enter a name for the new version.
6. Click **Save**. The Push configuration status dialog box opens.

Importing a PFX key container file from a device

A key container is a part of the key database that contains public and private keys belonging to a device. Use this procedure to create a new key container in CAE that encrypts and decrypts information.

Required for this procedure:

- P12 file stored in an accessible location.
- Password for P12 file.
- Device embeds CS brick 3.0 or upper.

1. Open Cybersecurity Admin Expert.
2. Select **MANAGEMENT OF SYSTEM** tab.
3. Right-click on a device > **Import a pfx**:

Status	Name	Type	Firmware	IP address	Security version	Version name	
	SecurityBrick_Simulator	C264	0.01	10.214.18.77 : 9867	1	Version 1	
	SecurityBrick_Simulator	EcoSUI	0.01	10.214.		Version 1	
	SecurityBrick_Simulator	C264	0.01	10.214.		Version 1	

Log on

Send DSS

View logs

Import a pfx

Get certificate

Send certificates

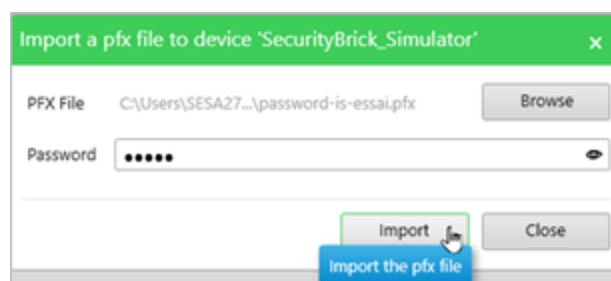
Remove certificates

Send security configuration

3 Device(s) Items per page 25 1

The Import a pfx file dialog box opens.


4. Click **Browse** to navigate to the PFX file you want to import.
5. Enter the PFX file password.
6. Click **Import**:



NOTE: PFX file is encrypted and password protected.

PFX file is imported inside the device.

Viewing Configuration History

1. Open Cybersecurity Admin Expert.
2. Select **MANAGEMENT OF SYSTEM**.
3. Click the **View History Configuration** icon  on the bottom right.

Working with CAE projects

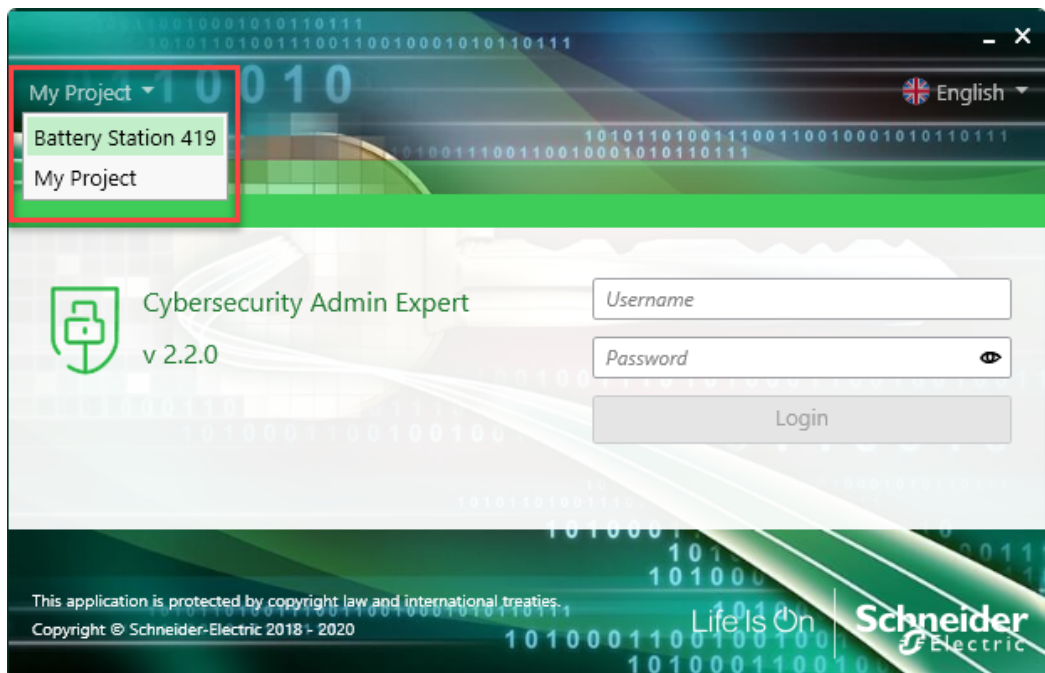
CAE projects are automatically stored in C:\ProgramData\Schneider Electric\CAE\Projects.

