# Technical Note

# Secure Isolated Networks and Data Diodes —Data Access Using KEPServerEX®

This note outlines how to provide access to data from secure isolated networks protected by a one-way data transfer solution – either a data diode or a network firewall - using KEPServerEX.

## 1. Secure Isolated Networks

Security is critical for modern Ethernet networks. Some types of secure networks must be completely isolated, yet the equipment on these networks may be monitored by systems outside the secure networks. Isolation of the secure network limits data retrieval to a one-way path inside the network to outside the network. No information can enter the secure network and only certain information can leave the secure network. Two solutions that are often used to provide this network isolation are data diodes and network firewalls.

## 2. Data Diode and Network Firewalls

A data diode is a technology that facilitates one-way transfer of data. The term “diode” is borrowed from electronics, where a diode is a semiconductor with two terminals, typically allowing the flow of electrical current in one direction only. In the case of data transfer, a data diode is typically a purpose-built Ethernet network hardware solution with a small Ethernet-oriented software stack designed to permit data flow over only one specific uni-directional data transport protocol – UDP (User Datagram Protocol). Additionally, the unique hardware of the data diode provides physical data transport in one direction only. Even if the software on the data diode hardware is attacked and modified, data transport into the secure network is prevented by lack of a physical network path.

It's important to note that data diodes are similar to, but not the same as, a network firewall. A firewall can also enforce one-way data transfer from secure network to the outside network, but it does so using software-defined rules: a physical path to the secure network is still present.

Whether using a data diode with purpose-built hardware or a network firewall that only permits outbound network traffic, this note describes how to build a data access solution using KEPServerEX.

- **Note**: Purpose-built data diode hardware solutions, especially those targeting industrial environments, may offer built-in support for certain industrial protocols. For example, some are capable of acting as OPC DA client and server, and a data access solution integrated using these protocols may be more optimal for the goals than the solution outlined in this guide. Check the specific protocol capabilities of the specific data diode before building a solution with this guide. Contact PTC Applications Engineers with questions: presales.support@kepware.com.

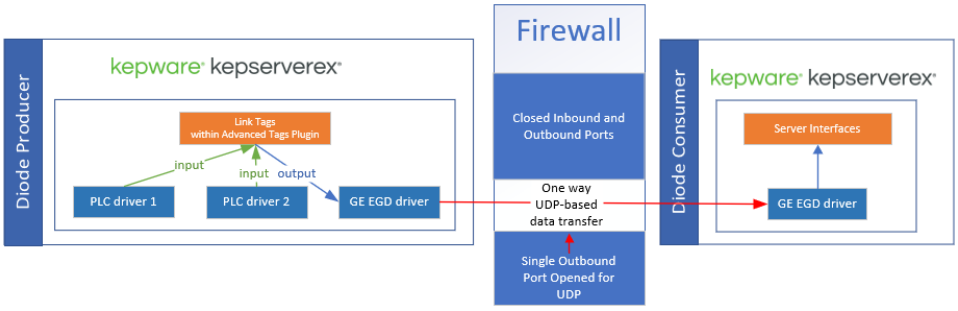
# 3. Terminology

**Diode Producer:** describes the system that pushes data out of the secure network.

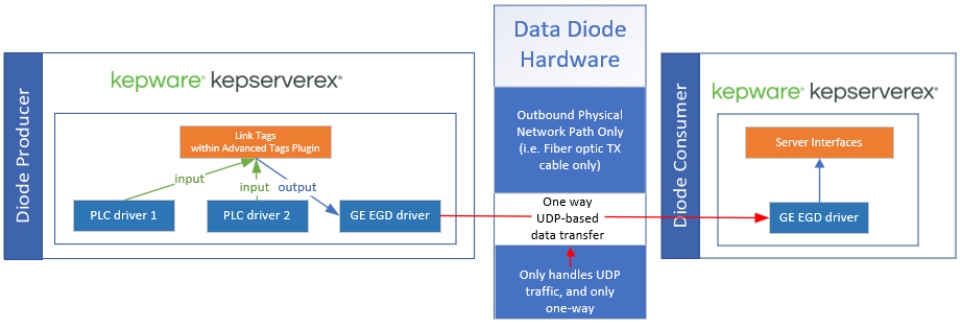
**Diode Consumer**: describes the system that receives the data from the secure network.

