Vantage

Administrator Guide

2025-07-03

Legal notices

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

Copyright

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

Vantage overview

Vantage™ *is a Software as a Service (SaaS) product that lets you monitor and protect your networks from anywhere in the world. Vantage lets you respond faster and more effectively to cyber threats, to ensure your operational resilience.*

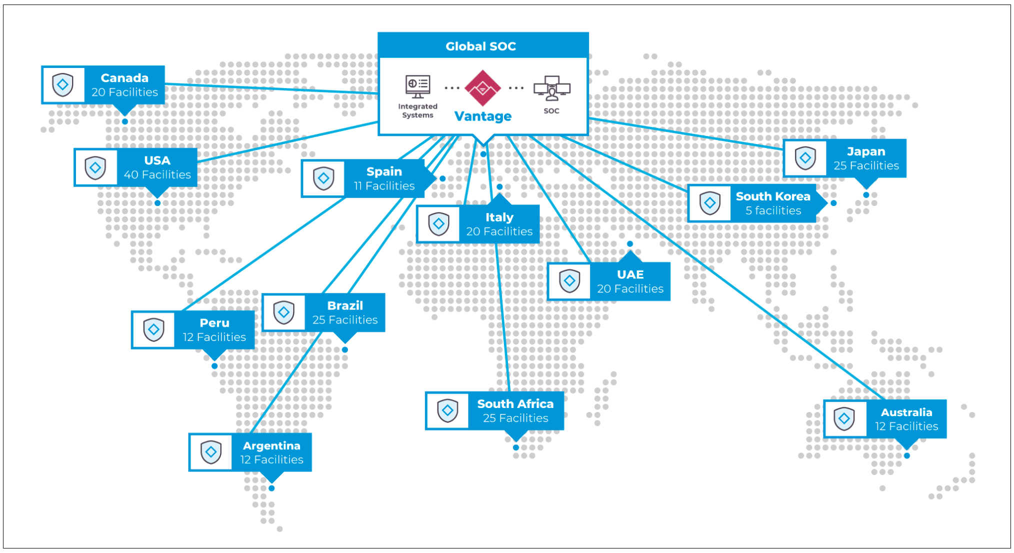


Figure 1. Vantage overview

General

Vantage uses the power and simplicity of *Software as a Service (SaaS)* to deliver unmatched security and visibility across your *operational technology (OT)*, *Internet of Things (IoT)*, and *information technology (IT)* networks.

Vantage lets you:

- Centrally manage all sensor deployments from a single application from anywhere in the world
- Monitor an unlimited number of devices
- Protect an unlimited number of locations

Identify

Vantage lets you discover and identify your assets and visualize your networks. Its ability to automate processes to create asset inventories eliminates blind spots and increases awareness of your networks.

Dashboards let you generate macro views, as well as see detailed information on assets and connections in your networks. Vantage also shows extensive node information such as names, types, and firmware versions as well as asset behavior, roles, protocols, and data flows.

Assess

Vantage shows security alerts, missing patches and vulnerabilities to let you automatically assess vulnerabilities and monitor risks. It also correlates known vulnerabilities to *Common Vulnerabilities and Exposures (CVE)* reports to quickly research the root cause and potential impact. Vulnerability dashboards let you prioritize your efforts to focus on high-impact risk reductions first.

Vantage continuously monitors all supported protocols for the *OT*, *IoT*, and *IT* industries. It summarizes *OT* and *IT* risk information and highlights indicators of reliability issues, such as unusual process values.

Detect

Vantage gives you constantly updated threat detection to identify cybersecurity and process-reliability threats. It detects early and late stage advanced threats and cyber risks.

Vantage combines behavior-based anomaly detection with signature-based threat detection for comprehensive risk monitoring.

An optional subscription to **Threat Intelligence™** gives you up-to-date threat detection and vulnerability identification, which uses indicators that have been created and curated by Nozomi Networks Labs.

In addition, an optional subscription to **Asset Intelligence™** gives you breakthrough anomaly-detection accuracy for *OT* and *IoT* devices, which accelerates incident response times.

Act

Vantage accelerates your global incident response capabilities. It does this by focusing your attention on critical vulnerabilities, and letting you prioritize activities that maximize risk reduction.

Pre-defined playbooks guide users, and specific teams, in their efforts to counter the different types of threats. A centralized dashboard consolidates data to create high-priority alerts across a global network.

Clear explanations describe what has happened, the possible cause, and suggested solutions for every alert, which reduces the need for additional investigation.

Vantage lets you group alerts into incidents. This gives security and operations staff a simple, clear, and consolidated view of what's happening in your networks.

Scale

Vantage aggregates data from an unlimited number of globally-deployed sensors. It delivers customizable summaries of essential information which lets you drill down to individual sites or assets.

It streamlines security processes across *IT* and *OT* for a cohesive response. It includes built-in integrations for asset, ticket and identity management systems, as well as for *security information and event management (SIEM)*.

Vantage lets you manage security risks centrally for all your global sites.

Architecture

You can use Vantage, and the flexible architecture and integrations with other systems, to create a customized solution.

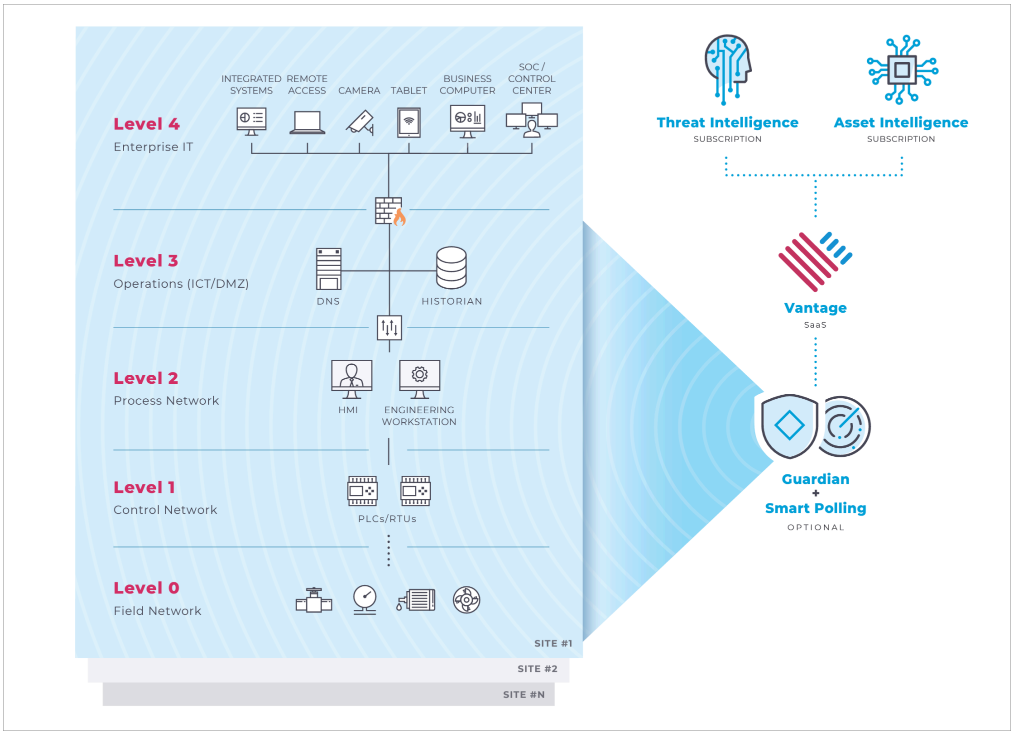


Figure 2. Vantage architecture

Data security in Vantage

It is important to understand how Vantage keeps your data secure.

Data privacy

For more details, see Nozomi Networks Vantage Data Privacy.

Data segregation and encryption

Data segregation is a key element of data security in Vantage. Every Vantage implementation has its own database. Access to an instance's database requires an encryption key that is only used for this instance.

FIPS support

The *National Institute of Standards and Technology (NIST)* develops *Federal Information Processing Standards (FIPS)*, which are publicly-announced standards for use in computer systems in-use with non-military United States government agencies and government contractors. The *FIPS* 140 series specifies requirements for cryptography modules within a security system protecting sensitive, but unclassified, data.

For implementations that adhere to *FIPS*, Nozomi Networks provides *FIPS*-compliant Vantage instances that use the FIPS-140-2 approved cryptography module.

Implementations that are *FIPS*-compliant are entirely separate from other Vantage instances and sensors:

- A *FIPS*-compliant Vantage instance only accepts connections from *FIPS* sensors
- A non-*FIPS* Vantage instance accepts only connections from non-*FIPS* sensors

While a *FIPS*-compliant sensor cannot connect to a standard, non-*FIPS* Vantage instance, an unlicensed sensor can connect to a *FIPS*-compliant Vantage instance. This allows Vantage to assign a license and enable *FIPS* mode on the sensor. Vantage now manages the sensor's license, and it can only connect to a *FIPS*-compliant Vantage instance.

To learn more about *FIPS*, contact Nozomi Networks.

FIPS-compliant Vantage and SAML configuration

When you use *security assertion markup language (SAML)* to Configure Vantage for SSO (on page 148), you must specify its *assertion consumer service (ACS) uniform resource locator (URL)*.

When you use *SAML* to configure Vantage for SSO, you must specify its *ACS URL*.

If your Vantage instance is *FIPS*-compliant, its *ACS URL* differs from the *ACS URL* of non-*FIPS* instances. For example:

- The *ACS URL* of a standard, non-*FIPS* Vantage instance is similar to: `https://customer1.customers.us1.vantage.nozominetworks.io`
- The *ACS URL* of a *FIPS*-compliant Vantage instance is similar to: `https://nozominetworkscom.customers.us1.vantage-govcloud.nozominetworks.io`

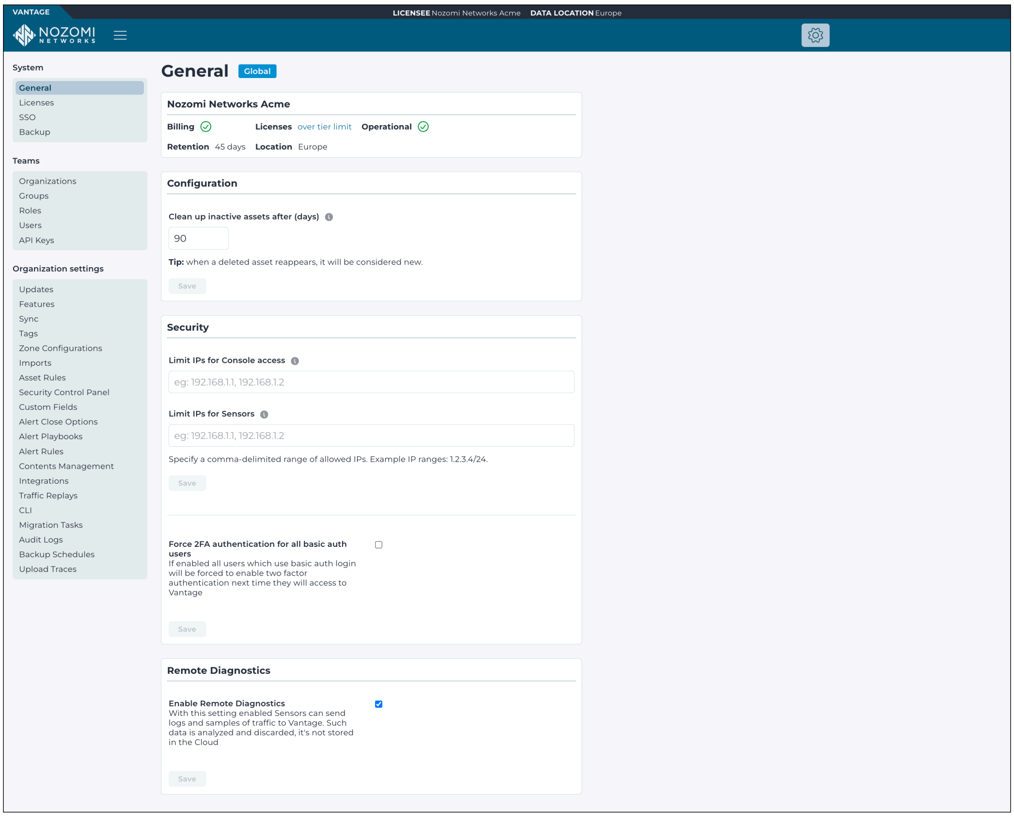
For more details about *ACS URL*s, see IdP configuration for SAML integration (on page 146).

For more details about *ACS URL*s, see **IdP configuration for SAML integration**, in the **Administrator Guide**.

Chapter 2. Administration

Administration page

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



LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

General

Nozomi Networks Acme

Billing ✓ **Licenses** over tier limit **Operational** ✓

Retention 45 days **Location** Europe

Configuration

Clean up inactive assets after (days): 90

Tip: when a deleted asset reappears, it will be considered new.

Security

Limit IPs for Console access: eg: 192.168.1.1, 192.168.1.2

Limit IPs for Sensors: eg: 192.168.1.1, 192.168.1.2

Specify a comma-delimited range of allowed IPs. Example IP ranges: 1.2.3.4/24.

Force 2FA authentication for all basic auth users □
If enabled all users which use basic auth login will be forced to enable two factor authentication next time they will access to Vantage

Remote Diagnostics

Enable Remote Diagnostics ☑
With this setting enabled Sensors can send logs and samples of traffic to Vantage. Such data is analyzed and discarded, it's not stored in the Cloud

Figure 3. Administration page

System

The **System** section has these pages:

- General (on page 17)
- Licenses (on page 19)
- SSO (on page 20)
- Backup (on page 25)

Teams

The **Teams** section has these pages:

- Organizations (on page 26)
- Groups (on page 28)
- Roles (on page 41)
- Users (on page 44)
- API Keys (on page 53)

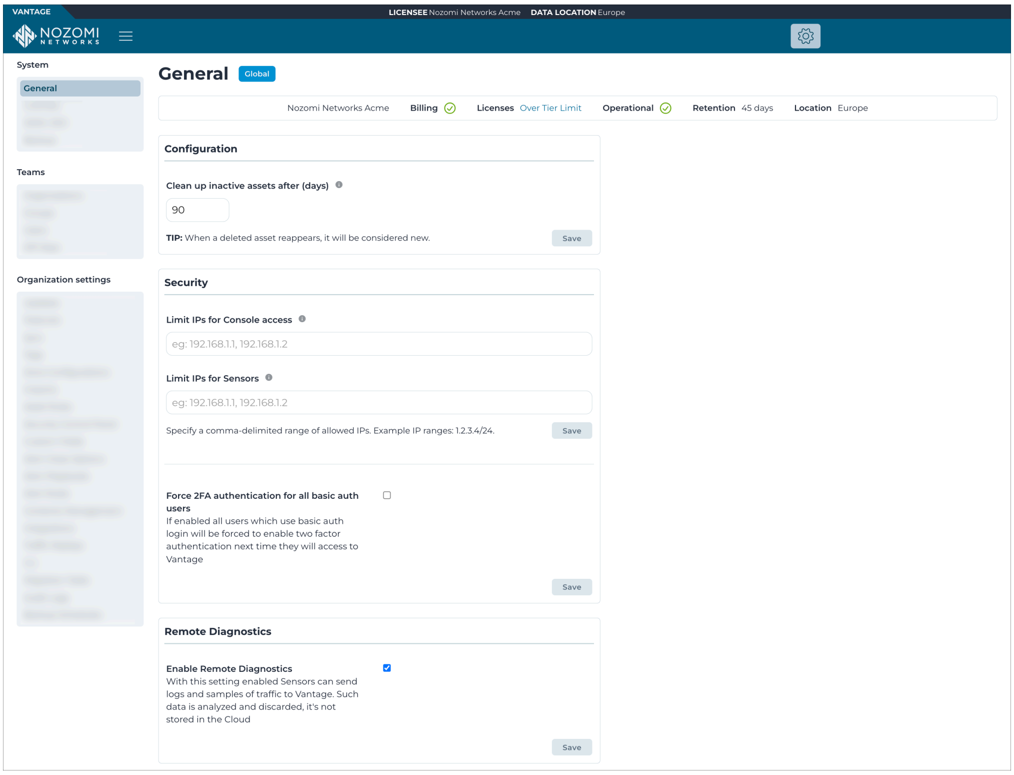
Organization settings

The **Organization settings** section has these pages:

System

General

*The **General** page shows a system summary of information for items such as, your company name, license status, billing information, and details about data storage.*



LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

General

General Global

Nozomi Networks Acme Billing ✓ Licenses Over Tier Limit Operational ✓ Retention 45 days Location Europe

Configuration

Clean up inactive assets after (days): 90

TIP: When a deleted asset reappears, it will be considered new. Save

Security

Limit IPs for Console access: eg: 192.168.1.1, 192.168.1.2

Limit IPs for Sensors: eg: 192.168.1.1, 192.168.1.2

Specify a comma-delimited range of allowed IPs. Example IP ranges: 1.2.3.4/24. Save

Force 2FA authentication for all basic auth users ☐
If enabled all users which use basic auth login will be forced to enable two factor authentication next time they will access to Vantage

Save

Remote Diagnostics

Enable Remote Diagnostics ☑
With this setting enabled Sensors can send logs and samples of traffic to Vantage. Such data is analyzed and discarded, it's not stored in the Cloud

Save

Figure 4. General page

Status

The status bar at the top of the pages shows information for:

- Billing
- Licenses
- Operational
- Retention
- Location

Configuration

The **Configuration** section lets you clean up inactive assets after a set number of days.

Security

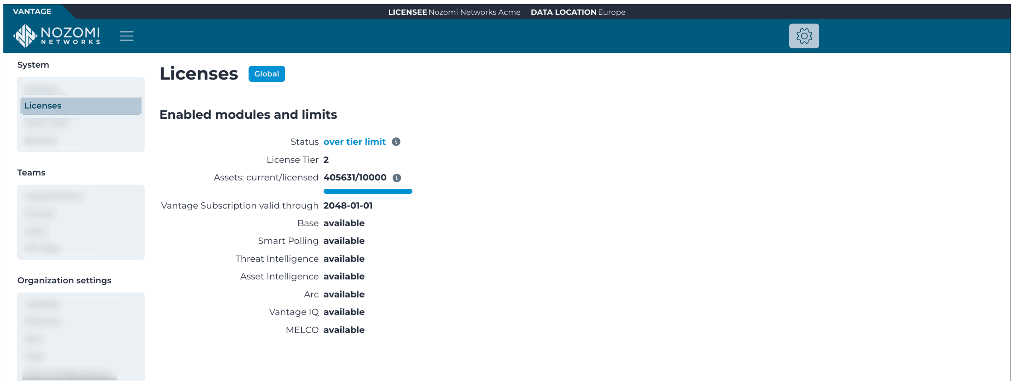
The **Security** sections lets you set a range of:

- Allowed *internet protocol (IP)* addresses that have console access
- Allowed sensors

For these settings, you must use comma-delimited entries, in *classless inter-domain routing (CIDR)* format.

Licenses

The ***Licenses*** *page shows more detailed information about your licenses, such as the modules that they enable and the limits they set.*



LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Licenses

Enabled modules and limits

Status	over tier limit
License Tier	2
Assets: current/licensed	405631/10000
Vantage Subscription valid through	2048-01-01
Base	available
Smart Polling	available
Threat Intelligence	available
Asset Intelligence	available
Arc	available
Vantage IQ	available
MELCO	available

Figure 5. Licenses page

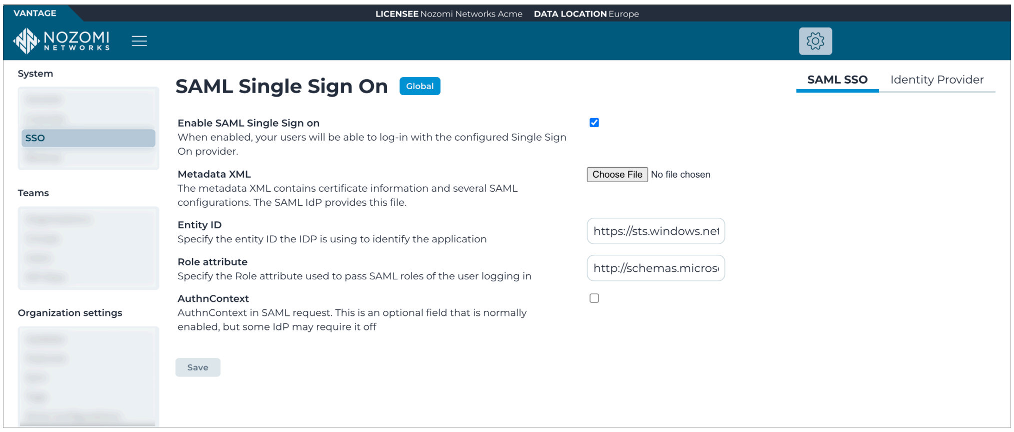
Enabled modules and limits

This section shows information for:

- Status
- License Tier
- Assets: current/licensed
- Base
- Smart Polling
- Threat Intelligence
- Asset Intelligence
- Arc
- Vantage IQ

SAML Single Sign On

*The **SAML Single Sign On** page lets you configure single sign-on (SSO) through security assertion markup language (SAML) integration.*



SAML Single Sign On

Enable SAML Single Sign on
When enabled, your users will be able to log-in with the configured Single Sign On provider. ☑

Metadata XML
The metadata XML contains certificate information and several SAML configurations. The SAML IdP provides this file. Choose File No file chosen

Entity ID
Specify the entity ID the IDP is using to identify the application https://sts.windows.net

Role attribute
Specify the Role attribute used to pass SAML roles of the user logging in http://schemas.micros

AuthnContext
AuthnContext in SAML request. This is an optional field that is normally enabled, but some IdP may require it off □

Figure 6. SAML SSO page

The SSO page has these tabs:

- SAML SSO (on page 21)
- Identity Provider (on page 22)

Related information

SAML integration configuration (on page 145)

IdP configuration for SAML integration (on page 146)

Troubleshooting SAML integration (on page 150)

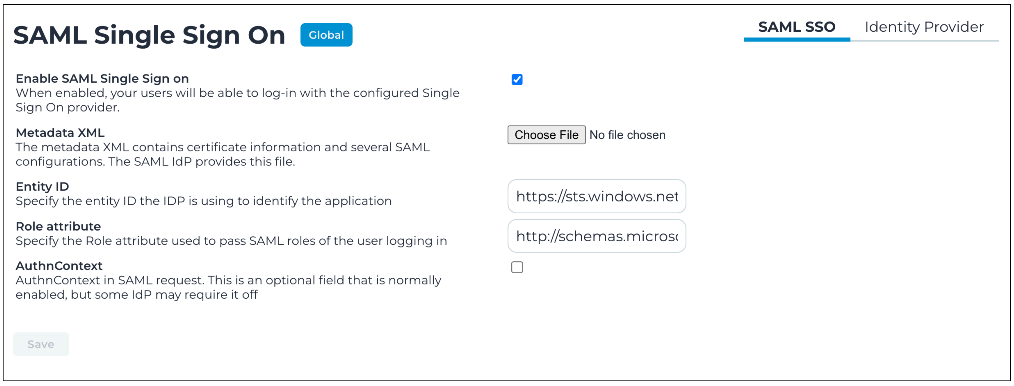
Configure your IdP for SAML integration (on page 147)

Configure Vantage for SSO (on page 148)

Configure a Google Workspace SAML application (on page 151)

SAML SSO

*The **SAML SSO** page lets you configure Single Sign-On (SSO) using Security Assertion Markup Language (SAML) integration and set up Vantage as an Identity Provider (IdP).*



SAML Single Sign On

Enable SAML Single Sign on
When enabled, your users will be able to log-in with the configured Single Sign On provider. ☑

Metadata XML
The metadata XML contains certificate information and several SAML configurations. The SAML IdP provides this file. Choose File No file chosen

Entity ID
Specify the entity ID the IDP is using to identify the application https://sts.windows.net

Role attribute
Specify the Role attribute used to pass SAML roles of the user logging in http://schemas.micros

AuthnContext
AuthnContext in SAML request. This is an optional field that is normally enabled, but some IdP may require it off ☐

Figure 7. SAML SSO page

Enabled SAML Single Sign On

This checkbox lets you enable *SAML single sign-on (SSO)*.

Metadata XML

This button lets you choose an *eXtensible Markup Language (XML)* file that you have downloaded from your *identity provider (IdP)*.

Entity ID

This field lets you enter the entity *identifier (ID)* that the *IdP* uses to identify the application.

Role attribute

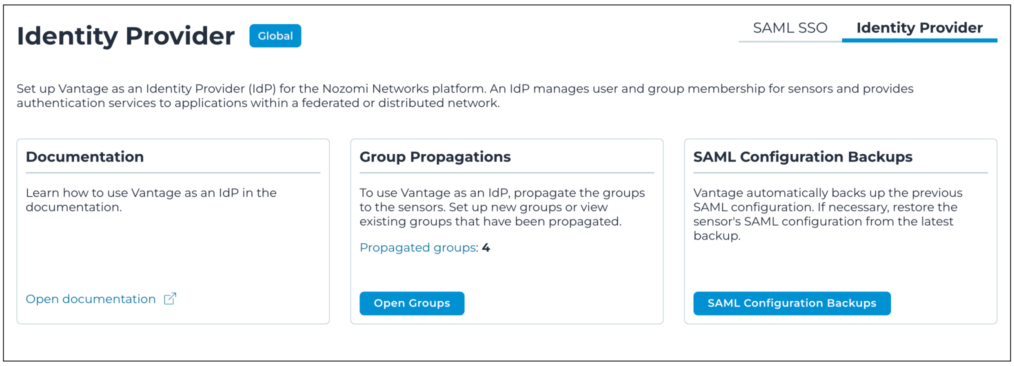
This field lets you enter the role attribute that is used to pass *SAML* roles for the user that is logging in.

AuthnContext

This checkbox is should normally be selected. However, for some *IdP* it might be required to deselect it.

Identity Provider

*The **Identity Provider** page lets you configure Vantage as an Identity Provider (IdP).*



Identity Provider Global

Set up Vantage as an Identity Provider (IdP) for the Nozomi Networks platform. An IdP manages user and group membership for sensors and provides authentication services to applications within a federated or distributed network.

Documentation

Learn how to use Vantage as an IdP in the documentation.

Open documentation

Group Propagations

To use Vantage as an IdP, propagate the groups to the sensors. Set up new groups or view existing groups that have been propagated.

Propagated groups: **4**

Open Groups

SAML Configuration Backups

Vantage automatically backs up the previous SAML configuration. If necessary, restore the sensor's SAML configuration from the latest backup.

SAML Configuration Backups

Figure 8. Identity Provider page

Documentation

This section has a link to the Technical Documentation.

Group Propagations

This section lets you open the **Groups** section so that you can propagate the groups to the applicable sensors, or view the propagation settings.

SAML Configuration Backups

This section lets you select **SAML Configuration Backups** to do a restore from the latest backup. For more details, see Restore a SAML configuration backup (on page 23).

Restore a SAML configuration backup

Learn how to restore a backup of your SAML configuration to revert to a previous setup.

About this task

When you propagate a group to a set of sensors, the system automatically attempts to save a backup of the current SAML sensor configuration. The backup will have these settings:

- `Nozomi URL`
- `Role attribute`
- `Metadata XML`

As long as each of the above values are not empty, the backup will be successful.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **SSO**.

   Result: The **SAML Single Sign On** page opens.

3. In the top right section, select **Identity Provider**.

   Result: The **Identity Provider** page opens.

4. In the **SAML Configuration Backups** section, select **SAML Configuration Backups**.

   Result: The **SAML Configuration Backups** page opens.

5. Choose a method to select one, or more, items.

   Choose from:

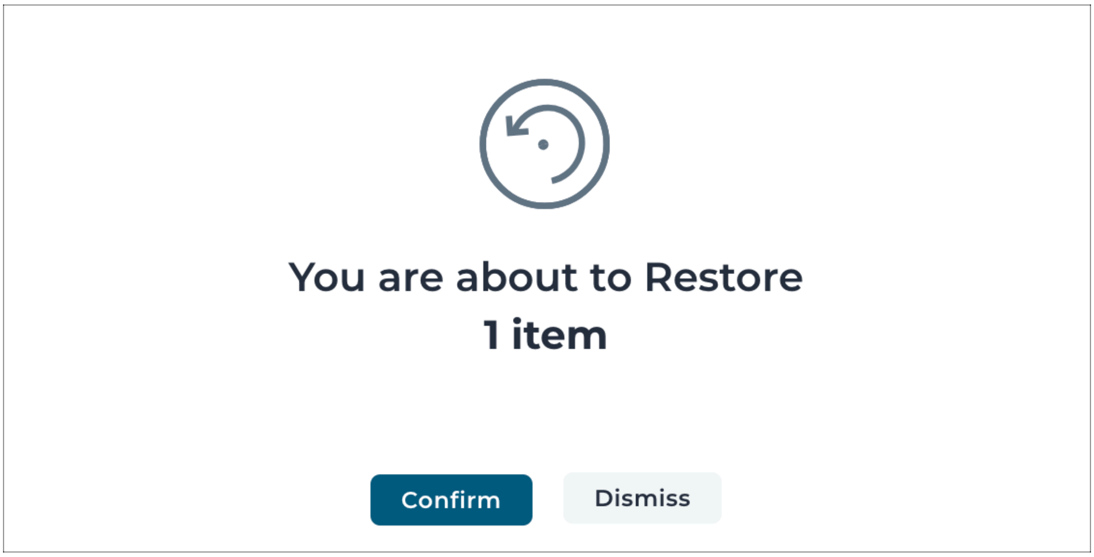
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

6. Select **Restore**.

> **Note:**
> When you try to restore more than one backup for a sensor, only the latest one will be restored.

Result: A dialog shows.

7. To restore the backup, select **Confirm**.



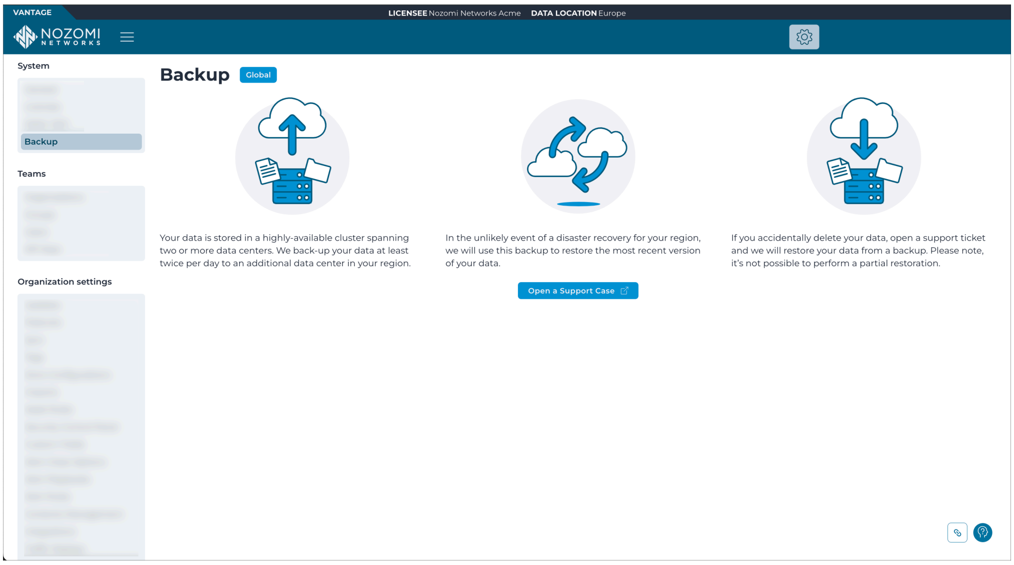
You are about to Restore
1 item

Results

The backup(s) has (have) been restored.

Backup

*The **Backup** page lets you review information about backup procedures. It also lets you open a support case.*



Your data is stored in a highly-available cluster spanning two or more data centers. We back-up your data at least twice per day to an additional data center in your region.

In the unlikely event of a disaster recovery for your region, we will use this backup to restore the most recent version of your data.

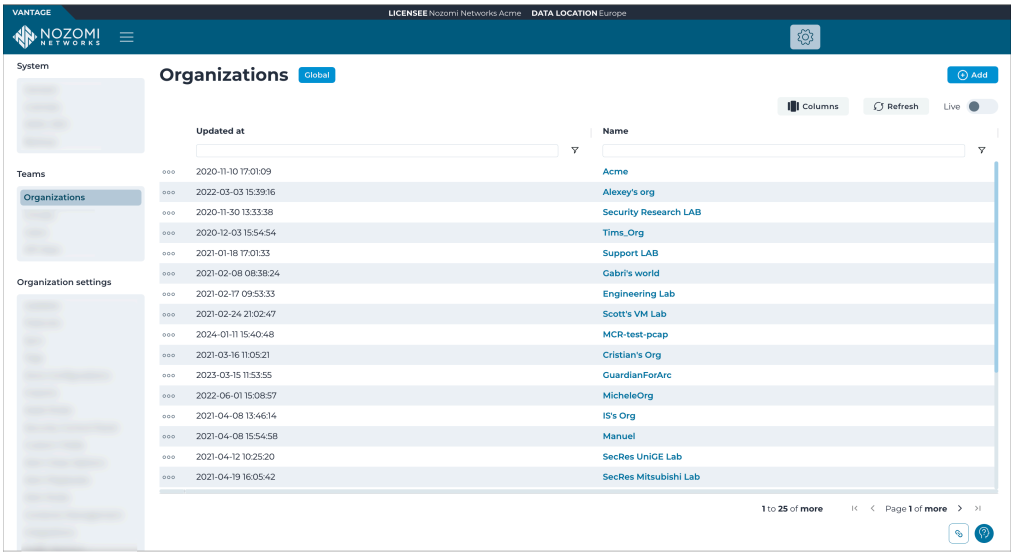
If you accidentally delete your data, open a support ticket and we will restore your data from a backup. Please note, it's not possible to perform a partial restoration.

Figure 9. Backup page

Teams

Organizations

*The **Organizations** page shows your organizations, which are logical subdivisions within your Vantage account.*



VANTAGE LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Organizations

Updated at	Name
2020-11-10 17:01:09	Acme
2022-03-03 15:39:16	Alexey's org
2020-11-30 13:33:38	Security Research LAB
2020-12-03 15:54:54	Tims_Org
2021-01-18 17:01:33	Support LAB
2021-02-08 08:38:24	Gabri's world
2021-02-17 09:53:33	Engineering Lab
2021-02-24 21:02:47	Scott's VM Lab
2024-01-11 15:40:48	MCR-test-pcap
2021-03-16 11:05:21	Cristian's Org
2023-03-15 11:53:55	GuardianForArc
2022-06-01 15:08:57	MicheleOrg
2021-04-08 13:46:14	IS's Org
2021-04-08 15:54:58	Manuel
2021-04-12 10:25:20	SecRes UniGE Lab
2021-04-19 16:05:42	SecRes Mitsubishi Lab

1 to 25 of more Page 1 of more

Figure 10. Organizations page

Add

This button lets you add a new organization.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add an organization

You can use the actions menu to add an organization.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Teams** section, select **Organizations**.

   Result: The **Organizations** page opens.

3. Select **Add new**.
4. In the **Organization name** field, enter a name for your new organization.
5. Select **Create**.

Results

The organization has been added.

Delete an organization

You can use the actions menu to delete an organization.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Teams** section, select **Organizations**.

   Result: The **Organizations** page opens.

3. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

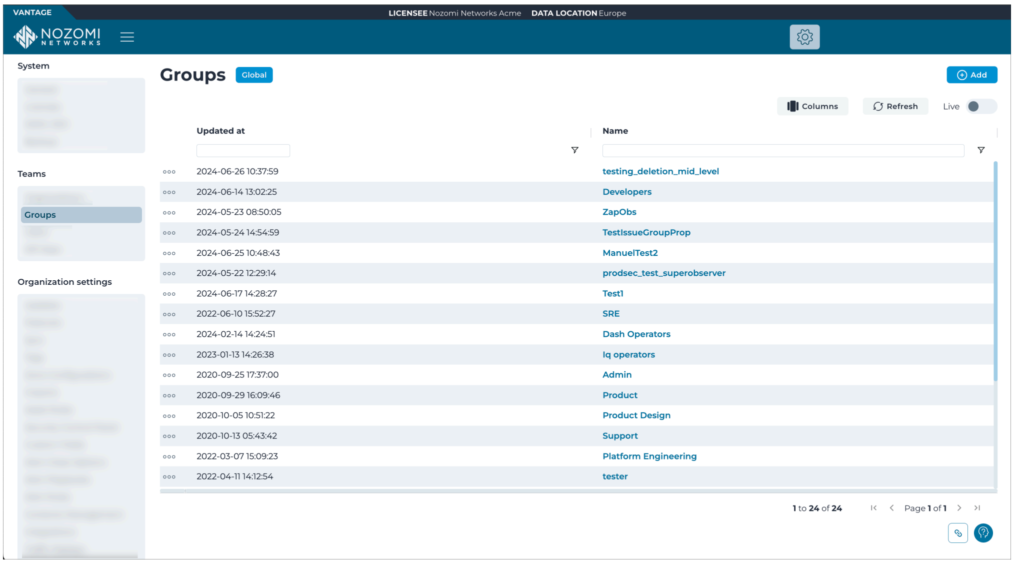
5. Select **Delete**.

