



Guardian Administrator Guide

N2OS v25.0.0 - 2025-03-12

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Copyright © 2013-2024, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction	5
Guardian overview	7
Chapter 2. Administration	9
Administration page	11
Settings	13
Security control panel	
Features	
Users management	
CLI	63
Dashboards	
Threat Intelligence	73
Custom fields	
Data integration	
Firewall integration	116
Credentials manager	
Zone configurations	
Synchronization settings	141
Alert playbooks	
System	
General	
Date and time	
Updates and licenses	
Network interfaces	
Upload traces	
Export	
Import	
Health	
Audit	
Data	
Migration tasks	
Operations	
Support	
Backup and restore	
Glossary	



Chapter 1. Introduction



Guardian overview

Guardian is the main Nozomi Networks sensor.

Asset discovery

Guardian gives you the ability to automatically track your *industrial control systems* (ICS), operational technology (OT) and Internet of Things (IoT)/Industrial Internet of Things (IIoT) assets.

- Highly accurate asset inventory of all communicating devices
- Extensive node information including name, type, serial number, firmware version and components
- Actionable risk assessment insights including security and reliability alerts, missing patches and vulnerabilities

Network visualization

Guardian gives you instant visibility of your entire network. This lets you:

- Have instant awareness of your OT/IoT networks and normal activity patterns
- Access key data such as traffic throughput, *transmission control protocol (TCP)* connections, and protocols
- Use intuitive dashboards and reports with macro and micro views, plus filtering and grouping

Automated vulnerability assessment

Guardian lets you quickly identify which *ICS*, *OT* and *IoT* devices are vulnerable. This provides:

- Efficient prioritization and remediation
- A faster response with vulnerability dashboards, drill-downs and reports
- Based on the U.S. government's *National Vulnerability Database (NVD)* for standardized naming, description and scoring

Continuously monitor your networks and automation systems. Guardian gives you:

- The ability to continuously monitor all your assets, network communications and supported protocols
- Easy access to summarized ICS, OT and IoT risk information
- The ability to highlight potential reliability issues, such as unusual process values

Anomaly-based detection

Guardian builds a baseline of your environment and uses that knowledge to detect threats such as transferred malware, suspicious communications, unwanted operations, or changes to the network.



Chapter 2. Administration



Administration page

The administration page lets a user with administrator privileges configure settings and do other tasks.

GUARDIAN	🔺 👁 🛛 LIVE 🛛 HOST ch-qa-g-std-vm-gen-ga-1.intr	a.nozorninetworks.com TIME DISK	used / free LICENSEE Nozomi Ne	tworks UPDATES TI 🗸 Arc 🗸	
NOZOMI =					
Settings Security control panel	Security control panel		Over	view Edit	Manage network learning
Features Users CLI		2	3	4	5
Dashboards Threat Intelligence Custom fields	Learning Securi Adaptive Curr	ty profile Zone co ent: high Defined S	Security Zones: 0	Alert tuning Rules: 3	Alert closing options Options: 2
Firewall integration Credentials manager	Learning	Nodes Links	Security profile		
Zone configurations Synchronization settings Alert playbooks	Last detected change a few seconds ago	\circ			
System	Learning 2023-11-17 12:17:49.650		Low	Medium	High Paranoid
General Date and time	Current mode OAdaptive Two phase - Learning	12487 0 0 11958 0	0 Tip: Use	e this level if you have dee	to knowledge about the
Updates and licenses Network interfaces	Process		networ networ verbose	k, can have access to sche k and want to have deep a Alerts are removed.	dule of changes in the visibility of events. Only more
Export	change 10 days ago				
Health Audit	Learning started 12:23:29.971				
Data Migration tasks	Zone configurations		Alert tuning		
Operations Support Backup and restore	Configured zones: 0		Number of aler	t rules: 3	3

Figure 1. Administration page

Settings

The **Settings** section has these pages:

- Security control panel (on page 13)
- Features (on page 28)
- Users management (on page 31)
- CLI (on page 63)
- Dashboards (on page 65)
- Threat Intelligence (on page 73)
- Custom fields (on page 79)
- Data integration (on page 81)
- Firewall integration (on page 116)
- Credentials manager (on page 134)
- Zone configurations (on page 137)
- Synchronization settings (on page 141)
- Alert playbooks (on page 152)

System

The **System** section has these pages:

- General (on page 157)
- Date and time (on page 158)
- Updates and licenses (on page 160)
- Network interfaces (on page 163)
- Upload traces (on page 173)
- Export (on page 179)
- Import (on page 183)
- Health (on page 197)
- Audit (on page 201)
- Data (on page 202)
- Migration tasks (on page 204)
- Operations (on page 206)
- Support (on page 208)
- Backup and restore (on page 209)

Settings

Security control panel

The **Security control panel** page shows an overview of the current status of the learning process and lets you configure the features that manage the: learning, security profile, zones, alerts tuning, and alert closing options.

GUARDIAN UVE HOST		24.5.0-11111529_AD4C2 TIME	14:46:08:792 DISK 8:7G used / 21G	free [LIMITS REACHED] LICENSEE Nozon	ni Networks. UPDATES Arc 🗸 Al 🗸 Ti 🖌 English 👻
NOZOMI =					
Settings Security control panel	Security control pan	el		Overview Edit	Manage network learning
	1	2	3	4	5
	Learning Adaptive	Security profile Current: high	Zone configurations Defined Security Zones: 0	Alert tuning Rules: 3	Alert closing options Options: 2
	Learning		Se	curity profile	
	Network	Nodes	Links		
	Last detected a few secon	ds ago			
System	Learning started 2023-11-17 12	:17:49.650		Low Medium	High Baranoid
	Current mode OAdaptive	Two rning 12655 0 0	12029 0 0	Low Medium	right Paranold
	Process			Tip: Use this level if you have de network, can have access to sci network and want to have deep	sep knowledge about the hedule of changes in the p visibility of events. Only more
	Last detected 10 days	ago		verbose Alerts are removed.	
	Learning started 2023-11- 1223-29	17 971			
	Zone configurations		Ale	ert tuning	
	Configured zones: 0		N	umber of alert rules: 3	
			n	nute	3

Figure 2. Security control panel page

The Security control panel page has these tabs:

- Overview (on page 14)
- Edit (on page 15)
- Manage network learning (on page 25)

Overview

The **Overview** page shows an overview of the learning status, security profile chosen, zone configurations, and alert tuning rules configured.

ecunty co			-	Overview	Edit	Manage network	learning
1		2	3			5	
Learn Adapt	ing Secur ive Cur	ity profile rent: high	Zone configura Defined Security Zo	ntions ones: 0	Alert tuning Rules: 0	Alert closing Options	options
Learning				Security p	rofile		
Network		Nodes					
Last detected change	a few seconds ago	\cap					
Learning started	2023-09-28 12:02:57.009			Low	Mediun	n High	Paranoid
Current mode	Adaptive Two phase · Learning	987 - 0 - 0 Links		Tip	: Use this level if you e network, can have	u have deep knowledge a access to schedule of ch	about
Process				in ev	the network and wa ents. Only more verk	int to have deep visibility pose Alerts are removed.	of
Last detecte change	d a month ago	\mathbf{O}					
Learning sta	rted never	644 - 0 - 0					
Zone config	urations			Alert tunir	g		
Configured	zones: 0			Number o	of alert rules: 0		

Figure 3. Overview page

The **Overview** page shows an overview for each of these pages:

- Learning (on page 16)
- Security profile (on page 19)
- Zone configurations (on page 20)
- Alert tuning (on page 21)
- Alert closing options (on page 24)

Edit

The **Edit** page lets you configure the security features through simple steps.

The **Edit** page has these pages:

- Learning (on page 16)
- Security profile (on page 19)
- Zone configurations (on page 20)
- Alert tuning (on page 21)
- Alert closing options (on page 24)

Learning

The **Learning** page lets you manage how the typical behavior and components of your environment are learned. The software needs to learn the normal processes, patterns and communication of your environment in order for it to be able to detect anomalies.



Learning Detection approach

This dropdown lets you choose from these options:

- Adaptive Learning (default)
- Strict

Adaptive Learning uses a less granular and more scalable approach to anomaly detection where deviations are evaluated at a global level, rather than at a single node level. For example, the addition of a device similar to the ones already installed in the learned network will not produce alerts. This holds true for the appearance of a similar communication. Adaptive Learning shows its maximum capabilities when combined with Asset Intelligence.

Strict uses a detailed anomaly-based approach, so that deviations from the baseline will be detected and alerted. This approach is called strict because it requires the learned system to behave like it has behaved during the learning phase, and requires some knowledge of the monitored system in order to be maintained over time.

The engine has two distinct learning goals: the network and the process. For both cases the engine can be in learning and in protection mode, and they can be governed independently.

Network Learning is the learning of:

- Nodes
- Links
- Protocols
- Function Codes for example, commands, that are sent from one node to another

A wide range of parameters is checked in this engine and can be fine-tuned.

Process Learning is the learning of variables, and their behavior. You can use specific checks to fine-tune this learning.

Phase switching

You can set this to one of these options:

- Dynamic
- Two-phase

Dynamic, or Dynamic window, lets you configure the time interval in which an engine considers a change to be learned. Every engine does this kind of evaluation **per node** and **per network segment**.

After this period of time, the learning phase is automatically, and safely, switched to protection mode. This:

- Raises alerts when something is different from the learned baseline
- Adds suspicious components to the environment with the is learned attribute set to off, in such a way that an operator can confirm, delete, or take the appropriate action in the Manage network learning (on page 25) page

In this way, stable network nodes and segments become protected automatically. This prevents you from being overwhelmed with alerts due to the premature closing of learning mode.

The **Two phase** dropdown lets you choose between:

- Learning
- Protecting

Learning: in this mode, the environment incorporates new behavior as learned.

Protecting: in this mode, you will receive alerts when an anomaly is detected

Variables

If you set the toggle to **Learning and Protecting**, an alert will be raised if a new *variable* is detected. You can set the toggle to **Disabled**, if you want to prevent this happening. For example, when you are making planned changes to your environment.

New values

If you set the toggle to **Learning and Protecting**, an alert will be dynamically raised if a change in the behavior of the process is detected. You can set the toggle to **Disabled**, if you want to prevent this happening. For example, when you are making planned changes to your environment.

Dynamic flow control

If you set the toggle to **Learning and Protecting**, an alert will be raised if reading and writing patterns of a *Variable* are detected. You can set the toggle to **Disabled**, if you want to prevent this happening. For example, when you are making planned changes to your environment.

Security profile

The **Security profile** page lets you change the visibility of alerts based on their type.

•	ol panel	0.00	erview Edit	Manage network learning
1	2	3	4	5
Learning	Security profile	Zone configurations	Alert tuning	Alert closing options
Adaptive	Current: high	Defined Security Zones: 0	Rules: 0	Options: 2
	() Changing the value of the change.	security profile will not affect exist	ing alerts, but only the aleri	ts created after the
Low	1	Medium	High	Paranoid
	Tip: Use this level if you have de network and want to have deep	eep knowledge about the network o visibility of events. Only more ver	, can have access to schedu bose Alerts are removed.	lle of changes in the
Page 1 of 4, 76 en	Tip: Use this level if you have denetwork and want to have deep Save	eep knowledge about the network o visibility of events. Only more ver	r, can have access to schedι bose Alerts are removed.	Ile of changes in the
Page 1 of 4 , 76 en	Tip: Use this level if you have denetwork and want to have deep Save	eep knowledge about the network o visibility of events. Only more ver	r, can have access to schedu bose Alerts are removed. Type name	Ile of changes in the Base risk
Page 1 of 4 , 76 en	Tip: Use this level if you have deen network and want to have deen stored and the second stored and the second stored and second stored an	Type ID	t, can have access to schedu bose Alerts are removed. Type name or unknown device	Je of changes in the Base risk
Page 1 of 4, 76 en From security Medium High	Tip: Use this level if you have deen network and want to have deen some start of the second s	Type ID INKNOWN-RTU ? Missing Up ? Duplicat	r, can have access to schedu bose Alerts are removed. Type name or unknown device ted IP	Base risk

General

When you change the value of the **Security Profile**, it has an immediate affect on newly-generated alerts, and it has no effect on existing alerts. The default setting is **Medium**.

Alerts which are not visible under the current configurations are not stored in the database, unless they are part of an incident. To change this behavior, you can set the option save_invisible_alerts to true

Low

Use this level if you are starting to get control of the network, you do not have deep information about it, or if you are resource-constrained. This level reduces that amount of alerts.

Medium

Use this level if you have some information about the network and how it operates, and have knowledge of scheduled network changes. In this scenario, it will be useful to help you understand if new elements should be allowed or not.

High

Use this level if you have deep knowledge about the network, can have access to schedule of changes in the network and want to have deep visibility of events. Only more verbose Alerts are removed.

Paranoid

Use this level for maximum visibility, but at the cost of a more time-consuming effort in alert management.

Zone configurations

You can select this to go to the **Zone configurations** page. You can customize all settings related to the learning engine and the security profile on a per-zone basis.

For more details, see **Settings > Zone configurations**.

Alert tuning

The **Alert tuning** page lets you customize the alert behavior. Specifically, you can impose conditions on one, or many, fields to match criteria. This feature can be selectively enabled for specific user groups.

		Ov	erview Edit	Manage Network Learning
1	2	3	A	5
Learning	Security profile	Zone configurations	Alert Tuning	Alert Closing Options
Adaptive	Current: medium	Defined Security Zones: 0	Rules: 0	Options: 2
Page 1 of 1, 0 entries		Execution policy: Lo	cal prevails 🐧 Live 🔳 🎵	Export all Import + Add
ACTIONS MAT	CHING ACTION	ARGUMENTS	PRIORITY N	OTE SOURCE

Figure 4. Alert tuning page

Execution policy

As alert rules can be propagated from upstream connections, conflicts between rules are possible. A conflict is detected when multiple rules, performing the same action, match an alert. To deal with these collisions, the execution algorithm takes into consideration the source of the rules. The user can choose three policies:

- **upstream_only**: alert rules are managed in the top *Central Management Console* (*CMC*), or with Vantage. Creation and modification are disabled in the lower-level sensors. Only the rules received from upstream are executed
- upstream_prevails: in case of conflicts, rules coming from upstream are executed
- local_prevails: in case of conflicts, rules created locally are executed

A special case is represented by the **mute** action. Consider the following example: the execution policy is **local_prevails** and a mute rule is received by Guardian from an upstream connection. This rule will be ignored if at least one local rule matches the alert. Conversely, with the execution policy set to **upstream_prevails**, local **mute** will be ignored if at least one rule coming from upstream matches the alert.

Live / refresh

The Live icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Export all

Use this to export the table.

Import

This lets you import alert rules.

Note:

The maximum file size is 2 *gigabyte (GB)*. The supported file type is .nozomi_alert_rules.

+ Add

This lets you add and configure an alert.

Alert configuration settings

Source IP	Enter the <i>internet protocol (IP)</i> address of the source that you want to filter.			
Destination IP	Enter the <i>IP</i> address of the destination that you want to filter.			
Source MAC	Enter the <i>media access control (MAC)</i> address of the source that you want to filter.			
Destination MAC	Enter the MAC address of the destination that you want to filter.			
Match IPs and MACs in both directions	Select this if you want to select all the communications between two nodes (<i>IP</i> or <i>MAC</i>) independently of their role in the communication (source or destination).			
Source Zone	Enter the zone of the source that you want to filter.			
Destination Zone	Specify the zone of the destination that you want to filter.			
Type ID	The type ID of the alert, this field is precompiled if you create a new modifier from an alert in the Alerts page.			
Trigger ID	Unique identifier corresponding to the specific condition that has triggered the alert.			
Protocol	Enter the protocol that you want to filter.			
Note	Enter free-form text that describes details of the alert rule.			
Execute action	 Select an action to perform on the matched alerts: Mute: Switch ON/OFF: to mute or not the alert Mute until: Specify a date until which the alert will be muted Change Security Profile visibility: Set to ON to force the visibility of the selected alert type for any selected profile, or to OFF to hide it for any selected profile. Useful for extending or reducing the default provided security profiles as needed Change trace filter: Define a custom trace filter to apply to this alert Assign playbook: Define a playbook to be attached to the matching alerts. The playbook to be attached has to be selected from the list of available playbook templates 			
Priority	Set a custom priority; when multiple rules trigger on an alert, the rule with the highest priority applies. Normal is the default value if no selection is made.			

Alert closing options

The **Alert closing options** page lets you customize the closure details of alerts and incidents. When alerts and incidents are closed, the user must choose the reason why the closure happens. There are two default reasons: **actual incident** and **baseline change**.

2	•	Overvi	ew Eait	Managenetwork learning
1	2	3	4	
Learning	Security profile	Zone configurations	Alert tuning	Alert closing options
Page 0 of 0 , 0 entries				Live • 🔿 🔶 + Ado
Actions		Reason for closing		Learn

Figure 5. Alert closing options page

Live / refresh

The Live $\bigcirc \bigcirc \bigcirc \bigcirc \bigcirc$ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This button lets you add a new alert closing option.

Manage network learning

The **Manage network learning** page lets you review and manage the Network Learning status in detail.

,	_	Overview	Edit Manage Network Learning
e 💽 🎵 📕 4 from the beginning 🏼 🎽 Nodes 🕶 Link	ks▼ Layout▼	III 2 ×	🛍 Delete 🖺 Learn 🛛 Save Discard
			Image: Constraint of the second s

Figure 6. Manage network learning page

The graph is initialized with the node and link not learned perspectives. The items that are not known to the system are highlighted in red or orange. This makes it easy to discover new elements, and take an action on them.

To the right of the graph view, is a panel with additional buttons.

Delete

This lets you delete the selected item(s) from the system.

Learn

This lets you add the selected item(s) in the system.

Save

When the configuration is complete, you can select **Save** to make the changes persistent.

Discard

This lets you discard all unsaved changes to the system.

Learn a protocol

The Manage network learning page lets you select links to let you learn protocols.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Security control panel.

Result: The Security control panel page opens.

3. In the top right section, select Manage network learning.

Result: The Manage network learning page opens.

4. Select a red or orange link.

Result: Information for the link will show in the pane on the right. If the protocol is *supervisory control and data acquisition (SCADA)*, a function code will also show.

- 5. In the pane on the right, below the selected link, select one, or more, protocol(s).
- 6. Select Learn.

Result: A save icon will show to the right of the selected item(s) and the **Save** and **Discard** buttons will be highlighted.

7. Select **Save**.

Result: The protocol(s) will be learned, and it will show green.

Results

If all protocols were learned, the link will show in gray. If only some of the protocols were learned, the link will show in orange.

Learn a node

The Manage network learning page lets you select links to let you learn protocols.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Security control panel.

Result: The Security control panel page opens.

3. In the top right section, select Manage network learning.

Result: The Manage network learning page opens.

4. Select a red or orange node.

Result: Information for the link will show in the pane on the right. For each node, the node id will be shown, and below two children items will show the node *IP* address and the *MAC* address.

- 5. In the pane on the right, below the selected node, select one, or more, item(s) to be learned.
- 6. Select **Learn**.



If you select **Delete**, all the items will be selected, and deleted.

Result: A save icon will show to the right of the selected item(s) and the **Save** and **Discard** buttons will be highlighted.

7. Select **Save**.

Result: The node(s), and all the selected items will show green.

Results

If all nodes were learned, the node will show in gray. If only some of the protocols were learned, the link will show in orange.

Features

The **Features** page shows an overview of the current status of system features configuration and lets you fine tune specific values.

NOZOMI NETWORKS =			Ø
Settings	Features	General	Retention
Features	IPv6 Cenerate Assets from IPv6 nodes Discovery Standard lightweight announcements to discover neighboring devices		
System			

Figure 7. Features page

The **Features** page has these tabs:

- General (on page 29)
- Retention (on page 30)

General

The **General** page lets you generate assets from IPv6 nodes.

Features	General	Retention
IPv6		
Generate Assets from IPv6 nodes		
Discovery Standard lightweight announcements to discover neighboring devices		
Save		

Figure 8. General page

IPv6

This checkbox enables the creation of assets with an IPv6 address that are detected through passive monitoring.

Discovery

This checkbox lets you enable/disable Discovery. The default setting is disabled.

Discovery is a method of identification of actors in the network through the usage of lightweight protocol-specific broadcast messages. These messages cause the actors to reply with identity information. The process is repeated with interleaving, predefined intervals. On each repetition, the sensor will identify the suitable network interfaces and send broadcast messages through them to reach the subnetworks the sensor is connected to.

Retention

The **Retention** page lets you select a specific number, or **Retention level**, for historical data persistence. In some cases, you can either completely disable the retention of a feature, or enable the advanced options that provide more specific settings.

	Save Canc
Alerts	Audit
When an alert is deleted, the related trace file is deleted too	Retention level: up to 100,000 items
Retention level: up to 500,000 items	Expiration: Never
Advanced options ON OFF	
	Captured URLs
Captured logs	Warning: Enable this feature only in small environments
Retention level: up to 25,000 items	COLLECTING Disabled
	 COLLECTING: enables historical data persistence up to chosen value DISABLED: disables historical data persistence
CLI action requests	
Retention level: up to 100,000 items	Dashboard configurations
•	Retention level: up to 10,000 items
Extended network statistics	•
COLLECTING Disabled	Health logs
 COLLECTING: enables historical data persistence up to chosen value DISABLED: disables historical data persistence 	Retention level: up to 5,000 items
Link events	Retention level up to 100.000 items
Warning: Enable this feature only in small environments COLLECTING Disabled	
① • COLLECTING: enables historical data persistence up to chosen value	Node CVEs
 DISABLED: disables historical data persistence 	Retention level: up to 400,000 items
Node CBE chapter	•
Retention level: up to 100.000 items	Eilee quarantine
	Applicable to monitored files reconstructed for analysis
	 Additional de Lucitica de lines reconstructed de la languis
Node points	Retention level: up to 50 items
Retention level: up to 1,000,000 items	
•	Scheduled updates
Reports saved locally	Retention level: up to 10,000 items
Retention level: up to 500 items	•
	Smart Polling execution history
Expiration: 90 days	Retention level: up to 100,000 items
•	•
Time machine snapshots	Terror concerted
Space retention level: 512 MB	Detention level: up to 10 000 items
Retention level: up to 50 items	Advanced options ON OFF
	Space retention level: 2.25 GB
Traces: generated continuous	•
Space retention level: 2.25 GB	licar saesione
•	Annlicable to ULUser sessions. Users need to reconnect as a their service in purced
Retention level: up to 10,000 items	Althouse on an analised and a second used in the production of a rule in second use and a second of the product of the prod
·	Retention level: up to 10,000 items
Traces: uploaded	
Retention level: up to 10 items	
•	
Variables history	
Retention level up to 1.000.000 items	

Figure 9. Retention page

Expiration

This lets you select a specific number of days for historical data persistence. To let the data persist forever, you can set this to **Never**.

Retention level

This lets you select a specific number of items for historical data persistence.

Space retention level

This lets you select a specific space size for historical data persistence.

Users management

The **Users management** page shows all the pages that you need to let you manage authentication and authorization policies for users and groups.

≡									ŝ
User	Users management			Gr	oups (DpenAPI Ke	ys Active Directory	LDAP SAM	ИL
Pa	ige 1 of 3,	55 entries					Live 💽 🕤 🕂	Add 🛔 Import config	uration
Ac		Username	Source	ls admi	Is suspende	Is expire	Groups	Last activity	
							· •		
		alessandro.zamberletti@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		2023
		giacomo.matteucci@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers	2023-12-01 11:57:20.562	2023
		admin	local	true	false	false	admins	2023-11-15 14:42:14.686	2023
		nicolo.ereni@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		2023
		cristian.pascottini@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		elia.battiston@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		2024
		alessandro.cavallaro@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers	2024-02-12 12:18:07.953	202
# Q4	a, 🗊	davide	local	true	false	false	admins		202
		alessandro.loforte@nozominetworks.com	saml	true	false	false	NozomiAzureAD_PlatformEngineering		202
		natalino.picone@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		moreno.carullo@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		gabriele	local	true	false	false	admins		202
		dario.andreani@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		alessio.zappa@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		giannim	local	true	false	false	admins		202
		roberto.ripamonti@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		manuel.lupato@nozorninetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		philip.trainor@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Product		202
		massimo.zappino@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers		202
		alessandro.duvia@nozominetworks.com	saml	true	false	false	NozomiAzureAD_PlatformEngineering		2023
		vlad.mihaescu@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers	2024-09-16 15:19:24.330	2023
		n2jarvis	local	true	false	false	admins		202
		mattia.lucariello@nozominetworks.com	saml	true	false	false	NozomiAzureAD_Developers	2024-02-29 16:30:51.339	202
		sdalessio	local	true	false	false	admins	2024-05-24 15:21:23.180	2023
		silvia.delrossi	local	true	false	false	admins		2023

Figure 10. Users management page

General

The Users management page has these tabs:

- Users
- Groups
- OpenAPI Keys
- Active Directory
- LDAP
- SAML

There are four different types of user:

- Local users (on page 31)
- Active Directory users (on page 32)
- LDAP users (on page 32)
- SAML users (on page 32)

Local users

Authentication is enforced with a password, and the user is created from the Web *user interface (UI)*.

