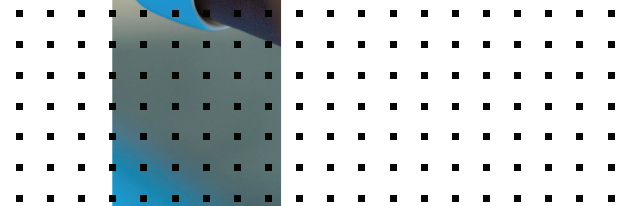


DEPLOYMENT GUIDE

# Fortinet FortiGate and Nozomi Networks Guardian



# Table of Contents

Overview . . . . .	3
Deployment Prerequisites . . . . .	3
Version Compatibility . . . . .	3
Licensing . . . . .	3
Deployment . . . . .	3
Architecture Overview . . . . .	3
FortiGate Configuration . . . . .	4
Interfaces . . . . .	4
Protocol Service . . . . .	7
Policy . . . . .	7
Create User for Nozomi Network's Guardian . . . . .	8
Nozomi Networks Configuration . . . . .	9
Enable FortiGate + Nozomi Networks Configuration. . . . .	9
Preparing the Integration for Testing and Deployment . . . . .	10
Placing Guardian in Learning Mode . . . . .	10
Placing the System in Protecting Mode . . . . .	11
Testing the Integration and Deployment . . . . .	11
References . . . . .	11



## Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at <https://www.fortinet.com>, the Fortinet Blog, or FortiGuard Labs.

## About Nozomi

Nozomi Networks is a leading provider of real-time visibility, advanced monitoring capabilities, and strong security for industrial control networks supporting critical infrastructure. Built by a team of industrial control systems (ICS) and network security expertise, Nozomi Networks' Guardian appliances and software inspect industrial networks non-intrusively and apply machine-learning (ML) with Artificial Intelligence (AI) technology to provide unique insight into the topology, devices, and behaviors present in it.

Industrial control systems have strict and unique environments that require security to be the top priority. In this document, we will look at the integration of Fortinet's FortiGate to Nozomi Networks' Guardian appliance, to bring the power of the Security Fabric to the industrial control systems.

## Version Compatibility

This Deployment and Integration Guide applies to FortiGates with FortiOS v5.4 and 5.6, and with Nozomi Networks' Guardian v17.0.0. This guide will assume the integration with FortiOS 5.6.

## Licensing

For licenses to the Nozomi Networks' Guardian, please contact Nozomi Networks respective sales team. <http://www.nozominetworks.com/company/contact-us.html>

## Deployment

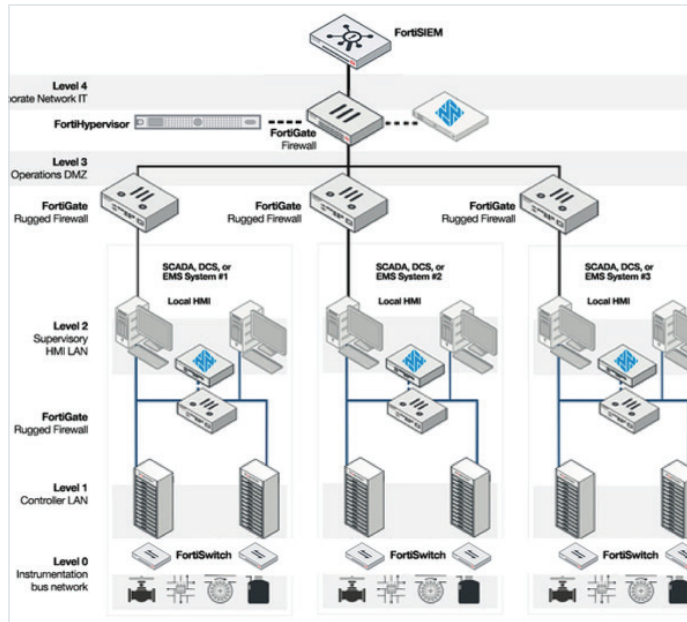
### Architecture Overview

This is an example of what a supervisory control and data acquisition (SCADA) network may look like, where the FortiGate and the Guardian are located as a point of convergence between the IT and the OT networks (and/or the process and OT networks).

