



Pulse Policy Secure: Nozomi Networks

Integration Guide

Product Release	9.1R8
Published	July 2020
Document Version	1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: Nozomi Networks

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

NOZOMI NETWORKS INTEGRATION USING HTTP ATTRIBUTE SERVER	3
PURPOSE OF THIS GUIDE	3
PREREQUISITES.....	3
USE CASES	3
CONFIGURING HTTP ATTRIBUTE SERVER	3
PPS AND NOZOMI NETWORKS INTEGRATION.....	5
OVERVIEW	5
CONFIGURING PPS WITH NOZOMI NETWORKS	6
PROFILER AND NOZOMI NETWORKS INTEGRATION	10
CONFIGURING NOZOMI NETWORKS AS COLLECTOR.....	10
TROUBLESHOOTING	11
APPENDIX	12
ALERT BASED ADMISSION CONTROL USING NOZOMI NETWORKS	13
OVERVIEW.....	13
DEPLOYMENT OF PPS WITH NOZOMI NETWORKS SCADAGUARDIAN.....	13
CONFIGURING PPS WITH NOZOMI NETWORKS.....	14
ADMISSION CONTROL TEMPLATE.....	15
ADMISSION CONTROL POLICIES.....	16
ADMISSION CONTROL CLIENT.....	18
CONFIGURING NOZOMI NETWORKS SCADAGUARDIAN	19
TROUBLESHOOTING	20
EVENT TYPES SUPPORTED BY NOZOMI NETWORKS.....	21
REQUESTING TECHNICAL SUPPORT.....	26
SELF-HELP ONLINE TOOLS AND RESOURCES.....	26
OPENING A CASE WITH PSGSC.....	26
REPORTING DOCUMENTATION ISSUES.....	27

Nozomi Networks Integration using HTTP Attribute Server

Purpose of this Guide

This guide describes how Pulse Policy Secure (PPS) fetches Operational Technology (OT) device attributes from Nozomi Networks and use them in role mapping rules to provide network segmentation. The Profiler can fetch the OT device information for visibility purpose. It also describes about how Pulse Policy Secure(PPS) and Nozomi Networks together can provide threat detection and threat response in ICS/OT environment using Admission Control.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

- Pulse Policy Secure at version 9.1R8.
- Nozomi Networks

Use Cases

The following use cases are supported with PPS and Nozomi networks integration:

1. Role Based Access Control (RBAC) for the endpoints based on the device attributes received from HTTP attribute server (Nozomi Networks).
2. Periodic compliance check for the endpoint using HTTP attribute server.
3. OT devices can be profiled using Profiler.

Configuring HTTP Attribute Server

The default Nozomi Networks template provides the list of possible attributes that can be received from the network security device along with attribute value. The template also provides possible actions that can be taken for an attribute. PPS is loaded with default template for Nozomi Networks.

Note: This configuration is common for both PPS and Profiler.

To add the HTTP Attribute server in PPS:

1. Select **Authentication > Auth.Servers**, select **HTTP Attribute Server** under **New** and Click **New Server**.
2. Enter the name.
3. Select **Nozomi Networks-SCADAguardian-ICS Security Solution** as template.
4. Enter the IP address or hostname of Nozomi Networks server.

5. Enter the user name and password (Admin credentials of Nozomi Networks).
6. Enter the backup host name/IP address, user name and password.
7. Click **Test Connection** to test connectivity between PPS and Nozomi Networks server.
8. Click **Save Changes**.

Figure 1 HTTP Attribute Server

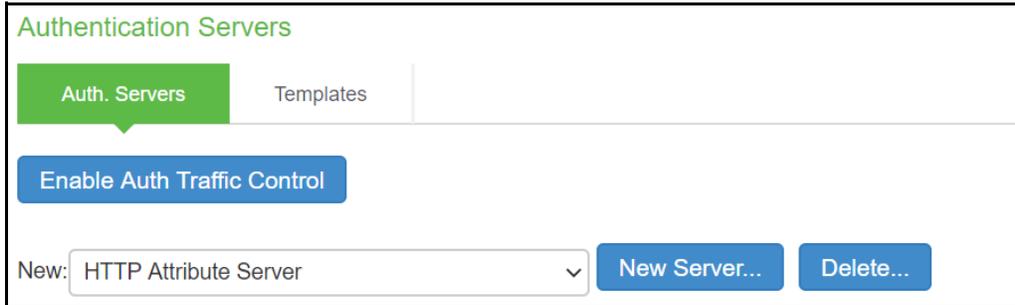


Figure 2 Template

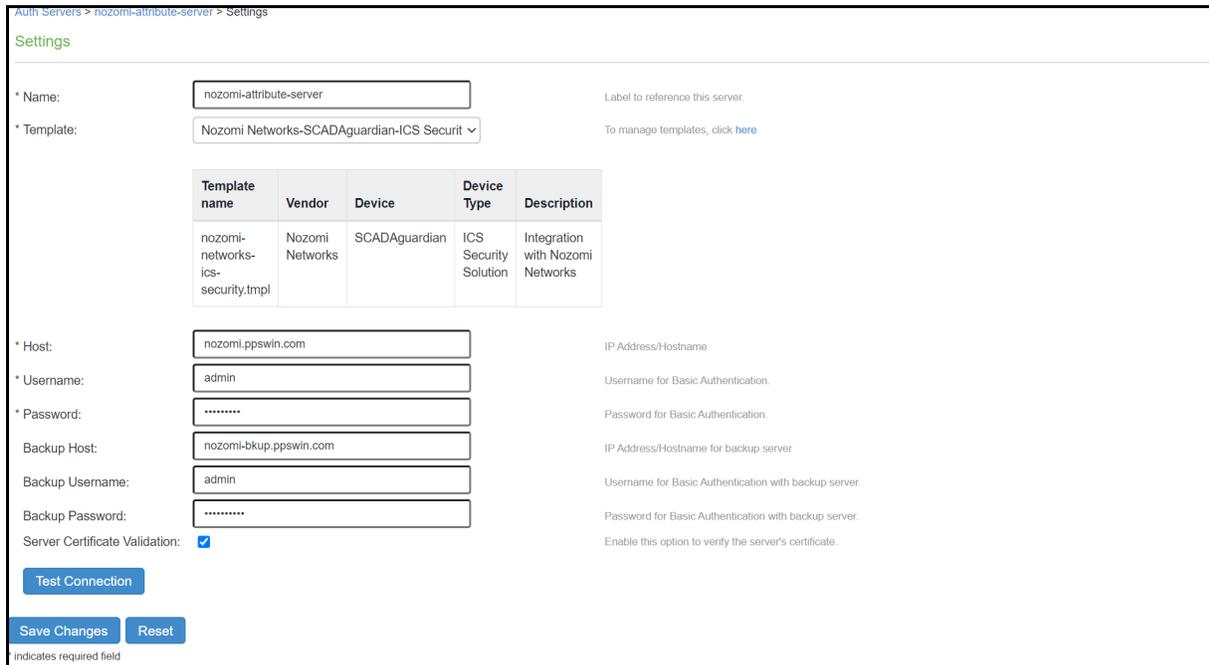


Figure 3 Available Templates

	Name	File Name	Vendor	Device	Device Type
1	nozomi-networks-ics-security.tpl <small>Integration with Nozomi Networks</small>	nozomi-networks-ics-security.tpl	Nozomi Networks	SCADAguardian	ICS Security Solution
2	mcafee-epo-endpoint-protection.tpl <small>Integration with McAfee ePO</small>	mcafee-epo-endpoint-protection.tpl	McAfee	McAfee ePolicy Orchestrator	Endpoint Protection Platform

Note:

- A subset of attributes supported by Nozomi Networks is added in the default template. A new template can be created by Admin and has to be uploaded on PPS for supporting any additional attributes apart from the one's in the default template.
- Nozomi Networks does not support more than 4 simultaneous TCP connections (See Nozomi Documentation for more details). During high load, PPS may establish more than 4 connections. Hence, it is recommended to use Profiler as a device attribute server (with Nozomi Networks as a collector) to overcome this limitation.