Recommendations:

- Document Project usernames and passwords according to your company's policies and standards.
- Follow user account management tasks as described by your organization or contact your network administrator.
- Store exported project XML files in a protected location. XML files are not encrypted.

Opening a Project

1. Open Cybersecurity Admin Expert.
2. Select the **Project** you want:



3. Log in.

You can also open a project when logged in to CAE by double-clicking the Project. You will be logged out and must log in again if project password is different.

Creating a Project

After creating a project, you will be logged out and must log in with the default SecurityAdmin username and password. Passwords can be different or the same for each Project.

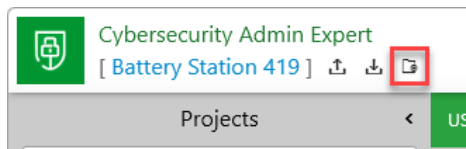
NOTICE

LOSS OF DATA

Record username and password information in a secure location.

Failure to follow these instructions can result in loss of data.

1. Open Cybersecurity Admin Expert.
2. Click the **Create** icon on the title bar:



3. Select the newly created project. The Project loading message box opens.
4. Click **OK**. CAE logs out of active project.
5. Enter username. Default is **SecurityAdmin**.
6. Enter password. Default is **AAAAAAAAA**.
7. Click **login**. The password dialog box opens.
8. Change default password.
9. Click **Save**. Cybersecurity Admin Expert opens.

Importing or exporting a Project

By default, import and export is only enabled for the security administrator (SECADM) role.

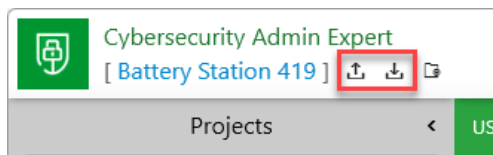
NOTICE

LOSS OF DATA

Record username and password information in a secure location.

Failure to follow these instructions can result in loss of data.

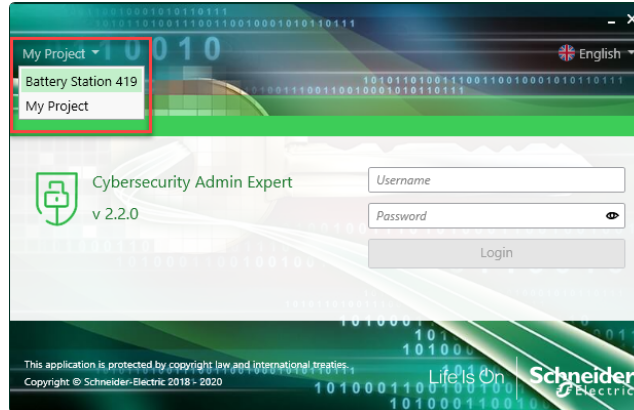
1. Open Cybersecurity Admin Expert.
2. Click the **Import** or **Export** icons on the title bar:



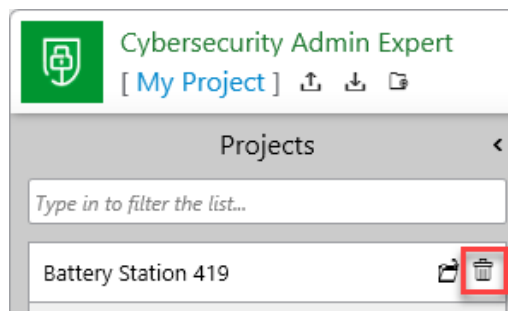
3. Browse to location of the project XML file.
4. Click **Import** or **Export > Close**.

Deleting a Project

1. Open Cybersecurity Admin Expert.
2. Select a different project than the one you want to delete:



3. Click the **Trash** icon beside the project you want to delete:



The Please confirm dialog box opens.

4. Click **Yes**.

Threat intelligence and CAE

Event logs can assist with monitoring suspicious activity and identifying the cause of cybersecurity breaches that could lead to a cybersecurity incident. See [Configuring CAE](#) for information on viewing configuration history.

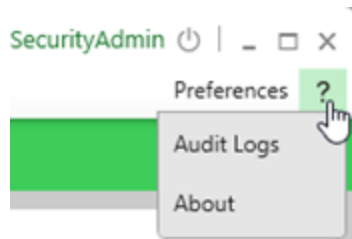
Setting up cybersecurity event logs

The event log can be used to monitor user logins and user account lockouts. Logs are based on Windows Event Viewer policies governed by your organization. Syslog server IP address, Syslog server IP port, and SNMP server IP address settings are not required for a standalone environment.