Results

The organization has been deleted.

Groups

*The **Groups** page shows all the user groups in your organization, and lets you create and configure groups.*



	Updated at	Name
○○○	2024-06-26 10:37:59	testing_deletion_mid_level
○○○	2024-06-14 13:02:25	Developers
○○○	2024-05-23 08:50:05	ZapObs
○○○	2024-05-24 14:54:59	TestIssueGroupProp
○○○	2024-06-25 10:48:43	ManuelTest2
○○○	2024-05-22 12:29:14	prodsec_test_superobserver
○○○	2024-06-17 14:28:27	Test1
○○○	2022-06-10 15:52:27	SRE
○○○	2024-02-14 14:24:51	Dash Operators
○○○	2023-01-13 14:26:38	Iq operators
○○○	2020-09-25 17:37:00	Admin
○○○	2020-09-29 16:09:46	Product
○○○	2020-10-05 10:51:22	Product Design
○○○	2020-10-13 05:43:42	Support
○○○	2022-03-07 15:09:23	Platform Engineering
○○○	2022-04-11 14:12:54	tester

1 to 24 of 24 Page 1 of 1

Figure 11. Groups page

Group membership

The access that Vantage grants to a user depends on the group that the user is a member of.

Your *IdP* normally manages group membership. When a user logs in to Vantage, the group membership details are read from the *IdP*, and the user is updated in Vantage. The user will be added to, or removed from, groups as necessary. When changes to group membership are made in your *IdP*, they will be applied the next time the user logs in to Vantage.

A *SAML* user must belong to a group that is defined in both Vantage, and the *IdP*. If this is not the case, the user will be denied access in Vantage. Groups are not synchronized between Vantage and your *IdP*. This can result in situations where groups in your *IdP* do not exist in Vantage, or groups in Vantage do not exist in your *IdP*. If a *SAML* user definition changes in the *IdP*, and none of its *SAML* groups now exist in Vantage, access will be denied.

Role assignments

The role assignments of a group determine the access granted to its users. This controls both access rights, and the scope where they apply.

Predefined roles set the combination of rights that the users of the group are granted. For example, the role of **Admin** has complete access, whereas, the role of **Assets Operator** has a much more limited set of permissions.

You can also select an organization in order to define access. If no organization is specified, the permissions for the role assignment will apply to your entire Vantage instance.

You can also further limit scope to a specific tag, or site, that has been defined in the organization. For more details, see Role assignment scope (on page 29).

Nozomi Networks recommends that you assign the most restrictive permissions that still allow your users to perform their tasks. Combine roles that apply to differing tags, sites, and organizations to create an access control policy that protects your Vantage instance, but does not hinder your users.

> **Note:**
> You should try to create the simplest, highest-level, most restrictive, access control policy that still permits your users to protect your assets.

Role assignment scope

If you do not specify an organization when you create a role assignment, access is granted for all objects in Vantage. For example, you could create an **Alerts Operator** role that grants access to all alerts in every organization.

To create a more granular access control policy, you can create multiple role assignments and restrict each one to a specific organization.

When you limit the scope of a role assignment to a specific organization, you can further limit the scope to an individual site, or tag, within that organization.

By defining different role assignments for various combinations of organization, tag, and site, you can create an access control policy that correctly grants, and denies, access to each Vantage user.

When you create multiple role assignments for a group, their scopes can overlap. For example, you can create two role assignments for a single organization, tag, or site. This might seem to be a permissions conflict, but in Vantage, granted permissions are cumulative. When multiple roles apply, the most lenient permission is granted.

If you were to assign to a group the role of both:

- **Alerts Operator**: *Grants* all access to alerts
- **Assets Operator**: *Denies* all access to alerts

In this scenario, the user will be *granted* all access to alerts.

Add

This button lets you add a group.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Roles and permissions

A list of the default roles and permissions in Vantage.

Role	Permissions
Admin	Grants full access to create, read, update, and delete all Vantage objects.
Alerts Operator	Allows users to manage alerts. Create, read, update, and delete alerts. Read organizations and settings.
Assets Operator	Allows users to manage assets. Create, read, update, and delete assets. Read organizations and settings.
Observer	Allows users to review assets, alerts, and vulnerabilities . Read access on assets, alerts, vulnerabilities, comments, organizations, and settings.
Superobserver	Allows a user to review everything. Read-only access to all Vantage objects.
Vulnerabilities Operator	Allows users to manage vulnerabilities. Create, read, update, and delete vulnerabilities. Read assets, organizations, and settings.

Add a group

*The **Groups** page lets you add a new user group for your organization.*

Before you begin

You must be signed in with admin rights to do this procedure.

Procedure

1. Log into Vantage as an administrator.
2. In the top navigation bar, select ⚙

   Result: The administration page opens.
3. In the **Teams** section, select **Groups**.

   Result: The **Groups** page opens.
4. Select **Add new**.

   Result: The **User Groups** page shows.
5. In the **Group name** field, enter a name for the group.
6. In the **SAML name or ID** field, enter the name or *ID* of a group as defined in your *IdP*.

   > **Note:**
   > This name or *ID* maps the Vantage group to the appropriate group in the *IdP* that provides *SAML*-authentication services to Vantage.
7. Select **Create**.

   Result: The group has been created.
8. Assign a role to the group (on page 32).

Assign a role to a group

Once you have added a new group to Vantage, you need to assign a role, or roles, to the group.

Before you begin

You must be signed in with admin rights to do this procedure.

Procedure

1. Log into Vantage as an administrator.
2. In the top navigation bar, select ⚙

   Result: The administration page opens.
3. In the **Teams** section, select **Groups**.

   Result: The **Groups** page opens.
4. In the **Name** column of the applicable group, select the hyperlink.

   Result: The details page for the groups shows.
5. Select **Roles**.
6. Select **Add**.

   Result: Data entry fields show.
7. Select the **Roles** dropdown and select the role that you want to assign to the group.

   Result: A matrix shows.
8. **Optional:** Select the **Restrict to Organization (optional)** dropdown and select an organization.

   > **Note:**
   > This will specify an organization to which these permissions will be granted.

   Result: Two more data entry fields show.
9. **Optional:** Choose an option to further restrict the access that you will grant to this role assignment.

   Choose from:

   - Select the **Restrict to Tag (optional)** dropdown and select a tag
   - Select the **Restrict to Site (optional)** dropdown and select a site

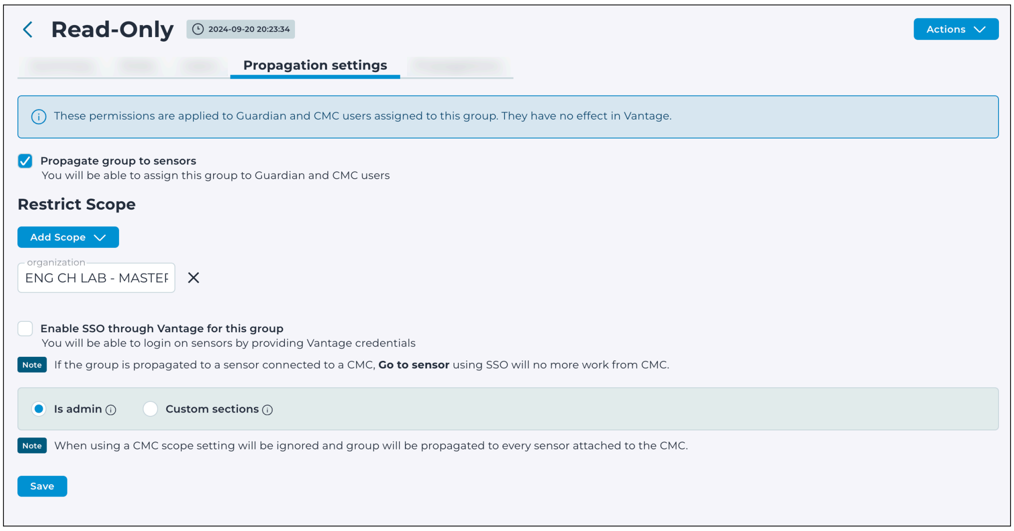
10. Select **Create**.
11. **Optional:** If this group should have additional permissions, select **Add New** and specify another role and scope of access.

Results

The role has been assigned.

Propagation settings

*The **Propagation settings** page allows you to propagate a group to sensors, configure remote group permissions, and define scope restrictions. You can also enable single sign-on (SSO) through Vantage, allowing users to authenticate using their Vantage credentials. If SSO is disabled, the group functions as a local group on the sensors.*



These permissions are applied to Guardian and CMC users assigned to this group. They have no effect in Vantage.

☑ Propagate group to sensors
You will be able to assign this group to Guardian and CMC users

Restrict Scope

organization: ENG CH LAB - MASTEF ×

□ Enable SSO through Vantage for this group
You will be able to login on sensors by providing Vantage credentials

Note If the group is propagated to a sensor connected to a CMC, **Go to sensor** using SSO will no more work from CMC.

● Is admin ○ Custom sections

Note When using a CMC scope setting will be ignored and group will be propagated to every sensor attached to the CMC.

Figure 12. Propagation settings - Is admin

Enable SSO through Vantage for this group

This checkbox lets you enable *SSO* and activates the configuration options in the sections below.

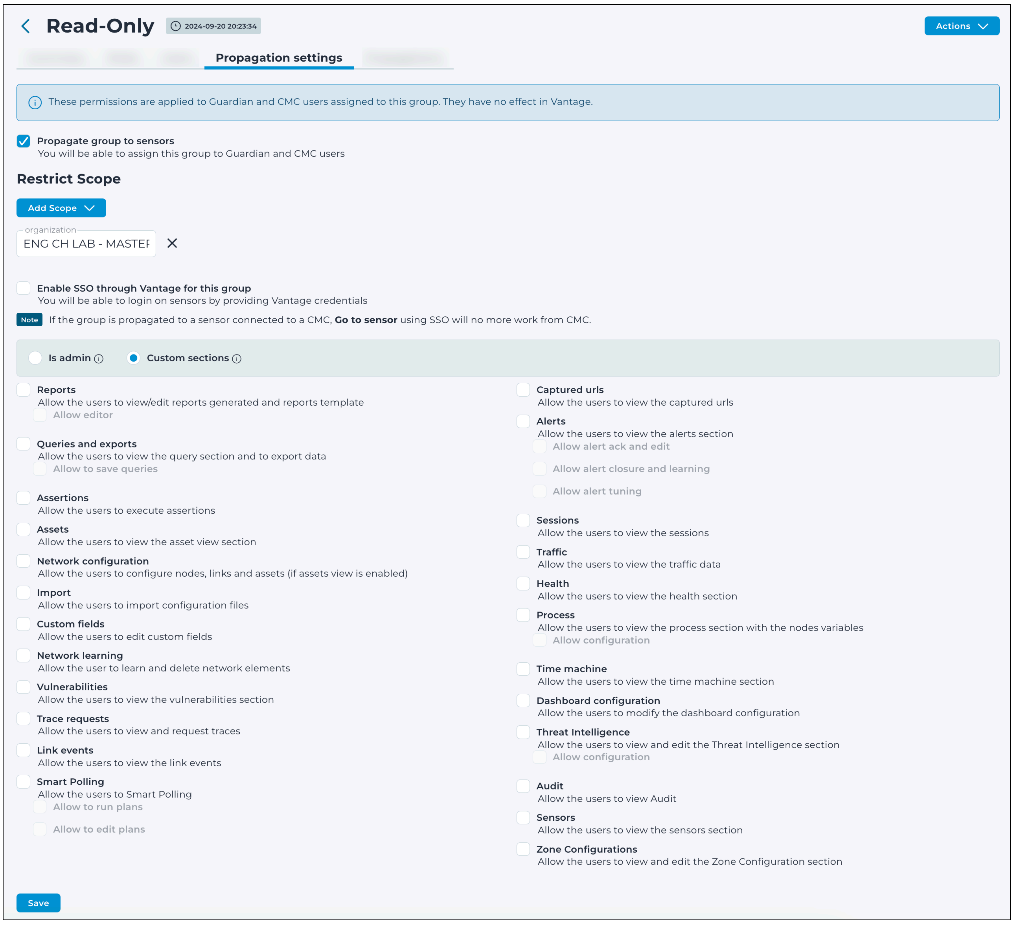
Remote group permissions

Is admin

This gives full administrator privileges to the users that are logged into the related sensors.

Note:
When using a *Central Management Console (CMC)*, the scope setting will be ignored, and the group **settings** will be propagated to every sensor that is attached to the *CMC*.

Custom sections



These permissions are applied to Guardian and CMC users assigned to this group. They have no effect in Vantage.

☑ Propagate group to sensors
You will be able to assign this group to Guardian and CMC users

Restrict Scope

organization: ENG CH LAB - MASTEF

□ Enable SSO through Vantage for this group
You will be able to login on sensors by providing Vantage credentials

Note If the group is propagated to a sensor connected to a CMC, **Go to sensor** using SSO will no more work from CMC.

○ Is admin ● Custom sections

□ Reports
Allow the users to view/edit reports generated and reports template
□ Allow editor

□ Queries and exports
Allow the users to view the query section and to export data
□ Allow to save queries

□ 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

□ Custom fields
Allow the users to edit custom fields

□ Network learning
Allow the user to learn and delete network elements

□ Vulnerabilities
Allow the users to view the vulnerabilities section

□ Trace requests
Allow the users to view and request traces

□ Link events
Allow the users to view the link events

□ Smart Polling
Allow the users to Smart Polling
□ Allow to run plans
□ Allow to edit plans

□ Captured urls
Allow the users to view the captured urls

□ Alerts
Allow the users to view the alerts section
□ Allow alert ack and edit
□ Allow alert closure and learning
□ Allow alert tuning

□ Sessions
Allow the users to view the sessions

□ Traffic
Allow the users to view the traffic data

□ Health
Allow the users to view the health section

□ Process
Allow the users to view the process section with the nodes variables
□ Allow configuration

□ Time machine
Allow the users to view the time machine section

□ Dashboard configuration
Allow the users to modify the dashboard configuration

□ Threat Intelligence
Allow the users to view and edit the Threat Intelligence section
□ Allow configuration

□ Audit
Allow the users to view Audit

□ Sensors
Allow the users to view the sensors section

□ Zone Configurations
Allow the users to view and edit the Zone Configuration section

Figure 13. Propagation settings - Custom sections

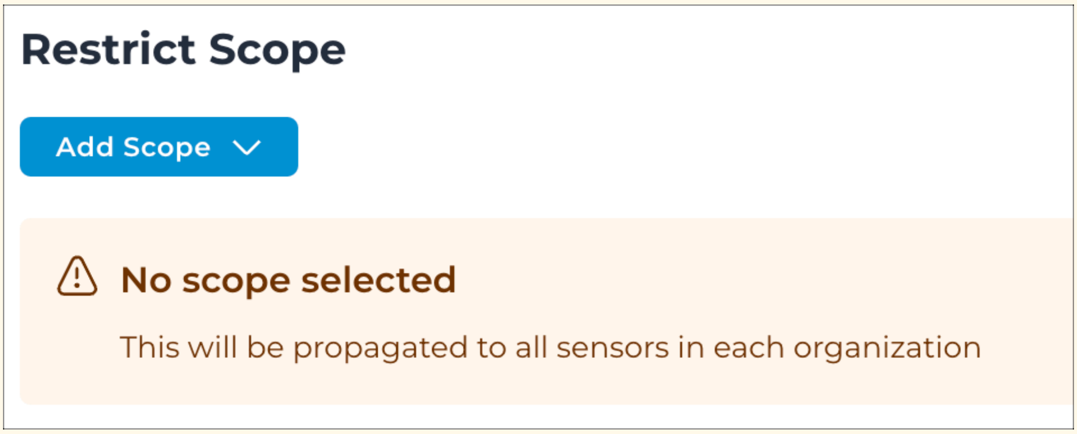
Restrict Scope

The **Add Scope** dropdown has these options:

- Organization
- Tag
- Site
- Sensor

The default setting is for the scope to be set to the current organization.

CAUTION:
If you remove the default setting, so that no scope is selected, the settings will be propagated to **every** sensor in **every** organization.



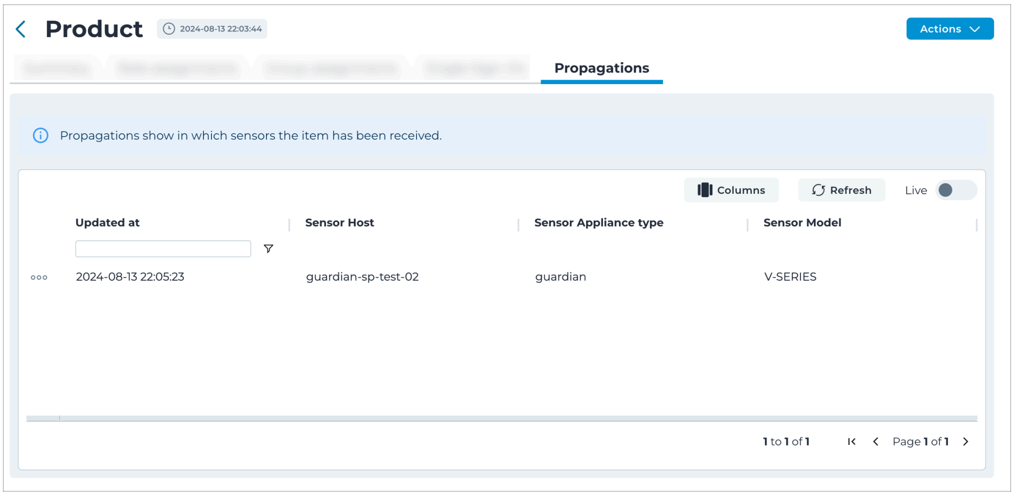
Restrict Scope

No scope selected

This will be propagated to all sensors in each organization

Propagations

*The **Propagations** page shows which sensors the groups have been propagated to.*



Propagations show in which sensors the item has been received.

Updated at	Sensor Host	Sensor Appliance type	Sensor Model
2024-08-13 22:05:23	guardian-sp-test-02	guardian	V-SERIES

1 to 1 of 1 Page 1 of 1

Figure 14. Propagations page

Limitations

- If the group is propagated to a sensor that is connected to a *CMC*, **Go to sensor** using *SSO* will no longer work from the *CMC*.
- You must manually delete groups from sensors when propagation is disabled, or when the sensor is no longer in scope (versions before 24.2.0.)
- The *SAML* logout protocol is not supported.

Use Vantage as the IdP for a group

Learn how you can use Security Assertion Markup Language (SAML) and Vantage as Identity Provider (IdP) to authenticate your sensors.

To enable your sensors to be able to use Vantage to log in, you need to propagate the groups to all those sensors for which you want to enable *SSO*. The correct *SAML* configuration will be also be propagated to the sensors.

Metadata XML

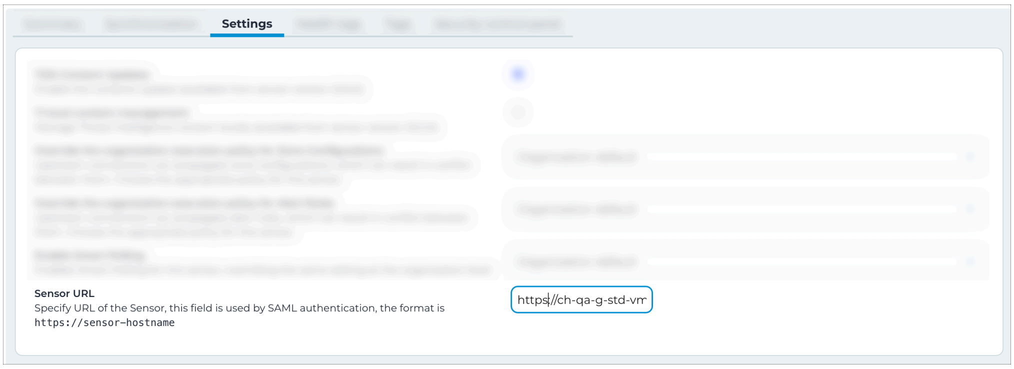
Each sensor has its own *SAML* metadata file, which is located at `<VANTAGE_URL>/api/v1/idp/<SENSOR_ID>/saml/metadata`

> **Note:**
> Only **admin** users can access the *SAML* metadata resource.

Sensor URL

The **Sensor URL** is a sensor setting which represents the *URL* of the sensor that the browser accesses. It is used for the *SAML* response callback.

To edit the **Sensor URL**, open the details page for the applicable sensor and go to **Settings > Sensor URL**.



Sensor URL
Specify URL of the Sensor, this field is used by SAML authentication, the format is `https://sensor-hostname`

https://ch-qa-g-std-vm

Figure 15. Sensor URL field

> **Note:**
> When a sensor is connected to Vantage, and a valid **Nozomi URL** has been previously set, it automatically sends its **Nozomi URL**. When **Sensor URL** is modified in Vantage, it will be propagated to the sensor, and will overwrite the existing **Nozomi URL**.

Use cases

Guardian(s) connected directly to Vantage, with no *CMC*s: No action is required.

Guardian(s) attached to a *CMC*, which is attached to Vantage:

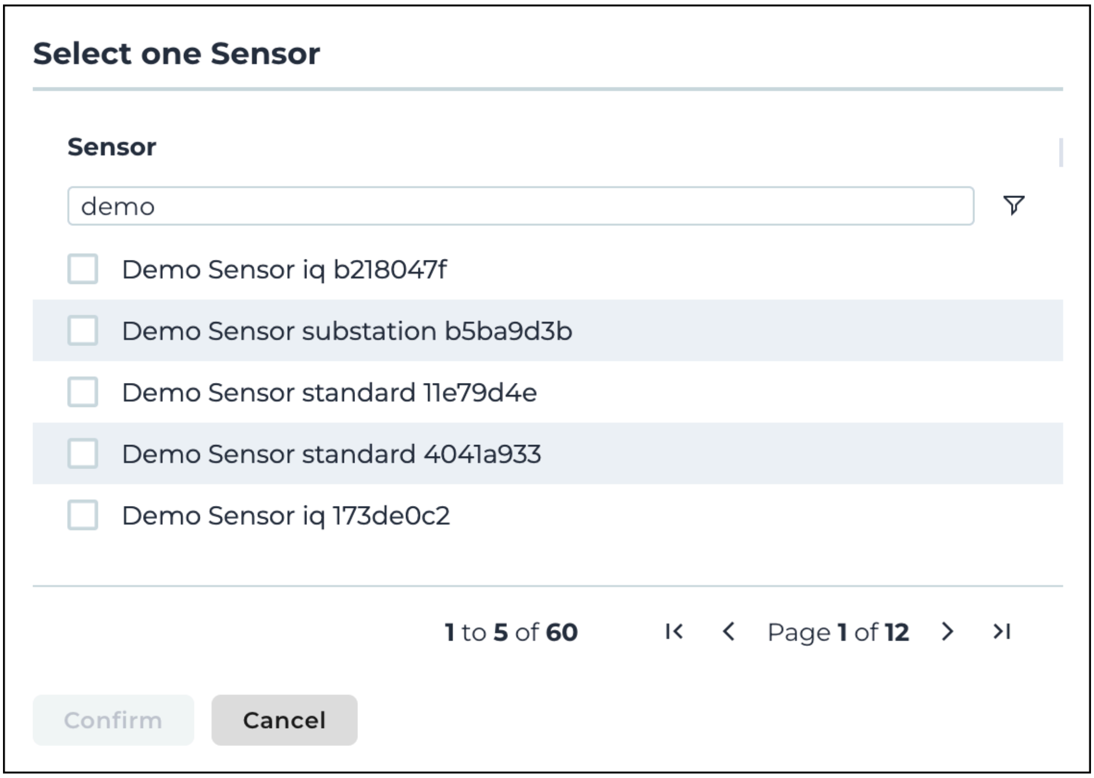
- If configuration is pushed on Guardians, the **Go to sensor** feature on the *CMC* using *SSO* will not work. (The **Go to sensor** feature on the *CMC* with local user will continue to work.) It is recommended that you:
    - Only push groups to the *CMC* that is directly attached to Vantage
    - Continue to manage the *SSO* to the Guardian from this *CMC*
- If **Go to sensor** feature on the *CMC* using *SSO* is not used, no action is required.

Connect a Guardian sensor with Vantage as IdP (example)

This example shows you how to connect a Guardian sensor to Vantage and assign users to a group named ***Admin****. This will lets the users to use Security Assertion Markup Language (SAML) to log in to the sensor.*

Procedure

1. Configure the Guardian and connect it to Vantage.
2. Open the details page for the sensor.
3. Select **Settings**.
4. In the **Sensor URL** field, enter details such as: `https://guardian1`
5. Do the steps below to propagate a group: `<Link to Single Sign-On>`.
6. Select the **Admin** group.
7. Select **Enable SSO through Vantage for this group**.
8. Select **Is admin**.
9. In the **Restrict Scope** section, select **Add Scope**.
10. From the dropdown, select **Sensor**.



Select one Sensor

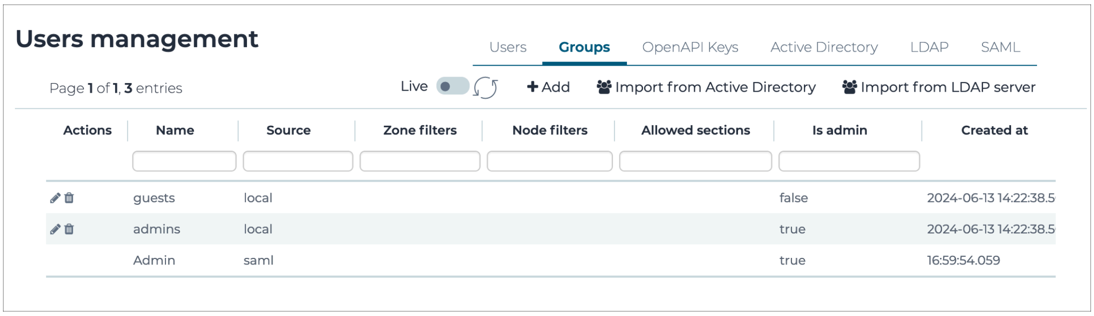
Sensor

demo

- □ Demo Sensor iq b218047f
- □ Demo Sensor substation b5ba9d3b
- □ Demo Sensor standard 11e79d4e
- □ Demo Sensor standard 4041a933
- □ Demo Sensor iq 173de0c2

11. Open the Guardian.
12. In the **username** field, enter the correct username.
13. In the **password** field, enter the correct password.
14. Go to **Settings > Users > Groups**.

15. Wait until you see the **Admin** group show.

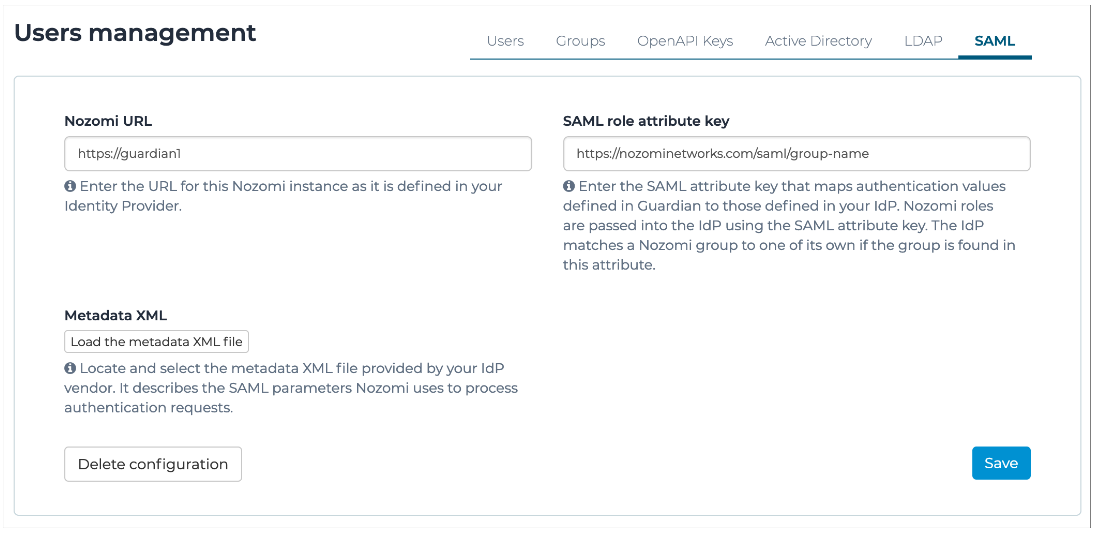


Users management

Page **1** of **1**, **3** entries

Actions	Name	Source	Zone filters	Node filters	Allowed sections	Is admin	Created at
✎ 🗑	guests	local				false	2024-06-13 14:22:38.5
✎ 🗑	admins	local				true	2024-06-13 14:22:38.5
	Admin	saml				true	16:59:54.059

16. To view the *SAML* configuration details, select **SAML**.



Users management

Nozomi URL

https://guardian1

Enter the URL for this Nozomi instance as it is defined in your Identity Provider.

SAML role attribute key

https://nozominetworks.com/saml/group-name

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.

Metadata XML

Load the metadata XML file

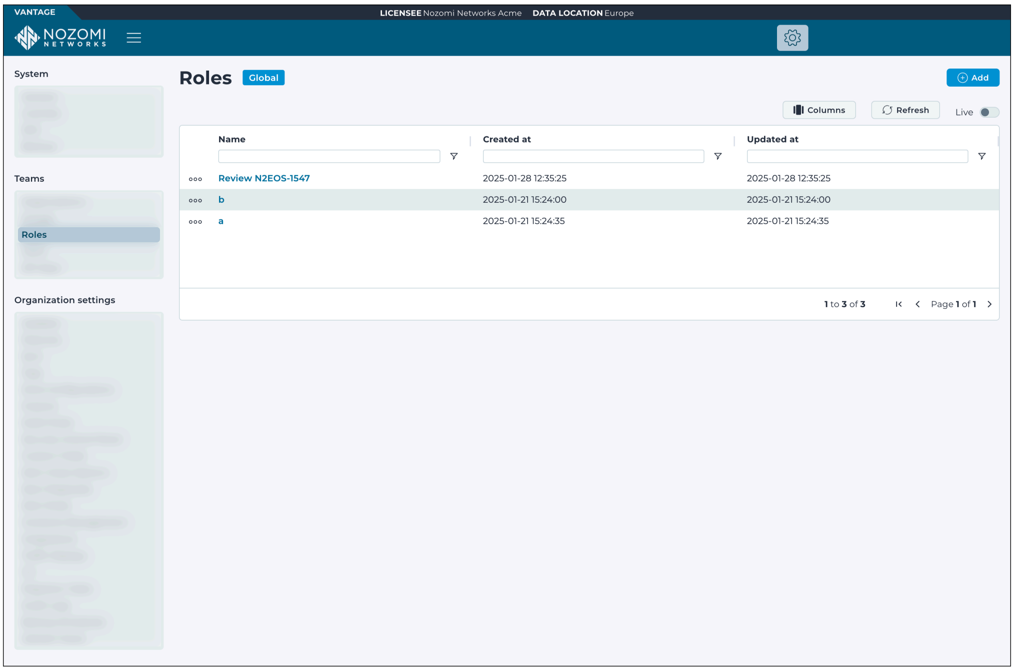
Locate and select the metadata XML file provided by your IdP vendor. It describes the SAML parameters Nozomi uses to process authentication requests.

17. Log out of the Guardian.
18. The *SSO* page shows.
19. Select **Single Sign On**.

    Result: You are logged into the Guardian with the credentials from Vantage.

Roles

*The **Roles** page shows all the assigned user roles in Vantage. It also lets you create new roles, and manage permissions and access levels efficiently.*



	Name	Created at	Updated at
ooo	Review N2EOS-1547	2025-01-28 12:35:25	2025-01-28 12:35:25
ooo	b	2025-01-21 15:24:00	2025-01-21 15:24:00
ooo	a	2025-01-21 15:24:35	2025-01-21 15:24:35

1 to 3 of 3 Page 1 of 1

Figure 16. Roles page

You can assign roles that show in the list to a group. For more details, see Assign a role to a group (on page 32).

Add

This button lets you add a new role (on page 42).

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add a role

*Use the **Add** button to create and configure a new role and assign permissions and settings.*

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

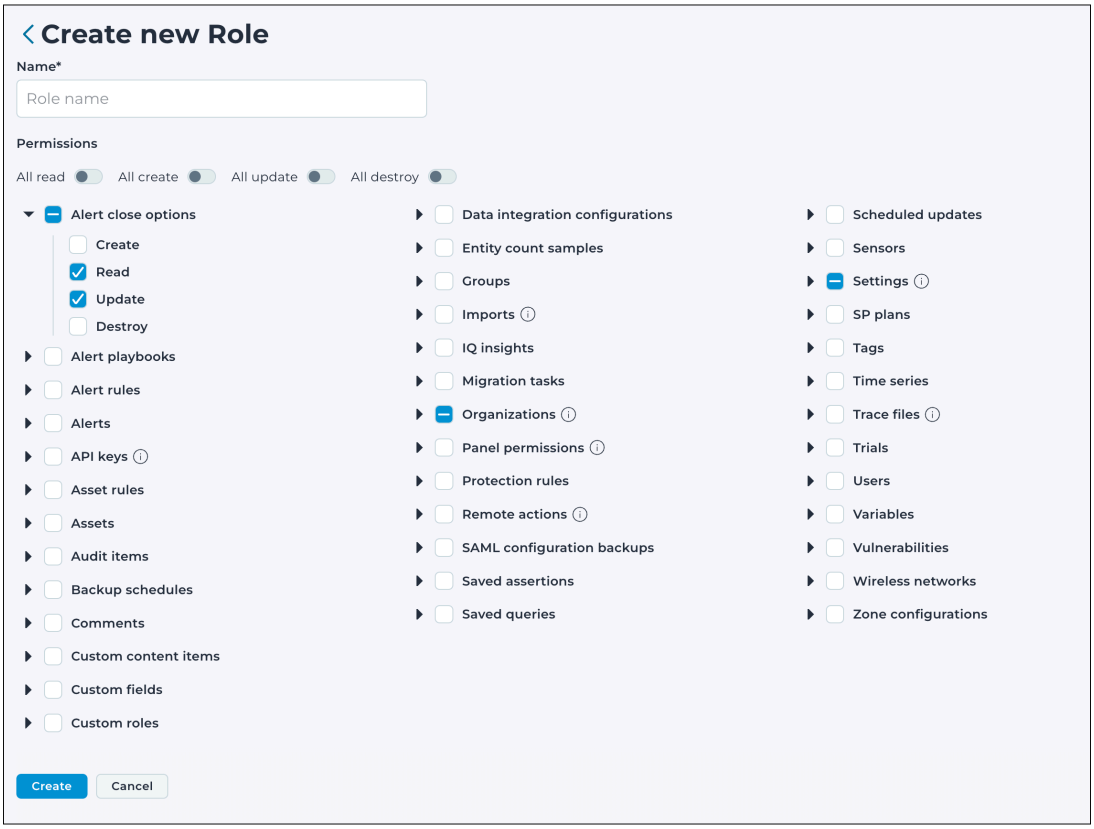
2. In the **Teams** section, select **Roles**.

   Result: The **Roles** page opens.

3. Select **Add**.

   Result: The **Create new Role** page opens.

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



Create new Role

Name*

Role name

Permissions

All read ○ All create ○ All update ○ All destroy ○

⊟ Alert close options
- □ Create
- ☑ Read
- ☑ Update
- □ Destroy

□ Alert playbooks
□ Alert rules
□ Alerts
□ API keys ⓘ
□ Asset rules
□ Assets
□ Audit items
□ Backup schedules
□ Comments
□ Custom content items
□ Custom fields
□ Custom roles
□ Data integration configurations
□ Entity count samples
□ Groups
□ Imports ⓘ
□ IQ insights
□ Migration tasks
⊟ Organizations ⓘ
□ Panel permissions ⓘ
□ Protection rules
□ Remote actions ⓘ
□ SAML configuration backups
□ Saved assertions
□ Saved queries
□ Scheduled updates
□ Sensors
⊟ Settings ⓘ
□ SP plans
□ Tags
□ Time series
□ Trace files ⓘ
□ Trials
□ Users
□ Variables
□ Vulnerabilities
□ Wireless networks
□ Zone configurations

Create Cancel

5. If applicable, use one or more of the toggles to apply settings on all options.

   You can choose from:

   - All read
   - All create
   - All update
   - All destroy

6. If necessary, select the options manually.

> **Note:**
> An icon next to some options lets you view additional information.