# 4. Topology Overview and Operation

The following architecture is an example solution built with two instances of KEPServerEX to accommodate one-way data transfer through a network firewall:




The same solution can be utilized to accommodate one-way data transfer through a data diode:



The **Diode Producer** is a Microsoft® Windows machine – either physical or virtual – running KEPServerEX. Within KEPServerEX, PLC drivers allow this instance to ingest data from systems locally within the secure network. A memory-based driver can be used if client applications within the secure network (like an HMI panel or a SCADA system) need to share data with clients outside of the secure network. On the Diode Producer, the GE EGD (Ethernet Global Data) driver allows <product 2> to push (or write) data one-way across the firewall or data diode that creates and secures the isolated network. On the Diode Producer, link tags within the Advanced Tags Plug-in allows the server to automatically move data from PLC drivers to the EGD driver for transmission across the firewall or data diode.

The **Diode Consumer** is a Microsoft® Windows machine – either physical or virtual – running KEPServerEX. The GE EGD driver allows <product 2> to ingest (read) the one-way data stream from the instance of the server within the secure network. On the Diode Consumer, as the EGD driver ingests tag values from the one-way data stream, the values are available to any component of KEPServerEX. This includes native server interfaces like OPC DA and OPC UA and ThingWorx AlwaysOn, as well as Plug-Ins (such as the IoT Gateway or DataLogger).

# 5. Protocol Description

Ethernet Global Data (EGD) is a network protocol created originally by GE and utilized by various devices and software applications for the purpose of generic information exchange. The EGD protocol utilizes UDP for data transport and contains no data transport layer or application layer message acknowledgements, making it a suitable protocol for use in this context.

**Note**: The destination port number for EGD messages is fixed at 18246. If using a network firewall to create the secure isolated network, this port should be opened for outbound UDP traffic.

# 6. PTC Licensing

The following licenses are required for the data diode solution:

- 2 x GE EGD drivers - one for the Diode Producer and one for the Diode Consumer
- 1 x Advanced Tags Plug-In for the Diode Producer
- ≥1 PLC drivers for the Diode Producer

**IMPORTANT**: String data types are NOT supported in EGD. If string support is desired for the GE EGD driver, consider using the User-Configurable (UCON) driver to build producer and consumer driver profiles. UCON supports UDP and protocols can be built with no expectation of application-layer acknowledgements.

*For more information, contact PTC Kepware Applications Engineers.*

# 7. Instructions

## 7.1 Install KEPServerEX

On the machine to be the Diode Consumer, install KEPServerEX. Ensure the GE EGD driver is selected for installation and select other components as needed.

On the machine to be the Diode Producer, install KEPServerEX. Ensure the GE EGD driver and the Advanced Tags Plug-In are selected for installation (select other components as needed).

- *For more information installation, see the **Installation Guide** at (https://www.kepware.com/getattachment/ef358e7a-6497-41ca-bfa8-6023bd0ca5c5/installation-guide_en.pdf).*

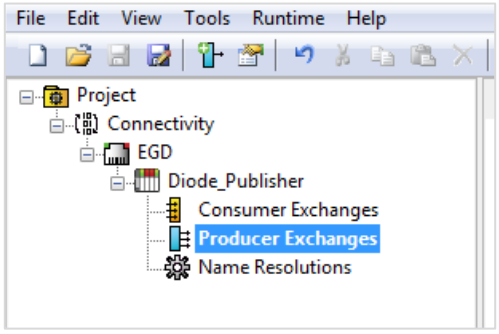
## 7.2 Configure KEPServerEX on the Diode Producer

- *For more information basic configuration, see the **Server Manual** at (https://www.kepware.com/getattachment/5759d980-7641-42e8-b4fb-7293c835a2f9/kepserverex-manual.pdf).*

1. Verify at least one PLC driver is configured in the project. If testing without a device, build a channel with the Simulator driver and create a ramping tag.