Active Directory users

Active Directory manages authentication. User properties and groups are imported from the Active Directory. You need to configure Active Directory (on page 53) for it to work correctly.

LDAP users

lightweight directory access protocol (LDAP) manages authentication. User properties and groups are imported from *LDAP*. You need to configure LDAP (on page 56) for it to work correctly.

SAML users

A password is not required as authentication is enforced through an authentication server that uses *security assertion markup language (SAML)*. You can use the Web *UI* to add users (on page 61), or to Import SAML users from a CSV file (on page 37).

Users

The **Users** page shows a list of users and lets you create and delete users, and change the password and/or username of existing users.

sers man	agement	Users	Groups	OpenAP	Pi Keys Ad	ctive Directory	LE	DAP SAML
Page 1 of 3, 66 entries						Live •	+ Add	lmport configuratio
ACTIONS USE		NAME	SOURCE	IS ADMIN	IS SUSPENDED	IS EXPIRED	GROUPS	
								- 🔻
			saml	true	false	false	NozomiAz	ureAD_Product
			saml	true	false	false	NozomiAz	ureAD_Developers
			saml	true	false	false	NozomiAz	ureAD_PlatformEngineeri
			saml	true	false	false	NozomiAz	ureAD_Developers
			local	true	false	false	NozomiAz	ureAD_Product
			local	true	false	false	admins	
			saml	true	false	false	NozomiAz	ureAD_Developers
			saml	true	false	false	NozomiAz	ureAD_Developers
			saml	true	false	false	NozomiAz	ureAD_Developers
			saml	true	false	false	NozomiAz	ureAD_Developers
			local	true	false	false	admins	
			saml	true	false	false	Technical	Marketing
1 Q 1			local	true	false	false	admins	

Figure 11. Users page

Add a user

The **Users** page lets you add a new user.

About this task

When you add a new user, you will typically select **Local** or **SAML** as the source. You can choose to select a user from the **Active Directory** or from **LDAP**, but you must first make sure that the user exists in the Active Directory or in LDAP. Therefore, in these cases, we recommend that you import these users directly from the Active Directory or from LDAP.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Users**.

Result: The Users management page opens.

3. In the top right section, select **Users**.

Result: The **Users** page opens.

4. In the top right section, select **+Add**.

Result: A dialog shows.

5. From the **Source** dropdown, select a source for the user.

New user		×
Source		
	Choose a source 🗸	
Username		_
Password 0		
Password confirmation		
Group		
	Choose one or more groups -	
Must update password		
Is suspended		
Is expired 0		
	New user	

Choose from:

- Local
- Active Directory
- LDAP
- SAML

Note: The dialog might change after you make your selection.

- 6. In the **Username** field, enter a value.
- 7. In the **Password** field, enter a password.

Note:
This step is not applicable if you chose SAML as the source.

8. In the **Password confirmation** field, enter the password again.

Note: This step is not applicable if you chose **SAML** as the source.

- 9. From the **Group** dropdown, select a group for the user.
- 10. Optional: If necessary, select Must update password. This is selected by default.

Note:

When this is selected, the user will be prompted to update their password the next time they log in.

11. Optional: If necessary, select Is suspended.

Note:

When this is selected, the user will not be able to log in.

12. Optional: If necessary, select Is expired.



When this is selected, the user is forced to change their password the first time that they log in after the expiration date.

13. Select New user.

Results

The user has been added.
Import SAML users from a CSV file

The **Users** page lets you import security assertion markup language (SAML) users from a comma-separated value (CSV) file.

About this task

The template for the *comma-separated value (CSV)* file is three fields for each row, separated by commas:

- The first field defines the user name
- The second field is the **Authentication** group that is associated with the user (typically an **Authentication**-only group)
- The last field includes one or more groups (separated by semicolons) that define additional groups associated with the user (typically used to define allowed features)

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the **Settings** section, select **Users**.

Result: The Users management page opens.

3. In the top right section, select **Users**.

Result: The Users page opens.

4. In the top right section, select **Import configuration**.

Result: A dialog shows.

5. Choose a method to upload a file.

Choose from:

- $\,\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the Drop a file here or click to upload field

6. If you chose the second method, select the correct file to upload.



Note:

The supported format is CSV. The maximum permitted file size is 2 GB.

7. Wait for the file to upload.

Results

Once the import is complete, you will receive a message with the number of users that have been correctly imported.

Edit a local user

You can use the **Users** page to edit the details for an existing user.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

- 2. In the **Settings** section, select **Users**.
 - Result: The Users management page opens.
- 3. In the top right section, select $\ensuremath{\textbf{Users}}.$

Result: The Users page opens.

4. To the left of the applicable user, select the earrow icon.

Result: A dialog shows.

5. Edit the details as necessary.

Edit user		×
Source Local		
Username		
Password 0		
Password confirmation		
Group		
	guests 🕶	
Must update password		
Is suspended		
Is expired 0		
	Edit user	

6. Select Edit user.

Results

The details for the local user have been edited.

Add an SSH key for an admin user

You can use secure shell (SSH) public keys to log into the SSH console without typing a password. You must add SSH public keys to the user account to configure SSH password-less authentication.

Procedure

1. In the top navigation bar, select $\overleftrightarrow{\mathcal{O}}$

Result: The administration page opens.

2. In the **Settings** section, select **Users**.

Result: The Users management page opens.

3. In the top right section, select **Users**.

Result: The Users page opens.

4. To the left of the applicable user, select the $\stackrel{ extsf{Q}}{ imes}$ icon.

Result: A dialog shows.

5. In the field, paste the public key in the SSH public keys for web user admin field.



Note:

Every admin user has a key. If you need more than one key, paste one per line. Non-admin users must use a password for *secure shell (SSH)* authentication. When an admin user leaves, the associated *SSH* keys are removed.

Note:

The pasted key should not contain new lines. The system will not use invalid keys.

- 6. Optional: To enable logging in with the root account, select Allow root login using SSH keys.
- 7. Select Edit ssh keys.

Results

The *SSH* public keys are propagated to all the sensors that are directly connected. The default key propagation interval is 30 minutes. You can change this with: conf.user configure ssh_key_update interval <seconds> in the **CLI**.

Groups

The Groups page shows a list of all the user groups.

Page 1 of 1,	9 entries		Liv	e 💽 🕥	+Add	Import from Act	ive Directory	🔮 Import	from LDAP server
ACTIONS	NAME		SOURCE	ZONE FILTER			SECTIONS IS	ADMIN	CREATED AT
	admins		local				tr	ue	2023-07-03 17:04:13.92
	TechnicalMarketing		local				tr	ue	2023-07-04 11:32:03.04
	NozomiAzureAD_Platform	Engineering	local				tr	ue	2023-07-21 17:30:09.42
	NozomiAzureAD_Develope	ers	local				tr	ue	2023-07-21 17:30:09.43
	NozomiAzureAD_Product		local				tr	ue	2023-07-21 17:30:09.43
	NozomiAzureAD_Technica	IMarketing	local				tr	ue	2023-07-21 17:30:09.43
ØÛ	guests		local				fa	lse	2023-09-08 15:44:54.3
	NozomiAzureAD_Knowled	geManagement	local				tr	ue	2023-09-13 09:06:13.102
	health		local			health	fa	lse	2023-09-19 12:46:26.165

Figure 12. Groups page

Authorization policies

User groups define authorization policies. Each group includes a:

- List of allowed features
- Filter to enable visualization of just specific node subsets

When a user belongs to a group, the user can only:

- Perform the operations that the group allows
- See the nodes that the group node filter defines

A user can belong to several groups and will inherit the authorizations of those groups. When a user belongs to multiple groups, any node that satisfies the filter of any group is visible, and its features are available.

Two group types have predefined authorization policies:

- Administrators: All features are available
- Authentication Only: Only the authentication feature is available

When a group is neither **Administrators** nor **Authentication Only**, the allowed features (sections) can be enabled/disabled individually.

Note:

After a reboot, the local default admin of the Web *UI* will automatically be recreated (within the default admin's user group) if it has been deleted, or if it doesn't exist. This is to make sure that a user cannot mistakenly delete it.

Note:

We recommend to have at least one group without admin privileges. Therefore, after a reboot, if a user group with no admin privileges doesn't exist, a guests user group will be created automatically, without a user in it.

Live / refresh

The Live \bigcirc icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

+Add

This lets you add a new group.

Import from Active Directory

This lets you import a group from Active Directory.

Import from LDAP server

This lets you import a group from a *LDAP* server.

Add a local group

The **Groups** page lets you add new user groups.

Procedure

- 1. In the top navigation bar, select 🛱 **Result:** The administration page opens.
- In the Settings section, select Users.
 Result: The Users management page opens.
- 3. In the top right section, select **Groups**.

Result: The Groups page opens.

4. In the top right section, select **+Add**.

Result: A dialog shows.

5. In the top left, select **General**.

New group	2
General Filters	
Name	
External UUID	
Propagate this users group to all the connected sensors	
Permissions	
Is admin	
Authentication only	
Allowed sections	
Reports (Allow editor)	
Allow the users to view/edit reports generated and reports template	
Queries and exports (Allow to save queries)	
Allow the users to view the query section and to export data	
Assertions	
Allow the users to execute assertions	
Assets	
Allow the users to view the asset view section	
Network configuration	
Allow the users to configure nodes, links and assets (if assets view is enabled)	
Import	
Allow the users to import configuration files	

6. In the **Name** field, enter a name for the group.

7. **Optional:** If necessary, in the **External UUID** field, enter a *universally unique identifier (UUID)*.

Note:

This is useful should the user group be created through *SAML* integration and the external *identity provider (IdP)* uses an *identifier (ID)* rather than a human-readable group name.

- 8. If you want the group to propagate to connected sensors, select **Propagate this** users group to all the connected sensors.
- 9. If the group belongs to a predefined type, select the appropriate one:

Choose from:

- Is admin
- Authentication only
- 10. If you do not select a predefined group type, continue with the steps below to manually select section(s) that the group can view and interact with.
 - a. In the top left, select **Filters**.
 - b. From the **Zone filters** dropdown, select one or more zone(s) to define zone filters to limit zone visibility to the users in the group.
 - c. In the **Node filters** field, enter a list of subnet addresses in *classless interdomain routing (CIDR)* format.



11. Select New group.

Results

The group has been added.

Edit a group

You can use the **Group** page to edit the details for an existing group.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Users**.

Result: The Users management page opens.

3. In the top right section, select **Groups**.

Result: The Groups page opens.

4. To the left of the applicable group, select the earrow icon.

Result: A dialog shows.

5. Edit the details as necessary.

Edit group	х
General Filters	
Name	
guests	
External UUID	
Propagate this users group to all the connected sensors	
Permissions	
Is admin	
 Authentication only 	
Allowed sections	
 Reports (Allow editor) 	
Allow the users to view/edit reports generated and reports template	
 Queries and exports (Allow to save queries) 	
Allow the users to view the query section and to export data	
Assertions	
Allow the users to execute assertions	
Assets	
Allow the users to view the asset view section	
Network configuration	
Allow the users to configure nodes, links and assets (if assets view is enable	rd)
Import	
Allow the users to import configuration files	

6. Select Edit group.

Results

The details for the group have been edited.

Import an Active Directory group

To permit Active Directory users to log into the system, you can import an existing group from an Active Directory infrastructure.

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the Settings section, select Users.

Result: The Users management page opens.

3. In the top right section, select Groups.

Result: The Groups page opens.

4. In the top right, select Import from Active Directory.

Result: A dialog shows.

5. In the Username field, enter the Active Directory user logon name.

Import	groups from	Active	Directory				×
Username		Password		Group name	▲ Retrieve groups	3	
Gilter by	group name						
O Specify a	n administrative user of t	he current A	Active Directory domain				
							Get also member-of groups Import configuration Cancel

Note:

This should be in format <domainname>\<domainusername> format.

- 6. In the **Password** field, enter a password.
- 7. To retrieve the list of groups, select Retrieve groups.

Note:

You can also select **Filter by group name**, and type the name of the group that you want to retrieve.

- 8. Filter and select the desired groups to import.
- 9. Optional: To import related groups, for example, parent groups, select Get also member-of groups.

10. Select Import configuration.

Result: The list of groups opens.

11. Edit the group permissions as necessary.

Note:

Active Directory users that belong to this group are automatically assigned to it and inherit all permissions of the configured group.

Results

Users can log into the system with the <domainname>\<domainusername> username and their current domain password in the login screen.

Import an LDAP group

To permit existing lightweight directory access protocol (LDAP) users to log into the system, you can import an existing group from an LDAP server.

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the Settings section, select Users.

Result: The Users management page opens.

3. In the top right section, select Groups.

Result: The Groups page opens.

4. In the top right, select **Import from LDAP server**.

Result: A dialog shows.

5. In the **Username** field, enter a username.

Import	groups from	LDAP server			×
Username		Password	Group name	a Retrieve groups	
Gilter by	group name				
O Specify ar	n administrative user of t	he current LDAP dom	in		
					Import configuration Cancel

Note:

This requires an admin user with full *LDAP* server permission. The **Username** for the *LDAP* server should be a distinguished name (DN) that follows the *LDAP* standard. For example, cn=username, cn=group, dc=nozominetworks, dc=com.

- 6. In the **Password** field, enter a password.
- 7. To retrieve the list of groups, select Retrieve groups.

Note:

You can also select **Filter by group name**, and type the name of the group that you want to retrieve.

- 8. Filter and select the desired groups to import.
- 9. Optional: To import related groups, for example, parent groups, select Get also member-of groups.

10. Select Import configuration.

Result: The list of groups opens.

11. Edit the group permissions as necessary.

Note:

LDAP users that belong to this group are automatically assigned to it and inherit all permissions of the configured group.

Results

Users can log into the system with the username and their current domain password in the login screen.

OpenAPI Keys

The **OpenAPI Keys** page lets you manage the openAPI keys. You can use OpenAPI keys for bearer token authentication instead of basic authentication, which uses a username and password.

sers II	lanayem	ent	Users	Groups	OpenAPI Keys	Active Directory	LDAP	SAML
Page 1 of	1, 4 entries						L	ive 🌒 💭
ACTIO	NAME	DE	SCRIPTION	ALLOWED IPS	LAST SIGN IN IP	LAST SIGN IN TIME	REVOKE TIME	USERNAME
/+	AKc4bded	Testl					2023-08-25 10:32:01.082	giacomo
ø û	AKc9c504	test s	olunk		10.41.132.182	2023-08-25 10:53:24.429	never	nicoloadmin
/0	AKc699b9	senor	bestemmio		10.41.132.182	2023-09-06 15:54:15.698	never	nicoloereni
/0	AK298f3f	Splun	kTestNicolo		10.41.132.182	2023-10-10 14:44:57.896	never	nicolosplunk

Figure 13. OpenAPI keys page

General

You can only assign OpenAPI keys to local users.

Local users can access their OpenAPI keys in **Personal settings > Other actions > Edit openAPI keys**.

For more details, see the **Guardian User Guide**.

For more details about open *application programming interface (API)* keys, see the **SDK User Manual**.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Active Directory

In addition to local users, you can configure existing Active Directory users for login.

sers management	Users	Groups	OpenAPI Keys	Active Directory	LDAP	SAML
Page 1 of 1, 0 entries					Live •	Add
ACTIONS	JSERNAME		DOMAIN NAME		DISTINGUISHED N	AME

Figure 14. Active Directory page

Active Directory permissions are defined based on the user group. When you set the primary group for a user, that user is excluded from the corresponding group membership in the Active Directory. This is because the Active Directory does not support primary group functionality. It does not query the primary group attribute when building the group membership of a user, therefore the primary group on the Active Directory server is not visible in Guardian.

Configure Active Directory integration

The Active Directory page lets you configure integration.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Users**.

Result: The Users management page opens.

3. In the top right section, select **Active Directory**.

Result: The Active Directory page opens.

4. In the top right, select +Add.

Result: A dialog shows.

5. In the **Username** field, enter a username.

New Active Directory Configurat	tion		×
Status:			
Username N070M(luser]		Password	
Domain Controller IP/Hostname 1			
LDAPS	Port		
e.g. 192.168.0.4 or host.dc.com		Check connection	
Add host			
Domain name		Distinguished name	_
e.g. NOZOMI		e.g. dc=nozomi,dc=local	
Connection timeout			
e.g. 10			
		Save Cancel	

6. In the **Password** field, enter a password.

Note:

In order to connect and integrate into the Active Directory, users must belong to at least one group with read permission on the server. Administrator privileges are not required.

7. In the Domain Controller IP/Hostname 1 section:

Choose from:

- To use *LDAP*, leave the **LDAPS** toggle unselected
- To use *lightweight directory access protocol secure (LDAPS)*, select the **LDAPS** toggle to on.

8. Optional: If necessary, and you chose LDAPS, select Verify SSL.



- 9. If you chose *LDAP*, in the **Port** field, enter a 389. If you chose *LDAPS*, in the Port field, enter 636.
- 10. To check that Active Directory is running correctly on the port, select **Check connection**.
- 11. To add another domain controller *IP* address, select **Add host**.

LDAP

The **LDAP** page shows a list of all the lightweight directory access protocol (LDAP) configurations.

Users management	Users	Groups	OpenAPI Keys	Active Directory	LDAP	SAML
Page 1 of 1, 0 entries					Live 🕚	Add
ACTIONS	USERN	IAME		DISTINGUISH	IED NAME	
There are no LDAP configuration	ons					

Figure 15. LDAP page

Add LDAP users

You can add existing lightweight directory access protocol (LDAP) users for login. LDAP permissions are defined based on the user group.

Before you begin

Make sure that you have:

- The domain name (i.e., pre-Windows 2000 name), referred to as <domainname>
- The domain distinguished name, referred to as <domainDN>
- One or more domain controller *IP* addresses, referred to as <domaincontrollerip>

About this task

The supported *LDAP* formats are:

- v2
- v3

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Users**.

Result: The Users management page opens.

3. In the top right section, select **LDAP**.

Result: The **LDAP** page opens.

4. In the top right section, select **+Add**.

Result: A dialog shows.

5. In the **Username** field, enter a username.

New LDAP Configuration		ж
Status:		
Username		Password
cn=username,cn=group1,dc=nozomi		
Domain Controller IP/Hostname 1		
LDAPS	Port	
e.g. 192.168.0.4 or host.dc.com	389	Check connection
Add host		
Distinguished name		
e.g. dc=nozomi,dc=local		
Connection timeout		
eg 10		
aigs to		
		Save Cancel

Note:

This requires an admin user with full *LDAP* server permission. The **Username** for the *LDAP* server should be a distinguished name (DN) that follows the *LDAP* standard. For example, cn=username, cn=group, dc=nozominetworks, dc=com.

- 6. In the **Password** field, enter a password.
- 7. In the Domain Controller IP/Hostname 1 section:

Choose from:

- To use *LDAP*, leave the **LDAPS** toggle unselected
- To use *LDAPS*, select the **LDAPS** toggle to on.
- 8. Optional: If necessary, and you chose LDAPS, select Verify SSL.

Note:

By default, the server's *SSL* certificate is not verified.

- 9. If you chose *LDAP*, in the **Port** field, enter a 389. If you chose *LDAPS*, in the Port field, enter 636.
- 10. To check that Active Directory is running correctly on the port, select **Check connection**.
- 11. To add another domain controller *IP* address, select Add host.
- 12. In the **Distinguished name** field, enter a value.

- 13. Optional: If necessary, select Connection timeout, and enter a value in seconds.
- 14. To save the changes and validate the data, select **Save**.

Note: If there are errors, they will show next to the **Status** field.

SAML

Nozomi Networks supports security assertion markup language (SAML) single sign-on (SSO) authentication.

Nozomi URL			SAML role a	ttribute key		
https://10.41.43.26			https://nozo	minetworks.com/saml/group-n	ame	
Enter the URL for this Nozon Identity Provider.	ni instance as it	is defined in your	Enter the : defined in G passed into 1 Nozomi grou	SAML attribute key that map uardian to those defined in y the IdP using the SAML attri up to one of its own if the gro	os authenticatior your IdP. Nozomi bute key. The IdF oup is found in th	n values roles are P matches a his attribute.
Metadata XML						
Metadata XML Load the metadata XML file						

Figure 16. SAML page

General

Your *IdP* must be compatible with *SAML* 2.0.

The *SAML* configuration process is often error-prone. To implement *SAML* integration you should be familiar with:

- The SAML protocol
- Your IdP software
- The exact details of your specific IdP implementation

Additional configuration

Typically, *SAML* with authentication, replies are sent back from the same host that originally received the request. Occasionally, *SAML* requests are chained between different *IdPs*, and replies might come from a different host. By default, the Web *UI* content security rules block these types of replies.

You can use the using the csp form-action-urls configuration key to override this behavior.

To accept replies from an *IdP* target *uniform resource locator (URL)* that differs from the one specified in the *SAML* metadata, you can issue the configuration rule: conf.user configure csp form-actionurls <additional_url> in the *command-line interface (CLI)*.

If you need to specify more than one *URL*, you should use spaces to separate them. After this change, you need to run the service webserver stop command, in a shell console to apply it.

Clock skew

Occasionally, the *IdP* and Guardian system times can differ. By default, the system accepts requests with up to 60 seconds difference. You can use the saml clock_drift configuration key to override this behavior.

To change the value, you can issue conf.user configure saml clock_drift <allowed_seconds> in the CLI.

After this change, you can run the service webserver stop command in a shell console to apply it.

Limitations

The SAML logout protocol is not supported.

Configure SAML integration

The **SAML** page lets you add and configure security assertion markup language (SAML).

Before you begin

Make sure that you have defined a new application in your IdP. This should consist of:

- The assertion consumer service (ACS) URL for Nozomi Networks. An ACS specifies the /auth path such as https://10.0.1.10/saml/auth
- The issuer URL for your IdP, which specifies the /saml/metadata path, such as /saml/metadata. This value depends on your IdP
- The metadata eXtensible Markup Language (XML) file that describes the SAML parameters of your *IdP*. Before configuring your Guardian, download the file from your *IdP* vendor and save it to a location accessible to Nozomi Networks.

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the Settings section, select Users.

Result: The Users management page opens.

3. In the top right section, select SAML.

Result: The SAML page opens.

4. In the Nozomi URL field, enter the URL for your Nozomi Networks instance.

Nozomi URL	SAML role attribute key
https://10.41.43.26	https://nozominetworks.com/saml/group-name
Enter the URL for this Nozomi instance as it is defined in your Identity Provider. Metadata XML	Enter the SAML attribute key that maps authentication values defined in Guardian to those defined in your IdP. Nozomi roles are passed into the IdP using the SAML attribute key. The IdP matches a Nozomi group to one of its own if the group is found in this attribute.
Load the metadata XML file	
O Locate and select the metadata XML file provided by your IdP vendor. It describes the SAML parameters Nozomi uses to process authentication requests.	

5. In the **SAML role attribute key** field, enter a string that will be used to map role names between Guardian and your *IdP*.

Note:

The value in this field is used to compare groups defined in Guardian with those defined in your *IdP*. The nature of this value depends on your *IdP*. (For example, if you are using Microsoft Office 365 as your *IdP*, the value might be http://schemas.microsoft.com/ws/2008/06/identity/ claims/role

- 6. Select **Save**.
- 7. On the Guardian login page, select **Single Sign On**.
- 8. To test the integration, use the credentials from your *IdP*.

Note:

For *SAML* to work properly, groups that match *SAML* roles must exist in the system. Groups are found using the role name. For example, if the *SAML* role attribute specifies an **Operator** role, the *IdP* looks for the **Operator** group when authorizing an authenticating user.

Results

SAML has been configured, and the login page shows a new Single Sign On button.

CLI

The **CLI** page lets you change configuration parameters and perform troubleshooting activities.



