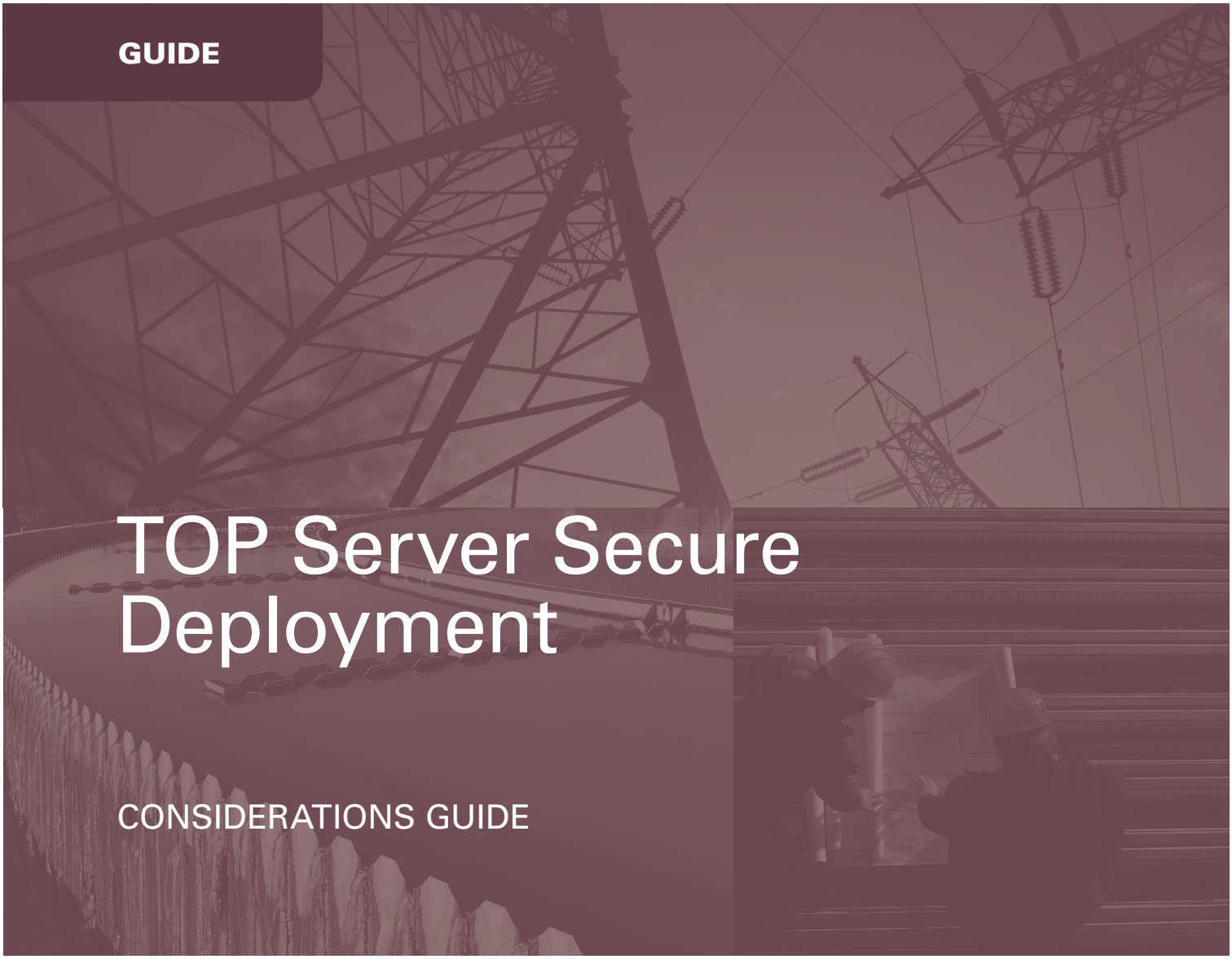
GUIDE



TOP Server Secure Deployment

CONSIDERATIONS GUIDE

Our mission is to provide you with the right software package to solve your industrial operation challenges.

Software toolbox®

Table of Contents

1. Introduction

TOP Server enables communication for industrial automation and the industrial IoT. It is often used in production systems in discrete, process, and batch manufacturing; oil and gas production and distribution; building automation; energy production and distribution; and more. Safety and uptime are key components of these systems, but cybersecurity threats are increasing in both frequency and complexity.

It is therefore paramount that when utilizing the software in a production environment, users of TOP Server deploy the application as securely as possible within the context of their application requirements, corporate IT guidelines, other internal company guidelines, or regulatory requirements.

This document provides best practices that existing and new users should consider if their business needs require deploying TOP Server with maximum security. When your needs dictate a maximum-security installation, it is recommended that administrators follow this guide as closely as possible when deploying TOP Server in a production environment. It is up to the user, their IT administration, or other responsible parties for your system to decide what parts of this guide to implement.

Users with active support & maintenance agreements may contact us with questions. Hands-on assistance with implementation of the suggestions in this guide are not included in the scope of product support but we can recommend a qualified system integrator or provide a quotation for consulting services if the scope is appropriate for our professional consulting services. Contact us if you need to discuss services or want an integrator recommendation.

2. Network Environment and System Configuration

Network security and Industrial Control System (ICS) network security is a highly complex subject. There is a set of industry best practices emerging that include network segmentation, use of DMZs, traffic evaluation, maintaining up-to-date physical and logical inventories, advanced algorithms for anomaly and intrusion detection, and constant reexamination of the network from a security standpoint. However, best practices are changing constantly, and implementation will vary based on the specific use cases (e.g. operations network, satellite or cell network, or local network on a machine).

The identification and implementation of network and ICS network best practices are beyond the scope of this document. Users should develop and maintain in-house expertise to help secure the ICS networks or work with a systems integrator with the requisite expertise. Users may also find it valuable to consult the organizations and resources listed below when developing a security strategy for the ICS networks.

