



Vantage for Government Administrator Guide

2026-09-02

Legal notices

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

Copyright

Copyright © 2013-2026, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

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

Contents

Chapter 1. Introduction.....	5
Vantage for Government overview.....	7
Architecture.....	9
Data security in Vantage.....	10
Get more from Vantage.....	11
Respond to the Get more from Vantage prompt.....	12
Chapter 2. Administration.....	15
Administration page.....	17
System.....	19
General.....	19
Licenses.....	23
SAML Single Sign On.....	24
Backup.....	29
Teams.....	30
Organizations.....	30
Groups.....	32
Roles.....	45
Users.....	48
API keys.....	55
Organization Settings.....	66
Updates.....	66
Features.....	73
Sensors Synchronization Settings.....	77
Tags.....	79
Zone Configurations.....	80
Imports.....	91
Asset Rules.....	103
Security Control Panel.....	107
Custom Fields.....	109
Credentials Manager.....	110
Alert Close Options.....	112
Alert Playbooks.....	115
Alert Rules.....	119
Contents Management.....	123
Traffic Replays.....	129
CLI.....	130
Migration tasks.....	131
Audit Logs.....	132
Backup Schedules.....	133

Upload Traces..... 137

Arc dependencies.....139

Chapter 3. SAML integration..... 153

 SAML integration configuration.....155

 IdP configuration for SAML integration..... 156

 Configure your IdP for SAML integration.....157

 Configure Vantage for SSO..... 158

 Troubleshooting SAML integration..... 160

 Configure a Google Workspace SAML application.....161

 Configure an Okta enterprise application.....163

 Configure an Azure Active Directory enterprise application..... 165

Glossary.....169

Chapter 1. Introduction



Vantage for Government overview

Vantage for Government is a Software as a Service (SaaS) product that lets you monitor and protect your networks. Vantage for Government lets you respond faster and more effectively to cyber threats, to ensure your operational resilience.

General

Vantage for Government (**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
- 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.

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

Related information

[Architecture \(on page 9\)](#)

[Data security in Vantage \(on page 10\)](#)

Architecture

You can use Vantage, and the flexible architecture, to create a customized solution.

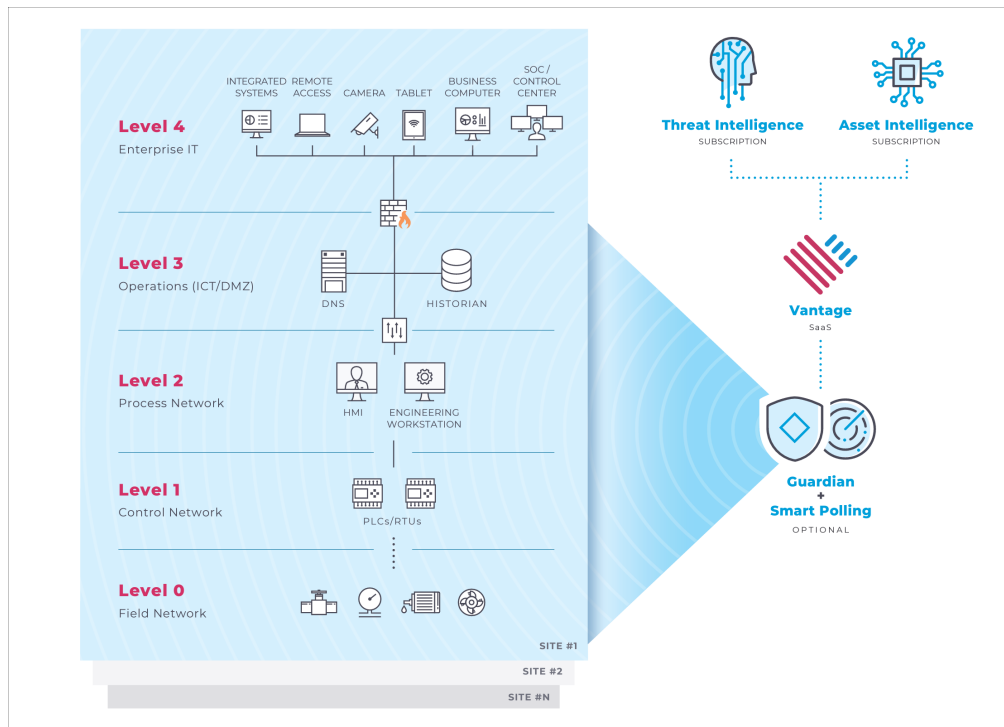


Figure 1. Vantage architecture

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.

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, you must specify its [assertion consumer service \(ACS\) uniform resource locator \(URL\)](#).

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 URLs](#), see **IdP configuration for SAML integration**, in the **Administrator Guide**.

Get more from Vantage

*The **Get more from Vantage** prompt helps root administrators optimize their environment by enabling Discovery and Smart Polling features. These capabilities improve asset visibility and support integration planning based on real usage data.*

Root administrators see the **Get more from Vantage** prompt after logging in. It collects details about software in the environment and offers the option to enable automatic Discovery and Smart Polling plans.

Completing the prompt is optional but recommended. Root administrators can choose to select:

- **Next** to continue with the setup
- **Assign to another user** to delegate the setup
- **Remind me later** to postpone the prompt

This proactive configuration helps Vantage deliver more relevant insights and accelerates time-to-value through intelligent automation.

Respond to the Get more from Vantage prompt

To help Vantage better understand their environment, root administrators see a guided setup dialog after logging in. This process collects preferences and offers the option to enable Discovery and Smart Polling. It improves asset visibility and supports tailored configuration recommendations.

About this task

After login, root administrators are prompted with a short setup dialog that helps identify the software in use and enables Discovery and Smart Polling features. Completing the prompt allows Vantage to automate data collection plans to enhance visibility and insights.

Procedure

1. Log in to Vantage as a root administrator.

Result: A **Get more from Vantage** dialog shows.

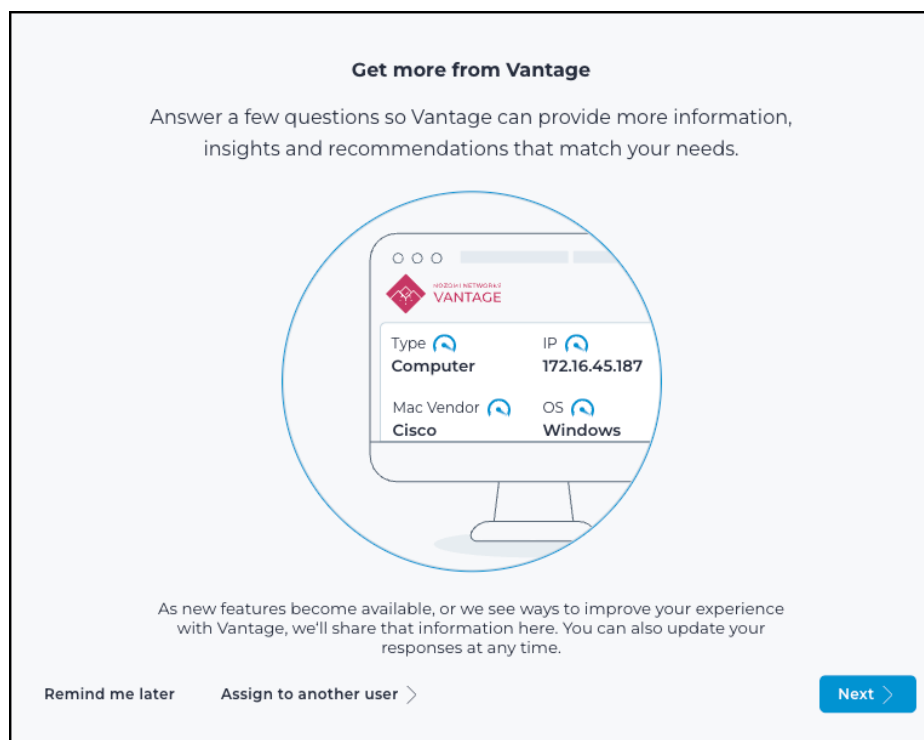


Figure 2. Get more from Vantage dialog

2. Select one of these options:

Choose from:

- **Remind me later:** The prompt will appear again the next time that you log in
- **Assign to another user:** Transfer the task to a different user
- **Next:** Complete the setup now

3. Select **Next**.

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

The screenshot shows the 'Asset Inventory' page in a three-step wizard. The steps are: 1. Integrations, 2. Asset inventory (current step), and 3. Finish. The 'Asset inventory' step is highlighted with a blue diamond icon. Below the step indicators, the heading 'Want a more complete asset inventory?' is followed by the text 'With Smart Polling and Discovery you can:'. A purple diamond icon with a network symbol is next to a bulleted list: 'Enrich device details', 'Refine your risk scoring', and 'Improve vulnerability visibility'. Below this list is a radio button group with two options: 'Enable Smart Polling and Discovery' (selected) and 'I'll configure this manually'. At the bottom of the page, there are three links: 'Remind me later', 'Assign to another user >', and a 'Back' button. A 'Next >' button is also present at the bottom right.

1 2 3
Integrations Asset inventory Finish

Want a more complete asset inventory?

With Smart Polling and Discovery you can:

- Enrich device details
- Refine your risk scoring
- Improve vulnerability visibility

☒ Enable Smart Polling and Discovery ☐ I'll configure this manually

Remind me later Assign to another user > < Back Next >

Figure 3. Asset Inventory page

4. On the **Asset Inventory** page:

Choose from:

- **Enable Smart Polling and Discovery** – Starts Discovery immediately and schedules Smart Polling plans automatically
- **No, I'll configure this manually** – Skips automated configuration for now

5. Select **Next**.

Result: The **Finish** page shows.

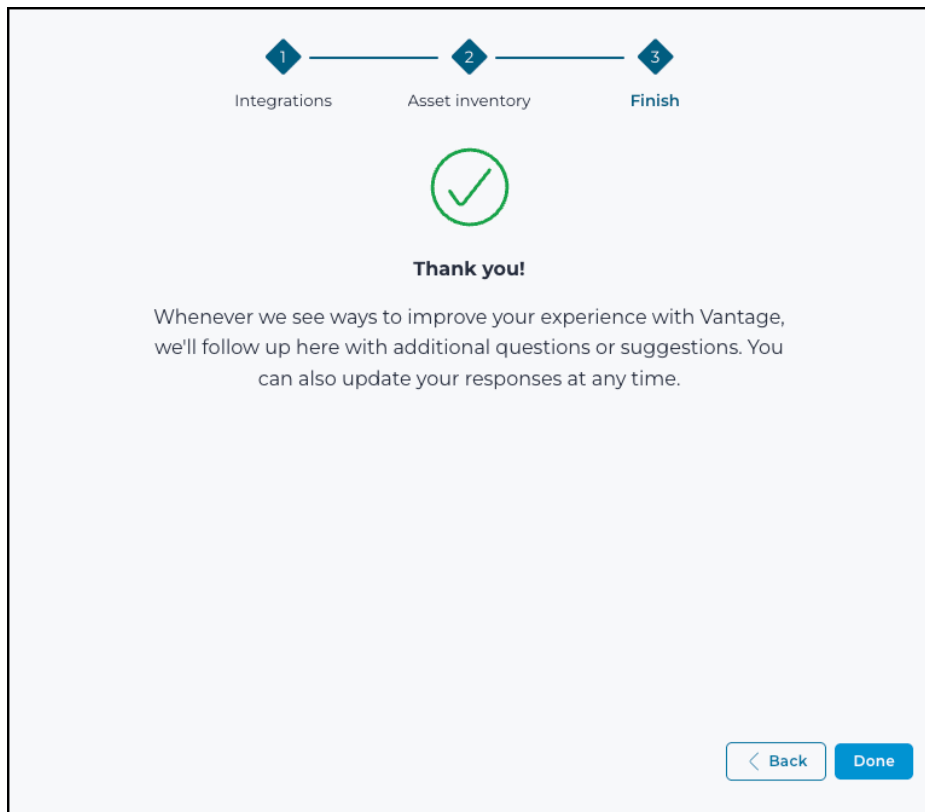


Figure 4. Finish page

Results

The setup is complete. Vantage uses this information to tailor support and improve asset visibility for your environment.

Chapter 2. Administration



Administration page

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

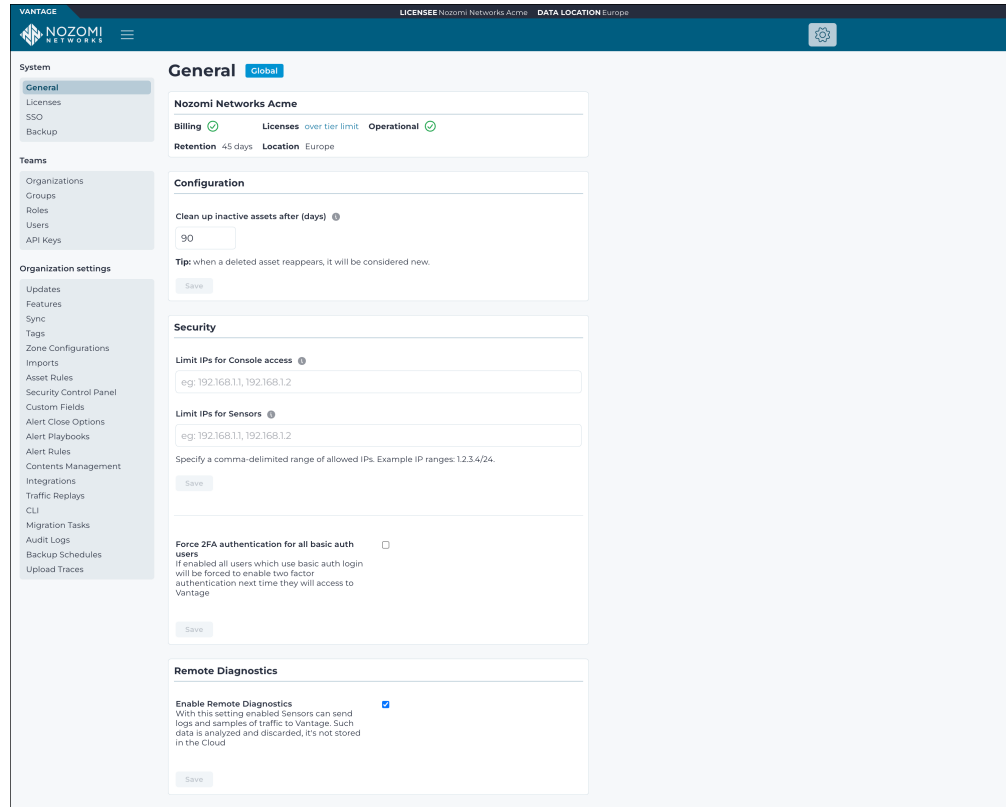


Figure 5. Administration page

System

The **System** section has these pages:

- [General](#) (on page 19)
- [Licenses](#) (on page 23)
- [SSO](#) (on page 24)
- [Backup](#) (on page 29)

Teams

The **Teams** section has these pages:

- [Organizations](#) (on page 30)
- [Groups](#) (on page 32)
- [Roles](#) (on page 45)
- [Users](#) (on page 48)
- [API Keys](#) (on page 59)

Organization settings

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

- [Updates \(on page 66\)](#)
- [Features \(on page 73\)](#)
- [Sensors Synchronization Settings \(on page 77\)](#)
- [Tags \(on page 79\)](#)
- [Zone Configurations \(on page 80\)](#)
- [Imports \(on page 91\)](#)
- [Asset Rules \(on page 103\)](#)
- [Security Control Panel \(on page 107\)](#)
- [Custom Fields \(on page 109\)](#)
- [Alert Close Options \(on page 112\)](#)
- [Alert Playbooks \(on page 115\)](#)
- [Alert Rules \(on page 119\)](#)
- [Contents Management \(on page 123\)](#)
- [Traffic Replays \(on page 129\)](#)
- [CLI \(on page 130\)](#)
- [Migration tasks \(on page 131\)](#)
- [Audit Logs \(on page 132\)](#)
- [Backup Schedules \(on page 133\)](#)
- [Upload Traces \(on page 137\)](#)
- [Arc dependencies \(on page 139\)](#)

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.

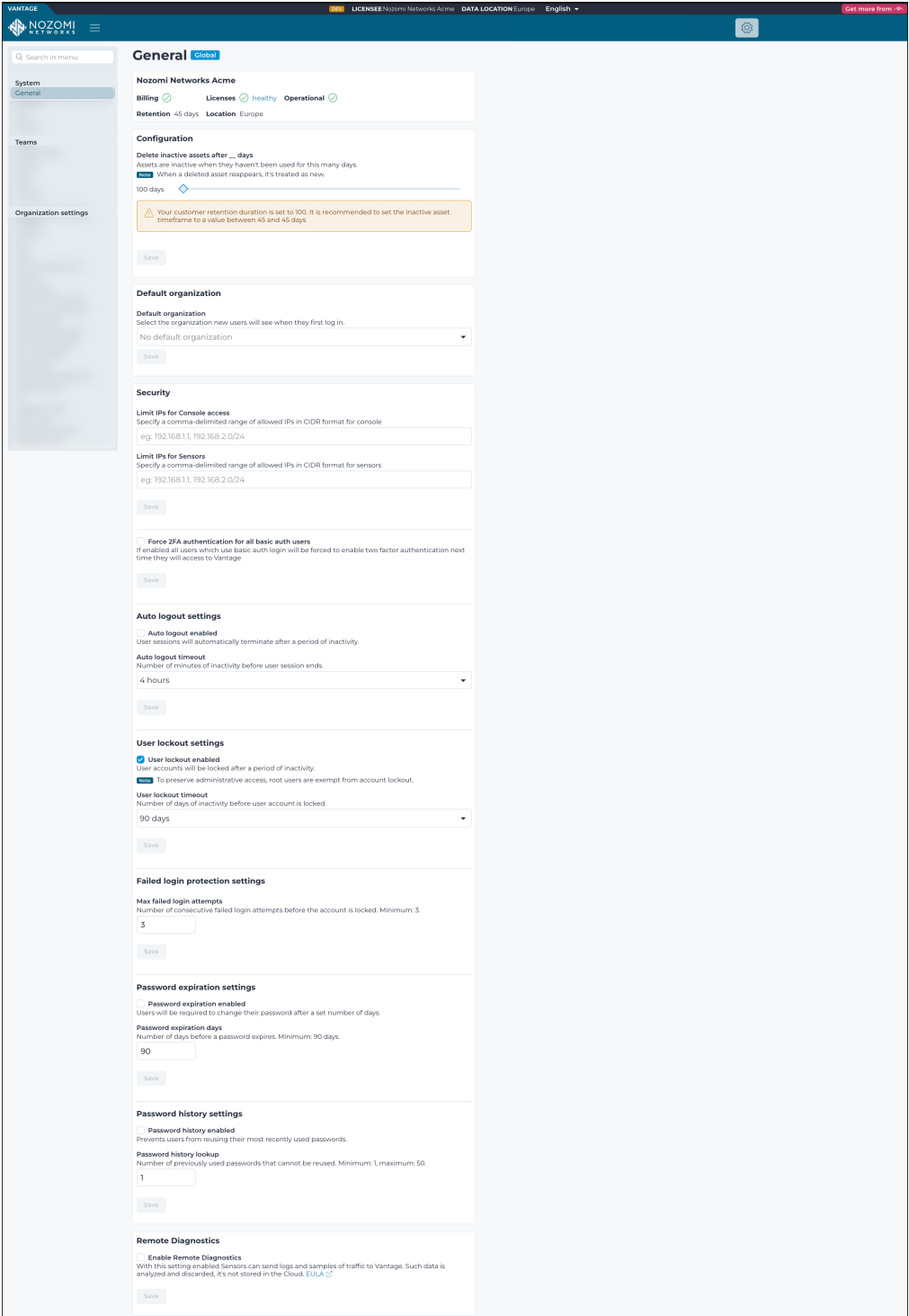


Figure 6. General page

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.

Default organization

The **Default organization** section lets you set the organization that new users are directed to at first login. Select an organization from the **Default organization** dropdown. To remove the default, clear the selection.

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.

Auto logout settings

The **Auto logout settings** section lets you automatically log out inactive users with browser windows or tabs open. When enabled, Vantage logs out users after the specified inactivity period. You can configure:

- **Auto logout enabled:** Enable or disable automatic logout for inactive users
- **Auto logout timeout:** Set the inactivity period before automatic logout occurs

Admin and root users can disable this behavior with the **Auto logout enabled** toggle.

User lockout settings

The **User lockout settings** section lets you automatically lock user accounts after a period of inactivity. This improves security. When enabled, users who do not log in within the configured period are automatically locked out. You can configure:

- **User lockout enabled:** Enable or disable automatic user account lockout for inactivity
- **User lockout timeout:** Set the number of days of inactivity before a user account is locked (30, 60, or 90 days)

**Note:**

Root users are exempt from account lockout to preserve administrative access.

