Secure Deployment Guide

Kepware Edge

December 2025
Ref. 1.00

Table of Contents

1. Introduction

Kepware Edge 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 deploy the application as securely as possible. This document guides users through the process of deploying Kepware Edge with maximum security. It is recommended that administrators follow this guide as closely as possible when deploying in a production environment.

Kepware recommends new users utilize this guide for new production installations whenever practical. Kepware also recommends existing users of the software compare existing configurations with the recommendations provided in this guide and adjust for best practices.

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 best practices emerging that includes 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 case (e.g. operations network, satellite or cell network, or local network on a machine). The identification and implementation of these 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.

Kepware Edge can be used to connect many thousands of different industrial automation devices and systems. As such, secure device and system configuration is beyond the scope of this document. Follow 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.

2.1 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 (http://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)

2.2 Resources for Container Security

Kepware Edge is delivered as a containerized product. It is recommended that those managing the installation and support of the Kepware Edge product develop internal expertise in containerization and best practices for container security. Some useful resources are listed below.

- Center for Internet Security (CIS) Docker Benchmarks (https://www.cisecurity.org/benchmark/docker)
- Red Hat Enterprise Linux Container Security Practices (https://docs.redhat.com/it/documentation/red_hat_enterprise_linux_atomic_host/7/html/container_security_guide/container_security_practices)
- National Institute of Standards and Technology Application Container Security Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf)

2.3 System Integrators

- System integrators connected with Kepware System Integrator Program (https://www.kepware.com/en-us/partners/system-integrators/)

3. Host Operating System

Kepware Edge should always be deployed in the most secure environment possible. Ensure the host operating system (OS) where Kepware Edge is deployed is secure from the outset and take all feasible measures to maintain the security of the OS for the life of the system. Kepware Edge 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.

3.1 System

Ensure appropriate access control measures are in place to limit physical access to the target hardware to appropriate users.

Always deploy on an actively supported modern operating system (x86-64). Be sure to maintain security patches on the OS 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".

Consult relevant security documentation for Kubernetes (Security | Kubernetes) and/or Docker Engine (Security | Docker Docs)

Encrypt the hard drive of the host machine to secure all data at rest.

Regularly scan the host system and all containerized images using respected security software with up-to-date and supported signature files.

Turn off any unused services on the host machine.

The user should not modify the containerized operating environment.

Limit container capabilities to only what is necessary. And apply network policies for isolation.

3.2 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.
- Monitor container runtime logs.

3.3 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. Deployment

4.1 Validation

4.1.1 Kepware maintains unique identification codes for officially released software. Customers should verify against these codes to ensure that only certified binaries are installed.

4.2 Deployment Security

4.2.1 A password for the administrator account must be set at container runtime. During container initialization, Kepware Edge searches for a password.txt file that contains the administrator account password or looks for an environmental variable (non-production/insecure). The password must be between 14 and 512 characters. Set the permissions on this file such that the Docker container user has read and write permissions. Place this file in a directory accessible to the container via a bind mount, as described in the Starting a Kepware Edge container instance section.

5. Post-Deployment

After the product has been deployed, there are several actions that the product administrator should perform to maintain the highest level of security. This includes configuring permissions for users, disabling any insecure interfaces that will not be used in the application, applying the appropriate permissions on the Application Data directory, and configuring user groups and users in a “least privilege” fashion.

5.1 User Management

5.1.1 Create strong user passwords for the Administrator, Anonymous, and ThingWorx Users with appropriate access.

The Administrator user account password cannot be reset, but 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.

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.

5.2 Permissions

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).
Configure event log viewing permissions with least-privilege principles to differentiate administrative and other users.

- Avoid well known, easily guessed, or common passwords. Store passwords securely.
- Do not share usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permission.

6. Secure Interfaces

Kepware Edge is designed to communicate over protocols commonly used in industrial automation and the Industrial Internet of Things (IIOT). Certain protocols are more secure and have more options for security than others. OPC UA, MQTT, and REST are popular protocols that can be configured to use a high level of security. There are other protocols that can also be configured securely (ThingWorx Native Interface and others).

- *Refer to the user manual for more information on other secure protocols.*
- When using the UNC paths, ensure the path is a trusted and secure location.
- Some protocols are adding certificate authentication for secure communications. For those drivers where it is available, certificates are managed through the command line utility.
- Avoid well known, easily guessed, or common passwords. Store passwords securely.
- Do not share usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permission.
- UA Anonymous logins are disabled by default. It is recommended to never permit anonymous UA client access.

7. Configuration API

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

7.1 Configuration API

7.1.1 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.

Set a strong password.

- The password must 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 usernames or passwords across multiple users. Create a new user or a new group when users or groups need varying levels of permission.

7.1.2 It is strongly recommended to only use HTTPS in both production and testing. HTTPS must be used for production.

7.1.3 Sanitize data both sent and received by the Configuration API.

- Ensure that invalid scripting characters and other malicious inputs are not being passed to the server from the clients.
- As a best practice, clear the browser cache after each session of Configuration API interaction.

8. Ongoing Maintenance

It is important to constantly evaluate and maintain the security of the system and the server when deployed in a production environment. This includes, but is not limited to, upgrading 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.

8.1 Upgrades

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

8.1.2 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 on 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."
- Automating these tests can expedite this process.

8.2 Diagnostics

8.2.1 Only utilize the various diagnostics features throughout the product when necessary and turn off diagnostic modes when not in use.

8.3 Project File Security

8.3.1 When saving a project, utilize all available security mechanisms, including encryption, password protection, limited access, and backup processes.

8.4 Documentation

8.4.1 Document all configuration, administrative, or runtime changes made to the server, as well as all systems that interact with the server.

Persisting configuration data is strongly recommended. Configuration data, such as the project file, certificates and endpoints, user management configuration, and other data are stored in the /opt/kepedge/v1/.config folder in the container file system. Persisting this folder allows for a container to be redeployed due to failure or planned updates while keeping all configuration data from the previous running state.

This enables roll-back to a previous system state as well as the ability to replicate any given configuration should it become necessary.

8.4.2 Regularly review the system configuration as compared to this guide and verify deviations are part of a conscious choice that does not compromise security.

9. Next Steps

1. Access additional information in the user manual.
2. Access Kepware's guides for information on getting started with product features.
3. Email sales@kepware.com to schedule an in-depth demonstration and to learn how to use the server in your specific environment.