TOP Server can be used to connect many thousands of different industrial automation devices and systems. As such, secure device and overall system configuration is beyond the scope of this document. Follow relevant vendor, internal, or industry best practices when deploying and connecting any and all devices. These include, but are not limited to, proper authentication of connections whenever available. As with ICS network security, it is recommended that users

develop internal expertise in this area or work with a qualified system integrator with knowledge of the specific devices in the environment.

Resources on ICS Network Security

- United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/cybersecurity)
- National Institute of Standards and Technology (https://www.nist.gov/)
    - National Institute of Standards and Technology's Guide to Industrial Control System Security (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)
- North American Electric Reliability Corp. Critical Infrastructure Protection Standards (https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx)

System Integrators

Contact Software Toolbox for recommended system integrators in your area.

3. Host Operating System

TOP Server should always be deployed in the most secure environment possible. Ensure the host operating system (OS) is secure from the outset and take all feasible measures to maintain the security of the OS for the life of the system. TOP Server should be deployed in an environment that utilizes the principles of "defense in depth" as opposed to one that utilizes a perimeter-oriented security philosophy. Specific aspects of a secure OS include, but are not limited to, system security, user management, firewall settings, and file management.

System

- Ensure appropriate access control measures in place to limit physical access to the target hardware to appropriate users.
- Always deploy TOP Server on an actively supported version of Windows and install Windows security patches in accordance with ICS security best practices.
    - As outlined by the ICS-CERT, **"**Organizations should develop a systematic patch and vulnerability management approach for ICS and ensure that it reduces the exposure to system vulnerabilities while ensuring ongoing ICS operations**".**
- Encrypt the hard drive of the host machine to secure all data at rest; however, recognize that encryption can affect performance of the operating system and all applications; and always consult your IT team before encrypting a drive, as they will likely have their own best practices.
- Regularly scan the host system using respected anti-malware software with up-to-date signature files.
- Turn off any unused services on the host machine.

- Optional: Running TOP server on its own machine or virtual. The more software you have on a machine, the more potential attack vectors you provide. In ICS it's commonplace to have OPC Servers and HMI software on the same machine. Just understand that in doing this, you need to consider the security of that machine as a whole and make sure you keep all the software up-to-date and follow other security best practices discussed in this guide.
- If you are using OPC DA as your primary means of connectivity to TOP Server, and you plan for off-machine communications, we highly recommend you consider a tunneling solution such as Cogent DataHub to provide higher security.

User Management

- Create a Windows user separate from the Administrator account to configure and manage TOP Server.
- Manage the OS Administrator account according to Windows best practices.
- User passwords must adhere to a formal password policy appropriate to the specific domain.
- Do not share logins or passwords across multiple users.
- Store passwords securely.
- Periodically review the access control model to ensure permissions are set using the principle of least privilege (i.e. permissions are granted only to users who need to perform required functions and are revoked when no longer necessary).

Perimeter

- Utilize a firewall to minimize external footprint and review firewall settings periodically.
- Utilize an intrusion detection system (IDS).
- Monitor remote access to the host operating system and log the activities.

Production Files

- For drivers and plug-ins that support saving files, such as the EFM Exporter Plug-in, Data-Logger and others, if you have the option to specify an UNC pathname for a destination, ensure the path is a trusted and secure location.

Non-Production Files

- Regularly remove any backup files from the production system.
- Regularly remove any sample or test files or scripts from the production system.

4. Installation

Users should validate the TOP Server install and only install the features required for the specific application. Set a strong administrator password during install.

Validation

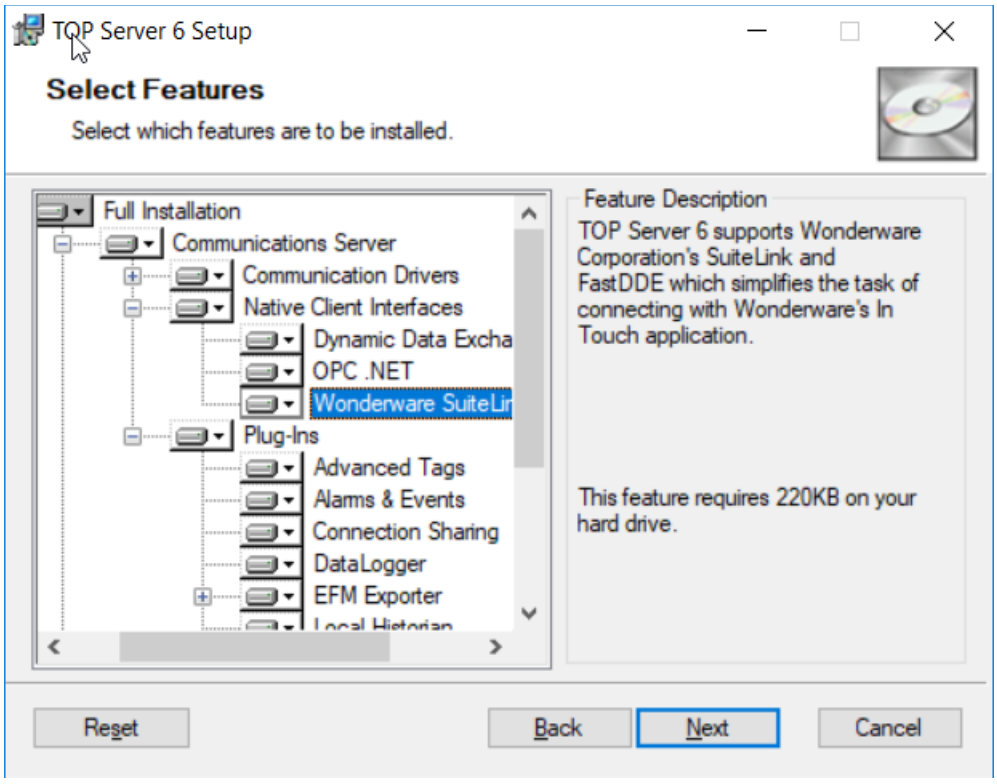
Software Toolbox maintains unique identification codes for officially released software.