## Deployment Prerequisites

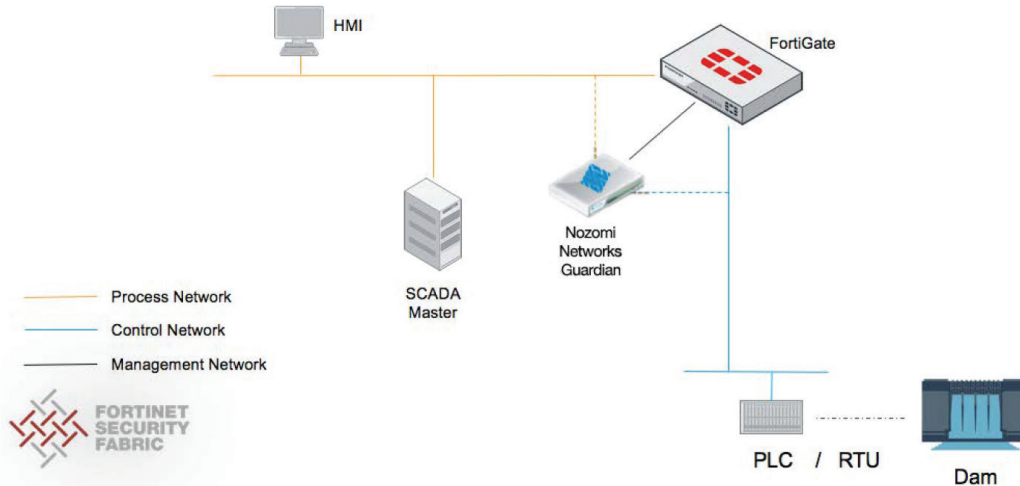
- FortiGate
- FortiSwitch
- Nozomi Networks' Guardian
- An ICS environment with IT and OT networks





The FortiGate sits in-line between the IT and the OT networks, and within the local environments of each OT network themselves—actively controlling traffic between the IT network and the OT network. The Nozomi Networks’ Guardian is connected in SPAN/port mirroring mode behind the respective switches, having visibility of network traffic of both networks.

For the purpose of this Integration Guide, we will focus on a single segment.



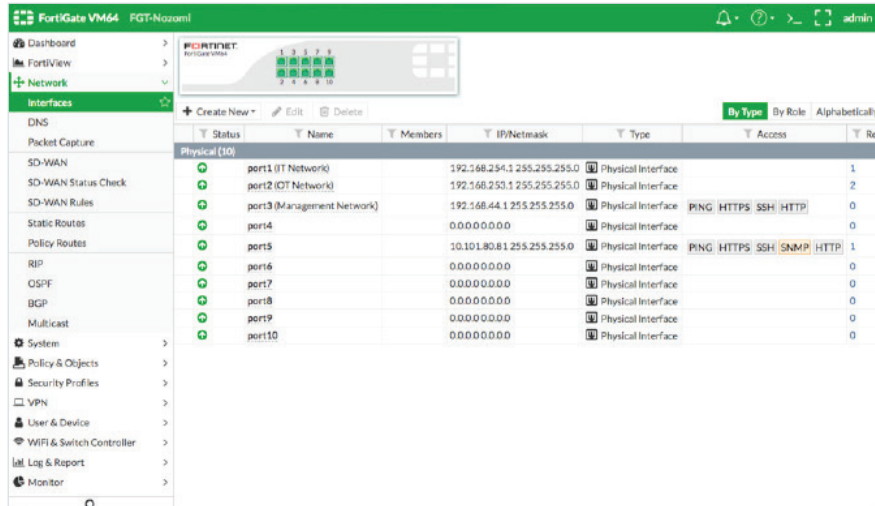
The communication between the FortiGate and the Guardian occurs over the Security Fabric via the management network.

### FortiGate Configuration

On the FortiGate, there are three basic requirements for the FortiGate to be in-line between the IT network and the OT network, and to be integrated with the Guardian. There are three interfaces to be configured, one service, and one policy.