1. Open Cybersecurity Admin Expert.
2. Select **SECURITY SETTINGS > Logs**.
3. Enter details.
4. Click **Save**.

Viewing and exporting cybersecurity event logs

1. Open Cybersecurity Admin Expert.
2. Click the **Question Mark** icon on the title bar:



3. Select **Audit Logs**. The Audit Logs window opens.
4. Click **Export**.
5. Enter a file name.
6. Click **Save**.

Windows Updates

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Apply the latest updates and hotfixes to your Operating System and software.

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

Be sure that all Windows updates and hotfixes—especially Windows security updates—are regularly applied to machines running Power Operation and Power Monitoring Expert.

If compatibility issues arise from Windows updates, they are considered high priority by the Power Operation with Advanced Reporting and Dashboards development team. They will be evaluated and resolved to deliver patches to enable the continued use of Windows security updates.

User accounts and passwords

Use the information provided in this chapter to make changes to user accounts, user account privileges, passwords, and CAE models and roles. Using CAE with Power Operation is optional.

Recommendations:

- Assign users only the essential privileges needed to perform their role.
- Revoke user privileges when no longer needed due to role change, transfer or termination. User credentials do not expire.
- Follow user account management tasks as described by your organization or contact your network administrator, for example, maximum password age or history policies.
- Use Windows Active Directory to perform periodic security and user account maintenance activities.

User account roles and privileges

- User accounts are assigned to roles that have variable permissions to read access or configuration privileges by default.
- Roles and privileges are created at the time of installation and stored in the project.
- User accounts, role names and mapping can be changed at any time after the project is set up.

When a project is restored from backup in Power Operation, so are all saved user accounts, roles, and mapping.

- Power Operation web application user account privileges are not the same as the roles and privileges in Plant SCADA, Windows, and Windows Active Directory.
- Active Directory Users are authenticated against Active Directory Windows Groups. Active Directory Windows Users added to local Windows Groups are not supported.
- For local Windows users, the local Windows groups are mapped to Power Operation user account privileges for Web Applications. See [Default user account roles and privileges for Power Operation web applications](#) and [Default Windows Groups privilege level mapping to Power Operation web applications](#).
- For Citect users, privilege levels are mapped to Power Operation web applications access levels. See [Default User account mapping between Citect and Power Operation web applications](#).

To optimize cybersecurity in a protected environment:

- Keep user accounts, roles and privileges up-to-date. See [Managing user accounts, roles, and mapping](#) for information about adding users and enforcing access.
- View security settings after making changes to ensure least privilege is applied. See [Viewing security settings](#) for details for viewing current settings.

Default user account roles and privileges for Power Operation web applications

Power Operation web applications	Power Operation roles and privileges					
	None = 0	Observer = 1	User = 2	Controller =3	Operator = 4	Administrator = 5
AlarmViewer.AcknowledgeAlarm				X	X	X
AlarmViewer.DeleteAny						X
AlarmViewer.EditAny						X
AlarmViewer.Owner				X	X	X
AlarmViewer.SetSystemDefaultItem						X
AlarmViewer.ViewIncidents			X	X	X	X
ApplicationAccess.AlarmViewer			X	X	X	X
ApplicationAccess.HmiApplication		X	X	X	X	X
ApplicationAccess.Event			X	X	X	X
ApplicationAccess.RealtimeData		X	X	X	X	X
ApplicationAccess.RealtimeTrend		X	X	X	X	X
ApplicationAccess.Tgml		X	X	X	X	X
ApplicationAccess.WebConfig		X	X	X	X	X
ConfigurationAccess.Alarms						X
ConfigurationAccess.CustomScripting						X
ConfigurationAccess.MyPreferences		X	X	X	X	X
ConfigurationAccess.Localization						X
ConfigurationAccess.Theme						X
ConfigurationAccess.Security						X
ConfigurationAccess.Tgml				X		X
Diagrams.Owner			X	X	X	X
Diagrams.EditAny						X
Diagrams.DeleteAny						X
Diagrams.SetSystemDefaultItem						X
Diagrams.ControlActions				X	X	X
RealtimeTrend.DeleteAny						X
RealtimeTrend.EditAny						X
RealtimeTrend.Owner				X	X	X
No Access	X					

Default Windows Groups privilege level mapping to Power Operation web applications

Adding local Windows Users to these groups will grant them the following mapped web applications privileges. For example, all local Windows Users added to the PSO_Controllers group will be granted the Web Application Controller = 3 access level. The values are a semicolon delimited list.