Customers should verify against these codes to ensure that only certified executables are installed. Follow our instructions to validate the software downloads.

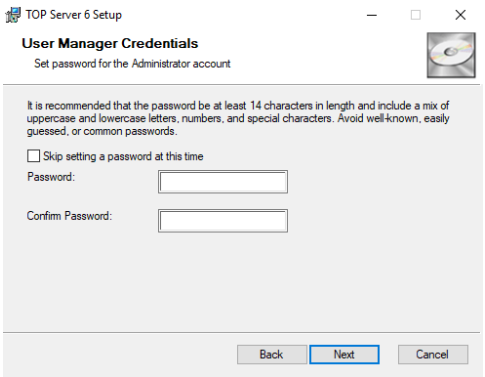
Installation

When presented with the Select Features dialog during the installation, install only the features required for the given production environment. Specifically, only install your required drivers, plug-ins, and native client interfaces that you will be using. For Wonderware users, if you need Suitelink install it, if not then don't install it.

If you aren't using the hardware key don't install the driver for it. You can always add them later if system requirements change, by re-running the installer.



When presented with the User Manager Credentials dialog during the installation password, set a strong administrator password. It is recommended that the password be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid well known, easily guessed, or common passwords. Store passwords securely as **they are not recoverable and will require re-installing the product if lost.**



Work with your IT on centralized storage of this information. Consider that you may not be working for the company or available when another employee needs this information.

Our support is NOT able to recover the passwords for you under any circumstances. Allowing our team to recover your passwords would defeat the purpose of protecting the security of YOUR information and thus create a vector a bad actor could use to extract your information.

Although we cannot recover passwords, additional administrative users can be added to the Administrator user group. Best practices suggest each user with administrative access be assigned unique accounts and passwords to ensure audit integrity and continual access through role and staff changes.

5. Post-Installation

After the product has been installed, there are several actions that the TOP Server administrator should perform to maintain the highest level of security. This includes configuring permissions for Microsoft users, disabling any insecure interfaces that the user will not be using in his or her application, applying the appropriate permissions on the Application Data directory, and configuring user groups and users in a "least privilege" fashion.

Application Data User Permissions

Configure the appropriate permissions on the TOP Server Application Data directory. This folder contains files critical to the proper functioning of TOP Server, and permissions on this folder dictate which users are able to configure the product. By default, TOP Server stores Application Data in 'C:\ProgramData\Software Toolbox\TOP Server'.

1. Using the Windows Security tab, within the Properties of the Application Data folder itself, grant the appropriate user or user group read and write permissions on the Application Data folder. If you are editing permissions using the advanced window, apply the permissions to this folder, subfolders and files.

    - The execute permission is not required to run TOP Server.

    - Only grant permissions to users or groups that require access to the application; do not grant permissions to all users.

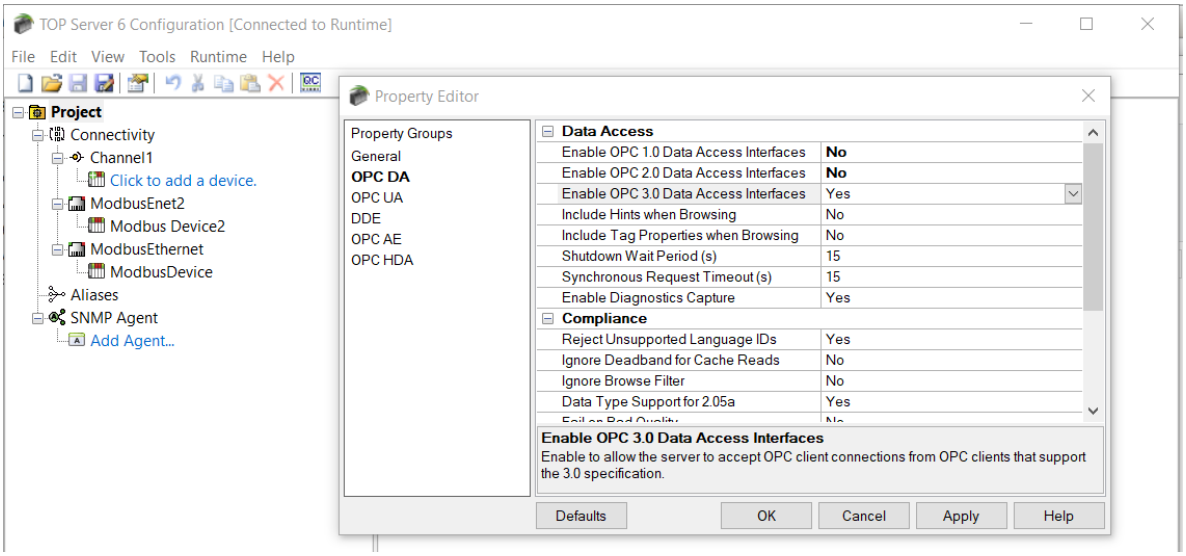
2. By default, the built in 'Users' Windows group inherits read-only permissions on the Application Data Directory. Remove this inherited permission set unless all members of the Users group are trusted to configure TOP Server.

    - **NOTE:** Both read and write permissions are required to open and change the configuration of TOP Server.

Disable Client Interfaces NOT used by YOUR application

Disable the OPC DA Interface if not required for the specific application. Or if you are only using the OPC DA 2.0 interface, disable the OPC DA 1.0 and 3.0 interfaces, which for many Wonderware users will be what they should do.

1. Run the TOP Server Configuration.
2. Right-click on Project and select **Project Properties**.



Select **OPC DA** Project Properties.

Disable OPC 1.0, 2.0, and 3.0 Data Access Interfaces by disabling the first three properties.