PPS and Nozomi Networks Integration

- [Overview](#) 5
- [Configuring PPS with Nozomi Networks](#) 6

Overview

Nozomi Networks has the capability to fetch details of ICS devices managed by Operational Technology. Operational technology devices include valves, transmitters, switches, sensors and actuators. These devices rely on custom protocols for managing and communication.

Nozomi Networks provides detailed information about OT devices like device category, OS, manufacturer, firmware version and so on. PPS integration with Nozomi Networks allows the retrieval of OT device details and use them for network segmentation by assigning enforcement policies based on VLAN or ACLs.

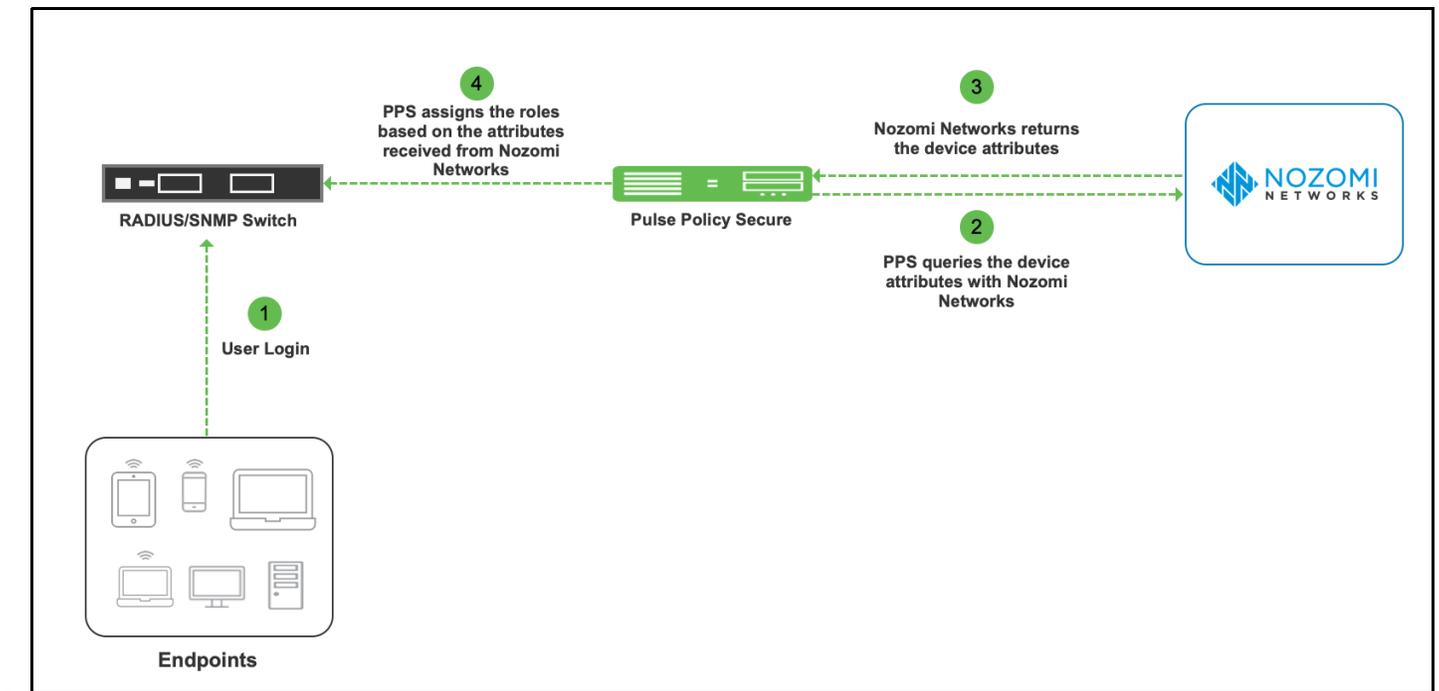
This section describes how to integrate Nozomi Networks device with PPS.

The authentication process is described below when PPS is configured for MAC address authentication:

1. Whenever a device tries to connect to the network, MAC Authentication request is generated to PPS. PPS can query Nozomi Networks for device attributes using device identifier like MAC address.
2. The retrieved attributes can be used in role mapping rules to determine role of the device. Based on the assigned role, device can be put in specific VLAN or ACL policies can be applied.
3. PPS periodically queries the Nozomi Networks for change in attributes and assigns the role accordingly.

Figure 4 PPS Nozomi Integration

Summary of



Configuring PPS with Nozomi Networks

A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.
 - Configure Nozomi Networks as HTTP attribute server in PPS.
 - Configure the Switches/WLC as RADIUS Client in PPS (Endpoint Policy > Network Access > Radius Clients > New Radius Client). Switch should be configured with PPS as a RADIUS server.
 - Configured HTTP attribute server has to be mapped as a "Device Attributes" under the realm configuration and role mapping rules can be used to assign the roles based on the attributes received from the attribute server.
1. Configure Nozomi Networks as HTTP attribute server in PPS ["Configuring HTTP Attribute Server" on page 3](#)
 2. Select **Endpoint Policy > MAC Address Realms**, click New to create the authentication realm. Under Device Attributes, select the Nozomi HTTP attribute server created earlier or **User Realms > Users > General**, select the Nozomi Networks server created in Device Attributes

Figure 5 MAC Address Realms

MAC Address Realms > Device attribute based MAC Realm > General

General Authentication Policy Role Mapping

* Name: Device attribute based MAC Label to reference this realm

Description:

When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: MAC Address Server Specify the server to use for authenticating users.

User Directory/Attribute: Same as above Specify the server to use for authorization.

Accounting: None Specify the server to use for Radius accounting.

Device Attributes: nozomi-attribute-server Specify the server to use for devices authorization.

Device Check Interval: 10 minutes Specify the interval to check device attributes server. disable=0, min=10, max=10080 minutes

▼ Dynamic policy evaluation

Enable dynamic policy evaluation

▼ Other Settings

Authentication Policy: Password restrictions

Role Mapping: Host Checker restrictions
2 Rules

[Save Changes](#)

* indicates required field

- Configure rules based on Device Attributes from **Endpoint Policy > MAC Address Realms** and click **Role Mapping > Role Mapping Rule**. Create a new rule, select Rule based on: **Device Attribute** and click **Update** or **User Realms > Users > Role Mapping > Role Mapping Rule**.

Figure 6 Device Attributes

MAC Address Realms > Device attribute based MAC Realm > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: Device attribute

* Name:

▼ Rule: If device has any of the following attribute values...

Attribute: (Select an attribute)

If more than one value for this attribute should match, enter one per line. You can use * wildcards

▼ then assign these roles

Available Roles:

- blockRole
- Eng
- Guest Admin
- Guest Sponsor
- Guest Wired Restricted
- Guest full access

Stop processing rules

To manage roles, see the [Roles](#)

Selected Roles:

- category
- firmwareVersion
- firstActivityTime
- hostname
- ip
- isBroadcast
- isConfirmed
- isDisabled
- isFullLearned
- isLearned

Figure 7 Role Mapping Rule

MAC Address Realms > Device attribute based MAC Realm > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name:

▼ Rule: If device has any of the following attribute values...