Figure 17. CLI page

Table 1. Useful commands

Command	Description
help	Shows a list of available commands
history	Shows previously entered commands
clear	Clears the console
find_cmd	Finds available CLI commands with a given sequence of space-separated keywords

Table 2. Keyboard shortcuts

Shortcut	Action
CTRL+R	Reverses search through the command history
esc	Cancels the search
Up arrow	Shows the previous search from the history

Table 2. Keyboard shortcuts (continued)

Shortcut	Action
Down arrow	Shows the subsequent search from the history
tab	Invokes the completion handler

Dashboards

The **Dashboards** page lets you create and configure widget-based dashboards that provide information about your network. The dashboards created here will show on the Guardian home page, and give an overview of the monitored environment.

NOZOMI =			Ś
Settings	Dashboard configuration	Import New dashb	oard Overview -
	Overview	+Add row Distory Delete @Edit Discard Clore	ne ੴExport ₿Save
			+ Add widget
	Top nodes by traffic	Top nodes by traffic	
Dashboards	172.17.9.73: 1.9 %	id_color id label	roles
and the second sec	172.16.60.31: 28.8 %	172.16.60.31	JSON View ["other"
10000	172.16.60.33: 3.3 %	172.16.57.114	JSON View ['backu
and the second sec	172.16.60.32: 4.2 %	52.239.176.74	JSON View ['web_s
10.24.0.50 52.239.176	10.24.0.50: 4.8 % 52.239.176.74: 13.1 % 172.16.57.114: 27.0 %	10.24.0.50	JSON View ["other"
		_	
			+ Add widget
and the second sec	Top Function Codes by count	Top Function Codes by count	
	icmp/3: 2.1 %	id_color protocol fc	description
System	rm samp/GelRequest. 2.4 % sing/Celficequest. 2.7 % oracle-tas/c.6.6 % samp/GelRequest. 51.7 %	snmp GetBulkRequest	n/a
1000		snmp GetResponse	n/a
		oracle-tns 6	Data
		snmp GetNextRequest	n/a
			+ Add widget

Figure 18. Dashboards page

Table 3. Default widgets

Widget	Description
Environment information	This provides a high level view of your network, in terms of the number of assets, nodes, links, protocols and variables
Asset overview	Assets, grouped by Purdue level
Alert flow over time	Alert risk charted over time
Latest alerts	Latest alerts (the most recent being first)
Failed assertions	List of failed assertions

Import

This lets you Import a dashboard (on page 71).

New dashboard

This lets you Create a dashboard (on page 67).

Dashboard selector

This dropdown lets you select from dashboards that already exist.

+ Add row

This lets you add a new row to the dashboard.

History

This lets you revert to a previous version of the dashboard.

Delete

This lets you delete the current dashboard.

Edit

This lets you edit the name and the group of users who can see this dashboard when they log in to the *CMC*.

Discard

This lets you discard the change that you have made to the dashboard.

Clone

This lets you clone the current dashboard to make a new one.

Export

This lets you export the current dashboard in *JavaScript Object Notation (JSON)* format.

Save

This lets you save the changes.

+ Add widget

This lets you add one, or more, widgets to the dashboard, that you can then configure.

Create a dashboard

You can use the **Dashboards** page to load a dashboard that has been created previously.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Dashboards**.

Result: The Dashboard configuration page opens.

3. In the top right section, select **New dashboard**.

Result: A dialog shows.

4. If you want the new dashboard to be based on a template, from the dropdown, select a dashboard.

Choose a dashboard template	×
Template	
Choose among the following 🗸	
	Ok Cancel
Note: If you do not select a template, an empty dashboa	ard will be created.

- 5. Select Ok.
- 6. In the top right section, select **Save**.

Result: A dialog shows.

7. In the **Name** field, enter a name for the dashboard.

Configure dashboard details	×
Name	
Group visibility	
Choose one or more groups -	
Save	el

- 8. From the **Group visibility** dropdown, select one or more groups to add the dashboard to.
- 9. Select **Save**.

Results

The dashboard has been created.

Related information Configure a dashboard (on page 69)

Configure a dashboard

Once a dashboard has been created, you can configure it.

Procedure

1. Choose a method.

Choose from:

- Create a dashboard (on page 67)
- Select a dashboard (on page 71)
- On the homepage after you log in. In the top right section of the dashboard, select the *icon*.
- 2. Optional: In the top right section, select + Add row.

Result: A new row shows.

3. In the top right section, select + Add widget.

Result: A list shows.

4. From the list, select one, or more widgets to add.

Result: The widgets are added to the row.

5. Select somewhere on the screen other than the list.

Result: The list closes.

- 6. **Optional:** If necessary, configure the widget.
 - a. Hover your mouse over the widget. **Result:** The configuration toolbar shows.
 - b. To increase the width of the widget, select ${}^{\leftarrow \rightarrow}$



c. To decrease the width of the widget, select $^{\rightarrow \leftarrow}$

- d. To increase the height of the widget, select $\;\downarrow\;$
- e. To decrease the height of the widget, select
- f. To adjust the height of all of the widgets in the same row, select ${
 m III}$
- g. To move the widget to the left, select
- h. To move the widget to the right, select
- i. To move the widget up to the row above, select igtarrow
- j. To move the widget down to the row below, select lacksquare
- k. To delete the widget, select $ar{\amalg}$
- 7. Select Save.

Results

The dashboard has been configured.

Select a dashboard

You can use the **Dashboards** page to load a dashboard that has been created previously.

Procedure

1. In the top navigation bar, select ξ

Result: The administration page opens.

2. In the **Settings** section, select **Dashboards**.

Result: The Dashboard configuration page opens.

3. In the top right section, select **New dashboard**.

Result: A dialog shows.

4. From the dropdown, select a dashboard.

Results

The applicable dashboard shows.

Import a dashboard

You can use the **Dashboards** page to import an existing dashboard.

About this task

You can export dashboards from the **Dashboards** page, or from the **Export data** page to export dashboards in *JSON* format. These files can then be imported into other *CMCs*.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Dashboards**.

Result: The Dashboard configuration page opens.

3. In the top right section, select Import.

Result: A dialog shows.

4. Select the JSON format dashboard file.

Results

The applicable dashboard has been imported.

Export a dashboard

You can use the **Dashboards** page to export an existing dashboard.

About this task

This procedure shows you how to export a dashboard from the **Dashboards** page. To export from the **Export data** page, see **System > Export > Export a content pack**. You can export dashboards from the **Dashboards** page, or from the **Export data** page.

Procedure

1. In the top navigation bar, select $\overleftrightarrow{\mathbb{S}}$

Result: The administration page opens.

2. In the **Settings** section, select **Dashboards**.

Result: The Dashboard configuration page opens.

3. In the top right section, select **Export**.

Results

The applicable dashboard has been exported in *JSON* format.
Threat Intelligence

The **Threat Intelligence** page lets you manage packet rules, YARA rules, Sigma rules, structured threat information expression (STIX) indicators and vulnerabilities to provide detailed threat information.

NOZOMI =							Ś
Settings	Threat Inte	lligence	Packet rules	Yara rules	Sigma rules	STIX indicators	Vulnerabilities
	Page 1 of 29, 7	20 entries				Liv	• • • • • • • • • • • • • • • • • • •
	Actions	Enabled		Name		Source	Created at
						. •	н∢⊧н
	- e q	ON OFF	NN-2021-0026			update_service	2021-10-07
	□ a q	ON OFF	WAGO Command Reboot			update_service	2020-06-02
Threat Intelligence		ON OFF	NN-2023-0062 and NN-2023	-0063		update_service	2023-05-29
	- a q	ON OFF	NN-2023-0030			update_service	2023-08-04
	- e q	ON OFF	NN-2023-0064			update_service	2023-05-29
	- e q	ON OFF	WAGO Command Device In	fo		update_service	2020-06-02
	- e q	ON OFF	CVE-2018-7794			update_service	2020-06-02
	- e q	ON OFF	CVE-2018-5452			update_service	2020-06-02
	- e q	ON OFF	NN-2023-0055 and NN-2023	-0056		update_service	2023-05-26
	□ = q	ON OFF	CVE-2018-5452			update_service	2020-06-02
	- A Q	ON OFF	Emerson DeltaV Telnet DoS			update_service	2020-06-02
vstem	□ = q	ON OFF	NN-2023-0057 and NN-2023	-0058		update_service	2023-05-26
,		ON OFF	Permanent denial of service	on Dahua Face Recogn	nition Access Controller	update_service	2021-10-22
	□ = q	ON OFF	NN-2023-0059			update_service	2023-05-30
		ON OFF	CVE-2020-25173			update_service	2020-06-24
	□ ≙ Q	ON OFF	TransLogic TLP20 Malforme	d Large		update_service	2021-08-03
	■ Q	ON OFF	NN-2023-0080			update_service	2023-06-29
	□ ≜ Q	ON OFF	CVE-2021-31988			update_service	2021-09-10
	■ a	ON OFF	CVE-2021-31987			update_service	2021-09-28
	□ ≜ Q	ON OFF	CVE-2021-32941			update_service	2021-04-21
	□ ≙ Q	ON OFF	CVE-2021-31987			update_service	2021-09-28
	□ ≙ Q	ON OFF	CVE-2021-31986			update_service	2021-09-29
	■ a	ON OFF	CVE-2021-41773			update_service	2021-10-06
		ON OFF	NN-2023-0068			update_service	2023-06-22
	□ ≙ Q	ON OFF	NN-2023-0051 and NN-2023	-0052		update_service	2023-05-25

Figure 19. Threat Intelligence page

The Threat Intelligence page has these tabs:

- Packet rules (on page 74)
- Yara rules (on page 75)
- Sigma rules (on page 76)
- STIX indicators (on page 77)
- Vulnerabilities (on page 78)

Packet rules

The **Packet rules** page lets you manage the packet rules for Threat Intelligence.

nreat Inte	elligence	Packet rules	Yara rules	Sigma rules	STIX indicators	Vulnerabilities
Page 1 of 29 , 1	719 entries					Live
ACTIONS	ENABLED		NAME		SOURC	E CREATED AT
■ ≙ Q	ON OFF	NN-2021-0026			update_ser	vice 2021-10-07
□ ≜ Q	ON OFF	WAGO Command Reboot	WAGO Command Reboot			vice 2020-06-02
■ a q	ON OFF	NN-2023-0062 and NN-2023	NN-2023-0062 and NN-2023-0063			vice 2023-05-29
🗆 🔒 Q	ON OFF	NN-2023-0030	NN-2023-0030		update_ser	vice 2023-08-04
🗏 🔒 Q	ON OFF	NN-2023-0064			update_ser	vice 2023-05-29
□ a q	ON OFF	WAGO Command Device In	fo		update_ser	vice 2020-06-02
■ Q	ON OFF	CVE-2018-7794			update_ser	vice 2020-06-02
□ ≜ Q	ON OFF	CVE-2018-5452	CVE-2018-5452			vice 2020-06-02
■ a q	ON OFF	NN-2023-0055 and NN-2023-0056			update_ser	vice 2023-05-26
□ ≜ Q	ON OFF	CVE-2018-5452			update_ser	vice 2020-06-02
■ a a	ON OFF	Emerson DeltaV Telnet DoS	Emerson DeltaV Telnet DoS			vice 2020-06-02
	ON OFF	NN-2023-0057 and NN-2023	-0058		update_ser	vice 2023-05-26

Figure 20. Packet rules page

Packet rules are executed on every packet. They raise an alert of type SIGN: PACKET-RULE if a match is found.

Live / refresh

The Live icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a new packet rule.

Yara rules

The Yara rules page lets you manage the Yara rules for Threat Intelligence.

Threat Int	elligence	Packet rules	Yara rules	Sigma rules	STIX indicators	Vulnerabilities
Page 1 of 82 ,	2028 entries					Live • 👩 + Add
ACTIONS	ENABLED	NAME			SOUR	CREATED AT
□ ≜ Q	ON OFF	ENTERPRISE_EXPLOIT_INCO	ONTROLLER_AsRock-PE)B-silent.yar	update_se	rvice 2022-04-12
□ a q	ON OFF	ENTERPRISE_RAT_ICECORE	ENTERPRISE_RAT_ICECORE_integrityinitkey-silent.yar			rvice 2022-04-12
■ a	ON OFF	ENTERPRISE_EXPLOIT_INCO	ENTERPRISE_EXPLOIT_INCONTROLLER_AsRock-Generic-silent.yar			rvice 2022-04-12
□ ≞ q	ON OFF	ENTERPRISE_RAT_(PassCV)	ENTERPRISE_RAT_{PassCV}Saber_Malware_4.yar			rvice 2016-10-20
■ A Q	ON OFF	ENTERPRISE_RAT_TAIDOOR	ENTERPRISE_RAT_TAIDOOR_sample.yar			rvice 2020-06-18
🗆 🖴 Q	ON OFF	ENTERPRISE_HACKTOOL_(E	Equation)jparsescan_sar	nple.yar	update_se	rvice 2017-04-08
- a q	ON OFF	ENTERPRISE_RAT_(APTI)AU	RIGA_module.yar		update_se	rvice 2019-02-06
🗆 🖴 Q	ON OFF	ENTERPRISE_RANSOMWAR	E_LockerGoga_sample.	yar	update_se	rvice 2019-03-20
A 4	ON OFF	ENTERPRISE_INFOSTEALER_(Strider)ProjectSauron_basex-module.yar update_service			rvice 2016-08-08	
□ ≞ q	ON OFF	ENTERPRISE_TROJAN_(APT20)Generic_Agent-pyyar update_service 2020			rvice 2020-01-08	
■ A	ON OFF	ENTERPRISE_RANSOMWARE_FenixLocker_sample.yar update_service 2021-05-10				
🗆 🖴 Q	ON OFF	ENTERPRISE_RAT_GORAT_s	ample_1.yar		update_se	rvice 2020-12-09

Figure 21. Yara rules page

YARA rules are executed on every file transferred over network protocols such as *hypertext transfer protocol (HTTP)* or *server message block (SMB)*. When a match is found, an alert of type SIGN:MALWARE-DETECTED is raised.

Live / refresh

The Live of icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a new Yara rule.

Sigma rules

The **Sigma rules** page lets you manage the Sigma rules for Threat Intelligence that are applicable in an Arc deployment.

hreat Inte	elligence	Packet rules	Yara rules	Sigma rules	STIX indicators	Vulnerabilities
Page 1 of 5, 10	4 entries				I	Live • 🕥 + Add
ACTIONS	ENABLED	NAME			SOURCE	CREATED AT
■ a q	ON OFF	ENTERPRISE_SUSPICIOUS	_Generic_TPM-activity	yml	update_service	2023-02-16
□ ≙ Q	ON OFF	ENTERPRISE_MINER_Gen	eric_commandline.yml		update_service	2021-10-26
■ a Q	ON OFF	ENTERPRISE_TROJAN_Get	neric_SSP-persistence;	/ml	update_service	2019-01-18
□ ≞ Q	ON OFF	ENTERPRISE_HACKTOOL_	pypykatz_lsass-dump-	calltrace.yml	update_service	2021-08-03
■ Q	ON OFF	ENTERPRISE_RANSOMWA	ENTERPRISE_RANSOMWARE_Maze_main.yml			2020-05-08
□ ≜ Q	ON OFF	ENTERPRISE_HACKTOOL_	Generic_SAMTHEADM	IN.yml	update_service	2022-09-09
■ a	ON OFF	ENTERPRISE_DROPPER_(Turla)Generic_PNG-dro	pper-WerFaultSvc.yml	update_service	2018-11-23
□ ≙ Q	ON OFF	ENTERPRISE_RANSOMWA	RE_Snatch_command	line.yml	update_service	2020-08-26
■ a q	ON OFF	ENTERPRISE_ROOTKIT_M	ENTERPRISE_ROOTKIT_Moriya_path.yml			2021-05-06
□ ≙ Q	ON OFF	ENTERPRISE_EXPLOIT_CVE-2021-41379_privilege-escalation.yml			update_service	2021-11-22
= e Q	ON OFF	ENTERPRISE_HACKTOOL_Dumpert_dump-file.yml			update_service	2020-02-04
□ ≜ Q	ON OFF	ENTERPRISE_RAT_PowerE	Drop_script.yml		update_service	2023-05-16

Figure 22. Sigma rules page

Sigma rules are versatile and generic rules written in the Sigma language. Primarily employed in threat detection and *security information and event management (SIEM)* systems, Sigma rules aim to standardize and offer a uniform method for describing log patterns across diverse security devices, applications, and platforms.

Live / refresh

The Live icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a new Sigma rule.

STIX indicators

The **STIX indicators** page lets you manage the structured threat information expression (STIX) indicators for Threat Intelligence.

nreat Intel	ligence	Packet rules	Yara rules	Sigma rules	STIX indicators	Vulnerabilities
Page 1 of 159, 3964 entries						Live
ACTIONS	ENABLED		NAME		SOURCE	CREATED AT
■ a q	ON OFF	Ukrainian DELTA sys	ems attack - RomCom	1	update_service	2023-02-03
□ ≜ Q	ON OFF	Reversing Labs @ 20	Reversing Labs @ 2023-04-07			2023-04-07
■ a	ON OFF	Covenant C2			update_service	2023-05-10
□ ≜ Q	ON OFF	Phishing emails lead	ing to information stea	aler trojans	update_service	2023-02-03
■ a q	ON OFF	Forshare - RAT			update_service	2023-02-03
🗆 🖴 Q	ON OFF	Trojan			update_service	2023-08-11
🗆 🖴 Q	ON OFF	Trojan			update_service	2023-07-06
🗆 🖴 Q	ON OFF	Trojan			update_service	2023-05-10
■ a q	ON OFF	Trojan	Trojan		update_service	2023-02-03
□ ≙ Q	ON OFF	sPowerShell - DROPPER		update_service	2023-02-03	
■ a q	ON OFF	MTS-ISAC - 071223			update_service	2023-07-20
□ a q	ON OFF	Generic IoT threats			update_service	2023-03-28

Figure 23. STIX indicators page

Structured Threat Information Expression (STIX) indicators contain information about malicious IP addresses, URLs, malware signatures, or malicious domain name server (DNS) domains. This information enriches existing alerts and raises new ones.

Live / refresh

The Live icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a new *STIX* indicator.

Vulnerabilities

The **Vulnerabilities** page lets you manage the vulnerabilities for Threat Intelligence.

reat Intelligence	Packet rules	Yara rules	Sigma rules	STIX indicators	Vulnerabilities	
Page 1 of 3, 55 entries					Live 💽 🕥	
	Name			S	Source	
					- •	
nvdcve-2.0-2023				update_service		
nvdcve-2.0-2022				update_service		
nvdcve-2.0-2021				update_service		
nvdcve-2.0-2019				update_service		
nvdcve-2.0-2017				update_service		
nvdcve-2.0-2016				update_service		
nvdcve-2.0-2015				update_service		
nvdcve-2.0-2013				update_service		
nvdcve-2.0-2011				update_service		
nvdcve-2.0-2009				update_service		
nvdcve-2.0-2007				update_service		

Figure 24. Vulnerabilities page

Vulnerabilities are assigned to each node, depending on the installed hardware, *operating system (OS)*, and the software identified in the traffic. The software uses *Common Vulnerabilities and Exposures (CVE)*, a dictionary that gives definitions for publicly-disclosed cybersecurity vulnerabilities and exposures.

Live / refresh

The Live \bigcirc icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a new vulnerability.

Custom fields

The **Custom fields** page lets you create a custom field to the **Nodes** (All-In-One CMC only) and **Assets** tables. A custom field lets you add information that might be relevant to your organization, and cannot be extracted from network traffic.

				ŝ
Settings	Custom f	ields		
	Page 1 of 1,	2 entries	Live 🖲	• 🗇 🕇 Add
	Actions	Name	Туре	Source
	0	TestPropagate	string	Downstream
		Daniel_2024_FROM_https:nozominetworkscom.customers.eu1.staging-slfkjne-vantage.nozominetworks.io	string	Upstream
Custom fields				

Figure 25. Custom fields page

Live / refresh

The Live of icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a custom field.

Data integration

Data integration overview

An overview of **Data integration** in the Nozomi Networks software.

The Nozomi Networks solution uses third-party platforms to exchange data, in specific formats and methods. After configuring the endpoints of the third-party platforms for data integration, Guardian generates messages for:

- Alerts
- Health
- Audits

Connectivity status and status is checked with the data integration endpoint. The third-party platforms that the Nozomi Networks solution uses for exchanging data are:

- Google Chronicle (Ingestion API UDM)
- IBM QRadar (LEEF)
- Common Event Format (CEF)
- ServiceNow
- Tanium
- Splunk Common Information Model (JSON)
- SMTP forwarding
- SNMP trap
- Syslog Forwarder
- Custom JSON
- Custom CSV
- DNS Reverse Lookup
- Kafka
- Cisco ISE
- External Storage
- Microsoft Endpoint Configuration Manager (WinRM RPC)
- Microsoft Endpoint Configuration Manager (DB)
- NetWitness
- Aruba ClearPass
- CarbonBlack Defense

Data integration

The **Data integration** page lets you exchange data with different third-party platforms.

NOZOMI =			ŝ
Settings	Data integration Page 1 of 1 0 entries	Liv	ve 🖲 🚑 🕂 Add
	Actions To URI Endpoint Configured as Connectivity status	Status	Last sent data
	There are no endpoints		
Data integration			

Figure 26. Data integration page

Live / refresh

The Live \bigcirc icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

This lets you add a new endpoint.

Google Chronicle (Ingestion API - UDM)

This integration lets you forward alerts, asset information and vulnerabilities to an instance of Google Chronicle.

To configure this integration, you need to upload the Service Account file and to specify the matching customer *ID*.

New Endpoint	×
Endpoint Configured as	
Google Chronicle (Ingestion API - UDM) 🗸	
To URI	
https://malachiteingestion-pa.googleapis.com	
Customer ID	
Import Service Account file	
\Box Send historical data as well as new data	
Enable sending Alerts	
Send only Alerts following Security Profile	
Alert query filter	
e.g. 'where risk > 6'	
Enable sending Asset information	
Enable sending Vulnerabilities	
New Endpoint Cancel	

Figure 27. Google Chronicle dialog

IBM QRadar (LEEF)

The IBM QRadar integration lets you send all alerts, and optionally health logs, in LEEF format. You can also send asset information to QRadar beginning with version 2.0.0 of the QRadar App.

You can select How this integration works to view additional details.

New Endpoint		×
Endpoint Configured as		
IBM QRadar (LEEF) 🗸		
How this integration we	orks	
Description		
To URI		
[TCP-UDP://]HOST:PORT		
 Send historical data as well as new data Enable sending Alerts 		
\Box Send only Alerts following Security Profile		
Alert query filter		
e.g. 'where risk > 6'		
Enable sending Health Logs		
Enable sending Asset information		
	New Endpoint C	ancel

Figure 28. IBM QRadar (LEEF) dialog

Common Event Format (CEF)

CEF lets you send alerts and health logs in CEF format. You can also enable encryption of the data through the TLS checkbox and check the validity of the CEF server's certificate with the CA-emitted **TLS** certificate checkbox.

You can select **How this integration works** to view additional details.

New Endpoint	×
Endpoint Configured as	
Common Event Format (CEF) 🕶	
How this integration works	
Description	
TLS Enabled Disabled To URI	
[TCP-UDP://]HOST:PORT	
Send historical data as well as new data	
Enable sending Alerts	
Send only Alerts following Security Profile	
Enable sending node custom fields	
Alert query filter	
e.g. 'where risk > 6'	
Enable sending Audit Logs	
Enable sending Health Logs	
New Endpoint Canc	el

Figure 29. Common Event Format (CEF) dialog

Custom fields

The Nozomi Networks solution has defined custom label fields in our common event format (CEF) implementation. Ensure that your integration recognizes these custom labels and deals with them appropriately.