**Note:**

You cannot change user lockout settings on [Federal Risk and Authorization Management Program \(FedRAMP\)](#) instances.

When this setting is enabled, you can manage individual user lockout behavior from the **Users** page with these actions:

- **Allow lock after inactivity:** Allow the user account to be automatically locked due to inactivity
- **Prevent inactivity lock:** Prevent the user account from being automatically locked due to inactivity
- **Unlock user (inactivity):** Unlock user accounts that have been locked due to inactivity

When you disable this setting, users retain access to Vantage and these actions are not available.

Failed login protection settings

The **Failed login protection settings** section lets you automatically lock user accounts after a set number of consecutive failed login attempts.

Max failed login attempts: Number of consecutive failed login attempts before the account is locked. The minimum value is 3.

Password expiration settings

The **Password expiration settings** section lets you require users to change their password after a set number of days. You can configure:

- **Password expiration enabled:** Enable or disable the password change requirement
- **Password expiration days:** Number of days before a password expires. The minimum value is 90 days.

Admin and root users can disable this behavior with the **Password expiration settings** toggle.

Password history settings

The **Password history settings** section prevents users from reusing their most recently used passwords.

Password history enabled: Enable or disable password history.

Password history lookup: Number of previously used passwords that cannot be reused. The minimum value is 1, and the maximum value is 50.

Admin and root users can disable this behavior with the **Password history settings** toggle.

Remote diagnostics

The **Remote diagnostics** section lets you enable remote diagnostics for your Vantage instance, which allows Nozomi Networks support to access diagnostic information for troubleshooting purposes.

Licenses

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

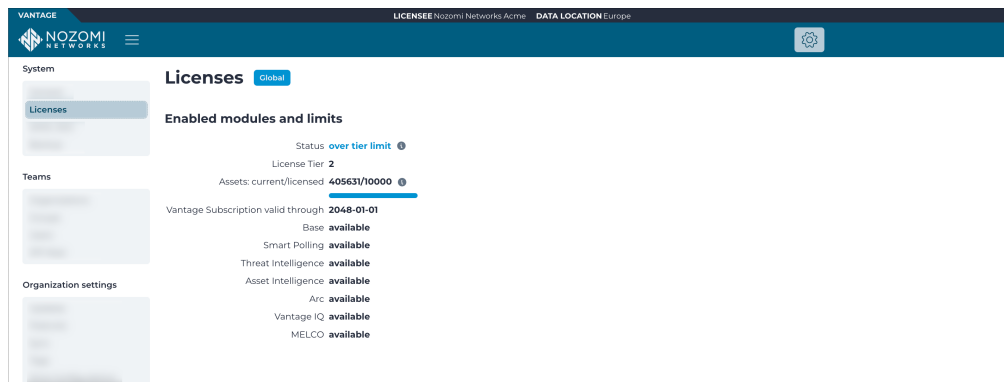


Figure 7. Licenses page

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.

The screenshot shows the 'SAML Single Sign On' configuration page in the Vantage Networks administrator interface. The page has a dark blue header with the 'VANTAGE' logo, 'NOZOMI NETWORKS' branding, and navigation links for 'LICENSEE', 'DATA LOCATION', and 'Europe'. A sidebar on the left contains a 'System' menu with 'SSO' selected, and 'Teams' and 'Organization settings' sections. The main content area is titled 'SAML Single Sign On' with a 'Global' toggle. It features a 'SAML SSO' tab and an 'Identity Provider' sub-tab. The configuration includes a checkbox to 'Enable SAML Single Sign on' (checked), a 'Metadata XML' upload section with a 'Choose File' button, and input fields for 'Entity ID' (https://sts.windows.net), 'Role attribute' (http://schemas.micros), and 'AuthnContext' (unchecked). A 'Save' button is at the bottom.

Figure 8. SAML SSO page

The SSO page has these tabs:

- [SAML SSO \(on page 25\)](#)
- [Identity Provider \(on page 26\)](#)

Related information

[SAML integration configuration \(on page 155\)](#)

[IdP configuration for SAML integration \(on page 156\)](#)

[Troubleshooting SAML integration \(on page 160\)](#)

[Configure your IdP for SAML integration \(on page 157\)](#)

[Configure Vantage for SSO \(on page 158\)](#)

[Configure a Google Workspace SAML application \(on page 161\)](#)

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 Global

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

Role attribute
Specify the Role attribute used to pass SAML roles of the user logging in

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

Save

Figure 9. 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).

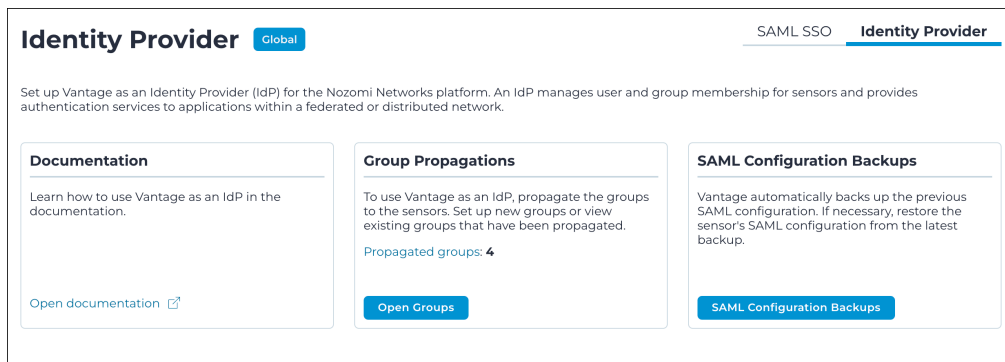


Figure 10. Identity Provider page

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 \(on page 27\)](#).

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**.

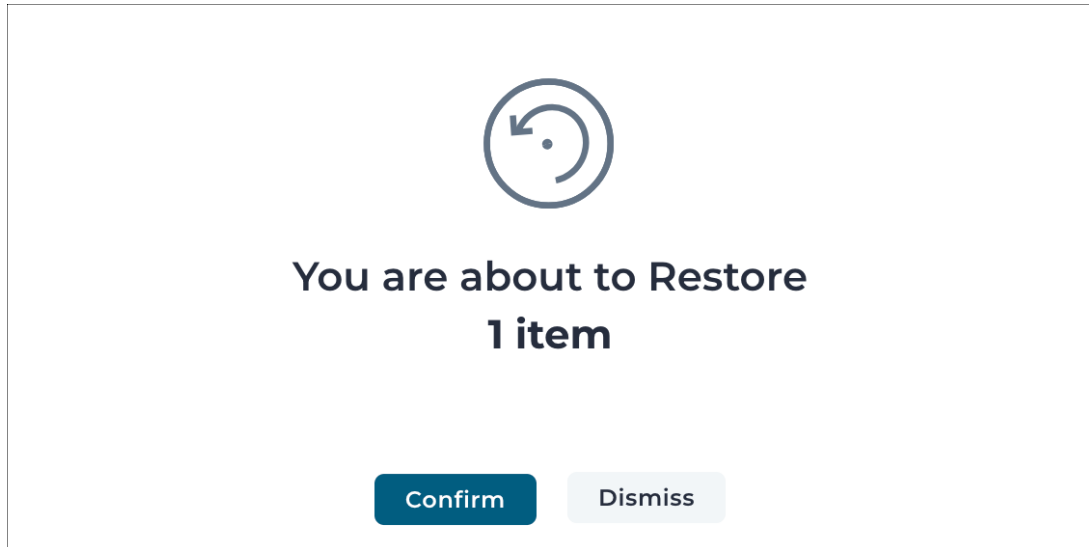


Note:

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**.



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.

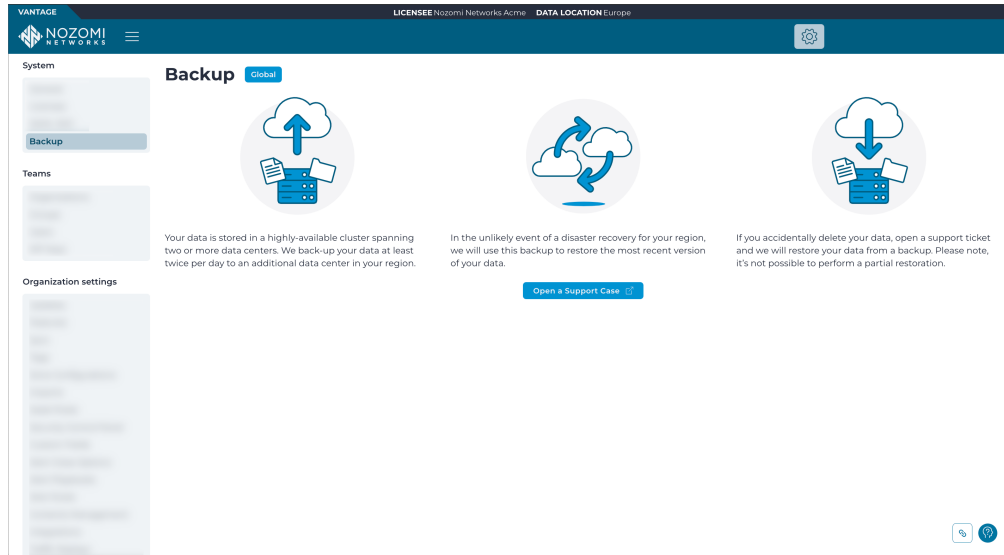


Figure 11. Backup page

Teams

Organizations

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

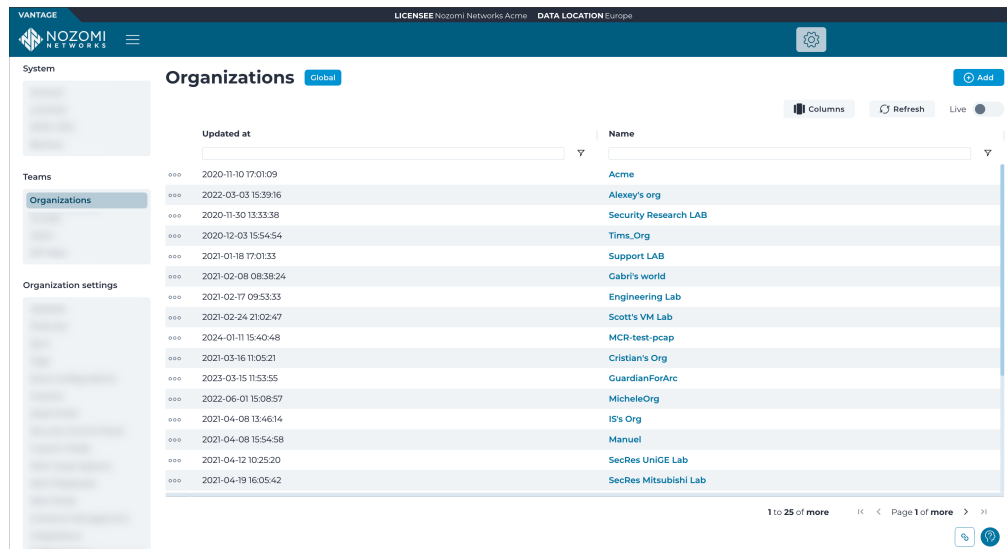


Figure 12. Organizations page

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.

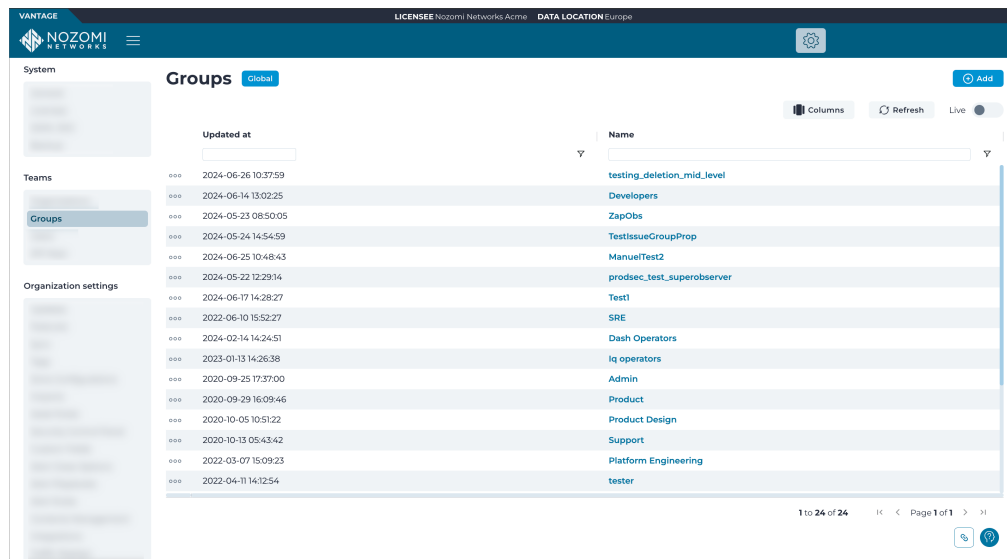


Figure 13. Groups page

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 \(on page 33\)](#).

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 \(on page 36\)](#).

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.

Read-Only

2024-09-20 20:23:34

Actions

Propagation settings

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

Add Scope

organization

ENG CH LAB - MASTER

X

☐ 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.

Save

Figure 14. 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

Read-Only 2026-09-20 20:23:54 Actions

Propagation settings

① 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

Add Scope

organization
ENG CH LAB - MASTEF X

☐ **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

Save

Figure 15. 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

Add 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.

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

Figure 16. 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**.

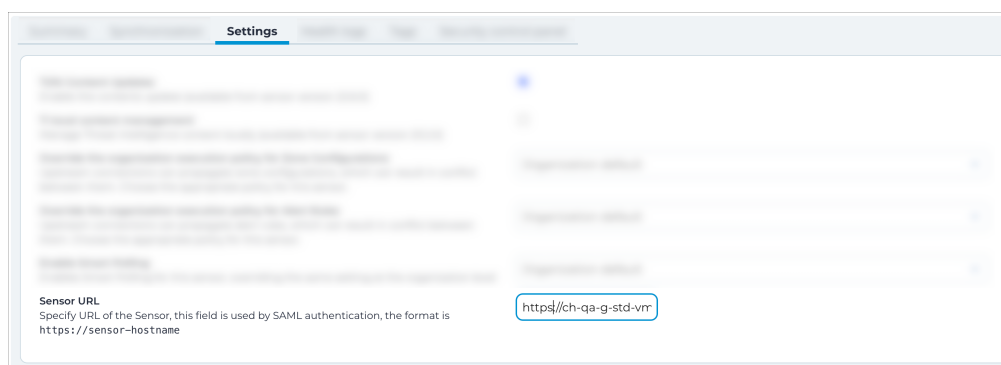


Figure 17. Sensor URL field

**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 [CMCs](#): 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 let the users 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

1 to 5 of 60

IK

<

Page 1 of 12

>

>I

Confirm

Cancel

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

Users

Groups

OpenAPI Keys

Active Directory

LDAP

SAML

Page 1 of 1, 3 entries

Live ☒

+ Add

Import from Active Directory

Import from LDAP server

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

Users

Groups

OpenAPI Keys

Active Directory

LDAP

SAML

Nozomi URL

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

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.

Delete configuration

SAML role attribute key

 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.

Save

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.

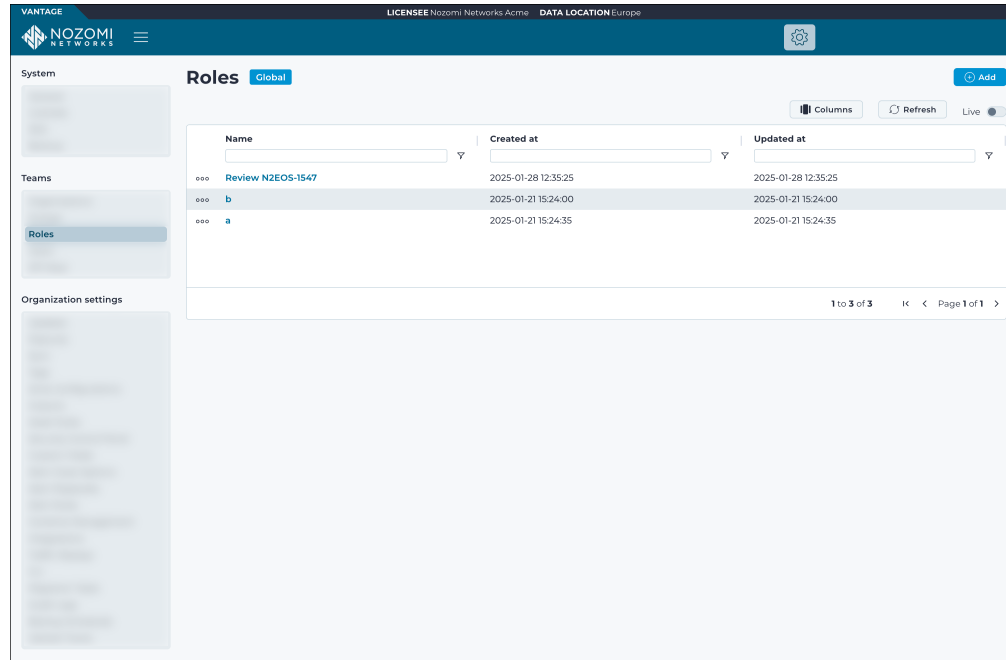


Figure 18. Roles page

You can assign roles that show in the list to a group. For more details, see [Assign a role to a group \(on page 36\)](#).

Add

This button lets you [add a new role \(on page 46\)](#).

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

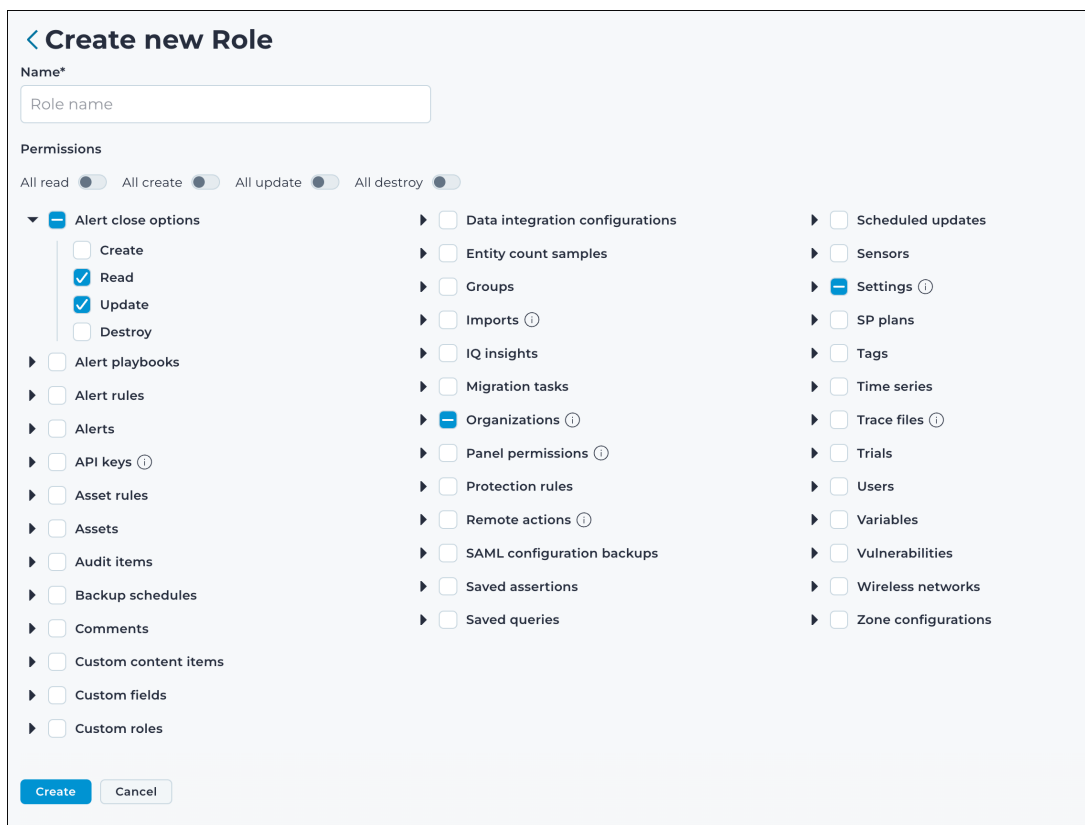
The **Live**  toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

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.



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 \(on page 36\).](#)

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

Figure 19. Users page

General

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

- [SAML users \(on page 48\)](#)
- [Local users \(on page 49\)](#)



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 \(on page 32\)](#)
- [SAML integration configuration \(on page 155\)](#)

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 \(on page 59\)](#).