Power Operation web application roles	Windows Group Privilege Levels
None = 0	N/A
Observer = 1	<pre><ConfigurationItem Key="OsObservers" Category="Security" Application="CitectPlatform"> <Value>PSO_Observers</Value> </ConfigurationItem></pre>
User = 2	<pre><ConfigurationItem Key="OsUsers" Category="Security" Application="CitectPlatform"> <Value>PSO_Users</Value> </ConfigurationItem></pre>
Controller = 3	<pre><ConfigurationItem Key="OsControllers" Category="Security" Application="CitectPlatform"> <Value>PSO_Controllers</Value> </ConfigurationItem></pre>
Operator = 4	<pre><ConfigurationItem Key="OsOperators" Category="Security" Application="CitectPlatform"> <Value>PSO_Operators</Value> </ConfigurationItem></pre>
Administrator = 5	<pre><ConfigurationItem Key="OsAdministrators" Category="Security" Application="CitectPlatform"> <Value>PSO_Administrators</Value> </ConfigurationItem></pre>

Default User account mapping between Citect and Power Operation web applications

Citect user account privileges map to Power Operation web applications roles and privileges. For example, a Citect privilege level 3 (Priv3) maps to access level 3, which is a Controller.

Power Operation web application roles	Plant SCADA privilege level	Configuration file default
None = 0	Priv0	<ul style="list-style-type: none"> <pre><ConfigurationItem Key="Priv0" Category="Security" Application="CitectPlatform"> <Value>0</Value> </ConfigurationItem></pre>

Power Operation web application roles	Plant SCADA privilege level	Configuration file default
Observer = 1	Priv1	<ul style="list-style-type: none"> • <code><ConfigurationItem Key="Priv1" Category="Security" Application="CitectPlatform"> <Value>1</Value> </ConfigurationItem></code>
User = 2	Priv2	<ul style="list-style-type: none"> • <code><ConfigurationItem Key="Priv2" Category="Security" Application="CitectPlatform"> <Value>2</Value> </ConfigurationItem></code>
Controller = 3	Priv3	<ul style="list-style-type: none"> • <code><ConfigurationItem Key="Priv3" Category="Security" Application="CitectPlatform"> <Value>3</Value> </ConfigurationItem></code>
	Priv4	<ul style="list-style-type: none"> • <code><ConfigurationItem Key="Priv4" Category="Security" Application="CitectPlatform"> <Value>3</Value> </ConfigurationItem></code>
Operator = 4	Priv5	<ul style="list-style-type: none"> • <code></ConfigurationItem> <ConfigurationItem Key="Priv5" Category="Security" Application="CitectPlatform"> <Value>4</Value></code>
	Priv6	<ul style="list-style-type: none"> • <code></ConfigurationItem> <ConfigurationItem Key="Priv6" Category="Security" Application="CitectPlatform"> <Value>4</Value> </ConfigurationItem></code>
Administrator = 5	Priv7	<ul style="list-style-type: none"> • <code><ConfigurationItem Key="Priv7" Category="Security" Application="CitectPlatform"> <Value>5</Value> </ConfigurationItem></code>
	Priv8	<ul style="list-style-type: none"> • <code><ConfigurationItem Key="Priv8" Category="Security" Application="CitectPlatform"> <Value>5</Value> </ConfigurationItem></code>

Managing user accounts, role names, and mapping

User account privileges can be modified and users can be added or removed at any time.

- Use Windows Authentication to create user accounts.
- Add at least one user to any project before you can run and view it. Each user must have a role and a user account.
- Document user account actions according to your company's policies and standards to keep a record of activities.

You can use single sign-on (SSO) to associate passwords for different products, such as Power Operation Studio and the Advanced Reporting and Dashboards Module. Single sign-on allows the project user, when logged in to the Power Operation Runtime, to access external applications, such as dashboards. See [Configure Single Sign-On \(SSO\)](#) for more information.

If your system includes Advanced Reporting and Dashboards Module, you can use single sign-on (SSO) to associate a Citect user with a Power Operation username/password or a Power Monitoring Expert username/password. See ["Using single sign-on and passwords" on page 75](#) for details.

For safety reasons, only advanced users should be given access to such features as controls and resets. User account privileges are defined in **Security > Roles**, located in the Power Operation Studio.

WARNING



POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices when configuring user access.

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

Change role names and mapping

Change role names and numbers to associate them to a role.