Field Value	Label Value	Label Sample	Field Sample
csl	cslLabel	Risk	Risk level for the alert
cs2	cs2Label	IsSecurity	Is this a security alert
cs3	cs3Label	ld	Alert ID (not Alert Type ID) of the alert in the Nozomi system
cs4	cs4Label	Detail	Alert details
cs5	cs5Label	Parents	Parent IDs of the alert if related to others
cs6	cs6Label	n2os_schema	This is the Nozomi Schema version
flexString1	flexString1Label	mitre_attack_techniques	T0843
flexString2	flexString2Label	mitre_attack_tactics	Impair Process Control, Inhibit Response Function, Persistence
flexString3	flexString3Label	Name	Suspicious Activity

The *common event format (CEF)* data integration now sends the name attribute of alerts in the flexString CEF field. For example:

```
nozomi-ids.local n2osevents[0]: CEF:0|Nozomi Networks|N2OS|
21.9.0-01051414_C13FC|SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS|Multiple
unsuccessful logins|8|
app=smb
dvc=172.16.193.105
dvchost=nozomi-ids.local
cs1=8.0
cs2=true
cs5=["22114bf0-813c-434c-b4d7-933d2a54b4e1"]
cs6=3 cs1Label=Risk
cs2Label=IsSecurity
cs3Label=Id
```

```
cs5Label=Parents
cs6Label=n2os_schema
flexString1=T0843
flexString1Label=mitre_attack_techniques
flexString2=impair_process_control, inhibit_response_function,
persistence
flexString2Label=mitre_attack_tactics
flexString3=suspicious_activity
flexString3Label=name
dst=192.168.1.77
dmac=f0:1f:af:f1:40:5c
dpt=445
msg=Multiple unsuccessful logins detected with protocol smb. The
usernames
'', 'DOMAIN\VCA07_12$' attempted at least 40 connections in 15 seconds
src=192.168.1.227
smac=d8:9e:f3:3a:cb:3a
spt=57280
proto=TCP
start=1651456283700
```

ServiceNow

The ServiceNow integration allows you to receive asset information from a ServiceNow instance and enrich local nodes.

You can select How this integration works to view additional details.

New Endpoint	×
Endpoint Configured as	
ServiceNow -	
How this integration works	
Description	
To URI	
https://instance.service-now.com	
 The strategy receives asset information from ServiceNow using HTTP R 	EST API
Password	
Node query filter	
e.g. 'where ip in_subnet? 192.168.1.0/24'	
New Endpoint	Cancel

Figure 30. ServiceNow dialog

Tanium

This integration enables seamless forwarding of node and asset data to a Tanium instance, facilitating centralized management and enhanced visibility within your network.

You can select How this integration works to view additional details.

Note:

If the Tanium instance does not have a valid signed *hypertext transfer protocol* secure (HTTPS) certificate authority (CA), users must add an ! before the URL. For example, !https://192.168.1.1



Nodes are sent, not assets.

Note:

Nodes are sent regardless of whether MAC addresses are confirmed or not (all nodes).



Note:

If integrating with the CMC, use All-In-One mode. This is because multicontext a CMC does not have nodes.

New Endpoi	nt			×
Endpoint Configured	d as			
	Т	Tanium 🗸		
	<u>How this i</u>	ntegration wor	<u>ks</u>	
Description				
To URI				
https://instance.taniu	m.com			
Username				
Password				
Node query filter				
e.g. 'where ip in_subr	et? 192.168.1.0/24'			
Receive assets	Send assets			
			New Endpoint	Cancel

Figure 31. Tanium dialog

Receive assets

The integration can be configured to receive asset data from Tanium. When configuring the integration to receive data, it is important to ensure that only one integration at a time is designated to interact with a specific endpoint. This means that if you have an integration set to receive data from an endpoint, another integration should not be set to send data to that same endpoint. This will help to avoid potential conflicts, or data inconsistencies.

Send assets

The integration can be configured to send asset data to Tanium. When configuring the integration to send data, it is important to ensure that only one integration at a time is designated to interact with a specific endpoint. This means that if you have an integration set to send data to an endpoint, another integration should not be set to receive data to that same endpoint. This will help to avoid potential conflicts, or data inconsistencies.

Splunk - Common Information Model (JSON)

If you need to send alerts to a Splunk - JavaScript Object Notation (JSON) instance, you can use integration. Data are sent in JSON format and you are also able to filter on alerts. You can also send health logs and audit logs.

You can select **How this integration works** to view additional details.

New Endpoint	×
Endpoint Configured as	
Splunk - Common Information Model (JSON) 🗸	
How this integration works	
Description	
To URI	
[TCP-UDP://]HOST:PORT	
(i) You need to specify the URI of a Splunk Forwarder able to accept data from a TCP or UDP port in the JSON format.	
\Box Send historical data as well as new data	
Enable sending Alerts (Intrusion Detection CIM)	
Send only Alerts following Security Profile	
Alert query filter	
e.g. 'where risk > 6'	
Enable sending Health Logs (Performance CIM)	
Enable sending Audit Logs (Change CIM)	
New Endpoint Cance	əl

Figure 32. Splunk dialog

SMTP forwarding

To send reports, alerts and/or health logs to an email address, you can configure a simple mail transfer protocol (SMTP) forwarding endpoint. In this case, you are also able to filter alerts.

New Endpoint	×
Endpoint Configured as	
SMTP forwarding 🗸	
Description	
To URI	
[SMTP://]HOST[:PORT]	
Email subject suffix	
Send historical data as well as new data	
Enable sending Report	
Enable sending Health Logs	
Enable sending Alerts	
Send only Alerts following Security Profile	
Alert query filter	
e.g. 'where risk > 6'	
Sender	
Recipients (comma separated)	
STARTTLS	
Authentication Mechanism: O NO AUTH PLAIN O LOGIN	
Username	
Password	
New Endpoint Cance	

Figure 33. SMTP forwarding dialog

SNMP trap

Use this kind of integration to send alerts through a simple network management protocol (SNMP) trap.

New Endpoint	2
Endpoint Configured as	
SNMP Trap 🗸	
To URI	
snmptrap://HOST[:PORT]/COMMUNITY/OID	
Alert query filter	
e.g. 'where risk > 6'	
	New Endpoint Cancel

Figure 34. SNMP trap dialog

Syslog Forwarder

Use this type of integration to send syslog events captured from monitored traffic to a syslog endpoint.

It is useful for passively capturing logs and forwarding them to a SIEM.

Note:

In order to enable syslog events capture see Enable Syslog capture feature in the Basic configuration section of the Configuration chapter of this manual.

New Endpoint	Ç
Endpoint Configured as	
Syslog Forwarder 🗸	
Description	
To URI	J
[TCP-UDP://]HOST:PORT	
(1) This integration allows to forward syslog entries captured in the network to Syslog server. To use it the passive log collection functionality has to be added - add probe protocol syslog capture_logs true in the n2os.conf.user file and reload the n2osids service.	
New Endpoint Cancel	

Figure 35. Syslog Forwarder dialog

Custom JSON

This type of integration uses the JavaScript Object Notation (JSON) format to send the results of the related query to a specific uniform resource identifier (URI).

New Endpoint	×
Endpoint Configured as	
Custom JSON 🗸	
Description	
To URI	
[TCP-UDP://]HOST:PORT	
Query	
e.g. 'variable_history sort time desc'	
	New Endpoint Cancel

Figure 36. Custom JSON dialog

Custom CSV

_

This type of integration sends the results of the specified query to a specific URI in comma-separated value (CSV) format.

New Endpoint		×
Endpoint Configured as		
Custom CSV 🗸		
Description		
To URI		
[TCP-UDP://]HOST:PORT		
Query		
e.g. 'variable_history sort time desc'		
	New Endpoint Cance	9

Figure 37. Custom CSV dialog

DNS Reverse Lookup

This integration sends reverse domain name server (DNS) requests for the nodes in the environment and uses the names provided by the DNS as nodes' labels. You can pre-filter the nodes by specifying a query filter.

The strategy runs once a day by default, but you can select **Rerun the strategy on all the data** to run it on demand.

New Endpoint		
Endpoint Configured as		
DNS Revers	e Lookup v	
Description		
To URI		
UDP://HOST[:PORT]		
Node query filter		
e.g. 'where ip in_subnet? 192.168.1.0/24'		
\Box Rerun the strategy on all the data		
	New Endpoir	t Cancel

Figure 38. DNS Reserve Lookup dialog

Kafka

The Kafka integration allows you to send the results of custom queries in JavaScript Object Notation (JSON) format to existing topics of a Kafka cluster.

You can select How this integration works to view additional details.

New Endpoint		×
Endpoint Configured as		
Kafka	▼	
How this integ	ration works	
Description		
To URI		
HOST:PORT		
Use SSL		
Query	Topic Name	
e.g. 'variable_history sort time desc'		
Add query		
\Box Create additional extended log file		
	New Endpoint Ca	ncel

Figure 39. Kafka dialog

Cisco ISE

With the Cisco ISE integration, you can use the simple text-oriented messagingprotocol (STOMP) to send the results of custom node queries to Cisco's ISE asset information, or you can use hypertext transfer protocol (HTTP) to receive asset information from a Cisco ISE instance and enrich local nodes.

You can select **How this integration works** to view additional details about certificate usage and Cisco ISE environment requirements.

Send assets configuration

New Endpoint	×
Endpoint Configured as	
Cisco ISE 🗸	
How this integration works]
Description	
To URI	
https://instance.cisco_ise.com	
Send assets Enrich assets	
Client name	
Import a CA certificate	
Import a certificate	
Import a key	
Key password	
Specify pxGrid key password	
Enable update Asset information	
Node query filter	
e.g. 'where ip in_subnet? 192.168.1.0/24'	
New Endpoint Car	ncel

Figure 40. Send assets dialog

To configure Cisco ISE, you need to create these custom string attributes:

- n2os_change_flag
- n2os_operating_system
- n2os_product_name
- n2os_vendor
- n2os_type
- n2os_appliance_site
- n2os_zone

You then need to create a new profile and set the required condition n2os_change_flag custom attribute equal to change.

You then need to modify the existing profiles or, if no profiles are expected to be assigned to assets from n2os, create a new profile. Add the required condition for n2os_change_flag.

Note:

Due to a long-standing bug in Cisco's PxGrid *API*, the performance when sending assets is halved, requiring two network calls for each updated record. Nozomi Networks is working with Cisco to address this issue. Cisco has not provided a target date for this bug.

Enrich assets

New Endpoint	×
Endpoint Configured as	
Cisco ISE 🗸	
How this integration works	
Description	
To URI	
https://instance.cisco_ise.com	
Send assets Enrich assets	
Username	
Password	
Import a certificate	
Import a key	
Node query filter	
e.g. 'where ip in_subnet? 192.168.1.0/24'	
New Endpoint Canc	el

Figure 41. Enrich assets dialog

External Storage

The external storage integration uploads files to an external machine. This enables the external machine to keep remote copies of files that are kept beyond the retention settings.

The file location becomes transparent to the user, who can retrieve them seamlessly from external storage when the files are removed from the local file system. You can also choose a connection protocol for storing the files. Available protocols are *SMB*, *file transfer protocol (FTP)*, and *SSH*.

Important:

Microsoft *OSs* are the only *OS* that support the *SMB* connection protocol. Compatibility with third-party devices is not guaranteed. These devices might require additional configuration changes, that include:

- Permission changes
- The creation of new network shares
- The creation of new users

Kerberos authentication is not supported.

This functionality is currently only available for trace *packet capture (pcap)* files on Guardian.

New Endpoint	×
Endpoint Configured as	
External Storage 🗸	
Description	
To URI	
Enable sending Traces	
① It includes alert traces and user requested traces	
Send historical data as well as new data	
Enable sending Continuous Traces	
(1) It includes only completed continuous traces	
Storage	
Choose a storage location/protocol 🗸	
	_
New Endpoint Cance	

Figure 42. External Storage dialog

Microsoft Endpoint Configuration Manager (WinRM RPC)

With the Windows Remote Management (WinRM) RPC, you can collect information coming from the Microsoft Endpoint Configuration Manager to update Windows nodes.

Collected items:

- **OS information**: Returns **OS** information as version, service pack, build and architecture
- Hostnames: Returns host name information to configure the node label
- Interfaces information: Returns interface data to populate the node MAC address
- **Installed software**: Returns installed software and populates the node *Common Platform Enumeration (CPE)*
- **Hotfixes**: Returns installed software version updates and checks to see if there are node *CVEs* to close

Note:

It is important to filter the strategy nodes because without the filter, the strategy waits for the timeout of non-Microsoft nodes that are not reachable. This significantly decreases the performance of the data integration strategy. If not specified, the port is the default: 5986 if *SSL* is enabled, 5985 otherwise.

New Endpoint	×
Endpoint Configured as	
Microsoft Endpoint Configuration Manager (WinRM RPC) $ullet$	
To URI	
microsoft.endpoint.configuration.manager.instance.com	
Use SSL	
Username	
username@domain-name	
Password	
Choose items to collect	
\Box OS information	
□ Hostnames	
□ Interfaces information	
Installed software	
□ Hotfixes	
Node query filter	
e.g. 'where os include? Window'	
New Endpoint Canc	el

Figure 43. Microsoft Endpoint Configuration Manager (WinRM RPC) dialog

Microsoft Endpoint Configuration Manager (DB)

The goal of this integration is to collect information from the Microsoft Endpoint Configuration Manager DB to update the existing Windows nodes.

Collected items:

- **OS information**: Returns *OS* information as version, service pack, build and architecture
- Hostnames: Returns host name information to configure the node label
- Interfaces information: Returns interface data to populate the node MAC address
- Installed software: Returns installed software and populates the node CPE
- **Hotfixes**: Returns installed software version updates and checks to see if there are node *CVEs* to close

Note:

It is important to filter the strategy nodes because without the filter, the unreachable non- Microsoft nodes time out, significantly decreases timing of the data integration. If not specified, the port is the default: 5986 if *SSL* is enabled, 5985 otherwise. The database name default value format is CM_[Site code], which may be changed by an administrator.

New Endpoint	×
Endpoint Configured as	
Microsoft Endpoint Configuration Manager (DB) 🗸	
How this integration works	
To URI	
microsoft.endpoint.configuration.manager.instance.com	
Use SSL	
Username	
username@domain-name	
Password	
Database name	
Choose items to collect	
□ OS information	
Interfaces information	
Installed software	
Node query filter	
e.g. 'where os include? Window'	
New Endpoint Canc	el

Figure 44. Microsoft Endpoint Configuration Manager (DB) dialog

NetWitness

If you require sending alerts to a NetWitness instance, you can utilize this integration. Data is transmitted in JavaScript Object Notation (JSON) format prepended by the **NOZOMI:** header. You can also apply filters, and determine whether historical data should be sent or not.

New Endpoint	×
Endpoint Configured as	
NetWitness 🗸	
Description	
To URI	
[TCP-UDP://]HOST:PORT[?max-size=10000]	
() You need to specify the URI of a NetWitness instance capable of receiving of from a TCP or UDP port.	data
\Box Send historical data as well as new data	
Enable sending Alerts	
Send only Alerts following Security Profile	
Alert query filter	
e.g. 'where risk > 6'	
New Endpoint Ca	ncel

Figure 45. NetWitness dialog
Aruba ClearPass

This integration lets you send node information to Aruba ClearPass. Only nodes with confirmed media access control (MAC) addresses are sent. You can specify a query filter to pre-filter the nodes. If **Enable update Node information** is not selected, nodes are only sent once.

New Endpoint		×
Endpoint Configured as		
Aruba ClearPass 🗸		
Description		
To URI		
HOST		
Node query filter		
e.g. 'where ip in_subnet? 192.168.1.0/24'		
Enable update Node information		
Username		
Password		
Bearer Token		
	New Endpoint	Cancel

Figure 46. Aruba ClearPass dialog

CarbonBlack Defense

The strategy runs once a day by default. The strategy uses its representational state transfer (REST) application programming interface (API) over hypertext transfer protocol secure (HTTPS) to extract information about nodes from an external CarbonBlack service.

New Endpoint	>
Endpoint Configured as	
CarbonBlack Defense 🗸	
Description	
To URI	
HOST	
Node query filter	
e.g. 'where ip in_subnet? 192.168.1.0/24'	
Organization key	
API key	
API ID	
 This integration allows you to receive nodes information from an external CarbonBlack Defense service, specifically it extracts Windows OS details. 	
New Endpoint Cano	cel

Figure 47. CarbonBlack Defense dialog

Nozomi syslog data events and syslog messages

For customers implementing syslog, Guardian generates three types of syslog events: alerts, health, and audit.

Note:

As the set of alert messages inside each alert type ID category increases over time, perform searches on alert type IDs, health type IDs, and audit type IDs, rather than on the alert message itself.

Alert events

A description of alert events in common event format (CEF).

Alert events

Alert events should be identified by the alert type ID. There are many alert types in the Nozomi Networks environment.

For a full list of alert types, see **Alerts** in the **Alerts and Incidents - Reference Guide**.

Alert events in CEF have the following format, as shown in this example:

```
<137>Oct 17 2019 22:32:23 local-sg-19.x n2osevents[0]: CEF:0|Nozomi
Networks |N2OS | 19.0.3-10142120_A2F44 | SIGN:MALWARE-DETECTED | Malware
detected
                    9
                    app=smb
                    dvc=172.16.248.11
                    dvchost=local-sg-19.x
                    cs1=9.0
                    cs2=true
                    cs3=d25c520f-7f79-4820-b5ae-d1b334b05c75
                    cs4={trigger_type: yara_rules, trigger_id:
MALW_DragonFly2.yar}
                    cs5=["5740a157-08e8-490f-85ad-eef23657e3cb"]
                    cs6=1
                    cs1Label=Risk
                    cs2Label=IsSecurity
                    cs3Label=Id
                    cs4Label=Detail
                    cs5Label=Parents
                    cs6Label=n2os_schema
                    flexString1=T0843
                    flexString1Label=mitre_attack_techniques
                    flexString2=Impair process (etc)
                    flexString2Label=mitre_attack_tactics
                    flexString3=Suspicious Activity
                    flexString3Label=name
                    dst=172.16.0.55
                    dmac=00:0c:29:28:dd:c5
                    dpt=445
                    msg=Suspicious transferring of malware named
 'TemplateAttack_DragonFly_2_0'
                    was detected involving resource '\\172.16.0.55\ADMIN
                    \CVcontrolEngineer.docx' after a 'read' operation
 [rule author: US-CERT
                    Code Analysis Team - improved by Nozomi Networks]
[yara file name:
                    MALW_DragonFly2.yar]
                    src=172.16.0.253
                    smac=00:04:23:e0:04:1c
                    spt=1148
                    proto=TCP
                    start=1571351543431
```

Note the **highlighted** part of the Alert message. This is the Alert Type *ID*. This should be used as the key for performing searches once Nozomi Networks syslog events have been ingested into the integration platform.

Best practice

Make sure that your parsing logic extracts the appropriate data. If you are integrating with *CEF* messages, a *CEF* parser must be used. Do not use regular expressions. This will ensure the integration integrity in the future. When using the correct parser for the data that is expected, be sure to test different inputs to ensure that data is correctly extracted from the messages.

Health events

A description of health events in common event format (CEF).

Health events

Health events in CEF have the following format, as shown in this example:

<131>Oct	10	2019	15:57:48 local-sg-19.x n2osevents[0]: CEF:0 Nozomi
			Networks N2OS 19.0.3-10201846_FD825 HEALTH Health
problem	0		
			dvchost=local-sg-19.x
			cs6=1
			cs6Label=n2os_schema
			msg=LINK_DOWN_on_port_em0

Note the **highlighted** part of the health message. This is the health type *ID*. This should be used as the key for performing searches once Nozomi Networks syslog events have been ingested into the integration platform.

Best practice

Make sure that your parsing logic extracts the appropriate data. If you are integrating with *CEF* messages, a *CEF* parser must be used. Do not use regular expressions. This will ensure the integration integrity in the future. When using the correct parser for the data that is expected, be sure to test different inputs to ensure that data is correctly extracted from the messages.

Audit events

A description of audit events in common event format (CEF).

Audit events in CEF are in this format:

```
<134>Oct 10 2019 16:00:18 local-sg-19.x n2osevents[0]: CEF:0|Nozomi
Networks|N2OS|19.0.3-10201846_FD825|AUDIT:SESSIONS:CREATE|User signed
in|0|
dvchost=local-sg-19.x
cs1=Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:69.0) Gecko/20100101
Firefox/69.0
cs6=1
cs1Label=browser
cs6Label=n2os_schema
msg=User signed in
src=172.16.248.1
suser=admin
start=1570723218425
```

Note the **highlighted** part of the audit message. This is the Audit Type ID. This should be used as the key for performing searches once Nozomi Networks syslog events have been ingested into the integration platform.

Best practice

Make sure that your parsing logic extracts the appropriate data. If you are integrating with *CEF* messages, a *CEF* parser must be used. Do not use regular expressions. This will ensure the integration integrity in the future. When using the correct parser for the data that is expected, be sure to test different inputs to ensure that data is correctly extracted from the messages.

Connectivity status and status

A description of Connectivity status and status in common event format (CEF).

Connectivity status and status

Connectivity status represents the connectivity status with the data integration endpoint, which is updated when a new connection is initiated. The value is **OK** if the data integration preliminary connection check returns a success response, otherwise you will see the value of the error / exception retrieved while performing these preliminary checks.

Status represents the state of the last data operation. For example, was the data integration able to send data, or did it receive errors. The value is **OK** if the integration returns a success response, a 200 status code, or similar. Otherwise the system displays the value of the error / exception retrieved while trying to send the data.

Both **Connectivity Status** and **Status** support the **OK** value across all data integrations. If either is not OK, one or more errors have occurred. The value then displays error details, depending on the specific data integration.

Configure data integration

The **Data integration** page lets you configure one of the available options.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

- In the Settings section, select Data integration.
 Result: The Data integration page opens.
- 3. In the top right section, select Add.

Result: A dialog shows.

4. From the **Choose a configuration** dropdown, select an option.

٢	lew Endpoint	×
E	ndpoint Configured as	
	Choose a cor	nfiguration -
	Google Chronicle (Ingestion API - UDM) IBM QRadar (LEEF)	
	Common Event Format (CEF)	
	ServiceNow	
	Tanium	
	Splunk - Common Information Model (JSON)	New Endpoint Cancel
	SMTP forwarding	
	SNMP Trap	
	Syslog Forwarder	
	Custom JSON	
	Custom CSV	
	DNS Reverse Lookup	
	CheckPoint IoT	
	Kafka	
	Cisco ISE	

5. Enter the details as necessary for the option that you chose.

Firewall integration

The **Firewall integrations** page shows all the firewall integrations and lets you add new ones.

NOZOMI =				ŝ
Settings	Firewall integrat	ion		Live C +
	Actions	Name	Host	User
-	There are no firewalls confi	gured		
Firewall integration				

Figure 48. Firewall integrations page

General

Guardian lets you configure firewall integrations. Guardian discovers, identifies, and learns the behavior of assets on your network. Through integration with the firewall, unlearned nodes and links are automatically blocked through block policies. Block policies are not created for nodes and links in the learned state.



Note:

For some firewall integrations, Guardian supports session kill.

After the integration has been set up, policies are produced and inserted in the firewall. The policies are displayed in the **Policies** section.

Features

Firewall integrations only work when, in the Security control panel (on page 13), the:

- Detection approach is set to Strict
- Phase switching is set to Protecting

It does not work when the policy for zones is set to override the **Protecting** and **Strict** mode. In this mode, we can see new nodes, but they are not learned.

If the global learning policy is set to **Adaptive Learning** and **Learning**, and a zone is set to **Adaptive Learning** and **Protecting**, we see new nodes, but they are not learned, however links to new nodes are learned automatically.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Add

The + icon lets you add a new firewall integration.

Configure Barracuda

Configure Guardian firewall integration with the Barracuda firewall.

Before you begin

Make sure that you have administrator privileges.

About this task

Guardian integration supports Barracuda API v8.3.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the **Choose firewall** dropdown, select **Barracuda**.

Result: A dialog shows.

5. If it is not populated already, in the **Host (CA-Emitted TLS Certificate)** field, enter the host *IP* address.

Choose firewall Barracuda •		30
Configuration	Options	
Host (CA-Emitted TLS Certificate Optional Required)	Enable nodes blocking Control nodes communication in the firewall according to the Environment status	
Nozomi Networks recommends the usage of SSL certificates in your environment	Enable links blocking Control links communication in the firewall according to the Environment status	
Range		
Cluster		
Shared firewall service name		
Rules list name		
Token		
Save		

- 6. In the **Range** field, enter the *IP* address range.
- 7. In the **Cluster** field, enter the cluster.
- 8. In the **Shared firewall service name** field, enter a name.
- 9. In the **Rules list name** field, enter a name.

- 10. In the **Token** field, enter the token.
- 11. Optional: If necessary, tune the integration's behavior in the Options section.
 - a. If necessary, select **Enable nodes blocking**.
 - b. If necessary, select **Enable links blocking**.
- 12. Select **Save**.

Results

Configure Cisco ASA

Configure Guardian firewall integration with the Cisco ASA firewall.

Before you begin

Make sure that you have administrator privileges.

Procedure

1. In the top navigation bar, select 🔅

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the **Choose firewall** dropdown, select **Cisco ASA**.

Result: A dialog shows.