Attribute:

If more than one value for this attribute should match, enter one per line. You can use * wildcards.

▼ then assign these roles

Available Roles:

- Agentless_full_role
- Agentless_rem_role
- blockRole
- Eng
- Guest Admin

Selected Roles:

- Compliant

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

*indicates required field

- Click **Save Changes**.

Once the role mapping rule is created. You can see the summary page as shown below. The following page shows the different rules created with the corresponding roles assigned.

Figure 8 Summary

MAC Address Realms > Device attribute based MAC Realm > Role Mapping

Role Mapping

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. device attribute "category" is "OT**"	→ Compliant	rule1	✓
<input type="checkbox"/>	2. username is ""	→ QuarantineRole	rul2	

Note: MAC Address is used as a device identifier to query attributes from Nozomi Networks. Without Host Checker, PPS doesn't learn the MAC address. For agent less sessions, Host Checker should be enabled to learn MAC address. For Agentless sessions/logs, pre-auth Host Checker must be enabled.

Profiler and Nozomi Networks Integration

The Nozomi Networks is configured as a HTTP Attribute Server and is available under Device Attribute Server settings. The server is manually selected as an active collector to collect information that is used to classify and categorize the devices. The attributes information helps for role mapping.

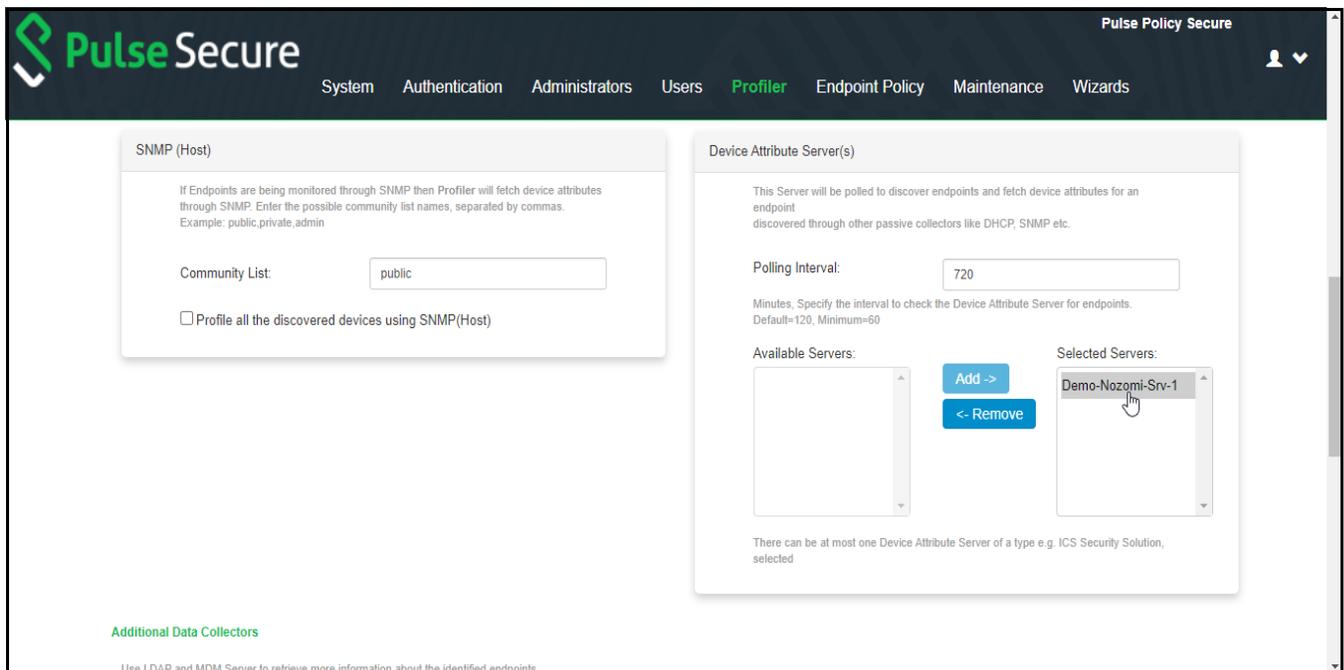
Note: The collector can only read devices that have a confirmed MAC address and are stored in the Profiler.

Configuring Nozomi Networks as Collector

To configure Nozomi Networks as a device attribute server to perform as an active collector:

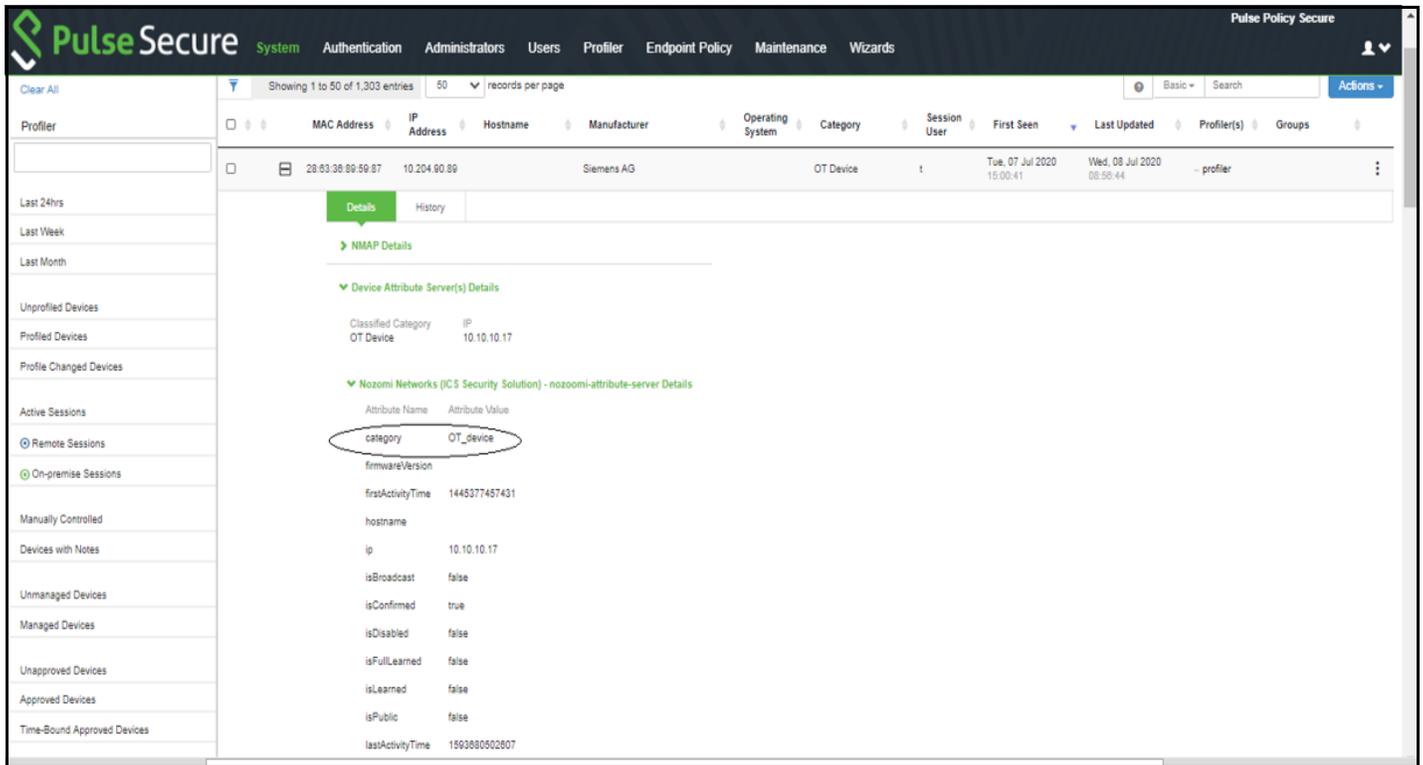
1. Configure Nozomi Networks as HTTP attribute server in PPS “[Configuring HTTP Attribute Server](#)” on [page 3](#)
2. Under **MAC Address Realms** or **User Realms**, select the Nozomi HTTP attribute server created in Device Attributes.
3. Navigate to **Profiler > Profiler Configuration > Advance Configuration**. Under Device Attribute Server, select the HTTP server as the device attribute server.