1. In Power Operation Studio: Click **Projects**  > choose a project.
2. Click **Security**  > **Roles**.
3. Change role information. For default privileges, see [User account roles and privileges](#).
4. Click **Save**.

WARNING



UNINTENDED EQUIPMENT OPERATION

- Do not use the software or devices for critical control or protection applications where human or equipment safety relies on the operation of the control action.
- Do not use the software to control time-critical functions.
- Do not use the software to control remote equipment without proper access control and status feedback.

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

Extensively test the deployed project to ensure that permissions are applied as intended because Power Operation lets you set user permissions on runtime graphical objects.

Add or change user accounts

1. In Power Operation Studio: Click **Projects**  > choose a project.
2. Click **Security**  > **Users**.
3. Add or change user information. For default privileges, see [User account roles and privileges](#).
4. Click **Save**.

Change Power Operation and Plant SCADA user roles, privileges, and mapping

Use the Schneider Electric Core Services configuration file `configuration.xml` to map Windows Groups and Citect privilege levels. The default installation path is: `C:\Program Files (x86)\Schneider Electric\Power Operation\v2021\Applications\AppServices\bin\`.

For example, to make Citect Priv3 equal Power Operation User, change the Value element for Priv3 to 2: `<ConfigurationItem Key="Priv3" Category="Security" Application="CitectPlatform"><Value>2</Value></ConfigurationItem>`.

For OsXXXX keys, the value is a semi-colon delimited list of Windows User Groups assigned for this access level.

See [User account roles and privileges](#) for details on default mapping.

Use Windows Integrated Users

You can incorporate Power Operation users and security options with the standard Windows security system. Using the integrated Windows security feature, the Windows user can log on to Power Operation runtime with runtime privileges and areas configured within the project. For a Windows user to be able to log on to runtime, it must be linked to a Power Operation "role," which is defined in the project with associated privileges.

To link a Windows user to a Power Operation role:

- Add the "role" that specifies the Windows security group of which the Windows user is a member.

The pre-existing AutoLogin capability is extended to include the client, when the user is a Windows user, having an associated Power Operation role.

To invoke this functionality for a Windows user:

- Set the `[Client]AutoLoginMode` parameter in the `Citect.ini` file.

Instead of using auto-login when the system starts up, users can also log in to Power Operation using any Windows user credential that is a member of the linked group.

When the name of a Power Operation user has the same name as a Windows user, the Power Operation user takes priority at runtime. However, if a valid Power Operation user login is unsuccessful, the Windows user credentials will not be checked and an alert will be generated to advise that the login was not effective.

Managing user account lockouts and timeouts

Use Active Directory and Windows authentication to manage user account lockouts and timeouts.

Passwords

Use the information provided in this chapter make changes to user account passwords.

Recommendations:

- Use complex passwords or passphrases.
- Document and store passwords and usernames in a protected location.
- Use Active Directory and Windows authentication for password management.
- Follow user account management tasks as described by your organization or contact your network administrator, for example, maximum password age or history policies.

Using single sign-on and passwords

With single sign-on (SSO), you associate a Citect user with a Power Operation username and password or a Power Monitoring Expert username and password. This allows the Citect user to access external applications, such as Dashboards, using an SSO user password from Power Monitoring Expert.

NOTE: SSO only works with Client Access.

Two-factor authentication

Two-factor authentication requires users to provide two pieces of proof of identity, such as a password and one other component. This feature allows you to add an additional layer of protection when user credentials are required; such as at log in, shutdown and control functions.

NOTE: For cybersecurity purposes, it is strongly recommended that you configure two-factor authentication in your projects; especially in deployments with control functionality.

Power Operation uses a one-time password (OTP) to accomplish two-factor authentication. OTP is implemented in Power Operation using a USB key device called a YubiKey. The YubiKey is designed to fit on a key ring or attached to a badge. It must be plugged into the client machine when the user authenticates.

Power Operation supports two-factor authentication on isolated networks; the Internet is not required. Additionally, it will work with physical machines, virtual machines, and Power SCADA Anywhere.

How does it work?

When a YubiKey is assigned to a Power Operation user, the YubiKey and the assigned user account share a secret code. The YubiKey uses this secret code to generate encrypted strings of text (the OTPs) when the user presses the button on the YubiKey.

Using the secret code, Power Operation decrypts the OTP to determine if the OTP is valid (ensuring that it has not been replayed, it is assigned to the current user, etc.). After successful authentication, Power Operation marks the OTP as expired and will no longer accept it as valid.

YubiKey selection

YubiKeys are not shipped with Power Operation.

YubiKey 5 and FIPS models are compatible and supported with Power Operation thick control clients.