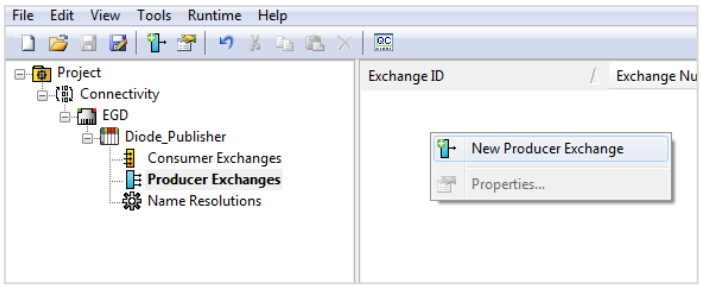
- **Note**: A tag address of "Rx" where x is 1 through 9999 automatically ramps (i.e. change in value) by one every time the tag is read.

2. Create a channel with the GE EGD driver, binding the channel to the network adapter of the host machine to be used to push messages outside the secure network.
3. Create a device on the channel.
4. Once the device is created, there are child elements available below the device.




5. Select **Producer Exchanges** and right-click anywhere on the Detail View. From the context menu, select **New Producer Exchange**.




6. In the Producer Exchanges dialogue, configure the following settings:

   **Exchange ID**: 1

   **Exchange Number**: 1

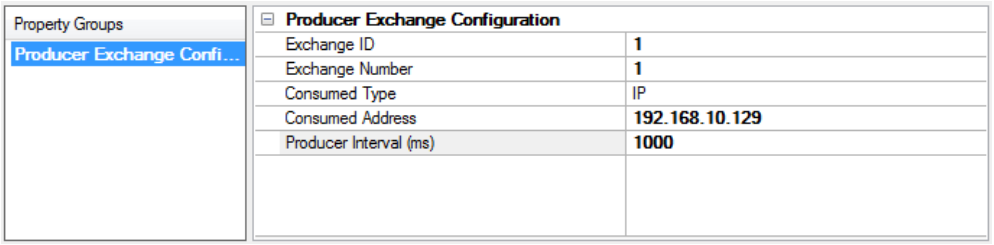
   **Consumed Type**: IP (though DNS / machine name and EGD Group ID are also supported)

   **Consumed Address**: IP address of the Diode Consumer machine

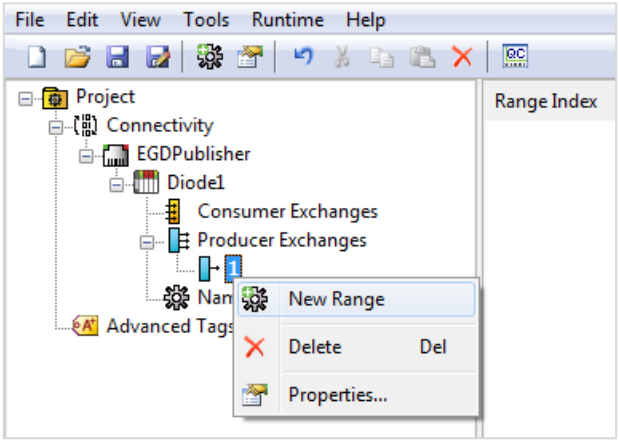
   - This is the IP address of the network adapter that the EGD driver channel object binds to in the instance of KEPServerEX on the Diode Consumer machine.

   **Producer Interval**: 1000 ms

   - This sends the value of all included tags from Producer to Consumer every 1000 ms regardless of Producer-side tag value change. Adjust the Producer interval to whatever frequency is required for data transmission goals and data resolution.




7. After selecting **OK** in the Producer Exchanges dialog box, right-click the new exchange listed under **Producer Exchanges** in the Project Tree and select **New Range**.



- **Notes**:
    - Different ranges are required depending on memory type desired. For the purpose of using EGD to create a data diode, the consideration of memory type should only relate to using memory types that accommodate desired data types from underlying systems. The %R and %I memory types are suggested for simplicity.
    - String data types are not supported in EGD. If string support is desired with the GE EGD driver, consider using the User-Configurable (UCON) driver to build producer and consumer driver profiles. UCON supports UDP and protocols can be built with no expectation of application-layer acknowledgements.

    *For more information about data type support, see the GE EGD Driver Manual.*

8. Enter the following information into the Range dialog box:

- **Note:** Range Index and Offset are automatically calculated and not user-configurable.