Figure 9 Configure Device Attribute Server



The DDR page displays the endpoint information collected by Nozomi collector.

Figure 10

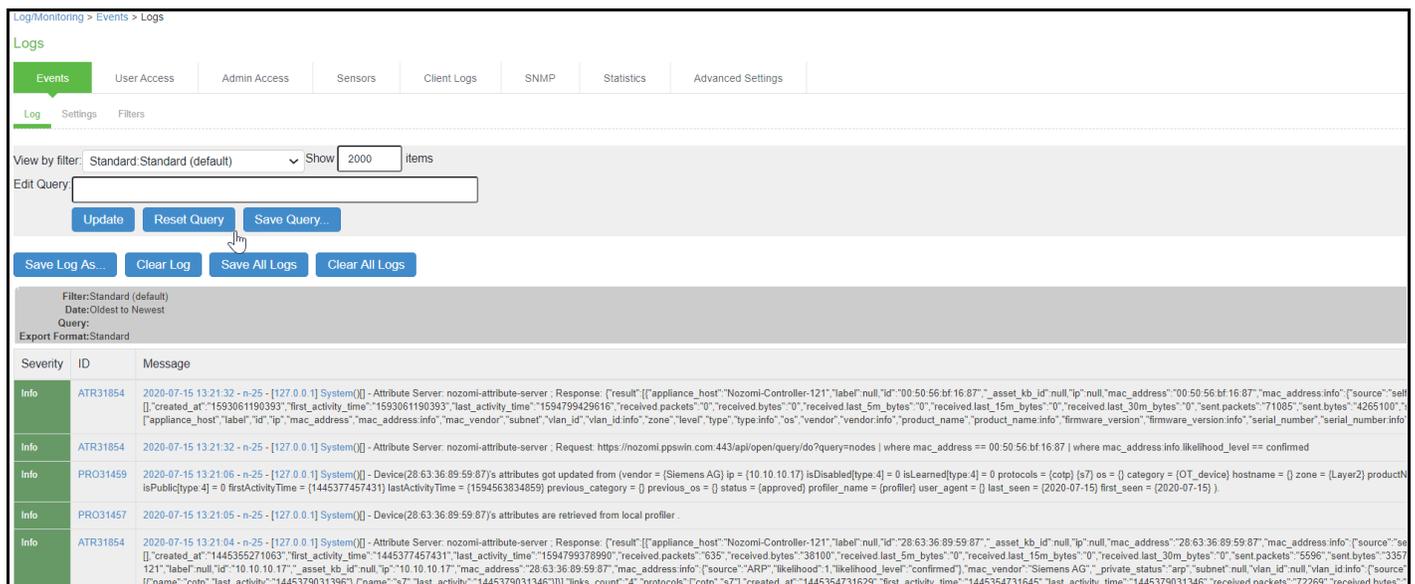


Troubleshooting

To verify the event logs on PPS, select System > Log/Monitoring > Events. You can verify that the event logs are generated every time when an event is received from Nozomi Networks.

To verify the user access logs, select System > Logs & Monitoring > User Access to verify the user login related logs like realm, roles, username and IP address.

Figure 11 Event Logs



You can also enable debug logs to troubleshoot any issues. Select Maintenance > Troubleshooting > Monitoring > Debug Log to enable debug logs.

Maintenance > Troubleshooting > User Session > Policy Tracing can be used to see which attributes are fetched from Nozomi Attribute Server or Profiler.

Appendix

Attributes exposed by the default Nozomi Networks template. Admin can add more attributes to the list by creating a new template and uploading it to PPS. PPS performs normalization of few attributes as used and displayed by Profiler. These attributes are category, hostname, manufacturer, ip, os, and macaddr.

```
"attributes" : [
  {"type" : "category"},
  {"label" : "hostname"},
  {"mac_vendor" : "manufacturer"},
  {"ip" : "ip"},
  {"os" : "os"},
  {"mac_address" : "macaddr"},
  {"vendor" : "vendor"},
  {"level" : "level"},
  {"roles" : "roles"},
  {"firmware_version" : "firmwareVersion"},
  {"product_name" : "productName"},
  {"level" : "level"},
  {"zone" : "zone"},
  {"is_broadcast" : "isBroadcast"},
  {"is_public" : "isPublic"},
  {"reputation" : "reputation"},
  {"is_confirmed" : "isConfirmed"},
  {"is_learned" : "isLearned"},
  {"is_disabled" : "isDisabled"},
  {"is_fully_learned" : "isFullLearned"},
  {"first_activity_time" : "firstActivityTime"},
  {"last_activity_time" : "lastActivityTime"}
]
```

Alert Based Admission Control using Nozomi Networks

- [Overview](#) 13
- [Deployment of PPS with Nozomi Networks SCADAguardian](#) 13
- [Configuring PPS with Nozomi Networks](#) 14
- [Configuring Nozomi Networks SCADAguardian](#) 19
- [Troubleshooting](#) 20

Overview

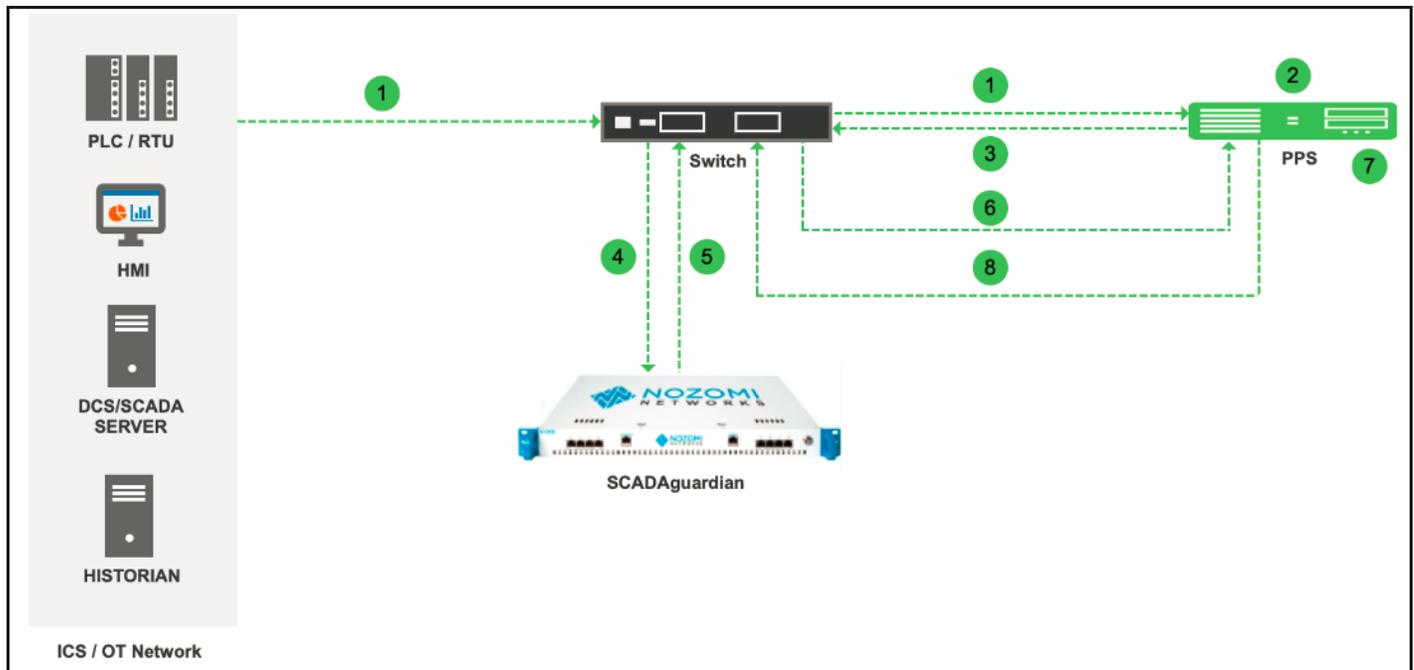
Nozomi Networks provides industry leading solution for real-time cyber security and visibility for Industrial Control Networks. It provides superior network and operational visibility and advanced threat detection Industrial Control System (ICS). Nozomi Networks SCADAguardian uses behavior based anomaly detection and multiple types of signature and rule based detection. SCADAguardian also generates different kinds of alerts when potentially dangerous conditions are met. These alerts are originated from different engines (Protocol Validation, Learned Behaviour, Built-in checks, Custom checks) in SCADAguardian.