5. If it is not populated already, in the Host field, enter the host *IP* address.

Choose firewall Cisco ASA +	
Configuration	Options
Host User Password	Enable nodes blocking Control nodes communication in the firewall according to the Environment status Enable links blocking Control links communication in the firewall according to the Environment status Enable session kill Kill malicious sessions when a new alert of the selected types is raised Policies are sent as enabled Policies are sent to the firewall with the 'status' set as 'enable' if the flag is checked else the 'status' is 'disable'

- 6. In the **User** field, enter your user name.
- 7. In the **Password** field, enter your password.
- 8. Optional: If necessary, tune the integration's behavior in the Options section.
 - a. If necessary, select Enable nodes blocking.
 - b. If necessary, select Enable links blocking.
 - c. If necessary, select **Enable session kill**. Then select the specific alert type(s).
 - d. If necessary, select **Policies are sent as enabled**.
- 9. Select **Save**.

Results

Configure Cisco FTD

Configure Guardian firewall integration with the Cisco FTD firewall.

Before you begin

Make sure that you have administrator privileges.

Procedure

1. In the top navigation bar, select 🖄 **Result:** The administration page opens.

2. In the **Settings** section, select **Firewall integration**.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the **Choose firewall** dropdown, select **Cisco FTD**.

Result: A dialog shows.

5. If it is not populated already, in the **Host** field, enter the host *IP* address.

Choose firewall Cisco FTD +	×
Configuration	Options
Host	Enable session kill Kill malicious sessions when a new alert of the selected types is raised
User	
Password	
Save	

- 6. In the **User** field, enter your user name.
- 7. In the **Password** field, enter your password.
- 8. Optional: If necessary, in the Options section, select Enable session kill. Then select the specific alert type(s).in the Options section.
- 9. Select **Save**.

Results

Configure Cisco ISE

Configure Guardian firewall integration with the Cisco ISE firewall.

Before you begin

Make sure that you have administrator privileges.

About this task

The integration between Guardian and Cisco ISE lets Cisco customers to extend network access controls and policy enforcement to their *OT* and *IoT* networks from the Cisco ISE. Guardian uses the pxGrid platform to integrate with Cisco ISE. Along with the client associated with the certificate and the certificate password, you need to upload the identity certificate and the private key. The preferred method of authenticating with the Cisco ISE is to use certificates. Guardian supports authentication with certificates issued by:

- The Cisco ISE internal CA
- An external CA (third-party certificates)

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the Choose firewall dropdown, select Cisco ISE.

Result: A dialog shows.

5. If it is not populated already, in the **Host** field, enter the host *IP* address.

Choose firewall Cisco ISE -	×
Configuration	Options
Host	Enable nodes blocking Control nodes communication in the firewall according to the Environment status
Client name	
Authenticate with certificate	
Use existing client	
O Generate a new client for username and password authentication. The name must not be already present in Cisco ISE. The password returned by Cisco ISE will be automatically added to the configuration in Cuardian	
Create client	
Save	

Note:

The host *IP* address is the *IP* address of the Cisco ISE firewall that you are configuring.

6. In the **Client name** field, enter the name of the client.

Note:

The client name is taken from the Cisco ISE pxGrid Services screen on the Cisco ISE Web *UI*. For more details, see the appropriate Cisco ISE documentation.

7. **Optional:** Authenticate with a Cisco ISE internal CA certificate. select

Authenticate with certificate., then enter the password in the Password field.

- a. Select Authenticate with certificate.
- b. In the **Password** field, enter your password.
- 8. Optional: Use a third-party certificate. check the Use third party certificate box,

then import the certificate(s), using one of the following methods

- a. Select Use third party certificate.
- b. Choose a method to import the certificate:

Choose from:

- Import the CA certificate
- Import the certificate
- Import the key
- If you chose, Import the CA certificate or Import the certificate, continue from step 10 (on page 123). If you chose Import the key, continue from step 11 (on page 123).

- 10. Import the certificate.
 - a. Select **Import the certificate**.
 - **Result:** a dialog shows.
 - b. Select the file and import it.
- 11. Import the key.
 - a. Select **Import the key**.
 - b. Select the file and import it.
- 12. Optional: If necessary, in the Options section, select Enable nodes blocking.
- 13. Select **Save**.

Results

Configure Fortinet FortiGate

Configure Guardian firewall integration with the Fortinet FortiGate firewall.

Before you begin

Make sure that:

- You have administrator privileges
- You have generated the REST API access token from the firewall admin Web UI
- You have added the Guardian address subnet to trusted hosts

Note:

The access token needs to have permission to insert, read, and delete entities such as:

- Addresses
- Addrgroups
- Routes
- Sessions
- Policies

About this task

Guardian integration supports FortiOS versions 6.2, 6.4, 7.0, 7.2. This integration uses the REST *API*.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the **Choose firewall** dropdown, select **Fortinet FortiGate**.

Result: A dialog shows.

5. If it is not populated already, in the **Host (CA-Emitted TLS Certificate)** field, enter the host *IP* address.

Configuration	Options
Host (CA-Emitted TLS Certificate Optional Required)	Insert a new policy on top of all policies If not checked, the new policy will be placed only on top of policies already submitted in the sense.
Nozomi Networks recommends the usage of SSL certificates in your environment	Interestion Control nodes communication in the firewall according to the Environment status
rdom (optional)	Enable links blocking Control links communication in the firewall according to the Environment status
Write vdoms separated by commas eg; vdom1, vdom2	 Enable session kill Kill malicious sessions when a new alert of the selected types is raised
Access token	Keep on killing sessions If checked, sessions with the same source and destination IP addresses and destinatio port of a killed session will be killed as well
Save	Enable ports check Insert a policy in the FortiGate firewall only if the source and destination firewall interfaces are different.
	 Enable transparent mode If enabled, layer 2 links and nodes communications will also be blocked according to the Environment status.
	Policies are sent as enabled Policies are sent to the firewall with the 'status' set as 'enable' if the flag is checked else the 'status' is 'disable'
	Enable logging

- 6. **Optional:** In the **vdom (optional)** field, enter one or more *Virtual DOM (vdom)s*. Use a comma to separate multiple entries.
- 7. In the Access token field, enter the access token.
- 8. **Optional:** If necessary, in the **Options** section, select one or more of these options:
 - a. Select Insert a new policy on top of all policies.
 - b. Select Enable nodes blocking.
 - c. Select Enable links blocking.
 - d. Select Enable session kill. Then select the specific alert type(s).
 - e. Select Keep on selecting sessions.
 - f. Select Enable ports check.
 - g. Select Enable transparent mode.
 - h. Select Policies are sent as enabled.
- 9. Select **Save**.

Results

Configure Palo Alto Networks v10.1

Configure Guardian firewall integration with the Palo Alto Networks v10.1 firewall.

Before you begin

Make sure that you have administrator privileges.

About this task

Starting with version 10.0, PAN-OS provides a REST *API*. The Guardian integration that relies on this new *API* supports the same features as the previous Palo Alto integration, plus these:

- **Commit by user**: Commits the current changes required by the user, which are represented by the credentials used for the *API*. Global commits are no longer performed
- Dynamic Access Groups for Node Blocking: Dynamic Access Group references a tag, which is then assigned to a new *IP* address for objects that are created on the firewall. This will automatically apply the global Guardian denylist rule to each new address without modifying the firewall ruleset



This firewall integration supports IPv6 addresses.

Procedure

1. In the top navigation bar, select 🔅

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the Choose firewall dropdown, select Palo Alto Networks v10.1+.

Result: A dialog shows.

5. If it is not populated already, in the **Host (CA-Emitted TLS Certificate)** field, enter the host *IP* address.

Choose firewall Palo Alto Networks v10.1+ +	
Configuration	Options
Host (CA-Emitted TLS Certificate Optional Required) Nozomi Networks recommends the usage of SSL certificates in your environment Virtual System name (optional) User	Firewall rules strategy (Block active alerts Block unlearned) Enable nodes blocking Control nodes communication in the firewall according to the Environment status Enable links blocking Control links communication in the firewall according to the Environment status Enable session kill Kill malicious sessions when a new alert of the selected types is raised Keep on killing sessions If checked, sessions with the same source and destination IP addresses and destination port of a killed session will be killed as well
Password	Policies are sent as enabled Policies are sent to the firewall with the 'status' set as 'enable' if the flag is checked else the 'status' is 'disable'

- 6. Optional: In the Virtual System name (optional) field, enter a name.
- 7. In the **User** field, enter your user name.
- 8. In the **Password** field, enter your password.
- 9. **Optional:** If necessary, in the **Options** section, select one or more of these options:
 - a. For Firewall rules strategy, select one of these options:
 - Block active alerts
 - Block unlearned
 - b. Select Enable nodes blocking.
 - c. Select Enable links blocking.
 - d. Select Enable session kill. Then select the specific alert type(s).
 - e. Select Keep on selecting sessions.
 - f. Select Policies are sent as enabled.
- 10. Select Save.

Results

Configure Stormshield SNS

Configure Guardian firewall integration with the Stormshield SNS firewall.

Before you begin

Make sure that you have administrator privileges.

Procedure

1. In the top navigation bar, select 🔅

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the Choose firewall dropdown, select Stormshield SNS.

Result: A dialog shows.

5. If it is not populated already, in the **Host (CA-Emitted TLS Certificate)** field, enter the host *IP* address.

1005e TIFeWall stormshield SNS -	
Configuration	Options
Host (CA-Emitted TLS Certificate Optional Required) Nozomi Networks recommends the usage of SSL certificates in your environment Authentication (Use Credentials Certificate) User	Enable nodes blocking Control nodes communication in the firewall according to the Environment status Enable links blocking Control links communication in the firewall according to the Environment status
Password	
Save	

6. In the **Authentication** section, choose an option:

Choose from:

- Credentials
- Certificate
- 7. If you chose Credentials, continue from do step 7.a (on page 128). If you chose

Certificate, continue from step 8 (on page 129).

- a. In the **User** field, enter your user name.
- b. In the **Password** field, enter your password.
- c. Go to step 12 (on page 129).

- 8. If you chose **Certificate**, choose an option:
 - Choose from:
 - $^{\circ}\,$ Import the certificate
 - Import the key
- 9. If you chose, **Import the certificate**, continue from step 10 (on page 129). If you chose **Import the key**, continue from step 11 (on page 129).
- 10. Import the certificate.
 - a. Select Import the certificate.

Result: a dialog shows.

- b. Select the file and import it.
- 11. Import the key.
 - a. Select Import the key.
 - b. Select the file and import it.
- 12. Optional: If necessary, tune the integration's behavior in the Options section.
 - a. If necessary, select Enable nodes blocking.
 - b. If necessary, select Enable links blocking.
- 13. Select **Save**.

Results

Configure TXone OT Defense Console

Configure Guardian firewall integration with the TXone OT Defense Console firewall.

Before you begin

Make sure that you have administrator privileges.

About this task

TXOne OT Defense Console (ODC) provides a REST *API* v1.1. The Guardian integration relying on this *API* supports the same features as previous integrations from Trend Micro.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the Choose firewall dropdown, select TXone OT Defense Console.

Result: A dialog shows.

5. If it is not populated already, in the **Host (CA-Emitted TLS Certificate)** field, enter the host *IP* address.

Choose firewall Txone ot Defense Console -		:
Configuration	Options	
Host (CA-Emitted TLS Certificate Optional Required)) Onzomi Networks recommends the usage of SSL certificates in your environment API Key	Enable nodes blocking Control nodes communication in the firewall according to the Environment status Enable links blocking Control links communication in the firewall according to the Environment status	
API key will be shown as User name API Secret Save		

- 6. In the **API Key** field, enter the **API** key.
- 7. In the **API Secret** field, enter the **API** secret.
- 8. Optional: If necessary, tune the integration's behavior in the Options section.
 - a. If necessary, select Enable nodes blocking.
 - b. If necessary, select Enable links blocking.
- 9. Select **Save**.

Results

Configure Check Point R81.20

Configure Guardian firewall integration with the Check Point R81.20 firewall.

Before you begin

Make sure that you have:

- Administrator privileges
- A valid username and password for authentication
- Access to the Check Point R81.20 management host
- The name of the gateway where the rules will be installed

About this task

Check Point R81.20 side, this firewall integration:

- Creates a Check Point R81.20 layer (Nozomi layer) containing the rules
- Adds the rules to block links and nodes that are unlearned

Note:

If a node or link changes its status to learned, the corresponding rule will be removed.

- Creates a session named **Nozomi Guardian** in the firewall to manage rule insertion and removal
- Generates Check Point R81.20 Service objects for link ports that are not already mapped in the firewall
- Creates host objects to be used in the block link and nodes rules

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Firewall integration.

Result: The Firewall integration page opens.

3. In the top right section, select +

Result: A dialog shows.

4. From the Choose firewall dropdown, select Check Point R81.20.

Result: A dialog shows.

5. If it is not populated already, in the **Host (CA-Emitted TLS Certificate)** field, enter the host *IP* address.

Choose firewall Check Point R81.20 -	
Configuration	Options
Host (CA-Emitted TLS Certificate Optional Required) O Nozomi Networks recommends the usage of SSL certificates in your environment User Password Cathunau page	 Enable nodes blocking Control nodes communication in the firewall according to the Environment status Enable links blocking Control links communication in the firewall according to the Environment status Policies are sent as enabled Policies are sent to the firewall with the 'status' set as 'enable' if the flag is checked else the 'status' is 'disable'
Save	

- 6. In the **User** field, enter your user name.
- 7. In the **Password** field, enter your password.
- 8. In the Gateway name field, enter a name.
- 9. **Optional:** Select **Enable nodes blocking**. Enable this option if you want to block nodes.
- 10. Optional: Select Enable links blocking.Enable this option if you want to block links.
- Optional: Select Policies are sent as enabled.
 Make sure that this option is selected so that policies are active upon deployment.
- 12. Select Save.

Results

Credentials manager

The **Credentials manager** is a tool that lets you centralize the management of monitored endpoints to make it easier to create, delete, or update the credentials that are needed to access those endpoints.

NOZOMI =			ŝ
Settings	Credentials manager		
	Page 1 of 1, 0 entries	Live 🖲 👩 🛛 Add identity 🕶	Import credentials from CSV 👻
	Actions Nam	Scope	
	There are no identities registered		
Credentials manager			

Figure 49. Credentials manager page

Credentials manager is a feature that lets you securely store passwords, and other sensitive information, that Guardian uses to:

- Access hosts through Smart Polling or Arc
- Decrypt encrypted transmissions that are passively detected

Before Credentials manager, Smart Polling managed device credentials. Users migrating their system over to a version with Credentials manager will have their existing device credentials automatically migrated over to Credentials manager as part of the execution of the migration tasks after the upgrade.

Add an identity

You can use Credentials manager to add identities.

About this task

Each identity has a unique name to distinguish it from other identities. To insert a node into the applicability list of an identity, you can:

- Enter an *IP* address, or a subnet mask, into the applicable field, or
- Select a set of nodes from a list

Note:

A node cannot belong to multiple identities for the same scope.

Procedure

1. In the top navigation bar, select $\langle \check{\varsigma} \rangle$

Result: The administration page opens.

2. In the Settings section, select Credentials manager.

Result: The Credentials manager page opens.

3. In the top right section, select Add identity.

Result: A dropdown shows.

4. From the dropdown, select the applicable option.

Result: A dialog shows.

- 5. Enter the details as necessary.
- Optional: Select Select nodes from list, or use Add node ID / subnet.
 Result: A dialog shows.
- 7. Optional: Select the nodes desired for the scope of applicability.
- 8. Select **Apply** to selected nodes.

Result: The nodes are associated to the credentials in the new identity.

9. Select **Save**.

Results

The identity has been added.

Import credentials from a CSV file

The **Credentials manager** lets you import credentials from a comma-separated value (CSV) file.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Credentials manager.

Result: The Credentials manager page opens.

3. In the top right section, select Import credentials from CSV.

Result: A dropdown shows.

4. From the dropdown, select the applicable option.

Result: A dialog shows.

5. Choose a method to upload a file:

Choose from:

- \circ Drag your file into the **Drop a file here or click to upload** field
- Click in the Drop a file here or click to upload field
- 6. If you chose the second method, select the correct file to upload.

Import credentials for DLMS/COSEM		×
Drop a file here or click to upload		
Maximum file size: 2G		
Supported formats:	Notes:	
Comma-separated values (.csv)		
Cancel	Impo	rt



- 7. Wait for the file to upload.
- 8. Select Import.

Zone configurations

The **Zone configurations** page shows all the zone configurations in your environment and lets you add new zone configurations and edit them.

NOZOMI =									ŝ
ettings	Zone conf	igurations							
	Page 1 of 2 , 2	7 entries		Execution policy:	ocal only 🕚	Import Export	all Live 💽 (🗇 🕇 Add	● 9 selected ▼
	ACTIONS	NAME	MATCHING S	MATCHING V A	SSIGNED VL	LEVEL	NODES OWN	SECURITY CO	SOURCE
		Broadcast	255.255.255.25						Local
	a	Layer2	00:00:00:00:0						Local
	€	Link-local	169.254.0.0/16						Local
	a	Loopback	127.0.0.0/8						Local
	€	Multicast	224.0.0.0/4						Local
	a	Unspecified	0.0.0/32						Local
	≙ ⊘	Internet	Fallback for p				Public		Local
	≙ ⊘	Undefined	Fallback for pr				Private		Local
Zone configurations	•	TEstingtesting	22.22.22.22-22			null			Upstream
	₽	Test Zone 1	1.1.1.0/24			null			Upstream

Figure 50. Zone configurations page

Execution policy

This shows information about the currently configured data synchronization policy.

Import

This button lets you import a configuration file (CFG).

Export all

This button lets you download a CFG of all the zone configurations.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

+ Add

This button lets you add a new zone configuration.

Column selection

The columns selection [©] icon lets you choose which columns to show or hide.

Name

The zone must be given a name without spaces. It must include at least one network segment.

Matching segments

This shows the information such as *IPs, IP* address range, or *MAC* address, matched by the node discovered within the range (only the IP range is shown in the column, not the nodes).

MAC address matching fallback

The node *ID* must match the zone network segments to make the node part of zone. There are cases where this matching strategy is not enough, for example if you want to have nodes without an *IP* as node *ID* match a zone defined with *MAC* address ranges. In those cases we can enable this fallback matching strategy in order to match against the *MAC* address of the node whenever the node *IP* does not match a segment.

Matching VLAN ID

This only lists nodes that belong to the related *virtual local area network (VLAN)*. This needs the *VLAN* tag to be extracted from the traffic.

For example, if a zone has been configured as 192.168.4.0/24, with a VLAN ID set to 5:

- There is a node 192.168.4.2, that belongs to the VLAN
- There is a node 192.168.4.3, that does not belongs to the VLAN

When filtering the view with this zone, only the node 192.168.4.2 will show.

Assigned VLAN ID

Nodes that belong to this zone are assigned this VLAN ID.

Level

The level defines the position of the nodes pertaining to the given zone within the Purdue model. Once a level has been set for a zone, all nodes included in that zone are assigned the same level, unless a per-node configuration has been specified as well. This means that, if two or more zones overlap, a node that belongs to all of them will inherit the level of the most restrictive zone.

For example, if 10.1.1.1/32 belongs to Zone 1 (Level 1) and 10.1.0.0/16 (Level 2) belongs to Zone 2, then 10.1.1.1 will be assigned.

Nodes ownership

Ownership of the nodes belonging to the given zone. Once the ownership has been set for a zone, all nodes included in that zone inherit such ownership, overwriting the single nodes' ownership.

Detection approach

Used to override the global settings from the **Learning** section of the Security control panel (on page 13).

Learning mode

Used to override the global settings from the **Learning** section of the Security control panel (on page 13).

Security profile

Used to override the global settings from the **Security profile** section of the Security control panel (on page 13).

Use node labels as Device IDs

This lets you use a node label, such as the computer name, as a device *ID*.

Network Throughput History

If enabled, nodes pertaining to the zone will have an extended history for bytes sent and received, and all links for bytes transferred. The fields, whose default setting is 0:

- last_lhour_bytes
- last_lday_bytes and
- last_1week_bytes

will typically work like their counterparts for 5, 15, and 30 minutes. These fields are evaluated every 5 minutes and their time span is:

- **last_lhour_bytes =>** the last hour at granularity of 5 minutes. For example, if it is 15:32 the field will cover the time span from 14:30 to 15:30
- **last_1day_bytes =>** the last day at granularity of 1 hour, but updated every 5 minutes. For example, if it is 15:32 on Tuesday, the field will cover the time span from 16:00 on Monday to 16:00 on Tuesday and the data is updated at 15:30 on Tuesday
- **last_1week_bytes =>** the last week at granularity of 1 day, but updated every 5 minutes. For example, if it is 15:32 on Tuesday, the field will cover the time span from 00:00 on Wednesday of the previous week to 24:00 on Tuesday of the current week, and the data is updated at 15:30 on Tuesday this week

Note:

The default setting is for **Network Throughput History** to be disabled and needs to be explicitly enabled in the **Retention** tab of the **Features Control Panel**. It is important to note that when it is activated, it will quickly consume extra disk space. The default setting for disk consumption is 512 *megabyte (MB)*. You can configure this from 64 *MB* to 5 *GB* in the **Features** page. When the disk consumption limit is reached, older data is erased to make room for more recent samples.

Add a zone configuration

You can configure and control zones in the Central Management Console (CMC) and then propagate them to all the Guardian sensors that are connected. You can specify an execution policy in the CMC to resolve zone conflicts.

Procedure

1. In the top navigation bar, select \bigotimes

Result: A menu shows.

2. In the Settings section, select Zone configurations.

Result: The Zone configurations page opens.

3. In the top right section, select **+Add**.

Result: A dialog shows.

4. Configure the settings as necessary. For more details, see **Zone configurations**.

Add a new configuration	×
Name	Level (Optional)
	Level -
Matching segments	① If set, the matching Node will have this level if a more specific one is not assigned on the node itself
e.g. 192.168.1.0/24 or 192.168.1.0/24,10.1.0.0/16 or 192.168.0.1-192.168.0.4 or 00:01:02:03:04:05-00:01:02:03:04:09	Nodes ownership (Optional)
① List of segments to match. They are matched in OR: at least one match is enough	Choose among the following▼
MAC address matching fallback	\bigcirc $% \left({{\rm{If}}} \right)$ if set, the Ownership that the nodes matching with this zone will be set to
() If set, the zone will be matched by MAC address whenever the IP does not match	Detection approach (Optional)
Matchine M AN ID (Optional)	Choose among the following 🗸
	① If set, this detection mode will override the global settings for this zone
ULAN ID to match against the node. If provided, is matched in AND with segments. Use this value to distinguish	Learning mode (Optional)
overlapping networks with different VLANs, or differentiate Layer2 nodes. Leave blank otherwise.	Choose among the following 🗸
Assigned VLAN ID (Optional)	① If set, this Learning mode will override the global settings for this zone
	Security profile (Optional)
① The VLAN ID that the node will be set to when matching with this zone, when the node VLAN ID is not clear from the traffic. The traffic information prevails.	(Use global Security profile) -
	① If set, this Security profile will override the global one for Alerts generated in the zone
	Use node labels as Device IDs
	Network Throughput History
	() If set, the zone will save more data. WARNING: this will take a lot of space
	Save Cancel

5. Select **Save**.

Results

The zone configuration has been added.

Synchronization settings

The **Synchronization settings** page lets you customize the parameters related to Vantage or Central Management Console (CMC).