7. Select **Create**.

Results

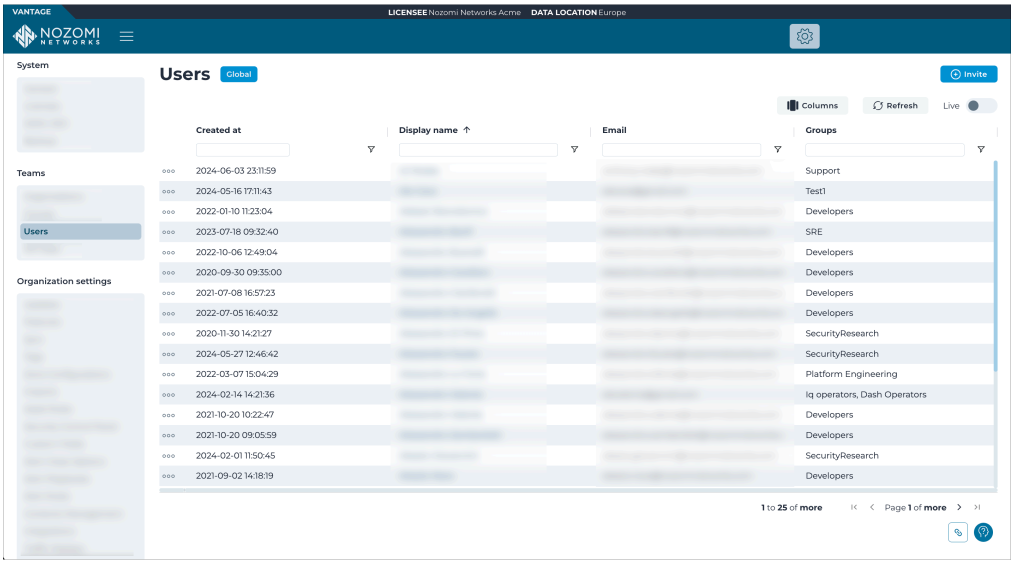
The role has been added.

What to do next

Assign the role to a group (on page 32).

Users

*The **Users** page shows all the users that have been assigned in Vantage.*



	Created at	Display name ↑	Email	Groups
○○○	2024-06-03 23:11:59	[redacted]	[redacted]	Support
○○○	2024-05-16 17:11:43	[redacted]	[redacted]	Test1
○○○	2022-01-10 11:23:04	[redacted]	[redacted]	Developers
○○○	2023-07-18 09:32:40	[redacted]	[redacted]	SRE
○○○	2022-10-06 12:49:04	[redacted]	[redacted]	Developers
○○○	2020-09-30 09:35:00	[redacted]	[redacted]	Developers
○○○	2021-07-08 16:57:23	[redacted]	[redacted]	Developers
○○○	2022-07-05 16:40:32	[redacted]	[redacted]	Developers
○○○	2020-11-30 14:21:27	[redacted]	[redacted]	SecurityResearch
○○○	2024-05-27 12:46:42	[redacted]	[redacted]	SecurityResearch
○○○	2022-03-07 15:04:29	[redacted]	[redacted]	Platform Engineering
○○○	2024-02-14 14:21:36	[redacted]	[redacted]	Iq operators, Dash Operators
○○○	2021-10-20 10:22:47	[redacted]	[redacted]	Developers
○○○	2021-10-20 09:05:59	[redacted]	[redacted]	Developers
○○○	2024-02-01 11:50:45	[redacted]	[redacted]	SecurityResearch
○○○	2021-09-02 14:18:19	[redacted]	[redacted]	Developers

1 to 25 of more Page 1 of more

Figure 17. Users page

General

Users represent the people and applications that interact with Vantage. The two types of user are:

- SAML users (on page 44)
- Local users (on page 45)

> **Note:**
>
> To authenticate users that will access Vantage through third-party applications, you will need to configure them.

SAML users

The majority of users in Vantage are *SAML* users and they are managed through your *IdP*.

A *SAML* user must go to the Vantage site and enter valid *SAML* credentials. The first time a *SAML* user logs in, Vantage retrieves authentication details from your *IdP*, and automatically creates the user. Vantage also adds the user to the appropriate groups, as defined in your *IdP*, and maps them to Vantage groups.

User groups are crucial to *SAML* integration in Vantage. For more details about user authentication, see:

- Group membership (on page 28)
- SAML integration configuration (on page 145)

Local users

These users are a small subset of your users, and include the main administrative account. These users only exist inside Vantage.

By default, Vantage includes an administrative user with complete access. This user is the primary administrator of your Vantage instance and is always managed locally. You can have other local users as well. For example, it is common to manage users of a Vantage sandbox as local users.

A local user will receive an email with an invite to join Vantage.

Note:

Because your *IdP* does not manage local users, two limitations apply:

- The group membership of a local user cannot be changed after the user is created. Nozomi Networks recommends that if you need to change the group membership for a user, you delete, and then create a local user again.
- A local account is never automatically deleted, so its *application programming interface (API)* keys are never automatically revoked. You must revoke the *API* keys for a local user to render them inert. For more details, see API Keys (on page 53).

Invite

This button lets you Invite a user (on page 46) to Vantage.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Invite a user

*You can use the **Users** page to send an email invite to someone to add them as a new user in Vantage.*

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

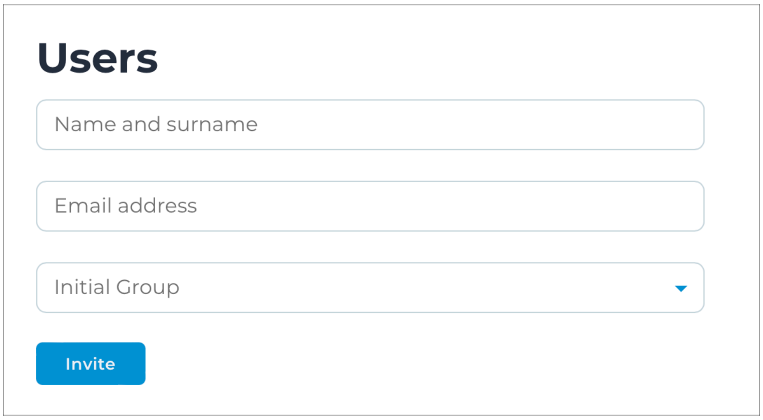
2. In the **Teams** section, select **Users**.

   Result: The **Users** page opens.

3. Select **Invite**.

   Result: Data entry fields show.

4. In the **Name and surname** field, enter the details as necessary.

5. In the **Email address** field, enter an email address for the user.
6. Select the **Initial Group** dropdown, and select an option.
7. Select **Invite**.

Results

The email invitation has been sent.

Resend an invite to a user

*You can use the **Users** page to resend an email invitation to a user that you want to invite to Vantage.*

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

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

   Result: The **Users** page opens.

3. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Resend Invite**.

Results

The email invitation has been sent again.

Delete a user

*You can use the **Users** page to delete a user from Vantage.*

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

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

   Result: The **Users** page opens.

3. Choose a method to open the actions menu.

   Choose from:

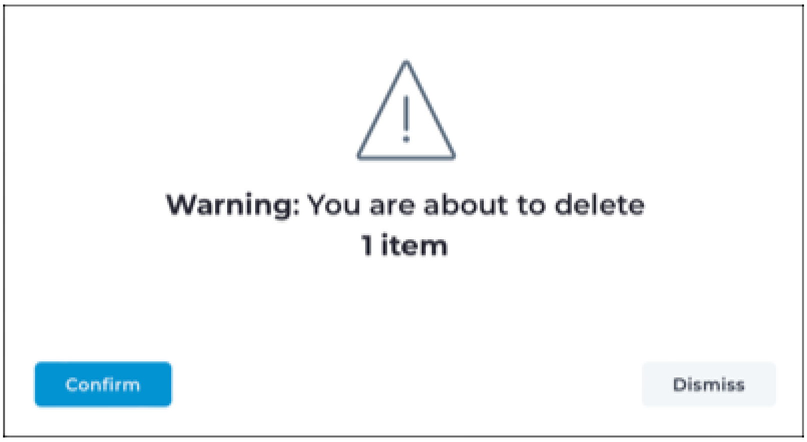
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Delete**.

   Warning: You are about to delete 1 item

   Result: A confirmation dialog shows.

6. Select **Confirm**.

Results

The user has been deleted.

API keys

API keys in Vantage

For third-party applications that integrate with Vantage, you must use API keys to authenticate them.

General

You can integrate Vantage with your third-party solutions. These applications connect to Vantage through the Nozomi Networks *API* to update data in Vantage, or to retrieve data from it. For example, you might use Splunk for *SIEM*. In this case, Splunk would connect to Vantage through the Nozomi Networks *API*. Through various *API* endpoints, your third-party applications can perform many actions, such as creating and deleting user groups or modifying alert rules.

Third-party applications

In order to authenticate, third-party applications must pass credentials in the form of an *API* key and token. To do this, you must:

1. Generate the *API* key and token in Vantage
2. Use your third-party application to call Vantage and pass the key and token for authentication

Nozomi Networks recommends that you:

- Assign a different key to each application
- Create a single user that all of your applications use to access Vantage

When you assign a different key to each application, audit log entries correctly attribute each action to the service that performed it.

When you use a single user to access Vantage, it keeps maintenance simple. However, for your specific use case, and security requirements, it is possible that it will be better to associate each application to a different user.

For more information on choosing the right approach for your implementation, see Considerations when you connect multiple applications to Vantage (on page 52).

Application IP address ranges

Your applications might connect from a completely different *IP* address range than your other Vantage users. For example, your *SIEM* might operate in the cloud. If you limit the range of *IP* addresses from which connections to Vantage must originate, you can override the *IP* address range that is defined in the **General** settings with a range that is defined for a specific *API* key.

Users

For *API* keys and users:

- Each *API* key is associated with a Vantage user. Keys are generated in the user's profile.
- The user associated with the *API* key must have sufficient permissions in Vantage. This user should be the *SAML* account of the person responsible for the integration.
- Your third-party application must pass the *API* key name and token in order to authenticate with Vantage.
- An *API* key remains valid until it is revoked, or until the user it belongs to is deleted

> **Note:**
> When an *API* key has been generated in the context of *SAML*-managed users, a *SAML* user's keys are not automatically revoked when the *SAML*-created user object is deleted. This is because your *IdP* is not aware of *API* keys. Therefore, you must manually revoke keys that have been generated for *SAML* users.

When you define a user to associate with your *API* key, you should carefully define the access that they are granted. You should consider limiting a:

- Scope
- Permissions
- Allowed *IP* address ranges

These precautions limit the actions your third-party applications can take in Vantage. For more details, see:

- Application IP address ranges (on page 49)
- User scope and permissions (on page 50)

These factors take on added importance in cases where multiple applications use them. For more details, see Considerations when you connect multiple applications to Vantage (on page 52).

User scope and permissions

The user associated with the *API* key needs explicit access to data and tasks in Vantage. This means that you should assign the user to a group and role which has appropriate permissions for the application's responsibilities. For example, if your application needs access to read all data, assign its group the **Superobserver** role. Or, assign the related group the role of **Assets Operator** if the user needs to:

- Create assets
- Read assets
- Update assets
- Delete assets

You should also limit access to the organizational scope where this application is permitted to act. If your application only needs data about one specific organization, select that organization when creating the user's group role assignments.

API authentication

Once you have the API key name and token from Vantage, you can define your API calls, including enabling authentication of a third-party application.

To connect to Vantage through the *API*, your third-party application must provide the *API* key name and key token.

The dedicated authentication endpoint is `api/v1/keys/sign_in`. This endpoint is available at the same base *URL* as the web *user interface (UI)*. Assuming this base *URL* is `VANTAGE_URL`, the full authentication *URL* is `https://VANTAGE_URL/api/v1/keys/sign_in`.

When your third-party connects to Vantage, it must:

- Pass the key name as the user name
- Pass the key token as the password

When Vantage successfully authenticates the calling application, it returns a *JSON web token (JWT)*. This token allows the application to connect for 30 minutes. After 30 minutes, the *JWT* expires. When your application attempts its next transaction, Vantage returns a `401 error` (*Unauthorized*). To continue to interact with Vantage, your application must pass the key name and key token to re-authenticate. Vantage generates a new *JWT* that allows your application to interact through the *API* for the next 30 minutes.

This security precaution means that your calling application must re-authenticate with Vantage in respond to a `401 error`.

When you need to define *API* calls, refer to the documentation for your third-party application that you want to perform actions in Vantage.

Considerations when you connect multiple applications to Vantage

It is important to choose the correct approach when you want to connect multiple applications to Vantage. In many cases, you can create a single user that all of your applications use to access Vantage. However, if you have several applications that perform different kinds of task, each application may need its own user dedicated to its exclusive use.

Choosing a method

When you determine whether applications should share Vantage users, consider:

- The level of permissions that each application needs
- The scope of operation that each application needs
- The *IP* address range of each application

One Vantage user dedicated to API access

The simplest approach is to create a single user. We recommend this approach when only one application connects to Vantage, or when multiple similar applications connect.

Create a single Vantage user for all third-party applications when:

- The applications perform the same tasks in Vantage, and
- The applications all need similar levels of access in Vantage, and
- The applications all share a similar *IP* address range

Defining a single user for all your applications can simplify maintenance of *API* access as it reduces the number of objects involved in the process.

Multiple applications with dedicated Vantage users

Your applications may differ from one another in several ways. The applications may perform different actions from one another, or they may be connecting from differing *IP* ranges. In such cases, we recommend that you create multiple Vantage users for *API* access. Devise an approach that requires the fewest number of user accounts. You may find that you need a dedicated user for each application, or you may see similarities that allow you to associate several applications with a single Vantage user.

Create multiple Vantage users for your third-party applications when:

- The applications perform differing tasks in Vantage, or
- The applications need different levels of access in Vantage, or
- The applications connect from different *IP* address ranges

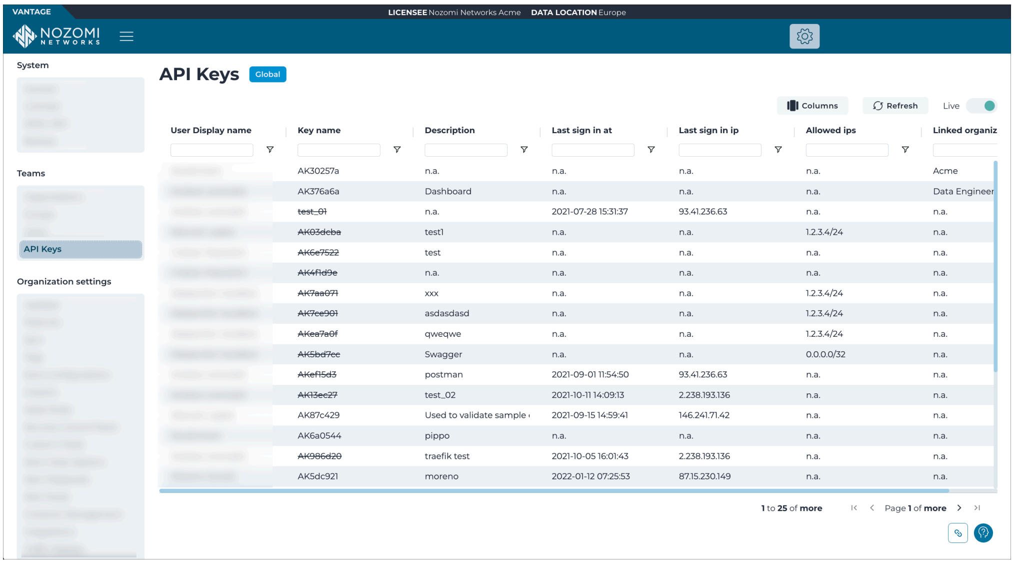
Defining dedicated users for your applications allows you to grant more precise access to each application that connects. For example, you can define an account that grants only access to view data, and one that has both view and update permissions. Therefore, you should:

- Create keys on the read-write account for your applications that must make updates in Vantage
- Create keys on the read-only account for those accounts that only retrieve data

This approach ensures that each connecting service is denied unnecessary access.

API Keys

The ***API Keys*** *page shows a list of all the API keys for every organization in the account.*



VANTAGE LICENSEE Nozomi Networks Acme DATA LOCATION Europe

System

Teams

API Keys

Organization settings

API Keys Global

Columns Refresh Live

User Display name	Key name	Description	Last sign in at	Last sign in ip	Allowed ips	Linked organiz
[redacted]	AK30257a	n.a.	n.a.	n.a.	n.a.	Acme
[redacted]	AK376a6a	Dashboard	n.a.	n.a.	n.a.	Data Engineer
[redacted]	~~test_01~~	n.a.	2021-07-28 15:31:37	93.41.236.63	n.a.	n.a.
[redacted]	~~AK03dcba~~	test1	n.a.	n.a.	1.2.3.4/24	n.a.
[redacted]	~~AK6e7522~~	test	n.a.	n.a.	n.a.	n.a.
[redacted]	~~AK4f1d9e~~	n.a.	n.a.	n.a.	n.a.	n.a.
[redacted]	~~AK7aa071~~	xxx	n.a.	n.a.	1.2.3.4/24	n.a.
[redacted]	~~AK7ce901~~	asdasdasd	n.a.	n.a.	1.2.3.4/24	n.a.
[redacted]	~~AKea7a0f~~	qweqwe	n.a.	n.a.	1.2.3.4/24	n.a.
[redacted]	~~AK5bd7ce~~	Swagger	n.a.	n.a.	0.0.0.0/32	n.a.
[redacted]	~~AKef15d3~~	postman	2021-09-01 11:54:50	93.41.236.63	n.a.	n.a.
[redacted]	~~AK13ec27~~	test_02	2021-10-11 14:09:13	2.238.193.136	n.a.	n.a.
[redacted]	AK87c429	Used to validate sample	2021-09-15 14:59:41	146.241.71.42	n.a.	n.a.
[redacted]	AK6a0544	pippo	n.a.	n.a.	n.a.	n.a.
[redacted]	~~AK986d20~~	traefik test	2021-10-05 16:01:43	2.238.193.136	n.a.	n.a.
[redacted]	AK5dc921	moreno	2022-01-12 07:25:53	87.15.230.149	n.a.	n.a.

1 to **25** of **more** Page **1** of **more**

Figure 18. API Keys page

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** ○ toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Generate an API key

Before you can use an API key, you must generate one.

Before you begin

Before you do this procedure, make sure that you have:

- Created a user to associate with your third-party application
- Assigned the user a role that grants the necessary permissions and scope within Vantage

About this task

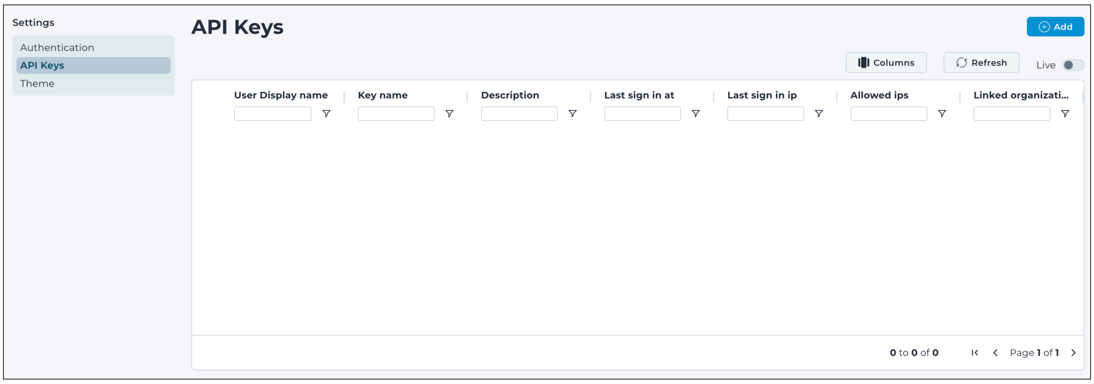
Once an *API* key has been created, you cannot edit it. You can only revoke it.

Procedure

1. Log into Vantage as the user who will own the *API* key.
2. In the top navigation bar, select 👤 **> Profile**.
3. Select **API Keys**.

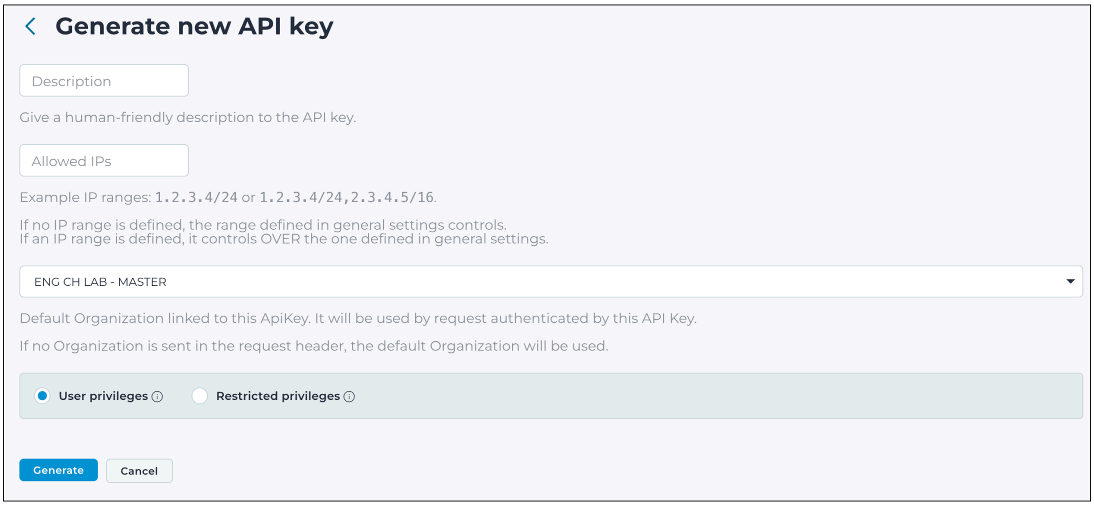
   Result: The **API Keys** page opens.

4. To generate a new *API* key, select **Add**.



User Display name	Key name	Description	Last sign in at	Last sign in ip	Allowed ips	Linked organizati...

5. In the **Description** field, enter a description for the *API* key.



Generate new API key

Description

Give a human-friendly description to the API key.

Allowed IPs

Example IP ranges: `1.2.3.4/24` or `1.2.3.4/24,2.3.4.5/16`.

If no IP range is defined, the range defined in general settings controls.
If an IP range is defined, it controls OVER the one defined in general settings.

ENG CH LAB - MASTER

Default Organization linked to this ApiKey. It will be used by request authenticated by this API Key.

If no Organization is sent in the request header, the default Organization will be used.

● User privileges ○ Restricted privileges

Note:
Nozomi Networks recommends that the description includes the name of the application that will connect with the *API* key.

6. **Optional:** Enter a range of allowed *IP* addresses in the **Allowed IPs** field. Only applications within this range will be permitted to connect with this key.

Note:
For these settings, you must use comma-delimited entries, in *CIDR* format. Values here will override the values in the **SECURITY** section on the General (on page 17) page.

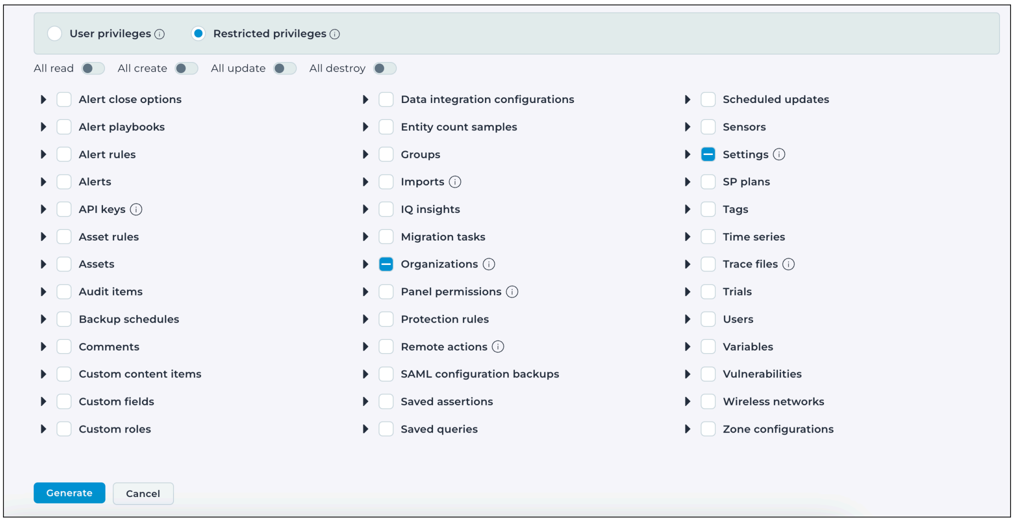
7. In the **Organization** field, select the organization that will be the default for this *API* key.

Note:
If an *API* request that uses this key doesn't include an organization, the default organization is used.

8. Select one of these options:

   Choose from:

   - **User privileges**
   - **Restricted privileges**



○ User privileges ⓘ ● Restricted privileges ⓘ

All read All create All update All destroy

- ☐ Alert close options
- ☐ Alert playbooks
- ☐ Alert rules
- ☐ Alerts
- ☐ API keys ⓘ
- ☐ Asset rules
- ☐ Assets
- ☐ Audit items
- ☐ Backup schedules
- ☐ Comments
- ☐ Custom content items
- ☐ Custom fields
- ☐ Custom roles
- ☐ Data integration configurations
- ☐ Entity count samples
- ☐ Groups
- ☐ Imports ⓘ
- ☐ IQ insights
- ☐ Migration tasks
- ⊟ Organizations ⓘ
- ☐ Panel permissions ⓘ
- ☐ Protection rules
- ☐ Remote actions ⓘ
- ☐ SAML configuration backups
- ☐ Saved assertions
- ☐ Saved queries
- ☐ Scheduled updates
- ☐ Sensors
- ⊟ Settings ⓘ
- ☐ SP plans
- ☐ Tags
- ☐ Time series
- ☐ Trace files ⓘ
- ☐ Trials
- ☐ Users
- ☐ Variables
- ☐ Vulnerabilities
- ☐ Wireless networks
- ☐ Zone configurations

User privileges applies the same permissions that the user has.

Restricted privileges allows you to define a set of permissions associated with the *API* key.

> **Note:**
> During execution, the key's effective permissions are the permissions common to both the user and the *API* key.

9. Select **Generate**.

   Result: Vantage generates a key and displays its:

   - Key name
   - Key token
   - Allowed ips
   - Linked organization

10. **Important:**
    You will need some of these values when you configure your third-party application. While the name is shown in the Vantage *UI* after this point, the token is not shown again. If you lose this data, you must generate a new *API* key.

    Record these details:

    - Key name
    - Key token
    - Allowed ips

Revoke an API key

Once an API key has been created, you cannot edit it. You can only revoke it.

Procedure

1. Log into Vantage as an administrator.
2. In the top navigation bar, select ⚙

   Result: The administration page opens.
3. In the **Teams** section, select **API Keys**.

   Result: The **API Keys** page opens.
4. In the **Key name** column, hover your mouse over the *API* key that you want to revoke.

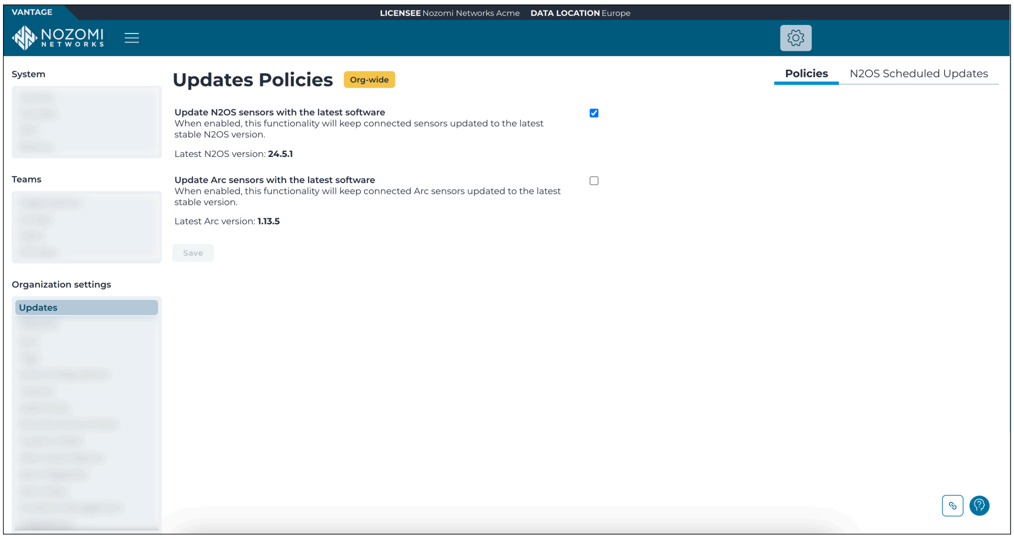
   Result: The 🗑 icon shows.
5. Select the 🗑 icon.

   Result: The *API* key has been revoked.

Organization Settings

Updates

*The **Updates** page gives you access to configuration tabs for update policies and to schedule updates.*



Updates Policies Org-wide

☑ Update N2OS sensors with the latest software
When enabled, this functionality will keep connected sensors updated to the latest stable N2OS version.

Latest N2OS version: **24.5.1**

□ Update Arc sensors with the latest software
When enabled, this functionality will keep connected Arc sensors updated to the latest stable version.

Latest Arc version: **1.13.5**

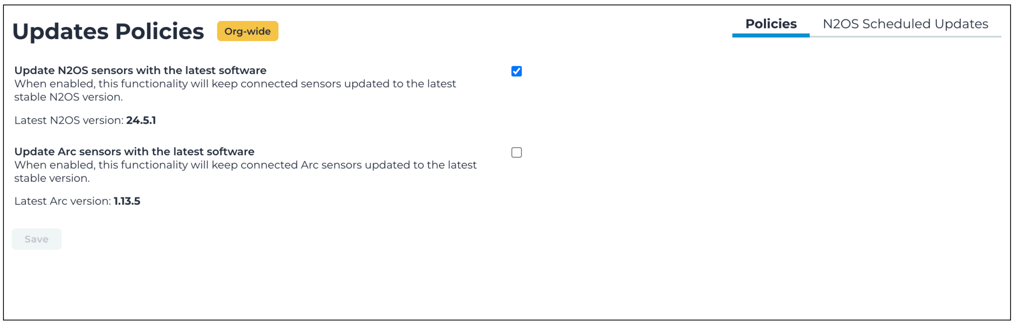
Figure 19. Updates page

The **Updates** pages has these tabs:

- Policies (on page 60)
- N2OS Scheduled Updates (on page 61)

Policies

*The **Policies** page lets you view and set the update policy for Vantage and its sensors. You can select options that will keep your sensors updated with the latest version of the applicable software.*



Update N2OS sensors with the latest software ☑
When enabled, this functionality will keep connected sensors updated to the latest stable N2OS version.

Latest N2OS version: **24.5.1**

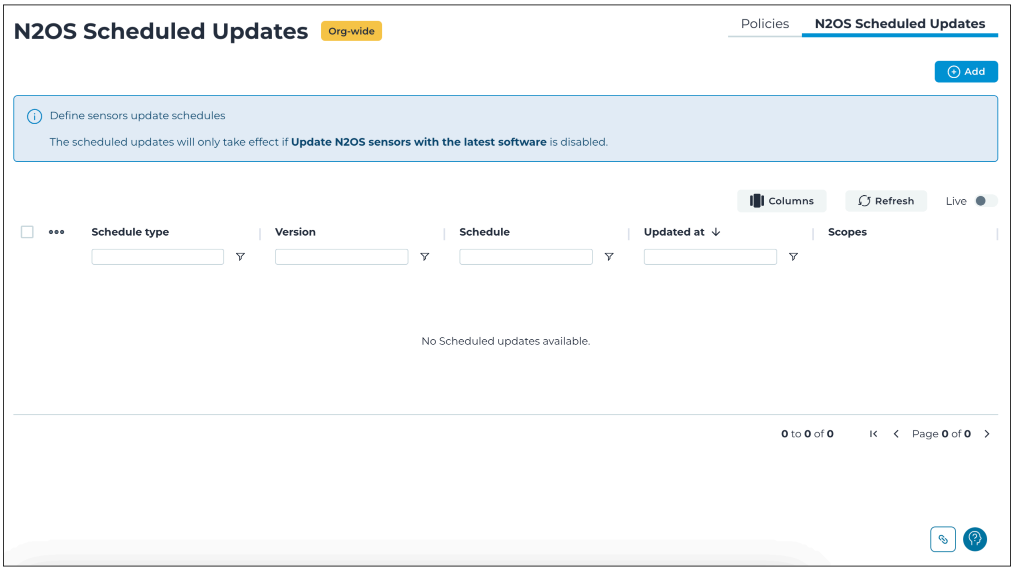
Update Arc sensors with the latest software □
When enabled, this functionality will keep connected Arc sensors updated to the latest stable version.

Latest Arc version: **1.13.5**

Figure 20. Policies page

N2OS Scheduled Updates

*The **N2OS Scheduled Updates** page lets you create and configure update schedules for N2OS sensors. You can schedule these types of updates: One-Shot, Recurrent, Delayed, and Version Offset.*



Define sensors update schedules

The scheduled updates will only take effect if **Update N2OS sensors with the latest software** is disabled.

Schedule type	Version	Schedule	Updated at	Scopes

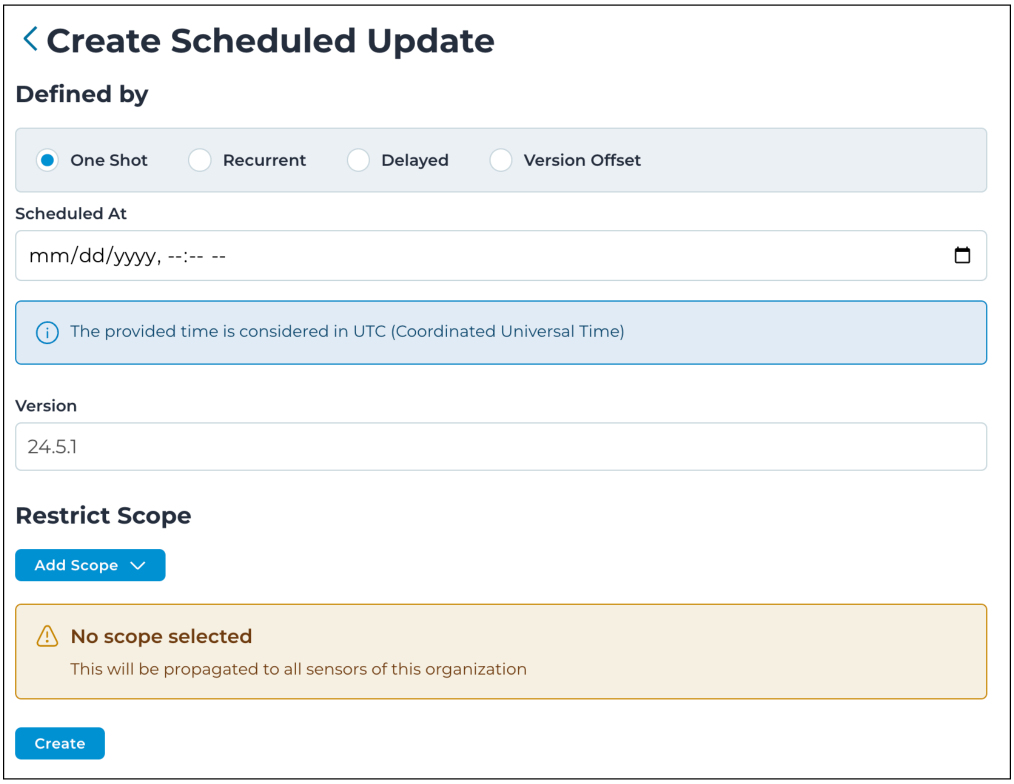
No Scheduled updates available.

0 to **0** of **0**   Page **0** of **0**

Figure 21. N2OS Scheduled Updates page

The **Add** button lets you choose a type of update to schedule.