Invite

This button lets you [Invite a user \(on page 50\)](#) 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

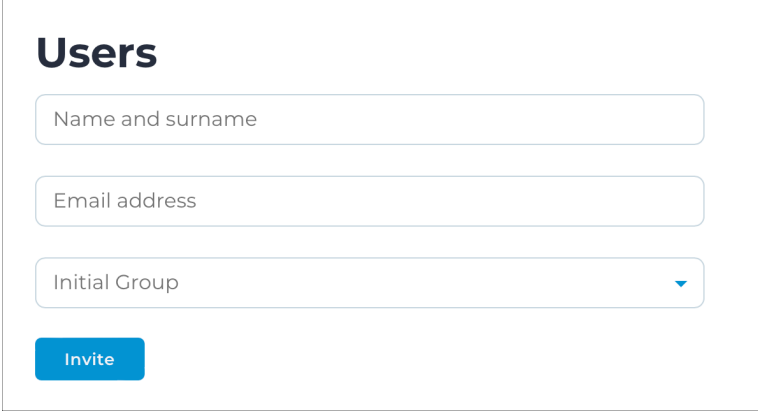
The **Live**  toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

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.



The screenshot shows a form titled "Users" with three input fields: "Name and surname", "Email address", and "Initial Group" (a dropdown menu). Below the fields is a blue button labeled "Invite".

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:

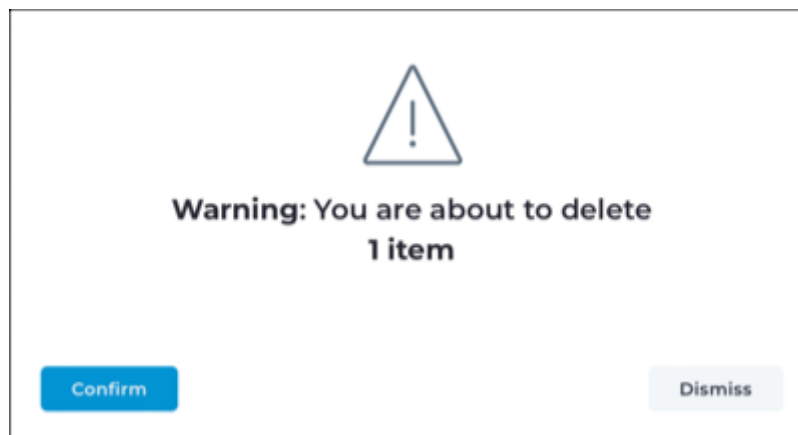
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the  icon

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**.



Result: A confirmation dialog shows.

6. Select **Confirm**.

Results

The user has been deleted.

Manage user lockout settings

You can use the **Users** page to control whether individual users are subject to automatic lockout after inactivity.

Before you begin

You must enable user lockout settings on the **General** page before these actions are available.

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 the appropriate action.

Choose from:

- **Allow lock after inactivity:** The user account will be locked if they do not log in within the configured period
- **Prevent inactivity lock:** The user account will not be locked due to inactivity

6. Select **Confirm**.

Results

The user lockout setting has been updated.

Unlock a user (inactivity)

You can use the **Users** page to unlock a user account that was automatically locked due to inactivity.

Before you begin

This action is only available for users who have been locked due to inactivity based on the configured user lockout settings.

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 **Unlock user (inactivity)**.
Result: A confirmation dialog shows.
6. Select **Confirm**.

Results

The user account has been unlocked and the user can log in again.

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 the Nozomi Networks [API](#) to update data in Vantage, or to retrieve data from it. Through various [API](#) endpoints, 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 \(on page 58\)](#).

Application IP address ranges

Your applications might connect from a completely different [IP](#) address range than your other Vantage users. For example, your [security information and event management \(SIEM\)](#) 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 \(on page 55\)](#)
- [User scope and permissions \(on page 56\)](#)

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 \(on page 58\)](#).

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.

User Display name	Key name	Description	Last sign in at	Last sign in ip	Allowed ips	Linked organiz
	AK30257a	n.a.	n.a.	n.a.	n.a.	Acme
	AK376a6a	Dashboard	n.a.	n.a.	n.a.	Data Engineer
	test_01	n.a.	2021-07-28 15:31:37	93.41.236.63	n.a.	n.a.
	AK03dcb8	test1	n.a.	n.a.	12.3.4/24	n.a.
	AK6e7522	test	n.a.	n.a.	n.a.	n.a.
	AK44fd9e	n.a.	n.a.	n.a.	n.a.	n.a.
	AK79e0f1	xxx	n.a.	n.a.	12.3.4/24	n.a.
	AK70e90f	asdasdasd	n.a.	n.a.	12.3.4/24	n.a.
	AK6e790f	qwewqe	n.a.	n.a.	12.3.4/24	n.a.
	AK5bdf0e	Swagger	n.a.	n.a.	0.0.0.0/32	n.a.
	AKef15d5	postman	2021-09-01 11:54:50	93.41.236.63	n.a.	n.a.
	AK13ec27	test_02	2021-10-11 14:09:13	2.238.193.136	n.a.	n.a.
	AK87c429	Used to validate sample	2021-09-15 14:59:41	146.241.71.42	n.a.	n.a.
	AK6a0544	pipoo	n.a.	n.a.	n.a.	n.a.
	AK096d20	traefik test	2021-10-05 16:01:43	2.238.193.136	n.a.	n.a.
	AK5dc921	moreno	2022-01-12 07:25:53	87.15.230.149	n.a.	n.a.

Figure 20. 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. Once a key is created, it cannot be edited, it can only be revoked or rotated.

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

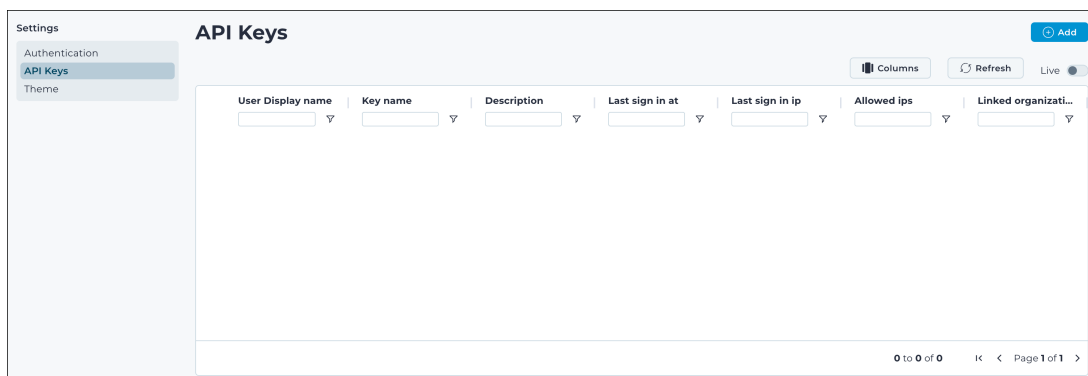
Once an [API](#) key has been created, you cannot edit it. You can only revoke it.

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**.



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 ⓘ

Generate Cancel

**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 \(on page 19\)](#) 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**

The screenshot shows the 'Restricted privileges' configuration window. At the top, 'User privileges' and 'Restricted privileges' are radio buttons, with 'Restricted privileges' selected. Below this are four radio buttons for 'All read', 'All create', 'All update', and 'All destroy'. The main area contains a grid of permissions, each with a checkbox and an expandable arrow. The permissions are organized into three columns. The 'Settings' option is highlighted with a blue square. At the bottom, there are 'Generate' and 'Cancel' buttons.

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

Revoke an API key in Vantage to immediately disable access for that credential. This action is irreversible and should be used when a key is no longer needed or may be compromised. Revoking a key does not impact other active keys.

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: A dialog shows.

6. Select **Confirm**.

Results

The [API](#) key has been revoked.

Rotate an API key

Rotate an existing API key in Vantage to replace it with a new one while maintaining access continuity. Key rotation enhances security by minimizing the risk of compromised credentials.

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 rotate.

Result: The  icon shows.

5. Select the  icon.

Result: A dialog shows.

6. Select **Confirm**.

Results

The [API](#) key has been rotated.

Organization Settings

Updates

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

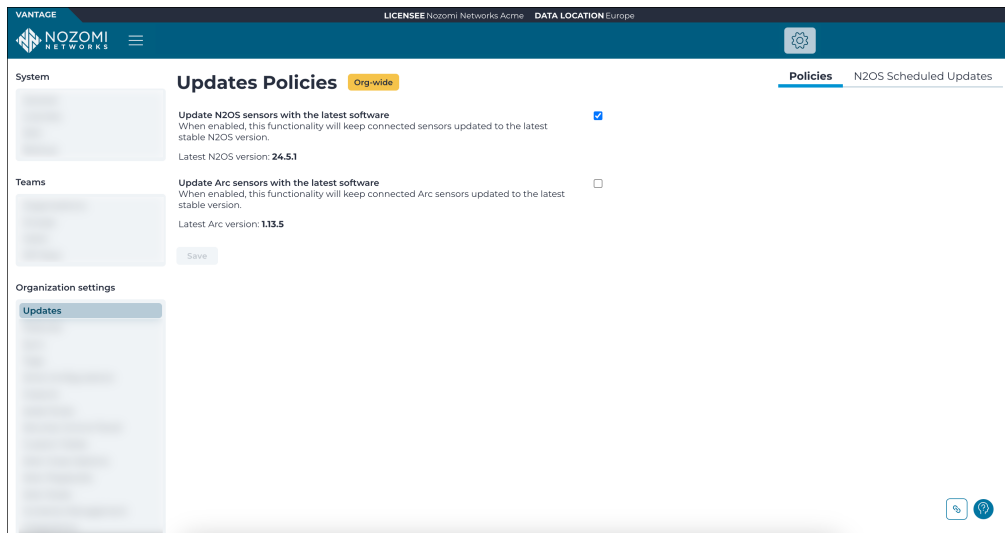


Figure 21. Updates page

The **Updates** pages has these tabs:

- [Policies](#) (on page 67)
- [N2OS Scheduled Updates](#) (on page 68)

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.

The screenshot shows the 'Updates Policies' page. At the top, there's a header with 'Updates Policies' and a yellow 'Org-wide' tag. To the right, there are two tabs: 'Policies' (which is active and underlined) and 'N2OS Scheduled Updates'. The main content area has two sections. The first section is titled 'Update N2OS sensors with the latest software'. It includes a description: 'When enabled, this functionality will keep connected sensors updated to the latest stable N2OS version.' and a checkbox that is checked. Below this, it says 'Latest N2OS version: 24.5.1'. The second section is titled 'Update Arc sensors with the latest software'. It includes a description: 'When enabled, this functionality will keep connected Arc sensors updated to the latest stable version.' and an unchecked checkbox. Below this, it says 'Latest Arc version: 1.13.5'. At the bottom left of the form, there is a 'Save' button.

Figure 22. 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.

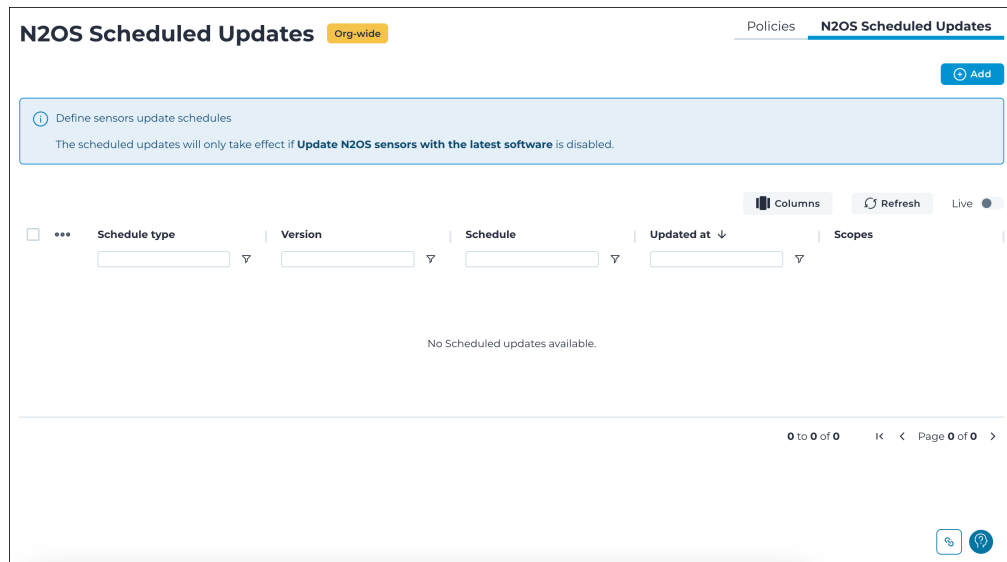


Figure 23. N2OS Scheduled Updates page

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

[Add Scope](#) 

 **No scope selected**
This will be propagated to all sensors of this organization

[Create](#)

Figure 24. 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 25. 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

Add Scope ▾

No scope selected
This will be propagated to all sensors of this organization

Create

Figure 26. 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

Add Scope

No scope selected

This will be propagated to all sensors of this organization

Create

Figure 27. 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.

The screenshot shows the Vantage web interface. The top navigation bar includes the Vantage logo, user information (LICENSEE: Nozomi Networks Acme, DATA LOCATION: Europe), and an Administration link. A left sidebar contains a search bar and menu items for System, Teams, and Organization settings, with the Features page selected. The main content area is titled 'Features' and has two tabs: 'General' (active) and 'Wireless'. The 'General' tab contains several sections: 'General' with checkboxes for 'Experimental and preview features' (checked) and 'Use Dashboards as home page' (unchecked); 'Sensor Stale Interval' with a slider set to 2h; 'Asset Inventory' with 'Smart Polling' and 'Discovery' both set to 'Enabled'; 'Vantage IQ' with 'Show Vantage IQ summaries' (checked) and 'Disable external processing for Vantage IQ Assistant' (checked); and 'Policies' with dropdowns for 'The default execution policy for Zone Configurations' (Disable vantage execution policy), 'The default execution policy for Alert Rules' (Local prevails), 'Alert deduplication' (Default), and 'Asset intelligence enrichment strategy' (Safe enrichment). A 'Create Windows CVEs only if hotfixes are known' checkbox is also present. A 'Save' button is at the bottom.

Figure 28. Features page

The **Features** page has these tabs:

- [General \(on page 74\)](#)
- [Wireless \(on page 76\)](#)

General

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

Features | Organization

General | Wireless

General

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

Asset Inventory

Smart Polling
Enables Smart Polling license on all sensors in this organization. The license can be enabled/disabled on individual sensors as well, and it overrides the organization value.
Enabled

Discovery
Enables Discovery (standard lightweight announcements to discover neighboring devices). This setting can be enabled or disabled on the individual sensors as well, and it overrides the organization value.
Enabled

Vantage IQ

☒ **Show Vantage IQ summaries**
AI-generated intelligent summaries will be displayed across product pages to help you quickly understand key information. This automated summary can be toggled off to hide it throughout Vantage.

☐ **Disable external processing for Vantage IQ Assistant**
Standard processing uses external servers to enable full AI capabilities. Data sent to external servers is never stored. Disabling external processing keeps data within your Vantage infrastructure but limits available features due to local processing constraints. In both cases, your data is never used for model training.

Policies

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

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

Alert deduplication
Groups matching alerts to reduce duplicates. Alert details include timestamps and occurrence count. Requires sensor version 25.1.0 or later.
Default

Asset intelligence enrichment strategy
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.
Safe enrichment

☒ **Create Windows CVEs only if hotfixes are known**
When this is checked, Windows CVEs are not created for assets whose hotfixes are not yet known, which avoids creating CVEs that may have already been mitigated.

Save

Figure 29. Features page

General

Experimental and preview features: This checkbox lets you enable/disable the use of experimental and preview features across the organization. These features are still in development and might change.

Use Dashboards as home page: This checkbox lets users set a customized dashboard as their home page. When disabled, the default overview pages are shown instead.

Sensor stale interval: Sets the threshold in hours after which a sensor is considered stale if it has not sent updates. This setting helps monitor sensor responsiveness.

Asset inventory

Enable Smart Polling: Enables Smart Polling for all sensors in the organization. This setting can be overridden by individual sensor configurations if they differ. You can select one of these options:

- Disabled
- Enabled

Discovery: Enables lightweight announcements for discovering neighboring devices. If disabled here, the setting is controlled at the sensor level. You can select one of these options:

- Disabled
- Enabled

Policies

The default execution policy for Zone Configurations: Determines whether upstream connections can overwrite zone configurations. Use this setting to prevent configuration conflicts. You can choose between these options:

- Disable vantage execution policy
- Local only
- Upstream only
- Apply all

The default execution policy for Alert Rules: Defines whether alert rules from upstream sources can override local configurations. Prevents alert conflicts by enforcing one source of truth.

Alert deduplication: Groups repeated alerts of the same type that share identical deduplication key values, instead of creating a separate alert entry each time. The expert view on the **Alerts** page shows the first and last occurrence timestamps and the total count for each grouped alert. This setting was previously only available via [command-line interface \(CLI\)](#). You can select one of these options:

- Enabled
- Disabled
- Default

For more details, see the **Alert deduplication** topic in the **Vantage User Guide** under **Alerts**.

Asset Intelligence enrichment strategy: Specifies how machine learning is used to enhance assets with enriched context such as classification or confidence levels. You can choose from these options:

- High confidence only
- Safe enrichment: Discards uncertain predictions when enriching assets
- Aggressive enrichment: Allows uncertain predictions when enriching assets

Changes can take up to 48 hours to take effect.



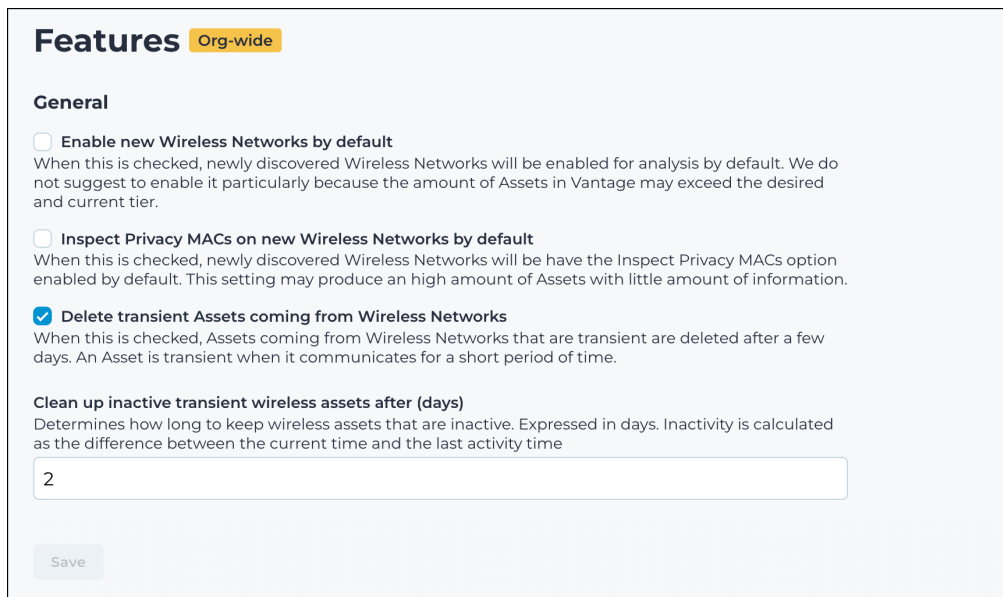
Note:

Safe and aggressive strategies are only available from version [Nozomi Networks Operating System \(N2OS\) v23.1.0](#) onward.

Create Windows CVEs only if hotfixes are known: Prevents creation of [CVEs](#) for Windows assets with unknown hotfix status. This avoids reporting issues that might have already been resolved.

Wireless

The **Wireless** page lets you configure Vantage settings for managing wireless networks, including how new networks and assets are handled.



The screenshot shows the 'Features' page for 'Wireless' settings. At the top, there's a header 'Features' with a yellow 'Org-wide' tag. Below this is a 'General' section. It contains three settings: 1. 'Enable new Wireless Networks by default' with an unchecked checkbox and a description: '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.' 2. 'Inspect Privacy MACs on new Wireless Networks by default' with an unchecked checkbox and a description: '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.' 3. 'Delete transient Assets coming from Wireless Networks' with a checked checkbox and a description: '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.' Below these is a section 'Clean up inactive transient wireless assets after (days)' with a description: 'Determines how long to keep wireless assets that are inactive. Expressed in days. Inactivity is calculated as the difference between the current time and the last activity time'. There is a text input field containing the number '2'. At the bottom left is a 'Save' button.