NOTE: YubiKey NOT supported with new PO 2021 HTML5 web client.

YubiKey models validated with “FIPS-compliant” enabled on Windows Server.

Supported YubiKey models compatible with Power Operation:

Model Number	Comments
YubiKey 5	NFC model not supported .
YubiKey 5 C FIPS	Meets AAL3 of NIST SP800-63B guidelines.

See <https://www.yubico.com> for more information.

Using CAE for user accounts and passwords

Using CAE with EcoStruxure Power Operation is optional.

You can use CAE to manage user accounts, passwords, user account lockouts and timeouts, models, and user roles.

See [Installing CAE](#) for information about installing the tool.

Managing CAE user accounts

User privileges can be modified. Users can be added or removed at any time.

Using CAE with EcoStruxure Power Operation is optional.

Recommendations:

- Align usernames and passwords with the limitations of system devices.
- Document and store passwords and usernames in a protected location.
- Assign users only the essential privileges needed to perform their role.
- Revoke user privileges when no longer needed due to role change, transfer, or termination. User credentials do not expire.
- Have two SecurityAdmin user accounts to reduce the risk of losing security administrator password and access.
- Follow user account management tasks as described by your organization or contact your network administrator.

User account security capabilities include:

- User account lockout criteria after unsuccessful login attempts.
- User account timeouts after session inactivity.

Adding a user account

NOTICE

LOSS OF DATA

Record username and password information in a secure location.

Failure to follow these instructions can result in loss of data.

1. Open Cybersecurity Admin Expert.
2. Select **USER ACCOUNTS** tab > **Add user account** button. The Add new User Account dialog box opens.
3. Enter details. Non-alphanumeric characters and spaces are not allowed in names.
4. Click **Save**.

Disabling, editing, or deleting a user account

SecurityAdmin user account can not be deleted.

NOTICE

LOSS OF DATA

Record username and password information in a secure location.

Failure to follow these instructions can result in loss of data.

1. Open Cybersecurity Admin Expert.
2. Select **User Accounts** tab > **User Accounts**:
 - Enable or disable user account: click **Enable** or **Disable** button.
 - Edit user account details: select a user account in the Selection pane, edit details.
 - Delete user account: select a user account in the Selection pane, click **Enable**. If deleting a user account, send and apply configuration to the device. See [Configuring CAE cyber-security](#) for information on sending and applying configuration to a device.

Managing user account lockouts and timeouts

Use Active Directory and Windows authentication to manage user account lockouts and timeouts.

Managing CAE passwords

Recommendations:

- Align usernames and passwords with the limitations of system devices.
- Use complex passwords or passphrases.
- Document and store passwords and usernames in a protected location.
- Have two security administrator (SecurityAdmin) user accounts to reduce the risk of losing security administrator password and access.

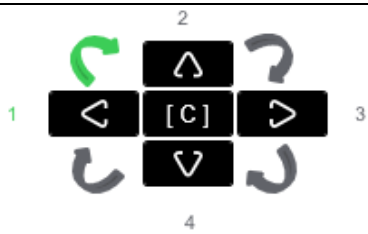
- Do not allow password history to contain a character repeated consecutively more than twice.
- Follow user account management tasks as described by your organization or contact your network administrator.

Password security capabilities include:

- Passwords can be different or the same for each Project.
- Password complexity configuration.
- Password history to limit the reuse of passwords.
- Default password change forced after first successful login of SECADM default user account.

Default passwords and usernames

Text passwords are mandatory. Arrow passwords are optional and are used to access a device through a display

Default User Account	Default Text Password	Default Arrow Password
SecurityAdmin	AAAAAAA	 <p>Enter this password twice, starting from the left arrow and move clockwise:</p> <ol style="list-style-type: none"> 1. Left 2. Up 3. Right 4. Down
DefaultEngineer		
DefaultInstaller		
DefaultOperator		
DefaultRbacMnt		
DefaultSecAud		
DefaultViewer		

Lost password

If user access information is lost, you will have to reinstall Cybersecurity Admin Expert. Data will be overwritten and devices will have to be reset to factory settings.

Password recommendations

- Username login should be different than e-mail address, first name, and last name.
- 8 character maximum for arrow password (required).
- 8 character minimum.
- 1 uppercase letter minimum.
- 1 lowercase letter minimum.
- 1 number minimum.
- 1 special character minimum.

Changing a password

NOTICE

LOSS OF DATA

Record username and password information in a secure location.

Failure to follow these instructions can result in loss of data.