One-Shot



Create Scheduled Update

Defined by

● One Shot ○ Recurrent ○ Delayed ○ Version Offset

Scheduled At

mm/dd/yyyy, --:-- --

The provided time is considered in UTC (Coordinated Universal Time)

Version

24.5.1

Restrict Scope

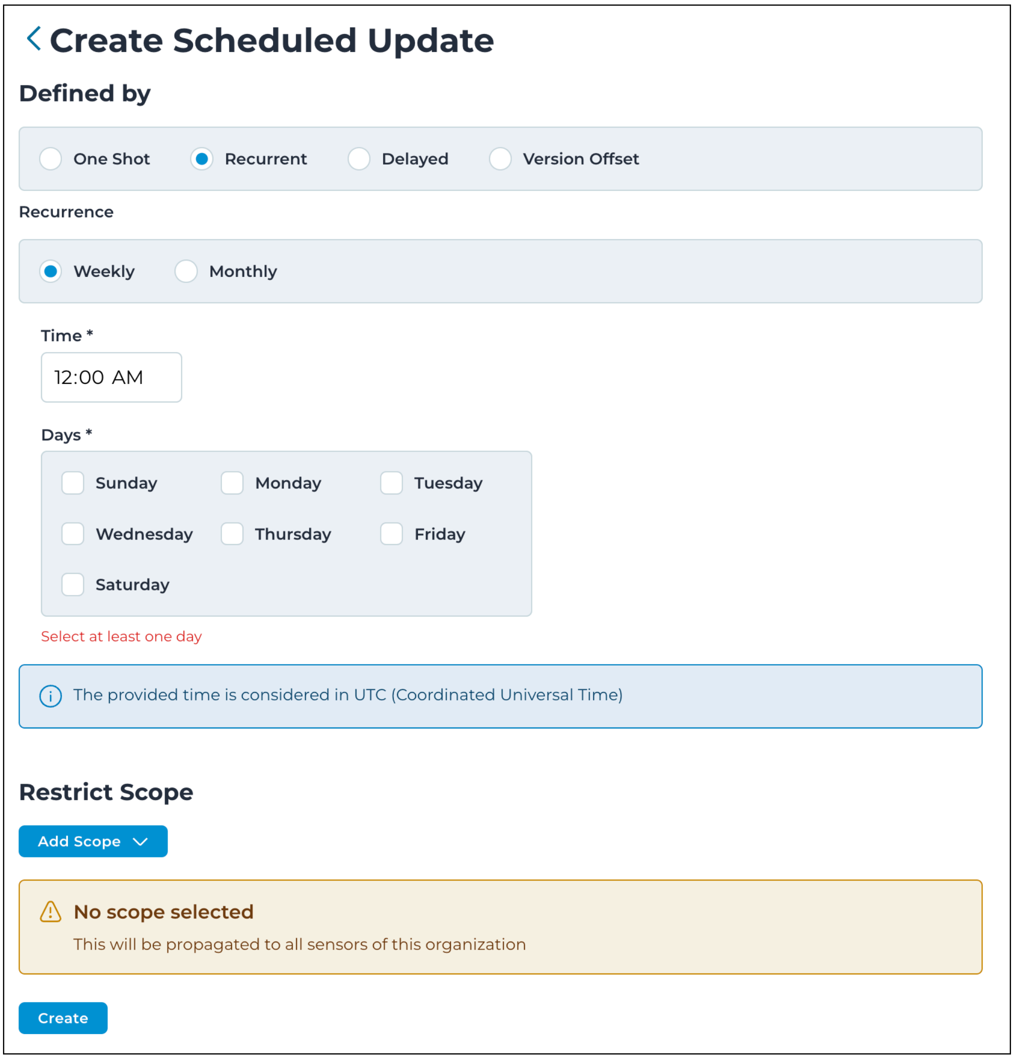
No scope selected

This will be propagated to all sensors of this organization

Figure 22. One-Shot

Schedule a single update to latest version, at a specified time.

Recurrent



Create Scheduled Update

Defined by

○ One Shot ● Recurrent ○ Delayed ○ Version Offset

Recurrence

● Weekly ○ Monthly

Time *

12:00 AM

Days *

□ Sunday □ Monday □ Tuesday
□ Wednesday □ Thursday □ Friday
□ Saturday

Select at least one day

The provided time is considered in UTC (Coordinated Universal Time)

Restrict Scope

Add Scope

No scope selected

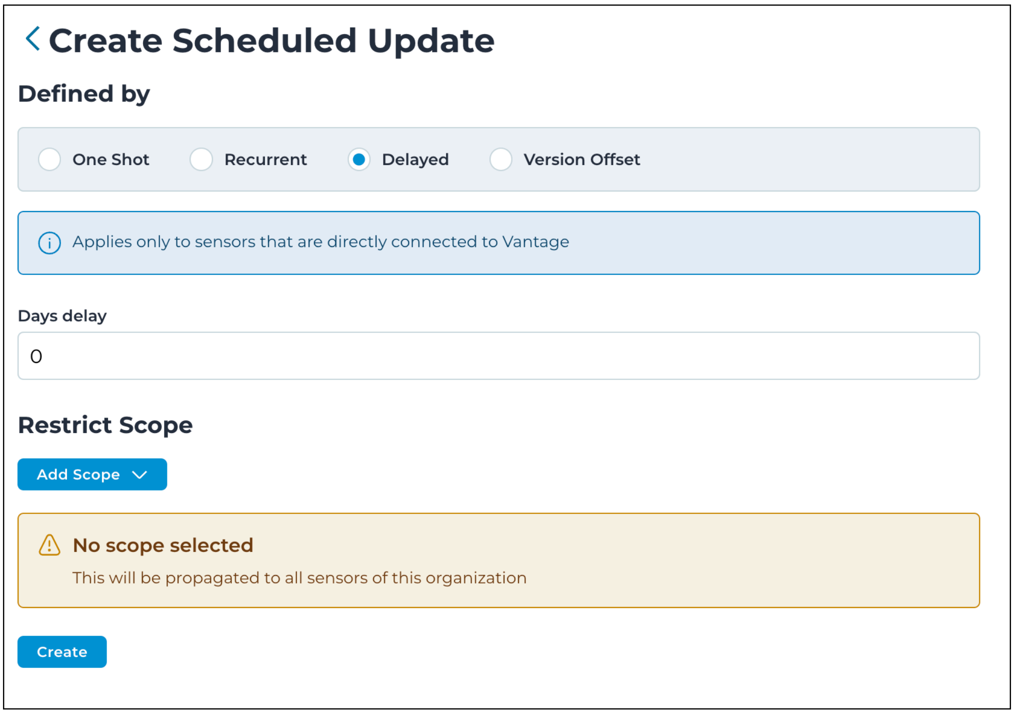
This will be propagated to all sensors of this organization

Create

Figure 23. Recurrent

Schedule a weekly or monthly recurring update, and configure the time and date of the update.

Delayed



Create Scheduled Update

Defined by

○ One Shot ○ Recurrent ● Delayed ○ Version Offset

Applies only to sensors that are directly connected to Vantage

Days delay

0

Restrict Scope

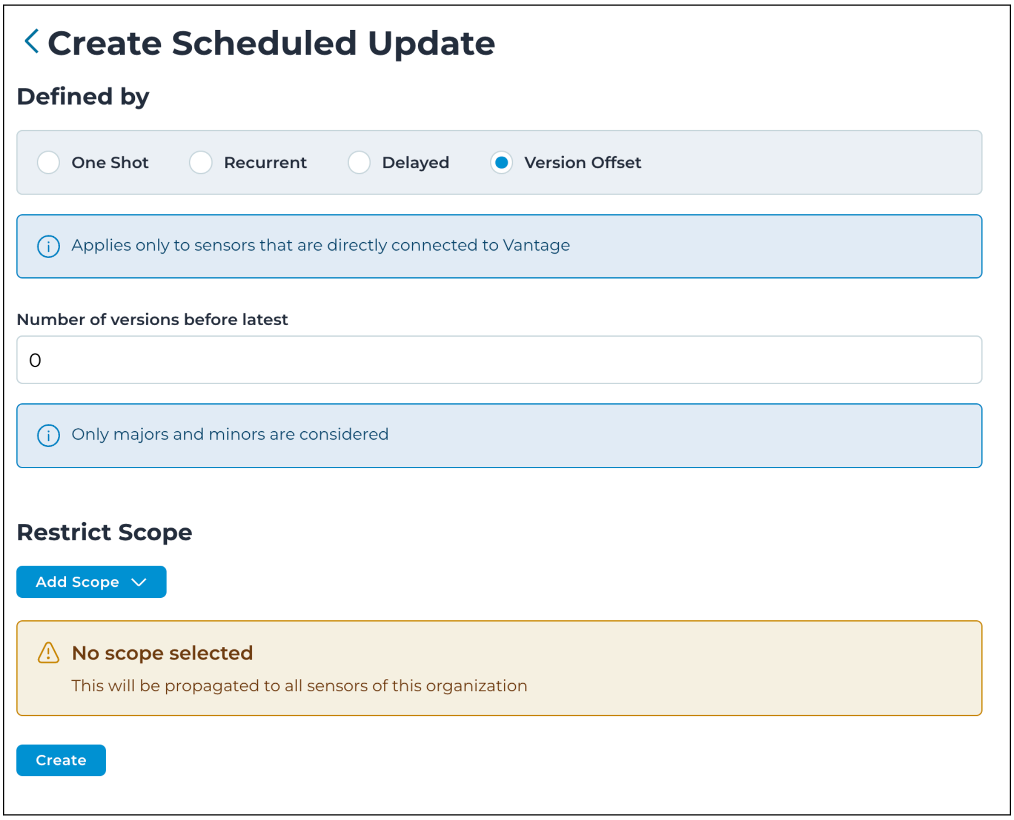
No scope selected

This will be propagated to all sensors of this organization

Figure 24. Delayed

Schedule updates after a specified number of days after the release of a new version.

Version Offset



Create Scheduled Update

Defined by

○ One Shot ○ Recurrent ○ Delayed ● Version Offset

Applies only to sensors that are directly connected to Vantage

Number of versions before latest

0

Only majors and minors are considered

Restrict Scope

No scope selected

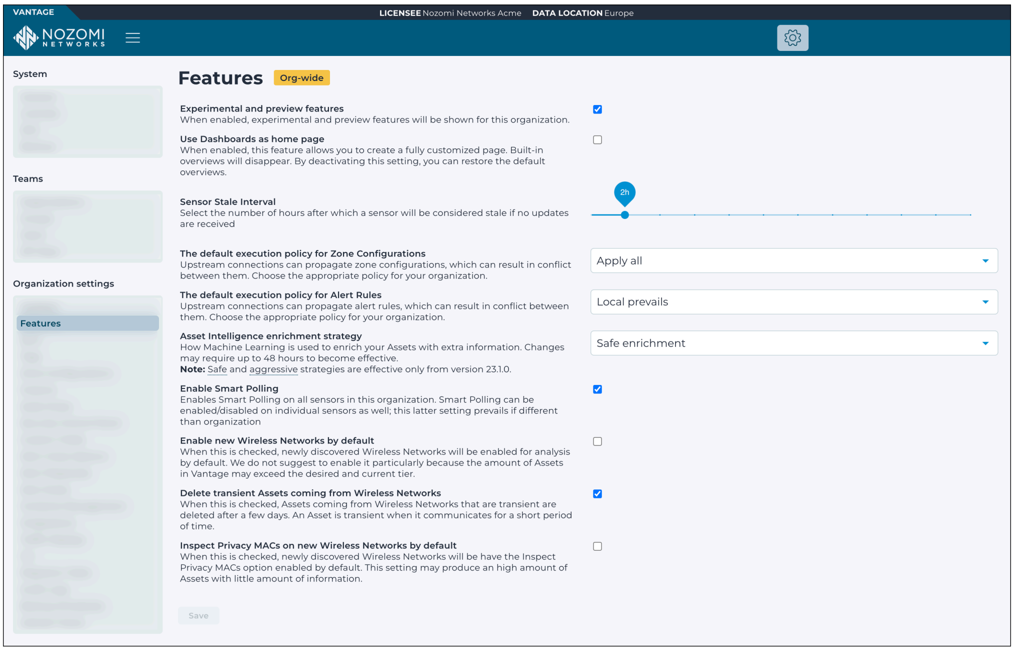
This will be propagated to all sensors of this organization

Figure 25. Version Offset

Keep the sensors at a specified number of versions before the latest one.

Features

*The **Features** page lets you configure Vantage to show, or hide, experimental and preview features for the selected organization.*



Features Org-wide

Experimental and preview features ☑
When enabled, experimental and preview features will be shown for this organization.

Use Dashboards as home page □
When enabled, this feature allows you to create a fully customized page. Built-in overviews will disappear. By deactivating this setting, you can restore the default overviews.

Sensor Stale Interval 2h
Select the number of hours after which a sensor will be considered stale if no updates are received

The default execution policy for Zone Configurations Apply all
Upstream connections can propagate zone configurations, which can result in conflict between them. Choose the appropriate policy for your organization.

The default execution policy for Alert Rules Local prevails
Upstream connections can propagate alert rules, which can result in conflict between them. Choose the appropriate policy for your organization.

Asset Intelligence enrichment strategy Safe enrichment
How Machine Learning is used to enrich your Assets with extra information. Changes may require up to 48 hours to become effective.
Note: Safe and aggressive strategies are effective only from version 23.1.0.

Enable Smart Polling ☑
Enables Smart Polling on all sensors in this organization. Smart Polling can be enabled/disabled on individual sensors as well; this latter setting prevails if different than organization

Enable new Wireless Networks by default □
When this is checked, newly discovered Wireless Networks will be enabled for analysis by default. We do not suggest to enable it particularly because the amount of Assets in Vantage may exceed the desired and current tier.

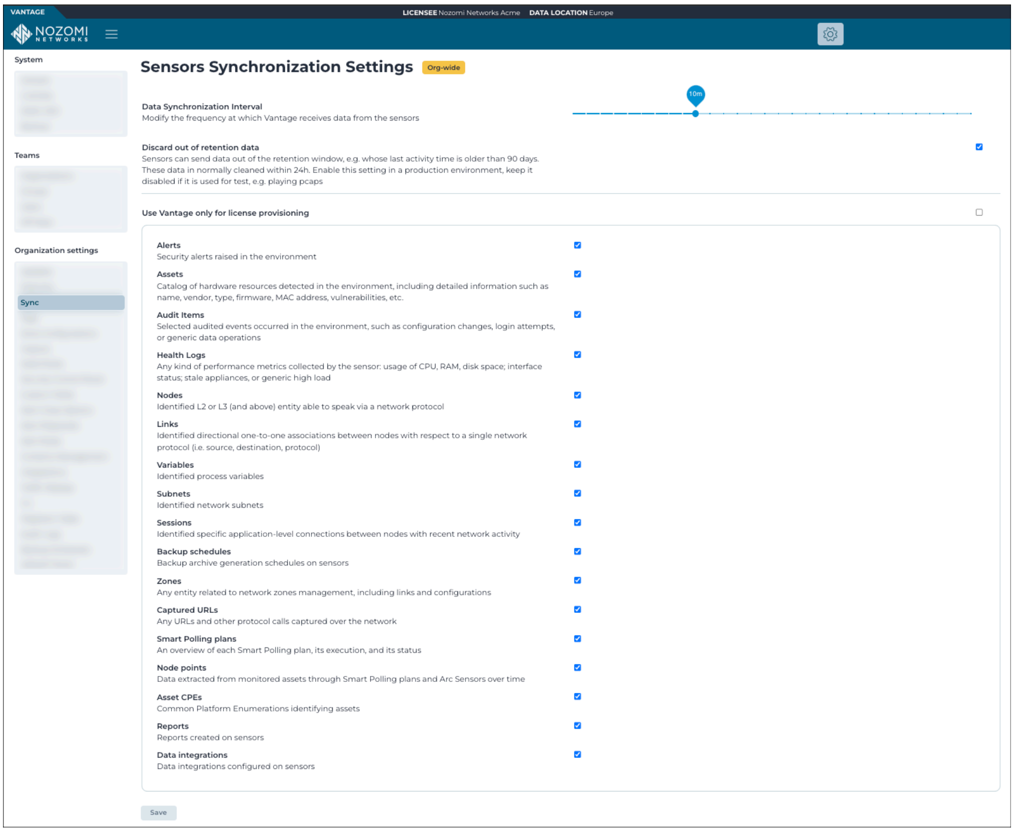
Delete transient Assets coming from Wireless Networks ☑
When this is checked, Assets coming from Wireless Networks that are transient are deleted after a few days. An Asset is transient when it communicates for a short period of time.

Inspect Privacy MACs on new Wireless Networks by default □
When this is checked, newly discovered Wireless Networks will be have the Inspect Privacy MACs option enabled by default. This setting may produce an high amount of Assets with little amount of information.

Figure 26. Features page

Sensors Synchronization Settings

*The **Settings Synchronization Settings** (**Sync**) page shows the settings that this sensor inherits from its organization.*



Sensors Synchronization Settings

Data Synchronization Interval
Modify the frequency at which Vantage receives data from the sensors

Discard out of retention data ☑
Sensors can send data out of the retention window, e.g. whose last activity time is older than 90 days. These data in normally cleaned within 24h. Enable this setting in a production environment, keep it disabled if it is used for test, e.g. playing pcaps

Use Vantage only for license provisioning ☐

Alerts ☑
Security alerts raised in the environment

Assets ☑
Catalog of hardware resources detected in the environment, including detailed information such as name, vendor, type, firmware, MAC address, vulnerabilities, etc.

Audit Items ☑
Selected audited events occurred in the environment, such as configuration changes, login attempts, or generic data operations

Health Logs ☑
Any kind of performance metrics collected by the sensor: usage of CPU, RAM, disk space; interface status; stale appliances, or generic high load

Nodes ☑
Identified L2 or L3 (and above) entity able to speak via a network protocol

Links ☑
Identified directional one-to-one associations between nodes with respect to a single network protocol (i.e. source, destination, protocol)

Variables ☑
Identified process variables

Subnets ☑
Identified network subnets

Sessions ☑
Identified specific application-level connections between nodes with recent network activity

Backup schedules ☑
Backup archive generation schedules on sensors

Zones ☑
Any entity related to network zones management, including links and configurations

Captured URLs ☑
Any URLs and other protocol calls captured over the network

Smart Polling plans ☑
An overview of each Smart Polling plan, its execution, and its status

Node points ☑
Data extracted from monitored assets through Smart Polling plans and Arc Sensors over time

Asset CPEs ☑
Common Platform Enumerations identifying assets

Reports ☑
Reports created on sensors

Data integrations ☑
Data integrations configured on sensors

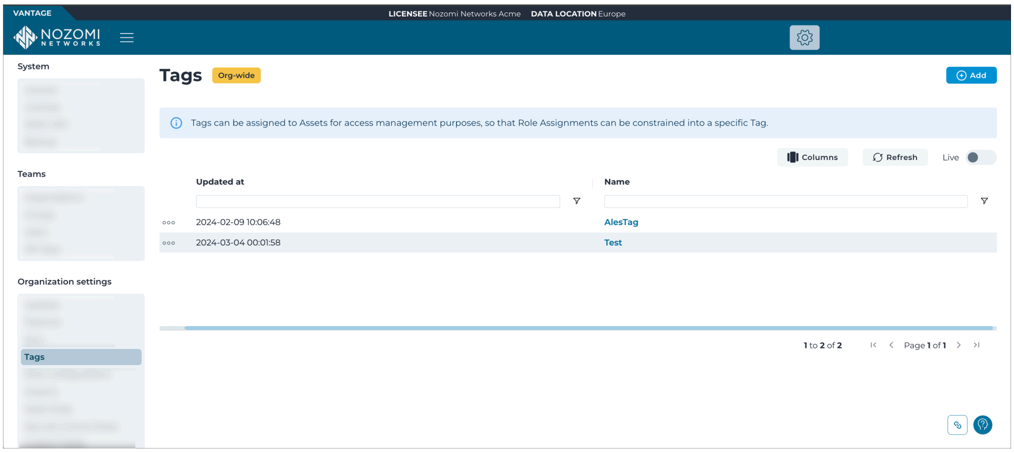
Figure 27. Sync page

Use Vantage only for license provisioning

This checkbox lets you only use Vantage for license provisioning. If this checkbox is not selected, you can edit the settings below. Changes made on this page affect this sensor, but not the default settings for its organization.

Tags

*The **Tags** page lets you assign tags to assets for access management purposes. This lets you constrain role assignments into a specific tag.*



Tags can be assigned to Assets for access management purposes, so that Role Assignments can be constrained into a specific Tag.

Updated at	Name
2024-02-09 10:06:48	AlesTag
2024-03-04 00:01:58	Test

Figure 28. Tags page

Add

This button lets you add a new tag.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Zone Configurations

The ***Zone Configurations*** *page shows all the zone configurations in your organization, and lets you add new ones.*

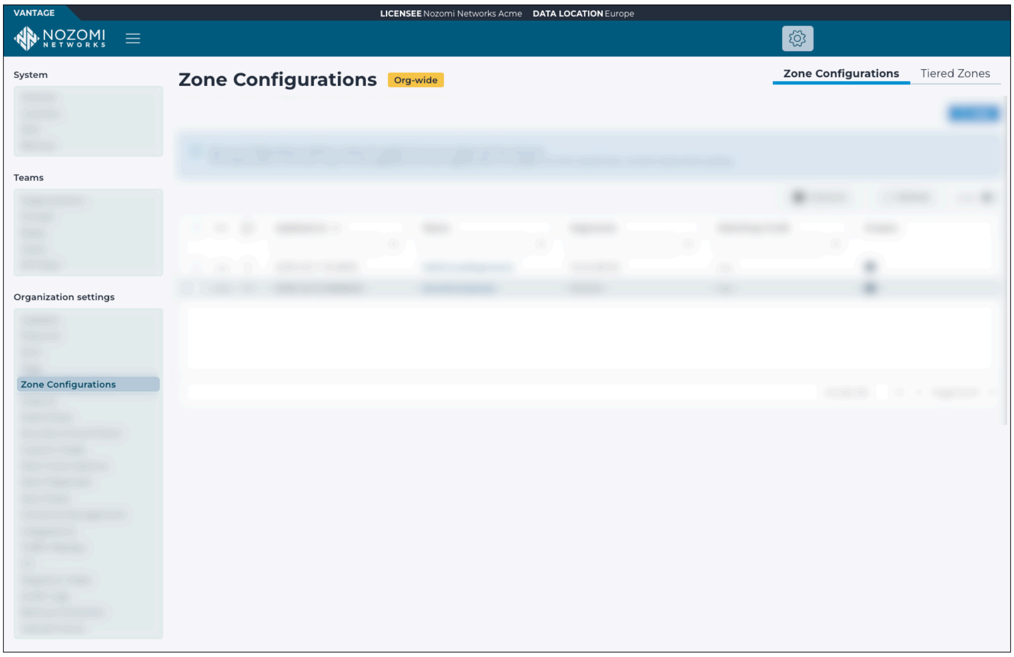


Figure 29. Zone Configurations page

Security zones are segmented sections of a network that limit access to the network's assets. The assets in each zone share some commonality that maps to a meaningful organizing principle used to categorize your assets. For example, the assets that compose an individual production line in a factory might be segmented into their own zone. In this case, you could create a zone configuration for each production line.

In Vantage, a zone configuration includes criteria that identify the assets that should belong to the zone. The configuration also specifies how Vantage handles these assets.

Zone configurations are propagated to sensors which receive the configuration. Your sensors rely on these configurations to categorize assets.

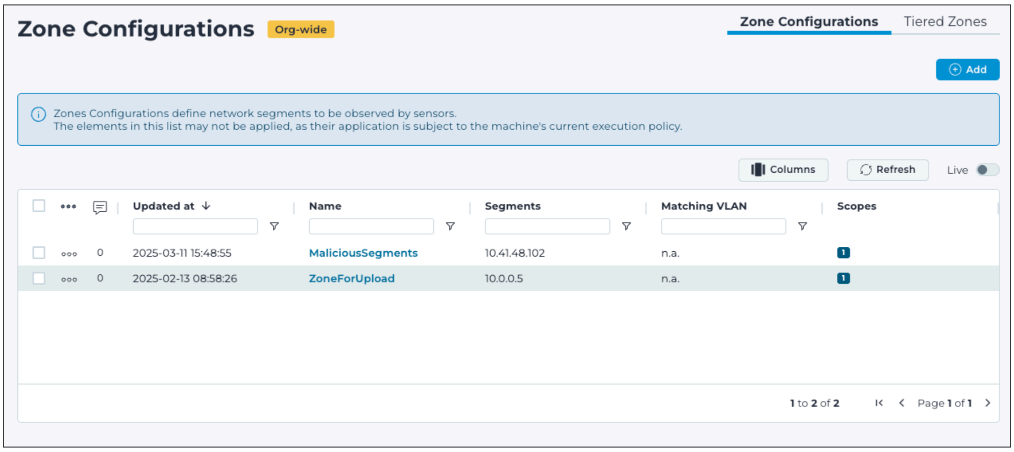
Zone configurations determine how Vantage categorizes and handles the segmentation of the assets and nodes on your network.

The **Zone Configuration** page has these tabs:

- Zone Configurations (on page 70)
- Tiered Zones (on page 77)

Zone Configurations

*The **Zone Configurations** page shows all the zone configurations in your organization, and lets you add new ones.*



Zones Configurations define network segments to be observed by sensors.
The elements in this list may not be applied, as their application is subject to the machine's current execution policy.

□	•••		Updated at ↓	Name	Segments	Matching VLAN	Scopes
□	○○○	0	2025-03-11 15:48:55	MaliciousSegments	10.41.48.102	n.a.	1
□	○○○	0	2025-02-13 08:58:26	ZoneForUpload	10.0.0.5	n.a.	1

1 to 2 of 2 Page 1 of 1

Figure 30. Zone Configurations page

Add

This button lets you add a new zone configuration (on page 71).

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add a zone configuration

Create a zone configuration by defining network criteria such as segments, MAC addresses, VLANs, and specifying behavior settings like detection and scope in the Zone Configurations page.

About this task

To create a zone configuration you need to:

- Define criteria that describe the objects that will be assigned to the zone. These criteria include options such as:
    - Network segment
    - *media access control (MAC)* address fallback
    - *virtual local area network (VLAN)* handling
- Specify the attributes that Vantage should apply to these assets and nodes

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

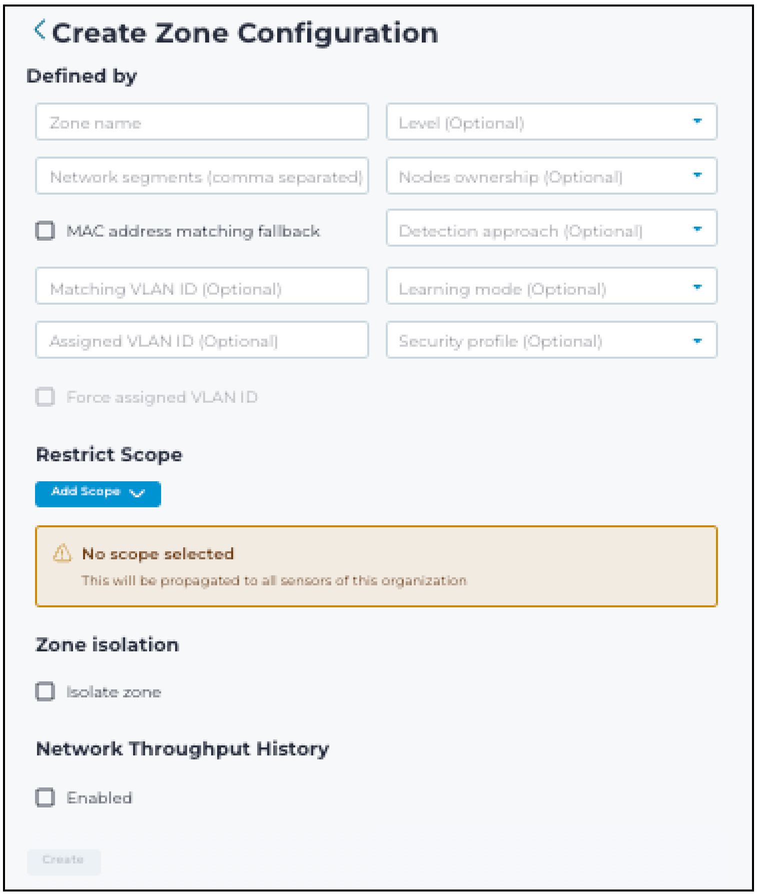
2. In the **Organization settings** section, select **Zone Configurations**.

   Result: The **Zone Configurations** page opens.

3. Select **Add**.

   Result: The **Create Zone Configuration** page shows.

4. In the **Zone name** field, enter a name for the zone.



‹ Create Zone Configuration

Defined by

Zone name
Level (Optional)
Network segments (comma separated)
Nodes ownership (Optional)
□ MAC address matching fallback
Detection approach (Optional)
Matching VLAN ID (Optional)
Learning mode (Optional)
Assigned VLAN ID (Optional)
Security profile (Optional)
□ Force assigned VLAN ID

Restrict Scope

⚠ No scope selected

This will be propagated to all sensors of this organization

Zone isolation

□ Isolate zone

Network Throughput History

□ Enabled

Note:
We recommend that you enter a name that is distinct in the wider context of your network. For example, enter a name that is meaningful when nodes in this zone appear in the graph.

5. In the **Network segments** field, specify the portion of the network that belongs to the zone.

Note:
You can enter one or more *IP* addresses to specify a network segment. To specify a range of addresses, use either *CIDR* notation, or enter two *IP* addresses that form a range. The range you specify must include both ends (e.g., `192.168.3.0-192.68.3.255`). To specify multiple network segments, you should separate them with a comma: `192.168.2.0/24, 192.168.3.0-192.68.3.255`

6. **Optional:** If you use *MAC* addresses to categorize nodes, select the **MAC address matching fallback** checkbox to enable this setting.

> **Note:**
> For a node to be considered part of a zone, its node *ID* must match one of the zone's network segments. In some cases, the node *ID* might not be sufficient to correctly categorize nodes. For example, you might want nodes that use an *IP* address as their node *ID* to belong to a zone that is defined with *MAC* address ranges instead of *IP* addresses. In such cases, enable this fallback matching strategy in order to match against the *MAC* address of the node whenever the node *IP* does not match any segment.

7. **Optional:** If you use *VLAN IDs* to categorize nodes, select the **Matching VLAN ID** checkbox to enable this setting.
8. **Optional:** If the zone only includes nodes that belong to a specific *VLAN*, select the **Matching VLAN ID** checkbox to enable this setting.

> **Note:**
> You can use *VLAN IDs* to determine which nodes are included in this zone. For example, in a zone where its network segment is defined as `192.168.4.0/24`, the *VLAN ID* is 5. The network has two nodes: `192.168.4.2` belongs to *VLAN* with *ID* 5 `192.168.4.3` doesn't belong to a *VLAN*. In this case, when **Matching VLAN ID** is enabled, only `192.168.4.2` is included in the zone.

9. In the **VLAN IDs** field, enter the *VLAN ID* of nodes that Vantage should include in this zone.
10. In the **Assigned VLAN ID** field, enter a *VLAN ID* to assign to nodes in this zone that do not already have an *ID*.

> **Note:**
> You can also select the **Force assigned VLAN ID** checkbox to overwrite the existing *VLAN IDs* of a node. When Vantage adds a node to this zone, it assigns the *VLAN ID* you enter in the **Assigned VLAN ID** field, regardless of its current value.

11. **Optional:** If your organization uses the Purdue Reference Model, select the appropriate level for the nodes in this zone in the **Level** dropdown list.

    Attention:
    In cases where a node belongs to multiple zones with different Purdue levels, you should use the most restrictive level.

    Note:
    When you filter the graph, you can select **Level** to review your Purdue level assignments.

12. **Optional:** In the **Nodes ownership** dropdown, select from:

    Choose from:
    - Public
    - Private

    Note:
    Private nodes belong to the local network, Public nodes do not.

13. **Optional:** In the **Detection approach** dropdown, select from:

    Choose from:
    - *Adaptive Learning* (default)
    - *Strict*

14. **Optional:** In the **Learning mode** dropdown, select from:

    Choose from:
    - Protecting
    - Learning

    Note:
    This setting determines whether sensors should monitor the zone against the existing baseline, or collect data about the zone's nodes and activity.

15. **Optional:** In the **Security profile** dropdown, select from:

    Choose from:

    - Low - Lowest visibility level. Only the most severe alerts are visible
    - Medium - Medium visibility level
    - High - High visibility level. All relevant alerts are visible. High is the default setting
    - Paranoid - Additional alerts that may be informational are added

    > **Note:**
    > The security profile determines the visibility of alerts that are raised by sensors monitoring nodes in this zone.

    > **Note:**
    > If you change the security profile for a zone configuration, it only affects newly-generated alerts. It has no effect on existing alerts.

16. In the **With Scope** section, select the **Add Scope** dropdown and select from:

    Choose from:

    - Tag
    - Site
    - Sensor

    > **Note:**
    > This lets you select the type of object that should restrict the scope of this zone configuration:
    >
    > - Tags are admin-defined keywords or terms applied to Vantage objects to provide finer control of system behavior
    > - Sites represent the real-world locations of your nodes
    > - Sensors are the downstream applications, such as *CMC*s and Guardians, that aggregate and send data to Vantage

    Result: A dialog opens.

17. Select the ▽ icon. Select an option to filter for the item you want to select.
18. **Optional:** If necessary, select **Isolate zone**.

    If selected, this zone's assets will not be merged with assets outside of this zone.

19. **Optional:** If necessary, in the **Network Throughput History** section, select **Enabled**.
20. Select **Confirm**.

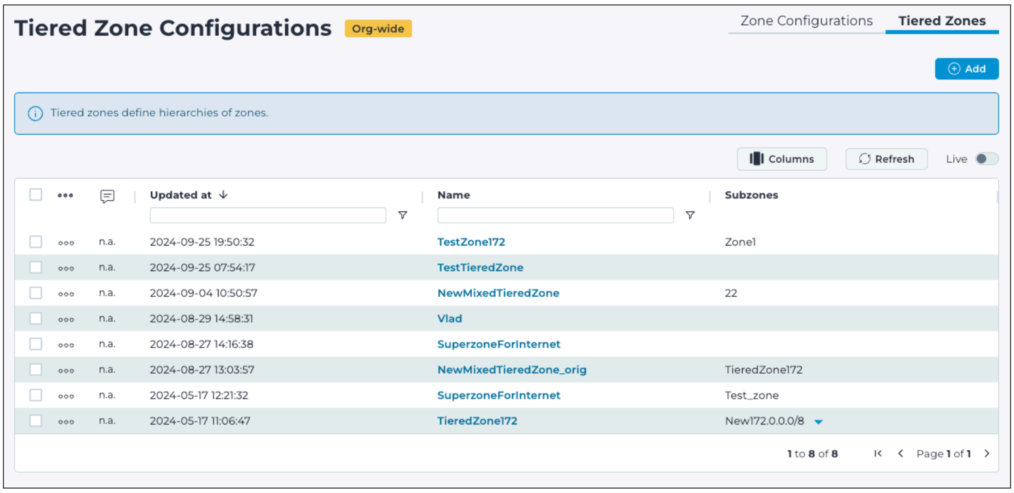
21. **Optional:** To add another item to define the scope, do steps 17 (on page 75) thru 20 (on page 75) again as necessary.
22. Select **Create**.

Results

The zone configuration has been created.

Tiered Zones

*The **Tiered Zones** page enables administrators to organize zones into hierarchical structures for more efficient management and configuration.*



Tiered zones define hierarchies of zones.

□	•••		Updated at ↓	Name	Subzones
□	○○○	n.a.	2024-09-25 19:50:32	TestZone172	Zone1
□	○○○	n.a.	2024-09-25 07:54:17	TestTieredZone	
□	○○○	n.a.	2024-09-04 10:50:57	NewMixedTieredZone	22
□	○○○	n.a.	2024-08-29 14:58:31	Vlad	
□	○○○	n.a.	2024-08-27 14:16:38	SuperzoneForInternet	
□	○○○	n.a.	2024-08-27 13:03:57	NewMixedTieredZone_orig	TieredZone172
□	○○○	n.a.	2024-05-17 12:21:32	SuperzoneForInternet	Test_zone
□	○○○	n.a.	2024-05-17 11:06:47	TieredZone172	New172.0.0.0/8 ▾

1 to 8 of 8 |< < Page 1 of 1 >

Figure 31. Tiered Zones page

Add

This button lets you Add a tiered zone configuration (on page 78).

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add a tiered zone configuration

Create a tiered zone configuration by assigning zones and subzones that inherit shared criteria such as network segments, MAC address fallback, and VLAN handling.

About this task

To create a zone configuration you need to:

- Define criteria that describe the objects that will be assigned to the zone. These criteria include options such as:
  - Network segment
  - *MAC* address fallback
  - *VLAN* handling
- Specify the attributes that Vantage should apply to these assets and nodes

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

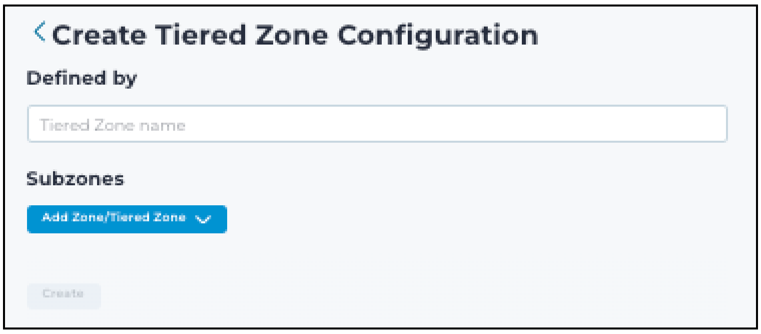
2. In the **Organization settings** section, select **Zone Configurations**.

   Result: The **Zone Configurations** page opens.

3. Select **Tiered Zones**.
4. Select **Add**.

   Result: The **Created Tiered Zone Configuration** page shows.

5. In the **Defined by** field, enter a name for the tiered zone.

   Create Tiered Zone Configuration

   Defined by

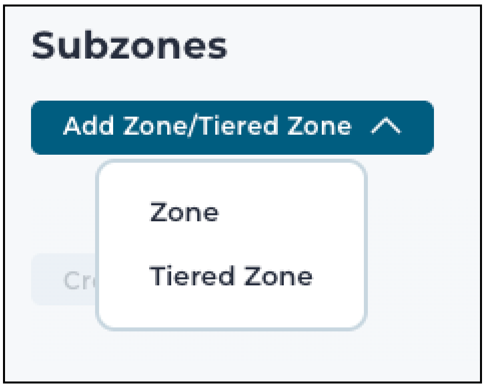
   Tiered Zone name

   Subzones

6. Select **Add Zone/Tiered Zone**.

   Result: A dialog shows.

