Rockwell Automation

Configuring Firewalls for FactoryTalk® AssetCentre v12.00

IT Infrastructure Recommendations

Table of Contents

1. Introduction and Document Purpose

This document is intended to show the following information:

- Data flow for specific scenarios and transactions common to FactoryTalk® AssetCentre, including:
    - Interfacing with a FactoryTalk® Network Directory
    - Communication using FactoryTalk® Linx or RSLinx® Classic
    - Working with a controller in an OT environment using Studio 5000 Logix Designer® editing software
- Services used in FactoryTalk® AssetCentre and additional services needed for FactoryTalk® AssetCentre to function properly
- Brief explanation of socket.io and DCOM communications
- Ports, services, and firewall rules necessary for the following FactoryTalk® AssetCentre components:
    - FactoryTalk® AssetCentre Server
    - FactoryTalk® AssetCentre Agent

- FactoryTalk® AssetCentre Client

Rockwell Automation understands that customers desire to know the ports used by our architecture, as it is something necessary to perform Risk Analysis/Threat Models on their architecture, and minimize the number of ports must be opened across a firewall in a more secure environment. This document is meant to show the ports, services, and firewall rules necessary for FactoryTalk® AssetCentre components to function properly. Keep in mind that additional ports must stay open because DCOM and dynamic ports are a requirement between the machines running various FactoryTalk® software applications (such as Studio 5000 Logix Designer®).

Note: Rockwell Automation recommends turning off IPV6 for FactoryTalk® network applications. Rockwell Automation products only support IPV4.

Network Firewalls general recommendations

Any firewalls (both physical and virtual) must allow the ports and protocols listed in the document to be open. Additionally, be sure that typical LAN speeds can be maintained, and no connectivity or latency issues were created.