Settings	Synchronization settings			General Save Cancel
	Sync token ey22jjoiMisinMiODveTZMVVdoaXVmcTc3VnDaTvyckxwMiBEM EtQTmskZ3VTjFMbg2cFB95ismODUVaEh4ODByVHF3bgXR EFIZX6bVNN0473V47MF08CX043F27bm7Vm86CVVhO2C xcFU5eDdIMVN3UnBNRVIOIMvaCl6NiABjNidDFidTZMjBp cDVINHBWM0Q2WEUxcmVPamRFVmF3ZTF3RUIRbIU9in0= Copy the token to the machine you want to synchronize/nepl	@ Copy	Sensor ID 64726cc5-fal6-459d-880d-dbb80918acc2 ① This ID indentifies the current sensor, it has to be us if enabled, the configuration to the upstream conne	ed in order to complete, ection
Synchronization settings	General settings Sensor update policy Update sensors On ortupdate sensors On the this sensor is updated, the update will be sent to all co sensors.	mnected	Upstream Connection ON OFF Check connection Connection is workin Chable upstream connection to avoid potential dat Use proxy connection	g a loss.
System			Host (CA-Emitted TLS Certificate Optional) Required) Intrasilich-ga-cmc-std-nemcl00-gen-dyn-Lintanzeominetw Nozomi Networks recommends the usage of SSL ce emivicomment Sync token ey02ijeaMilsaMi0D/mTVtyUmin2/Q4g22ncmEIZe4Q3V/hax	orks.com rtificates in your RVRWIwNzVkWESDNWR

Figure 51. Synchronization settings page

The Synchronization settings page has these tabs:

- General (on page 142)
- Data Diode (on page 143)

General

The **General** page lets you customize the parameters related to Vantage or Central Management Console (CMC).

nchronization settings	General Data Diode
	Save Cancel
Sync token Copy Copy the token to the machine you want to synchronize/replicate with	Sensor ID This string indentifies the current sensor. It's used to connect this sensor to Vantage.
General settings Sensor update policy Update sensors Do not update sensors	Upstream Connection OR OFF Check connection Connection is working ① Enable upstream connection to avoid potential data loss.
Once this sensor is updated, the update will be sent to all connected sensors.	Use proxy connection
	Nozomi Networks recommends the usage of SSL certificates in your environment
	Sync token

Figure 52. General page

Sync token

To synchronize/replicate with another machine, you will need to copy the **Sync token** to the machine you want to synchronize with.

Sensor ID

This is the *ID* of the current sensor.

General settings

The Sensor update policy has two options:

- Update sensors
- Do not update sensors

Upstream Connection

This section has a toggle that can be set to **ON** or **OFF**. When this is set to **ON**, you can select **Check connection** to make sure that the connection is okay.

The **Use proxy connection** checkbox lets you use an auxiliary system that provides a gateway between the sensor and the upstream sensor or connection.

The Host (CA-Emitted TLS Certificate) field is where you need to enter the *IP* address of the machine that you want to connect to. This can be set to either:

- Optional
- Required

The **Sync token** field lets you enter the synchronization token for the upstream machine.

Data Diode

Administrator Guide

Data diodes provide unidirectional network communication to securely transfer data from high-security environments, ensuring critical infrastructure and industrial control systems are protected from inbound cyber threats.

General	Data Die
	Save

Figure 53. Data Diode page

Disabled

When this checkbox is selected, the data diode functionality is disabled.

Producer

When this checkbox is enabled, it allows the Guardian to send data out to the data diode and the upstream CMC.

When **Producer** is enabled, the fields below show.

- Protocol (communication protocol to be used)
- Token (of the upstream CMC)
- Host (address of the data diode)
- Username (for the data diode)
- Password (for the data diode)
- Directory (the location on the data diode to store the data)

This enables one-way data transfer to the data-diode and the upstream CMC system.

Data diodes

Data diodes provide unidirectional network communication to securely transfer data from high-security environments, ensuring critical infrastructure and industrial control systems (ICS) are protected from inbound cyber threats.

In cybersecurity software, data diodes are used to establish unidirectional network communication, which allows data to flow in only one direction. This ensures that sensitive networks can send out information, such as system logs or alerts, without risking inbound connections that attackers could exploit. Data diodes prevent a reverse flow of data to effectively block potential cyberattacks and data leaks.


Data diodes are particularly crucial in securing critical infrastructure and *ICS*, such as power grids and water supply systems. They allow operational data to be monitored externally without exposing these systems to outside threats. Additionally, they isolate high-security networks from less secure ones, maintaining strict separation to prevent unauthorized access while enabling necessary data sharing.

This technology secures data transfer to protect the integrity of logs and alerts, which supports compliance with regulatory requirements. As they use a physical barrier against cyber threats, data diodes enhance the security posture of organizations in sectors where safeguarding data and maintaining system integrity are critical.

Unlike firewalls, which allow controlled bidirectional communication and require ongoing management, data diodes provide a hardware-based, one-way data flow that is inherently more secure against breaches. This makes them ideal for environments that require absolute isolation.

Data diodes complement firewalls, and offer simpler, fail-safe protection for high-risk, unidirectional data transfer scenarios.

Configure a Guardian as a producer

Configure a Guardian sensor to communicate to an upstream data diode and Central Management Console (CMC).

About this task

Use this task to configure a Guardian as a data producer for secure, one-way data transfer through a data diode. You'll set up communication with the Central Management Console (CMC) and establish the necessary connection for a secure data flow.



Note:

Different types of data diode are available. Therefore, this procedure does not go into detail about the data diode settings.

Procedure

- 1. Open the consumer CMC,
- 2. In the top navigation bar, select \bigotimes

Result: The administration page opens.

3. In the Settings section, select Synchronization settings.

Result: The Synchronization settings page opens.

- 4. Select Data Diode.
- 5. In the **Status** section, select **Consumer**.

Result: The Token field shows.

6. To copy the token, select **Copy**.

Disabled	Producer	• Consumer	
ſoken			
			С Сору

- 7. Open the producer Guardian.
- 8. In the top navigation bar, select \bigotimes

Result: The administration page opens.

9. In the Settings section, select Synchronization settings.

Result: The Synchronization settings page opens.

10. Select Data Diode.

Result: The Data Diode page shows.

11. In the **Status** section, select **Producer**.

Result: The producer fields show.

12. In the **Token** field, paste the consumer token that you copied in step 6 (on page 146).

chronization settings	General	Data Diode
		Save Can
Status		
Disabled • Producer		
Token		
Protocol		
Choose a data transfer protocol 🔹		
Host		
Username		
Password		
Directory (files will be stored here)		
Make sure the user has permissions to list, read and write within the folder		

- 13. From the **Protocol** dropdown, select the applicable protocol.
- 14. In the **Host** field, enter the URL of the data diode.
- 15. In the **Username** field, enter the username for the data diode.
- 16. In the **Password** field, enter the password for the data diode.
- 17. In the **Directory** field, enter the data diode location in which the data will be stored.
- 18. Select Save.
- 19. Select General.

Result: The General page shows.

20. In the Upstream Connection section, enter some text in the Host field.

ichronization settings	General Data Diode
	Save Cancel
ync token Copy Copy the token to the machine you want to synchronize/replicate with	Sensor ID Copy This string indentifies the current sensor. It's used to connect this sensor to Vantage.
Seneral settings Sensor update policy Update sensors Do not update sensors	Upstream Connection ON OFF Check connection Connection is working C Enable upstream connection to avoid potential data loss.
 Once this sensor is updated, the update will be sent to all connected sensors. 	Use proxy connection Host (CA-Emitted TLS Certificate Optional Required) Nozomi Networks recommends the usage of SSL certificates in your environment
	Sync token

You can enter any text in the **Host** field, but you cannot leave it empty.

21. In the **Sync token** field, enter some text.

You can enter any text in the **Sync token** field, but you cannot leave it empty.

22. Select **Save**.

Results

Communication between the producer and the consumer has been configured.

Connect a sensor to CMC

Connect one or more sensors to a Central Management Console (CMC).

Procedure

- 1. Open the CMC.
- 2. In the top navigation bar, select 🐼 **Result:** A menu shows.
- 3. In the Settings section, select Synchronization settings.

Result: The Synchronization settings page opens.

- 4. In the top left Sync token section, select Copy.
- 5. Open the sensor that you want to connect to the CMC.
- 6. In the top navigation bar, select \bigotimes

Result: A menu shows.

7. In the Settings section, select Synchronization settings.

Result: The Synchronization settings page opens.

- 8. Go to the **Upstream Connection** section, in the **Sync token** field, paste the sync token that you copied from the *CMC*.
- 9. In the Host field, paste the IP of the CMC. The HTTPS protocol will be used.
- 10. **Optional:** If no CA-emitted certificates are used, you can select Optional to make the verification of certificates optional.
- 11. To make sure that the connection has worked correctly, select Check connection. Result: If the connection is working, green text that states Connection is working shows.
- 12. Select Save.
- 13. Go back to the CMC.
- 14. In the top navigation bar, select Sensors.

Result: The Sensors page opens.

15. In the list, make sure that the sensor you just connected shows.

Note:

When a sensor is connected for the first time, it will notify its status and receive firmware updates. However, it will not be permitted to perform additional actions. To enable a complete integration of the sensor you will need to allow the sensor.

Results

The sensor has been connected to the CMC.

Alert playbooks

Alert playbooks overview

An explanation of alert playbooks.

Alert playbooks are a set of instructions that guide you on how to take the correct action when an alert is raised.

An alert playbook describes the actions, tasks and other guidelines that users should follow when an alert is raised. You use an alert rule to assign an alert playbook to a specific alert. When that type of alert is raised, the alert rule that matches will insert a copy of the alert playbook into the alert.

Alert rules can use different matching criteria to assign the same alert playbook to multiple different alerts types. For more details, see **Configure an alert**, in the **User Guide**.

Once an alert playbook is visible on a triggered alert (from the Alerts panel), you can modify it without affecting the original. This is typically used to add notes for the specific alert, or to mark completed actions.

Note:

When you create an alert playbook, or an alert rule in *CMC*/Vantage, it will be propagated to all the connected sensors.

Alert playbooks

The Alert playbooks page shows a list of all the alert playbooks.

NOZOMI =				ŝ
Settings	Alert playbooks			
	Page 1 of 1, 2 entries	+ Add	Live 🌑 🕥	● Actions, Name -
	Acti Name			
	✓ ① TechDocs test			
	Mattia Playbook			
Alert playbooks				

Figure 54. Alert playbooks page

Add

This lets you add new alert playbooks.

Live / refresh

The Live $\bigcirc \bigcirc \bigcirc \bigcirc \bigcirc$ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection ${}^{igodoldsymbol{\Theta}}$ icon lets you choose which columns to show or hide.

Create an alert playbook

You can use the Alert playbooks page to create a new alert playbook.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Alert playbooks**.

Result: The **Alert playbooks** page opens and shows a list of available alert playbooks.

3. In the top right, select + Add.

Result: A dialog shows.

4. In the **Name** field, enter a name for the alert playbook.

Create playbook	×
Name	
Playbook	
	li
Playbook contents accepts Markdown syntax	
Create playbook	

- 5. In the **Playbook** field, enter the relevant steps to follow when an alert related to this playbook is raised.
- 6. Select Create playbook.

Results

The alert playbook has been created.

Edit an alert playbook

After an alert playbook has been created, you can edit the details.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the Settings section, select Alert playbooks.

Result: The **Alert playbooks** page opens and shows a list of available alert playbooks.

3. From the list, select an alert playbook template.

Note:

The list will be empty if:

- No alert playbooks have been created
- One or more alert playbooks have been created, but they were created in an upstream Vantage or *CMC*
- 4. To the left of the applicable alert playbook, select the \checkmark icon.

Result: A dialog shows.

5. Optional:

If necessary, in the **Name** field, edit the text.

Edit playbook Name Malware Detection Daybook 1. Identify Download the PCAP of the alert Validate and Notify Playbook contents accepts Markdown syntax

Edit playbook

- 6. **Optional:** If necessary, in the **Playbook** field, edit the text.
- 7. Select Edit playbook.

Results

The alert playbook has been edited.

Delete an alert playbook

You can use the **Alert playbooks** page to delete an alert playbook.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **Settings** section, select **Alert playbooks**.

Result: The **Alert playbooks** page opens and shows a list of available alert playbooks.

3. To the left of the applicable alert playbook, select the fill icon.

Note:

If an alert rule(s) that is related to the alert playbook, you will be prompted to confirm the deletion. If you proceed with the deletion, all alert rules associated with the alert playbook are also deleted.

Result: A dialog shows if the alert playbook is related to an alert rule(s).

4. To confirm the deletion, select **Yes**.

Delete playbook TechDocs test?	×	
Yes	No	

Results

The alert playbook has been deleted.

System

General

The **General** page lets you change the hostname and specify a login banner on a sensor.

NOZOMI =		ŵ
Settings	General	
	Hostname	
	lab-r50.intra.nozominetworks.com	
	Login banner	
	Description	
	Site	
6 mb m		
System	Save	
General		

Figure 55. General page

Date and time

The **Date and time** page lets you configure the date and time of a sensor.

NOZOM! =		ŝ
Settings	Date and time	
	Timezone Local: UTC (UTC-00.00) Sove Date (format cojymmddHHMM.ss) Since this sensor is connected to Vantage or a CMC, it will use its date: 2023103523.49 NTP Cnabled	
	Offreebsd.pool.ntp.org.1freebsd.pool.ntp.org	
	Save	
System		
Date and time		

Figure 56. Date and time page

Timezone

This dropdown lets you select a timezone.

Date

This section lets you **Pick a date** and, optionally set the sensor as a client. The date settings are disabled if the sensor is connected to an upstream Vantage or *CMC*.

NTP (Network Time Protocol)

The **Enabled** checkbox lets you synchronize the servers in the network to the computer clock time. To do this you must enter a list of comma-separated server addresses.

Note:

When a sensor is attached to Vantage or a *CMC*, you cannot manually set its date and time. Sensors that are connected to Vantage or a *CMC* (with no *network time protocol (NTP)* configured) will automatically get time synchronization from Vantage, or the parent *CMC*.

Configure the date and time

You can configure the timezone and the current date and time of the sensor. You can also write a list of comma-separated server addresses to enable time synchronize with a network time protocol (NTP).

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the System section, select Date and time.

Result: The Date and time page opens.

- 3. From the **Timezone** dropdown, select the correct option.
- 4. Select **Save**.
- 5. In the **Date** field, select **Pick a date**.

Note:

If the sensor is connected to Vantage or a *CMC*, the date is automatically taken from upstream.

- 6. Optional: If applicable, select Set as client.
- 7. Select Save.
- 8. **Optional:** To synchronize the servers in the network to the computer clock time, in the **NTP** section, select **Enabled**.
- 9. **Optional:** In the **Servers** field, enter the applicable list of comma-separated server addresses.
- 10. Select **Save**.

Results

The date and time settings have been configured.

Updates and licenses

The **Updates and licenses** page lets you configure and manage the base software license and the licenses for optional features, such as Smart Polling, Threat Intelligence, Asset Intelligence, Arc, and Federal Information Processing Standards (FIPS).

NOZOMI =			Ø
Settings	Updates and licenses		Set new license
	Base	Smart Polling	Threat Intelligence
	Current license - Full Advanced: monitoring, security, and Smart Polling License strate Polling License Resemi Networks Arem 20/2055 0494-433-603- (license manged by Vontage Strategies - Strategies -	The base lisense is Full Advanced and it includes Smart Polling. No license is required.	Updates This machine is connected to Varitage or a CMC, it's up to it to decide white the reade Threat Instilligence provided by Nozomi Networks
System			
	Asset Intelligence	Arc	Nozomi TI Expansion Pack, Powered by Mandiant
Updates and licenses	Updates This machine is connected to Varitage or a CMC, it's up to it to decide whether to enable Asset Intelligence provided by Nozomi Networks	Current license This license supports an unlimited number of Arc sensors Updates Arc is correctly synchronized with Varitage or the parent CMC. This machine is connected to Varitage or a CMC, it's up to it to decide whether to enable Arc provided by Natorn's Networks Version 2004/09/ESE7,VI.03.2 (024-09-16):5.47)	Current license License ID:052c07-4c06-4d6 License ID:052c07-4c06-4d6 License Maxael Networks Acere [Ilcense managed by Variage] The license of this sensor is managed through the Variage subscription
	FIPS		
	No license Contact Nozomi Networks to purchase a FIPS license.		

Figure 57. Updates and licenses page

Base

This section is for the base license, which is mandatory, and includes passive monitoring.

Smart Polling

This section lets you enable an optional license for Smart Polling.

Threat Intelligence

This section lets you enable an optional license for Threat Intelligence.

Asset Intelligence

This section lets you enable an optional license for Asset Intelligence.

Arc

This section lets you enable an optional license for Arc.

Threat Intelligence Mandiant

This section lets you enable an optional license for Threat Intelligence Mandiant.

FIPS

This section is an information-only panel that shows details about an optional *Federal Information Processing Standards (FIPS)* license. To install *FIPS*, you need to enable *FIPS* mode in a console.

License status

Each section that has an active license will show the License status.

License status	Description	
UNLICENSED	Functionality is disabled.	
ок	Functionality is enabled. Be aware of the expiration date to allow time for renewals. If a license is issued with node limits, and the limits are exceeded, functionality is only enabled for the covered nodes within the limits. New nodes are not analyzed.	
EXPIRING 30 days before the expiration date, notifications will show in the UI remind users of the impending expiration of their current license a take actions towards renewing their license.		
EXPIRED	Starting from the expiration date, notifications will show in the <i>UI</i> to notify users of the expiration of their current license and to take actions towards renewing their license. Nozomi Networks offers a grace period after the official expiration date. In this grace period, the license still functions as it would in the OK status. The grace period provides time for an emergency renewal of the license. After the grace period is over, functionality is disabled. The contents that were analyzed or imported before the expiration date remain, however no new analyses are performed, and no new signatures are imported.	

Table 4. License status

Install a license

Before you can use a product, you must install the applicable license.

Before you begin

If you are installing an additional license, make sure that you have installed a base license first.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Updates and licenses.

Result: The Updates and licenses page opens.

3. In the top right of the section, select **Set new license**.

Updates and licenses	Set new license
Base	

Result: A dialog shows.

4. To copy the Machine ID, select Copy.

Set new license	×
License key	
Verify and apply	

- 5. Send the machine *ID* to Nozomi Networks with your license request.
- 6. Wait to receive your license key from Nozomi Networks.
- 7. In the **License key** field, paste the license key.
- 8. Select Verify and apply.

Results

The license has been installed.

Network interfaces

The Network interfaces page shows information on how much network traffic is being ingested/captured.

									ŝ
Settings	Netwo	ork interfa	ces						
	Som \$100 - 100 \$25M 0	09:41:15	09:41:20 09:4	11:25 09:41:30	09:41:35 09:4	1:40 09:41:45	09:41:50	0N OFF Time wind	ow Im Ih Id Iw Q
					🛑 interface	e port1			
	Actions	Interface	Enabled	Is mirror	MGMT filter	BPF filter	NAT	Denylist enabled	Denylist file
and the second sec									
the second s	÷	port1	true	true	on			false	-
	÷	port2	true	false	on			false	
the second se	2	port3	true	false	on			false	
	÷	port4	true	false	on			false	-
System									
Network interfaces									

Figure 58. Network interfaces page

Throughput

This shows the amount of information that is being shown.

ON/OFF

This toggle lets you set the automatic update of the diagram.

Time window

This lets you choose the timeframe of the window. You can choose between:

- One minute
- One hour
- One day
- One week

Configure a NAT rule

The **Network interfaces** page lets you configure network address translation (NAT) rules.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Network interfaces.

Result: The Network interfaces page opens.

3. To the left of the applicable interface, select the \rightleftharpoons icon.

Result: A dialog shows.

4. In the **Label** field, enter a label for the interface.

Cor	Configure interface				
Interfa	ace				
portl					
Label					
1	The label must differ from other labels and network interface names The label can contain only alphanumeric characters and '-' / '_' symbols Interface name will be used as label if empty value is provided				
Enabl	e ON OFF				
Enable NAT	e ON OFF				
Enable NAT Origin	e ON OFF				
Enable NAT Origin	e ON OFF al subnet 92.168.0.0				
Enable NAT Origin e.g. 1 Transl	e ON OFF nal subnet 92.168.0.0 lated subnet				
Enable NAT Origin e.g. 1 Transl	e ON OFF nal subnet 92.168.0.0 lated subnet 0.1.0.0				
Enable NAT Origin e.g.1 Transl e.g.1 CIDR	e ON OFF hal subnet 92168.0.0 lated subnet 0.1.0.0 mask				
Enable NAT Origin e.g. 1 Transl e.g. 1 CIDR (e ON OFF al subnet 92.168.0.0 lated subnet 0.1.0.0 mask h6				
Enable NAT Origin e.g. 1 Transl e.g. 1 CIDR 1 e.g. /	e ON OFF hal subnet 92168.0.0 lated subnet 0.1.0.0 mask N6 This rule allow the rewriting of source and destination IPs of packets sniffed o				
Enable NAT Origin e.g.1 Transl e.g.1 CIDR (e.g./	e ON OFF al subnet 92168.0.0 lated subnet 0.1.0.0 mask 16 This rule allow the rewriting of source and destination IPs of packets sniffed of this interface.				

Note:

The label will show instead of the network interface name in all areas of the user interface.

- 5. **Optional:** To disable the network interface from sniffing traffic, select the toggle to **OFF**.
- 6. In the **NAT** section, configure the settings as necessary for the *network address translation (NAT)* rule.

Note:

The *NAT* rule lets you rewrite the source and destination *IP* addresses of packets sniffed on this interface. For example, to translate 192.168.1.100 in 10.1.1.100 you have to configure the rule: 192.168.0.0 10.1.0.0 /16.

- a. In the **Original subnet** field, enter a value.
- b. In the **Translated subnet** field, enter a value.
- c. In the CIDR mask field, enter a value.
- 7. Select **Save**.

Results

The NAT rule has been configured.

Configure a BPF filter

The Network interfaces page lets you configure Berkeley Packet Filters (BPF).

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Network interfaces.

Result: The Network interfaces page opens.

3. To the left of the applicable interface, select the \rightleftharpoons icon.

Result: A dialog shows.

4. In the Label field, enter a label for the interface.

Configure interface	ж
Interface port1	
Label	
 The label must differ from other labels and network interface The label can contain only alphanumeric characters and '-' /'. Interface name will be used as label if empty value is provide 	names _'symbols d
Enable ON OFF	
NAT	
Original subnet	
e.g. 192.168.0.0	
Translated subnet	
e.g. 10.1.0.0	
CIDR mask	
e.g. /16	
 This rule allow the rewriting of source and destination IPs of this interface. e.g. to translate 192.168.1.100 in 10.1.1.100 you have to configure 192.169.0.101.0.0 //s 	backets sniffed on the rule:

Note:

The label will show instead of the network interface name in all areas of the user interface.

- 5. **Optional:** To disable the network interface from sniffing traffic, select the toggle to **OFF**.
- 6. In the **BPF filter** section, choose a method to use to configure the *Berkeley Packet Filter (BPF)* settings.

Choose from:

- To use the visual editor, go to step 7 (on page 168)
- To manually enter a filter, go to step 8 (on page 168)

- 7. Use the visual editor.
 - a. Select **BPF filter editor**.

BPF filter		
BPF filter editor		
Manual insertion of a	custom filter expression 🧃	
e.g. tcp port 502		

Result: A dialog shows.

b. Edit the settings as necessary.

BPF filter editor This editor supports the most common BPF syntax. If you wish to enter an advanced filter please use the "Manual insertion" from the previous window.	×
NOT Add rule Add grou C V Delete	2
Current BPF Filter	ncel

c. Select **Ok**.

8. Manually enter a *BPF*.

BPF filter	
BPF filter editor	
Manual insertion of	a custom filter expression 🦲
e.g. tcp port 502	

- a. Set the Manual insertion of a custom expression toggle to on.
- b. Manually enter the *BPF*.
- c. Select **Save**.

Results

The *BPF* has been configured.

Configure a denylist

The Network interfaces page lets you configure denylists.

About this task

In the **Denylist** section, you can upload a text file that contains a denylist. This can contain a list of *IP* addresses that are explicit, or with netmasks, or wildcards, that Guardian will not process. A wildcard in digit 2, 3 or 4 is equivalent to a /8, /16 or /24 netmask. The effect is similar to that of a *BPF*, however a denylist can handle tens of thousands of *IP* addresses, which is beyond the capabilities of a *BPF*.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Network interfaces.

Result: The Network interfaces page opens.

3. To the left of the applicable interface, select the \rightleftharpoons icon.

Result: A dialog shows.

4. In the **Label** field, enter a label for the interface.

Cor	nfigure interface	×
Interf	ace	
portl		
Label		
1	The label must differ from other labels and network interface names The label can contain only alphanumeric characters and '-' / '_' symbols Interface name will be used as label if empty value is provided	
Enabl	ON OFF	
Enabl NAT	ON OFF	
Enabl NAT Origir	al subnet	
Enabl NAT Origir	nal subnet	
Enabl NAT Origir e.g.1 Trans	Ie ON OFF nal subnet 192.168.0.0 lated subnet	
Enabl NAT Origir e.g.1 Trans	le ON OFF nal subnet 192.168.0.0 lated subnet 10.1.0.0	
Enabl NAT Origir e.g.1 Trans e.g.1 CIDR	le ON OFF nal subnet 192.168.0.0 lated subnet 10.1.0.0 mask	
Enabl NAT Origir e.g.1 Trans e.g.1 CIDR	le ON OFF nal subnet 192.168.0.0 lated subnet 10.1.0.0 mask /16	
Enabl NAT Origir Trans CIDR (e.g. /	Ie ON OFF This rule allow the rewriting of source and destination IPs of packets sniffed	d on
Enabl NAT Origir (e.g. 1 Trans (e.g. 1) CIDR (e.g. /) () =	le ON OFF hal subnet l92.168.0.0 lated subnet l0.1.0.0 mask //6 This rule allow the rewriting of source and destination IPs of packets sniffed this interface.	i on

Note:

The label will show instead of the network interface name in all areas of the user interface.

