



Vantage Administrator Guide

2024-09-09

Legal notices

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

Copyright

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

Third Party Software

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

Contents

Chapter 1. Introduction.....	5
Vantage overview.....	7
Architecture.....	9
Data security in Vantage.....	10
Chapter 2. Administration.....	13
Administration page.....	15
System.....	17
General.....	17
Licenses.....	19
SAML Single Sign On.....	20
Backup.....	21
Teams.....	22
Organizations.....	22
Groups.....	24
Users.....	30
API keys.....	35
Organization Settings.....	43
Update Policy.....	43
Features.....	44
Sensors Synchronization Settings.....	45
Tags.....	46
Zone configurations.....	47
Imports.....	54
Asset Rules.....	55
Alert Close Options.....	59
Alert Playbooks.....	61
Alert Rules.....	65
Integrations.....	69
Traffic Replays.....	79
CLI.....	80
Migration tasks.....	81
Audit Logs.....	82
Backup Schedules.....	83
Chapter 3. Migration.....	87
Migration to N2OS 22.6.0.....	89
Migrate to the N2OS 22.6.0 data model.....	91
N2OS 22.6.0 Data Model Changes.....	94
Chapter 4. SAML integration.....	97

SAML integration configuration.....	99
IdP configuration for SAML integration.....	100
Configure your IdP for SAML integration.....	101
Configure Vantage for SSO.....	102
Troubleshooting SAML integration.....	104
Configure a Google Workspace SAML application.....	105
Configure an Okta enterprise application.....	107
Configure an Azure Active Directory enterprise application.....	109
Glossary.....	113

Chapter 1. Introduction



Vantage overview

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

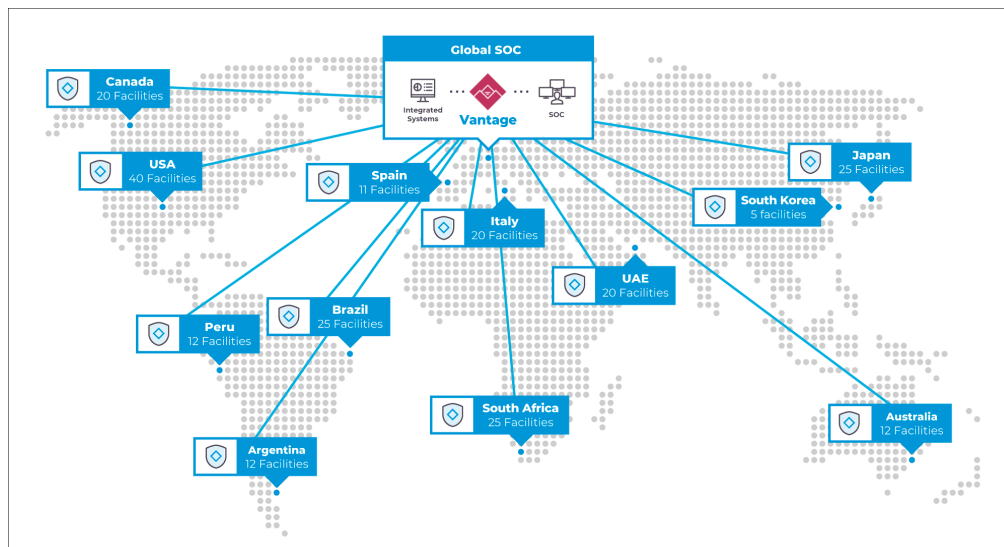


Figure 1. Vantage overview

General

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

Vantage lets you:

- Centrally-manage all sensor deployments from a single application
- Centrally-manage all sensor deployments from anywhere in the world
- Monitor an unlimited amount of devices
- Protect an unlimited amount 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 threat. A centralized dashboard consolidates data to create high-priority alerts across a global network.