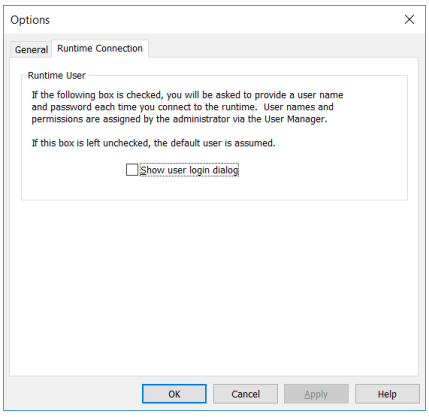
Repeat these steps any time a new project is created that does not require OPC DA connectivity as this is not a system wide setting, but a project by project setting. For System Integrators, this is helpful on their engineering workstations since different client systems will have different TOP Server configurations.

NOTE: Disabling the OPC DA interface will deny access to the built-in Quick Client tool used for testing connectivity. For OPC UA, if you disable OPC DA, utilize a third-party tool, such as UA Expert, to test connectivity via OPC UA. If using Suitelink use the WWClient test tool that comes with Wonderware products.

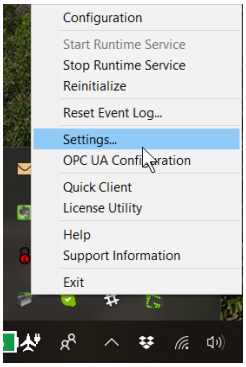
Consider requiring a password to connect to the Runtime

You can require the user to enter a password each time the configuration application connects to the TOP Server Runtime. As an added security measure you may wish to restrict connections to the runtime service from the Configuration UI.

To enable this in the Configuration UI click on Tools->Options in the menu and go to the Runtime Connection tab and click “Show user login dialog” as shown here.

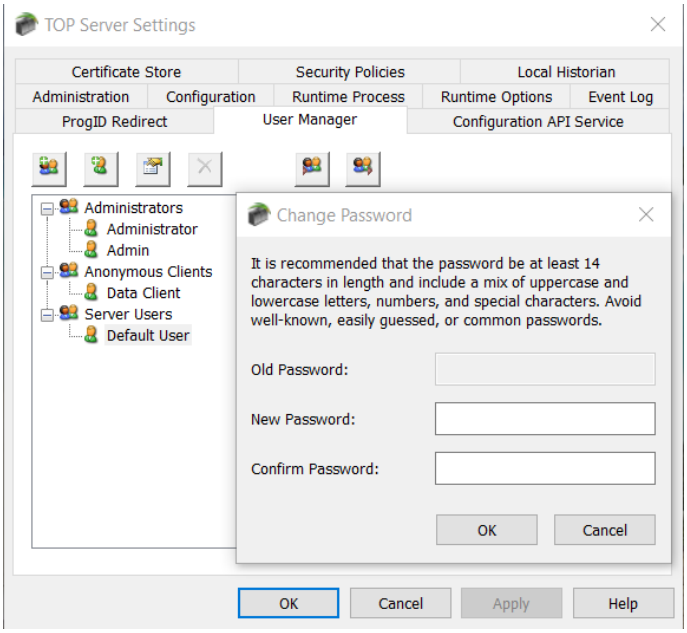


TOP Server User Configuration



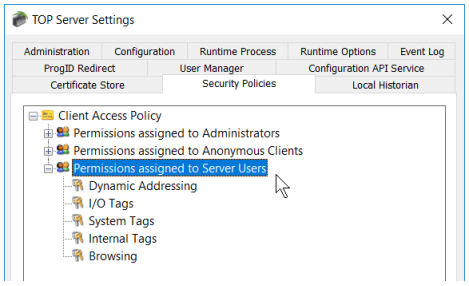
Create a strong user password for the user Default User in the Server Users user group. The Default User cannot be deleted so if you want to control access to your Configuration UI we highly recommend you perform this step.

1. Open the Administrative Settings by right-clicking the TOP Server icon in the system tray and choosing **Settings**.
    1. Select the **User Manager** tab.
    2. The username and password required to access the **Settings** menu with the appropriate level of permissions in this instance will be the Administrator username and password.
    3. Double-click on **Default User** under the Server Users group.
    4. Set a strong password.



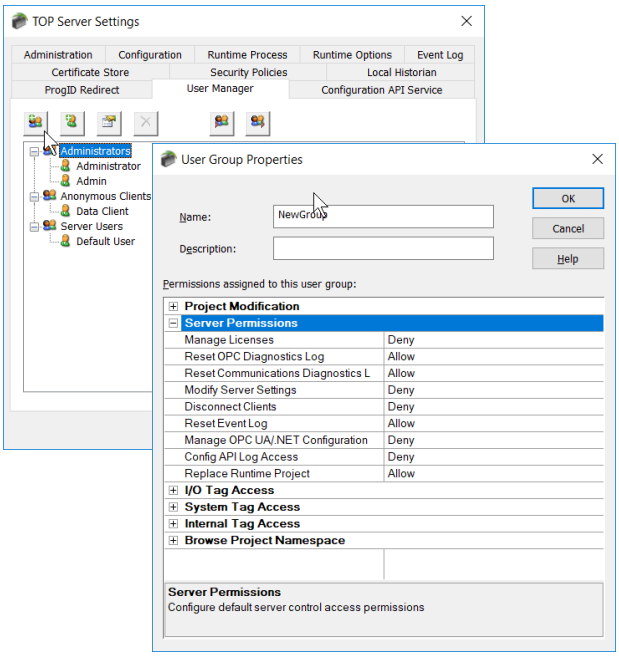
It is recommended that the password be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid well known, easily guessed, or common passwords**. Store passwords securely as our support team is NOT able to recover passwords for you.**

Adjust permissions for the Default User according to the principles of least privilege (i.e. permissions are granted only users that need to perform required functions and revoked when no longer necessary).