Figure 30. Features page

Enable new Wireless Networks by default

When enabled, newly discovered wireless networks are automatically available for analysis. This option may generate a large number of assets in Vantage and should be used with caution.

Inspect Privacy MACs on new Wireless Networks by default

When enabled, Vantage inspects privacy MAC addresses on new wireless networks by default. This setting can increase the number of assets with limited identifying information.

Delete transient Assets coming from Wireless Networks

Removes transient assets from wireless networks after a short time. Transient assets are devices that connect briefly and do not remain active.

Clean up inactive transient wireless assets after (days)

Defines how long inactive transient wireless assets are kept before deletion. The value is expressed in days and is calculated based on the difference between the current time and the last recorded activity.

Sensors Synchronization Settings

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

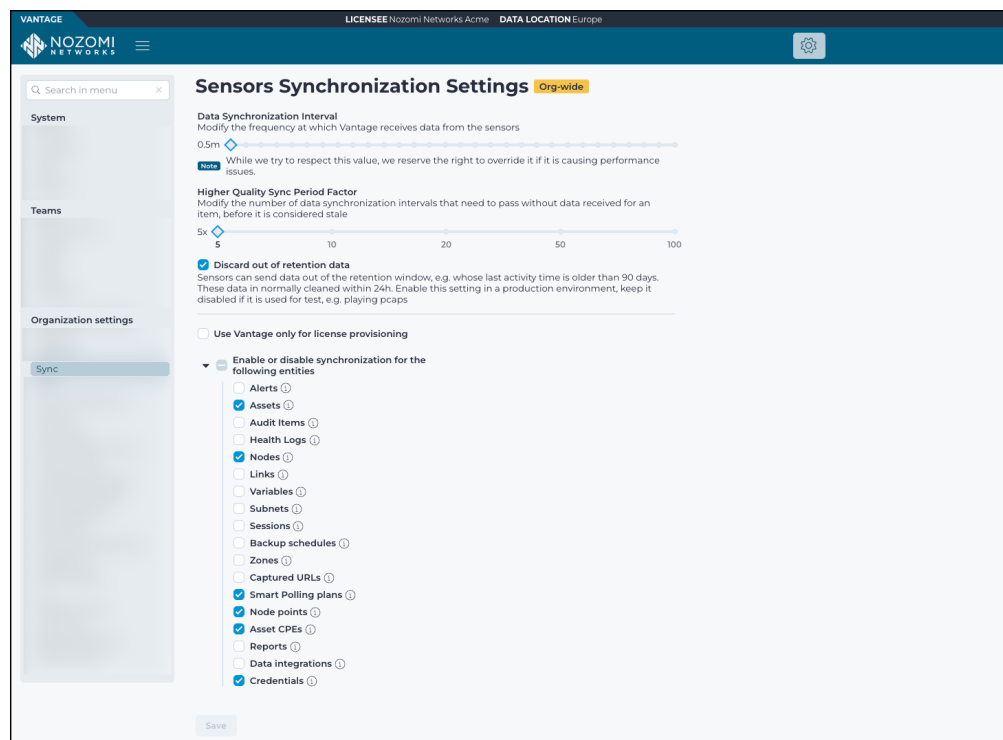


Figure 31. Sync page

Data Synchronization Interval

The **Data Synchronization Interval** setting controls how frequently Vantage receives updates from sensors. You can use the slider to adjust the interval. Shorter intervals enable more frequent data transfers and longer intervals reduce the load on the system.

Although the system attempts to respect the selected interval, Nozomi Networks might override it if there are performance issues. This ensures system stability while maintaining data availability.

When choosing a synchronization interval, consider the trade-off between data freshness and system performance. In high-performance or data-sensitive environments, shorter intervals may be preferred.

Higher Quality Sync Period Factor

The **Higher Quality Sync Period Factor** setting defines how many synchronization intervals must pass without receiving new data for an item before Vantage considers it stale.

You can use the slider to adjust this setting. A higher factor allows more time before data is flagged as stale, which is useful for less frequently updated sensors or non-critical data. A lower factor tightens the threshold, prompting the system to replace local data views more frequently with those from the downstream appliance.

Set this value based on the expected reporting frequency of your sensors and the criticality of the data they provide. Balancing sensitivity and tolerance helps avoid false positives while maintaining visibility into sensor health.

Discard out of retention data

Enable the **Discard out of retention data** checkbox to automatically remove sensor data that falls outside the configured retention window. For example, if a sensor sends data with a timestamp older than 90 days, Vantage discards it instead of storing or processing it.

This setting helps maintain data hygiene in production environments by ensuring that outdated data does not interfere with current analysis. Vantage typically removes this data within 24 hours.

Disable this setting if you are testing with archived or historical data, such as during [packet capture \(pcap\)](#) replays or forensic investigations. In production, keep it enabled to reduce storage usage and maintain data accuracy.

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.

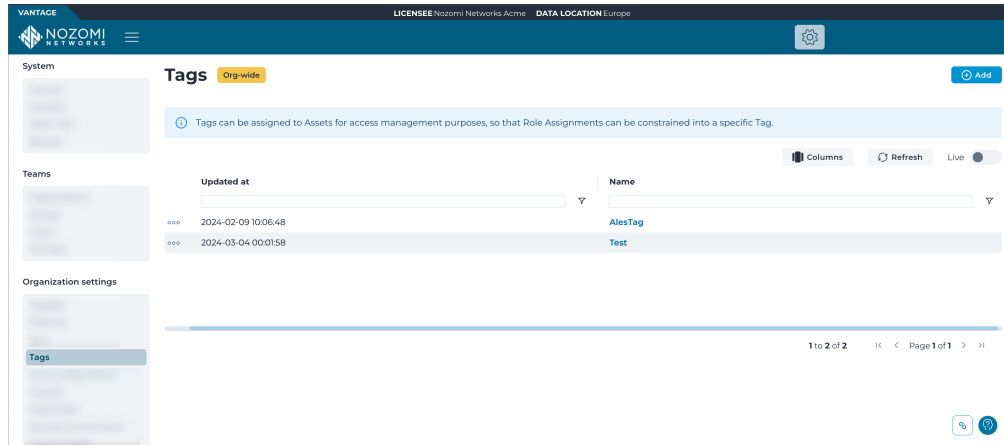


Figure 32. Tags page

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.

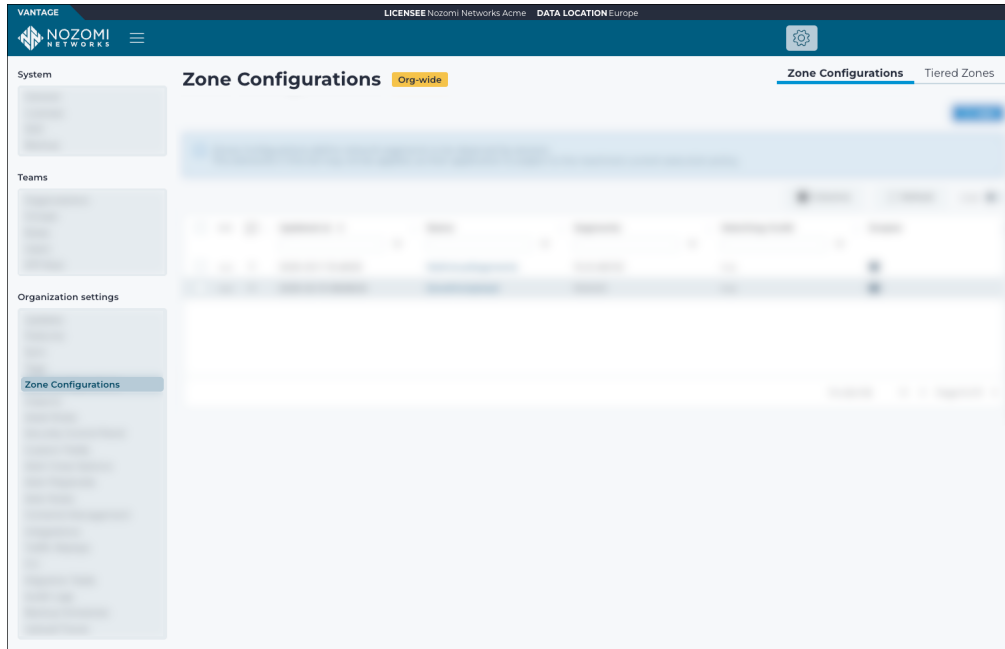


Figure 33. Zone Configurations page

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 \(on page 81\)](#)
- [Tiered Zones \(on page 88\)](#)

Zone Configurations

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

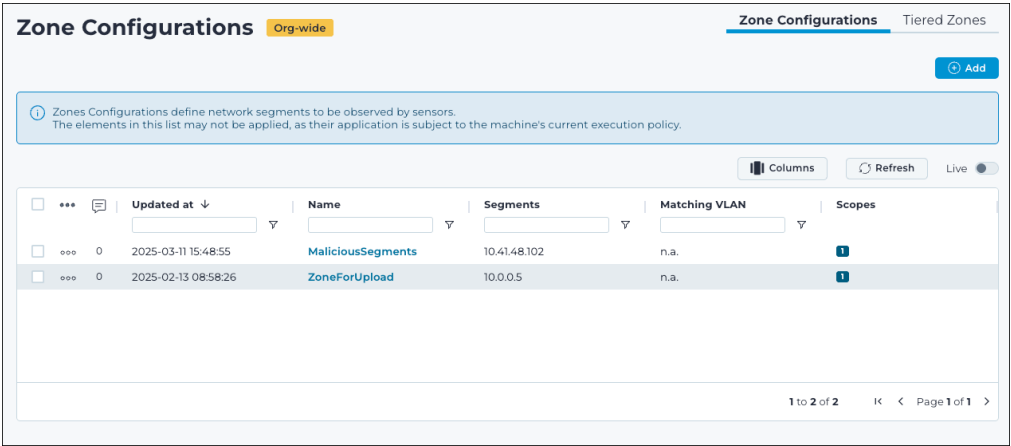


Figure 34. Zone Configurations page

Add

This button lets you [add a new zone configuration \(on page 82\)](#).

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

You can use the **Zone Configurations** page to add a new zone configuration.

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.

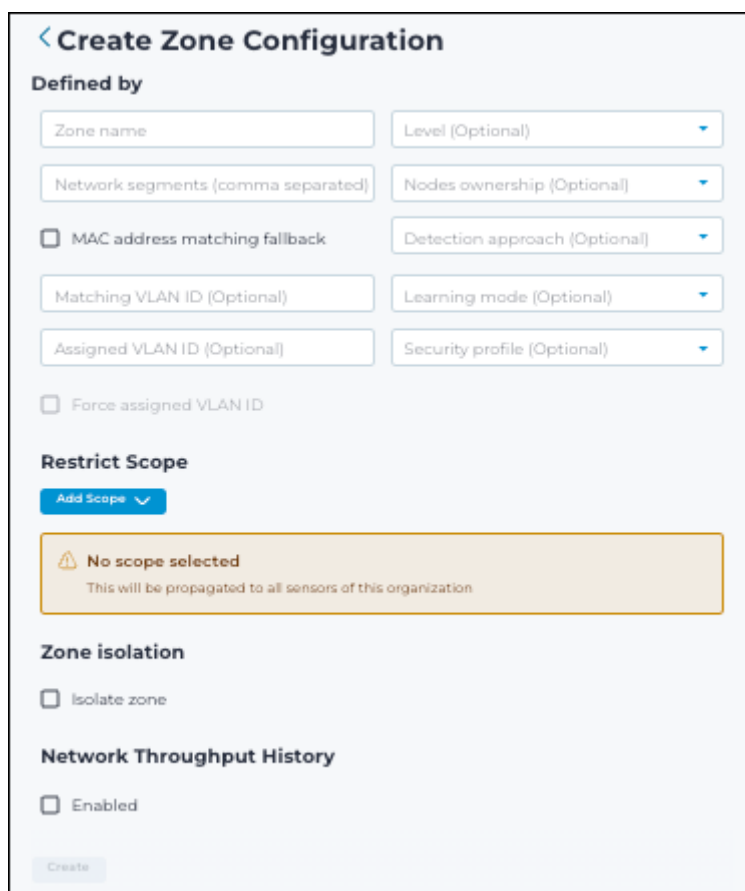
2. In the **Organization settings** section, select **Zone Configurations**.

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.



The screenshot shows the 'Create Zone Configuration' form. It has a title bar with a back arrow and the title 'Create Zone Configuration'. Below the title is a section 'Defined by' containing several input fields and dropdown menus: 'Zone name' (text input), 'Level (Optional)' (dropdown), 'Network segments (comma separated)' (text input), 'Nodes ownership (Optional)' (dropdown), 'MAC address matching fallback' (checkbox), 'Detection approach (Optional)' (dropdown), 'Matching VLAN ID (Optional)' (text input), 'Learning mode (Optional)' (dropdown), 'Assigned VLAN ID (Optional)' (text input), and 'Security profile (Optional)' (dropdown). There is also a checkbox for 'Force assigned VLAN ID'. Below this is a section 'Restrict Scope' with an 'Add Scope' button and a warning box stating 'No scope selected' and 'This will be propagated to all sensors of this organization'. The next section is 'Zone isolation' with an 'Isolate zone' checkbox. Below that is 'Network Throughput History' with an 'Enabled' checkbox. At the bottom is a 'Create' button.

**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 [CMCs](#) 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 \(on page 86\)](#) thru [20 \(on page 86\)](#) 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.

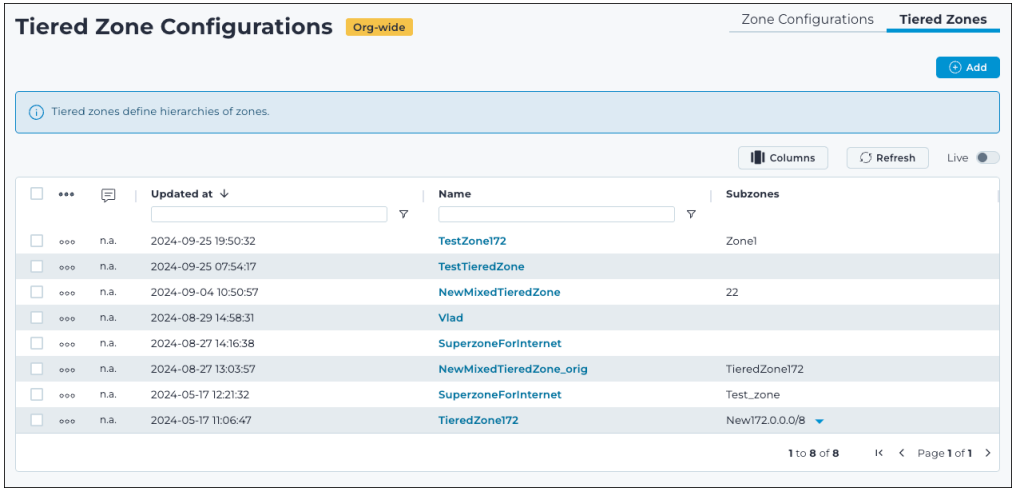


Figure 35. Tiered Zones page

Add

This button lets you [Add a tiered zone configuration \(on page 89\)](#).

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.

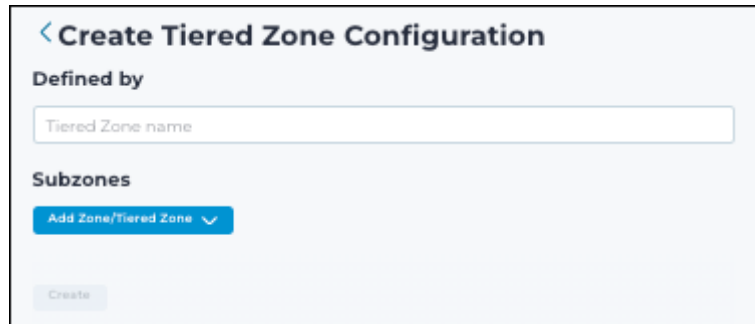
About this task

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

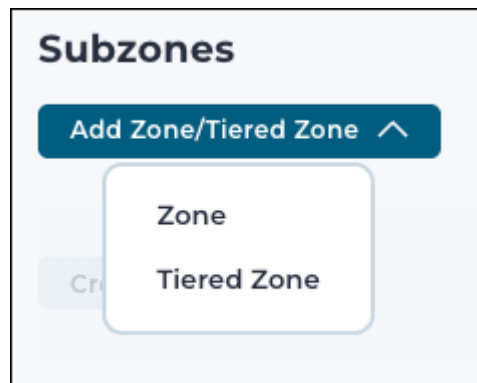
Procedure

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.



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 is organized into four tabs where you can view the history of completed imports and start new ones: **Assets**, **Arc**, **Zone Configurations**, and **N2OS Content Packs**.

The screenshot shows the 'Imports' page in the Nozomi Vantage interface. The page has a sidebar with navigation options: System, Teams, Organization settings, and Imports (selected). The main content area is titled 'Imports' and has a sub-tab 'Org-wide'. Below the title, there is a message: 'You can see the list of imported Assets.' and an 'Add' button. A table displays the list of imported assets with columns: Created at, User display name, Sensor host, File name, Vendor name, and Contents. The table contains 12 rows of data. At the bottom right, it shows '1 to 12 of 12' and 'Page 1 of 1'.

Created at	User display name	Sensor host	File name	Vendor name	Contents
2024-02-28 09:21:00.260	Alessandro Cavallaro	ch-qa-g-std-vm-gen...	test_import.csv	n.a.	("rules":["vi node 8...
2025-05-06 10:49:18.376	Paolo Di Francescanto...	ch-qa-g-std-vm-uploa...	to_import_lab_master...	n.a.	("rules":["vi node 62...
2025-04-25 13:31:30.629	Giacomo Matteucci	ch-qa-g-std-cnt-gen...	export_query_a2f20elb...	n.a.	("rules":["vi node 18...
2025-05-06 12:02:05.309	Paolo Di Francescanto...	ch-qa-g-std-vm-uploa...	import_new1.csv	n.a.	("rules":["vi node 75...
2025-05-06 12:31:23.277	Paolo Di Francescanto...	ch-qa-g-std-cnt-gen...	import_gen.csv	n.a.	("rules":["vi node 5f...
2025-06-13 09:04:23.028	Alessio Nava	1785e6b0428b	b1.csv	n.a.	("rules":["vi node 8c...
2025-06-17 12:50:39.354	Gerasimos Dimitriadis	1785e6b0428b	assets_7k.csv	n.a.	("rules":["vi node a6...
2025-06-13 09:35:45.244	Alessio Nava	1785e6b0428b	b2_csv	n.a.	("rules":["vi node 8c...
2025-06-13 09:40:48.845	Alessio Nava	1785e6b0428b	b2_csv	n.a.	("rules":["vi node 8c...
2025-06-17 11:16:28.037	Alessio Nava	ch-qa-g-std-vm-ha-ma...	a1.csv	n.a.	("rules":["vi node ec...
2025-06-25 13:44:17.452	Gerasimos Dimitriadis	ch-qa-g-std-vm-qualys...	test_import.csv	n.a.	("rules":["vi node 3b...
2025-09-02 17:01:08.030	Alessio Nava	1785e6b0428b	pluto.csv	n.a.	("rules":["vi node 1f...

Figure 36. Imports page

Imports tabs

The **Imports** page has these tabs:

Assets

Lists all confirmed asset imports, including hardware configuration and project files. For more details, see [Import assets \(on page 93\)](#).

Arc

Lists all confirmed Arc data archive imports. For more details, see [Import an Arc data archive \(on page 96\)](#).

Zone Configurations

Lists all confirmed zone configuration imports. For more details, see [Import zone configurations \(on page 98\)](#).

N2OS Content Packs

Opens the **Content Packs** page, where you can manage **N2OS** content pack imports. For more details, see [Import an N2OS content pack \(on page 101\)](#).

Columns

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

Live

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

Refresh

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

Import assets

You can import asset information into Vantage by uploading a hardware configuration file, a project file, or a CSV file.

Procedure

1. In the top navigation bar, select .
Result: The administration page opens.
2. In the **Organization settings** section, select **Imports**.
Result: The **Imports** page opens.
3. Select the **Assets** tab.
4. Select **Add**.
Result: The **Import assets** page opens.
5. In the **Sensor** dropdown list, select the sensor to import the data into.