Pulse Policy Secure(PPS) can be deployed in ICS/OT network to provide authentication and access control. PPS can consume alerts generated by Nozomi Networks SCADAguardian and takes appropriate action to restrict access of anomalous device \ endpoint.

Deployment of PPS with Nozomi Networks SCADAguardian

This section describes the integration of PPS with Nozomi Networks. PPS receives the threat alert information from Nozomi networks solution and takes an action at the endpoint based on the admission control policies.

Figure 12 Deployment of PPS with Nozomi Networks



CS security vendors such as Nozomi Networks are deployed to passively analyse industrial protocol communication for automatic asset discovery and threat detection.

1. The device connects to PPS through Switch.
2. The device session is created on the PPS.
3. The device access details are pushed to Switch using ACL.
4. The Nozomi Networks SCADAguardian monitors the device traffic.
5. The Nozomi Networks SCADAguardian generates the syslog messages for the device.
6. The syslog message is sent to PPS if any suspicious traffic or activity is detected from the device.
7. Pulse Policy Secure(PPS) processes the received syslog message and actions are taken based on the configured policies.
8. New/Updated ACL details are pushed to Switch for updating the enforcement of the device.

Configuring PPS with Nozomi Networks

The network security devices are configured with PPS for admission access control. A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.
- Configure Nozomi Networks SCADAguardian as a client in PPS.
- Configure PPS details in SCADAguardian

- Configure PPS to block/quarantine the endpoint based on the SCADAguardian admission control template.

This section covers the following topics:

- [“Admission Control Template” on page 15](#)
- [“Admission Control Policies” on page 16](#)
- [“Admission Control Client” on page 18](#)

Admission Control Template

The admission control template provides the list of possible events that can be received from the network security device along with regular expression to parse the message. The template also provides possible actions that can be taken for an event.

Pulse Policy Secure(PPS) is loaded with default templates for SCADAguardian (**nozomi-scadaguardian-cef.itmpl**).

You can view the list of configured integration templates that provides the list of network security devices and the supported protocol type using Endpoint Policy > Admission Control > Templates.

To view the admission control templates:

1. Select **Endpoint Policy > Admission Control > Templates**.

Figure 13 Existing Template

	Name	File Name	Protocol Type	Vendor	Device Type
1	fortigate-text.itmpl Syslog integration with Fortinet Fortigate Firewall using text format messages.	fortigate-text.itmpl	Syslog	Fortinet	Firewall
2	fortianalyzer-text.itmpl Syslog integration with FortiAnalyzer using text format messages.	fortianalyzer-text.itmpl	Syslog	Fortinet	Analyzer
3	fortigate-cef.itmpl Syslog integration with Fortinet Firewall using CEF format messages.	fortigate-cef.itmpl	Syslog	Fortinet	Firewall
4	paloaltonetworksfw-ietf-bsd.itmpl Syslog integration with Palo Alto Networks Firewall using IETF/BSO format messages.	paloaltonetworksfw-ietf-bsd.itmpl	Syslog	Palo Alto Networks	Firewall
5	fortianalyzer-cef.itmpl Syslog integration with Forti Analyzer using CEF format messages.	fortianalyzer-cef.itmpl	Syslog	Fortinet	Analyzer
6	juniper-policy-enforcer-http.itmpl Integration with Juniper's Policy Enforcer which sends endpoint control commands to PPS.	juniper-policy-enforcer-http.itmpl	HTTP	Juniper Networks	Policy Enforcer
7	nozomi-scadaguardian-cef.itmpl Syslog integration with Nozomi Network's SCADAguardian using CEF format messages.	nozomi-scadaguardian-cef.itmpl	Syslog	Nozomi Networks	SCADAguardian

Admin can also create templates and can upload it to PPS.

Admission Control > Templates > nozomi-scadaguardian-cef.itmpl

nozomi-scadaguardian-cef.itmpl

* Name: Label to reference this template.

Description:

Template File: No file chosen Template file

Current Template file:  nozomi-scadaguardian-cef.itmpl

Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity information received from the network security device.

To view and add the new integration policy:

1. Select **Endpoint Policy > Admission Control > Policies**.
2. Click **New Policy**.
3. Enter the policy name.
4. Select **Nozomi Networks-SCADAguardian-Syslog-CEF** as a template.
5. Under **Rule on Receiving**, select the event type severity score. Refer to [Event Types supported by Nozomi Networks 21](#) for more information on supported event types. The event types and the severity score are based on the selected template.
6. Under **then perform this action**, select the desired action.
 - Ignore (log the event) —Received syslog event details are logged on the PPS and no specific action is taken.
 - Terminate user session— Terminates the user session on the PPS for the received messages.
 - Block the endpoint from authenticating to the network — Blocks the endpoint from authenticating to the network.
 - Put the endpoint into a quarantine network by assigning this role — choose the role to put endpoint in quarantine role. Specify whether to apply the role assignment permanently or only for the session.

Note: Admission Control Policy action is not taken for endpoints behind Network Address Translation (NAT).

7. Under **Roles**, specify:
 - Policy applies to ALL roles—To apply the policy to all users.
 - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
 - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.
8. Click **Save changes**.

Figure 14 Configuration Policies

Admission Control > Configure > Policies > polci

polci

* Name: Label to reference this policy.

* Template: Template used by the client

Template name	Vendor	Device	Protocol	Format	Description
nozomi-scadaguardian-cef.itmpl	Nozomi Networks	SCADAguardian	Syslog	CEF	Syslog integration with Nozomi Network's SCADAguardian using CEF format messages.

▼ Rule on receiving

*Events: Events supported

*Severity Score(>=): When Severity Score is greater than or equal to selected value

▼ Count these many times

*Count: (1-256)

▼ then perform this action

Ignore (just log the event)
 Terminate user session
 Block the endpoint from authenticating to the network
 Put the endpoint into a quarantine network by assigning this role:

Make this role assignment

Permanent
 For this session only

▼ Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

* indicates required field

Once the policy is created. You can see the summary page as shown below. The following page shows the different policies created for different events with different user roles.