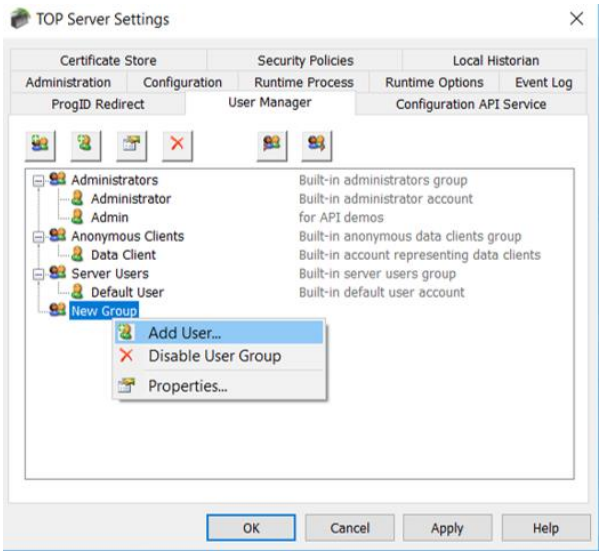
1. Open the **Security Policies** tab in TOP Server Settings.
2. Expand Permissions assigned to Server Users and adjust permissions according to the principles of least privilege.

If configuration users of TOP Server require varying levels of permissions, create additional server user groups as necessary and adjust the permissions according to the principles of least privilege.



1. Open the **User Manager** tab in TOP Server Settings.
2. Click **New Group**.
    1. Assign permissions to the newly created group according to the principles of least privilege.
    2. Right-click on the new group.
    3. Click **Add User**.
    4. Set a strong password. It is recommended that the password be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters.

- Avoid well known, easily guessed, or common passwords. Store passwords securely.
- Do not share user names or passwords across multiple users! Create a new user and / or a new group when users need varying levels of permissions.



6. Configuring Client Interfaces that Offer Advanced Security

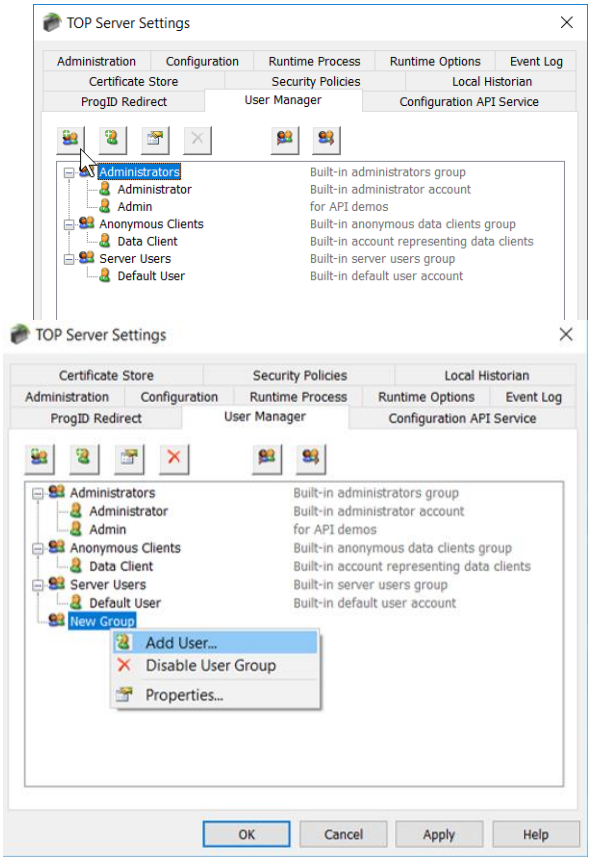
TOP Server is designed to communicate over protocols commonly used in industrial automation OPC UA is a popular protocol that can be configured to use a high level of security. There are other protocols that can also be configured securely (SNMP and DNP3, for example, among others)

Refer to the TOP Server manual for more information on other secure protocols.

Anytime you have the option to specify a UNC path, ensure the path is a trusted and secure location.

OPC UA

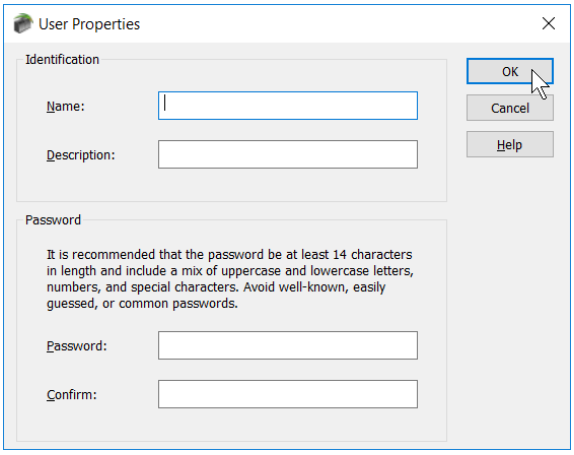
Create a server user group for the specific purpose of using the OPC UA interface and adjust the permissions for that group according to the principle of least privilege.



1. Open the User Manager in TOP Server Settings.
    1. Click New Group.
    2. Assign permissions to the new group according to the principles of least privilege.
    3. Right-click on the new group.
    4. Click **Add User**.
    5. Set a strong password.

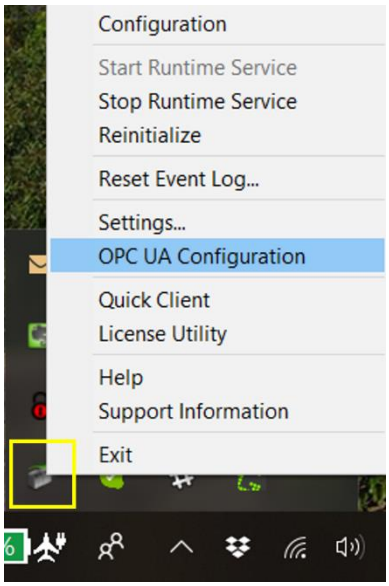
- It is recommended that the password be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid well known, easily guessed, or common passwords. Store passwords securely.
- Do not share user names or passwords across multiple users!