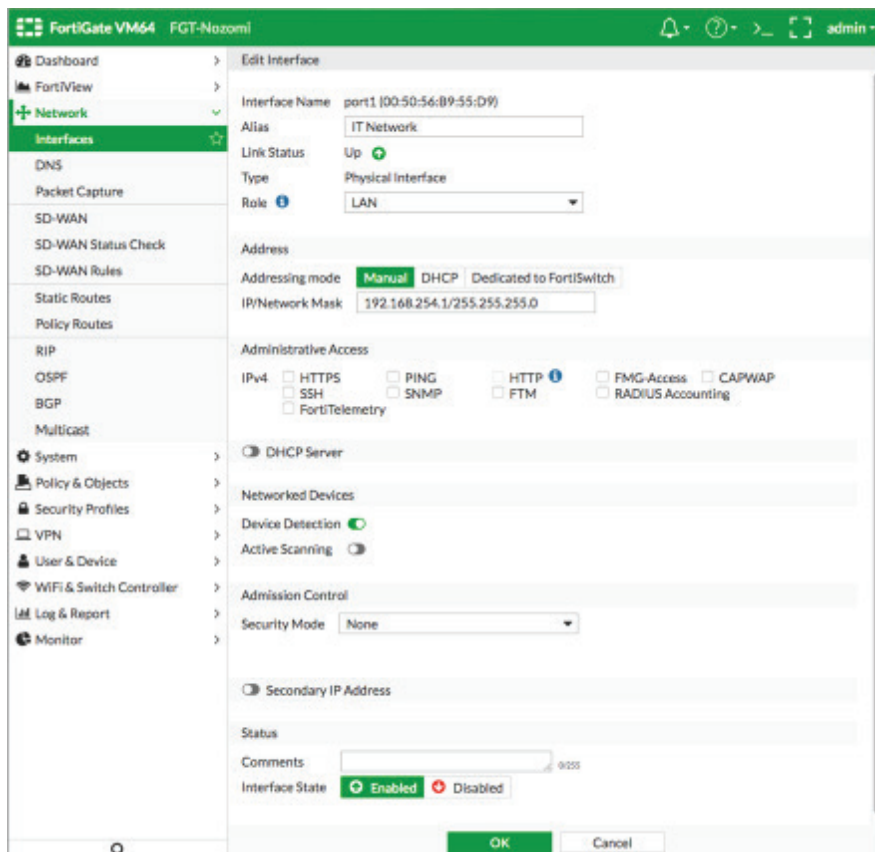
## Interfaces



	Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (10)							
SD-WAN	Up	port1 (IT Network)		192.168.254.1/255.255.255.0	Physical Interface		1
SD-WAN Status Check	Up	port2 (OT Network)		192.168.253.1/255.255.255.0	Physical Interface		2
SD-WAN Rules	Up	port3 (Management Network)		192.168.44.1/255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	0
Static Routes	Up	port4		0.0.0.0/0.0.0.0	Physical Interface		0
Policy Routes	Up	port5		10.101.80.81/255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP	1
RIP	Up	port6		0.0.0.0/0.0.0.0	Physical Interface		0
OSPF	Up	port7		0.0.0.0/0.0.0.0	Physical Interface		0
BGP	Up	port8		0.0.0.0/0.0.0.0	Physical Interface		0
Multicast	Up	port9		0.0.0.0/0.0.0.0	Physical Interface		0
	Up	port10		0.0.0.0/0.0.0.0	Physical Interface		0

### 1. IT Network

A port on the FortiGate is required to be configured for the IT network on a dedicated subnet. Ensure that no Administrative Access options are enabled for this port. ICS environments require tightly secured networks. As such, the least possible administrative access to the interface is recommended.



FortiGate VM64 FGT-Nozomi

Dashboard FortiView Network Interfaces

Interface Name: port1.100-50-56:09-55:D9

Alias: IT Network

Link Status: Up

Type: Physical Interface

Role: LAN

Addressing mode: Manual DHCP Dedicated to FortiSwitch

IP/Network Mask: 192.168.254.1/255.255.255.0

Administrative Access:

IPv4:  HTTPS  PING  HTTP  FMG-Access  CAPWAP  
 SSH  SNMP  FTM  RADIUS Accounting  
 FortiTelemetry

DHCP Server

Networked Devices

Device Detection:

Active Scanning:

Admission Control

Security Mode: None

Secondary IP Address

Status

Comments:

Interface State:  Enabled  Disabled

OK Cancel

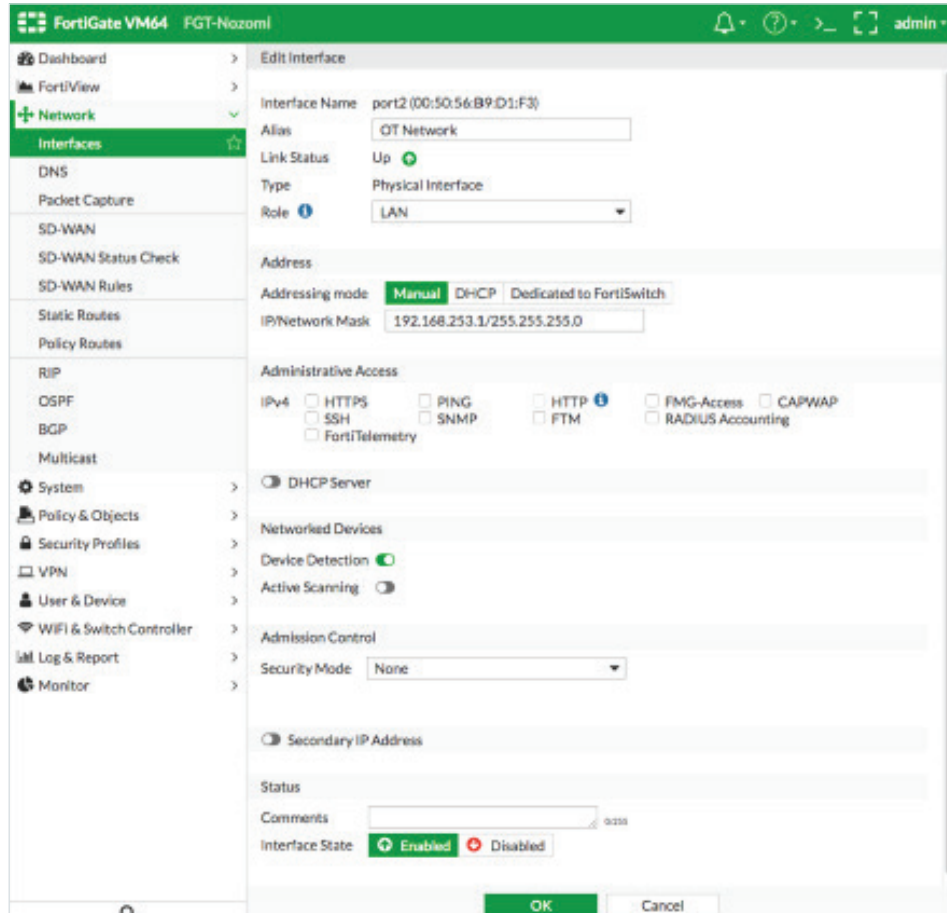
Also ensure that the **“Active Scanning”** option is **disabled**, as this creates unnecessary noise on the network, which may impede the integration with the Guardian.

This port will act as the gateway of the IT network.



## 2. OT Network

Similarly, a port on the FortiGate is required to be configured for the OT network on a dedicated subnet. Ensure that no Administrative Access options are enabled for this port. ICS environments require tightly secured networks. As such, the least possible administrative access to the interface is recommended.



Also ensure that the **“Active Scanning”** option is disabled, as this creates unnecessary noise on the network, which may impede the integration with the Guardian.

This port will act as the gateway of the OT network.

## 3. Management Network

A management network needs to be created on which the FortiGate will communicate with the Guardian and from which it can be managed.



## Protocol Service

Create services for your environment's required protocols.

Typically, these are SCADA-oriented protocols such as MODBUS, DNP3, Profibus, FIP, etc. In this example we are creating a service for the MODBUS protocol.