7. Choose one of these options:



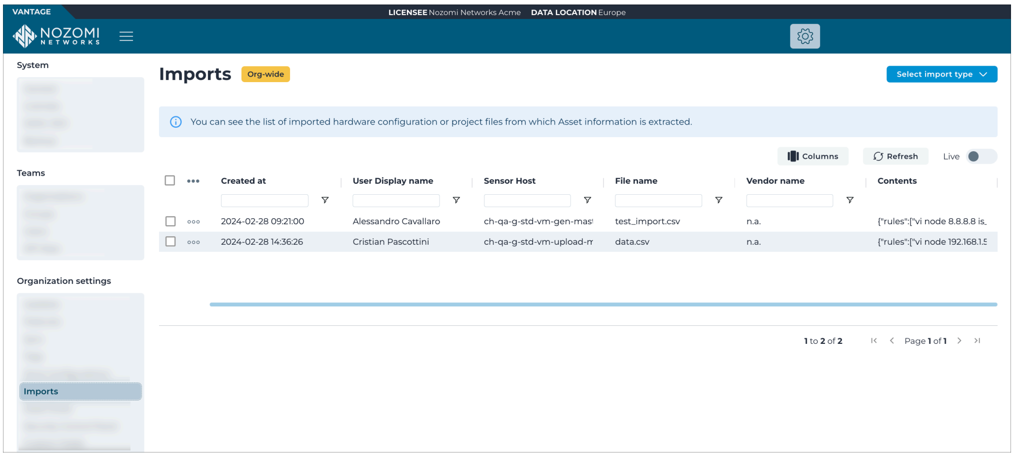
   Choose from:
   - Zone
   - Tiered Zone
8. Select one zone/tiered zone.
9. Select **Confirm**.
10. Select **Create**.

Results

The tiered zone configuration has been created.

Imports

*The **Imports** page lets you see the list of imported hardware configuration, or project files, from which asset information is extracted.*



Imports

Org-wide

Select import type

You can see the list of imported hardware configuration or project files from which Asset information is extracted.

Columns Refresh Live

☐	•••	Created at	User Display name	Sensor Host	File name	Vendor name	Contents
☐	○○○	2024-02-28 09:21:00	Alessandro Cavallaro	ch-qa-g-std-vm-gen-mast	test_import.csv	n.a.	{"rules":["vi node 8.8.8.8 is_
☐	○○○	2024-02-28 14:36:26	Cristian Pascottini	ch-qa-g-std-vm-upload-m	data.csv	n.a.	{"rules":["vi node 192.168.1.5

1 to 2 of 2 Page 1 of 1

Figure 32. Imports page

Select import type

This button lets you select an type to import.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

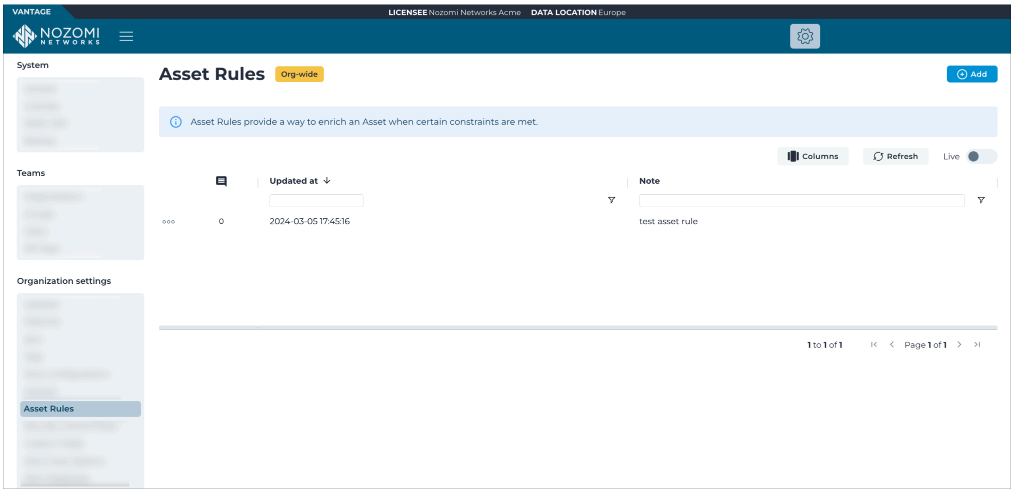
The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Asset Rules

*The **Asset Rules** page shows all the asset rules in your organization, and lets you add new ones.*



Asset Rules

Asset Rules provide a way to enrich an Asset when certain constraints are met.

		Updated at ↓	Note
ooo	0	2024-03-05 17:45:16	test asset rule

1 to 1 of 1 Page 1 of 1

Figure 33. Asset Rules page

Add

This button lets you add a new asset rule.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add an asset rule

You can use the actions menu to add an asset rule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Asset Rules**.

   Result: The **Asset Rules** page opens.

3. Select **Add new**.

   Result: The **Create Asset Rule** page shows.

4. Configure the asset rule as necessary.
5. Select **Create**.

Results

The asset rule has been created.

Edit an asset rule

You can use the actions menu to edit an asset rule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Rules**.

   Result: The **Alert Rules** page opens.

3. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Edit**.

Results

You can now edit the asset rule.

Delete an asset rule

You can use the actions menu to delete an asset rule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Rules**.

   Result: The **Alert Rules** page opens.

3. Choose a method to open the actions menu.

   Choose from:

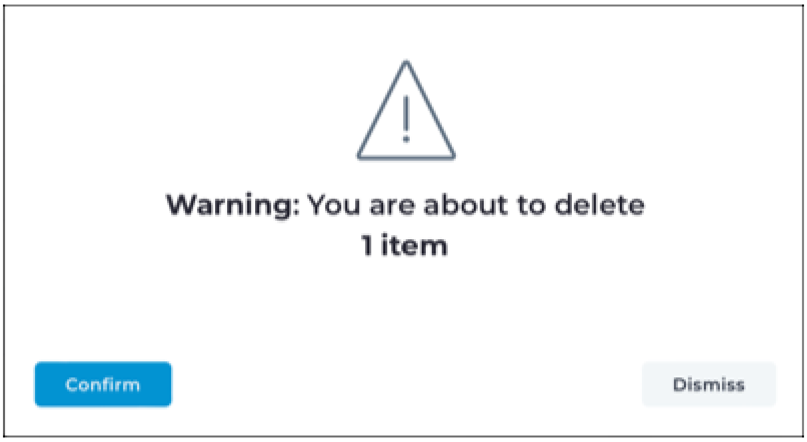
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Delete**.



Warning: You are about to delete 1 item

   Result: A confirmation dialog shows.

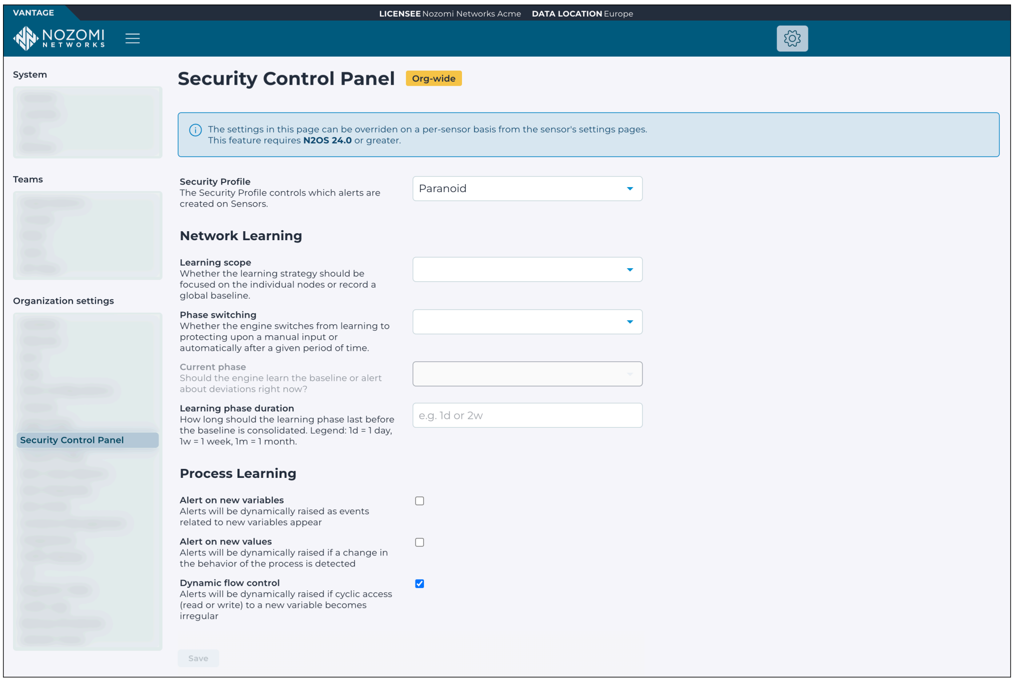
6. Select **Confirm**.

Results

The asset rule has been deleted.

Security Control Panel

*The **Security Control Panel** allows administrators to configure security settings across the organization.*



LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

Security Control Panel

The settings in this page can be overriden on a per-sensor basis from the sensor's settings pages.
This feature requires **N2OS 24.0** or greater.

Security Profile
The Security Profile controls which alerts are created on Sensors. — Paranoid

Network Learning

Learning scope
Whether the learning strategy should be focused on the individual nodes or record a global baseline.

Phase switching
Whether the engine switches from learning to protecting upon a manual input or automatically after a given period of time.

Current phase
Should the engine learn the baseline or alert about deviations right now?

Learning phase duration
How long should the learning phase last before the baseline is consolidated. Legend: 1d = 1 day, 1w = 1 week, 1m = 1 month. — e.g. 1d or 2w

Process Learning

☐ **Alert on new variables**
Alerts will be dynamically raised as events related to new variables appear

☐ **Alert on new values**
Alerts will be dynamically raised if a change in the behavior of the process is detected

☑ **Dynamic flow control**
Alerts will be dynamically raised if cyclic access (read or write) to a new variable becomes irregular

Figure 34. Security Control Panel page

Security Profile

Choose an option to determine which alerts are generated on Sensors:

- Low
- Medium
- High
- Paranoid

Network Learning

Configure how the system:

- Learns network activity
- Detects anomalies
- Applies security measures

Learning scope: Choose an option to determine what the system should focus on:

- **Adaptive Learning** (default): This option establishes a global baseline for the protected environment, and notifies you about deviations. For instance, it triggers an alert if the system detects a node in the network with a previously unseen *MAC* vendor.
- **Strict**: This option establishes individual baselines for each network entity and notifies you of every change. For example, it triggers an alert whenever a new node appears in the network, or when two nodes start communicating.

> **Note:**
> The **Strict** approach is suitable for static networks, where the conditions rarely change and the nodes have fixed addresses. In all other situations, this mode will cause too many alerts, especially in networks with dynamic addressing. In a typical installation, we recommend that you use the default approach, and only enable the strict mode in zones with static addressing through the **Zone configurations** settings.

Phase switching: Choose an option to determine whether switching between learning and protection modes happens manually or automatically:

- Manual
- Dynamic

Current phase: Choose an option to determine whether the engine is learning or alerting on deviations:

- Learning
- Protecting

Learning phase duration: Specifies the duration before a baseline is finalized.

Process Learning

Process learning enables the system to detect and alert on changes in process behavior, enhancing security monitoring.

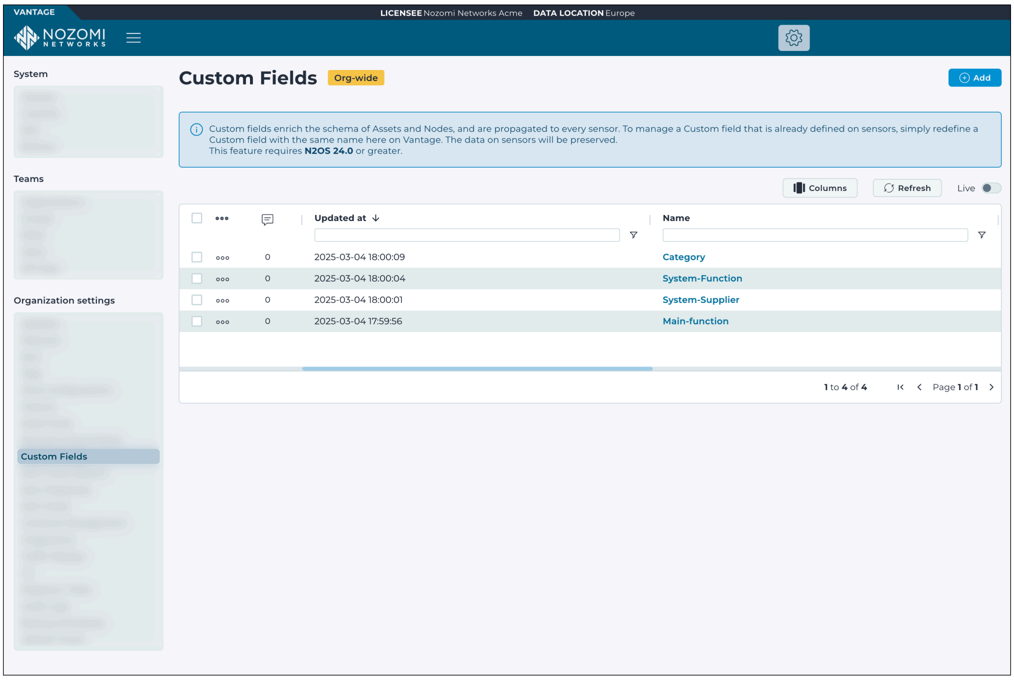
Alert on new variables: Select to raise alerts when the system detects the introduction of new process-related variables that were not previously observed.

Alert on new values: Select to generate alerts when the system detects a significant change in process values, indicating a potential anomaly.

Dynamic flow control: Select to trigger alerts when the system detects irregular patterns in cyclic access (read or write operations) to process variables.

Custom Fields

*The **Custom Fields** page lets you enrich the schema of assets and nodes, and propagate the information to every sensor.*



Custom Fields

Custom fields enrich the schema of Assets and Nodes, and are propagated to every sensor. To manage a Custom field that is already defined on sensors, simply redefine a Custom field with the same name here on Vantage. The data on sensors will be preserved.
This feature requires **N2OS 24.0** or greater.

□	•••		Updated at ↓	Name
□	○○○	0	2025-03-04 18:00:09	Category
□	○○○	0	2025-03-04 18:00:04	System-Function
□	○○○	0	2025-03-04 18:00:01	System-Supplier
□	○○○	0	2025-03-04 17:59:56	Main-function

1 to 4 of 4 Page 1 of 1

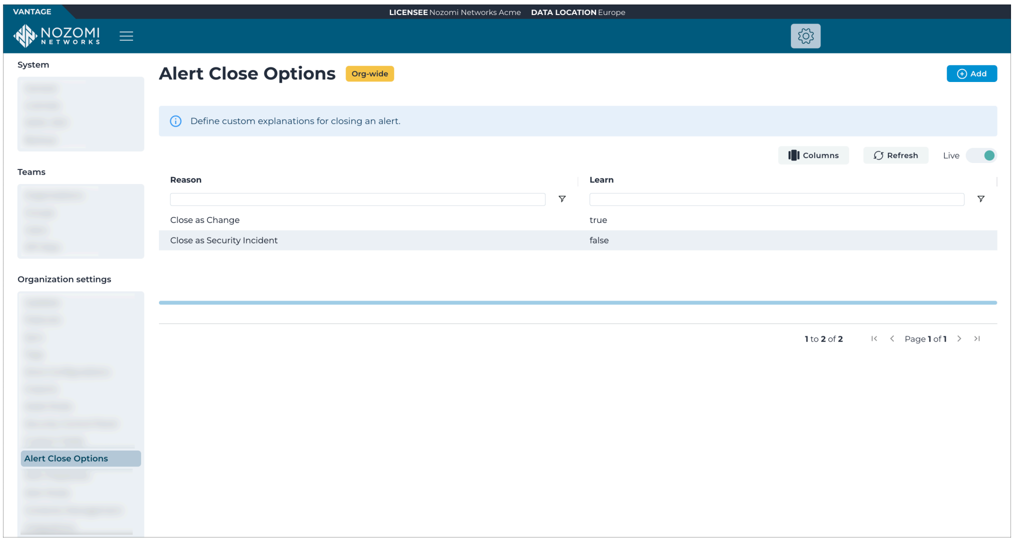
Figure 35. Custom Fields page

Add

The **Add** button lets you create a new custom field.

Alert Close Options

The ***Alert Close Options*** *page lets you define custom explanations for closing an alert.*



Alert Close Options

Define custom explanations for closing an alert.

Reason	Learn
Close as Change	true
Close as Security Incident	false

1 to 2 of 2 Page 1 of 1

Figure 36. Alert Close Options page

Add

This button lets you add a new alert closing option.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** ○ toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add an alert closing option

You can use the actions menu to add an alert closing option.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Close Options**.

   Result: The **Alert Close Options** page opens.

3. Select **Add new**.

   Result: The **Create Alert Option** page shows.

4. In the **Reason for closing** field, enter a reason.
5. Choose an option:

   Choose from:

   - Treat as incident
   - Learn

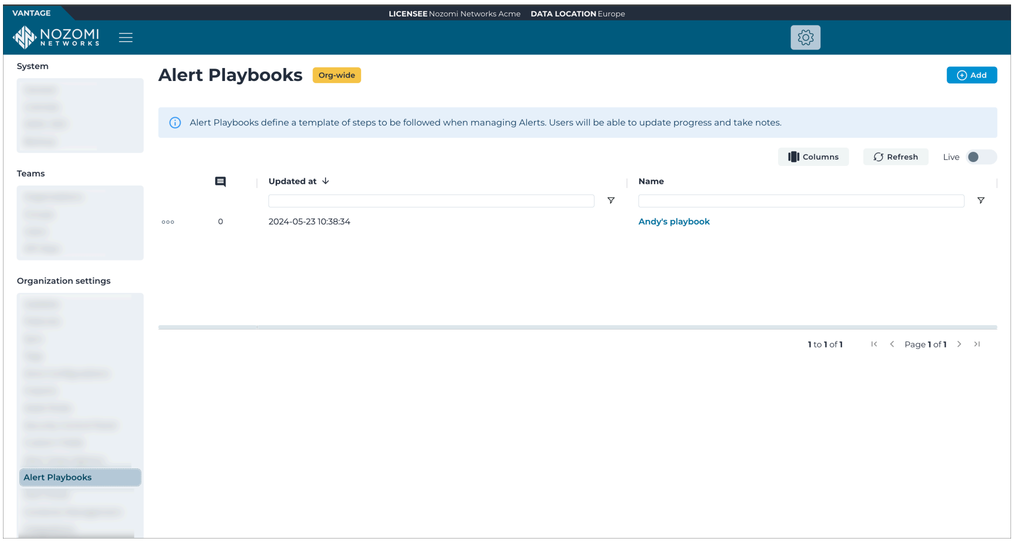
6. Select **Create**.

Results

The alert closing option has been created.

Alert Playbooks

*The **Alert Playbooks** page lets you define templates to follow to manage alerts. An alert playbook defines custom content that instructs alert operators, and other users, how to manage various types of alerts. Playbooks are associated with alerts that match criteria specified in an alert rule. When a matching alert is raised, the playbook's content is included on the new alert's **Details** page. You and your team can update this content to record progress and take notes particular to this alert.*



Alert Playbooks define a template of steps to be followed when managing Alerts. Users will be able to update progress and take notes.

		Updated at ↓	Name
◦◦◦	0	2024-05-23 10:38:34	Andy's playbook

1 to 1 of 1 Page 1 of 1

Figure 37. Alert Playbooks page

Add

This button lets you add a new alert playbook.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add an alert playbook

You can use the actions menu to add an alert playbook.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Playbooks**.

   Result: The **Alert Playbooks** page opens.

3. In the **Organization settings** section, select **Alert Rules**.

   Result: The **Alert Rules** page opens.

4. Select **Add new**.

   Result: The **Create Alert Playbook** page shows.

5. Configure the alert playbook as necessary.
6. Select **Create**.

Results

The alert playbook has been created.

Edit an alert playbook

You can use the actions menu to edit an alert playbook.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Playbooks**.

   Result: The **Alert Playbooks** page opens.

3. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Edit**.

   Result: The **Edit Alert Playbook** page opens.

6. Edit the alert playbook as necessary.
7. Select **Update**.

Results

The alert playbook has now been edited.

Delete an alert playbook

You can use the actions menu to delete an alert playbook.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Playbooks**.

   Result: The **Alert Playbooks** page opens.

3. Choose a method to open the actions menu.

   Choose from:

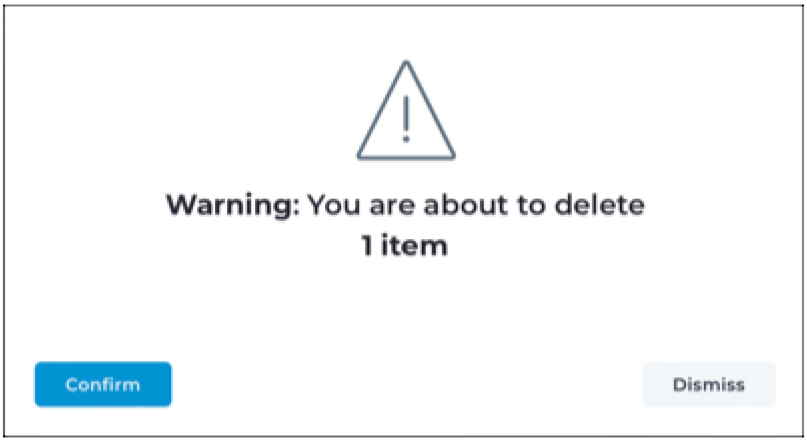
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Delete**.

   Warning: You are about to delete 1 item

   Result: A confirmation dialog shows.

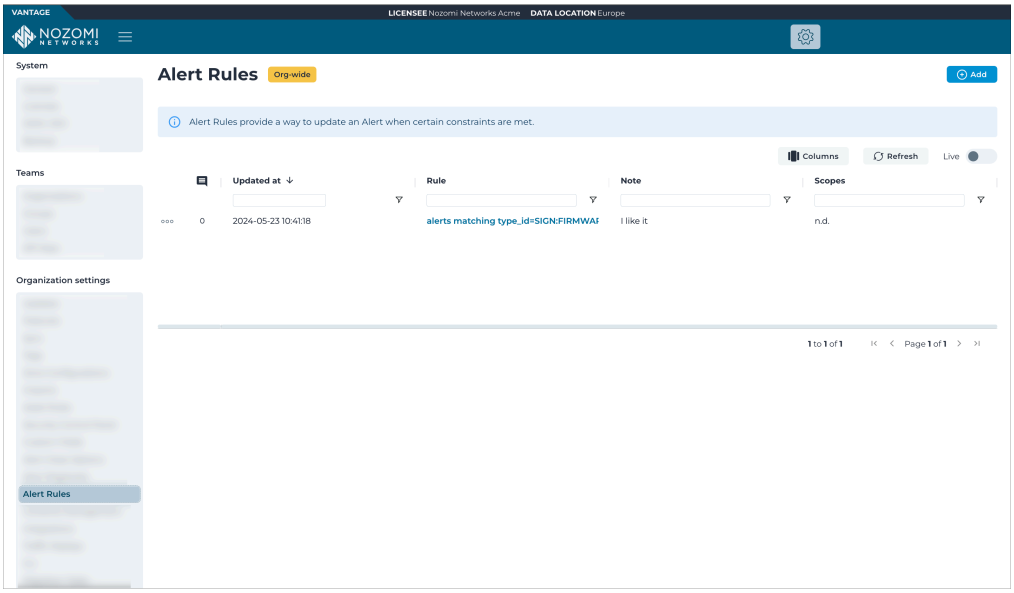
6. Select **Confirm**.

Results

The alert playbook has been deleted.

Alert Rules

*The **Alert Rules** page shows all the alert rules that you have defined, and lets you add new ones.*



Alert Rules provide a way to update an Alert when certain constraints are met.

		Updated at ↓	Rule	Note	Scopes
○○○	0	2024-05-23 10:41:18	alerts matching type_id=SIGN:FIRMWAI	I like it	n.d.

1 to 1 of 1 Page 1 of 1

Figure 38. Alert Rules page

General

Alert rules define how a sensor will handle an alert when it occurs. When an alert that matches the specified conditions occurs, the sensor that raised it will take the specified action. For example, you might have a sensor where a specific type of alert is expected. In this case, you could create a rule that identifies this sensor, and the exact type of alert, and then it will instruct the sensor to mute the alert.

Add

This button lets you add an alert rule.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add an alert rule

You can use the actions menu to add an alert rule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Rules**.

   Result: The **Alert Rules** page opens.

3. Select **Add new**.

   Result: The **Create Alert Rule** page shows.

4. Configure the alert rule as necessary.
5. Select **Create**.

Results

The alert rule has been created.

Edit an alert rule

You can use the actions menu to edit an alert rule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Rules**.

   Result: The **Alert Rules** page opens.

3. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Edit**.

Results

You can now edit the alert rule.

Delete an alert rule

You can use the actions menu to delete an alert rule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Alert Rules**.

   Result: The **Alert Rules** page opens.

3. Choose a method to open the actions menu.

   Choose from:

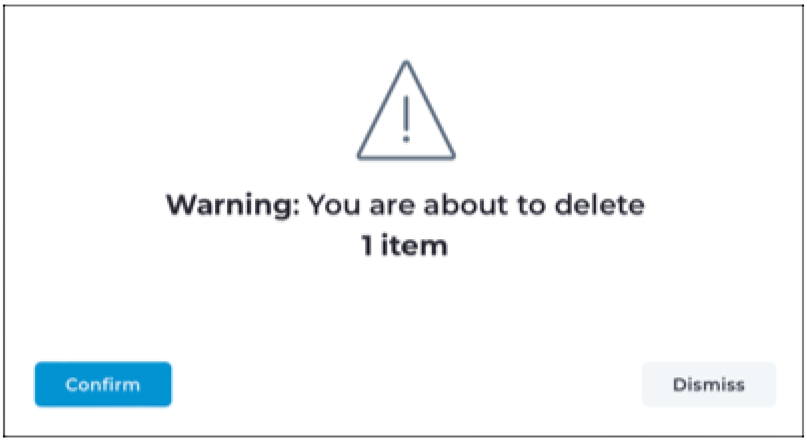
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Delete**.

   Warning: You are about to delete 1 item

   Result: A confirmation dialog shows.

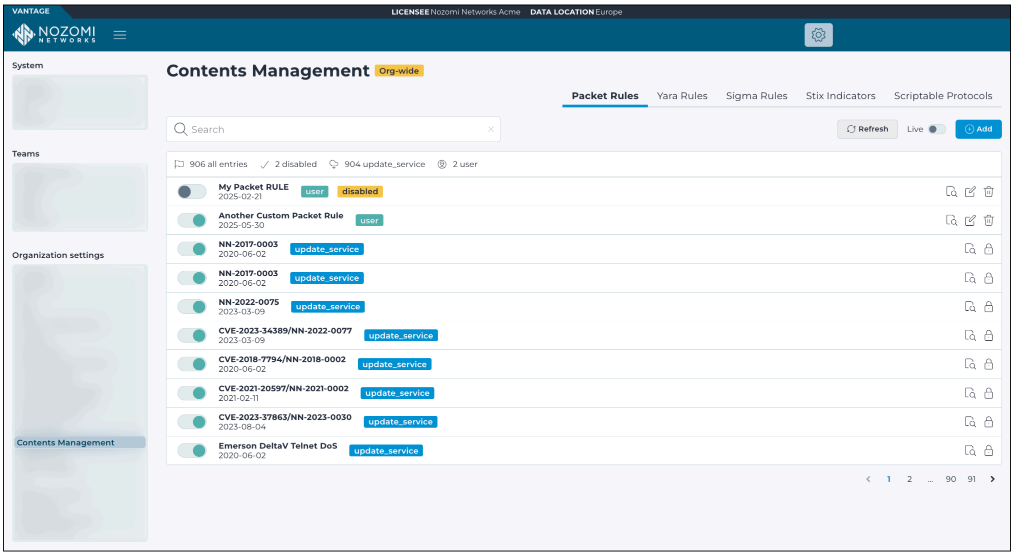
6. Select **Confirm**.

Results

The alert rule has been deleted.

Contents Management

*Use the **Contents Management** page to view, create, and manage detection content across the organization. Tabs organize content types such as packet rules, Yara rules, and Sigma rules. This interface helps streamline the application of threat detection logic in Vantage.*



Rule	Date	Tags
My Packet RULE	2025-02-21	user disabled
Another Custom Packet Rule	2025-05-30	user
NN-2017-0003	2020-06-02	update_service
NN-2017-0003	2020-06-02	update_service
NN-2022-0075	2023-03-09	update_service
CVE-2023-34389/NN-2022-0077	2023-03-09	update_service
CVE-2018-7794/NN-2018-0002	2020-06-02	update_service
CVE-2021-20597/NN-2021-0002	2021-02-11	update_service
CVE-2023-37863/NN-2023-0030	2023-08-04	update_service
Emerson DeltaV Telnet DoS	2020-06-02	update_service

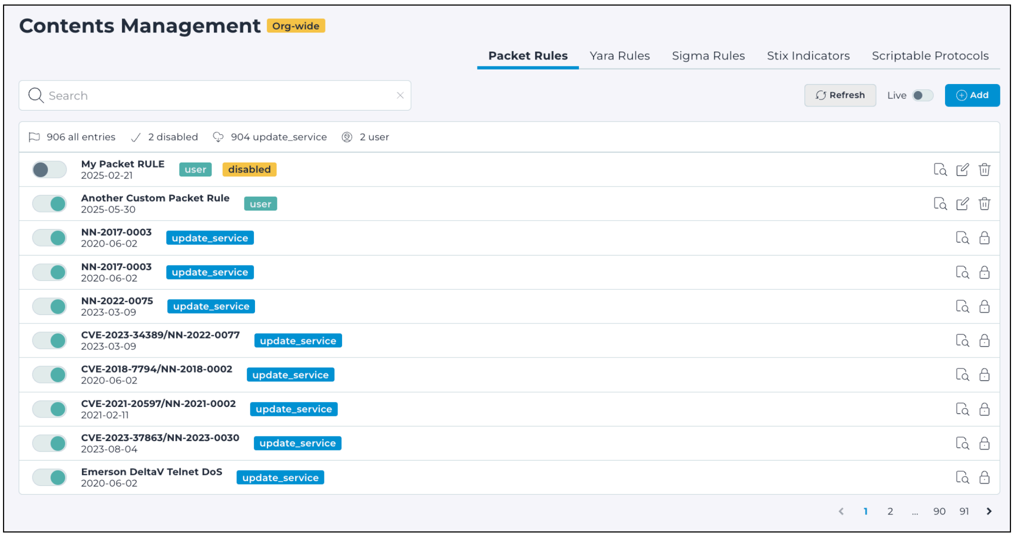
Figure 39. Contents Management page

The **Contents Management** page has these tabs:

- Packet Rules (on page 99)
- Yara Rules (on page 100)
- Sigma Rules (on page 101)
- Stix Indicators (on page 102)
- Scriptable Protocols (on page 103)

Packet Rules

Packet rules identify network traffic patterns and enable detection of specific behaviors or threats. Use this page to review, enable, disable, or add custom packet rules. Actions help tailor detection capabilities across the monitored environment.



Rule	Date	Tags
My Packet RULE	2025-02-21	user disabled
Another Custom Packet Rule	2025-05-30	user
NN-2017-0003	2020-06-02	update_service
NN-2017-0003	2020-06-02	update_service
NN-2022-0075	2023-03-09	update_service
CVE-2023-34389/NN-2022-0077	2023-03-09	update_service
CVE-2018-7794/NN-2018-0002	2020-06-02	update_service
CVE-2021-20597/NN-2021-0002	2021-02-11	update_service
CVE-2023-37863/NN-2023-0030	2023-08-04	update_service
Emerson DeltaV Telnet DoS	2020-06-02	update_service

Figure 40. Packet Rules page

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

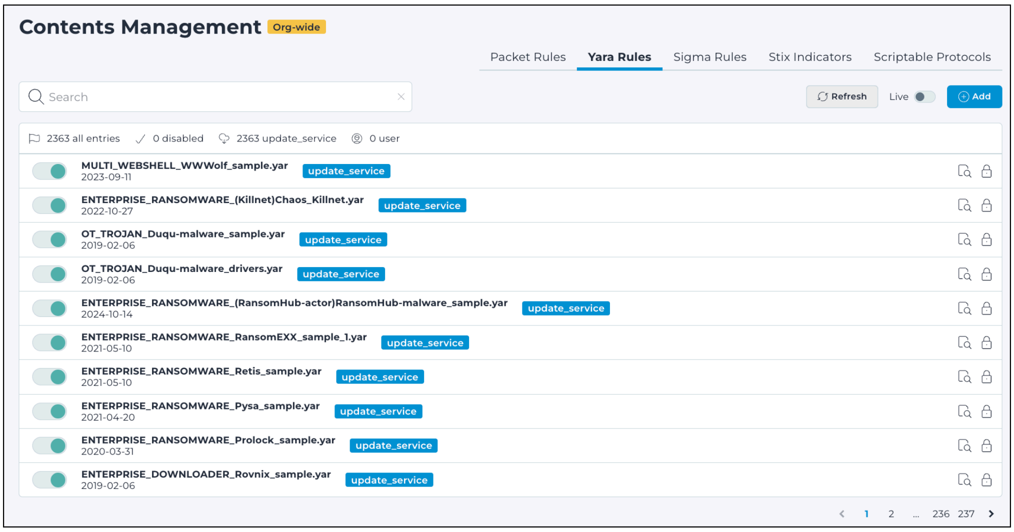
The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add

The **Add** button lets you add new content.

Yara Rules

Yara rules define patterns to identify malware or suspicious files based on textual or binary signatures. Use this page to view, update, and manage Yara detection logic across your organization. These rules match known indicators within file content to enhance threat detection.



2363 all entries 0 disabled 2363 update_service 0 user

MULTI_WEBSHELL_WWWolf_sample.yar 2023-09-11	update_service
ENTERPRISE_RANSOMWARE_(Killnet)Chaos_Killnet.yar 2022-10-27	update_service
OT_TROJAN_Duqu-malware_sample.yar 2019-02-06	update_service
OT_TROJAN_Duqu-malware_drivers.yar 2019-02-06	update_service
ENTERPRISE_RANSOMWARE_(RansomHub-actor)RansomHub-malware_sample.yar 2024-10-14	update_service
ENTERPRISE_RANSOMWARE_RansomEXX_sample_1.yar 2021-05-10	update_service
ENTERPRISE_RANSOMWARE_Retis_sample.yar 2021-05-10	update_service
ENTERPRISE_RANSOMWARE_Pysa_sample.yar 2021-04-20	update_service
ENTERPRISE_RANSOMWARE_Prolock_sample.yar 2020-03-31	update_service
ENTERPRISE_DOWNLOADER_Rovnix_sample.yar 2019-02-06	update_service

Figure 41. Yara Rules page

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

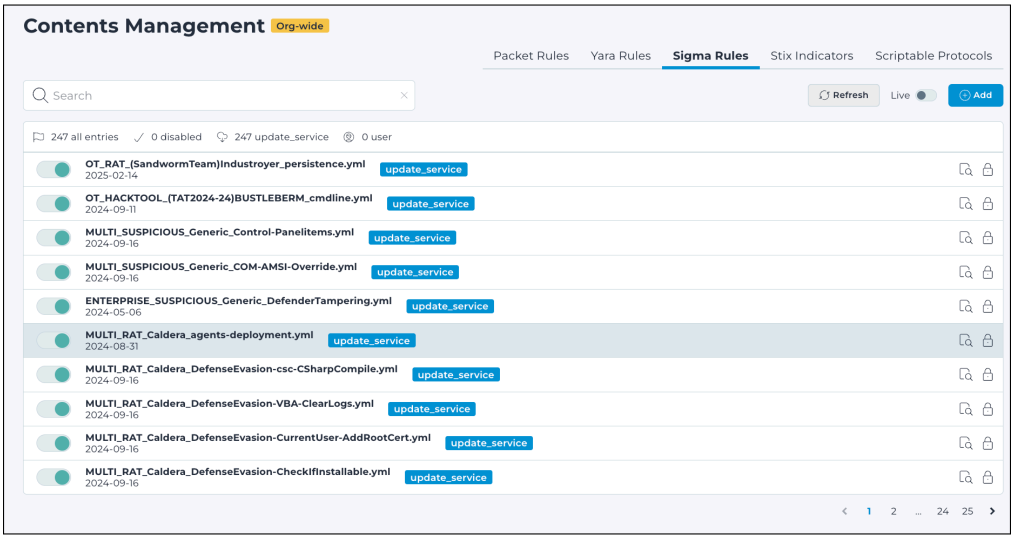
The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add

The **Add** button lets you add new content.