5. **Optional:** To disable the network interface from sniffing traffic, select the toggle to **OFF**.

6. In the **Denylist** section, set the **Enable denylist** toggle to on.

enylist Inable denylist	
Drop a file here or clic	k to upload
Maximum file size: 2G	
Supported formats:	Notes:
txt (.txt)	
	Save Cancel

7. Choose a method to upload the denylist file:

Choose from:

- $\,\circ\,$ Drag the denylist file into the Drop a file here or click to upload field
- Click in the Drop a file here or click to upload field and located the file to be uploaded

Note:

A denylist must contain:

- One entry per line
- A dash (-) followed by a space and an *IP* address. Optionally, it can contain a wild card or a netmask.

Note:

The maximum file size is 2 GB. The supported file type is text files (.txt).

Results

The denylist has been configured.

Denylist examples

<pre>- 192.168.1.* - 192.168.2.1 - 192.168.2.6192.168.3.90 - 192.168.4.1/20 - 192.168.5.1 tcp 80 - 192.168.5.2 tcp 80 100-110 - 192.168.5.3 udp 11 22 2000-30000</pre>	A wildcard in the IP in position 2, 3 or 4 is equivalent to a subnet ending in /8, /16 or /24. The last lines block only packets from a specific host/port (or set of ports).
- 192.168.2.* - 192.168.2.1	These entries are not disjoint, but the Guardian is able to fix automatically the conflict.
- 192.168.3.2 tcp 80 - 192.168.3.1/24 tcp 100	A logical error: 192.168.3.2 is an ambiguous match.
- 192.168.3.1 tcp 100 - 192.168.3.2 tcp 80 - 192.168.3.3192.168.3.255 tcp 100	As the entries do not intersect, this is the right way to fix the error above.
- 192.168.3.3 tcp 80 - 192.168.3.3 udp 100	These lines are in conflict: an ip can be associated with at most one port filter.

Upload traces

The **Upload traces** page lets you upload trace files and select the options for the uploaded file.

ttings Upload traces Image: Support of the state of th	tings Upload traces Image: Strate	NOZOMI =		
Option:	Option: Use trace timestamps Delete data before play Auto play trace after upload Replay speed Maximum speed Drop some traces here or click to upload Supported formats: PCAP and PCAPNG - Maximum file size: 20 Last uploaded traces Page1 of 1.2 entries Live Isupported formats: PCAP and PCAPNG - Maximum file size: 20 Last uploaded traces Page1 of 1.2 entries Isupported formats: PCAP and PCAPNG - Maximum file size: 20 Last uploaded time. Last played time Isupported formats: PCAP and PCAPNG - Maximum file size: 20 Isupported formats: PCAP and PCAPNG - Maximum file size: 20 Lest uploaded time. Last played time Isupported formats: PCAP and PCAPNG - Maximum file size: 20 Isupported formats: PCAP and PCAPNG - Maximum file size: 20 Isupported formats: PCAP and PCAPNG - Maximum file size: 20 	ttings	Upload traces	
Image: Drop some traces here or click to upload Supported formats: PCAP and PCAPNG - Maximum file size: 2G Image: Drop some traces here or click to upload Image: Drop some traces here or clic	Image: Drop some traces here or click to upload Supported formats: PCAP and PCAPNG - Maximum file size: 2G Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Supported formats: PCAP and PCAPNG - Maximum file size: 2G Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces here or click to upload Image: Drop some traces h		Options:	
Supported formats: PCAP and PCAPNG - Maximum file size: 2C Last uploaded traces Page 1 of 1, 2 entries Live @ () % 6 selected ~ Actions Last uploaded time. Last played time Filename Note ···	Supported formats: PCAP and PCAPNG - Maximum file size: 2C Last uploaded traces Page 1 of 1, 2 entries Live		Drop some traces here or click to upload	
Last uploaded traces Page 1 of 1.2 entries Live 0 6 selected Actions Last uploaded time. Last played time Filename Note ··· H + H H + H Note ··· H + H H + H	Last uploaded traces Page 1 of 1,2 entries Live			
Actions Last uploaded time Last ploaged time Filename Note N ← N	Actions Last uploaded time Last played time Filename Note K + V K K + V K		Supported formats: PCAP and PCAPNG - Maximum file size: 2G	
	Image: Non-State		Last uploaded traces Page 1 of 1 2 entries	● 6 selected ▼
em	em		Supported formats PCAP and PCAPING - Maximum Hile szer 2G Last uploaded traces Page 1 of 1.2 entries Live Actions Last uploaded time Filename	⊛ 6 selected ▼ Note
tem	tem		Supported formats PCAP and PCAPING - Maximum this size 2G Last uploaded traces Page 1 of 1.2 entries Actions Last uploaded time. Last played time Filename K ← X K ← X	€ selected
			Actions Last uploaded traces Page 1of1.2 entries Live ● () Actions Last uploaded time Last played time Filename K <+> N	® 6 selected ▼ Note
		stem	Supported formats PCAP and PCAPAG - Maximum Hills size 2G Last uploaded traces Page 1of1 2 entries Live ● 5 Actions Last uploaded time_ Last played time Filename ··· H 4 + N H 4 + N D © 2023-10-375/54-1891 2023-10-33175/31996 vuido.pcap - D © 2023-10-251817/07/766 2023-10-251817/59/590 TCPI02 57 pcap -	Image: Selected ▼ Note
		stom	Supported formats PCAP and PCAPAG - Maximum Hills size 2G Last uploaded traces Page 1 of 1.2 entries Live ● 5 Actions Last uploaded time_ Last played time Filename ··· H ← H H H ← H □ 2023-10-3715/54.1891 2023-10-33175/311996 vuido.pcap - □ ≥ 2023-10-251817/07/66 2023-10-251817/59/590 TCP102 57 pcap -	6 selected • Note

Figure 59. Upload traces page

Use trace timestamps

You can select this option to use the time captured in the trace file. Otherwise, the current time is used.

Important:

We recommend not selecting this checkbox because it causes data to be hidden due to time filters.

Delete data before play

Select this option to delete the data in the sensor before you run the play action. When multiple traces are played at once, deletion is applied only before running the first trace.

Auto play trace after upload

Select this option to play the trace immediately after the upload is complete.

Replay speed

You can choose from the available options to customize the maximum throughput at which the *pcap* is played.

Upload field

You can click in the upload field, or drag a file into the upload field to upload a trace. The recommended formats are:

- pcap
- packet capture next generation (pcapNg)

The maximum file size that you can upload is 2 GB.

Live / refresh

The Live \bigcirc (\bigcirc icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection ${}^{igodoldsymbol{\Theta}}$ icon lets you choose which columns to show or hide.

Actions

The Actions column lets you:

- Replay a trace file (on page 176)
- Edit a note for a trace file (on page 176)
- Delete a trace file (on page 178)

Last uploaded traces

Before you take an action, you can use this element to filter and sort the traces. You can select the text in the header to sort in ascending or descending order. You can then select the header again to toggle between the two.

Last played time

Before you take an action, you can use this element to filter and sort the traces. You can select the text in the header to sort in ascending or descending order. You can then select the header again to toggle between the two.

Upload a trace file

The Upload traces page lets you upload a trace file.

Procedure

1. In the top navigation bar, select 🐼

Result: The administration page opens.

2. In the System section, select Upload traces.

Result: The Upload traces page opens.

3. Choose a method to upload a trace file.

Choose from:

- $\circ\,$ Drag your image file into the Drop some traces here or click to upload field
- Click in the Drop some traces here or click to upload field
- 4. If you chose the second method, select the correct file to upload.

Dptions: Use trace timestamps Replay speed Maximum spe	Delete data before play 1	Auto play trace after upload	
	Drop some traces here or o	lick to upload	
Supported formats: PCAP	and PCAPNG - Maximum file size	x 2G	
~			_



5. Wait for the file to upload.

Results

The trace file has been uploaded.

Replay a trace file

After you have uploaded a trace file, you can replay it whenever you want.

About this task

As a result of playing traces, alerts can be generated. If the played file is artificial, the system might not recognize the alert timestamp. In this case, a value containing InvalidDate shows in the time column of the alert table.

Procedure

1. In the top navigation bar, select $\langle S \rangle$

Result: The administration page opens.

2. In the System section, select Upload traces.

Result: The Upload traces page opens.

3. Choose a method.

Choose from:

- To replay a single file, go to step 4 (on page 176)
- To replay multiple files, go to 5 (on page 176)
- 4. To replay a single file, to the left of the applicable trace file, select the 🕨 icon.
- 5. Replay multiple files.
 - a. Select multiple checkboxes for the items that you want to choose.
 - b. In the Actions column, select the ••• icon.
 Result: A menu shows.
 - c. From the menu, select **Play selected**.

Results

The trace file(s) has (have) been replayed.

Edit a note for a trace file

After you upload a trace file, you can write a note for it, or edit an existing one.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Upload traces.

Result: The Upload traces page opens.

- 3. To the left of the applicable trace file, select the ${\ensuremath{ \ensuremath{ \ensuremath$
- 4. Write or edit the details as necessary.
- 5. Select **Save**.

Results

The note has been edited.

Delete a trace file

After you have uploaded a trace file, you can delete it.

Procedure

- 1. In the top navigation bar, select 🛱 **Result:** The administration page opens.
- 2. In the **System** section, select **Upload traces**.

Result: The Upload traces page opens.

3. To the left of the applicable trace file, select the $\widehat{\mathbb{I}}$ icon.

Results

The trace file has been deleted.

Export

The **Export** page lets you export data in content packs.

Settings	Export data	
	Export content pack	
	• You can export entire sections or individual groups.	
	🗌 Reports 🗸	
	🗌 Queries 🗸	
	🗋 Dashboards 🗸	
	🗋 Alert playbooks 🗸	
	Alert Rules associated to the Playbooks	
	Export data	
the second s		
System		
Export		

Figure 60. Export page

General

You can export data in content packs, which are files in *JSON* format that you can open and read with a text reader.

Content packs

Content packs are a reporting and query feature that packages multiple templates into a single file for team collaboration. A single content pack can contain one or more:

- Reports
- Queries
- Dashboards
- Alert playbooks

Note:

When you select **Alerts Playbooks**, you get the option to choose **Alert Rules associated with the Playbooks**.

Content packs package data in a single file, which can then be distributed to a team of people. They can then be edited and used across multiple systems. This is especially useful in complex reporting arrangements, such as compliance with government regulations, or hunting for a specific threat.

The file expands so you can add other information in the *JSON* format to the content pack. The Nozomi Networks product ignores data that it doesn't understand and continues to parse the file. This lets you add data for other systems to the content pack.



When you export a dashboard and insert the related content pack into a new Guardian instance, the dashboards load and function the same as those from the original Guardian. Imported dashboards include all the queries and widgets associated with the original saved dashboards.
Export a content pack

You can use the **Export** page to export data in content packs which can contain report, queries, dashboards, or alert playbooks.

About this task

This procedure shows you how to export a content pack from the **Export** page. To export directly from a dashboard, see **Settings > Dashboards > Export a dashboard**.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Export.

Result: The Export data page opens.

- 3. In the Export content pack section, select options that you want to export.
- 4. Optional: Export reports.
 - a. Select the **Reports** checkbox.
 - b. Select the ✓ icon.Result: The section expands.
 - c. Optional: If necessary, select individual items as necessary.
- 5. **Optional:** Export queries.
 - a. Select the **Queries** checkbox.
 - b. Select the ✓ icon.
 Result: The section expands.
 - c. Optional: If necessary, select individual items as necessary.
- 6. Optional: Export dashboards.
 - a. Select the **Dashboards** checkbox.
 - b. Select the ✓ icon.
 Result: The section expands.
 - c. Optional: If necessary, select individual items as necessary.

- 7. Optional: Export alert playbooks.
 - a. Select the **Alert Playbooks** checkbox.

 - c. **Optional:** If necessary, select individual items as necessary.
 - d. Optional: If necessary, select Alert Rules associated to the Playbooks.
- 8. Select Export data.

Import

The **Import** page lets you import data from multiple different sources, and in multiple formats.

NOZOMI =				ŝ
ettings	Import data			
		Import nodes - CS	SV file 🗸	
		Import nodes - CSV file		
		O Load node information from CSV files. Th node to be modified, a row with columns s (i.e., vendor, serial number, custom fields) specify the column names. Select 'Override	ne file must contain, for each pecifying the additional data . Optionally, a header can a manual data' to replace	
		manually edited values. NOTE: some fields may not be overwritten.	and Confirmed Mac Addresses	
		🗹 Has header 🗌 Override manual data	Separator Comma 🗸	
		Drop a file here or clir	sk to upload	
		Diop a menere or circ		
		Maximum file size: 2G		
		Supported formats:	Notes:	
		Comma-separated values (.csv)		
stem				
Import				

Figure 61. Import page

Import nodes

This feature lets you bind fields from a CSV files to Nozomi Networks fields so that you can add nodes (flag **create non-existing nodes**), or enrich existing ones. For each modified node, the file must include a row with columns that specify the additional data.

Note:

Some special fields and confirmed *MAC* addresses are restricted to specific values and so they might not be overwritten.

Import variables

This feature lets you add new variables (flag **create non-existing variables**), or to enrich existing variables. For each modified variable, the file must include a row with columns that specify the additional data.

Import asset types

This feature lets you enlarge the built-in set of asset types with a set of new custom types. The *CSV* file should include a header row labeled **Name** and the list of asset type names in the following rows, one per row. A name identifies each asset type. This means that, during the import process, duplicate names are ignored and notified.

Default asset types

actuator

audio_video

AVR

barcode_reader camera

computer

controller

digital_io

drone

DSL_modem

firewall

gateway

HMI IED

infusion_system

inverter

IO_module

IOT_device

light_bridge

media_converter

medical_imager

meter

mobile_phone

network_security_appliance

OT_device

other

PDU PLC

power_generator

power_line_carrier

printer_scanner

radio_transmitter

robot

router

RTU

sensor

server

switch tablet time_appliance UPS VOIP_phone WAP

Import configuration / project file

This feature lets you import a project file. The information written in the project file is added to the asset data.

Note:

For XML Profinet GSDML, you can import an *XML* Profinet GSDML file that describes a physical device. Information in the file lets Guardian extract and display information about the device configuration when device configuration packets are displayed in traffic.

Supported file type	Imported fields
Allen-Bradley	ip, firmware version, product name, modules (i.e. port, address, product code, firmware version, product name, vendor)
Honeywell TDS	label, vendor
IEC 61850 SCL/SCD	ip, VLAN, product name, asset type, vendor, AppID, data model Note : Importing this file changes the knowledge of the IEC 61850 data model in use in the system, thus improving Guardian's ability to accurately extract variables. Existing variables related to this protocol are deleted to avoid inconsistencies with those extracted from traffic after the import.
Profinet IOCM	modules (i.e. slot, subslot, vendor, software release, hardware release). It might also extract variables
Rockwell Harmony	ip, product name
Siemens	ip, mac address, vendor, product name, label, modules (i.e. rack, slot, subslot, product code, module code)
Triconex	ip, label, vendor
Yokogawa Centum	ip, label, vendor, product name, modules (i.e. slots, each with vendor, product name, firmware version)

Table 6. Supported file types for configuration / project files

Import content pack

You can use the **Export** page to export data in content packs and then you can use the **Import** page of a different machine to import them. For more details, see Export (on page 179).

Import Arc data archive

When Arc is in **Offline** mode, the data is collected locally and then exported in an archive file from the machine. The archive file can then be manually imported into *CMC*, Guardian, or Vantage.

Import nodes from a CSV file

You can use the **Import** page to import nodes from a comma-separated value (CSV) file.

About this task

This feature lets you bind fields from a *CSV* files to Nozomi Networks fields so that you can add nodes, or enrich existing ones. For each modified node, the file must include a row with columns that specify the additional data.

Note:

Some special fields and confirmed *MAC* addresses are restricted to specific values and so they might not be overwritten.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Import.

Result: The Import data page opens.

3. From the dropdown at the top of the page, select Import nodes - CSV file.

Result: The Import nodes - CSV file section shows.

- 4. **Optional:** If the *CSV* file has headers in the first line of the file, select **Has header** to view the column titles.
- 5. **Optional:** If you want the file data to replace field values that were previously imported or manually overridden, select **Override manual data**.
- 6. From the **Separator** dropdown, select the correct option.
- 7. Choose a method to upload a file.

Choose from:

- $\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the **Drop a file here or click to upload** field

8. If you chose the second method, select the correct file to upload.

Import nodes - C	SV file 🗸
Import nodes - CSV file	
D Load node information from CSV files. I node to be modified, a row with columns (i.e., vendor, serial number, custom fields specify the column names. Select 'Overric manually edited values. NOTE: some field may not be overwritten.	he file must contain, for each specifying the additional data). Optionally, a header can le manual data' to replace s and Confirmed Mac Addresses
🗹 Has header 🗌 Override manual data	Separator Comma 🗸
Drop a file here or cl	ick to upload
Maximum file size: 2G	
Supported formats:	Notes:
Comma-separated values (.csv)	

	Note:
	The supported format is CSV.
	The maximum permitted file size is 2 <i>GB</i> .

9. Wait for the file to upload.

Results

The CSV file has been uploaded.

Import variables from a CSV file

You can use the **Import** page to import variables from a comma-separated value (CSV) file.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Import.

Result: The Import data page opens.

3. From the dropdown at the top of the page, select Import variables - CSV file.

Result: The Import variables - CSV file section shows.

- 4. **Optional:** If the *CSV* file has headers in the first line of the file, select **Has header** to view the column titles.
- 5. From the **Separator** dropdown, select the correct option.
- 6. Choose a method to upload a file.

Choose from:

- $\,\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the **Drop a file here or click to upload** field

7. If you chose the second method, select the correct file to upload.

Imp	ort variables - CSV file 🗸
Import variables - CS	/ file
Load variable information variable to be modified, a row data (i.e., name, label, unit). names. NOTE: some fields ar written if the values differ frc	rom CSV files. The file must contain, for each (with columns specifying the additional Optionally, a header can specify the column restricted to specific values and won't be m them.
✓ Has header	Separator Comma 💙
Drop a	ile here or click to upload
Maximum file size: 2G	
Supported formats:	Notes:
Comma-separated values (.csv)	
	Import variables - CS • Load variable information f variable to be modified, a row data (i.e., name, label, unit). names. NOTE: some fields are written if the values differ from I Has header Drop a f Maximum file size: 2G Supported formats: Comma-separated values (csv)

The supported format is CSV. The maximum permitted file size is 2 GB.

8. Wait for the file to upload.

Results

The CSV file has been uploaded.

Import asset types from a CSV file

You can use the **Import** page to import asset types from a comma-separated value (CSV) file.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Import.

Result: The Import data page opens.

3. From the dropdown at the top of the page, select Import asset types - CSV file.

Result: The Import asset types - CSV file section shows.

4. Choose a method to upload a file.

Choose from:

- $\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the Drop a file here or click to upload field
- 5. If you chose the second method, select the correct file to upload.

Import asset type	es - CSV file 🔻
Import asset types - CSV file	
O Load asset types information from CS header row with 'name' and, for each as asset type name	V files. The file should contain a set type to import, a row with the
Drop a file here or	click to upload
Maximum file size: 2G	
Supported formats:	Notes:
Comma-separated values (.csv)	



The supported format is CSV. The maximum permitted file size is 2 GB.

6. Wait for the file to upload.

Results

The CSV file has been uploaded.

Import a configuration or project file

You can use the **Import** page to import configuration or project files.

Procedure

1. In the top navigation bar, select $\textcircled{\begin{tmatrix} \label{eq:constraint} \label{eq:constraint} \end{tmatrix}}$

Result: The administration page opens.

2. In the System section, select Import.

Result: The Import data page opens.

3. From the dropdown at the top of the page, select **Import configuration / project file**.

Result: The Import configuration / project file - CSV file section shows.

4. Choose a method to upload a file.

Choose from:

- $^\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the Drop a file here or click to upload field

5. If you chose the second method, select the correct file to upload.

Import co	nfiguration / project file 👻
Import configuration /	oroject file or project files to extract some relevant ted file formats is given below).
Drop a file	here or click to upload
Maximum file size: 2G	
Supported formats:	Notes:
Rockwell Harmony (.conf, .rsx, .rsh)	
Yokogawa CENTUM VP (.gz, .zip)	
Siemens (.cfg)	
IEC 61850 SCL/SCD (.scd, .icd, .cid)	Existing IEC 61850 variables may be deleted
Triconex (.pt2)	
Allen-Bradley (.I5x)	
Honeywell TDS (.txt, .zip)	
Profinet IOCM (.xml)	
Siemens AML (.aml)	
Mitsubishi (.gxw)	

Note:

Supported formats are:

- Rockwell Harmony (.conf, .rsx, .rsh)
- Yokogawa CENTUM VP (.gz, .zip)
- Siemens (.cfg)
- IEC 61850 SCL/SCD (.scd, .icd, .cid)
- Triconex (.pt2)
- Allen-Bradley (.15x)
- Honeywell TDS (.txt, .zip)
- Profinet IOCM (.xml)
- Siemens AML (.aml)
- Mitsubishi (.gxw)

The maximum permitted file size is 2 GB.

Note:

For Yokogawa format you need to create a ZIP file that includes:

- *.edf
- /ETC/SystemRevisionInf.txt
- project.atr

6. Wait for the file to upload.

Results

The file has been uploaded.

Import a content pack

You can use the *Import* page to import content packs.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Import.

Result: The Import data page opens.

3. From the dropdown at the top of the page, select **Import content pack**.

Result: The Import content pack section shows.

4. Choose a method to upload a file.

Choose from:

- $\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the Drop a file here or click to upload field
- 5. If you chose the second method, select the correct file to upload.

Import of	ontent pack 🗸
Import content pack	
Load Nozomi content pack.	
Drop a file here	e or click to upload
Maximum file size: 2G	
Supported formats:	Notes:
Nozomi content pack (.json)	

Note:

The supported format is *JSON*.

The maximum permitted file size is 2 GB.

6. Wait for the file to upload.

Results

The JSON file has been uploaded.

Import an Arc data archive

You can use the Import page to import an Arc data archive.

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the System section, select Import.

Result: The Import data page opens.

3. From the dropdown at the top of the page, select Import Arc data archive.

Result: The Import Arc data archive section shows.

4. Choose a method to upload a file.

Choose from:

- $^\circ\,$ Drag your file into the Drop a file here or click to upload field
- Click in the Drop a file here or click to upload field
- 5. If you chose the second method, select the correct file to upload.

Import Arc d	ata archive 🗸	
Import Arc data archive		
Dead data collected by an Arc offline	e execution.	
Drop a file here o	or click to upload	
Maximum file size: 2G		
Supported formats:	Notes:	
Arc data archive (.zip)		



6. Wait for the file to upload.

Results

The *ZIP* file has been uploaded.

Health

The Health page lets you monitor the health of your sensors.



Figure 62. Health page

The Health page has these tabs:

- Performance (on page 198)
- Health log (on page 200)

Performance

The **Performance** page has graphical sections that show percentage usage for central processing unit (CPU), random-access memory (RAM), and disk usage. It also has a **Services** section.



Figure 63. Performance page

Graphs

The page shows graph for:

- CPU percentage usage
- RAM MB usage
- Disk percentage usage

The vertical axis show percentage usage and the horizontal axis shows time.

These sections have an **ON/OFF** toggle and time controls that let you choose the timeframe of the window. You can choose between:

- One minute
- One hour
- One day
- One week

Services

This section shows information about:

- The intrusion detection system (IDS)
- Alerts
- Sandbox
- Trace
- Vulnerabilities

Health log

The **Health log** page shows the details of performance issues that the sensor experiences. The information is for such as central processing unit (CPU), random-access memory (RAM), and disk usage, interface status, stale sensors, or generic high load.