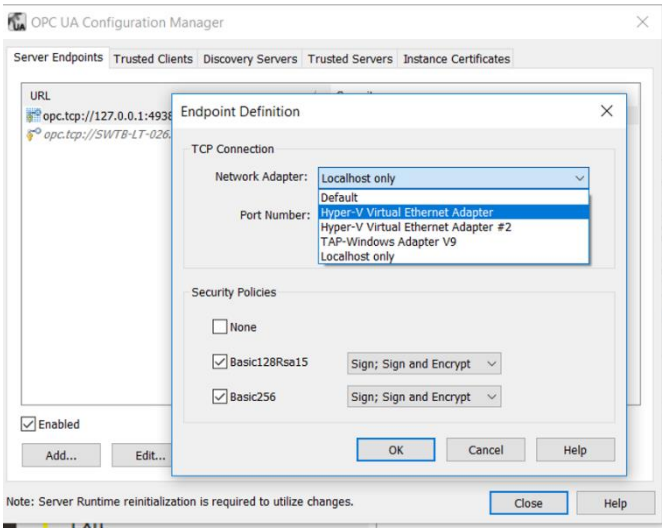
- Create a new user and / or a new group when users need varying levels of permissions.
- UA Anonymous logins are disabled by default. It is recommended to never permit anonymous UA client access.



When building the OPC UA server endpoint, utilize the strongest security settings currently available.

1. Open the OPC UA Configuration Manager by right-clicking the TOP Server icon in the system tray and choosing **OPC UA Configuration**.
2. Click on the **Server Endpoints** tab.
3. Click the **Add...** button to define a new endpoint.
4. Ensure the most up-to-date Security Policy options are checked.
   For example, in the below screen, using Basic256 would be most
   current option.
5. Consider removing any unused OPC UA endpoints. For example if you are using Basic256 then why have the other less secure endpoints available.
6. Click **OK**.

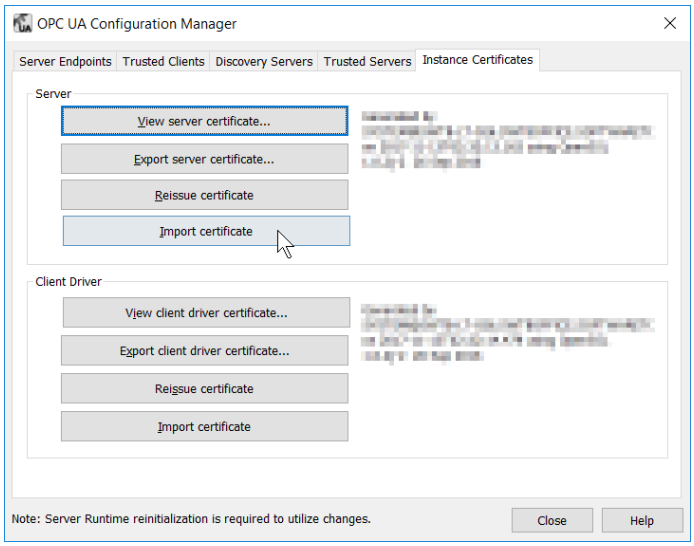




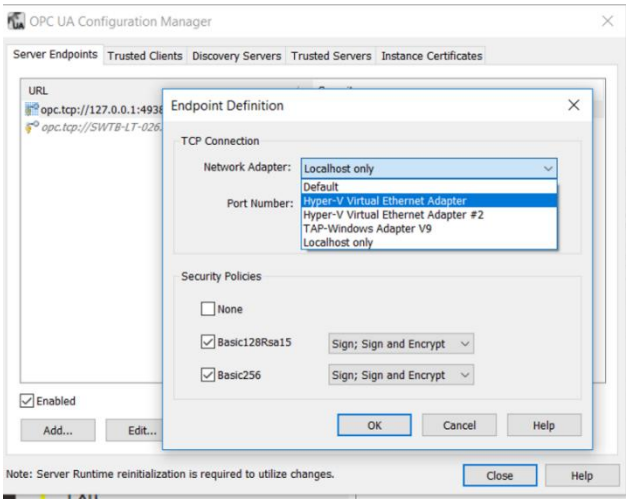
Utilize a Certificate Authority (CA)-signed certificate, when possible. If you prefer to not do this for your own business reasons, then consider generating your own self-signed certificate using the latest version of OpenSSL. Instructions on using the Reissue Certificate button in the OPC UA Configuration Manager are found in the TOP Server help file.

NOTE: TOP Server limits self-signed certificates to a lifetime of two years in keeping with generally accepted encryption practices. Although you may choose to self-sign a longer certificate using an external utility, it is not recommended.

In the Instance Certificate tab of the OPC UA Configuration Manager, click **Import Certificate** and import a certificate signed by a CA.



- When building the OPC server endpoint, utilize a network adapter accessible only from the network that is running the OPC UA Client accessing TOP Server (i.e. do not utilize a network adapter accessible to the internet or to other networks that are not required for connectivity).



    1. Open the OPC UA Configuration Manager.
    2. Add a new endpoint.

    Ensure the network adapter used is accessible only from the network that is running the OPC UA Client.

MQTT Client Driver

When configuring the MQTT broker that TOP Server will connect to, set a strong username and password, utilize strong and modern encryption, and utilize a Certificate Authority (CA)-signed certificate when possible.

If you prefer to not use a CA-signed certificate for your own business reasons, then consider generating your own self-signed certificate using the latest version of OpenSSL. Instructions on using the Reissue Certificate button in the OPC UA Configuration Manager are found in the TOP Server help file.

Configuring these items will depend on the specific MQTT broker utilized.