Sigma Rules

Sigma rules provide a standardized format for describing detection logic based on event logs. Use this page to manage Sigma rules that identify suspicious activity across log sources. These rules support consistent threat detection across heterogeneous environments.



247 all entries ✓ 0 disabled 247 update_service 0 user

OT_RAT_(SandwormTeam)Industroyer_persistence.yml 2025-02-14	update_service
OT_HACKTOOL_(TAT2024-24)BUSTLEBERM_cmdline.yml 2024-09-11	update_service
MULTI_SUSPICIOUS_Generic_Control-Panelitems.yml 2024-09-16	update_service
MULTI_SUSPICIOUS_Generic_COM-AMSI-Override.yml 2024-09-16	update_service
ENTERPRISE_SUSPICIOUS_Generic_DefenderTampering.yml 2024-05-06	update_service
MULTI_RAT_Caldera_agents-deployment.yml 2024-08-31	update_service
MULTI_RAT_Caldera_DefenseEvasion-csc-CSharpCompile.yml 2024-09-16	update_service
MULTI_RAT_Caldera_DefenseEvasion-VBA-ClearLogs.yml 2024-09-16	update_service
MULTI_RAT_Caldera_DefenseEvasion-CurrentUser-AddRootCert.yml 2024-09-16	update_service
MULTI_RAT_Caldera_DefenseEvasion-CheckIfInstallable.yml 2024-09-16	update_service

‹ 1 2 ... 24 25 ›

Figure 42. Sigma Rules page

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

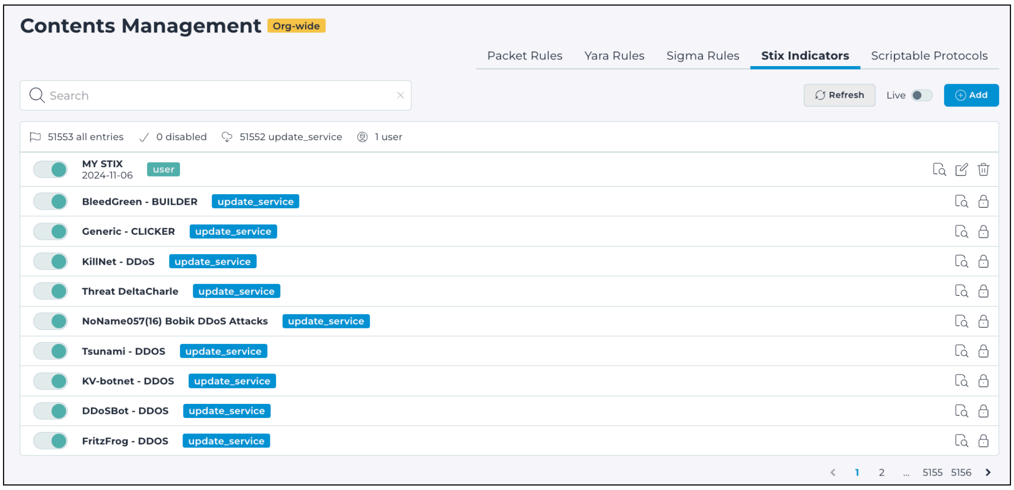
The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add

The **Add** button lets you add new content.

Stix Indicators

Stix indicators provide structured threat intelligence data to support automated detection of malicious activity. Use this page to view and manage indicators sourced from known attack patterns and threat actor behaviors. These indicators enhance visibility into emerging threats across your network.



51553 all entries ✓ 0 disabled 51552 update_service 1 user

MY STIX 2024-11-06	user	
BleedGreen - BUILDER	update_service	
Generic - CLICKER	update_service	
KillNet - DDoS	update_service	
Threat DeltaCharle	update_service	
NoName057(16) Bobik DDoS Attacks	update_service	
Tsunami - DDOS	update_service	
KV-botnet - DDOS	update_service	
DDoSBot - DDOS	update_service	
FritzFrog - DDOS	update_service	

Figure 43. Stix Indicators page

Refresh

The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

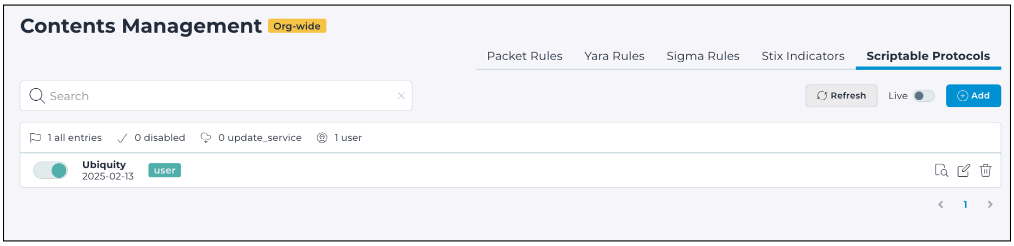
The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add

The **Add** button lets you add new content.

Scriptable Protocols

Scriptable protocols allow custom protocol behavior to be defined through scripting for specialized network communication. Use this page to view and manage uploaded scriptable protocol definitions. This enables flexible parsing and monitoring of non-standard or proprietary protocols in Vantage.



Contents Management Org-wide

Packet Rules | Yara Rules | Sigma Rules | Stix Indicators | Scriptable Protocols

Search

Refresh Live Add

1 all entries 0 disabled 0 update_service 1 user

Ubiquity 2025-02-13 user

‹ 1 ›

Figure 44. Scriptable Protocols page

Refresh

The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

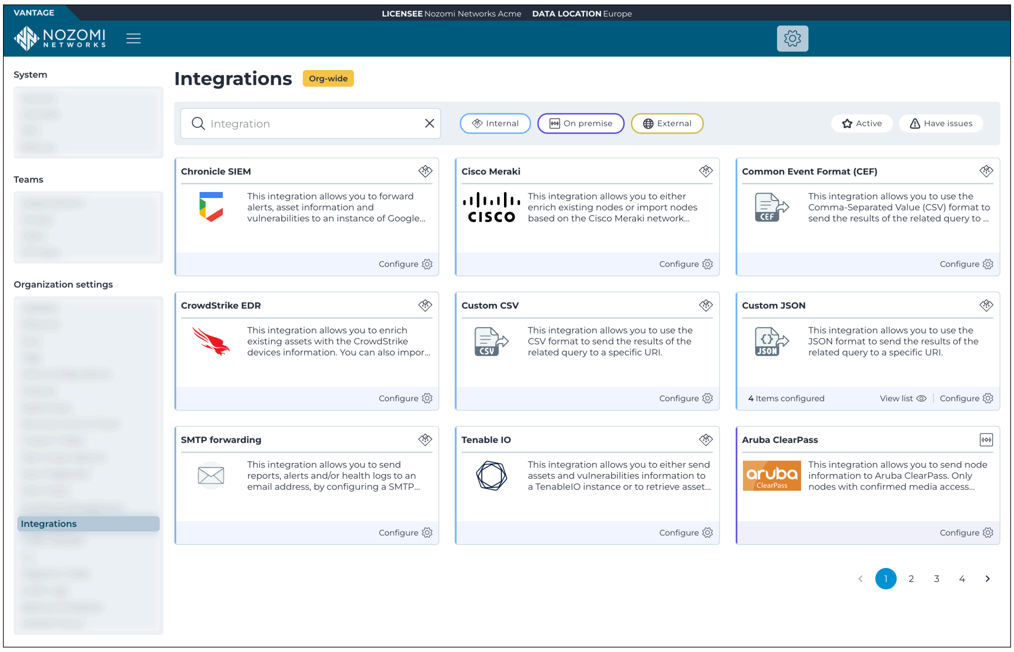
The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add

The **Add** button lets you add new content.

Integrations

*The **Integrations** page lets you use one of the available applications to connect an organization with a third-party application.*



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

Cisco Meraki — This integration allows you to either enrich existing nodes or import nodes based on the Cisco Meraki network...

Common Event Format (CEF) — This integration allows you to use the Comma-Separated Value (CSV) format to send the results of the related query to ...

CrowdStrike EDR — This integration allows you to enrich existing assets with the CrowdStrike devices information. You can also impor...

Custom CSV — This integration allows you to use the CSV format to send the results of the related query to a specific URI.

Custom JSON — This integration allows you to use the JSON format to send the results of the related query to a specific URI.

SMTP forwarding — This integration allows you to send reports, alerts and/or health logs to an email address, by configuring a SMTP...

Tenable IO — This integration allows you to either send assets and vulnerabilities information to a TenableIO instance or to retrieve asset...

Aruba ClearPass — This integration allows you to send node information to Aruba ClearPass. Only nodes with confirmed media access...

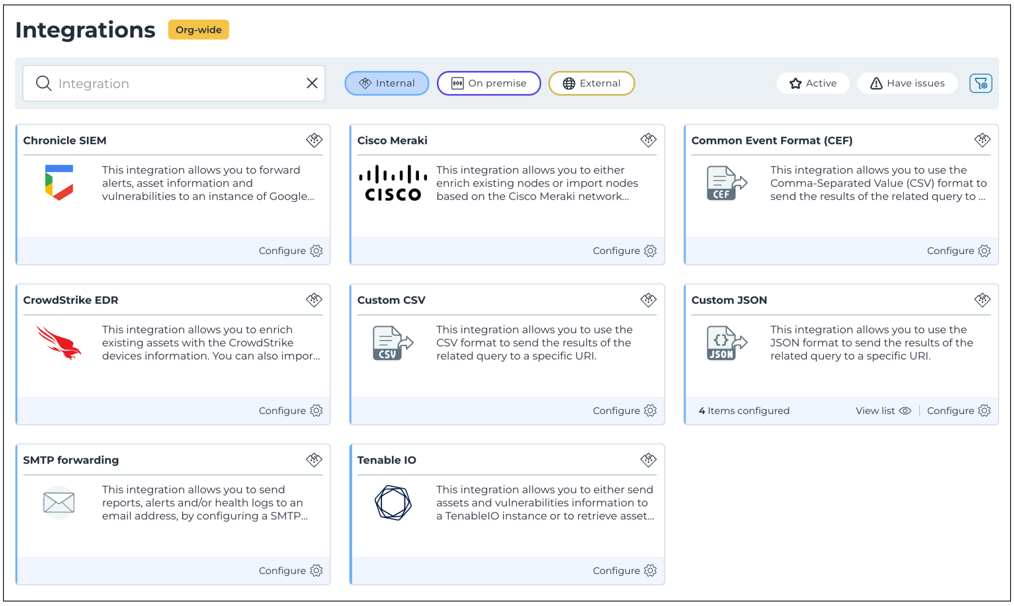
Figure 45. Integrations page

Vantage has these types of integrations:

- Internal integrations (on page 105)
- On premise integrations (on page 122)
- External integrations (on page 123)

Internal integrations

A description of the internal integrations page. These are integrations that you can configure in Vantage, to run in Vantage.



Integrations Org-wide

Integration ✕ Internal On premise External Active Have issues

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

Cisco Meraki
This integration allows you to either enrich existing nodes or import nodes based on the Cisco Meraki network...
Configure

Common Event Format (CEF)
This integration allows you to use the Comma-Separated Value (CSV) format to send the results of the related query to ...
Configure

CrowdStrike EDR
This integration allows you to enrich existing assets with the CrowdStrike devices information. You can also impor...
Configure

Custom CSV
This integration allows you to use the CSV format to send the results of the related query to a specific URI.
Configure

Custom JSON
This integration allows you to use the JSON format to send the results of the related query to a specific URI.
4 Items configured View list | Configure

SMTP forwarding
This integration allows you to send reports, alerts and/or health logs to an email address, by configuring a SMTP...
Configure

Tenable IO
This integration allows you to either send assets and vulnerabilities information to a TenableIO instance or to retrieve asset...
Configure

Figure 46. Internal integrations page

Search bar

This lets you use the integration name as a filter.

Internal

This button lets you show the internal integrations.

On premise

This button lets you show the on premise integrations.

External

This button lets you show the external integrations.

Active

This button lets you show only the integrations that have been configured at least once.

Have issues

This button lets you show only the integrations that show a minimum of one issue over all of their configurations.

Clear all filters button

The clear all filters icon lets you clear all filters that have previously been used.

View list

This button opens a page that lets you see a list of the related integrations.

Configure

This button opens the related configuration page.

Cisco Meraki

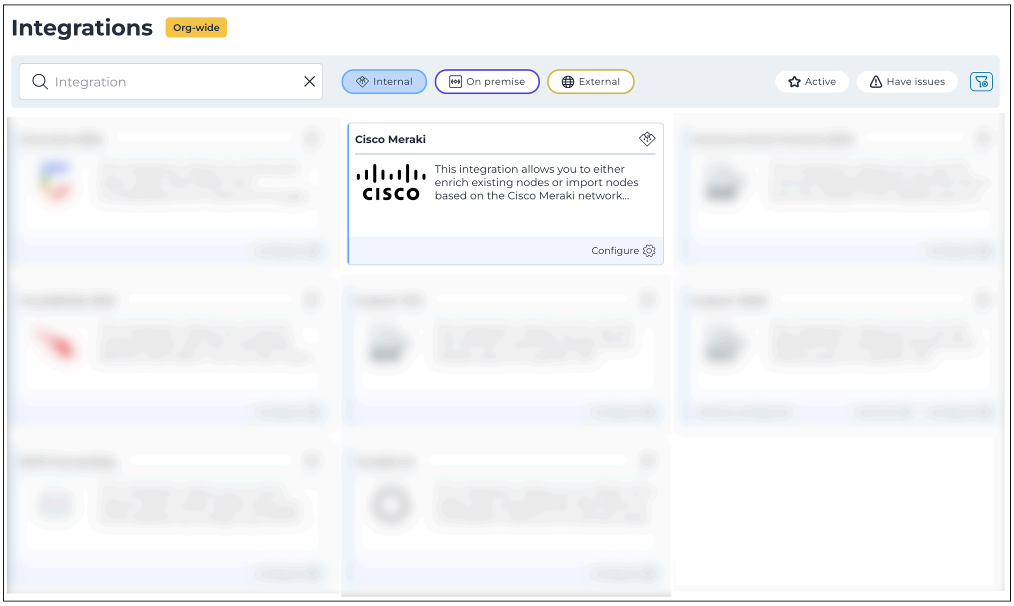
Overview

*This documentation describes the **Cisco Meraki** internal integration with Nozomi Networks Vantage.*

The **Cisco Meraki** integration lets you enrich existing nodes, or import nodes, based on Cisco Meraki network client information. It operates exclusively to enhance Nozomi Networks data with asset information from Cisco Meraki devices, without pushing data back to the Cisco Meraki device.

The asset information gathered through this integration is correlated with Vantage's Threat Intelligence. This provides valuable insights into vulnerabilities that affect assets that are connected to Cisco Meraki networks.

You can find the **Cisco Meraki** integration in ⚙ **> Integrations > Internal**.



This integration allows you to either enrich existing nodes or import nodes based on the Cisco Meraki network...

Figure 47. Internal integrations

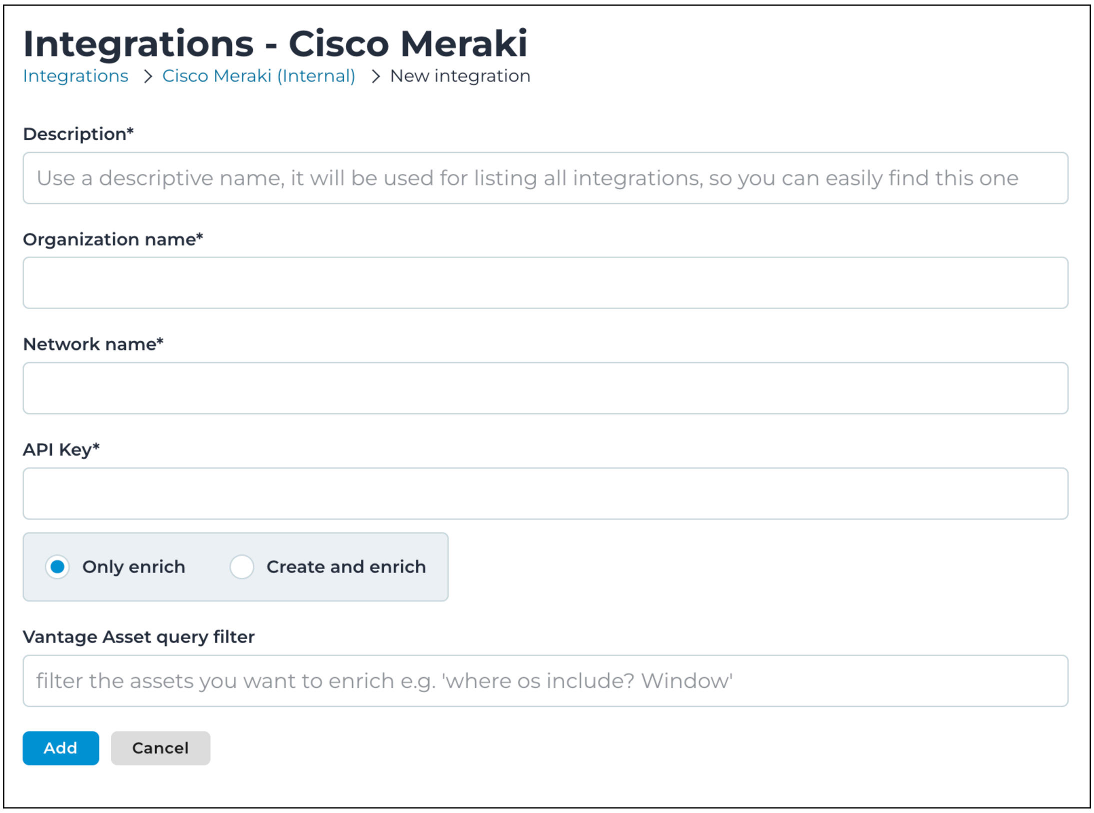
Configure the Cisco Meraki integration

*This task gives the necessary steps to configure the **Cisco Meraki** integration in your system. It helps you to select the necessary features, enter the required credentials, and apply the configuration to enhance asset enrichment.*

Procedure

1. Go to ⚙ **> Integrations > Internal > Cisco Meraki**.
2. In the bottom right corner, select **Configure**.

   Result: The **Cisco Meraki** integration settings page opens.
3. In the **Description** field, enter details that will help you to easily identify it in the future.



Integrations - Cisco Meraki

Integrations > Cisco Meraki (Internal) > New integration

Description*

Use a descriptive name, it will be used for listing all integrations, so you can easily find this one

Organization name*

Network name*

API Key*

● Only enrich ○ Create and enrich

Vantage Asset query filter

filter the assets you want to enrich e.g. 'where os include? Window'

4. In the **Organization name** field, enter a name for the organization.
   This is a key identifier in the Meraki dashboard and is used to group and manage networks under a single administrative entity. It serves as the top-level container within the Meraki dashboard hierarchy, and it is typically associated with a business, institution, or organization that manages Meraki devices.

5. In the **Network name** field, enter a name for the network.
   This is a specific collection of devices and configurations within an organization. It is a unique identifier for a group of Meraki devices, such as switches, access points, cameras, or firewalls that are managed as a single entity within the Meraki dashboard.
6. In the **API Key** field, enter the *API* key.
   This is a unique, secret key that is associated with a Meraki dashboard account. It is used to authenticate and authorize access to the Meraki dashboard *API*. This allows users, or systems, to programmatically interact with, and manage Meraki devices and configurations.
7. Choose an option:

   Choose from:
   - **Only enrich**
   - **Create and enrich**
8. If you chose **Create and enrich**, select a sensor from the dropdown.
9. **Optional:** Use the **Vantage Asset query filter** to filter the assets you would like to enrich.
   For example, you can use a query such as: **where os include? Windows**
   To make sure that your query is correct, you can use the **Queries** section to check and validate the query before you apply it to asset enrichment.

   > **Note:**
   > You can only filter Vantage assets if the **Create and enrich** option is not selected. If it is selected, you can only use Meraki filters.

10. To apply the configuration, select **Add**.

CrowdStrike

Overview

*This documentation describes the **CrowdStrike EDR** integration with Nozomi Networks Vantage.*

The **CrowdStrike EDR** integration lets you enrich existing assets in Nozomi Networks Vantage. It also lets you create the CrowdStrike assets that are not yet present in Vantage.

You can find the **CrowdStrike EDR** integration in ⚙ **> Integrations > Internal**.

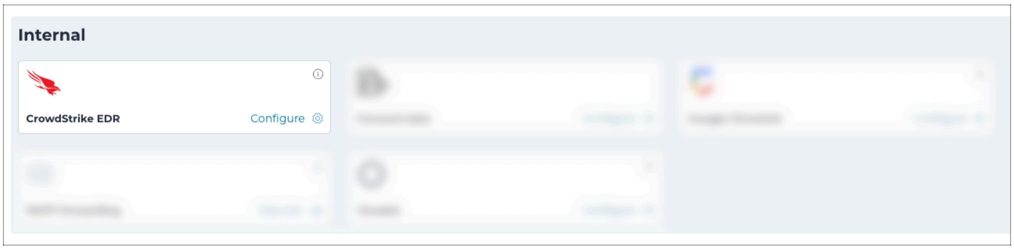


Figure 48. Internal integrations

Requirements

*The requirements for the **CrowdStrike EDR** integration.*

To do the **CrowdStrike EDR** integration, you will need this information, the:

- Endpoint
- Client ID
- Client secret

Note:

To generate Client ID and Client secret, you should use these permissions:

- HOSTS
- HOST GROUPS
- ASSETS

Configure the CrowdStrike EDR integration

*This task gives the necessary steps to configure the **CrowdStrike EDR** integration in your system. It helps you to select the necessary features, enter the required credentials, and apply the configuration to enhance asset enrichment.*

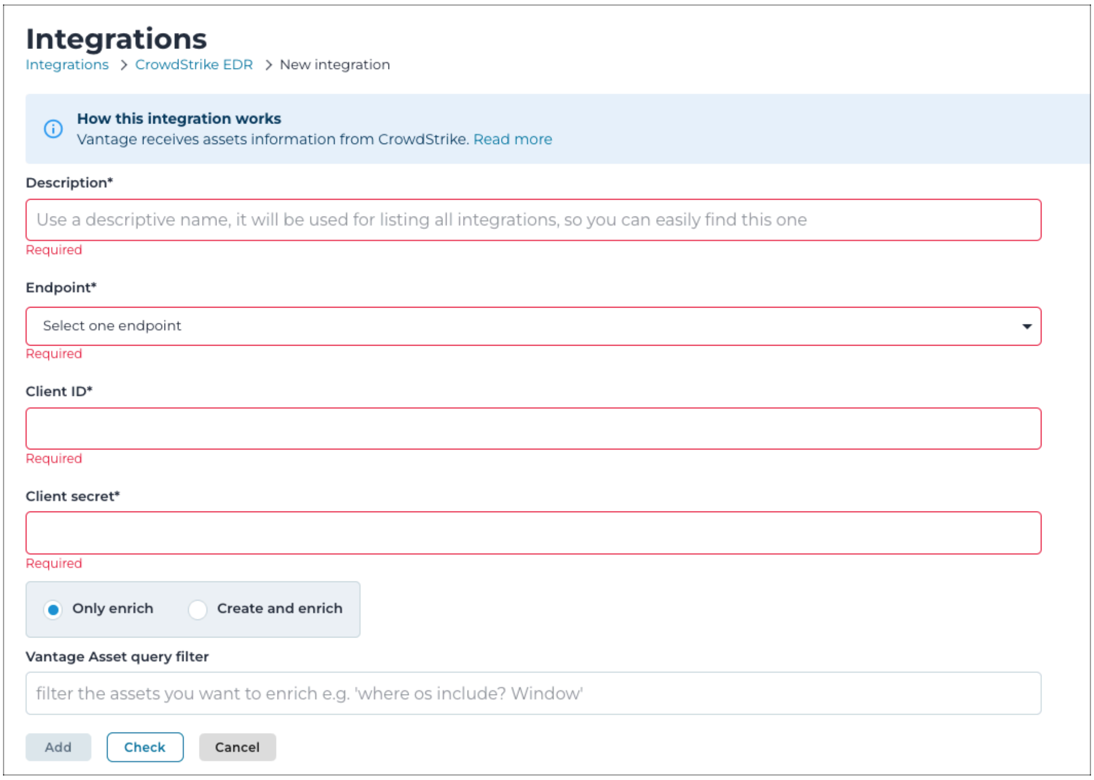
Before you begin

In the **Administration > Features** section, select the **Preview experimental and preview** features checkbox.

Procedure

1. Go to ⚙ **> Integrations > Internal > CrowdStrike EDR**.
2. In the bottom right corner, select **Configure**.

   Result: The **CrowdStrike EDR** integration settings page opens.
3. In the **Description** field, enter details that will help you to easily identify it in the future.



Integrations

Integrations > CrowdStrike EDR > New integration

How this integration works
Vantage receives assets information from CrowdStrike. Read more

Description*
Use a descriptive name, it will be used for listing all integrations, so you can easily find this one
Required

Endpoint*
Select one endpoint
Required

Client ID*
Required

Client secret*
Required

● Only enrich ○ Create and enrich

Vantage Asset query filter
filter the assets you want to enrich e.g. 'where os include? Window'

4. From the **Endpoint** dropdown, select the appropriate CrowdStrike endpoint.
5. In the **Client ID** field, enter the CrowdStrike client ID.
6. In the **Client secret** field, enter the CrowdStrike client secret.

7. Choose an option:

   Choose from:

   - **Only enrich**
   - **Create and enrich**
8. If you chose **Create and enrich**, enter details in the **CrowdStrike query filter**.
9. **Optional:** Use the **Vantage Asset query filter** to filter the assets you would like to enrich.

   For example, you can use a query such as: **where assets include? Windows.**

   To make sure that your query is correct, you can use the **Queries** section to check and validate the query before you apply it to asset enrichment.

   > **Note:**
   > You can only filter Vantage assets if the **Create and enrich** option is not selected. If it is selected, you can only use CrowdStrike filters.

10. To apply the configuration, select **Add**.

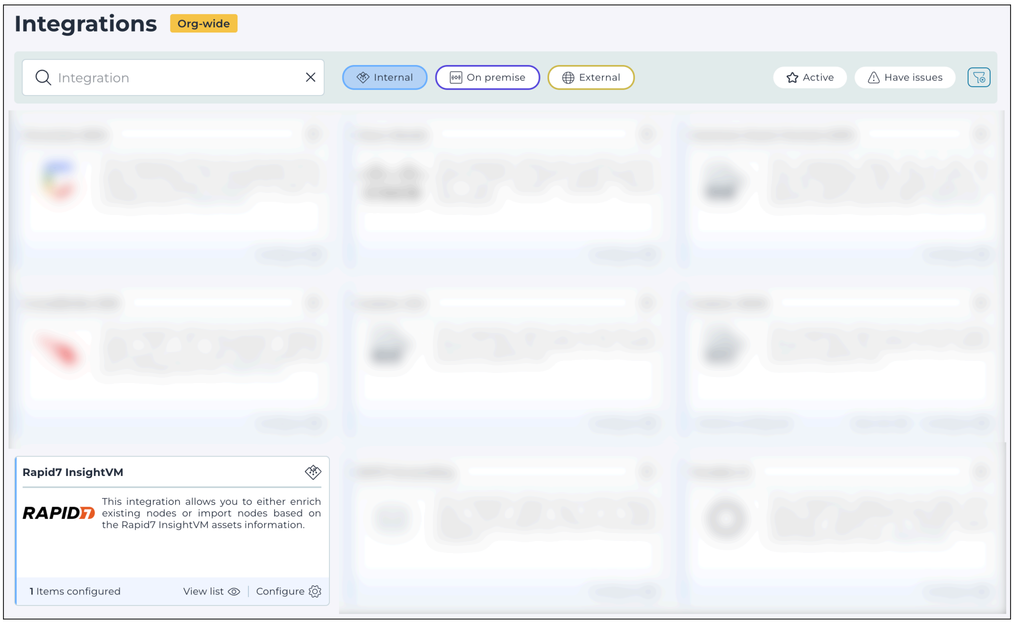
Rapid7 InsightVM

Overview

*This documentation describes the **Rapid7 InsightVM** internal integration with Nozomi Networks Vantage.*

The **Rapid7 InsightVM** integration lets you enrich existing nodes, or import nodes, based on **Rapid7 InsightVM** assets information.

You can find the **Rapid7 InsightVM** integration in ⚙ **> Integrations > Internal**.



This integration allows you to either enrich existing nodes or import nodes based on the Rapid7 InsightVM assets information.

Figure 49. Internal integrations

Configure the Rapid7 InsightVM integration

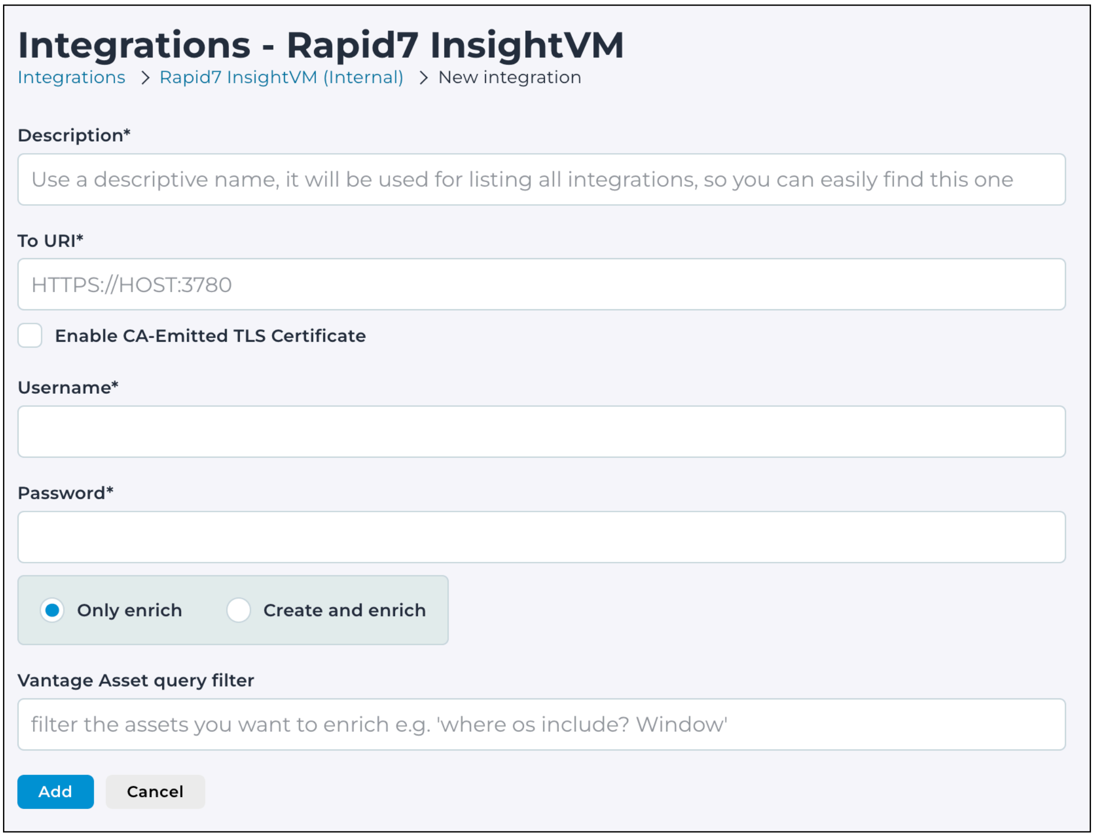
*This task gives the necessary steps to configure the **Rapid7 InsightVM** integration in your system. It helps you to select the necessary features, enter the required credentials, and apply the configuration to enhance asset enrichment.*

Procedure

1. Go to ⚙ **> Integrations > Internal > Rapid7 InsightVM**.
2. In the bottom right corner, select **Configure**.

   Result: The **Rapid7 InsightVM** integration settings page opens.

3. In the **Description** field, enter details that will help you find the integration again.



Integrations - Rapid7 InsightVM

Integrations > Rapid7 InsightVM (Internal) > New integration

Description*

Use a descriptive name, it will be used for listing all integrations, so you can easily find this one

To URI*

HTTPS://HOST:3780

□ Enable CA-Emitted TLS Certificate

Username*

Password*

● Only enrich ○ Create and enrich

Vantage Asset query filter

filter the assets you want to enrich e.g. 'where os include? Window'

Add Cancel

4. In the **To URI** field, enter the host *uniform resource identifier (URI)* information.
5. In the **Username** field, enter your username.
6. In the **Password** field, enter your password.
7. Choose an option:

   Choose from:

   - **Only enrich**
   - **Create and enrich**

8. If you chose **Create and enrich**, select a sensor from the dropdown.

9. **Optional:** Use the **Vantage Asset query filter** to filter the assets you would like to enrich.

   For example, you can use a query such as: **where os include? Windows**

   To make sure that your query is correct, you can use the **Queries** section to check and validate the query before you apply it to asset enrichment.

   > **Note:**
   > You can only filter Vantage assets if the **Create and enrich** option is not selected.

10. To apply the configuration, select **Add**.

Tenable

Tenable data integration

A description of how the Tenable data integration for Vantage works.

Send assets

This integration sends assets information stored in Vantage to a TenableIO instance.

> **Note:**
>
> Only assets that have a confirmed *MAC* address are taken into consideration.

The asset information that follows is sent to TenableIO:

- `ip`
- `mac_address`
- `os`
- `name`
- `type` (mapped to TenableIO system type: router, embedded, and general-purpose)
- `cpe` (having a likelihood greater or equal to 0.7)

The source value, which can be used to filter assets on TenableIO, used to import the assets on TenableIO is 'External Source - ' concatenated with the description specified when creating the integration.

Send vulnerabilities

The Tenable integration sends asset vulnerabilities stored in Vantage to a TenableIO instance when **Enable sending Asset Vulnerabilities** is selected. Vulnerabilities are sent if they match the following requirements:

- They refer to an asset having an *IP* address
- They have a likelihood value greater than, or equal to 0.7
- They are unresolved
- The *CVE* identifier must be accepted by at least one of the TenableIO Plugins
- There is a match between the `Asset vendor` and `Matching cpes` fields with the Tenable Plugin `xref` and `cpe` fields. In the case of the , only the vendor information is used. If multiple plugins match, Vantage sends them all. The accuracy value submitted in the `Plugin Output` is 90%.

- There is a match between the `Asset vendor` or `Matching cpes` fields with the Tenable Plugin `xref` or `cpe` fields. In the case of the , only the vendor information is used. If multiple plugins match, Vantage sends those that match *s*. If they do not match by *s*, Vantage uses the vendor information instead. If there are several that match, Vantage sends all the matching plugins. For example, Vantage sends only those that match *s*, or those that match the vendor, but not both. The accuracy value submitted in the `Plugin Output` is 60%.
- There is no match between the `Asset vendor` or `Matching cpes` fields with the Tenable Plugin `xref` or `cpe` fields. In the case of the , only the vendor information is used. None are sent, unless only one plugin is available. The accuracy value submitted in the `Plugin Output` is 5%.

The vulnerabilities information that follows is sent to TenableIO:

- `cve`
- `time`

The output value of the TenableIO Plugin is set to `Imported from`, concatenated with the source value, and the accuracy value - as defined in the Send vulnerabilities (on page 116) section above.

Enrich assets

This integration lets you enrich existing assets that are stored in Vantage with information from TenableIO assets.

Note:

Only assets which have a confirmed *MAC* address are taken in consideration.

These fields are enriched:

- `label`
- `os`
- `mac_address`

Note:

The enrichment is performed only if the TenableIO asset is composed of a single:

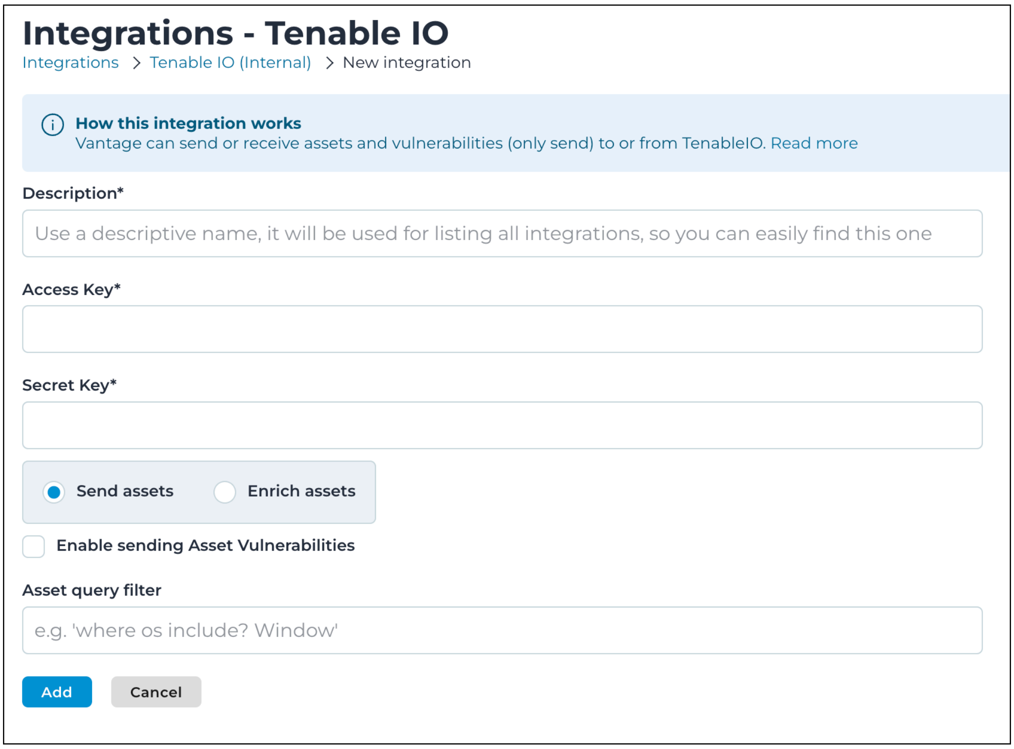
- *IP* address
- *MAC* address
- *operating system (OS)*, or
- Label

Edit configuration

It is possible to edit an existing integration configuration.