Page 1 of 200 , 5000 ent	ries	Export 📋	Live 💽 🞵	Appliance hose	t, Description, Time
	APPLIANCE HOST		Live	DESCRIPTION	l
11:15:37.026	lab-r50.intra.nozominetworks.com		is under high load		
11:10:37.190	lab-r50.intra.nozominetworks.com		is under high load		
11:05:36.519	lab-r50.intra.nozominetworks.com		is under high load		
11:00:36.562	lab-r50.intra.nozominetworks.com		is under high load		
10:55:36.444	lab-r50.intra.nozominetworks.com		is under high load		
10:50:35.998	lab-r50.intra.nozominetworks.com		is under high load		
10:45:35.995	lab-r50.intra.nozominetworks.com		is under high load		
10:40:35.993	lab-r50.intra.nozominetworks.com		is under high load		
10:35:35.999	lab-r50.intra.nozominetworks.com		is under high load		
10:30:35.992	lab-r50.intra.nozominetworks.com		is under high load		
10:25:35.988	lab-r50.intra.nozominetworks.com		is under high load		
10:20:35.988	lab-r50.intra.nozominetworks.com		is under high load		
10:15:35.986	lab-r50.intra.nozominetworks.com		is under high load		
10:10:35.986	lab-r50.intra.nozominetworks.com		is under high load		
10:05:35.985	lab-r50.intra.nozominetworks.com		is under high load		
10:00:35.985	lab-r50.intra.nozominetworks.com		is under high load		
09:55:35.980	lab-r50.intra.nozominetworks.com		is under high load		
09:50:35.983	lab-r50.intra.nozominetworks.com		is under high load		
09:45:35.979	lab-r50.intra.nozominetworks.com		is under high load		
09:40:35.981	lab-r50.intra.nozominetworks.com		is under high load		
09:35:35.783	lab-r50.intra.nozominetworks.com		is under high load		
09:30:35.782	lab-r50.intra.nozominetworks.com		is under high load		
09:25:35.782	lab-r50.intra.nozominetworks.com		is under high load		
09:20:35.780	lab-r50.intra.nozominetworks.com		is under high load		
09:15:35.781	lab-r50.intra.nozominetworks.com		is under high load		

Figure 64. Health log page

The central processing unit (CPU) percentage usage, random-access memory (RAM) MB usage and disk percentage usage will show as:

- Good
- Average, or
- Poor

Stale or **unreachable** describes the status of the communication between Remote Collector, Guardian, and *CMC* (sync). It means that the last time the sensor communicated back to the upstream, the configured threshold was exceeded.

Audit

The **Audit** page shows a list of all relevant user actions, from login/logout to configuration operations, such as manually learning or deleting objects from the environment. This includes all recorded user actions based on the internet protocol (IP) address and username of the user who performed the action.

NOZOMI =				
ettings	Audit			
	Page 1 of 573.14	315 entries		Export [[↑]] Live 💽 🦪 Selected 🕶
	A - 41 Time			
	Act IIm		Username	
	0	10 (1172)76		Uses sent looped out vie set from best 30 /1379376
	Q 15.55.47.	10.41.132.136	root	User root logged out via sen from host 10.41.32.130
	Q 1554-54	000 10.41.152.156	root	User root logged in via son from host io-#LIS2.156
	Q 13:13:30	00 10.41.278.171	root	User root theu to login via san using a key associated to admini (key value = 200000223)211012
	Q 13:12:303	00 10.41.238.131	root	User root logged out via set from host 10.41238.131
	0 1312:264	00 10.41250.151	root	Liser root tried to login via service room a key associated to nºlaryis (key value = AAAAB3N7aChy
	0 1312:264	10.0 10.41.238.131	root	Liser root logged out via sch from host 10.61 238 131
	0 1312:04	10.41.238.131	root	User root lagged out in Jan Horn has 10-41238.131
	0 13:12:03:	00	root	User root tried to login via ssh using a key associated to nZiarvis (key value = AAAAB3NzaC1v
	0 13:12:02	000 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q 13:11:55.0	00 10.41.132.196	root	User root logged out via ssh from host 10.41.132.196
	Q 13:11:41.0	00 10.41.238.131	root	User root logged in via ssh from host 10.41.238.131
	Q, 13:11:40.0	00	root	User root tried to login via ssh using a key associated to n2jarvis (key value = AAAAB3NzaC1y
em	Q, 13:11:40.0	00 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q, 13:11:39.0	00 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q 13:11:20.0	00 10.41.238.131	root	User root logged in via ssh from host 10.41.238.131
	Q 13:11:19.0	10.41.238.131	root	User root logged in via ssh from host 10.41.238.131
	Q 13:11:18.0	00	root	User root tried to login via ssh using a key associated to n2jarvis (key value = AAAAB3NzaCly
	Q 13:11:03.0	00 10.41.238.131	root	User root lagged out via ssh from host 10.41.238.131
	Q 13:11:03.0	00 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q 13:11:02.0	00 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q 13:11:02.0	00 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q 13:11:02.0	00 10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
idit	Q 13:11:01.0	10.41.238.131	root	User root logged out via ssh from host 10.41.238.131
	Q 13:10:41.0	00	root	User root tried to login via ssh using a key associated to n2jarvis (key value = AAAAB3NzaCly
				1 2 3 4 5 6 7 573 ·

Figure 65. Audit page

Export

The **Export** $\stackrel{(\uparrow)}{\square}$ icon lets you export the current list in either CSV or Microsoft Excel format.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection $^{igodoldsymbol{\Theta}}$ icon lets you choose which columns to show or hide.

Data

The **Data** page lets you selectively reset several kinds of data. You can select **All**, **Only data**, or **None**, depending on the type of user data that you want to reset.

NOZOMI =		ŝ
Settings	Data	
	Reset different kind of data for all the users All Only data None	
-	Environment Reset network nodes, assets, links and variables (learned data is lost)	
	Network Reset link event history, network charts data and captured URLs/files	
	Process history Reset the variables history	
	CPEs and CVEs Reset the information related to vulnerabilities	
	□ Alerts Reset the alerts	
	Traces Reset generated traces, both requested by users and automatically generated	
	Time machine Reset the snapshots of the time machine	
System	Queries Reset the queries and query groups	
	Assertions Reset the assertions	
	Smart Polling Delete Smart Polling node points	
	Learning Reset to 'Learning' phase	
	Reset	
Data		

Figure 66. Data page

Environment

Reset network nodes, assets, links and variables (learned data is lost).

Network

Reset link event history, network charts data and captured URLs/files

Process history

Reset the variables history.

CPEs and CVEs

Reset the information related to vulnerabilities.

Alerts

Reset the alerts.

Traces

Reset user-requested and automatically-generated traces.

Time machine

Reset the snapshots of the time machine.

Queries

Reset the queries and query groups.

Assertions

Reset the assertions.

Smart Polling

Delete Smart Polling node points.

Learning

Reset to the **Learning** phase.

Migration tasks

The **Migration tasks** page gives you access to automated tasks that help you migrate the system configuration and settings to newer standards.

		Ŕ
Settings	Migration tasks	
	Data Model Updates The sensor is currently synchronized with Vantage or the parent CMC. Migration tasks are managed from there.	
	Credentials Import into Credentials Manager The sensor is currently synchronized with Vantage or the parent CMC. Migration tasks are managed from there.	
System		
-		
_		
Migration tasks		

Figure 67. Migration tasks page

Migration tasks are a helper tool that can be used to apply specific changes to configuration, settings and data to make use of new features, or adapt to model changes. These tasks become available upon the installation of new versions of the software, and are described in the related release notes.

Migration tasks can only be executed from the top-level *CMC* of an installation. Guardians that are not connected to a *CMC* can also run migration tasks. If the installation is connected to Vantage, then Vantage can run the migration tasks.

Each migration task is presented separately, giving an overview of the changes that will be applied on each connected sensor. Tasks can be executed on individual Guardians, or on *CMCs*, When a *CMC* executes the migration tasks, all the sensors that are connected downstream, either directly or indirectly, receive the instruction to execute the task. You can select **Execute all** to apply the migration tasks globally. With this approach, migration tasks can be ignored, which disables the execution of the corresponding task on the chosen sensor, or sensors.

When the migration task is executed, a spinning wheel shows next to the sensors that are executing it. Since the execution of a task is an asynchronous process, it can take up to several minutes to complete. During this time, it is safe to leave the page, or disconnect from the Web *UI*. The **Migration tasks** page will report the result of each execution.

You can select **Hide permanently** to hide migration tasks. This hides the migration task and it cannot be executed again.

Operations

The **Operations** page lets you reboot or shutdown the sensor, or manage the software updates for your sensor.

NOZOMI =		ĝ
Settings		
	Reboot Shutdown	
	Software Update This software version is controlled by Vantage or a CMC. 	
	New scheduled update	
	Scheduled updates	
	Page 1 of 1, 0 entries Actions Sensors	Live • 5
	No scheduled update	
System		
Operations		

Figure 68. Operations page

Reboot

This lets you reboot the system.

Shutdown

This lets you shutdown the system.

Software update

This lets you update the software on the sensor. If there is an upstream Vantage or *CMC* that is in control of the sensor, this button will be inactive.

New scheduled update

This lets you set a schedule for the updates.

Reboot or shutdown the system from the web UI

You can reboot or shutdown the system from the web UI.

About this task

The reboot and shutdown commands are performed from the web UI. Alternatively, you can perform both commands from the shell console (inside an *SSH* session).

Procedure

1. In the top navigation bar, select \bigotimes

Result: The administration page opens.

2. In the **System** section, select **Operations**.

Result: The Operations page opens.

3. Choose the action that you want to do:

Choose from:

- In the top left corner, select **Reboot**
- In the top left corner, select **Shutdown**

Reboot Sh	utdown			
) This software	version is controlled by Vantage	∋ or a CMC.		
New schedule	d update			
cheduled u	pdates			
Page 1 of 1, 0	entries			Live • 🥥
	Next occurrence	Schedule type	Sensors	Version
Actions				
No schedu	Jled update			

Results

The system reboots or shuts down.

Support

The **Support** page section lets you generate a support archive that you can then send to Customer Support when you need technical support.

	Ø	
Settings	Support	
	Cenerate Support Archive Cick on Download to generate and download the support archive to send to the Nozomi Networks Support Comparison Support Archive Comparison Archive Comparison Archive does not contain sensitive information about the network. It should be used only when the normal archive cannot be shared Download	e
System		
Support		

Figure 69. Support page

General

You can generate a support archive that can then be uploaded to a support case in the Customer Support Portal.

Anonymize Support Archive

This option removes sensitive network information from the generated archive. This option should only be used when a normal archive cannot be shared.

Backup and restore

The **Backup and restore** page lets you generate and schedule backup archives as well as restore the software from a backup.

			<u>نې</u>
Settings	Backup and restore	Backup	Restore
		-	
System			
Backup and restore			

Figure 70. Backup and restore page

The **Backup and restore** page has these tabs:

- Backup
- Restore

Important:

Backups do not contain data that relates to vulnerabilities or schedules. Therefore, restored machines will preserve the old tables with the previous:

- Vulnerabilities
- Report schedules
- Backup and restore schedules

Backup

The **Backup** page lets you generate and schedule backup archives as well as restore the software from a backup.

Settings Backup and restore Backup Restore Schedule Backup Archive generation Click on Schedule backup and setup the backup settings Page 1 of 1 entries Lve • • • • • • • • • • • • • • • • • • •	:		PMI ≡	
ystem Schedule Backup Archive generation Click on Schedule backup and setup the backup settings Page 1 of 1.0 entries Liv e i i e i e securio. Actions Name Recurrence (server th Max stored b Storage Include trace Encryption Last executio Status Schedule backups Circk due backup Archive Circerate Backup Archive Click on Townload to generate and download the backup archive 	Backup Restc	Backup and restore		ettings
Actions Name Recurrence (server ti Max stored b Storage Include trace Encryption Last execution Status There are no scheduled backups Schedule backup Available disk space: 30C / 39C Cenerate Backup Archive Cick on "Download" to generate and download the backup archive		Schedule Backup Archive generation Click on "Schedule backup" and setup the backup settings 		
tem Actions Name Recurrence (server ti Max stored b Storage Include trace Encryption Last executio Status There are no scheduled backups Schedule backup Available disk space: 30G / 39G TELOR Cenerate Backup Archive Ciccut on Download the backup archive	Live • 9 selected •	Page 1 of 1, 0 entries		
tem Available disk space: 30C / 39C There are no scheduled backups Schedule backup Teoremate Backup Archive O Click on Deventioned the backup archive	e trace Encryption Last executio Status	Actions Name Recurrence (server ti Max sto		
Cenerate Backup Archive Click on Download to generate and download the backup archive		Available disk space: 30C / 39C 78.0%		stem
Generate Backup Archive Cilck on Download' to generate and download the backup archive Cilck on Download' to generate and download the backup archive				
		Generate Backup Archive Click on 'Download' to generate and download the backup archive		
Download		Download		

Figure 71. Backup page

Schedule Backup Archive generation

This lets you schedule the generation of a backup archive. For more details, see the **Guardian and CMC Maintenance Guide**.

Generate Backup Archive

This section lets you generate a backup archive. For more details, see the **Guardian and CMC Maintenance Guide**.

The supported format is **nozomi_backup**.

Restore

The **Restore** page lets you restore a previous backup, and to schedule the restoration of a backup archive.

NOZOMI =		贷
Settings	Backup and restore	Backup Restore
	Restore Previous Backup O Select a previous backup to restore	
	Page 1 of 1,0 entries	Live •
	Actions Name Size	
	No backup file stored	
	Upload a previous backup to restore	
system	Drop a file here or click to upload	
	Maximum file size: 2G	
	Supported formats: Notes:	
	(nozomi_backup)	
	Schedule Restore Archive	
Backup and restore	Click on 'Schedule restore' and setup the restore settings	
	Schedule restore	

Figure 72. Restore page

Restore Previous Backup

This section lets you restore a previously created backup. For more details, see the **Guardian and CMC Maintenance Guide**.

Schedule Restore Archive

This lets you schedule the restoration of a backup archive. For more details, see the **Guardian and CMC Maintenance Guide**.



Glossary



Amazon Machine Image

An AMI is a type of virtual appliance that is used to create a virtual machine for the Amazon Elastic Compute Cloud (EC2), and is the basic unit of deployment for services that use EC2 for delivery.

Amazon Web Services

AWS is a subsidiary of the Amazon company that provides on-demand cloud computing platforms governments, businesses, and individuals on a pay-asyou-go basis.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Assertion Consumer Service

An ACS is a version of the SAML standard that is used to exchange authentication and authorization identities between security domains.

Asset Intelligence™

Asset Intelligence is a continuously expanding database of modeling asset behavior used by N2OS to enrich asset information, and improve overall visibility, asset management, and security, independent of monitored network data.

Berkeley Packet Filter

The BPF is a technology that is used in some computer operating systems for programs that need to analyze network traffic. A BPF provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in the similar method to the sensor.

Central Processing Unit

The main, or central, processor that executes instructions in a computer program.

Certificate Authority

A certificate, or certification authority (CA) is an organization that stores, signs, and issues digital certificates. In cryptography, a digital certificate certifies the ownership of a public key by the named subject of the certificate.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

Command-line interface

A command-line processor uses a command-line interface (CLI) as text input commands. It lets you invoke executables and provide information for the actions that you want them to do. It also lets you set parameters for the environment.

Comma-separated Value

A CSV file is a text file that uses a comma to separate values.

Common Event Format

CEF is a text-based log file format that is used for event logging and information sharing between different security devices and software applications.

Common Platform Enumeration

CPE is a structured naming scheme for information technology (IT) systems, software, and packages. CPE is based on the generic syntax for Uniform Resource Identifiers (URI) and includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

Common Weakness Enumeration

CWE is a category system for software and hardware weaknesses and vulnerabilities. It is a community project with the aim to understand flaws in software and hardware and create automated tools that can be used to identify, fix, and prevent those flaws.

Configuration file

A CFG file is a configuration, or config, file. They are files that are used to configure the parameters and initial settings for a computer program.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

ESXi

VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS). Instead, it includes and integrates vital OS components, such as a kernel.

Extensible Markup Language

XML is a markup language and file format for the storage and transmission of data. It defines a set of rules for encoding documents in a format that is both humanreadable and machinereadable.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

File Allocation Table

FAT is a file system architecture used in computers for managing disk space. It maintains a table to track the allocation of files on a disk, supporting efficient data storage, access, and management

File Transfer Protocol

FTP is a standard communication protocol that is used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client-server model architecture that uses separate control and data connections between the client and the server.

Fully qualified domain name

An FQDN is a complete and specific domain name that specifies the exact location in the hierarchy of the Domain Name System (DNS). It includes all higher-level domains, typically consisting of a host name and domain name, and ends in a top-level domain.

Gigabit per second

Gigabit per second (Gb/s) is a unit of data transfer rate equal to: 1,000 Megabits per second.

Gigabyte

The gigabyte is a multiple of the unit byte for digital information. One gigabyte is one billion bytes.

Graphical User Interface

A GUI is an interface that lets humans interact with electronic devices through graphical icons.

Graphics Interchange Format

GIF is a bitmap image format that is widely used on the internet.

High Availability

High Availability is a mode that permits the CMC to replicate its own data on another CMC.

Host-based intrusiondetection system

HIDS is an internal Nozomi Networks solution that uses sensors to detect changes to the basic firmware image, and record the change.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Identifier

A label that identifies the related item.

Identity Provider

An IdP is a system entity that creates, maintains, and manages identity information. It also provides authentication services to applications within a federation, or a distributed network.

Industrial Control Systems

An ICS is an electronic control system and related instrumentation that is used to control industrial processes.
Industrial Internet of Things

The IIoT is a name for interconnected devices, sensors, instruments, which are networked together with industrial applications. This connectivity allows for analysis and data collection, which can facilitate improvements in efficiency and productivity.

Internet Control Message Protocol

ICMP is a supporting protocol in the internet protocol suite. Network devices use it to send error messages and operational information to indicate success or failure when communicating with another IP address. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems.

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

Intrusion Detection System

An intrusion detection system (IDS), which can also be known as an intrusion prevention system (IPS) is a software application, or a device, that monitors a computer network, or system, for malicious activity or policy violations. Such intrusion activities, or violations, are typically reported either to a system administrator, or collected centrally by a security information and event management (SIEM) system.

JavaScript Object Notation

JSON is an open standard file format for data interchange. It uses human-readable text to store and transmit data objects, which consist of attribute-value pairs and arrays.

Joint Photographic Experts Group

JPEG, or JPG, is a method of lossy compression that is used for digital images. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality.

Lightweight Directory Access Protocol

LDAP is an open, vendorneutral, industry standard application protocol that lets you access and maintain distributed directory information services over an internet protocol (IP) network.

Lightweight Directory Access Protocol Secure

LDAP over SSL or Secure LDAP is the secure version of LDAP.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Megabyte

The megabyte is a multiple of the unit byte for digital information. One megabyte is one million bytes.

National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Network Address Translation

NAT is a method of mapping an internet protocol (IP) address space into another one. This is done by modifying network address information in the IP header of packets while in transit across a traffic routing device.

Network Interface Controller

A network interface controller (NIC), sometimes known as a network interface card, is a computer hardware component that lets a computer connect to a computer network.

Network Time Protocol

The NTP is a networking protocol to synchronize clocks between computer systems over variable-latency, packetswitched data networks.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Nozomi Networks Query Language (N2QL)

N2QL is the language used in queries in Nozomi Networks software.

Open Virtual Appliance

An OVA file is an open virtualization format (OVF) directory that is saved as an archive using the .tar archiving format. It contains files for distribution of software that runs on a virtual machine. An OVA package contains a .ovf descriptor file, certificate files, an optional .mf file along with other related files.

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/ or monitors industrial assets, devices and processes.

Packet Capture

A pcap is an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Packet Capture Next Generation

A pcapNg is the latest version of a pcap file, an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Portable Document Format

PDF is a Adobe file format that is used to present documents. It is independent of operating systems (OS), application software, hardware.

Portable Network Graphics

PNG is a raster graphics file format that supports lossless data compression.PNG was developed as an improved, non-patented replacement for graphics interchange format (GIF).

Privacy-Enhanced Mail

PEM is a standard file format that is used to store and send cryptographic keys, certificates, and other data. It is based on a set of 1993 IETF standards.

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

Protected Extensible Authentication Protocol

PEAP is a protocol that encloses the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.

Random-access Memory

Computer memory that can be read and changed in any order. It is typically used to store machine code or working data.

Representational State Transfer

Representational State Transfer (REST) is an architectural style for designing networked applications. It uses stateless, client-server communication via standard HTTP methods (GET, POST, PUT, DELETE) to access and manipulate web resources represented in formats like JSON or XML.

Secure Copy Protocol

SCP is a protocol for the secure transfer of computer files between a local host and a remote host, or between two remote hosts. It is based on the secure shell (SSH) protocol.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

Secure Sockets Layer

A secure sockets layer ensures secure communication between a client computer and a server.

Security Assertion Markup Language

SAML is an open standard, XML-based markup language for security assertions. It allows for the exchange of authentication and authorization data different parties such as a service provider and an identity provider.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Server Message Block

Is a communication protocol which provides shared access to files and printers across nodes on a network of systems. It also provides an authenticated interprocess communication (IPC) mechanism. SFTP was proposed as an unsecured file transfer protocol with a level of complexity intermediate between TFTP and FTP. It was never widely accepted on the internet.

Simple Mail Transfer Protocol

SMTP is an internet standard communication protocol that is used for the transmission of email. Mail servers and other message transfer agents use SMTP to send and receive mail messages.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

Simple Text Oriented Messaging Protocol

STOMP is a simple textbased protocol, for working with message-oriented middleware (MOM). It provides an interoperable wire format that allows STOMP clients to talk with any message broker supporting the protocol.

Structured Threat Information Expression

STIX[™] is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Supervisory control and data acquisition

SCADA is a control system architecture which has computers, networked data communications and graphical user interfaces for high-level supervision of processes and machines. It also covers sensors and other devices, such as programmable logic controllers (PLC), which interface with process plant or machinery.

Text-based User Interface

In computing, a textbased (or terminal) user interfaces (TUI) is a retronym that describes a type of user interface (UI). These were common as an early method of human-computer interaction, before the more modern graphical user interfaces (GUIs) were introduced. Similar to GUIs, they might use the entire screen area and accept mouse and other inputs.

Threat Intelligence™

Nozomi Networks **Threat** Intelligence[™] feature monitors ongoing OT and IoT threat and vulnerability intelligence to improve malware anomaly detection. This includes managing packet rules, Yara rules, STIX indicators, Sigma rules, and vulnerabilities. **Threat** Intelligence[™] allows new content to be added, edited, and deleted, and existing content to be enabled or disabled.

Transmission Control Protocol

One of the main protocols of the Internet protocol suite.

Transport Layer Security

TLS is a cryptographic protocol that provides communications security over a computer network. The protocol is widely used in applications such as: HTTPS, voice over IP, instant messaging, and email.

Uniform Resource Identifier

A URI is a unique string of characters used to identify a logical or physical resource on the internet or local network.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Uninterruptible Power Supply

A UPS is an electric power system that provides continuous power. When the main input power source fails, an automated backup system continues to supply power.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

Universal Plug and Play

UPnP is a network protocol that enables devices to automatically discover and communicate with each other using broadcast messages. While it facilitates easy device identification and connectivity, UPnP lacks robust authentication, making it vulnerable to unauthorized access in cybersecurity contexts.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

User Datagram Protocol

UDP is a lightweight, connectionless communication protocol used for fast, time-sensitive data transmission, such as video streaming, online gaming, and VoIP. UDP prioritizes speed and low latency over guaranteed delivery or error correction.

User Interface

An interface that lets humans interact with machines.

Variable

In the context of control systems, a variable can refer to process values that change over time. These can be temperature, speed, pressure etc.

Virtual DOM

A virtual DOM, or vdom, is a lightweight JavaScript representation of the Document Object Model (DOM). It is used in declarative web frameworks such as Elm, React, and Vue.js. It enables the updating of the virtual DOM is comparatively faster than updating the actual DOM.

Virtual Hard Disk

VHD is a file format that represents a virtual hard disk drive (HDD). They can contain what is found on a physical HDD, such as disk partitions and a file system, which in turn can contain files and folders. They are normally used as the hard disk of a virtual machine (VM). They are the native file format for Microsoft's hypervisor (virtual machine system), Hyper-V.

Virtual Local Area Network

A VLAN is a broadcast domain that is isolated and partitioned in a computer network at the data link layer (OSI layer 2).

Virtual Machine

A VM is the emulation or virtualization of a computer system. VMs are based on computer architectures and provide the functionality of a physical computer.

ZIP

An archive file format that supports lossless data compression. The format can use a number of different compression algorithms, but DEFLATE is the most common one. A ZIP file can contain one or more compressed files or directories.