Technical Note

Creating a More Secure Environment for IIoT Data with KEPServerEX and the IoT Gateway

This document explains how to leverage the KEPServerEX® IoT Gateway security features and the standard means of data security in both a LAN and WAN environment. As industrial data moves from isolated plant floor networks onto corporate and public networks, specific precautions should be taken to verify that this data is not being viewed, intercepted, or manipulated in any unauthorized manner. Each of the IoT Gateway agent types are discussed. A basic understanding of network topology and transport technologies is required to properly secure an IoT Gateway installation.

1. MQTT Agent

The IoT Gateway MQTT agent pushes data to, and receives data from, a third-party MQTT broker. It is the third-party broker that must be configured to safeguard IoT data. Refer to the MQTT broker's accompanying documentation for the best, up-to-date security practices. The MQTT protocol supports basic authentication and SSL encryption. It is recommended that SSL encryption be enabled on the broker and used for communication between the IoT Gateway agent and the broker. Some brokers may be configured to accept both SSL and non-SSL encrypted connections at the same time. It is essential to verify that the MQTT agent connection URL starts with "ssl://" rather than "tcp://" to ensure that the SSL encrypted connection is being used. If the broker is not configured to support SSL encryption, all communication (including usernames and passwords for basic authentication) is transmitted as clear text.

Basic authentication allows the broker to verify client connections. Depending on the broker software used, the authentication may be configured to allow granular control of read and/or write access to each topic on the broker. This granularity should be used to only allow the appropriate MQTT clients write access to the topic used to provide data to the IoT

Gateway MQTT agent. Once the MQTT agent has been allowed to subscribe to a topic ("iotgateway/write" by default), any other MQTT client that writes to that topic with the proper data format manipulates the values of tags exposed by the MQTT agent. Additionally, the IoT Gateway MQTT agent publishes data to the broker by default on the "iotgateway" topic. Basic authentication should be used to prevent other clients from writing to this topic to prevent injection or manipulation of data sent by the IoT Gateway. Basic authentication can also be configured to limit which MQTT clients have read access to the data. Once basic authentication is configured on the broker, the username and password configured for the IoT Gateway MQTT agent should be set under the security tab. It is recommended that this account have write-only access to the "iotgateway" topic and read-only access to the "iotgateway/write" topic.

Additional ways to secure your MQTT communications would include configuring both the KEPServerEX machine and the MQTT broker on the same private LAN or on a VPN, though transport encryption with SSL and basic authentication should still be utilized to protect the data. It is not recommended to have the IoT Gateway MQTT agent configured to accept writes from an open and publically accessible broker. This could allow for malicious data to be written to tags exposed by the agent.

2. REST Client Agent

Similar to the MQTT agent, the REST client agent security is primarily dependent on how the receiving third-party REST server is configured. Refer to the REST server's accompanying documentation for best, up-to-date security practices. The REST client agent is a one-way publish-only agent, providing read access to the tags exposed. It does not allow writing tag values. The REST client agent supports both unencrypted and encrypted connections to a REST server endpoint through HTTPS. Non-HTTPS connections transmit all data in plain text, including usernames and passwords used by basic authentication. It is recommended when connecting to a REST server that SSL encryption be used by using a URL that starts with "HTTPS://".

It is also recommended that the third-party REST server endpoint (where the REST client agent is publishing data) be configured to only allow HTTPS POST requests from authenticated users. Once user credentials are configured within the third-party REST server, set the username and password on the security tab of the REST client agent.

As with the MQTT agent, configuring the REST client agent and the third-party REST server on the same private local network or VPN reduces the vulnerability of the data, though basic authentication and transport encryption with HTTPS should still be utilized to protect the data.

3. REST Server Agent

Unlike the other two agents, most security for the IoT Gateway REST server agent is configured within the KEPServerEX IoT Gateway. The provisions in KEPServerEX enable basic authentication with granular access control and transport encryption. As with the other two agents, configuring the REST server agent to use HTTPS ensures the use of transport encryption. Caution should be applied to disabling HTTPS within the REST server agent, as data would be transmitted unencrypted. Generally, HTTPS Should be enabled at all times. The IoT Gateway creates a default certificate for HTTPS, though the REST server agent has

the ability to import any certificate generated by a Certificate Authority. *Refer to the product manual for further instructions.*

By default, anonymous login is disabled, requiring the use of a username and password for basic authentication between the REST client and the server. The username and passwords are configured in the KEPServerEX settings under the User Manager Security Policies. Follow the organization's best past practices for ensuring appropriate password strength, especially for all default accounts. Using the Security Policies manager, individual users may be assigned appropriate read and/or write access to specific tags exposed by the REST server, based on role and requirements. Instructions for configuring users are found in the KEPServerEX Help document.

By default, only read access is granted to tags exposed by the IoT Gateway REST server agent, regardless of how user access is setup within the Securities Policy Manager. This should only be altered if one or more REST clients need to write through the REST server interface.

The IoT Gateway REST server agent should not be configured to accept writes from anonymous users if the server is available publically; this could cause malicious data to be written to tags exposed by the agent. KEPServerEX with IoT Gateway REST server agent should not be placed on a public network without authentication and encryption.

4. Overall Recommendations

- Always use username and password authentication to provide read and/or write access to data, especially when on a publically accessible network.
- Always use SSL or HTTPS to provide transport-level encryption.
- Always leave write access disabled (default setting) within the agent properties if clients only require read access of the data.
- When possible; configure KEPServerEX and other brokers, servers, or clients on a private networks or use a private VPN.