You can edit these fields:

- Access Key
- Secret Key
- Asset query
- Scan name



Integrations - Tenable IO

Integrations > Tenable IO (Internal) > New integration

How this integration works
Vantage can send or receive assets and vulnerabilities (only send) to or from TenableIO. Read more

Description*

Use a descriptive name, it will be used for listing all integrations, so you can easily find this one

Access Key*

Secret Key*

● Send assets ○ Enrich assets

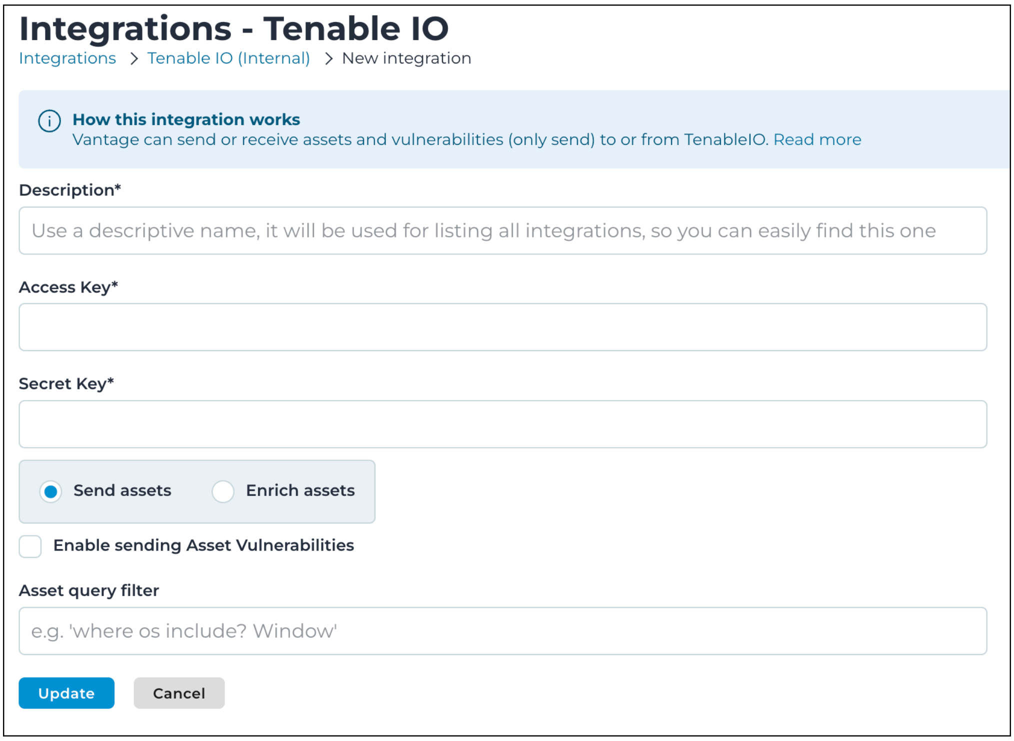
□ Enable sending Asset Vulnerabilities

Asset query filter

e.g. 'where os include? Window'

Figure 50. Edit configuration fields

Once you have updated the fields, you can select **Update**.



Integrations - Tenable IO

Integrations > Tenable IO (Internal) > New integration

How this integration works
Vantage can send or receive assets and vulnerabilities (only send) to or from TenableIO. Read more

Description*: Use a descriptive name, it will be used for listing all integrations, so you can easily find this one

Access Key*:

Secret Key*:

● Send assets ○ Enrich assets

□ Enable sending Asset Vulnerabilities

Asset query filter: e.g. 'where os include? Window'

Figure 51. Update integrations

Requirements

The necessary access and permissions that are required to configure the Tenable integration.

The Tenable integration requires:

- An **Access Key** with at least `SCAN MANAGER [40]` user permissions and `CAN EDIT [64]` scan permissions
- A **Secret Key** with at least `SCAN MANAGER [40]` user permissions and `CAN EDIT [64]` scan permissions

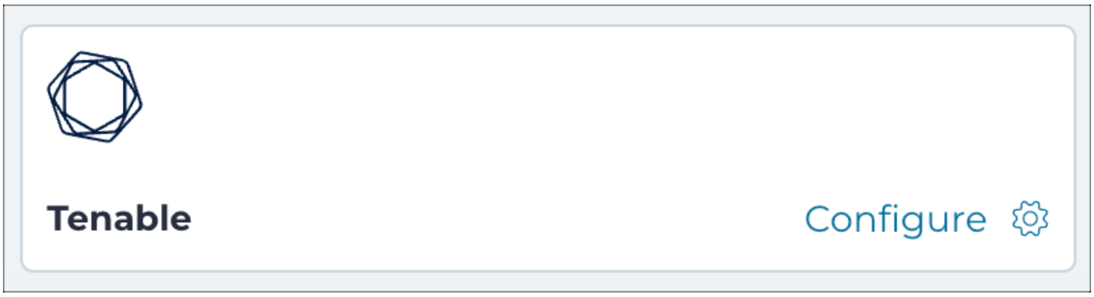
If the integration is configured to also send asset vulnerabilities, then you need to set user permissions to `ADMINISTRATOR [64]`.

Configure the Tenable integration

This task provides detailed steps to configure the Tenable integration. This includes setting up asset vulnerabilities, entering necessary information, and enabling experimental features if required.

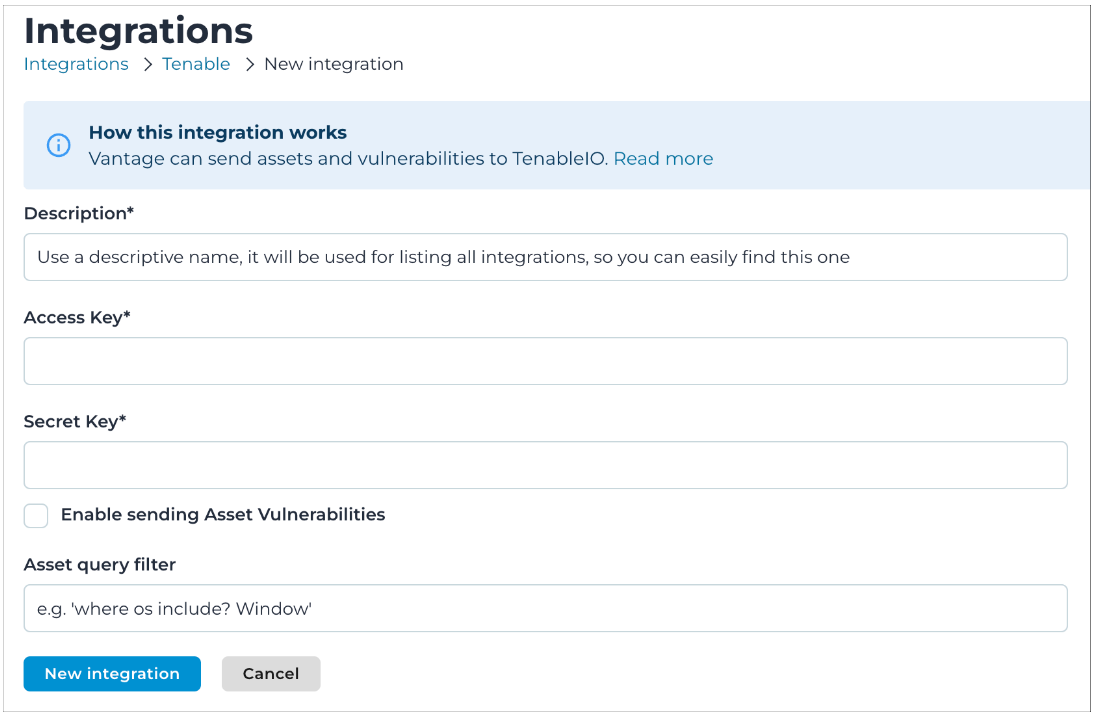
Procedure

1. Select **Administration**.



Result: Integrations and Tenable integration will show inside the **Internal integration** group.

2. Select **Configure**.



Integrations

Integrations > Tenable > New integration

How this integration works
Vantage can send assets and vulnerabilities to TenableIO. Read more

Description*

Use a descriptive name, it will be used for listing all integrations, so you can easily find this one

Access Key*

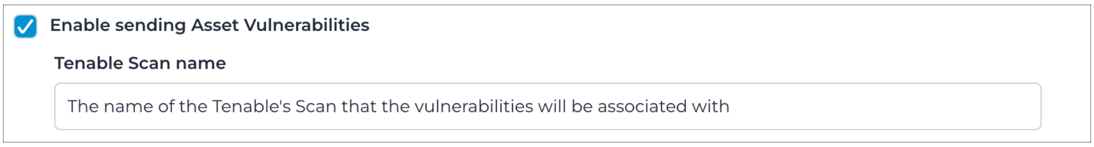
Secret Key*

□ **Enable sending Asset Vulnerabilities**

Asset query filter

e.g. 'where os include? Window'

3. If **Enable sending Asset Vulnerabilities** is selected, enter the **Tenable Scan name** that will be used when importing vulnerabilities. That scan must exist in Tenable and must have been started at least once.



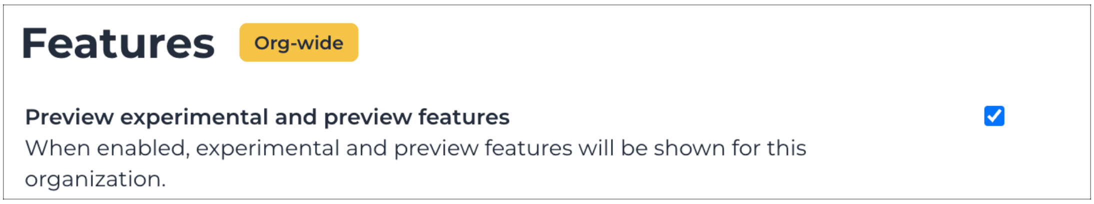
☑ Enable sending Asset Vulnerabilities

Tenable Scan name

The name of the Tenable's Scan that the vulnerabilities will be associated with

4. **Optional:**

   Asset Vulnerabilities is an experimental feature. To use it, you must go to **Organization settings > Features** and select **Preview experimental and preview features**.



Features Org-wide

Preview experimental and preview features ☑

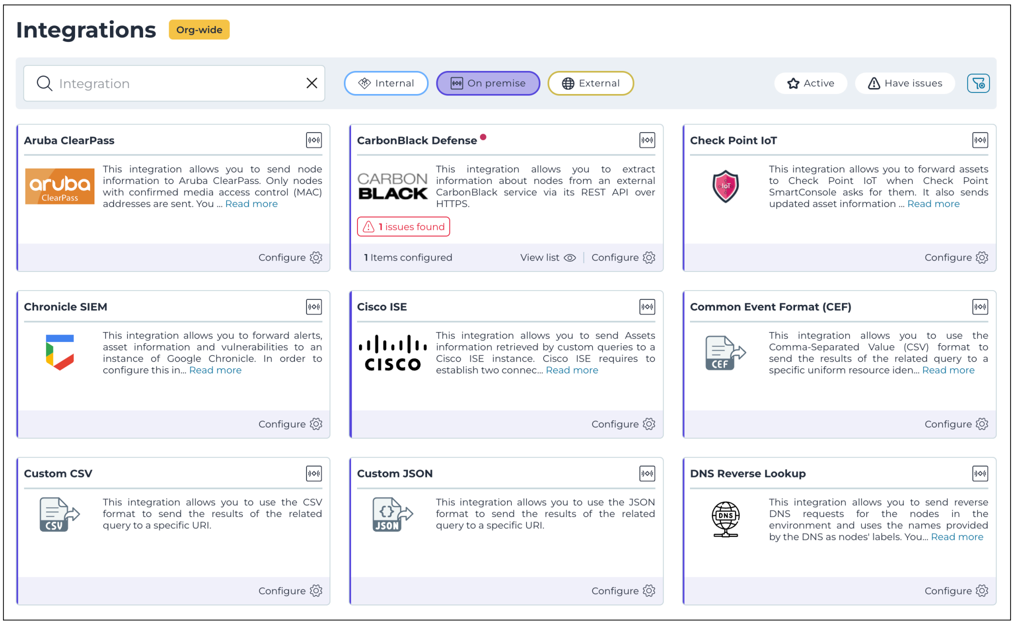
When enabled, experimental and preview features will be shown for this organization.

5. Enter the information in the applicable fields, as necessary.
6. Select **New integration**.

On premise

On premise integrations

A description of the on premise integrations page. These are integrations that you can configure from Vantage for local sensors.



Aruba ClearPass
This integration allows you to send node information to Aruba ClearPass. Only nodes with confirmed media access control (MAC) addresses are sent. You ... Read more

CarbonBlack Defense
This integration allows you to extract information about nodes from an external CarbonBlack service via its REST API over HTTPS.

Check Point IoT
This integration allows you to forward assets to Check Point IoT when Check Point SmartConsole asks for them. It also sends updated asset information ... Read more

Chronicle SIEM
This integration allows you to forward alerts, asset information and vulnerabilities to an instance of Google Chronicle. In order to configure this in... Read more

Cisco ISE
This integration allows you to send Assets information retrieved by custom queries to a Cisco ISE instance. Cisco ISE requires to establish two connec... Read more

Common Event Format (CEF)
This integration allows you to use the Comma-Separated Value (CSV) format to send the results of the related query to a specific uniform resource iden... Read more

Custom CSV
This integration allows you to use the CSV format to send the results of the related query to a specific URI.

Custom JSON
This integration allows you to use the JSON format to send the results of the related query to a specific URI.

DNS Reverse Lookup
This integration allows you to send reverse DNS requests for the nodes in the environment and uses the names provided by the DNS as nodes' labels. You... Read more

Figure 52. On premise integrations page

In Vantage, it is possible to configure integrations on local sensors. If you select the checkbox in ⚙ **> Organization settings > Sync > Data integrations**, you will see a list of integrations configured on sensors that Vantage has grouped by integration type.

Search bar

This lets you use the integration name as a filter.

Internal

This button lets you show the internal integrations.

On premise

This button lets you show the on premise integrations.

External

This button lets you show the external integrations.

Active

This button lets you show only the integrations that have been configured at least once.

Have issues

This button lets you show only the integrations that show a minimum of one issue over all of their configurations.

View list

This button opens a page that lets you see a list of the related integrations.

Configure

This button opens the related configuration page.

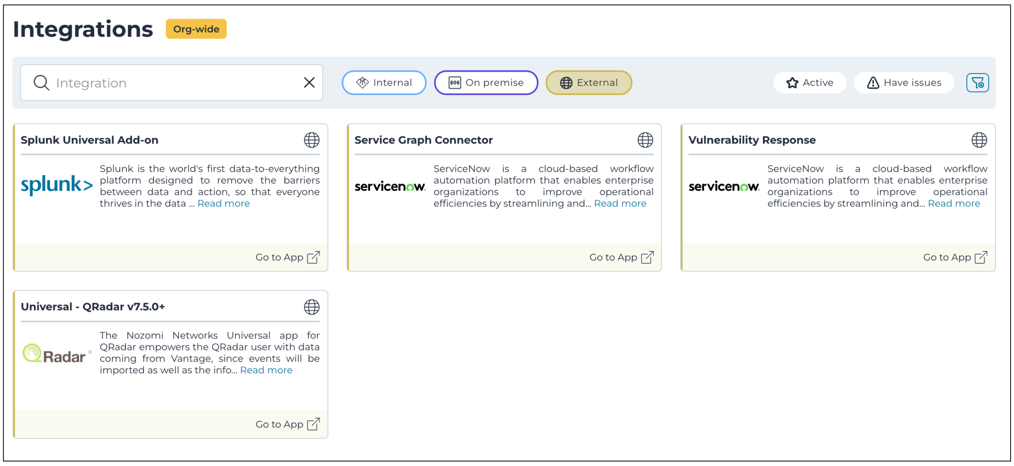
Available integrations

For more details about integrations available in Guardian, see the **Data integration** section in the **Guardian - Administrator Guide**.

For more details about integrations available in *CMC*, see the **Data integration** section in the **CMC - Administrator Guide**.

External integrations

A description of the external integrations page. External integrations are integrations that you can configure in an external system.



Splunk Universal Add-on

Splunk is the world's first data-to-everything platform designed to remove the barriers between data and action, so that everyone thrives in the data ... Read more

Go to App

Service Graph Connector

ServiceNow is a cloud-based workflow automation platform that enables enterprise organizations to improve operational efficiencies by streamlining and... Read more

Go to App

Vulnerability Response

ServiceNow is a cloud-based workflow automation platform that enables enterprise organizations to improve operational efficiencies by streamlining and... Read more

Go to App

Universal - QRadar v7.5.0+

The Nozomi Networks Universal app for QRadar empowers the QRadar user with data coming from Vantage, since events will be imported as well as the info... Read more

Go to App

Figure 53. External integrations page

Search bar

This lets you use the integration name as a filter.

Internal

This button lets you show the internal integrations.

On premise

This button lets you show the on premise integrations.

External

This button lets you show the external integrations.

Active

This button lets you show only the integrations that have been configured at least once.

Have issues

This button lets you show only the integrations that show a minimum of one issue over all of their configurations.

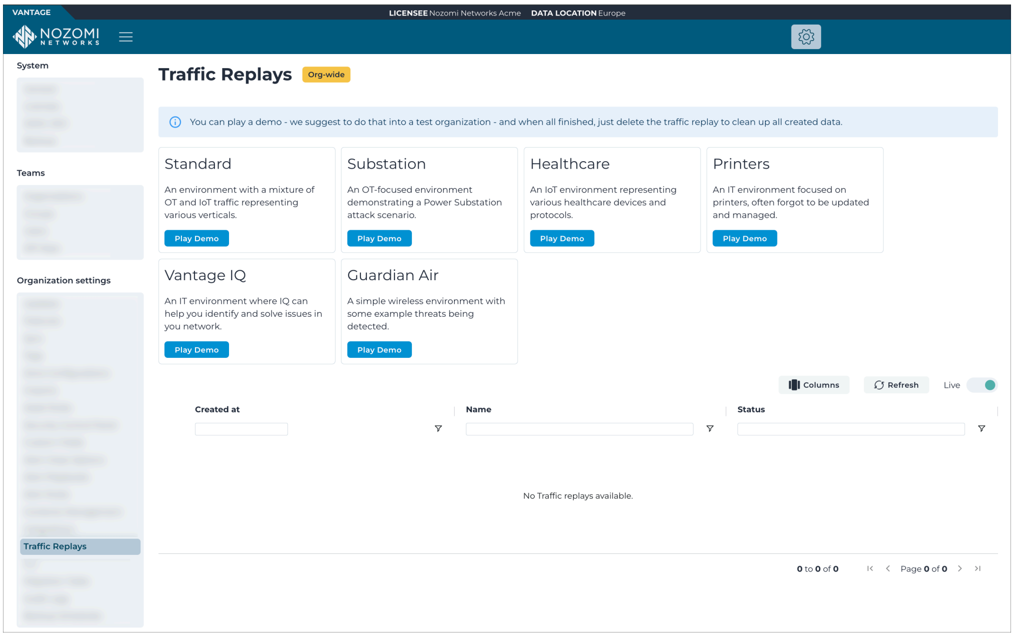
Go to App

This button opens the correct external page for the related Nozomi Networks application.

For more details about external Vantage integrations, see **Integration Guides**.

Traffic Replays

*The **Traffic Relays** page lets you load demonstration data into your environment so that you can test various features and explore Vantage. Nozomi Networks provides several traffic replays, which demonstrate different scenarios, such as an OT-focused Power Station attack.*



VANTAGE

LICENSEE Nozomi Networks Acme DATA LOCATION Europe

System

Teams

Organization settings

Traffic Replays

Traffic Replays Org-wide

You can play a demo - we suggest to do that into a test organization - and when all finished, just delete the traffic replay to clean up all created data.

Standard
An environment with a mixture of OT and IoT traffic representing various verticals.
Play Demo

Substation
An OT-focused environment demonstrating a Power Substation attack scenario.
Play Demo

Healthcare
An IoT environment representing various healthcare devices and protocols.
Play Demo

Printers
An IT environment focused on printers, often forgot to be updated and managed.
Play Demo

Vantage IQ
An IT environment where IQ can help you identify and solve issues in you network.
Play Demo

Guardian Air
A simple wireless environment with some example threats being detected.
Play Demo

Columns Refresh Live

Created at	Name	Status

No Traffic replays available.

0 to 0 of 0 Page 0 of 0

Figure 54. Traffic Replays page

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

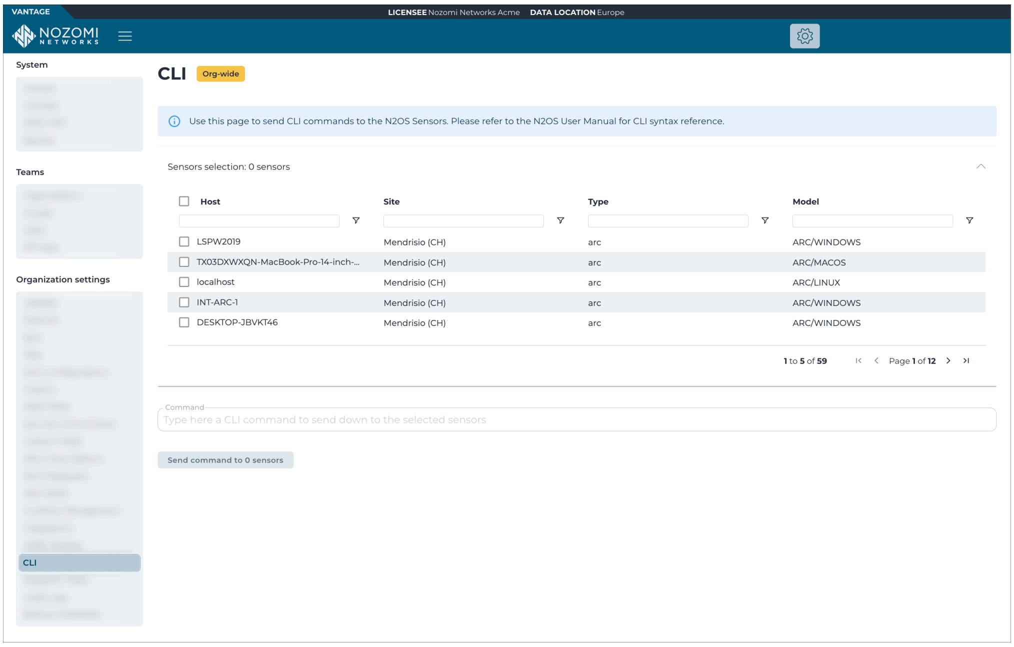
The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

CLI

*The **CLI** page lets you select sensors and use the text field to enter a command to execute. Vantage shows the output of sensors in the web UI.*



Use this page to send CLI commands to the N2OS Sensors. Please refer to the N2OS User Manual for CLI syntax reference.

Sensors selection: 0 sensors

☐ Host	Site	Type	Model
☐ LSPW2019	Mendrisio (CH)	arc	ARC/WINDOWS
☐ TX03DXWXQN-MacBook-Pro-14-inch-...	Mendrisio (CH)	arc	ARC/MACOS
☐ localhost	Mendrisio (CH)	arc	ARC/LINUX
☐ INT-ARC-1	Mendrisio (CH)	arc	ARC/WINDOWS
☐ DESKTOP-JBVKT46	Mendrisio (CH)	arc	ARC/WINDOWS

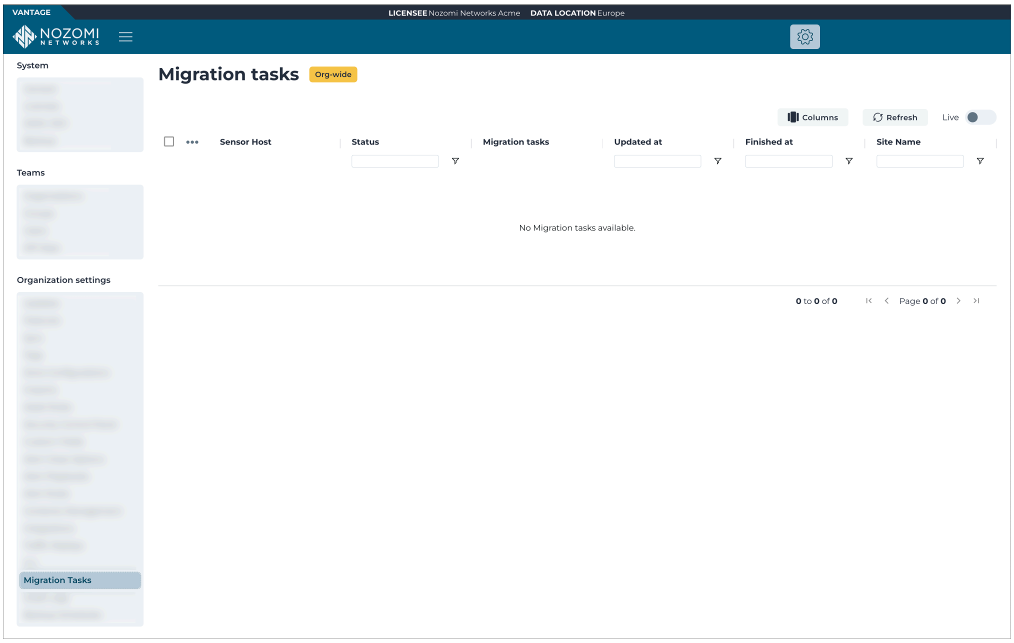
1 to 5 of 59 Page 1 of 12

Command: Type here a CLI command to send down to the selected sensors

Figure 55. CLI page

Migration tasks

*The **Migration tasks** page lets you update your Vantage instance and downstream sensors to adapt to changes in new versions of N2OS.*



□	Sensor Host	Status	Migration tasks	Updated at	Finished at	Site Name

No Migration tasks available.

0 to 0 of 0 Page 0 of 0

Figure 56. Migration tasks page

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

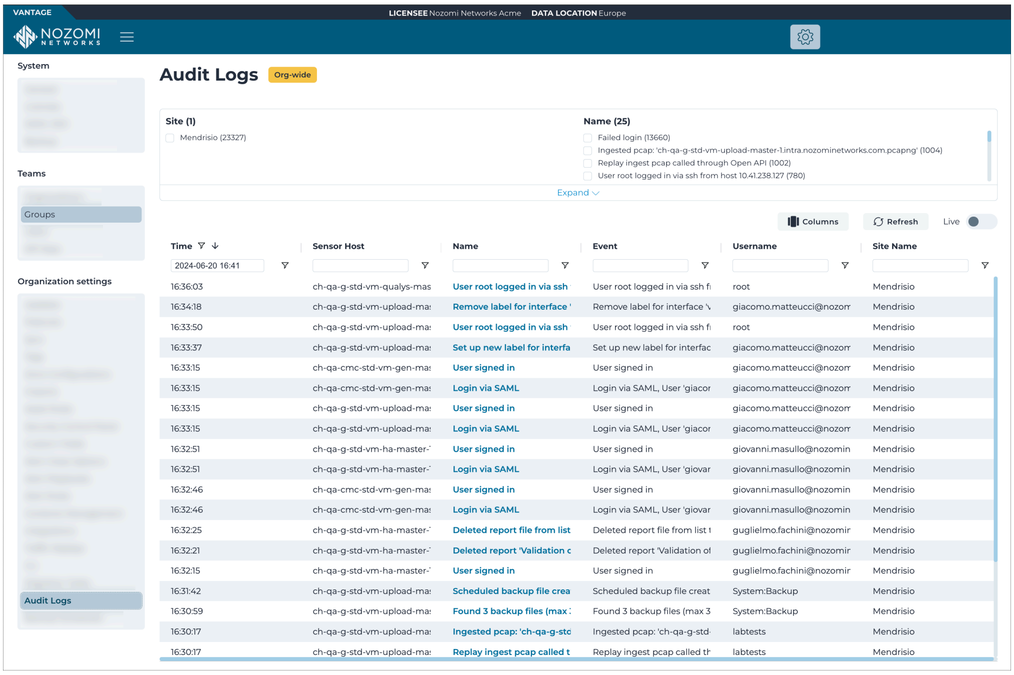
The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Audit Logs

*The **Audit Logs** page shows detailed operational information about your sensors and the activities that they monitor.*



Audit Logs

Site (1)

- □ Mendrisio (23327)

Name (25)

- □ Failed login (13660)
- □ Ingested pcap: 'ch-qa-g-std-vm-upload-master-1.intra.nozominetworks.com.pcapng' (1004)
- □ Replay ingest pcap called through Open API (1002)
- □ User root logged in via ssh from host 10.41.238.127 (780)

Time	Sensor Host	Name	Event	Username	Site Name
2024-06-20 16:41					
16:36:03	ch-qa-g-std-vm-qualys-mas	User root logged in via ssh	User root logged in via ssh fi	root	Mendrisio
16:34:18	ch-qa-g-std-vm-upload-ma	Remove label for interface '	Remove label for interface 'v	giacomo.matteucci@nozom	Mendrisio
16:33:50	ch-qa-g-std-vm-upload-ma	User root logged in via ssh	User root logged in via ssh fi	root	Mendrisio
16:33:37	ch-qa-g-std-vm-upload-ma	Set up new label for interfa	Set up new label for interfac	giacomo.matteucci@nozom	Mendrisio
16:33:15	ch-qa-cmc-std-vm-gen-ma	User signed in	User signed in	giacomo.matteucci@nozom	Mendrisio
16:33:15	ch-qa-cmc-std-vm-gen-ma	Login via SAML	Login via SAML, User 'giacor	giacomo.matteucci@nozom	Mendrisio
16:33:15	ch-qa-g-std-vm-upload-ma	User signed in	User signed in	giacomo.matteucci@nozom	Mendrisio
16:33:15	ch-qa-g-std-vm-upload-ma	Login via SAML	Login via SAML, User 'giacor	giacomo.matteucci@nozom	Mendrisio
16:32:51	ch-qa-g-std-vm-ha-master-	User signed in	User signed in	giovanni.masullo@nozomin	Mendrisio
16:32:51	ch-qa-g-std-vm-ha-master-	Login via SAML	Login via SAML, User 'giovar	giovanni.masullo@nozomin	Mendrisio
16:32:46	ch-qa-cmc-std-vm-gen-ma	User signed in	User signed in	giovanni.masullo@nozomin	Mendrisio
16:32:46	ch-qa-cmc-std-vm-gen-ma	Login via SAML	Login via SAML, User 'giovar	giovanni.masullo@nozomin	Mendrisio
16:32:25	ch-qa-g-std-vm-ha-master-	Deleted report file from list	Deleted report file from list t	guglielmo.fachini@nozomir	Mendrisio
16:32:21	ch-qa-g-std-vm-ha-master-	Deleted report 'Validation c	Deleted report 'Validation of	guglielmo.fachini@nozomir	Mendrisio
16:32:15	ch-qa-g-std-vm-ha-master-	User signed in	User signed in	guglielmo.fachini@nozomir	Mendrisio
16:31:42	ch-qa-g-std-vm-upload-ma	Scheduled backup file crea	Scheduled backup file creat	System:Backup	Mendrisio
16:30:59	ch-qa-g-std-vm-upload-ma	Found 3 backup files (max :	Found 3 backup files (max 3	System:Backup	Mendrisio
16:30:17	ch-qa-g-std-vm-upload-ma	Ingested pcap: 'ch-qa-g-std	Ingested pcap: 'ch-qa-g-std-	labtests	Mendrisio
16:30:17	ch-qa-g-std-vm-upload-ma	Replay ingest pcap called t	Replay ingest pcap called th	labtests	Mendrisio

Figure 57. Audit logs page

Name

This section shows a list of the different types of audit logs.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

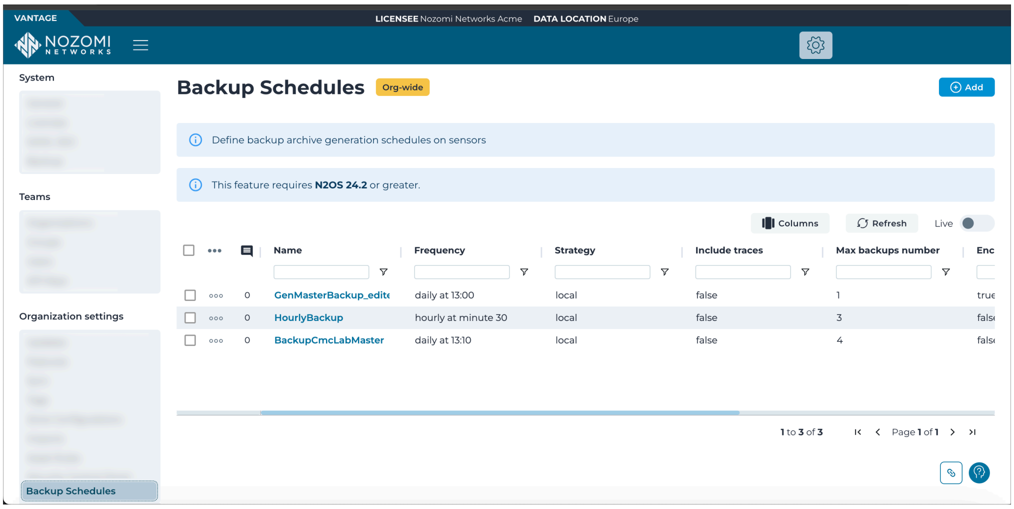
The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Backup Schedules

*The **Backup Schedules** page lets you manage, view, add, edit, and delete backup schedules.*



LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Backup Schedules

Define backup archive generation schedules on sensors

This feature requires **N2OS 24.2** or greater.

□	•••		Name	Frequency	Strategy	Include traces	Max backups number	Enc
□	○○○	0	GenMasterBackup_edite	daily at 13:00	local	false	1	true
□	○○○	0	HourlyBackup	hourly at minute 30	local	false	3	fals
□	○○○	0	BackupCmcLabMaster	daily at 13:10	local	false	4	fals

1 to 3 of 3 Page 1 of 1

Figure 58. Backup Schedules page

Add

This button lets you Add a backup schedule (on page 130).

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Add a backup schedule

You can use the actions menu to add a new backup schedule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Backup Schedules**.

   Result: The **Backup Schedules** page opens.

3. Select **Add**.

   Result: The **Create Backup Schedule** page shows.

4. Configure the backup schedule as necessary.
5. Select **Create**.

Results

The backup schedule has been created.

Edit a backup schedule

You can use the actions menu to edit a backup schedule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Backup Schedules**.

   Result: The **Backup Schedules** page opens.

3. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. Select **Edit**.

Results

You can now edit the backup schedule.

Delete a backup schedule

You can use the actions menu to delete a backup schedule.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Organization settings** section, select **Backup Schedules**.

   Result: The **Backup Schedules** page opens.

3. Choose a method to open the actions menu.

   Choose from:

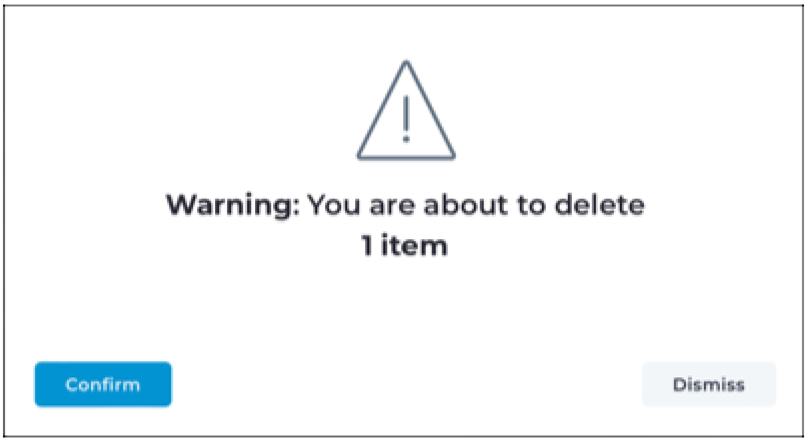
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

4. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Delete**.