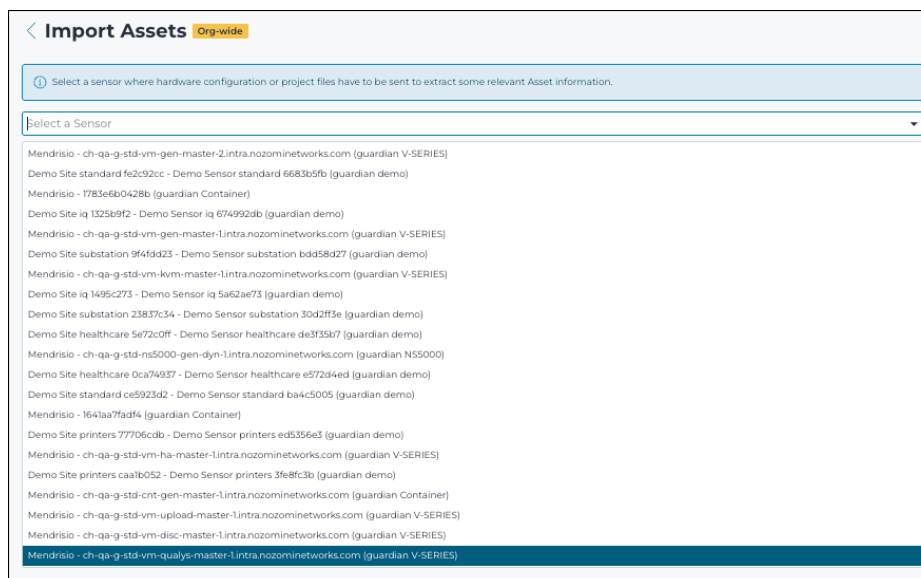


Figure 37. Import assets - sensor selection

6. Drag and drop your file onto the upload area, or select **Choose a file from your computer**.

A list of **Allowed formats** shows.

Result: Vantage detects the file format and shows a confirmation message.

- For non-*comma-separated value (CSV)* files (hardware configuration or project files), the **File options** step shows immediately.
- For *CSV* files, the **File options** step shows after the format is confirmed.

The screenshot shows the 'Import Assets' interface. At the top, there's a header with a back arrow, the title 'Import Assets', and a 'Org-wide' tag. Below the header is a blue box with an information icon and the text: 'Select a sensor where hardware configuration or project files have to be sent to extract some relevant Asset information.' Underneath is a dropdown menu showing 'Mendrisio - 1783e6b0428b (guardian Container)'. The main area is a large rectangle with a cloud icon and an upward arrow, containing the text 'Choose a file from your computer or drop one here' and 'Maximum file size: 500.0 MB'. At the bottom, there's a section titled 'Allowed formats:' with two columns of file formats.

Allowed formats:

Comma-separated Values (.csv)	Allen-Bradley (.lsx)
Rockwell Harmony (.conf, .rsx, .rsh)	Honeywell TDS (.txt, .zip)
Yokogawa CENTUM VP (.gz, .zip)	Profinet IOCM (.xml)
Siemens (.cfg)	Siemens AML (.aml)
IEC 61850 SCL/SCD (.scd, .icd, .cid)	Mitsubishi Electric (.gxw, .gx3)
Triconex (.pt2)	Emerson Ovation XML (.htm, .html)

Figure 38. Import assets - file upload

7. In the **File options** step, select the options that apply to your file:

Option	Description
File has header	Select if the first row of the <i>CSV</i> contains column names.
Create non-existent assets	Select to add new assets that are not already in Vantage.
Confirm MAC addresses if provided	Select to validate <i>MAC</i> addresses included in the file.
Enable AI enrichment	Select to use <i>Asset Intelligence (AI)</i> to enrich the imported asset data.

8. Select **Next**.

Result: For *CSV* files, the **Fields binding** step shows, where you can map the columns in your file to Vantage asset fields.

9. **Optional:** If the **Fields binding** step shows, map each column in your [CSV](#) to the corresponding Vantage field, then select **Next**.
10. Review the import summary and select **Import** to complete the import.

Results

The asset data is imported into the selected sensor. A confirmation message shows when the import completes. You can view the results on the **Assets** tab of the **Imports** page.

Import an Arc data archive

You can import an Arc data archive into Vantage to transfer Arc sensor data, including network activity and asset information.

Before you begin

Obtain the Arc data archive [ZIP](#) file exported from your Arc sensor.

Procedure

1. In the top navigation bar, select 

Result: The administration page opens.

2. In the **Organization settings** section, select **Imports**.

Result: The **Imports** page opens.

3. Select the **Arc** tab.

4. Select **Add**.

Result: The **Import Arc data archive** page opens.

5. Drag and drop the Arc data archive [ZIP](#) file onto the upload area, or select **Choose a file from your computer**.

Result: Vantage processes the archive and detects the Arc data archive format. A status message confirms the detected format.

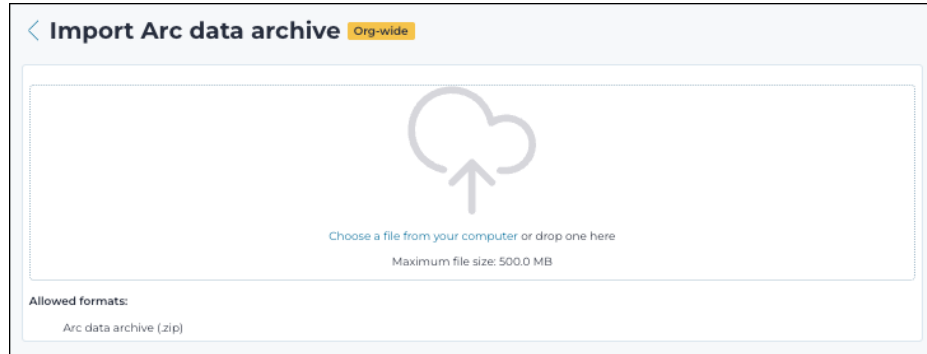


Figure 39. Import Arc data archive - file upload

6. Assign the archive to a sensor:

Option	Steps
Select sensor	Select a sensor from the list, then select Continue .
Create new sensor	Enter the sensor hostname in the Sensor host field, then select Continue .

Result:

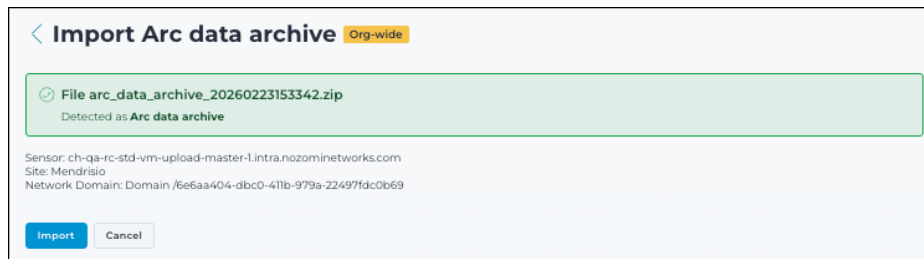


Figure 40. Import Arc data archive - sensor selection

7. Select **Import**.

Results

The Arc data archive contents are sent to the selected sensor. A confirmation message shows when the import completes. You can view the results on the **Arc** tab of the **Imports** page.

Import zone configurations

You can import zone configurations from a CSV file to create new ones or update existing ones in bulk.

Before you begin

Prepare a [CSV](#) file that includes a header row. For **Update** mode, the [CSV](#) must also include an ID column so that each row can be matched to an existing zone configuration.

Procedure

1. In the top navigation bar, select 

Result: The administration page opens.

2. In the **Organization settings** section, select **Imports**.

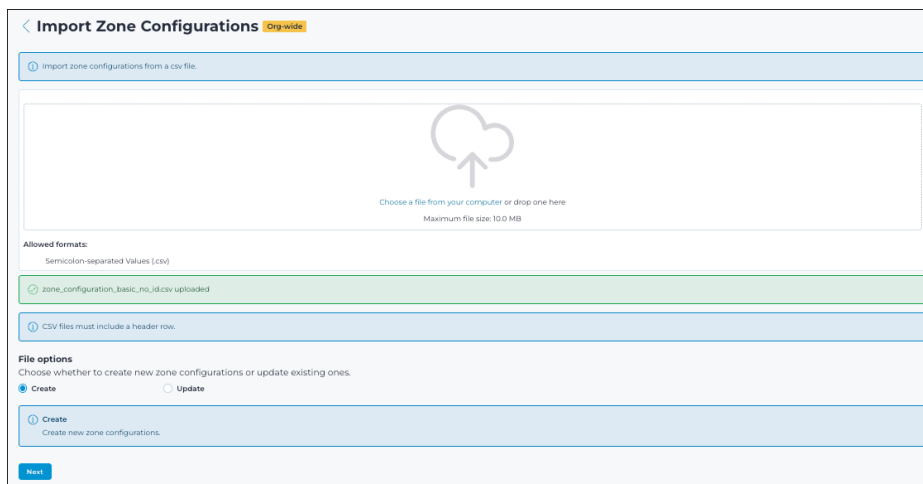
Result: The **Imports** page opens.

3. Select **Select import type** and choose **Zone Configurations**.

Result: The **Import Zone Configurations** page opens, and prompts you to choose a file.

4. Choose your [CSV](#) file.

Result: The file is uploaded and the **File options** step shows, with a confirmation that the file has been uploaded.



The screenshot shows the 'Import Zone Configurations' page with a 'Org-wide' tag. It features a file upload area with a cloud icon and an arrow, prompting the user to 'Choose a file from your computer or drop one here' with a 'Maximum file size: 10.0 MB' limit. Below this, it lists 'Allowed formats: Semicolon-separated Values (.csv)'. A green bar indicates 'zone_configuration_basic_no_id.csv uploaded'. A blue bar contains the instruction 'CSV files must include a header row.' The 'File options' section allows choosing between 'Create' (selected) and 'Update'. A final blue bar shows 'Create' with the subtext 'Create new zone configurations.' and a 'Next' button at the bottom.

Figure 41. Import zone configurations - file upload confirmation

5. In the **File options** step, select a mode:

Mode	Description
Create (default)	Add new zone configurations. The <i>ID</i> column is not required in your <i>CSV</i> .
Update	Match rows by <i>ID</i> to update existing zone configurations. You must bind the <i>ID</i> field in the next step.

6. Select **Next**.

Result: The **Fields binding** step shows. This lets you map the columns from your *CSV* to the Vantage zone configuration fields.

7. Map each column in your *CSV* to the corresponding Vantage field.



Attention:

If you selected **Update** mode, you must bind the **ID** field. Fields marked with an asterisk (*) are mandatory and must be bound before you can continue.

8. Select **Next**.

Result: The **Review** step shows a summary of the zone configurations that will be created or updated. Only non-zero counts are shown. For example, **3 zone configurations will be created**.

Import Zone Configurations Org-wide

Import zone configurations from a csv file.

Fields binding

Please bind all fields marked with an asterisk (*) to continue to the next step.

Your field	Value	Bind to
Name	ZoneConfig1	name
Segments	10.5.0.0/16	segments
ScopeValue	Scope1	scope_value
Scopetype	Tag	scope_type

Confirm

Figure 42. Import zone configurations - review summary

9. Review the summary and select **Confirm** to complete the import.

Results

The zone configurations are imported. A success message confirms that the import has completed. You can view the results on the **Imports** page.

Import an N2OS content pack

You can import an N2OS content pack into Vantage to distribute preconfigured content, such as report templates and query groups, to compatible sensors.

Before you begin

Sensors must be running [N2OS](#) v25.6.0 or later to receive content packs.

Procedure

1. In the top navigation bar, select 

Result: The administration page opens.

2. In the **Organization settings** section, select **Imports**.

Result: The **Imports** page opens.

3. Select the **N2OS Content Packs** tab.

Result: The **Content Packs** page opens, listing previously imported content packs.

4. Select **Add**.

Result: The **Import N2OS Content Pack** page opens.

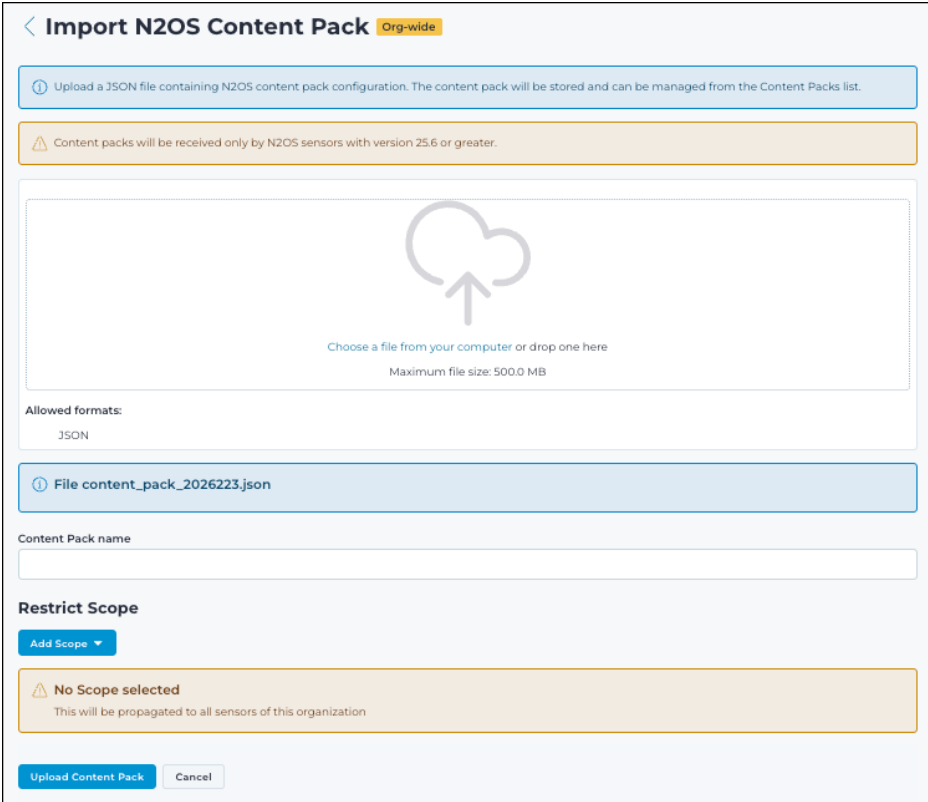


Figure 43. Import N2OS Content Pack page

5. In the **Content Pack name** field, enter a name for the content pack.
6. Drag and drop the content pack *JavaScript Object Notation (JSON)* file onto the upload area, or select **Choose a file from your computer**.
7. Select **Upload Content Pack**.

Results

The content pack is imported into Vantage and will be distributed to sensors running *N2OS* v25.6.0 or later. You can view and manage imported content packs on the **Content Packs** page.

Asset Rules

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

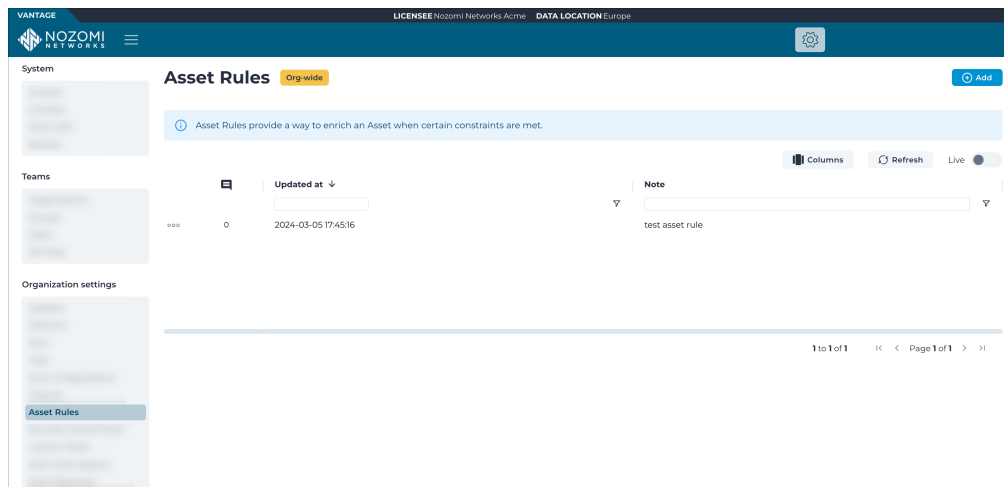


Figure 44. Asset Rules page

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:

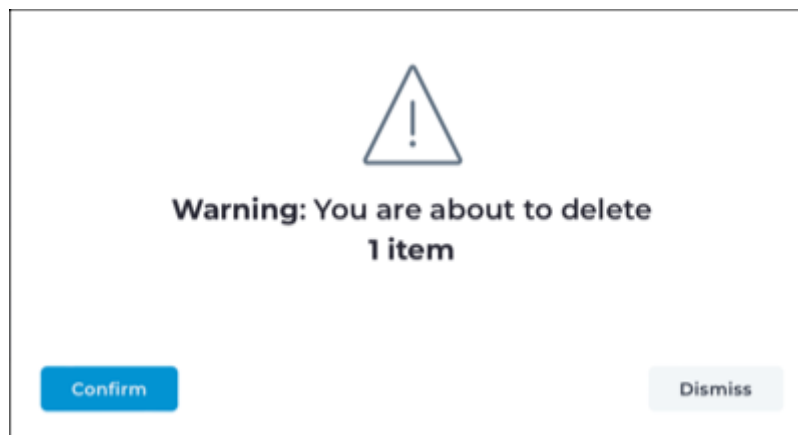
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the  icon

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**.



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.

The screenshot shows the 'Security Control Panel' interface. On the left is a sidebar with 'System', 'Teams', and 'Organization settings' sections. The 'Security Control Panel' is selected under 'Organization settings'. The main content area has a title bar with 'Security Control Panel' and 'Org-wide'. Below this is a note: 'The settings in this page can be overridden on a per-sensor basis from the sensor's settings pages. This feature requires N2OS 24.0 or greater.' The settings are organized into sections: 'Security Profile' (dropdown: Paranoid), 'Network Learning' (Learning scope: dropdown, Phase switching: dropdown, Current phase: dropdown), 'Learning phase duration' (text input: e.g. 1d or 2w), and 'Process Learning' (Alert on new variables: unchecked, Alert on new values: unchecked, Dynamic flow control: checked). A 'Save' button is at the bottom.

Figure 45. 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.

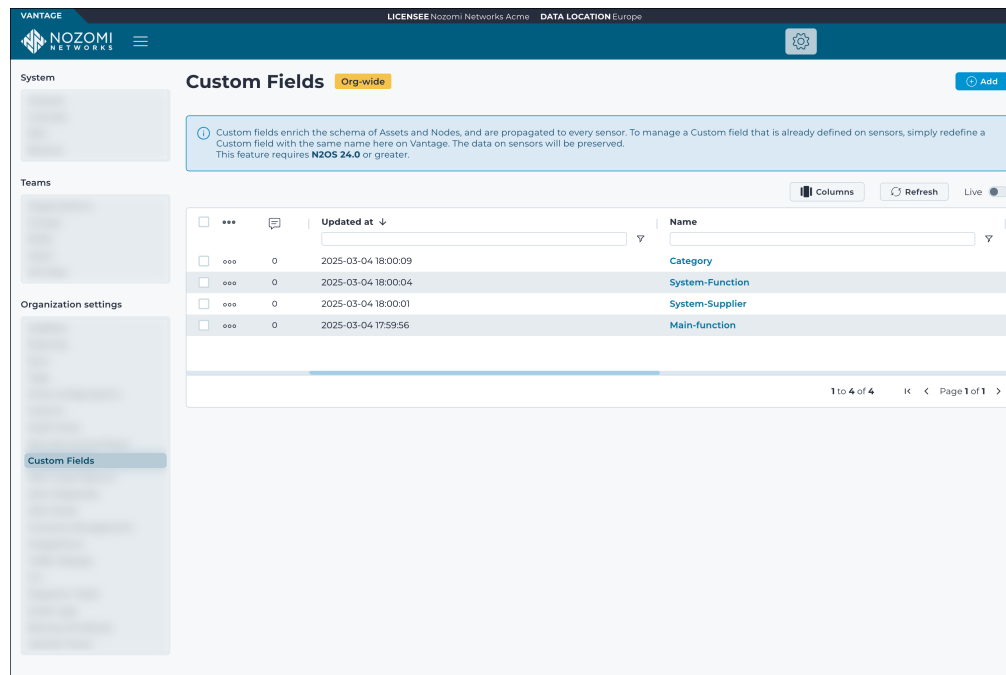


Figure 46. Custom Fields page

Add

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

Credentials Manager

Use the **Credentials Manager** to define credentials that authorize access to hosts through Smart Polling or Arc. This enables secure data collection and encrypted transmission decryption. You can add, customize, and manage credentials for various device types.