Admission Control > Configure > Policies

Policies

Configure Templates

Clients Policies

New Policy Duplicate Delete ↑ ↓ Save Changes

10 records per page Search:

	Name	Protocol Type	Vendor	Device Type	Event	Severity	Action	Applies to
<input type="checkbox"/>	1 polci	Syslog	Nozomi Networks	SCADAguardian	Man-in-the-middle attack	1	quarantineEndpoint	All
<input type="checkbox"/>	2 Copy of polci	Syslog	Nozomi Networks	SCADAguardian	Slave sync asked	1	quarantineEndpoint	All

Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

To add a client:

1. Select **Endpoint Policy > Admission Control > Clients**.
2. Click **New Client**.
3. Enter the name of the client.
4. Enter the description.
5. Enter the IP address of the Nozomi client.
6. Select the Protocol Type as Syslog.
7. Select the Vendor as Nozomi Networks.
8. Select Device Type as SCADAguardian.
9. Click **Save Changes**.

Pulse Secure System Authentication Administrators Users Endpoint Policy Maintenance Wizards

Admission Control > Configure > Clients

Clients

Configure Templates

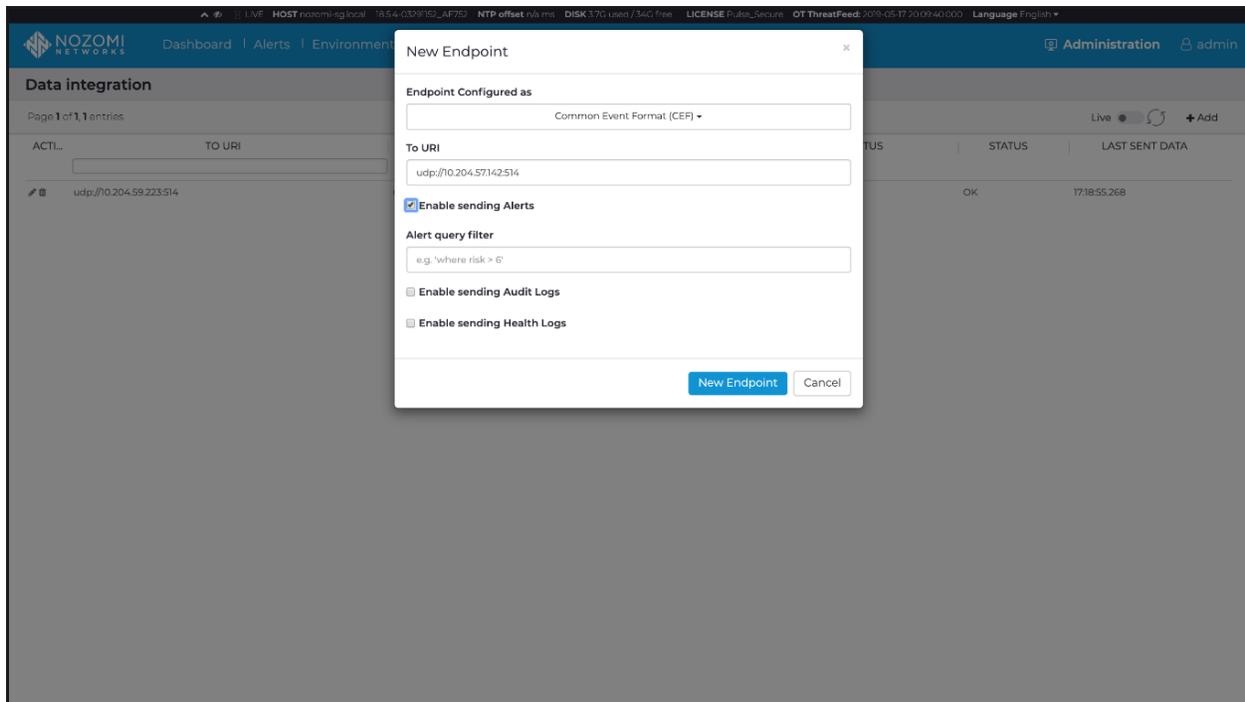
Clients Policies

New Client Duplicate Enable Disable Delete

10 records per page Search:

	Name	IP Address	Protocol Type	Vendor	Device Type	Enabled
<input type="checkbox"/>	1 nozomi	10.204.57.144	Syslog	Nozomi Networks	SCADAguardian	✓

← Previous 1 Next →



ACT...	TO URI	ENDPOINT CONFIGURED AS	CONNECTIVITY STATUS	STATUS	LAST SENT DATA
	udp://10.204.57.142:514	Common Event Format (CEF)	OK	OK	17:18:55.268
	udp://10.204.59.223:514	Common Event Format (CEF)	OK	OK	17:18:55.268

Configuring Nozomi Networks SCADAguardian

To receive the alert information, PPS details are added in SCADAguardian admin interface.

1. Select **Administration > Data Integration**.
 - a. Click **+Add** to add new Endpoint.
 - b. Under Endpoint Configured as, select **Common Event Format (CEF)**.
 - c. Under **To URL**, enter the Protocol (TCP or UDP), IP address of PPS, and port number.
 - d. Select the checkbox **Enable sending Alerts**.
 - e. Enter the filter query if only specific alert information should be sent to PPS.

For example, if administrator wants to send information to PPS for alerts with risk score of more than 6, specify "where risk > 6" in query filter.

Troubleshooting

To verify the event logs on PPS, select **System > Log/Monitoring > Events**.

You can verify that the event logs are generated every time when an event is received from SCADAguardian.

Pulse Secure System Authentication Administrators Users Endpoint Policy Maintenance Wizards

Log/Monitoring > Events > Logs

Events | User Access | Admin Access | Sensors | Client Logs | SNMP | Statistics | Advanced Settings

Log Settings Filters

View by filter: Standard Standard (default) Show 200 items

Edit Query:

Update Reset Query Save Query...

Save Log As... Clear Log Save All Logs Clear All Logs

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	INT31545	2019-07-02 15:14:01 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:
Info	INT31545	2019-07-02 15:13:50 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:
Info	INT31545	2019-07-02 15:13:39 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:
Info	INT31545	2019-07-02 15:13:27 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message: <137>Jul 02 2019 15:26:38 nozomi-sg local n2osevents[0]: CEF:0 Nozomi Networks NZOS 18.5.4-03291152_AFT52 SIGN-ARP-DUP Duplicate IP(S) app=arp dvc=10.204.57.144 dvchost=nozomi-sg.local cs1=5.0 cs2=true cs1Label=Risk cs2Label=InSecurity dmac=02.61.6a.64.26.25 dpt=0 msg=IP 172.16.0.253 is duplicated by MACs: 00.21.86.f5.06.ae, f2.a4.ee.ae:47.59 smax=00.21.86.f5.06.ae spl=0 proto=ETHERNET start=156208119554
Info	INT31545	2019-07-02 15:13:16 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:
Info	INT31545	2019-07-02 15:13:04 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:
Info	INT31545	2019-07-02 15:12:53 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:
Info	INT31545	2019-07-02 15:12:42 - n-31 - [127.0.0.1] System[] - Message received from client: 10.204.57.144 message:

To verify the user access logs, select **System > Logs & Monitoring > User Access** to verify the user login related logs like realm, roles, username and IP address.

Pulse Secure System Authentication Administrators Users Endpoint Policy Maintenance Wizards

View by filter: Standard Standard (default) Show 200 items

Edit Query:

Update Reset Query Save Query...