1. Open Cybersecurity Admin Expert.
2. Select **SECURITY SETTINGS** tab > **User Accounts**.
3. Edit details.
4. Click **Save changes**.

Changing password complexity

1. Open Cybersecurity Admin Expert.
2. Select **SECURITY SETTINGS** tab > **User Accounts** > **Password complexity** drop-down list:

Password Complexity Option	Description
None	Default password requirements.
IEEESTd1686	8 character minimum, 1 uppercase letter minimum, 1 lowercase letter minimum, 1 number minimum, and 1 special character minimum.
NERC CIP	8 character minimum, including 3 character minimum of any: uppercase letter, lowercase letter, number, or special character.

3. Click **Save changes**.

Limiting the reuse of passwords

1. Open Cybersecurity Admin Expert.
2. Select **SECURITY SETTINGS** tab > **User Accounts** > **Number of previous passwords which cannot be reused**.
3. Click **Save changes**.

Managing CAE user account lockouts and timeouts

Lockout and timeout settings can be applied to all roles or customized for individual roles. Account locking can not be disabled for critical power or plant automation systems.

User account lockouts and timeouts capabilities include:

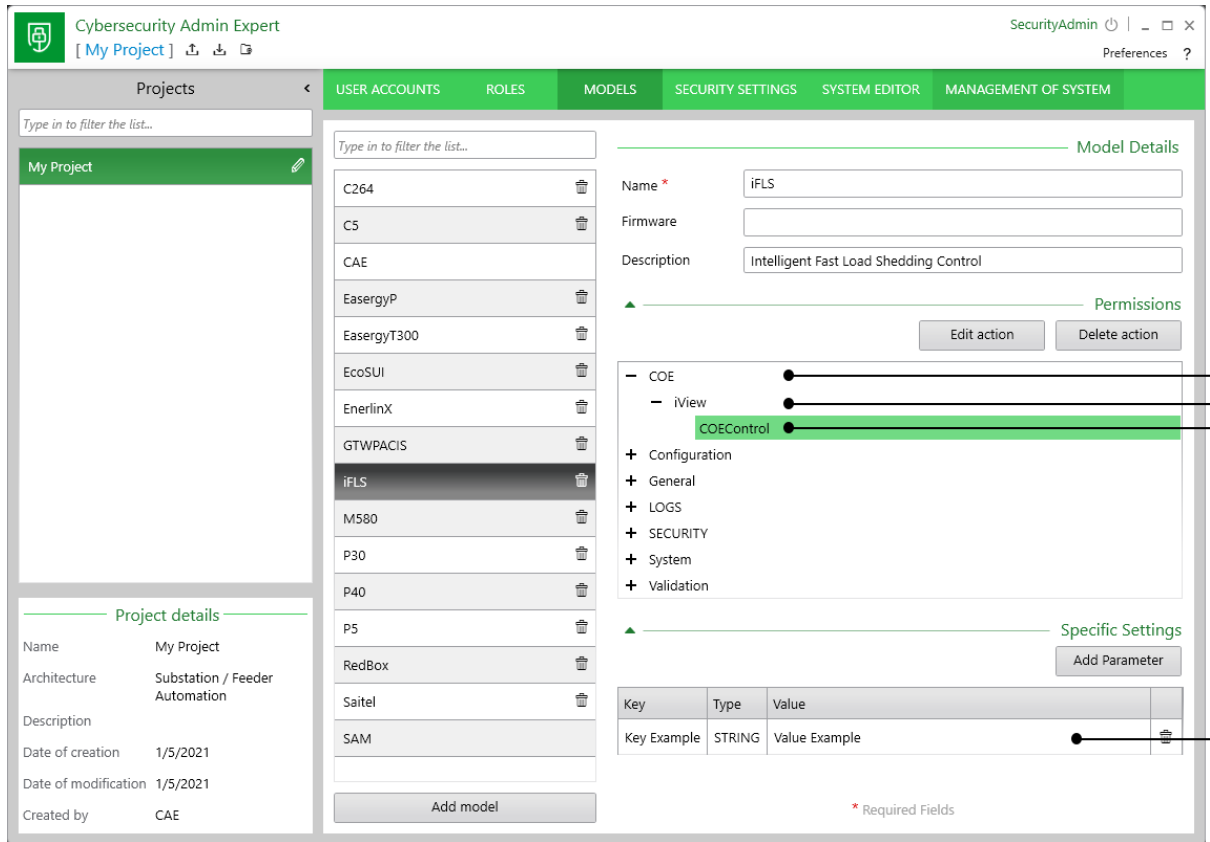
- Lockout after unsuccessful login attempts.
 - Lockout duration.
 - Session inactivity timeout.
1. Open Cybersecurity Admin Expert.
 2. Select **SECURITY SETTINGS** tab > **User Accounts** and the security options you want:
 - Minimum inactivity period (min) – set session inactivity timeout.
 - Allow user account locking: enable or disable account lockouts.
 - Maximum login attempts: set number of incorrect login attempts before lockout.
 - Password attempts timer (min): length of time user must wait after lockout.
 - Automatic user account unlocking: enable or disable unlocking of user accounts after defined lockout duration length.
 - User account lockout duration: define lockout duration length.
 3. Click **Save**.