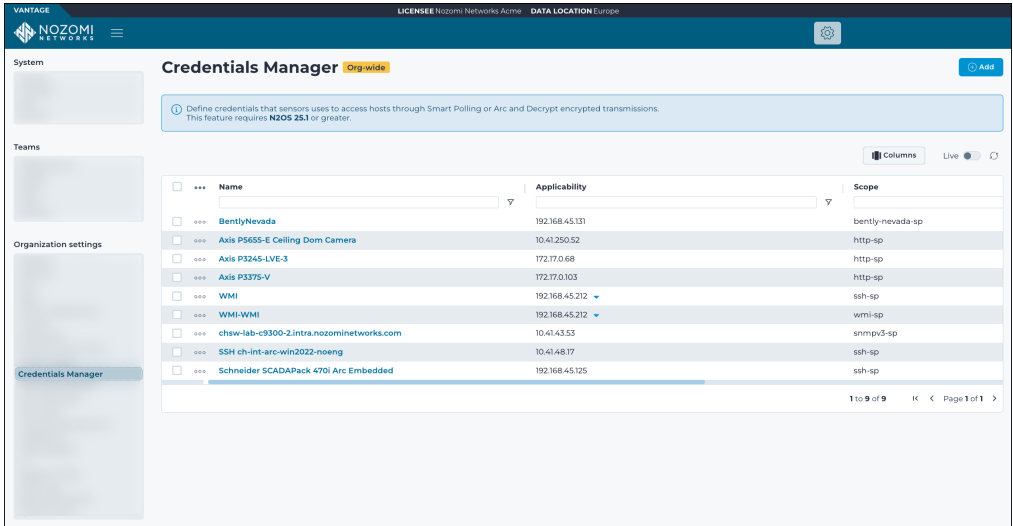


Figure 47. Credentials Manager page

Add

The **Add** button lets you create a new credential.

Columns

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

Live

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

Refresh

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

Add a credential

Add credentials to authorize access to assets through Smart Polling or Arc. Select an identity, configure options, and confirm to store the new credential. This allows secure, role-based access management for connected devices.

Procedure

1. In the top navigation bar, select 
Result: The administration page opens.
2. In the **Organization settings** section, select **Credentials Manager**.
Result: The **Credentials Manager** page opens.
3. Select **Add**.
Result: The **Create Credentials** page shows.
4. From the **Identity** dropdown, select the applicable identity.
The identity that you choose will affect the configuration options that show.
5. Configure the credential as necessary.
6. Select **Confirm**.

Results

The credential has been added.

Alert Close Options

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

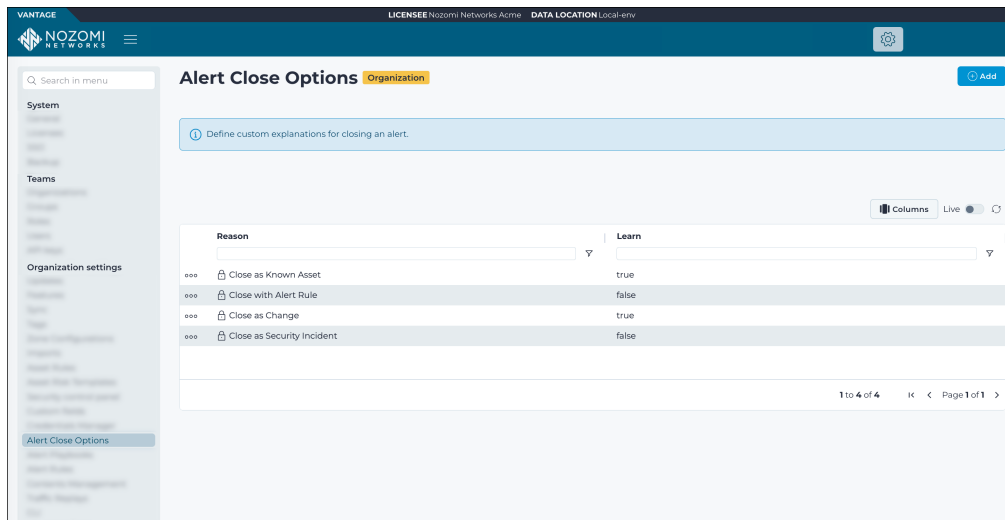


Figure 48. Alert Close Options page



Note:

Built-in alert closing options cannot be edited or deleted. Only custom options that you create are editable.

Built-in options

Vantage includes four built-in alert closing options that are available to all organizations:

- **Close as Security Incident:** Marks the alert as a confirmed security incident. Vantage generates new alerts if a similar event happens again.
- **Close as Change:** Marks the alert as an expected change. Vantage learns the change so that similar future alerts are suppressed.
- **Close with Alert Rule:** Creates an alert rule to mute future alerts that match the same conditions. Only appears when the alert has deduplication components that Vantage can use to create an alert rule.
- **Close as Known Asset:** Marks the asset as known in its current geofence area and updates its location. Only appears for geofence alerts where the asset has an associated geofence area.

Learn behavior

When you close an alert with a Learn option, Guardian integrates the detected change into the network baseline. For example, new nodes or communication patterns that triggered the alert are recorded as safe so they do not generate new alerts. Learn is only applicable to alerts related to deviations from the baseline. If an alert cannot be learned, Vantage presents only the options that don't have the **Learn** flag.

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.

Live

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

Refresh

The  icon lets you immediately refresh the current view.

Table

Column label	Description
Created at	Shows when the alert closing option was created.
Updated at	Shows when the alert closing option was last updated.
Reason	Shows the label for this alert closing option. This label appears in the Reason dropdown when you close an alert.
Learn	Indicates whether closing an alert with this option triggers Learn. When enabled, Guardian integrates the detected change into the network baseline so that it does not generate new alerts.

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.

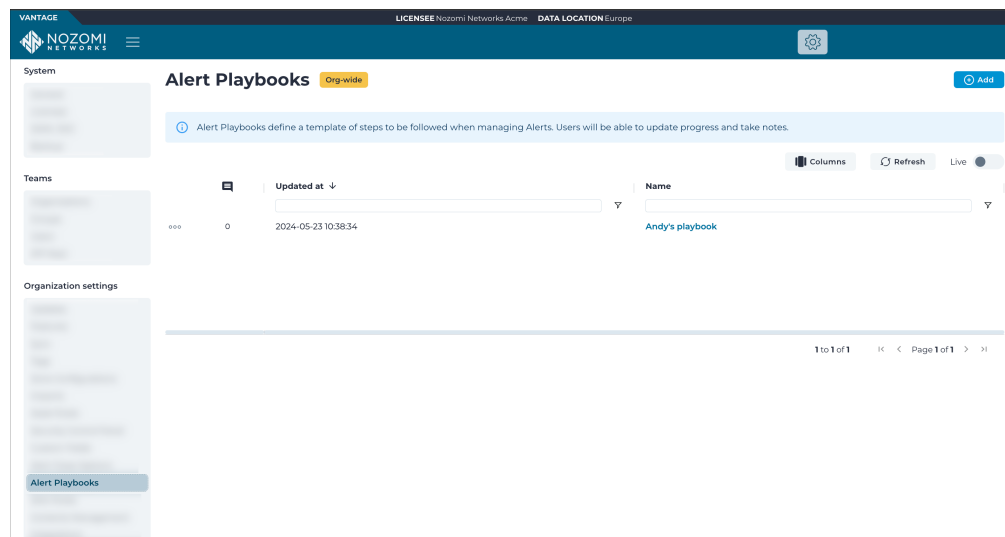


Figure 49. Alert Playbooks page

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

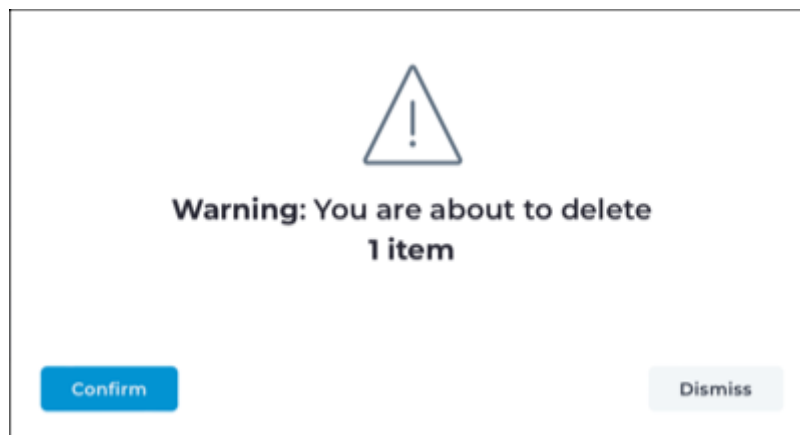
The alert playbook has now been edited.

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**.



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.

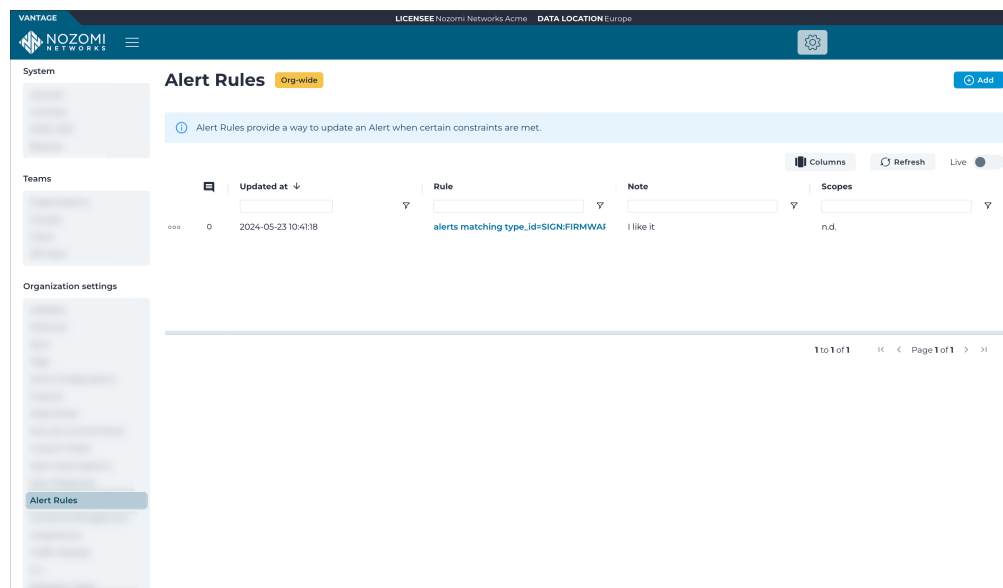


Figure 50. Alert Rules page

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

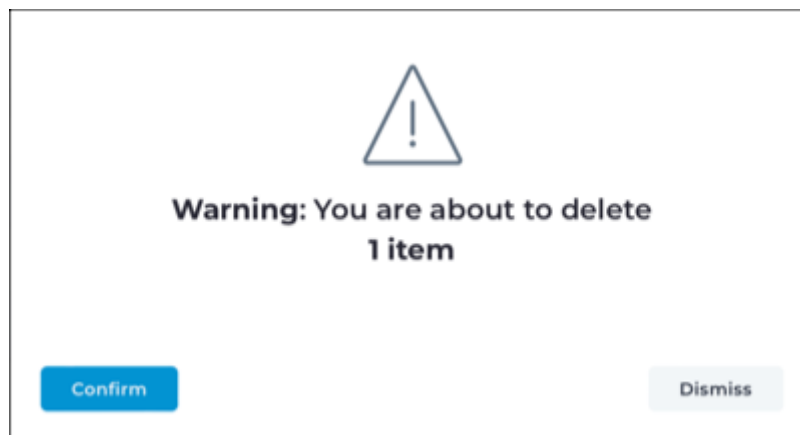
You can now edit the alert rule.

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**.



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.

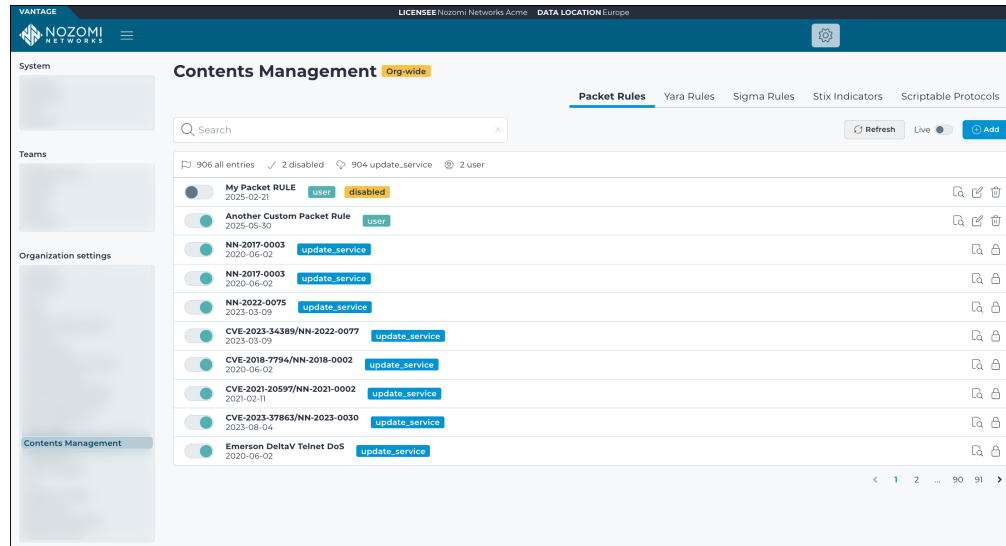


Figure 51. Contents Management page

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

- [Packet Rules](#) (on page 124)
- [Yara Rules](#) (on page 125)
- [Sigma Rules](#) (on page 126)
- [Stix Indicators](#) (on page 127)
- [Scriptable Protocols](#) (on page 128)

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.

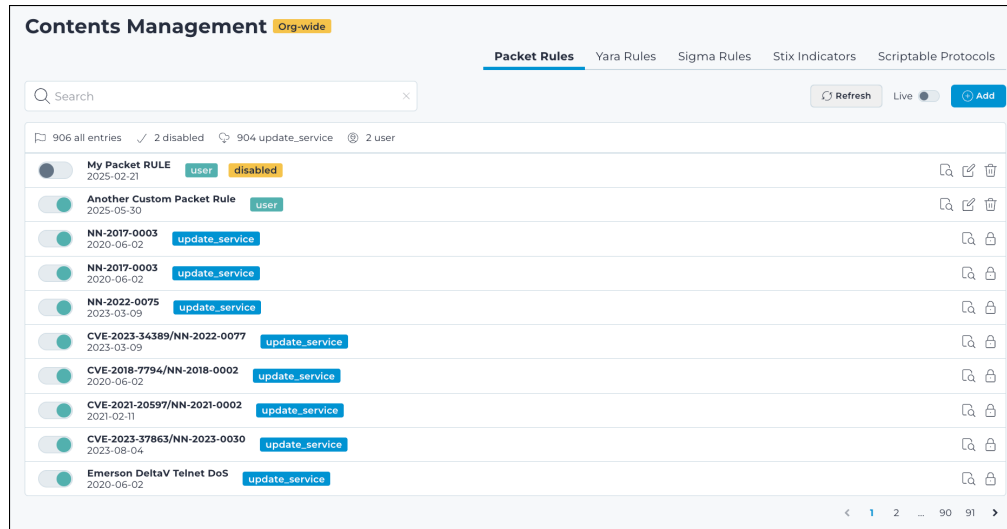


Figure 52. Packet Rules page

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.

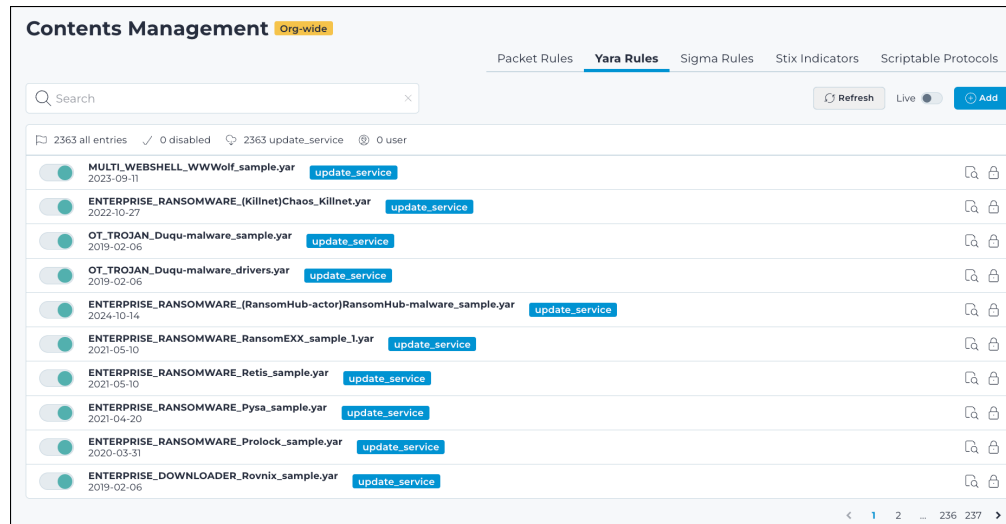


Figure 53. Yara Rules page

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.

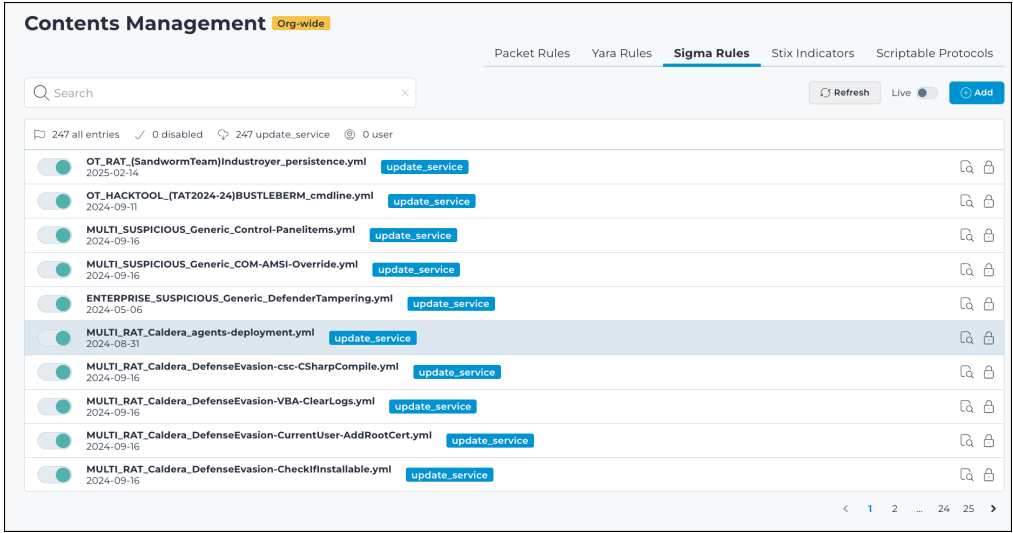


Figure 54. Sigma Rules page

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.

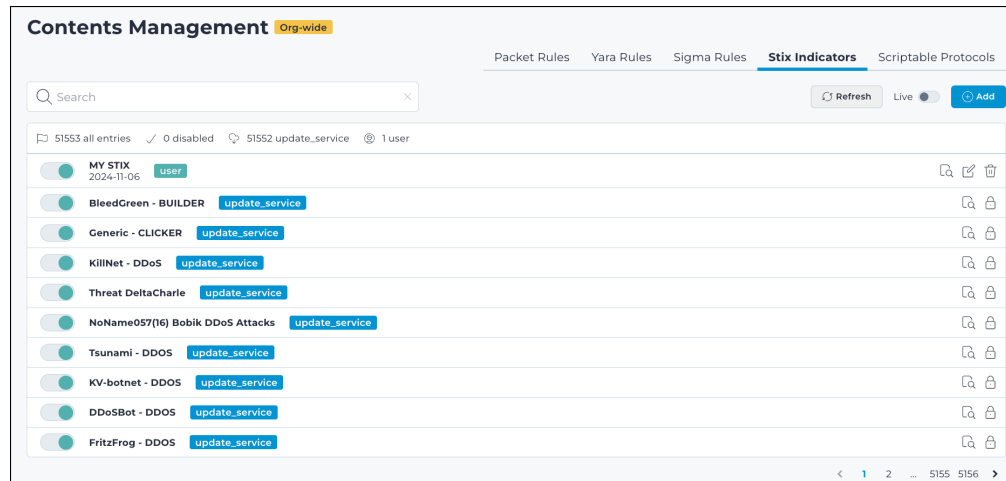


Figure 55. Stix Indicators page

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.

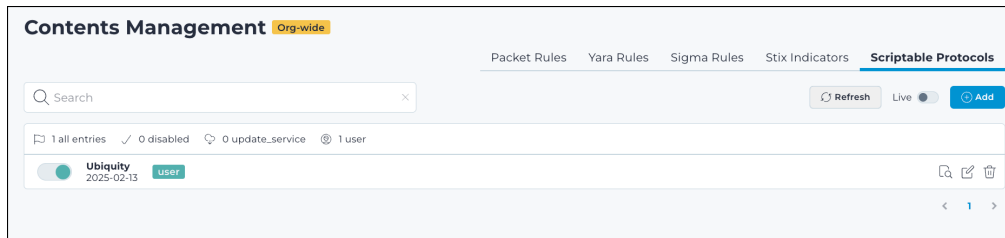


Figure 56. Scriptable Protocols page

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.