Service Name	Category	Details	IP/FQDN	Show in Service List	Ref.
ALL	General	ANY		<input checked="" type="checkbox"/>	59
ALL ICMP	General	ICMP/ANY		<input checked="" type="checkbox"/>	0
ALL TCP	General	TCP/1-65535	0.0.0.0	<input checked="" type="checkbox"/>	0
ALL UDP	General	UDP/1-65535	0.0.0.0	<input checked="" type="checkbox"/>	0
<b>Web Access (2)</b>					
HTTP	Web Access	TCP/80	0.0.0.0	<input checked="" type="checkbox"/>	1
HTTPS	Web Access	TCP/443	0.0.0.0	<input checked="" type="checkbox"/>	2
<b>File Access (8)</b>					
AFS3	File Access	TCP/7000-7009 UDP/7000-7009	0.0.0.0	<input checked="" type="checkbox"/>	0
FTP	File Access	TCP/21	0.0.0.0	<input checked="" type="checkbox"/>	0
FTP_GET	File Access	TCP/21	0.0.0.0	<input checked="" type="checkbox"/>	0
FTP_PUT	File Access	TCP/21	0.0.0.0	<input checked="" type="checkbox"/>	0
NFS	File Access	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	<input checked="" type="checkbox"/>	0
SAMBA	File Access	TCP/139	0.0.0.0	<input checked="" type="checkbox"/>	1
SMB	File Access	TCP/445	0.0.0.0	<input checked="" type="checkbox"/>	1
TFTP	File Access	UDP/69	0.0.0.0	<input checked="" type="checkbox"/>	0

Name this service "Modbus" and select Protocol Type as TCP/UDP/SCTP and Destination Port as "TCP" and port 502. Click OK.

**Edit Service**

Name:

Comments:

Show in Service List:

Category:

**Protocol Options**

Protocol Type:

Address:

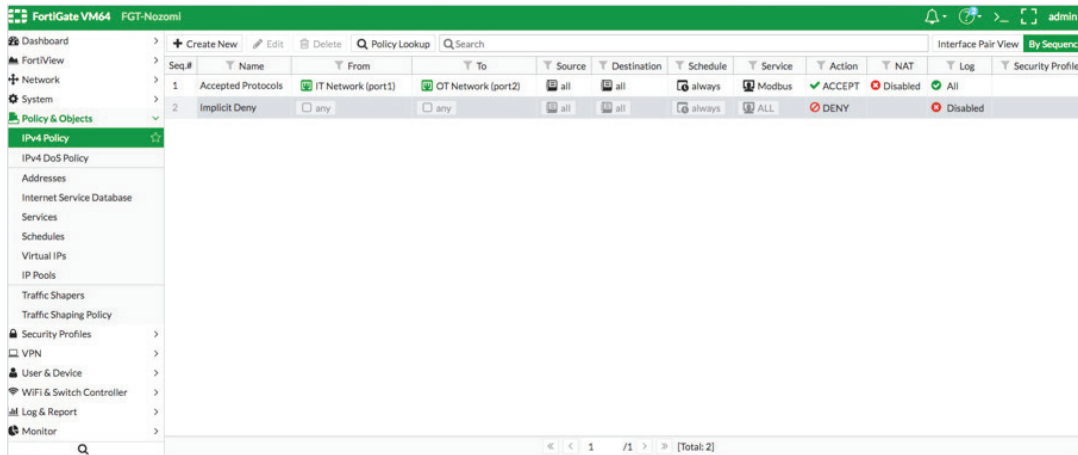
Destination Port:

Specify Source Ports:

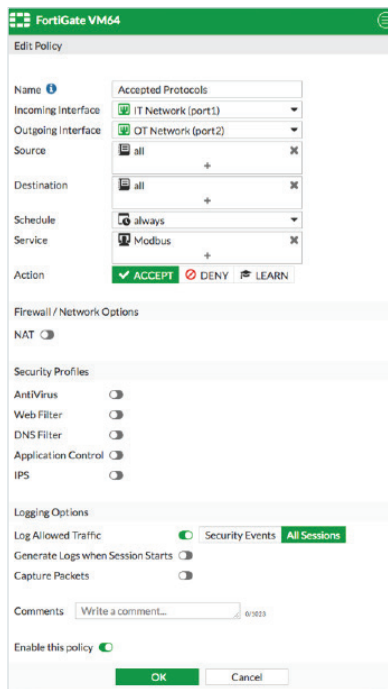
## Policy

Creation of one policy is required for traffic coming in from the IT network to the OT network, allowing only the protocol services created from the previous step. Ensure that NAT is disabled, and for the purpose of analysis of incidents, enable all logging.