Save Log As... Clear Log Save All Logs Clear All Logs

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	EAM24805	2019-07-02 15:13:27 - n-32 - [127.0.0.1] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - RADIUS authentication accepted for 00.21.86.f5.d6.ae (realm 'Device Wired Realm') from location-group 'Default' and attributes are: NAS-IP-Address = 10.204.66.50, NAS-Port = 103, NAS-Port-Type = 15
Info	EAM24638	2019-07-02 15:13:27 - n-32 - [0.0.0.0] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - User assigned RADIUS attribute(s) (Juniper-Switching-Filter=Match Destination-ip 10.96.69.26 Action allow Match Destination-mac ##### Action allow Match Ip-protocol 17 Destination-port 67 Action allow Match Ip-protocol 17 Destination-port 53 Action allow)
Info	AUT24562	2019-07-02 15:13:27 - n-32 - [127.0.0.1] System[] - MAC address login succeeded for 00.21.86.f5.d6.ae[Device Wired Realm] from 00.21.86.f5.d6.ae.
Info	AUT23574	2019-07-02 15:13:27 - n-32 - [127.0.0.1] System[] - 00.21.86.f5.d6.ae[Device Wired Realm] logged out from IP (0.0.0.0) because user started new session from IP (0.0.0.0).
Info	AUT24326	2019-07-02 15:13:27 - n-32 - [0.0.0.0] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - Primary authentication successful for 00.21.86.f5.d6.ae[Guest Wired Authentication] from 00.21.86.f5.d6.ae
Info	COA24753	2019-07-02 15:13:27 - n-32 - [0.0.0.0] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - Session Termination Disconnect Message sent to RADIUS Client f5ad for agent at 00.21.86.f5.d6.ae has succeeded.
Info	INT31554	2019-07-02 15:13:27 - n-31 - [127.0.0.1] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - Changed role for endpoint: to Device Restricted Role
Info	INT31555	2019-07-02 15:13:27 - n-31 - [127.0.0.1] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - Endpoint with MAC address: 00.21.86.f5.d6.ae has been quarantined
Info	EAM24805	2019-07-02 15:13:12 - n-32 - [127.0.0.1] 00.21.86.f5.d6.ae[Device Wired Realm][Device Full Access Role] - RADIUS authentication accepted for 00.21.86.f5.d6.ae (realm 'Device Wired Realm') from location-group 'Default' and attributes are: NAS-IP-Address = 10.204.66.50, NAS-Port = 103, NAS-Port-Type = 15
Info	EAM24638	2019-07-02 15:13:12 - n-32 - [0.0.0.0] 00.21.86.f5.d6.ae[Device Wired Realm][Device Full Access Role] - User assigned RADIUS attribute(s) (Juniper-Switching-Filter=Match Destination-ip 0.0.0.0 Action allow)
Info	AUT24562	2019-07-02 15:13:12 - n-32 - [127.0.0.1] System[] - MAC address login succeeded for 00.21.86.f5.d6.ae[Device Wired Realm] from 00.21.86.f5.d6.ae.
Info	AUT24326	2019-07-02 15:13:11 - n-32 - [0.0.0.0] 00.21.86.f5.d6.ae[Device Wired Realm][Device Restricted Role] - Primary authentication successful for 00.21.86.f5.d6.ae[Guest Wired Authentication] from 00.21.86.f5.d6.ae

You can also verify whether the quarantined/blocked host is listed in the Infected Devices report, which lists the mac address, IP address, and the device status. To verify the reports, select **System > Reports > Infected Hosts**.

The screenshot shows the Pulse Secure interface for the 'Infected Devices' report. The navigation menu includes System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. The 'Reports' section is active, and the 'Infected Devices' report is selected. The report title is 'Infected Devices Report' with a download option for CSV or Tab Delimited. There are filter fields for Device Status (Blocked, Quarantined), Username, IP Address, and MAC Address, along with an 'Apply Filter' button. Below the filters are 'Clear Host' and 'Clear All Hosts' buttons. A note states: '*Below listed devices are permanently blocked or quarantined as per Admission Control policy'. The table below shows one result:

MAC Address	Username	IP Address	Blocked By	Device Status
00-21-96-f5-d6-ae	00:21:96:f5:d6:ae		Nozomi SCADAguardian Device	Quarantined

1 results found

You can also enable debug logs to troubleshoot any issues. Select **Maintenance > Troubleshooting > Monitoring > Debug Log** to enable debug logs.

Event Types supported by Nozomi Networks

The following table describes the detailed description about events supported by Nozomi Networks.

Category	Type ID	Name	Definition
Custom Checks	PROC:STALE-VARIABLE	Stale variable	A variable configured with: check_last_update N does not have its value updated for more than N seconds.
Learned Behavior/ Custom Checks	PROC:CRITICAL-STATE-ON	Critical state on	The system has entered in a Process Critical State that has either been learned or inserted as a custom check
Custom Checks	PROC:INVALID-VARIABLE-QUALITY	Invalid variable quality	A variable configured with: check_quality N keeps its value with an invalid quality for more than N seconds.
Built-in Checks	NET:RST-FROM-SLAVE	Slave sent RST on Link	A slave closed the connection to the master. This can be due to the device restarting or behaving in a strange manner.
Custom Checks	NET:INACTIVE-PROTOCOL	Inactive protocol	A link configured with :check_last_activity N stays inactive for more than N seconds.

Category	Type ID	Name	Definition
Built-in Checks	SIGN:TCP-SYN-FLOOD	TCP SYN flood	This kind of alert occurs when either one or many hosts send a great amount of TCP SYN packets to a single host.
Built-in Checks	SIGN:MALICIOUS-PROTOCOL	Malicious Protocol detected	Malicious Protocol detected
Built-in Checks	SIGN:FIRMWARE-CHANGE	Firmware change requested	Firmware change requested
Built-in Checks	SIGN:MAN-IN-THE-MIDDLE	Man-In-the-middle attack	This kind of alert is raised when a Man-In-the-middle attack is detected.
Protocol Validation	SIGN:DHCP-OPERATION	DHCP operation	A DHCP request from an unknown device has been found in the network, as a sign of a new device which is trying to obtain an address.
Built-in Checks	SIGN:CPE:CHANGE	Installed software change detected	This kind of alert is raised after the detection of an installed software change.
Built-in Checks	SIGN:PROTOCOL-ERROR	Protocol error	A generic protocol error occurred, this usually relates to a state machine, option or other general violation of the protocol.
Built-in Checks	SIGN:ILLEGAL-PARAMETERS	A request with illegal parameters was asked	A request with illegal parameters was asked
Built-in Checks	SIGN:UNSUPPORTED-FUNC	Unsupported function was asked	An unsupported function has been called on the remote peer. It might be because of a malfunctioning software is trying to perform an operation without success or that a malicious attacker is trying to understand the functionalities of the device.
Built-in Checks	SIGN:MALICIOUS-DOMAIN	Malicious domain	Malicious domain
Built-in Checks	SIGN:NETWORK-SCAN	Network Scan	Network Scan
Protocol Validation	SIGN:NETWORK-MALFORMED	Malformed network packet	A malformed packet is detected during the Deep Packet Inspection phase.
Built-in Checks	SIGN:PROGRAM:CHANGE	Program change detected	The program on the OT device has been uploaded and changed. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to read the program logic.
Built-in Checks	SIGN:CONFIGURATION-CHANGE	Configuration change requested	The configuration on the device has been uploaded and changed. This can be a legitimate operation during maintenance or an unauthorized tentative to modify the behaviour of the device.
Learned Behavior	VI:NEW-NODE:MALICIOUS-IP	Bad reputation ip	Bad reputation ip