Traffic Replays

The **Traffic Replays** 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.

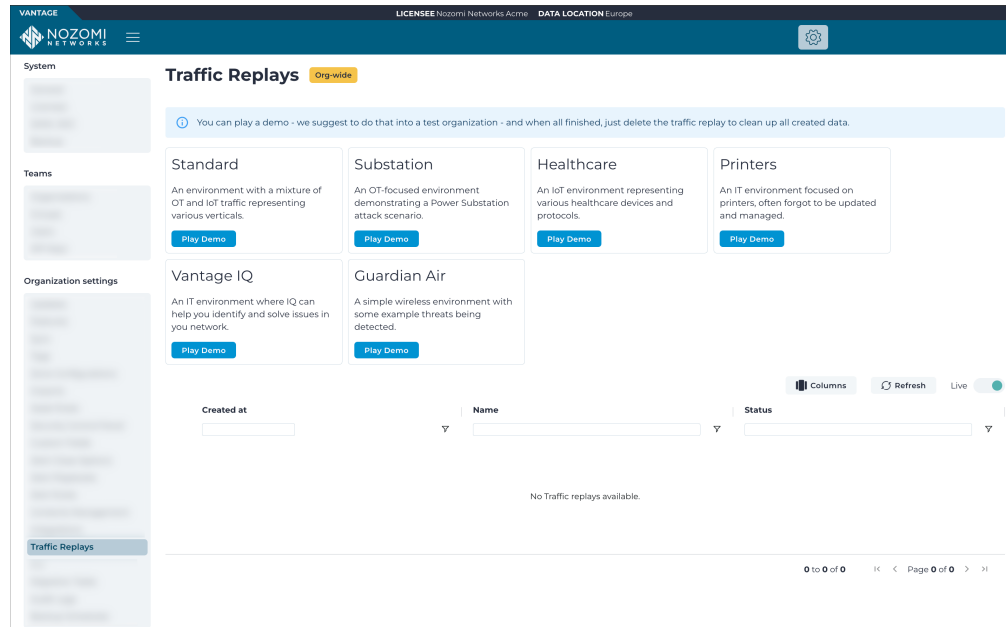


Figure 57. Traffic Replays page

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.

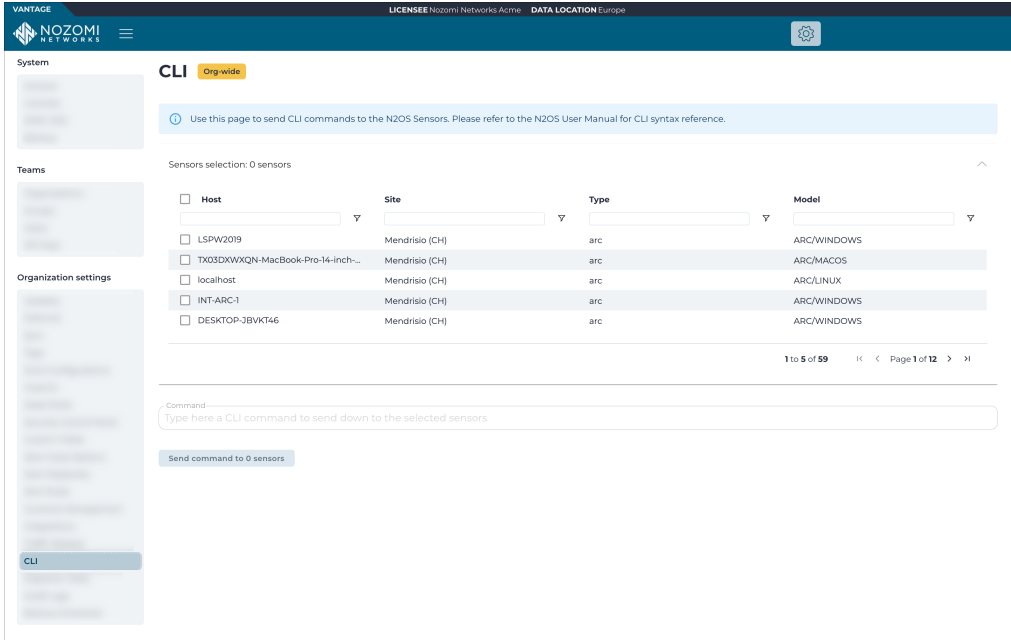


Figure 58. CLI page

Migration tasks

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

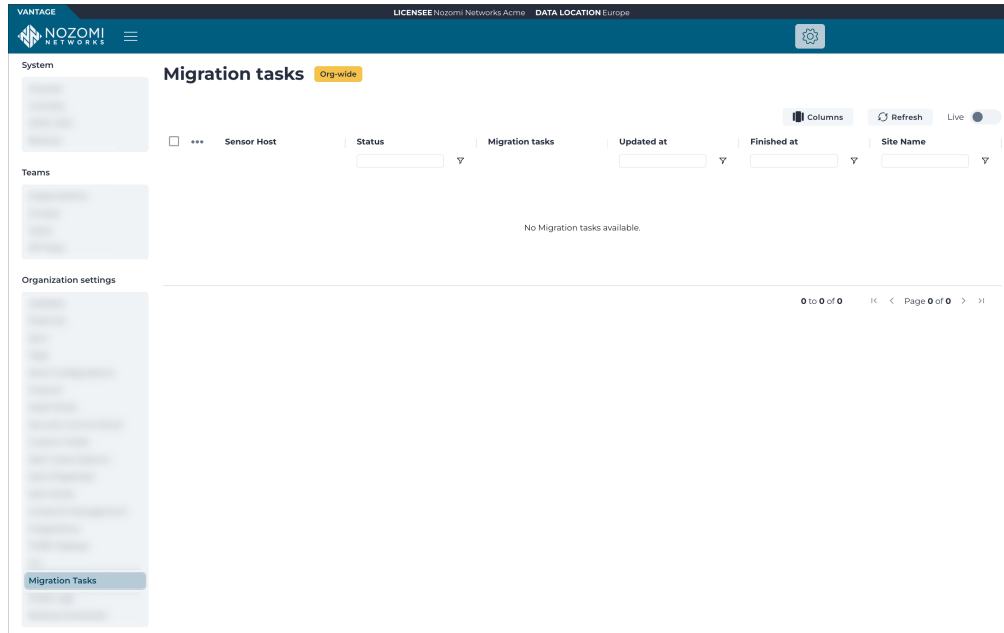


Figure 59. Migration tasks page

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.

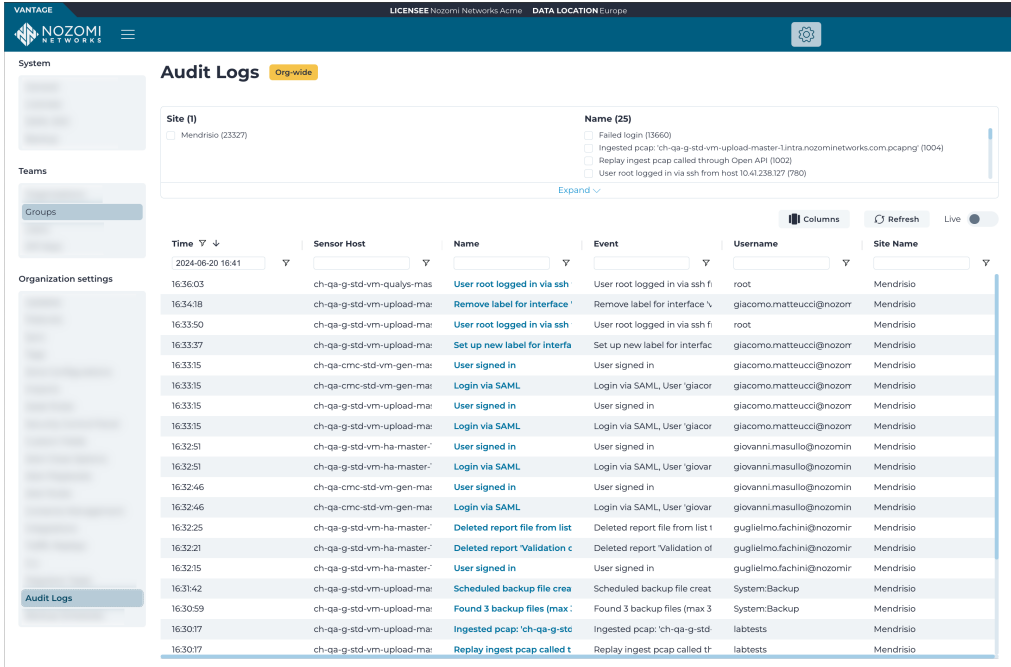


Figure 60. Audit logs page

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.

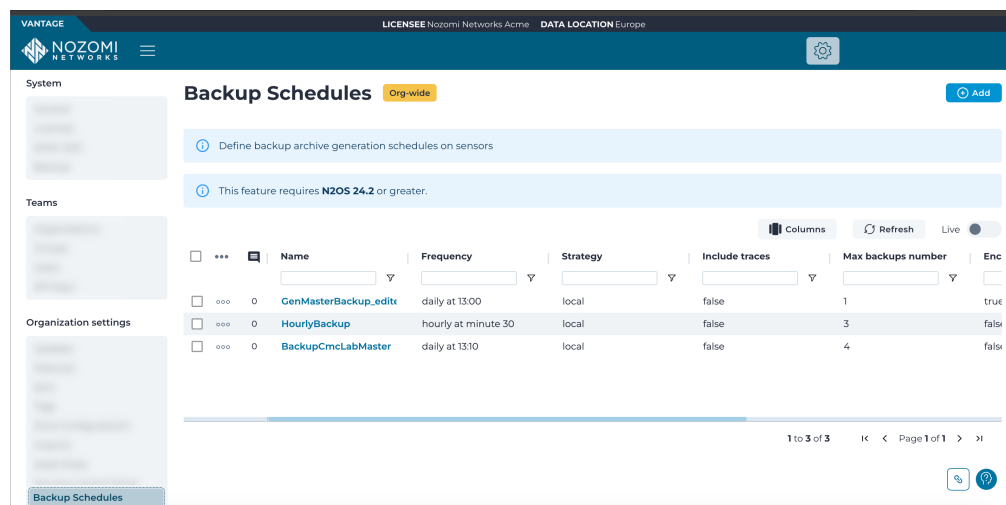


Figure 61. Backup Schedules page

Add

This button lets you [Add a backup schedule \(on page 134\)](#).

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:

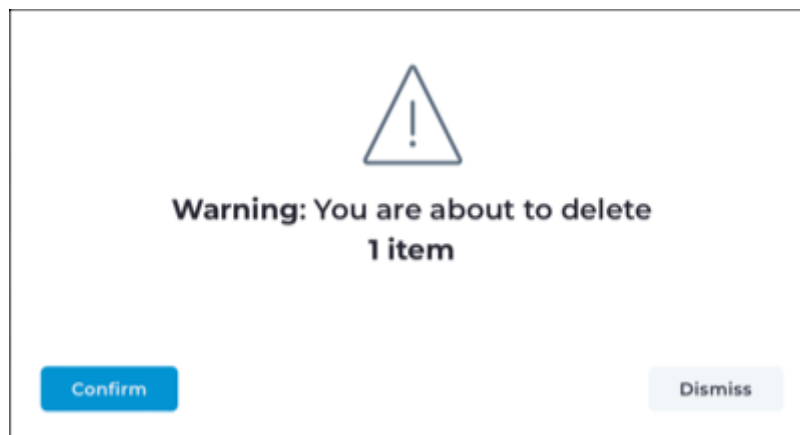
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the  icon

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**.



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.

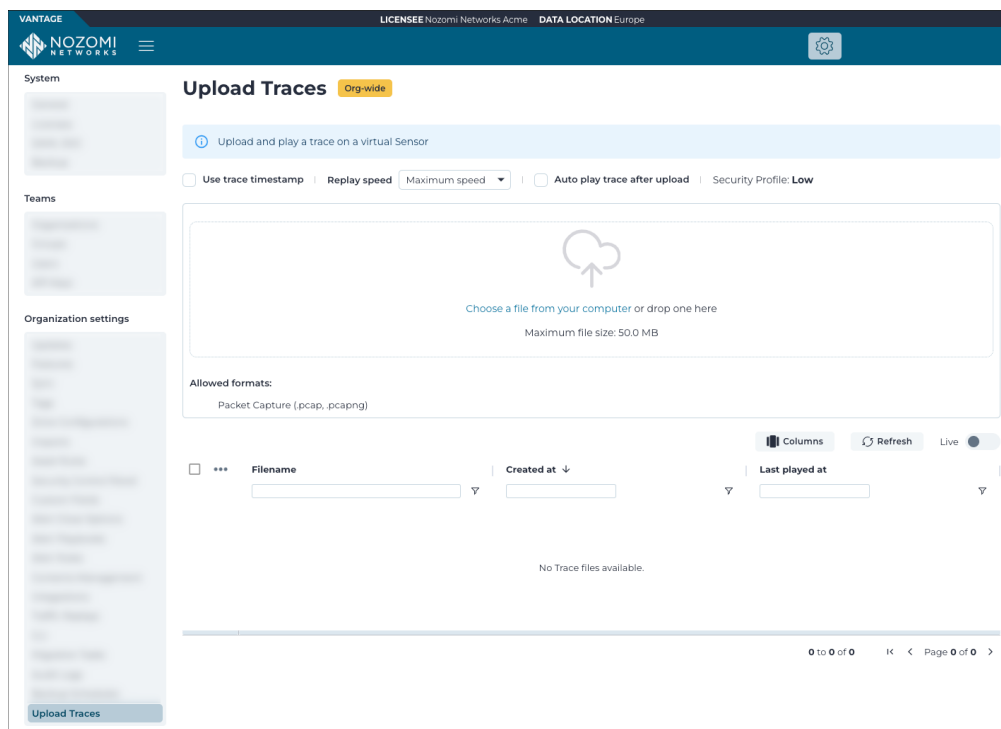


Figure 62. Upload Traces page

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

- Site
- Network domain
- Virtual sensor

When other *pcaps* 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.

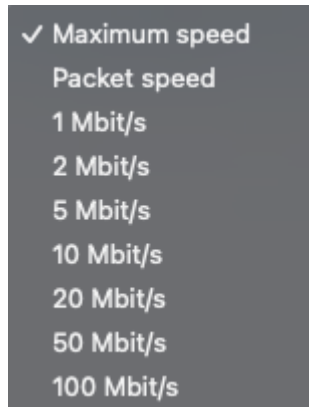


Figure 63. Replay speed dropdown

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.

Arc dependencies

The **Arc dependencies** page shows the dependencies used by the Arc sensors in your organization, and lets you apply actions to multiple sensors at once.

Name	Description	Source	Dependency type	Operating system	Available version
Easefilter	Needed to improve threat prevention	Arc bundle	software	Windows	5.8.6.2
Libpcap	Needed for Traffic monitoring	OS native	software	macOS	n.a.
Npcap	Needed for Traffic monitoring	Arc bundle	software	Windows	5.1.88.504
UsbPcap	Needed for USB detections	Arc bundle	software	Windows	1.5.4
Powershell core script block logging	Needed for local behavior analysis	OS native	setting	Windows	n.a.
Symon	Needed for local behavior analysis	Microsoft	software	Windows	latest
Symon Legacy	Needed for local behavior analysis on older version of Windows	Customer uploaded	software	Windows	n.a.
Windows Powershell script block logging	Needed for local behavior analysis	OS native	setting	Windows	n.a.

Figure 64. Arc dependencies page

The table shows one row for each dependency that's used across the Arc sensors in your organization, with these columns. You can use the filter under each column header to narrow the list:

- Name
- Description
- Source
- Dependency type
- Operating system
- Available version

The **Source** column shows one of these values:

- **Arc bundle:** The dependency ships with Arc
- **OS native:** The dependency is part of the sensor's *operating system (OS)*
- **Customer uploaded:** The dependency's bundle file is uploaded by your organization
- The name of a third-party vendor (for example, **Microsoft**): The dependency is maintained externally by that vendor



Note:

The **Arc dependencies** page isn't shown for organizations in License-only mode.

For each dependency, the actions menu lets you apply an action to one or more sensors at the same time. The menu only shows the actions that apply to that dependency:

- **Install**, **Uninstall**, and **Update** show for software dependencies, except those with a **Source** of **OS native**. For a **Customer uploaded** dependency, **Install** and **Update** also require a bundle to have already been uploaded.
- **Enable** and **Disable** show for setting dependencies.

- **Download** shows for dependencies other than those with a **Source** of **OS native**, and for **Customer uploaded** dependencies only once a bundle has been uploaded.
- **Upload** shows only for **Customer uploaded** dependencies.

Sensors that require a reboot before an action can be applied aren't selectable in the target-sensor dialog.

**Note:**

For sensors running Windows 7 or Windows Server 2008 R2, upload the **Sysmon Legacy** dependency instead of **Sysmon**. The latest compatible version is **13.34**, and the bundle must be a [ZIP](#) archive containing **Sysmon.exe** and **Sysmon64.exe**.

Related information

Install an Arc dependency on multiple sensors (on page 141)
Uninstall an Arc dependency from multiple sensors (on page 143)
Update an Arc dependency on multiple sensors (on page 145)
Enable an Arc dependency on multiple sensors (on page 147)
Disable an Arc dependency on multiple sensors (on page 149)
Download an Arc dependency bundle (on page 151)
Upload an Arc dependency bundle (on page 152)

Install an Arc dependency on multiple sensors

You can use the **Arc dependencies** page to install a software dependency on multiple sensors at the same time.

About this task

The **Install** action isn't available for a dependency with a **Source** of **OS native**. For a **Customer uploaded** dependency, it's only available once a bundle has been uploaded.

Procedure

1. In the top navigation bar, select 

Result: The administration page opens.
2. In the **Organization settings** section, select **Arc dependencies**.

Result: The **Arc dependencies** page opens.
3. For the applicable dependency, open the actions menu and select **Install**.

Result: A dialog shows, listing the sensors that are eligible for the action.
4. Select the sensors that you want to install the dependency on.

Easefilter version 5.8.6.2			
☐	Host	Model	Status
☐	Fanless	ARC/WINDOWS	stale
☐	LSPW8	ARC/WINDOWS	active
☐	LE-TOYODA	ARC/WINDOWS	active
☐	ch-int-arc-n150-w11-1	ARC/WINDOWS	active
1 to 4 of 4 < > Page 1 of 1			
Dismiss Confirm			



Note:

You can use the column filters to narrow the list, or select the header checkbox to select all the sensors that are currently shown. Sensors that require a reboot before the action can be applied aren't selectable.

5. Select **Confirm**.

Result: The dialog shows a confirmation message and the **Allow reboot if required** checkbox.

6. **Optional:** Select the **Allow reboot if required** checkbox.



Note:

If this operation requires a reboot, the sensor is restarted automatically to complete it.

7. Select **Confirm**.

Result: The operation starts. You can monitor its progress on the **Async operations** page. A results dialog shows how many sensors succeeded and how many failed.

Results

The dependency is installed on the selected sensors.

Related information

[Arc dependencies \(on page 139\)](#)

[Uninstall an Arc dependency from multiple sensors \(on page 143\)](#)

[Update an Arc dependency on multiple sensors \(on page 145\)](#)

Uninstall an Arc dependency from multiple sensors

You can use the **Arc dependencies** page to uninstall a software dependency from multiple sensors at the same time.

About this task

The **Uninstall** action isn't available for a dependency with a **Source** of **OS native**.

Procedure

1. In the top navigation bar, select .
Result: The administration page opens.
2. In the **Organization settings** section, select **Arc dependencies**.
Result: The **Arc dependencies** page opens.
3. For the applicable dependency, open the actions menu and select **Uninstall**.
Result: A dialog shows, listing the sensors that are eligible for the action.
4. Select the sensors that you want to uninstall the dependency from.

Do you want to uninstall Npcap from **?**

☐ **Allow reboot if required**
If this operation requires a reboot, the sensor will be restarted automatically to complete it.

Cancel Confirm

**Note:**

You can use the column filters to narrow the list, or select the header checkbox to select all the sensors that are currently shown. Sensors that require a reboot before the action can be applied aren't selectable.

5. Select **Confirm**.

Result: The dialog shows a confirmation message and the **Allow reboot if required** checkbox.

6. **Optional:** Select the **Allow reboot if required** checkbox.