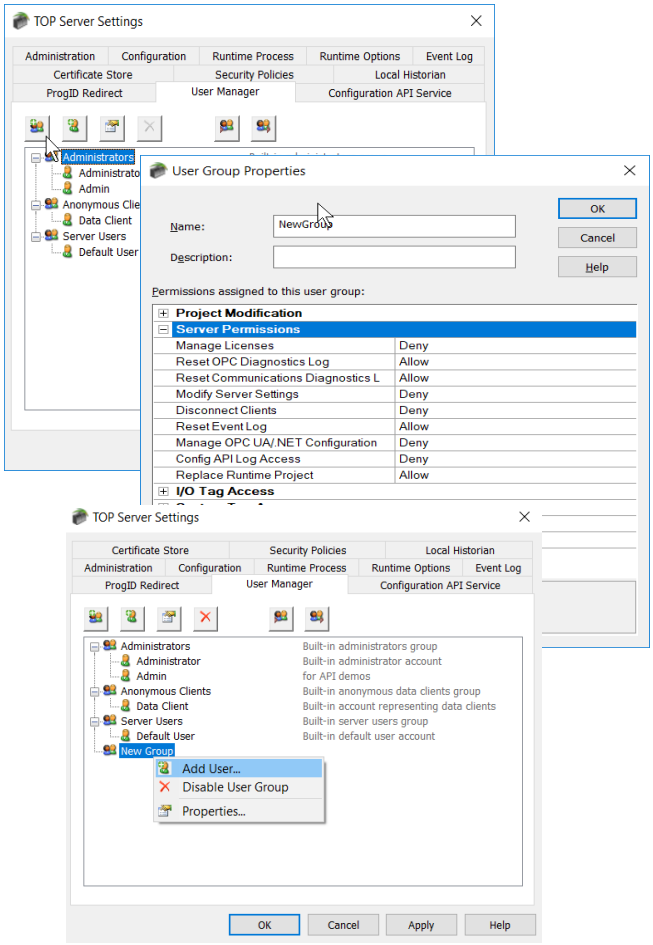
7. Configuration API – RESTful implementation

The Configuration API allows users to programmatically configure certain TOP Server drivers and plug-ins. It allows users with many instances of TOP Server or constantly changing products to seamlessly update their configurations. It is important to utilize this feature using the highest level of security possible.

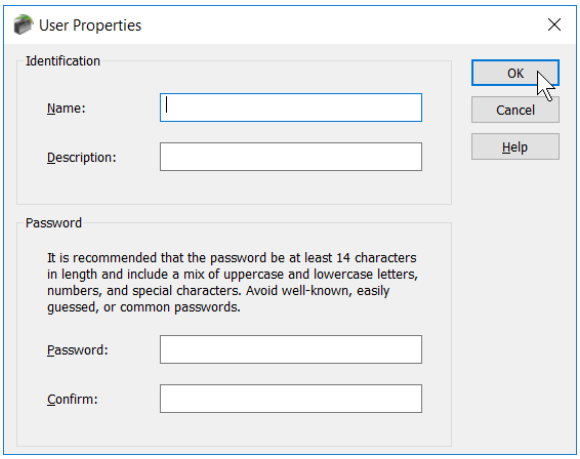
The Configuration API is disabled by default, which means you have protection from the start. If you choose to enable the Configuration API, here are some things to consider.

Create a server user group for the specific purpose of using the Configuration API and adjust the permissions for that group according to the principle of least privilege.

1. Open the User Manager in TOP Server Settings (accessible by right-clicking the TOP Server icon in the system tray).
2. Click **Add Group**.
3. Assign permissions to the newly created group according to the principles of least privilege.
4. Right-click on the new group and choose **Add User….**



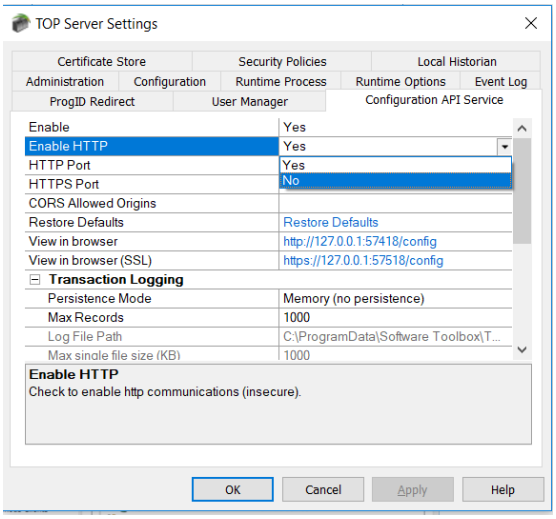
- Set a strong password.
- It is recommended that the password be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid well known, easily guessed, or common passwords. Store passwords securely.
- Do not share user names or passwords across multiple users;
- Create a new user when necessary and a new group when users need varying levels of permissions.



Consider Disabling HTTP

- Consider only HTTPS; do not enable HTTP for production use unless you are confident in the security of your network. If you are using the Software Toolbox .NET API wrapper for the REST config API, please contact us for consultation on security.

  To configure available interfaces:
- Open the Configuration API Service Settings in TOP Server Settings (accessible by right-clicking the TOP Server icon in the system tray).



Utilize a Certificate Authority (CA)-signed certificate when possible.

In the Configuration API Service Settings, click **Import Certificate**... and import a certificate signed by a CA.

In the Configuration API Service Settings, input white- listed domains into the **CORS allowed origins** setting.

- It is recommended to populate CORS (Cross Origin Domain Sharing) settings with white-listed domains.
- Do NOT use the option of an asterisk to accept all.
- Monitor transaction logs and server event log as long as the Configuration API is in use
- The endpoint for the Config API event log is /config/v1/event_log, and can be retrieved by issuing a “get” to that endpoint.