Category	Type ID	Name	Definition
Built-in Checks	SIGN:OT_DEVICE-REBOOT	OT device reboot requested	The OT device has been requested to reboot by the sender host. This event may be something correct during Engineering operations on the OT device, for instance the maintenance. However, it may indicate suspicious activity of an attacker trying to disrupt the process being controlled by the OT device.
Custom Checks	PROC:NOT-ALLOWED-INVALID-VARIABLE	(Variable quality is not allowed)	A variable that has been configured with a specific check has been detected to have a not allowed quality.
Built-in Checks	SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS	Multiple unsuccessful logins	This kind of alert occurs when a host is repeatedly trying to login to a service without success.
Custom Checks	PROC:SYNC-ASKED-AGAIN	Slave sync asked	A new general interrogation command is issued, this can be an anomaly since this command should be performed once per OT device.
Built-in Checks	SIGN:OT_DEVICE-STOP	OT device stop requested	The OT device program has been requested to stop by the sender host. This event may be something correct during Engineering operations on the OT device, for instance the maintenance of the program itself. However, it may indicate suspicious activity of an attacker trying to halt the process being controlled by the OT device.
Built-in Checks	SIGN:OT_DEVICE-START	OT device start requested	The OT device program has been requested to start again by the sender host. This event may be something correct during Engineering operations on the OT device, for instance the maintenance of the program itself or a reboot of the system for updates. However, it may indicate suspicious activity of an attacker trying to manipulate the state of the OT device.
Learned Behavior	VI:PROC:PROTOCOL-FLOW-ANOMALY	Protocol flow anomaly	This kind of alert is raised when the Process-related behavior of a protocol changes in a suspicious manner.
Built-in Checks	SIGN:DEV-STATE-CHANGE	Device state change	This kind of alert is raised when a change of the state of a device is detected, for example when an OT device is asked to enter in a new mode or a factory reset is issued.
Built-in Checks	SIGN:PROGRAM:UPL OAD	Program uploaded to device	The program of the OT device has been uploaded. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to disrupt the normal behavior of the system.

Category	Type ID	Name	Definition
Built-in Checks	SIGN:CLEARTEXT-PASSWORD	Cleartext password	Cleartext password
Built-in Checks	SIGN:TCP-SYN-FLOOD	TCP SYN flood	This kind of alert occurs when one or many host send a great amount of TCP SYN packets to a single host.
Built-in Checks	PROC:WRONG-TIME	Process time issue detected	A slave reported a wrong time regarding Process data. This may be due to incorrect time synchronization of the slave, a misbehavior or a sign of compromise of the device.
Protocol Validation	SIGN:SCADA-INJECTION	SCADA packet Injection4	A traffic injection of SCADA packets has been detected in the network.
Built-in Checks	SIGN:ARP:DUP	Duplicate IP	This kind of alert occurs when a duplicated IP is spotted on the network by analyzing the ARP protocol.
Built-in Checks	SIGN:PACKET-RULE	Packet rule match	A packet rule has matching a specific security check has matched. This Alert requires to thoroughly check what happened to verify if an attacker is trying to compromise one or more host.
Learned Behavior	VI:NEW-PROTOCOL:CONFIRMED	New protocol confirmed	A protocol between two nodes has been confirmed at Layer 4 (the endpoint has accepted the connection).
Custom Checks	NET:LINK-RECONNECTION	Link reconnection	A link configured as persistent has a new TCP handshake.
Built-in Checks	SIGN:MALICIOUS-IP	Bad ip reputation	Bad ip reputation
Learned Behavior	VI:PROC:VARIABLE-FLOW-ANOMALY	Variable flow anomaly	The access over time to a variable has changed in a unexpected manner.
Built-in Checks	SIGN:PROC:MISSING-VAR	Missing Variable Requested	A tentative to access a nonexistent variable has been performed. This can be due to a reconnaissance activity or configuration change.
Learned Behavior	VI:NEW-NET-DEV	New network device detected	A new unseen network device, such as a switch, router or firewall has appeared in the network.
Protocol Validation	SIGN:SCADA-MALFORMED	Malformed SCADA packet	A malformed packet is detected during the Deep Packet Inspection phase.
Learned Behavior	VI:PROC:NEW-VAR	New SCADA variable appeared	A new variable has been detected in a SCADA slave.
Learned Behavior	VI:NEW-FUNC-CODE	New function code detected	A node starts using a function code as never seen earlier.
Learned Behavior	VI:NEW-PROTOCOL:APPLICATION	New application detected	A Layer 7 protocol has been detected in a Layer 4 protocol.

Category	Type ID	Name	Definition
Built-in Checks	SIGN:MALWARE-DETECTED	Malware detected	A malicious payload has been transferred over the network.
Learned Behavior	VI:NEW-PROTOCOL	New protocol used	A new protocol has been tried between two nodes.
Learned Behavior	VI:NEW-LINK	New target used	A node tries to communicate with a node not contacted before.
Learned Behavior	VI:NEW-ARP	New ARP from unknown MAC addresses	A new unseen node appeared through ARP traffic. This Alert is useful to detect also devices that are connected near the sniff interfaces of SCADAguardian but are not sending relevant application-level packets through the network.
Learned Behavior	VI:NEW-NODE:TARGET	New target node appeared	A new unseen node starts to send packets in the network.
Built-in Checks	SIGN:PASSWORD:WEAK	Weak password used	Weak password used
	SIGN:DDOS	DDOS attack	DDOS attack
	SIGN:MULTIPLE-OT_DEVICE-RESERVATIONS	Multiple OT device reservations	Multiple OT device reservations
Learned Behavior	VI:NEW-NODE	New node appeared	A new unseen node starts to send packets in the network.
Built-in Checks	SIGN:PROGRAM:DOWNLOAD	Program downloaded from device	The program of the OT device has been downloaded from another host. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to read the program logic.
Learned Behavior	VI:PROC:NEW-VALUE	New SCADA variable value	A new variable value or behavior has been detected in a SCADA slave.
Learned Behavior/ Custom Checks	PROC:CRITICAL-STATE-OFF	Critical state off	The system has exited from a Process Critical State.
Protocol Validation	SIGN:INVALID-IP	Invalid IP	A packet with invalid IP packets reserved for special purposes (e.g. loopback addresses). Packets with such addresses can originate from misconfiguration or spoofing/denial of service attacks.
Learned Behavior	VI:NEW-SCADA-NODE	New SCADA node appeared	A new unseen node speaking SCADA protocols starts to send packets in the network.
Learned Behavior	VI:NEW-MAC	New Mac address	A new unseen MAC address has appeared in the network.

Category	Type ID	Name	Definition
Built-in Checks	SIGN:UNSUPPORTED-FUNC	Unknown RTU ID requested	An unsupported function has been called on the remote peer. This may mean that a malfunctioning software is trying to perform an operation without success or that a malicious attacker is trying to understand the functionalities of the device.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit <https://support.pulsesecure.net/product-service-policies/>

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.pulsesecure.net>
- Search for known bugs: <https://support.pulsesecure.net>
- Find product documentation: <https://www.pulsesecure.net/techpubs>
- Download the latest versions of software and review release notes: <https://support.pulsesecure.net>
- Open a case online in the CSC Case Management tool: <https://support.pulsesecure.net>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://support.pulsesecure.net>

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: <https://kb.pulsesecure.net>
- Ask questions and find solutions at the Pulse Community online forum: <https://community.pulsesecure.net>

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at <https://support.pulsesecure.net>.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see <https://support.pulsesecure.net/support/support-contacts/>

Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (<https://support.pulsesecure.net>). Include a full description of your issue or suggestion and the document(s) to which it relates.