Warning: You are about to delete 1 item

   Result: A confirmation dialog shows.

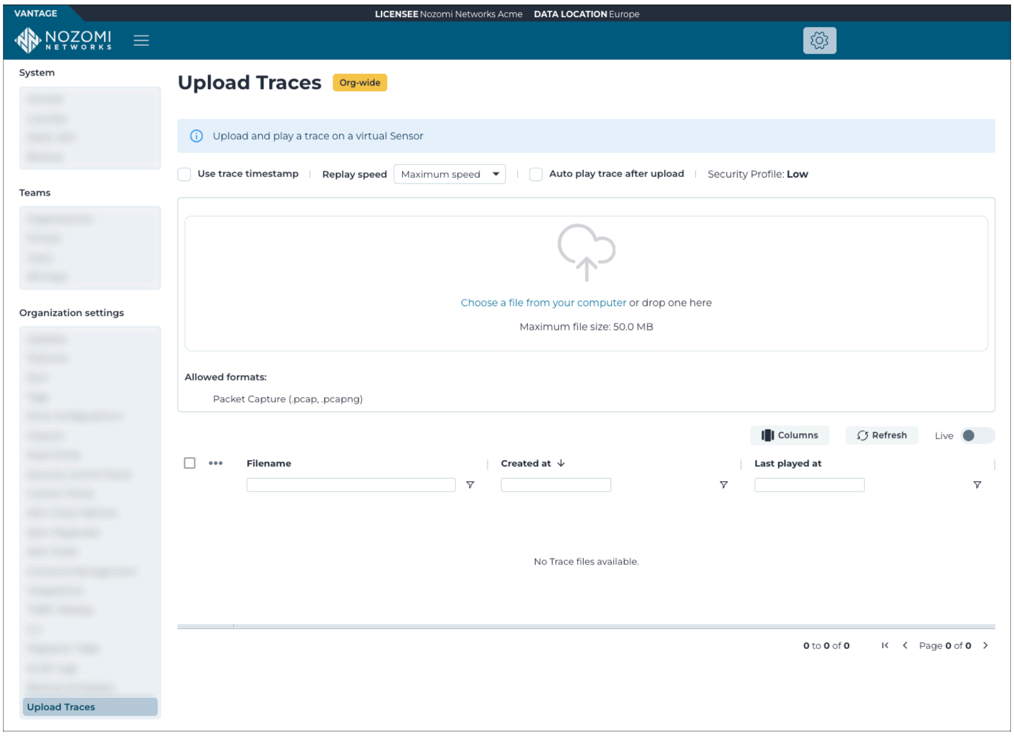
6. Select **Confirm**.

Results

The backup schedule has been deleted.

Upload Traces

*The **Upload Traces** page lets you upload a trace, or packet capture (pcap) file, that is related to the active organization.*



Upload Traces

Upload and play a trace on a virtual Sensor

☐ Use trace timestamp | Replay speed Maximum speed ▾ | ☐ Auto play trace after upload | Security Profile: Low

Choose a file from your computer or drop one here

Maximum file size: 50.0 MB

Allowed formats:

Packet Capture (.pcap, .pcapng)

☐	Filename	Created at ↓	Last played at

No Trace files available.

0 to 0 of 0 Page 0 of 0

Figure 59. Upload Traces page

When a *packet capture (pcap)* is played for the first time, a **Play Context** is created automatically. This consists of a:

- Site
- Network domain
- Virtual sensor

When other *pcap*s are played, they play over the same **Play Context** until the sensor, or the site, is deleted. In that case, a new context will be generated when playing a file.

The sensor is named **Trace Sensor XXX** where **XXX** is a randomized value. This is placed in the sensor list like the others. There is no separation of *pcap* data versus production data.

For each organization, there can be only be one **Trace Sensor**. We suggest that you create a separate organization to avoid mixing *pcap* data with production data.

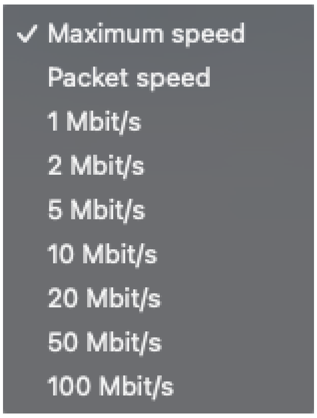
The **Trace Sensor** is a real Guardian running in the cloud. Therefore, it goes through the standard synchronization process. For this reason, data will only show in the *UI* after a few seconds.

Use trace timestamp

Select this to keep the original timestamps from the trace logs. This will ensure accurate event timing during analysis.

Replay speed

This dropdown lets you select the playback speed of the trace.



- ✓ Maximum speed
- Packet speed
- 1 Mbit/s
- 2 Mbit/s
- 5 Mbit/s
- 10 Mbit/s
- 20 Mbit/s
- 50 Mbit/s
- 100 Mbit/s

Figure 60. Replay speed dropdown

Auto play trace after upload

This lets you choose whether or not the trace will automatically play after it has been uploaded. If it is not selected, you have to manually select the ▷ icon to the left of the file that you've just uploaded. Alternatively, you can select multiple files to play and select the **Play Traces** option.

Security Profile

This shows the security level applied to the trace upload.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Chapter 3. Migration

Migration to N2OS 22.6.0

The current N2OS release includes important changes that might require additional steps when you upgrade from an earlier release.

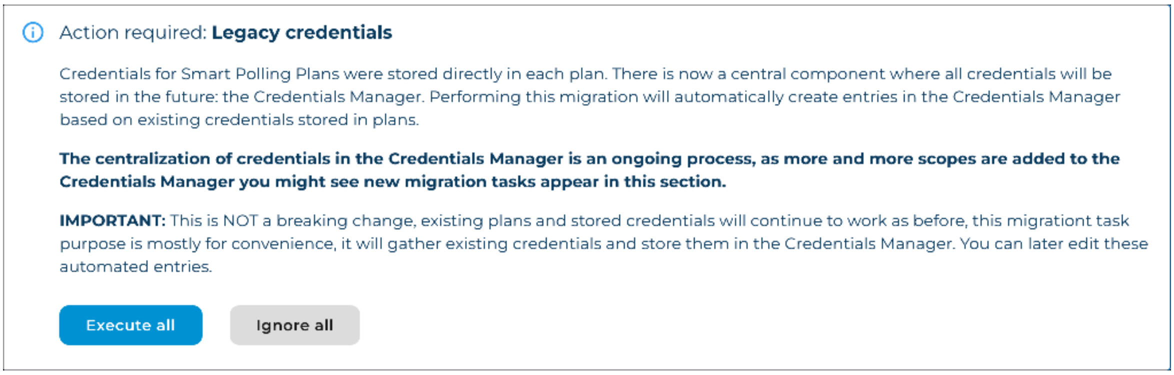
Migration tasks are tools that help administrators update Vantage installations to adapt to changes in new versions of *Nozomi Networks Operating System (N2OS)*. For more information about these tools, please refer to the **N2OS User Manual** and the **N2OS Release Notes**.

Credentials Manager

In *N2OS* version 22.6.0, we introduced the Credentials Manager, which lets you securely store passwords and other sensitive information that Guardian uses to access hosts through Smart Polling, or to decrypt encrypted transmissions that are detected passively. This task can migrate existing credentials from your existing Smart Polling plan configurations to the new Credentials Manager. This improves the maintainability of these sensitive data.

Running this migration task is not necessary to ensure that Smart Polling continues working correctly with the new version, but it will organize the credentials in a more controlled way. Nozomi Networks recommends that you do this task.

You can select **Execute all** to migrate to the Credentials Manager.



Action required: **Legacy credentials**

Credentials for Smart Polling Plans were stored directly in each plan. There is now a central component where all credentials will be stored in the future: the Credentials Manager. Performing this migration will automatically create entries in the Credentials Manager based on existing credentials stored in plans.

The centralization of credentials in the Credentials Manager is an ongoing process, as more and more scopes are added to the Credentials Manager you might see new migration tasks appear in this section.

IMPORTANT: This is NOT a breaking change, existing plans and stored credentials will continue to work as before, this migrationt task purpose is mostly for convenience, it will gather existing credentials and store them in the Credentials Manager. You can later edit these automated entries.

Data Model Manager

In *N2OS* version 22.6.0, we have updated the names of selected table fields and values, as described in N2OS 22.6.0 Data Model Data Model Changes. To make sure that the new names and structures are used, these changes might require user intervention to adapt saved:

- Queries
- Assertions
- Custom reports
- Alert rules
- Data integrations scope

When you upgrade to *N2OS* version 22.6.0, you can manage this migration from Vantage.

Note:
In some cases, other systems integrated with *N2OS* through the *API* are also impacted.

For more details, see the Nozomi Support Knowledge Base articles about these data model changes.

If you need to delay these changes, you should disable automatic software updates for your downstream installation.

Complete strings and substrings

The migration might affect these two types of strings:

- Complete strings: Complete strings are those where the items to be changed appear as a whole
- Substrings: Substrings are those that do not show the full name

Where a complete string is used to reference the table field, or value, Vantage can automatically migrate your sensors to use the new data model. Where a substring is used to refer to a table field or value that has changed, you must take additional steps outside of the Migration tasks (on page 127) page.

Examples of complete strings:

- `query: alerts | where type_id == SIGN:TCP-MALFORMED`
- `alert rule having in scope type_id: SIGN:TCP-MALFORMED`

Examples of substrings:

- `query: alerts | where type_id include? SIGN:TCP`
- `query: alerts | where type_id include? SIGN:`
- `query: alerts | where type_id include? LINK`

Migrate to the N2OS 22.6.0 data model

This procedure gives you all the steps that you might need to do to migrate to the N2OS 22.6.0 data model.

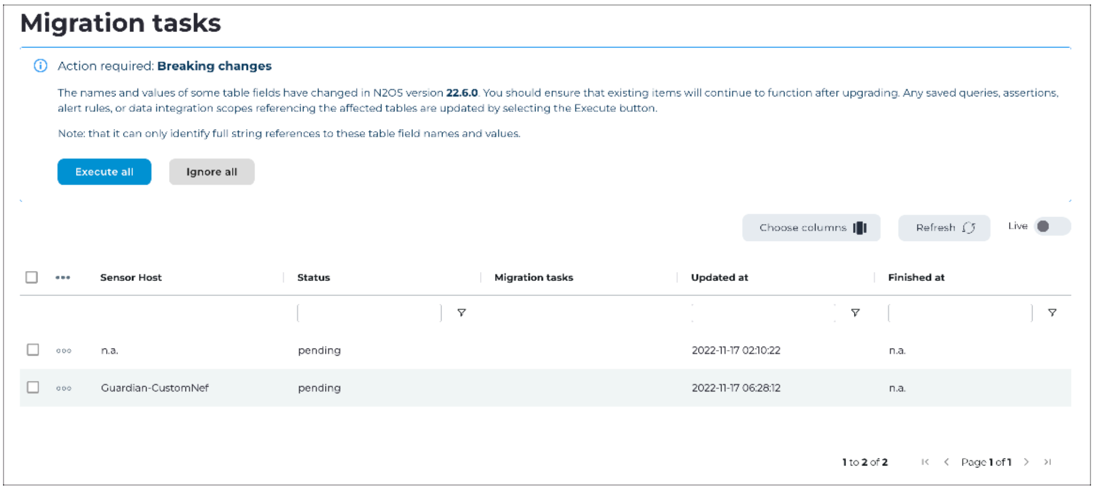
Procedure

1. Upgrade to N2OS 22.6.0 to get the health logs to help migration to the new data model.
2. In the top navigation bar, select ⚙

   Result: The administration page opens.
3. In the **Organization settings** section, select **Migration Tasks**.

   Result: The **Migration Tasks** page opens.
4. In the **Description** field, enter the string `Recommended changes` of the table to search for instances of the old names.

   Result: Vantage returns the complete strings that need to be updated. By default, the health logs where this data is collected are synchronized to Vantage, so you see an overview of all such logs throughout your entire installation.
5. Before you do the next steps, review the results to understand these changes.



Migration tasks

Action required: **Breaking changes**

The names and values of some table fields have changed in N2OS version **22.6.0**. You should ensure that existing items will continue to function after upgrading. Any saved queries, assertions, alert rules, or data integration scopes referencing the affected tables are updated by selecting the Execute button.

Note: that it can only identify full string references to these table field names and values.

□	•••	Sensor Host	Status	Migration tasks	Updated at	Finished at
□	○○○	n.a.	pending		2022-11-17 02:10:22	n.a.
□	○○○	Guardian-CustomNef	pending		2022-11-17 06:28:12	n.a.

> **Note:**
>
> The changes are applied to the complete downstream installation. This means that when you execute the changes in Vantage, the changes will be applied to all CMCs and Guardians that are connected downstream.

6. Choose the method that you want to use.

   Choose from:

   - If you want to execute or ignore the changes individually, do steps 7 (on page 140) and 8 (on page 140).
   - If you want to execute all the changes together, go to step 9 (on page 140)

   > **Note:**
   > Nozomi Networks recommends that you execute all the changes together.

7. Choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
8. Select **Execute** or **Ignore** as applicable.
9. Select **Execute all**.
10. To verify that the changes have been successfully applied in your *N2OS* environment, run the shell command: `n2os-recommended-changes`

    Result: If the changes were made successfully, the list will be empty.

11. **Optional:** If necessary, update substrings that have changed.

    > **Note:**
    > Because Vantage can only manage migration for complete strings, you might need to take additional steps to address substrings that are used for:
    >
    > - Saved queries
    > - Assertions
    > - Custom reports
    > - Alert rules
    > - Other items within the scope of integration

    a. Review the table and field names that have changed in N2OS 22.6.0 Data Model Changes (on page 141) and make a note of those that might impact your installation.
    b. Review your sensors' contents to identify all the references that still need to be updated.
    c. To replace the old names with the new names, manually edit the applicable substrings.

N2OS 22.6.0 Data Model Changes

A list of the changes to the table fields and values in N2OS version 22.6.0.

Field in scope	Current	New	Description/Rationale
alerts: type_id	SIGN:TCP- MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA- NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA- INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN- FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization

Field in scope	Current	New	Description/Rationale
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization

Chapter 4. SAML integration

SAML integration configuration

It is important to understand how Vantage uses security assertion markup language (SAML) single sign-on (SSO) for authentication.

General

Vantage supports *SAML SSO* authentication. Our integration requires your *IdP* to be compatible with *SAML* 2.0. To authenticate, Vantage requires the user's:

- Email address
- Entity ID attributes

The *SAML* configuration process is often error prone. This section assumes that you're familiar with:

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

You will need to configure:

- Configure your IdP for SAML integration (on page 147)
- Configure Vantage for SSO (on page 148)

Group creation

Before authentication can work correctly, you will need to have a Vantage group that matches your *IdP*'s roles.

You can use the roles **SAML ID** or **SAML name** as defined in your *IdP*.

When you create a group in Vantage, enter the **SAML ID** or **SAML name** of the corresponding *IdP* role. If a Vantage group isn't mapped to an *IdP* role, authentication will fail for users assigned that role.

When a user logs into Vantage and authenticates, if the Vantage group doesn't include that user, Vantage will automatically add the user to the group.

For more details, see Group membership (on page 28).

IdP configuration for SAML integration

It is important to understand the different parameters that are needed to configure your identity provider (IdP) for security assertion markup language (SAML) integration in Vantage.

Assertion Consumer Service

An *ACS* specifies an `/auth` path, such as `https://YOUR_VANTAGE_URL/api/v1/saml/auth`, where `YOUR_VANTAGE_URL` is the custom *URL* you use to access Vantage. For example, `customer1.customers.us1.vantage.nozominetworks.io`

In your *IdP*, you should define this in the attribute statement.

If your Vantage instance is *FIPS*-compliant, it uses a different *ACS URL*. For more details, see FIPS support (on page 10).

Entity ID

The entity ID will be declared in the metadata *XML* file that you download from your *IdP*.

Nozomi Networks frequently sees entity IDs in the form: h`ttps://YOUR_IDP_URL/UNIQUE_ID`, where:

- `YOUR_IDP_URL` is the *URL* of your *IdP* and
- `UNIQUE_ID` is the identifier that your *IdP* assigns to Vantage

Note:
The Entity ID can also be known as:

- Audience URI
- Issuer
- Reply URL
- SP Entity ID

Your *IdP* vendor and *SAML* implementation determine the content and format of an entity ID. The `https://YOUR_IDP_URL/UNIQUE_ID` format is common, but your *IdP* or specific *SAML* implementation might require different values.
When configuring your *IdP*, use the following values:

- **ACS URL:** `https://YOUR_VANTAGE_URL/api/v1/saml/auth`
- **Entity ID:** `https://YOUR_VANTAGE_URL/api/v1/saml/metadata`

Replace `YOUR_VANTAGE_URL` with the actual domain for your Vantage deployment (for example, `customer1.customers.us1.vantage.nozominetworks.io`).

Vantage can integrate with many *IdP*. For more details about specific *IdP*, see:

- Configure an Azure Active Directory enterprise application (on page 155)
- Configure an Okta enterprise application (on page 153)
- Configure a Google Workspace SAML application (on page 151)

Configure your IdP for SAML integration

Before you configure Vantage's settings for single sign-on (SSO), you need to define a new application in your identity provider (IdP).

Before you begin

Before you do this procedure, you should familiarize yourself with IdP configuration for SAML integration (on page 146).

Procedure

1. Configure the *ACS URL* for Vantage.
2. Define the entity ID in the attribute statement of your *IdP*.

Configure Vantage for SSO

Before you can use single sign-on authentication in Vantage, you must configure Vantage.

Before you begin

Before you do this procedure, make sure that you have:

- Completed the Configure your IdP for SAML integration (on page 147) procedure
- Downloaded an *XML* file from your *IdP* to a location that your browser can access

> **Note:**
> In order for *SAML* to work correctly, groups that correspond to your *SAML* roles must already exist in Vantage. Groups are found using the role's name; for example, if the *SAML* name attribute specifies `daf0ff75-d045-4a5a-8747-6d2a2ee47cdd`, the *IdP* looks for the `daf0ff75-d045-4a5a-8747-6d2a2ee47cdd` role when authorizing an authenticating user.

Procedure

1. Log in to Vantage as an administrator.
2. In the top navigation bar, select ⚙

   Result: The administration page opens.
3. In the **System** section, select **SSO**.

   Result: The **SAML Single Sign On** page opens.
4. Select the Enable **SAML Single Sign on** checkbox.
5. To the right of the **Metadata XML** field, select **Choose File**
6. Locate and select the metadata file that you downloaded from your *IdP*.

   > **Note:**
   > This file gives Vantage the necessary parameters to configure *SAML* for your *IdP*.
7. In the **Entity ID** field, enter the *ID* assigned to the Vantage application in the *IdP*.

   > **Note:**
   > The form of this *ID* determines how authentication is processed. For example, if the value you enter specifies *hypertext transfer protocol secure (HTTPS)*, Vantage uses the *HTTPS* protocol when it processes login requests.

8. In the **Role attribute** field, enter a string that will be used to map role names in your *IdP* to groups in Vantage.

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

9. Select **Save**.
10. Test the integration.
    a. On the Vantage login page, enter a *SAML* user name.
    b. Select **Next**.
    c. Select **Single Sign On**.

> **Note:**
> Nozomi Networks products do not support the logout *SAML* protocol.

> **Note:**
> Before authentication can succeed, Vantage groups that match your *IdP*'s roles must exist . To map groups to roles, you can use the role's *SAML* *ID* or *SAML* name, as defined in your *IdP* . When you create a group in Vantage, you enter the *SAML* *ID* or *SAML* name of the related *IdP* role. If a Vantage group isn't mapped to an *IdP* role, authentication fails for users assigned that role.

> **Note:**
> When a user logs in to Vantage and authenticates, and the Vantage group doesn't include that user, Vantage adds the user to the group automatically.

Troubleshooting SAML integration

Methods that you can use to test that the security assertion markup language (SAML) integration has been successful.

Once *SAML* is configured, the login page displays a new **Single Sign On** button. You can test the integration with Vantage as you would other applications that authenticate through your *IdP*.

If authentication fails, Vantage writes errors to the audit logs. Please contact Nozomi Networks for help troubleshooting *SAML* issues.

Note:
To troubleshoot authentication in real-time, you should install a browser plug-in such as **SAML Chrome Panel**. Such developer tools can provide helpful *SSO* information

Configure a Google Workspace SAML application

You can integrate Google Workspace with Vantage to provide single sign-on (SSO) services. You should also refer to the Google Workspace documentation for more details on their solution. This topic describes Vantage-specific configuration details when using Google Workspace as your identity provider (IdP).

About this task

The Google Workspace group that is used for *SSO* with Vantage must have the same name as the group in Vantage.

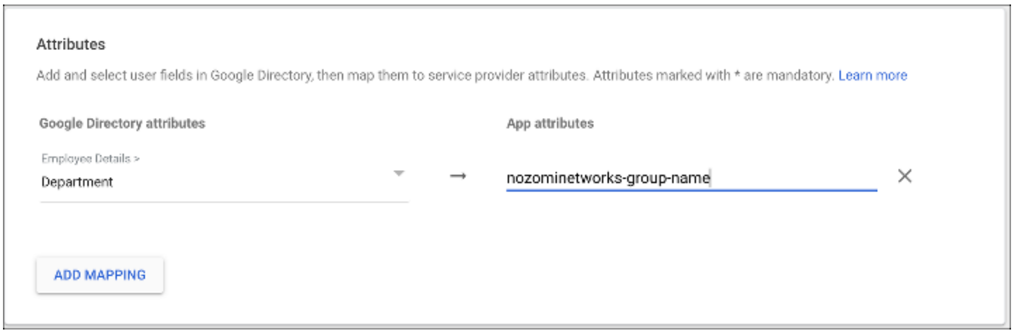
Procedure

1. In the Google Workspace Admin console Home page, navigate to **Apps > Web and Mobile Apps**
2. Select **Add App**.
3. Select **Add custom SAML app**.
4. Enter a name such as **Vantage**.
5. **Optional:**

   Upload an image to use as an icon in the *SAML* app.

6. Select **Continue**.
7. Under **Option 1: Download IdP metadata**, select **Download Metadata**.
8. Save this file to a location that the browser that you use for Vantage can access.
9. Select **Continue**.
10. In the **Service Provider Details** window, specify the Google Identity Provider details for the app.
    a. In the **ACS URL** field, enter the Assertion Consumer Service (ACS) URL for Vantage: `https://YOUR_VANTAGE_URL/api/v1/saml/auth`
    b. In the **Entity ID** field, enter the Service Provider (SP) Entity ID for Vantage: `https://YOUR_VANTAGE_URL/api/v1/saml/metadata`
    c. In the **Name ID** section, from the **Name ID format** dropdown, select **EMAIL** .
    d. In the **Name ID** dropdown, select **Basic Information > Primary Email**.
11. Select **Continue**.

12. Specify how Google's directory attributes are mapped to the Vantage app's attributes.
    a. On the left, select an attribute from those defined in Google Workspace.
    b. On the right, enter `nozominetworks-group-name`
    c. Select **ADD MAPPING**.



Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. Learn more

Google Directory attributes: Employee Details > Department → App attributes: nozominetworks-group-name

13. Select **Finish**.
14. Before you continue, make sure that you grant your users access to the new Vantage application. The simplest approach is to enable **ON** for everyone for Google Workspace's User access option.
15. Configure Vantage for SSO (on page 148).

Results

The application has been configured.

Configure an Okta enterprise application

You can integrate Okta with Vantage. To do this you must create an enterprise application in Okta and assign users to it.

About this task

Okta groups are mapped to groups in Vantage using the group identifier. The group must exist in both Vantage and Okta and its **Group ID** in Okta must match its **SAML Name** or **ID** in Vantage. During authentication, Okta passes the Okta attribute statements defined for the authenticating user. Vantage ignores those for groups that don't match any of its own. For more details, see Group creation (on page 145).

Procedure

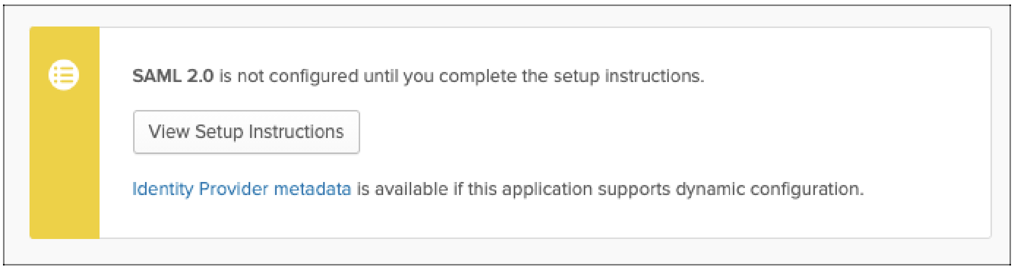
1. In the Okta Admin console, select **Applications > Create App Integration**.
2. Select **SAML 2.0**.
3. Enter a name such as **Vantage**
4. Select **Next**.
5. Enter the **Single sign on URL** that corresponds to the *ACS URL* for Vantage:

   `https://YOUR_VANTAGE_URL/api/v1/saml/auth`
6. Enter the **Audience URI**: `https://YOUR_VANTAGE_URL/api/v1/saml/metadata`

   The **Audience URI** is also known as **Audience Restriction** or **SP Entity ID**.
7. Define **Group Attributes Statements**.

   > **Note:**
   > Vantage authentication relies on group attribute statements. You must create such statements for all group that are used for authentication. Users that belong to the group pass the statement you define. *XREF*

8. After you have entered these values, confirm your choices and select **Save**.
9. Assign users to the enterprise application to grant them access. For more details, see the Okta documentation.
10. Download the Okta *IdP* metadata file.
    a. In Okta, select the Vantage enterprise application's **Sign On** tab.
    b. Select the **Identity Provider Metadata** link.



SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

11. Save this file to a location that the browser that you use for Vantage can access.
12. Configure Vantage for SSO (on page 148).

Configure an Azure Active Directory enterprise application

You can integrate Azure Active Directory with Vantage. To do this you must create an enterprise application in Azure Active Directory and assign users to it.

Before you begin

An Azure Active Directory group that is to be used with Vantage must:

- Be of type **office 365mail enabled security or security**
- Have the **AuthNContext** property set to true

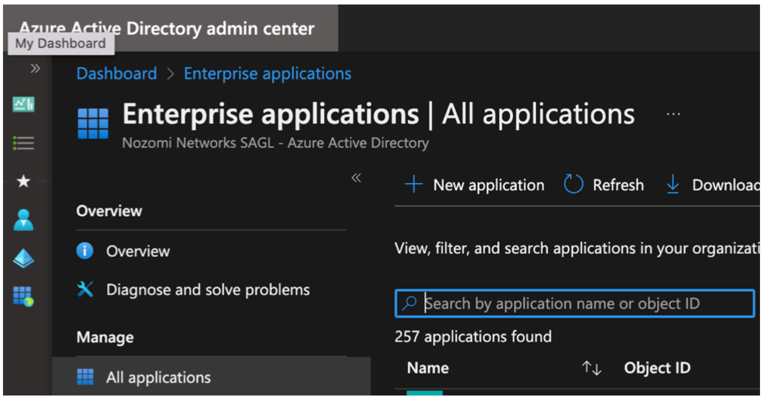
> **Note:**
> Users, guests, and applications contained directly in this group are granted access to Vantage. Azure denies access to users contained in the group's subgroups.

About this task

During authentication, Azure passes the *universally unique identifier (UUID)* of all the security groups that are defined for the authenticating user. Vantage ignores those that don't match any of its own groups. For more details, see Group creation (on page 145).

Procedure

1. Select **My Dashboard > Enterprise applications | All Applications**.


Azure Active Directory admin center
My Dashboard
Dashboard > Enterprise applications
Enterprise applications | All applications
Nozomi Networks SAGL - Azure Active Directory
New application
Refresh
Download
Overview
Overview
Diagnose and solve problems
Manage
All applications
View, filter, and search applications in your organizati
Search by application name or object ID
257 applications found
Name
Object ID

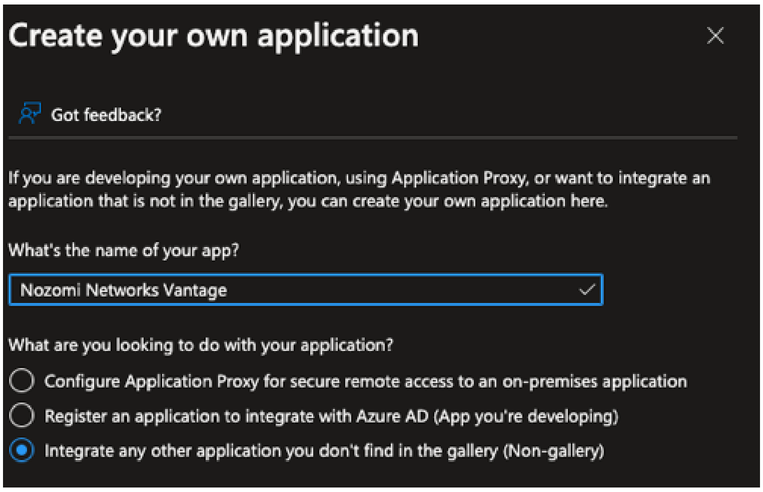
2. Select **+ New application**.

   Result: A dialog shows.

3. Select **Create your own application**.

   Result: A dialog shows.

4. In the **What's the name of your app?** filed, enter a name such as: **Nozomi Networks Vantage**.



Create your own application

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Nozomi Networks Vantage

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

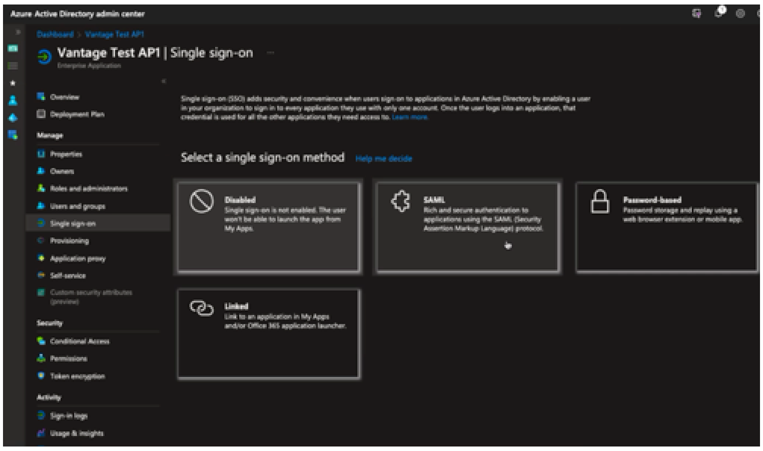
○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

5. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.
6. Enter any other Azure Active Directory details that are needed to complete the configuration of the new application. Select **Create**.

   Result: The application has been created.

7. Open the application.
8. Select **Single sign-on > SAML**.



Single sign-on (SSO) adds security and convenience when users sign-on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more

Select a single sign-on method Help me decide

Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based Password storage and replay using a web browser extension or mobile app.

Linked Link to an application in My Apps and/or Office 365 application launcher.

9. Specify the **Reply URL** which corresponds to the *ACS URL* for Vantage:
   `https://YOUR_VANTAGE_URL/api/v1/saml/auth`
10. Define the **Entity ID** for Vantage:
    `https://YOUR_VANTAGE_URL/api/v1/saml/metadata`

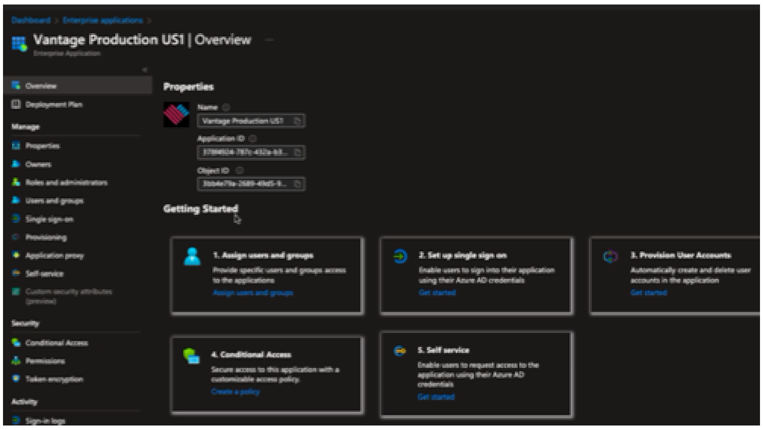
11. Define attributes and claims.

> **Note:**
> Vantage authentication relies on user group claims. You must create such claims for any group used for authentication. Users that belong to the group pass the claim that you define.

12. **Optional:**

    Upload an image to use as an icon in the *SAML* app.

13. After the application has been configured, it will show in Azure.



Vantage Production US1 | Overview

Enterprise Application

Properties

Name: Vantage Production US1

Application ID: 378f4924-787c-432a-b3...

Object ID: 3bb4e79a-2689-49d5-9...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

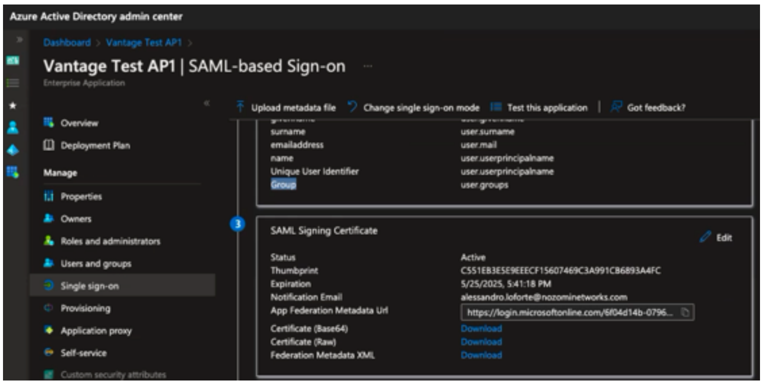
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

14. Download the Azure Active Directory metadata file.
    a. In the **SAML Signing Certificate section**, to the right of **Federation Metadata XML**, select **Download**.



Vantage Test AP1 | SAML-based Sign-on

surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

SAML Signing Certificate

Status	Active
Thumbprint	C551EB3E5E9EEECF15607469C3A991CB6893A4FC
Expiration	5/25/2025, 5:41:18 PM
Notification Email	alessandro.loforte@nozominetworks.com
App Federation Metadata Url	https://login.microsoftonline.com/6f04d14b-0796...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

    b. Save this file to a location that the browser that you use for Vantage can access.

15. Configure Vantage for SSO (on page 148).

Results

The application has been configured.

Glossary

Adaptive Learning

Adaptive Learning is when deviations are evaluated at a global level, rather than at the level of a single node. For example, using adaptive learning approach, the sensor doesn't raise an alert when it detects a device similar to those already installed in the network. This also applies for newly-detected communications that are similar to those previously detected. Adaptive learning is especially powerful and offers its best effect when combined with Asset Intelligence.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Artificial Intelligence

AI is computer intelligence, as opposed to human or animal intelligence. It is *artificial* because it is a digital computer that can perform tasks that are commonly associated with intelligent beings. *Intelligence* is the ability to learn and to reason.

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.

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 a similar way as on the sensor.

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 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.

Exploit Prediction Scoring System

EPSS is a cybersecurity risk assessment framework that predicts the likelihood of a software vulnerability being exploited in the wild. It uses data-driven models based on real-world exploit activity, vulnerability metadata, and other threat intelligence sources to help organizations prioritize patching efforts.

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 human-readable and machine-readable.

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.

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.

Information Technology

IT is the use of computers to process, create, store, and exchange data and information.

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.

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.

JSON web token

A JWT is an internet standard to create data with optional encryption and/or optional signature whose payload holds JSON that asserts some number of claims. The tokens are signed either using a private secret or a private/ public key.

Known Exploited Vulnerabilities

A list of software vulnerabilities that threat actors have actively exploited. Cybersecurity organizations track KEVs to help prioritize patching and mitigate security risks.

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.

National Institute of Standards and Technology

NIST is an agency of the United States Department of Commerce. NIST's mission is to promote American innovation and industrial competitiveness.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

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).

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

Remote Terminal Unit

An RTU is a microprocessor-controlled electronic device that acts as an interface between a SCADA (supervisory control and data acquisition) system, or distributed control system, to a physical object. It transmits telemetry data to a master system, and uses messages from the master supervisory system to control connected objects.

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.

Single Sign-on

SSO is an authentication method that lets users log in to one or more related, but independent, software systems.

Software as a Service

SaaS is a software licensing and delivery model. This type of software is hosted centrally and licensed on a subscription basis.

Strict (Learning)

Strict (Learning) is a mode which relies on a detailed anomaly-based approach. Each node is evaluated at the node level; when deviations from the baseline are detected, the sensor raises alerts. This approach is called strict because once a system is learned, it is expected to always behave as it did during the learning phase; maintaining systems with the Strict approach requires detailed knowledge of your system.

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.

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.

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.

Two-factor authentication

2FA is a method that lets you add additional security to an account. The first factor is a standard password, the second factor is a code that is used on an app on a mobile device or computer that verifies the user.

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.

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.

User Interface

An interface that lets humans interact with machines.

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).