    **Name:** a unique identifier

    **Description:** optional summary of the range

    **Reference:** %R if Integer and Floating Point data types are desired; %I if Boolean types are desired *(see Help file for more options).*

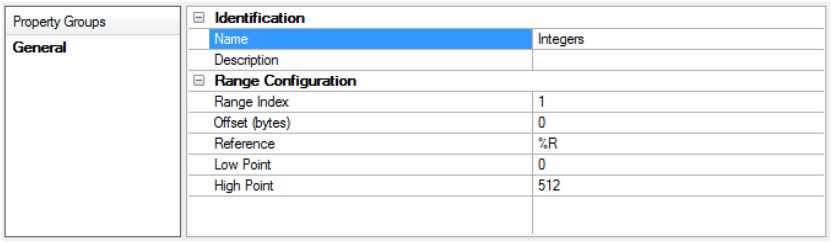
    **Low Point:** the starting count of individual values to store in this range regardless of data type, such as 0, 1.

    - The value of Low Point and High Point will be used to determine the total number of tags (individual values) that can be utilized within the range.
    - The value of Low Point is usually either 0 (for integer memory types) or 1 (for Boolean memory types). As an example, "1" represents a single bit when the range is assigned a %I Boolean memory type and "1" represents a single 16-bit register when the range is assigned a %R memory type.

    **High Point**: the ending count of individual values to store in this range, such as 512. Consider High Point as the total number of individual values to store in this range.

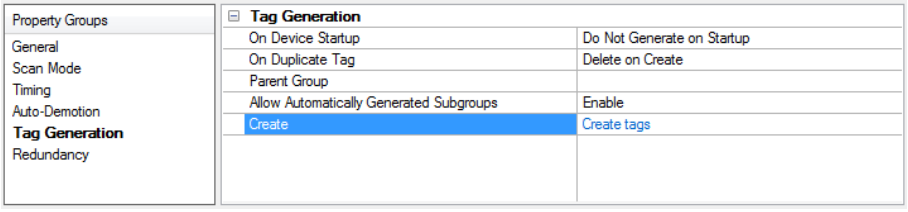
    - Example: if the High Point value is 512 and the range memory type set to %R / Integer, it means that (Qty 512) 16-bit tag data types (Word, Short, etc.) can be stored, (Qty 128) 32-bit tag data types (Float, Long, DWord, etc.) can be stored, and so on. Mixtures of tag data types are possible as long as they are supported by the memory type assigned to the range *(see Help file for more details)*.

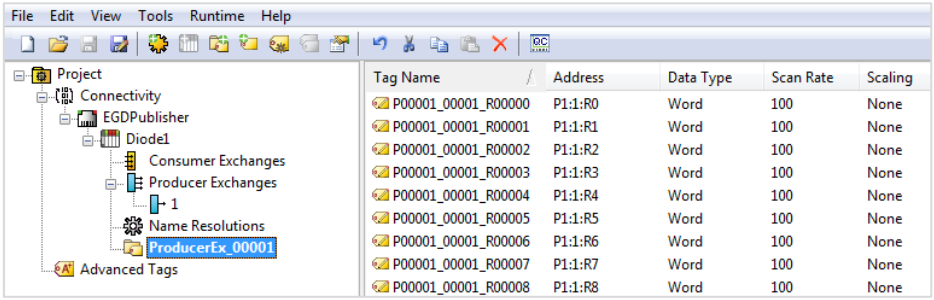



9. Once each desired range has been added, open **Device Properties** and select the **Tag Creation** property group.

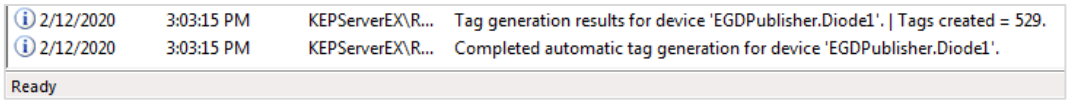
10. Click **Create Tags** to automatically create tags within the EGD driver based on the previously configured address ranges:




11. Verify that in the server project, there is a new folder below the device object whose name is the Product Name and Exchange number.




12. Verify that Informational messages in the event log indicate that tag generation was successfully completed.



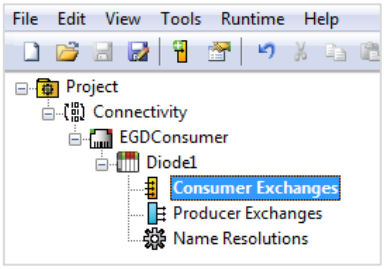

## 7.3 Configure KEPServerEX on the Diode Consumer

1. Create a channel with the GE EGD driver, binding the channel to the network adapter of the host machine to use to receive messages from inside the secure network.