Please follow the screenshot for the settings for the policy.



## Create User for Nozomi Networks' Guardian

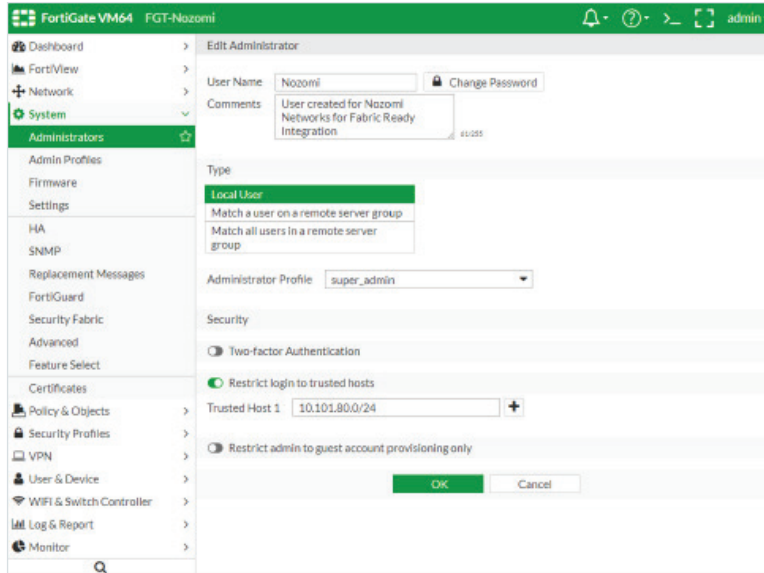
Create a new user for the Nozomi Networks' Guardian to access the FortiGate for the integration.

Go to System > Administrators and click on "Create New." Enter the details for the user account and enter the details as shown in the screenshot below.

1. Enter the User Name, Password, and Comments.
2. Select the Type of the user to be "Local User."
3. Set Administrator Profile to "super\_admin."
4. Enable Restrict login to trusted hosts and put in the IP of the Nozomi Networks' Guardian.
5. Click **OK**.







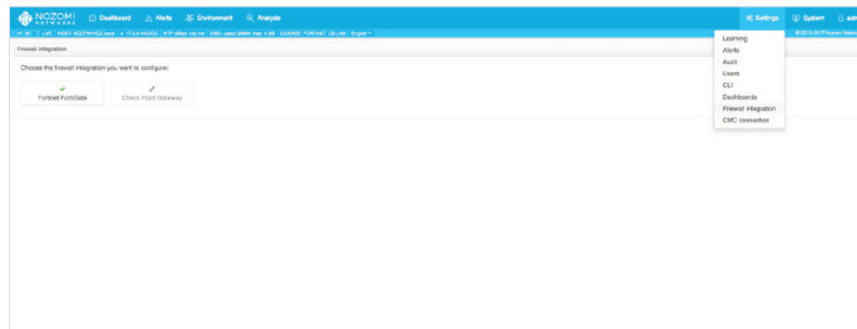
## Nozomi Networks Configuration

The configuration on the Guardian requires connectivity to the management interface and all the security integration options enabled. Ensure that the management interface of the Nozomi Networks' Guardian can reach using protocol ssh on port 22 the management

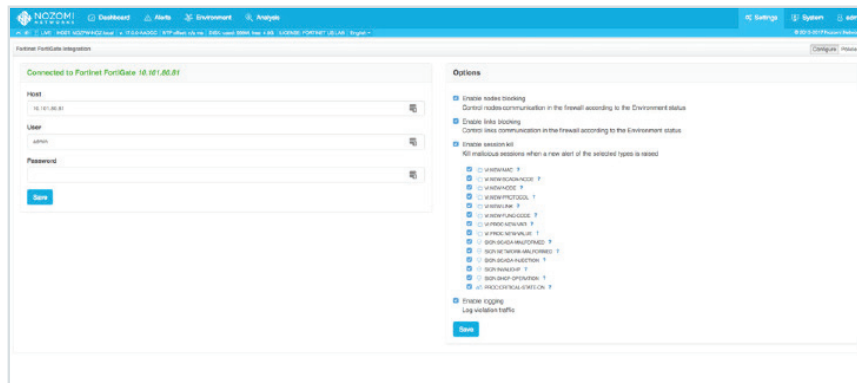
Ensure that the Guardian is connected to a switch for the IT network and the OT network in SPAN/mirrored ports. This gives the Guardian visibility of the SCADA traffic between the networks.