Note:

If this operation requires a reboot, the sensor is restarted automatically to complete it.

7. Select **Confirm**.

Result: The operation starts. You can monitor its progress on the **Async operations** page. A results dialog shows how many sensors succeeded and how many failed.

Results

The dependency is uninstalled from the selected sensors.

Related information

[Arc dependencies \(on page 139\)](#)

[Install an Arc dependency on multiple sensors \(on page 141\)](#)

Update an Arc dependency on multiple sensors

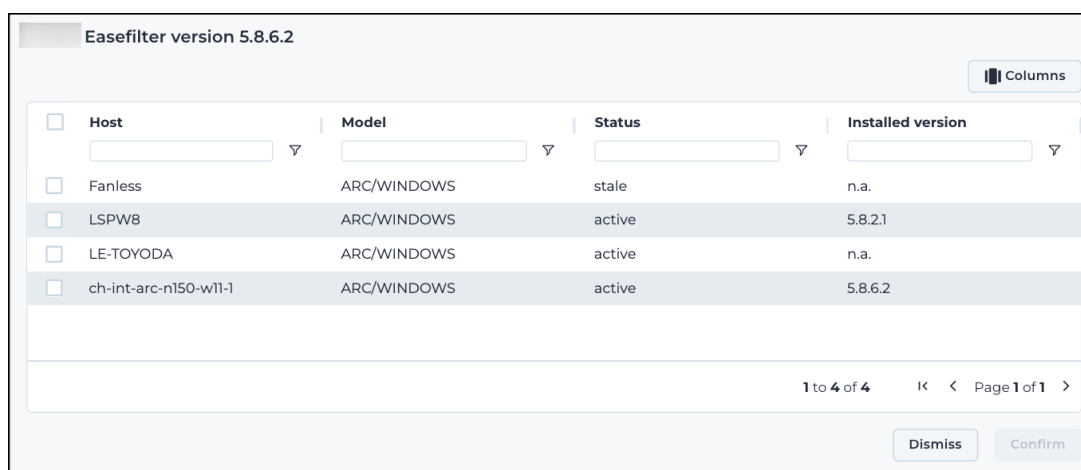
If a newer version is available for an installed software dependency, you can update it on multiple sensors at the same time.

About this task

The **Update** action is only available for a software dependency that doesn't have a **Source** of **OS native**. For a **Customer uploaded** dependency, it's only available once a bundle has been uploaded.

Procedure

1. In the top navigation bar, select 
Result: The administration page opens.
2. In the **Organization settings** section, select **Arc dependencies**.
Result: The **Arc dependencies** page opens.
3. For the applicable dependency, open the actions menu and select **Update**.
Result: A dialog shows, listing the sensors that are eligible for the action.
4. Select the sensors that you want to update the dependency on.



☐	Host	Model	Status	Installed version
☐	Fanless	ARC/WINDOWS	stale	n.a.
☐	LSPW8	ARC/WINDOWS	active	5.8.2.1
☐	LE-TOYODA	ARC/WINDOWS	active	n.a.
☐	ch-int-arc-n150-w11-1	ARC/WINDOWS	active	5.8.6.2



Note:

You can use the column filters to narrow the list, or select the header checkbox to select all the sensors that are currently shown. Sensors that require a reboot before the action can be applied aren't selectable.

5. Select **Confirm**.

Result: The dialog shows a confirmation message and the **Allow reboot if required** checkbox.

6. **Optional:** Select the **Allow reboot if required** checkbox.



Note:

If this operation requires a reboot, the sensor is restarted automatically to complete it.

7. Select **Confirm**.

Result: The operation starts. You can monitor its progress on the **Async operations** page. A results dialog shows how many sensors succeeded and how many failed.

Results

The dependency is updated to the available version on the selected sensors.

Related information

[Arc dependencies \(on page 139\)](#)

[Install an Arc dependency on multiple sensors \(on page 141\)](#)

Enable an Arc dependency on multiple sensors

You can use the **Arc dependencies** page to enable a setting dependency on multiple sensors at the same time.

Procedure

1. In the top navigation bar, select 
Result: The administration page opens.
2. In the **Organization settings** section, select **Arc dependencies**.
Result: The **Arc dependencies** page opens.
3. For the applicable dependency, open the actions menu and select **Enable**.
Result: A dialog shows, listing the sensors that are eligible for the action.
4. Select the sensors that you want to enable the dependency on.

Do you want to enable Powershell core script block logging o...

☐ **Allow reboot if required**
If this operation requires a reboot, the sensor will be restarted automatically to complete it.

Cancel Confirm



Note:

You can use the column filters to narrow the list, or select the header checkbox to select all the sensors that are currently shown. Sensors that require a reboot before the action can be applied aren't selectable.

5. Select **Confirm**.
Result: The dialog shows a confirmation message and the **Allow reboot if required** checkbox.

6. **Optional:** Select the **Allow reboot if required** checkbox.



Note:

If this operation requires a reboot, the sensor is restarted automatically to complete it.

7. Select **Confirm**.

Result: The operation starts. You can monitor its progress on the **Async operations** page. A results dialog shows how many sensors succeeded and how many failed.

Results

The dependency is enabled on the selected sensors.

Related information

[Arc dependencies \(on page 139\)](#)

[Disable an Arc dependency on multiple sensors \(on page 149\)](#)

Disable an Arc dependency on multiple sensors

You can use the **Arc dependencies** page to disable a setting dependency on multiple sensors at the same time.

Procedure

1. In the top navigation bar, select .

Result: The administration page opens.

2. In the **Organization settings** section, select **Arc dependencies**.

Result: The **Arc dependencies** page opens.

3. For the applicable dependency, open the actions menu and select **Disable**.

Result: A dialog shows, listing the sensors that are eligible for the action.

4. Select the sensors that you want to disable the dependency on.

Do you want to disable Windows Powershell script block logg...

☐ **Allow reboot if required**
If this operation requires a reboot, the sensor will be restarted automatically to complete it.

Cancel Confirm



Note:

You can use the column filters to narrow the list, or select the header checkbox to select all the sensors that are currently shown. Sensors that require a reboot before the action can be applied aren't selectable.

5. Select **Confirm**.

Result: The dialog shows a confirmation message and the **Allow reboot if required** checkbox.

6. **Optional:** Select the **Allow reboot if required** checkbox.



Note:

If this operation requires a reboot, the sensor is restarted automatically to complete it.

7. Select **Confirm**.

Result: The operation starts. You can monitor its progress on the **Async operations** page. A results dialog shows how many sensors succeeded and how many failed.

Results

The dependency is disabled on the selected sensors.

Related information

[Arc dependencies \(on page 139\)](#)

[Enable an Arc dependency on multiple sensors \(on page 147\)](#)

Download an Arc dependency bundle

You can download the bundle file for a dependency from the **Arc dependencies** page.

About this task

The **Download** action isn't available for a dependency with a **Source** of **OS native**, or for a **Customer uploaded** dependency for which no bundle has been uploaded yet.

Procedure

1. In the top navigation bar, select 

Result: The administration page opens.
2. In the **Organization settings** section, select **Arc dependencies**.

Result: The **Arc dependencies** page opens.
3. For the applicable dependency, open the actions menu and select **Download**.

Arc dependencies Organization						
Name	Description	Source	Dependency type	Operating system	Available version	
... Easefilter 	Needed to improve threat prevention	Arc bundle	software	Windows	5.8.6.2	
Libpcap 	Needed for Traffic monitoring	OS native	software	macOS	n.a.	
... Npcap 	Needed for Traffic monitoring	Arc bundle	software	Windows	5.188.504	
... UsbPcap 	Needed for USB detections	Arc bundle	software	Windows	1.5.4	
... Powershell core script block logging 	Needed for local behavior analysis	OS native	setting	Windows	n.a.	
... Sysmon 	Needed for local behavior analysis	Microsoft	software	Windows	latest	
... Sysmon Legacy 	Needed for local behavior analysis on older version of Windows	Customer uploaded	software	Windows	n.a.	
... Windows Powershell script block logging 	Needed for local behavior analysis	OS native	setting	Windows	n.a.	

Results

The dependency's bundle file starts to download in your browser.

Related information

Arc dependencies (on page 139)

Upload an Arc dependency bundle (on page 152)

Upload an Arc dependency bundle

For a dependency with a **Source** of **Customer uploaded**, you can upload its bundle file from the **Arc dependencies** page.

Procedure

1. In the top navigation bar, select .

Result: The administration page opens.

2. In the **Organization settings** section, select **Arc dependencies**.

Result: The **Arc dependencies** page opens.

3. For the applicable dependency, open the actions menu and select **Upload**.



Note:

If a bundle has already been uploaded for the dependency, it's replaced.

Result: The **Upload** dialog shows.

4. In the **Bundle** field, choose the [ZIP](#) archive that holds the dependency.
5. In the **Version** field, enter the version number of the uploaded bundle.
6. Select **Confirm**.

Results

The bundle is uploaded for the dependency.

Related information

Arc dependencies (on page 139)

Download an Arc dependency bundle (on page 151)

Chapter 3. 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 \(on page 157\)](#)
- [Configure Vantage for SSO \(on page 158\)](#)

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 \(on page 32\)](#).

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:

`https://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 \(on page 165\)](#)
- [Configure an Okta enterprise application \(on page 163\)](#)
- [Configure a Google Workspace SAML application \(on page 161\)](#)

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 \(on page 156\)](#).

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 \(on page 157\)](#) 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**.

The screenshot shows a configuration window titled "Attributes". Below the title is a subtitle: "Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)".

There are two main columns: "Google Directory attributes" and "App attributes".

Under "Google Directory attributes", there is a dropdown menu showing "Employee Details >" and "Department".

Under "App attributes", there is a text input field containing "nozominetworks-group-name" and a close button (X).

An arrow points from the "Department" dropdown to the "nozominetworks-group-name" input field.

At the bottom left, there is a button labeled "ADD MAPPING".

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 \(on page 158\)](#).

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 \(on page 155\)](#).

Procedure

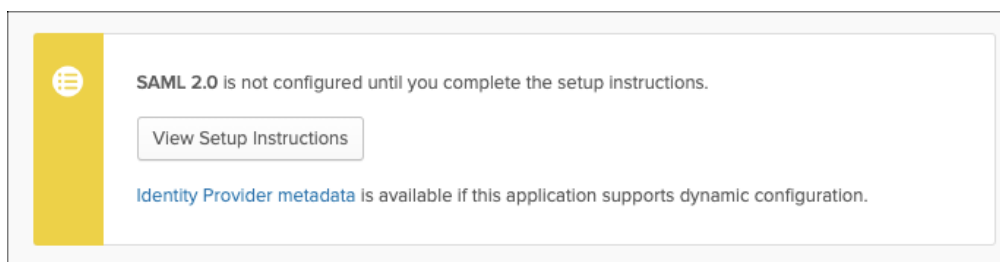
1. In the Okta Admin console, select **Applications > Create App Integration**.
2. Select **SAML 2.0**.
3. Enter a name such as **Vantage**
4. Select **Next**.
5. Enter the **Single sign on URL** that corresponds to the [ACS URL](#) for Vantage:
`https://YOUR_VANTAGE_URL/api/v1/saml/auth`
6. Enter the **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.



11. Save this file to a location that the browser that you use for Vantage can access.
12. [Configure Vantage for SSO \(on page 158\)](#).

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:

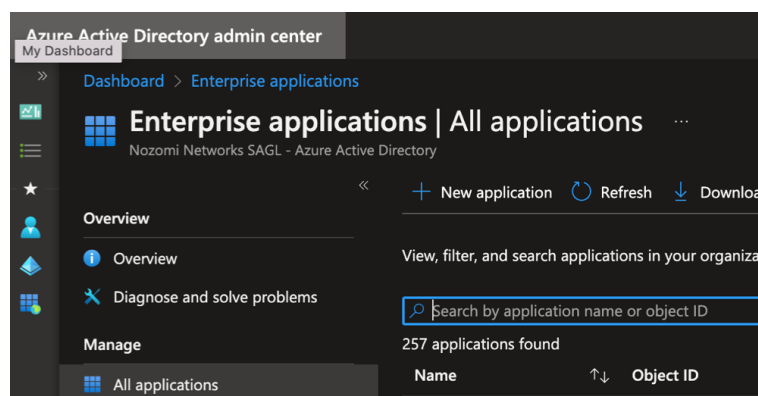
Users, guests, and applications contained directly in this group are granted access to Vantage. Azure denies access to users contained in the group's subgroups.

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 \(on page 155\)](#).

Procedure

1. Select **My Dashboard > Enterprise applications | All Applications**.



2. Select **+ New application**.

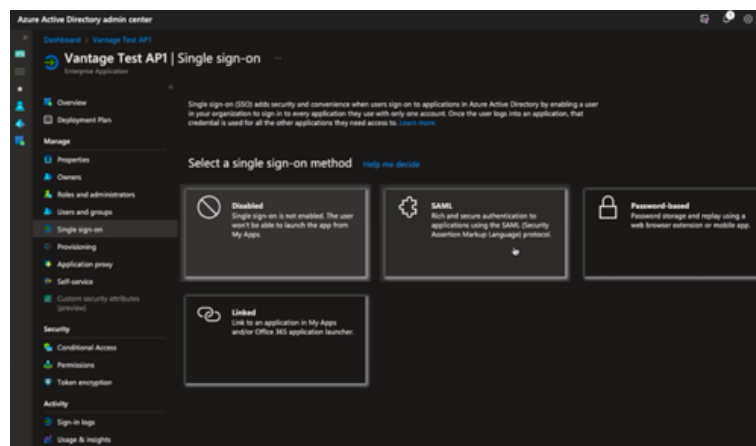
Result: A dialog shows.

3. Select **Create your own application**.

Result: A dialog shows.

- In the **What's the name of your app?** field, enter a name such as: **Nozomi Networks Vantage**.

- Select **Integrate any other application you don't find in the gallery (Non-gallery)**.
 - 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.
- Open the application.
 - Select **Single sign-on > SAML**.



- Specify the **Reply URL** which corresponds to the [ACS URL](#) for Vantage:
`https://YOUR_VANTAGE_URL/api/v1/saml/auth`
- Define the **Entity ID** for Vantage:
`https://YOUR_VANTAGE_URL/api/v1/saml/metadata`

11. Configure attributes and claims, including group claims, so that Azure passes group membership information to Vantage.

**Note:**

Vantage authentication relies on user group claims. You must configure Azure to emit the security group IDs for the authenticating user. Vantage uses these IDs to determine group membership and grant access accordingly.

- a. In the **Attributes & Claims** section, select the edit icon.
- b. Select **Add a group claim**.
- c. In the **Group Claims** dialog, select **Security groups**.
- d. Set the **Source attribute** field to **Group ID**.
This causes Azure to emit the group's object ID (*UUID*), which Vantage uses to match groups and automatically add authenticated users to the correct group.
- e. Select **Save**.

12. Optional:

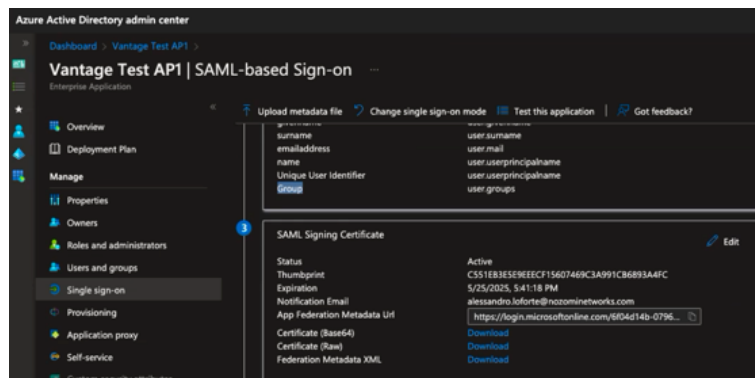
Upload an image to use as an icon in the [SAML](#) app.



13. After the application has been configured, it will show in Azure.



14. Download the Azure Active Directory metadata file.
 - a. In the **SAML Signing Certificate** section, to the right of **Federation Metadata XML**, select **Download**.



- b. Save this file to a location that the browser that you use for Vantage can access.

15. [Configure Vantage for SSO \(on page 158\)](#).

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.

Address Resolution Protocol

ARP is a communication protocol that is used to discover the link layer address, such as a [MAC](#) address, that is associated with a given internet layer address. This is typically an IPv4 address.

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.

Authorization to Operate

ATO is a formal declaration by a designated authorizing official that authorizes operation of an information system and explicitly accepts the risk to organizational operations, organizational assets, individuals, or other organizations based on the implementation of an agreed-upon set of security controls.

Berkeley Packet Filter

The BPF is a technology that is used in some computer operating systems for programs that need to analyze network traffic. A BPF provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in a similar way as on the sensor.

Central Processing Unit

The main, or central, processor that executes instructions in a computer program.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

Command-line interface

A command-line processor uses a command-line interface (CLI) as text input commands. It lets you invoke executables and provide information for the actions that you want them to do. It also lets you set parameters for the environment.

Comma-separated Value

A CSV file is a text file that uses a comma to separate values.

Common Event Format

CEF is a text-based log file format that is used for event logging and information sharing between different security devices and software applications.

Common Platform Enumeration

CPE is a structured naming scheme for information technology (IT) systems, software, and packages. CPE is based on the generic syntax for Uniform Resource Identifiers (URI) and includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

Common Vulnerability Scoring System

CVSS is a standardized framework used in cybersecurity to assess the severity of software vulnerabilities. It provides a numerical score to help prioritize risk management and response efforts.

Controlled Unclassified Information

CUI is information that requires safeguarding or dissemination controls pursuant to federal law, regulations, and government-wide policies, but is not classified under Executive Order 13526.

Coordinated Universal Time

Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time. It is based on International Atomic Time (TAI) with leap seconds added to synchronize with Earth's rotation.

cURL

cURL is a command-line tool and library used to transfer data to or from a server. It supports many protocols, including HTTP, HTTPS, FTP, and more. In API contexts, curl is commonly used to test and interact with endpoints by sending requests and receiving responses.

Department of Defense

DoD is the executive branch department of the United States federal government responsible for coordinating and supervising all agencies and functions directly related to national security and the United States Armed Forces.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

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.

Federal Information Security Management Act

FISMA is a United States federal law that defines a framework of guidelines and security standards to protect government information and operations. It requires federal agencies to develop, document, and implement programs to provide information security for their data and information systems.

Federal Risk and Authorization Management Program

FedRAMP is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies.

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.

Link Layer Discovery Protocol

LLDP is a vendor-neutral link layer protocol used by network devices for advertising identity, capabilities, and neighbors on a local area network.

Management Information Base

An MIB is a collection of definitions that specify the properties of the managed resources within a network device (like routers or switches) and how they can be accessed using SNMP (Simple Network Management Protocol).

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Megabyte

The megabyte is a multiple of the unit byte for digital information. One megabyte is one million bytes.

National 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.

National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Newline Delimited JSON

NDJSON is a data format where each line is a valid JSON value, used for streaming or storing structured records efficiently.

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).

Plan of Action and Milestones

POA&M is a document that identifies tasks that need to be accomplished to address security weaknesses or deficiencies. It details resources required, milestones for completion, and scheduled completion dates for each task. It is a key tool for tracking and managing remediation efforts in federal security compliance programs.

Portable Document Format

PDF is a Adobe file format that is used to present documents. It is independent of operating systems (OS), application software, hardware.

Portable Executable

PE is a file format used by Windows operating systems (OS) for executable files, object code, and dynamic link libraries (DLLs). PE files contain the code and resources needed to run programs on Windows.

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.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

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 Assessment Report

SAR is a comprehensive document that details the results of an independent security assessment of an information system. It includes findings, vulnerabilities, and recommendations from the assessment process and is a required component of the FedRAMP authorization.

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.

Security Requirements Guide

SRG is a Department of Defense publication that provides security requirements and controls for information systems and cloud computing services at various impact levels.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

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.

System Security Plan

SSP is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned to meet those requirements. It is a key component of the FedRAMP authorization process.

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.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

User Datagram Protocol

UDP is a lightweight, connectionless communication protocol used for fast, time-sensitive data transmission, such as video streaming, online gaming, and VoIP. UDP prioritizes speed and low latency over guaranteed delivery or error correction.

User Interface

An interface that lets humans interact with machines.

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).

Windows Remote Management

Is a Microsoft implementation of Web Services-Management in Windows which lets systems access or exchange management information across a common network. You can utilize the built-in command line tool, or scripting objects, WinRM can be used with remote computers that may have baseboard management controllers (BMCs) to acquire data.

ZIP

An archive file format that supports lossless data compression. The format can use a number of different compression algorithms, but DEFLATE is the most common one. A ZIP file can contain one or more compressed files or directories.