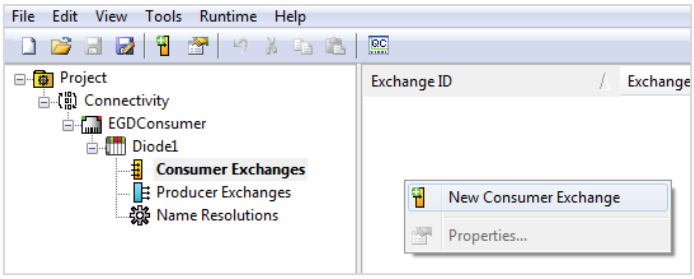
2. Create a device on the channel.

3. Once the device is created, there are child elements available below the device.




4. Select **Consumer Exchanges** and right-click anywhere on the Detail View, then select **New Consumer Exchange**.




5. In the Consumer Exchanges dialog box, configure the following settings:

   **Exchange ID**: 1

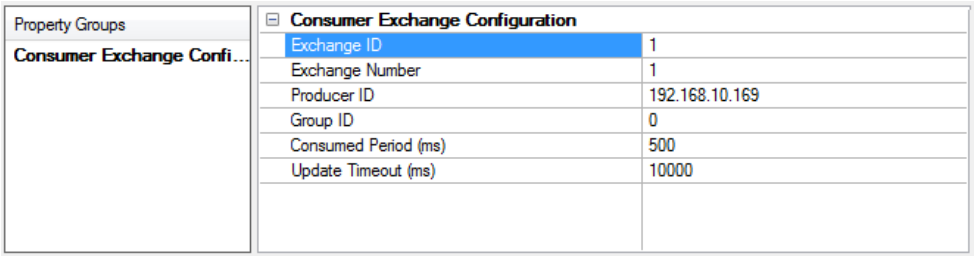
   **Exchange Number**: 1

   **Producer ID**: IP address or host name of Diode Producer

   **Group ID**: leave as 0 / default unless consuming broadcast or multicast vs unicast *(see the EGD driver Help file for more details)*

   **Consumed Period**: 2 x Producer Interval configured on Diode Producer

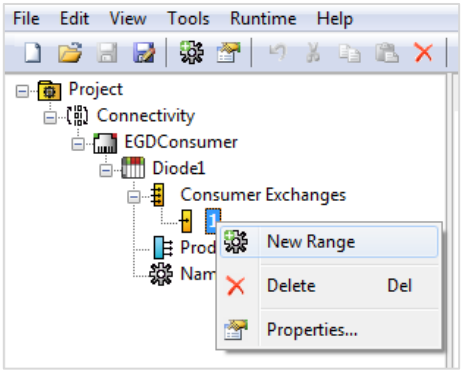
   **Timeout**: 10,000 ms (user-configurable)