## Enable FortiGate + Nozomi Networks Configuration

1. Under Settings > Firewall Integration, choose "Fortinet FortiGate."



2. Insert the IP address of the management interface of the FortiGate and the user with the password created on the FortiGate for the integration.



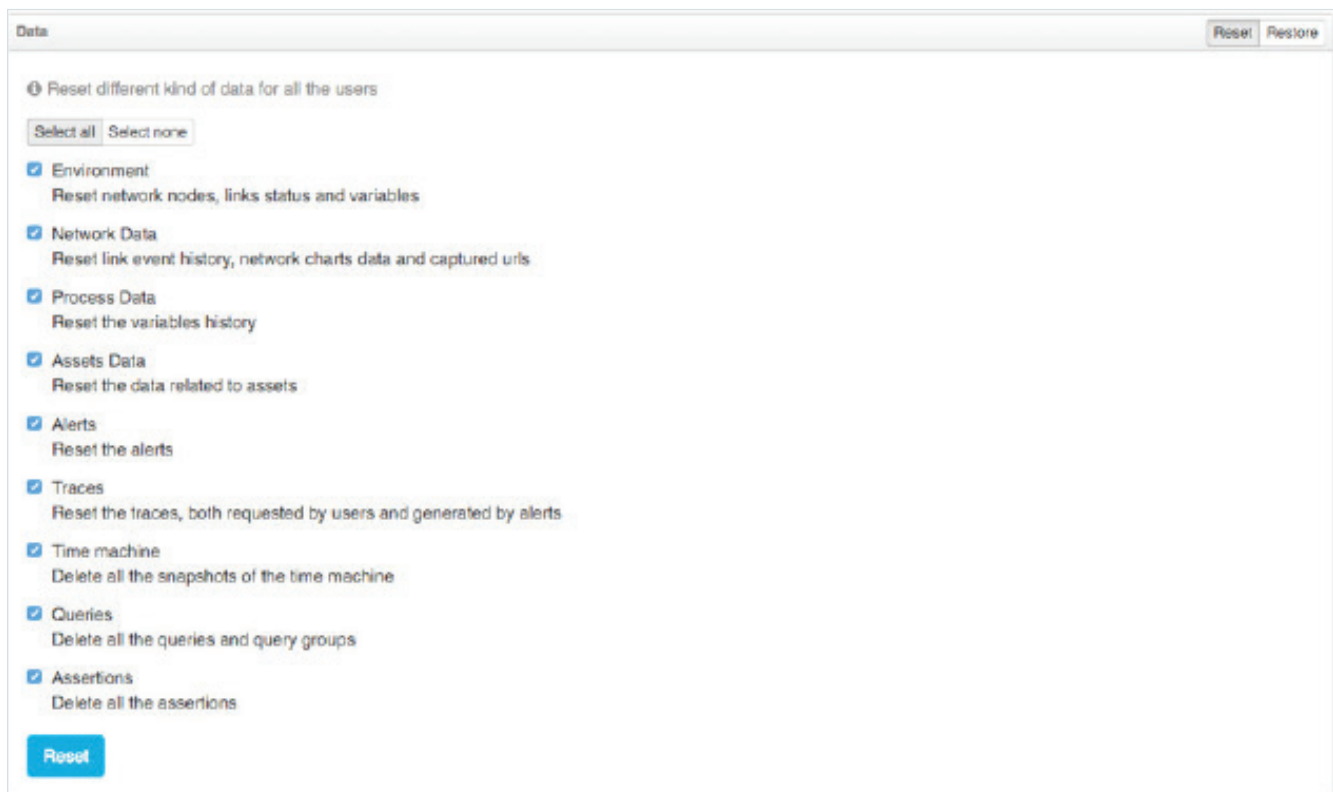
## Preparing the Integration for Testing and Deployment

The Nozomi Networks' Guardian works on the basis of behavioral analysis and machine learning. When a Guardian is placed in a new environment, the appliance has to be put in the "Learning" state, prior to live production deployment, for a designated amount of time prior to enabling Protecting mode.