Managing CAE models

A model is a representation of a program or device in the control system and its objects, such as a tool, utility, or an application function block. Set-up models in CAE to assign them to roles.

A model includes security capabilities to create:

- Permissions for components in a model.
- Objects for the permissions.
- Actions for each permission.
- Parameters for Device Specific Settings (DSS) (optional).



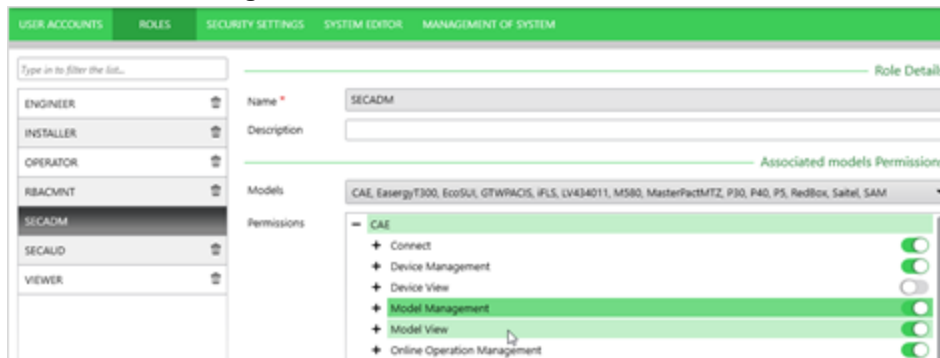
Recommendations:

- Assign roles only the essential privileges needed to perform their job.
- Follow user account management tasks as described by your organization or contact your network administrator.

Showing MODELS tab

The MODELS tab is hidden by default and can be enabled using a security administrator (SecurityAdmin) user account.

1. Open Cybersecurity Admin Expert.
2. Select **ROLES** tab > **SECADM** role.
3. Expand **CAE** item in the **Permissions** area.
4. Enable **Model Management** and **Model View**:



5. Click **Save changes**. The MODELS tab is added.

Adding, editing, or deleting a model

Default models are predefined and cannot be edited.

1. Open Cybersecurity Admin Expert.
2. Select **MODELS** tab:
 - Add model: click **Add model** button, edit details.
 - Edit model: select a model and edit details.
 - Delete model: select a model and click the **Trash icon**. SAM model can not be deleted.
3. Click **Save changes**.

Adding or editing model Permissions, Objects, Actions, or Parameters

1. Open Cybersecurity Admin Expert.
2. Select **MODELS** tab > select a model:
 - Add or edit Permissions: click **Add permission** or select a permission and click **Edit permission**.
 - Add or edit Object: select a permission and click **Add object** or select an object and click **Edit object**.
 - Add or edit Action: select an object and click **Add action** or select an action and click **Edit action**.
 - Add Parameter for DSS: scroll down and click **Add Parameter**. You can set specific security parameters by model, such as disabling a USB port or WI-FI access.

Managing CAE user roles

Use this procedure to define permissions for system components. Model permissions for roles are deactivated by default for newly added roles.

Recommendations:

- Assign roles only the essential privileges needed to perform their job.
 - Follow user account management tasks as described by your organization or contact your network administrator.
1. Open Cybersecurity Admin Expert.
 2. Select **ROLES** tab:
 - Add a new role: click the **Add role** button, edit details.
 - Edit role: select role and edit details.
 - Delete role: select a role and click the **Trash icon**. The SECADM role can not be deleted.
 3. Click **Save changes**.

You can disable the ability to connect to a device through its front panel using the security administrator (SecurityAdmin) user account. This is available in the in the SECURITY SETTINGS tab for Substation and Feeder Automation architectures

Schneider Electric

35 rue Joseph Monier
92500 Rueil Malmaison – France
www.se.com

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

©2021 Schneider Electric. All Rights Reserved.

7EN02-0465-00 07/2021