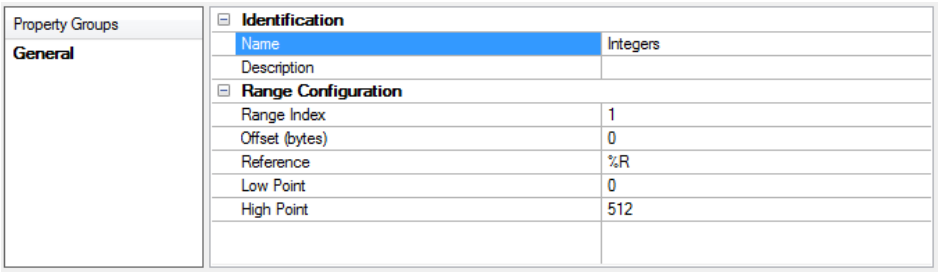

6. Right-click the new exchange under **Consumer Exchanges** in the Project Tree and select **New Range**.

**Note**: The configuration of these ranges must match the Diode Producer ranges.

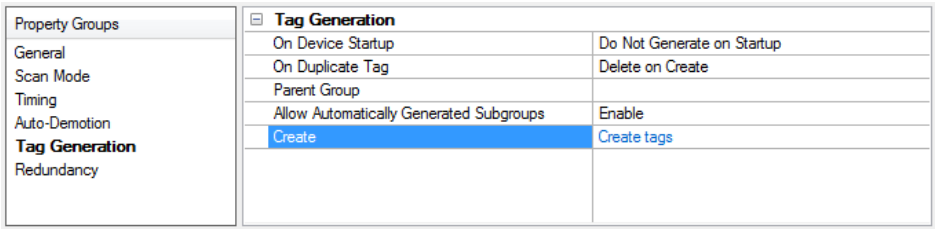



7. Enter the same values set for the Diode Producer Exchange Range for the Diode Consumer Range properties. The Diode Consumer ranges must match the Diode Producer ranges.

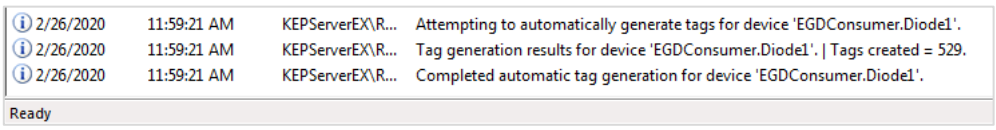



8. After each desired range is added, open Device Properties and select the T**ag Creation** property group.

9. Click **Create Tags** to automatically creates tags within the EGD driver based on the previously configured Address Ranges.

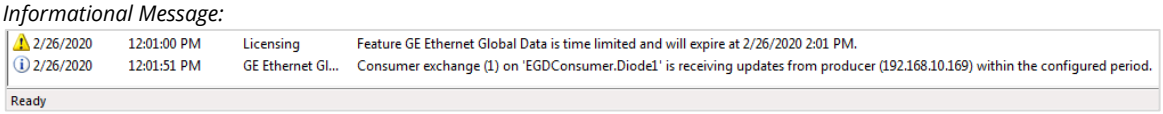



10. Verify Informational messages in the event log indicate that tag generation was successfully completed.



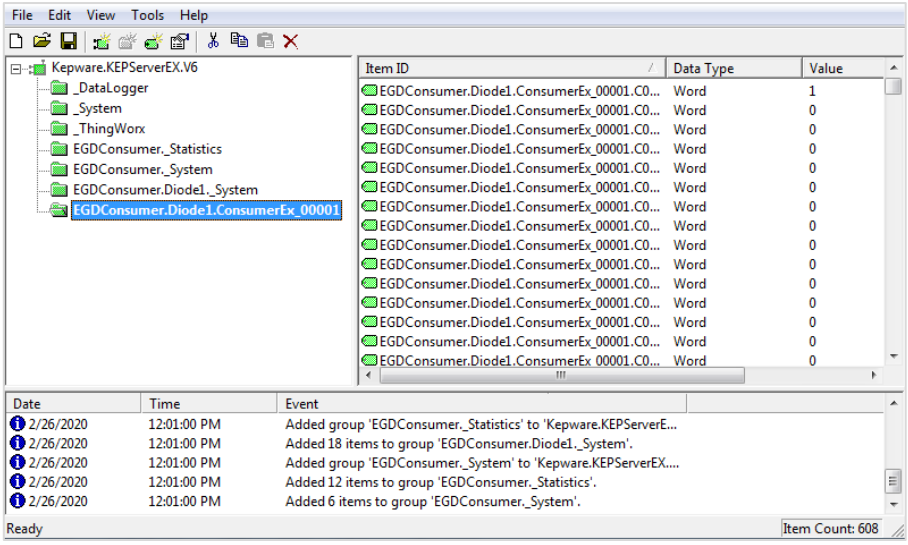

11. On the Diode Consumer system, launch **QuickClient** application from the server to check the data flow between the Producer and Consumer. Informational messages in the event log should indicate the Diode Consumer is receiving updates from the Diode Producer, and the tags should have “Good” quality.

*Informational Message:*



*Quick Client:*




## 7.4 Next Steps

Now that the data diode is functional and successfully passing data from Producer to Consumer, populate the Producer's tags with data from devices on the secure isolated network. To do this, use the Link Tags functionality within the Advanced Tags Plug-in.

- *For more information on Link Tags within the Advanced Tags Plug-in, see the Link Tags Overview Video and Advanced Tags Product Page. Contact PTC Kepware Applications Engineers for additional assistance.*