### Placing Guardian in Learning Mode

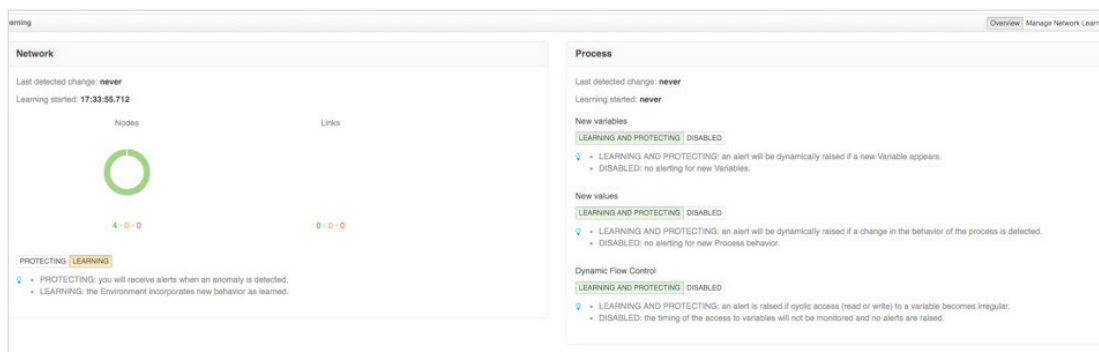
To ensure that the Guardian is in Learning mode, all prior data must first be reset to a clean state:

1. Log in to the Guardian.
2. Go to System → Data.
3. Clear all settings by clicking on "Select all."
4. Click on "Reset" and enter your password.



This will ensure that the appliance is started from a clean state with no prior learning.

To ensure that the system is in Learning mode:



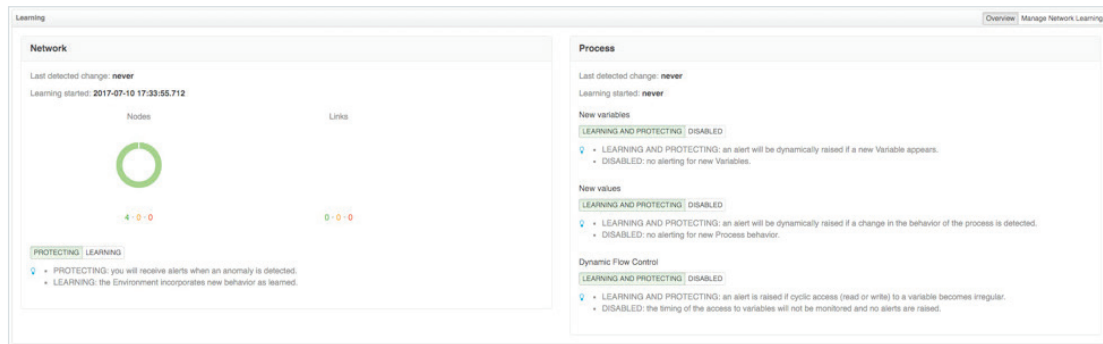
1. Log in to the Guardian.
2. Ensure that both the Network and Process sections have “Learning” selected. Here, you will be able to see the amount of time since the system has been in Learning mode.

## Placing the System in Protecting Mode

Once the Guardian has been in Learning mode for an appropriate amount of time, it can now be put into “Protecting” mode to begin actively monitoring the ICS environment.

To put the system into Protecting mode:

1. Click on “Settings” and go to “Learning.”
2. Under the “Network” section, click on “Protecting.”



## Testing the Integration and Deployment

Before testing the integration, you should ensure that the Guardian’s baseline and the learning phase is completed.

To test the Integration, please refer to the Nozomi Networks Integration Video to replicate the scenarios.

## References

1. FortiGate/FortiOS Admin Guides  
<http://docs.fortinet.com/fortigate/admin-guides>
2. Nozomi Networks Guardian Data Sheet  
<http://www.nozominetworks.com/downloads/US/Nozomi-Networks-SG-Data-Sheet.pdf>
3. Nozomi Networks Guardian Resources  
<http://www.nozominetworks.com/resources.html>
4. Fortinet User Community  
<https://fuse.fortinet.com>