8. Ongoing Maintenance & Monitoring

It is important to constantly evaluate and maintain the security of the system and of TOP Server when deployed in a production environment. This includes, but is not limited to, upgrading TOP Server to the latest version as soon as possible, monitoring external dependencies, and following security best practices throughout the lifecycle of the system and in the environment.

TOP Server Upgrades

It is critical that users, especially users deploying TOP Server in safety-critical environments, upgrade to the latest version as soon as possible to take advantage of security enhancements.

It is important to be able to quickly validate newer versions of the software before deploying in a production environment.

Users should have a plan in place to quickly validate and implement new versions without any impact to operations. The ICS CERT recommends that "system administrators should test all patches off-line in a test environment that contains the same model and type of ICS to determine whether the patch has unintended consequences.

Diagnostics

Only utilize the various diagnostics features throughout the product when necessary and turn off diagnostic modes when not in use. The reasoning here is to only make information that provides more details on the operations of the product available when needed and to those that need it.

External Dependencies

Monitor all external dependencies and upgrade to the latest version as soon as possible. By external dependencies we may the external libraries, third party configuration tools, or communications cards in the target that some drivers require.

Examples include the Fanuc Focus libraries, Beckhoff TwinCAT libraries, and others.

If a driver has external dependencies, they are documented in the driver help file in a topic named "External Dependencies"

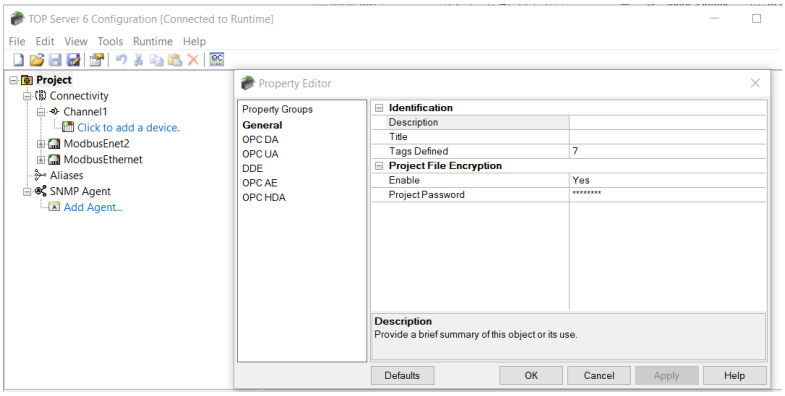
You would have obtained these from their respective vendors when you first setup TOP Server and you should maintain contact with those suppliers to know about updates.

Project File Security

When saving a project, utilize all available security mechanisms.

1. Open the TOP Server Configuration.
    1. Open **Project Properties**.
    2. Open the **General** properties group.

- Set a strong password to protect .opf project files.
- It is recommended that the password be at least 14 characters in length and include a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid well known, easily guessed, or common passwords.
- Store passwords securely.
- Project files saved as JSON are human readable and editable. End users should exercise caution when using this format.



Documentation

1. It is recommended to document all configuration, administrative, or runtime changes made to TOP Server, as well as all systems that interact with TOP Server.
2. You must have a process to ensure this documentation is updated as changes are made. If you don't have any change management process in place, now would be a good time to start one. Doing anything is better than doing nothing.
3. This will enable roll-back to a previous system state as well as the ability to replicate any given configuration should it become necessary.
4. Regularly review the system configuration as compared to this guide and verify deviations are part of a conscious choice that does not compromise security.

System Recovery

Despite all your best efforts, somethings things may happen. You should have a solid disaster recovery plan in place that includes at a minimum these considerations:

1. **Are your machine backups done in a way such that you are not over-writing the last backups every time?** If your machine were to be compromised and some of the data encrypted by a bad actor, but not to the point your OS won't boot, and then your backup runs, and you overwrite the one and only copy of your backup with encrypted data, you have a problem.
2. **Keep up with your installers and licenses for your machine!** This includes your TOP server installer, activation ID, Emergency Activation ID and serial # from your product delivery email. Our support gets calls asking us to magically know what license was on a machine. Sometimes we can help if you entered good registration notes when unlocking your license, but sometimes there's not much we can do. Treat your installer and license keys just like your car and its keys.
3. **Keep secure, password protected backup *.OPF files** on a different machine or network server.

Ongoing Monitoring

You should also monitor your machines ongoing health and use features within TOP Server that are available to help you do that. You should also be working with your IT department on implementing best practices used in other parts of your business for monitoring system health and dealing with problems proactively.

1. TOP Server Event Logs – these logs can tell you a lot, and you should consider monitoring them. The TOP Server has a built in OPC Alarms & Events interface that you can configure and then connect your overall alarm management system to and generate notifications for abnormal conditions.

2. TOP Server System Monitor driver – this driver can monitor the health of the PC, or server that TOP server is running on, and you can use the resulting information to generate alarms in your HMI/SCADA system. If you suddenly see problems with resource utilization on your system, and nothing has changed in the configuration, then you may need ask "has my system been compromised and are there now rogue processes running?"

3. Windows Event Logs – your IT department may take care of this for you. If not there are many commercially available tools on the market that you can use to monitor your Windows Event Logs for problems you care about and notify you when there are problems.

9. Next Steps & Other Resources

Access additional information in the TOP Server Version 6 product manual.

Access Software Toolbox's guides for information on getting started with TOP Server features.

Download the latest version of TOP Server from our website

TOP Server OS Support Matrix

TOP Server Release Notes

Email sales@softwaretoolbox.com to schedule an in-depth demonstration and to learn how to use TOP Server in the specific environment.

For technical questions regarding this document, consult our Support Team; however recognize some questions may require our cybersecurity resources to comment, so answers may take longer than our normal support response time.

Software toolbox®

888 665 3678 TOLL FREE
+1 704 849 2773 GLOBAL
Charlotte, NC USA GLOBAL HQ
www.softwaretoolbox.com WEB

Our mission is to provide you with the right software package to solve your industrial operation challenges.