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

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

Scale

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

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

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

Architecture

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

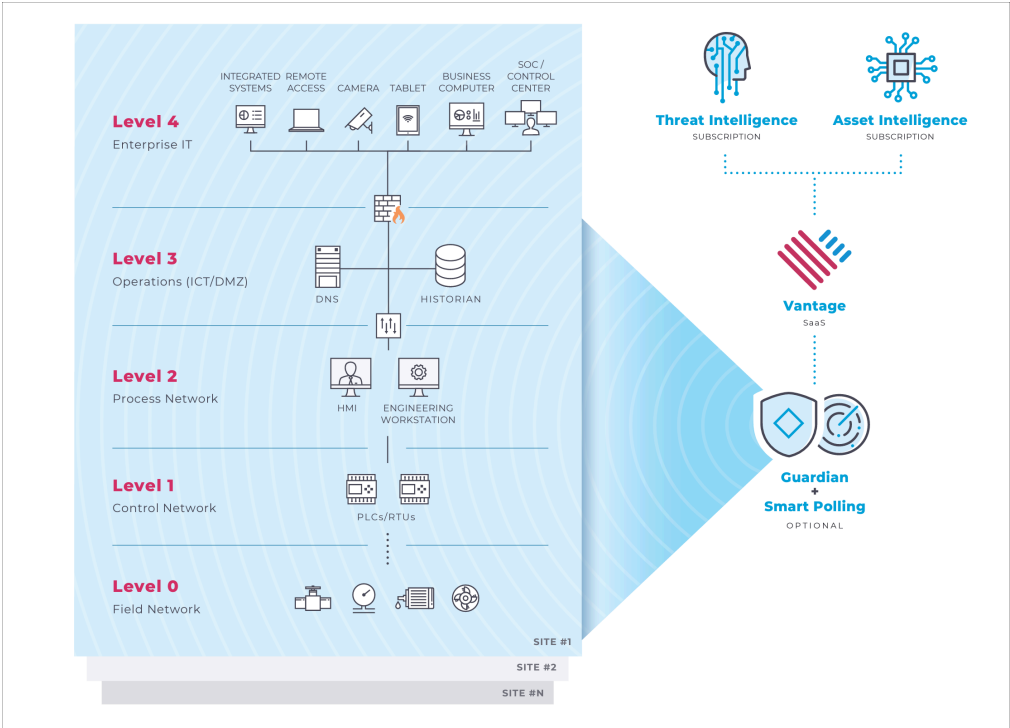


Figure 2. Vantage architecture

Data security in Vantage

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

Data privacy

For more details, see [Nozomi Networks Vantage Data Privacy](#).

Data segregation and encryption

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

FIPS support

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

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

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

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

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

To learn more about *FIPS*, contact [Nozomi Networks](#).

FIPS-compliant Vantage and SAML configuration

When you use *security assertion markup language (SAML)* to [Configure Vantage for SSO \(on page 102\)](#), you must specify its *assertion consumer service (ACS) uniform resource locator (URL)*.

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

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

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

For more details about *ACS URLs*, see [IdP configuration for SAML integration \(on page 100\)](#).

For more details about [ACS URLs](#), see **IdP configuration for SAML integration**, in the **Administrator Guide**.



Chapter 2. Administration



Administration page

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

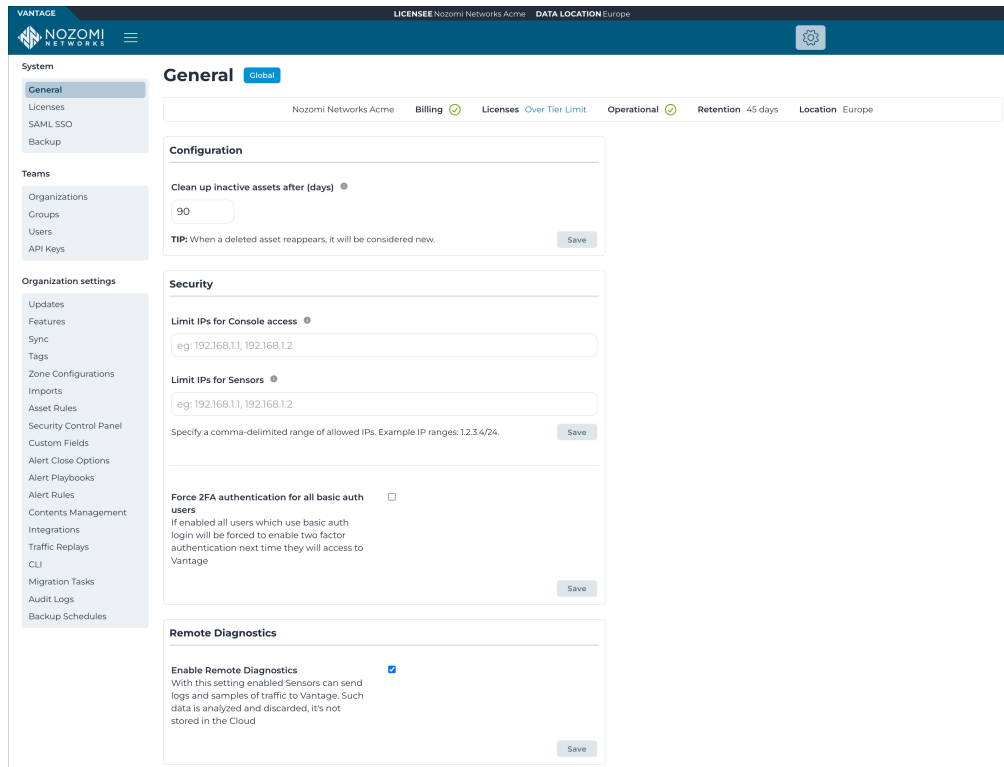


Figure 3. Administration page

System

The **System** section has these pages:

- [General](#) (on page 17)
- [Licenses](#) (on page 19)
- [SAML Single Sign On](#) (on page 20)
- [Backup](#) (on page 21)

Teams

The **Teams** section has these pages:

- [Organizations](#) (on page 22)
- [Groups](#) (on page 24)
- [Users](#) (on page 30)
- [API Keys](#) (on page 39)

Organization settings

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

- [Update Policy \(on page 43\)](#)
- [Features \(on page 44\)](#)
- [Sensors Synchronization Settings \(on page 45\)](#)
- [Tags \(on page 46\)](#)
- [Zone Configurations \(on page 48\)](#)
- [Imports \(on page 54\)](#)
- [Asset Rules \(on page 55\)](#)
- [Alert Close Options \(on page 59\)](#)
- [Alert Playbooks \(on page 61\)](#)
- [Alert Rules \(on page 65\)](#)
- [Integrations \(on page 69\)](#)
- [Traffic Replays \(on page 79\)](#)
- [CLI \(on page 80\)](#)
- [Migration tasks \(on page 81\)](#)
- [Audit Logs \(on page 82\)](#)

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.

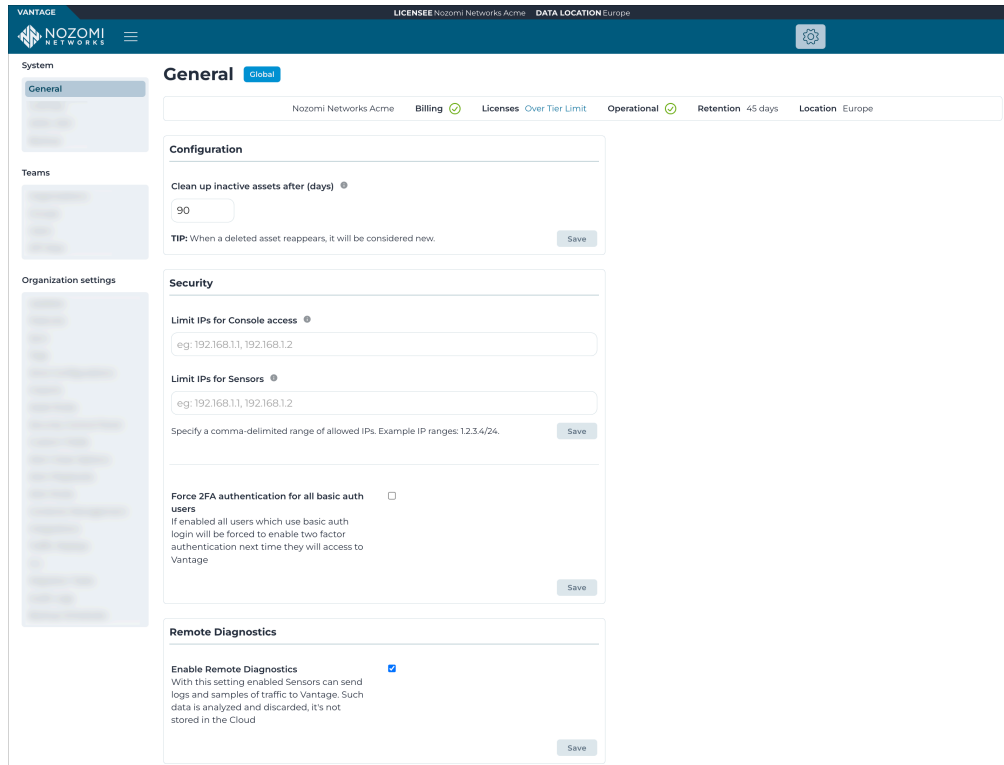


Figure 4. General page

Status

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

- Billing
- Licenses
- Operational
- Retention
- Location

Configuration

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

Security

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

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

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

Licenses

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

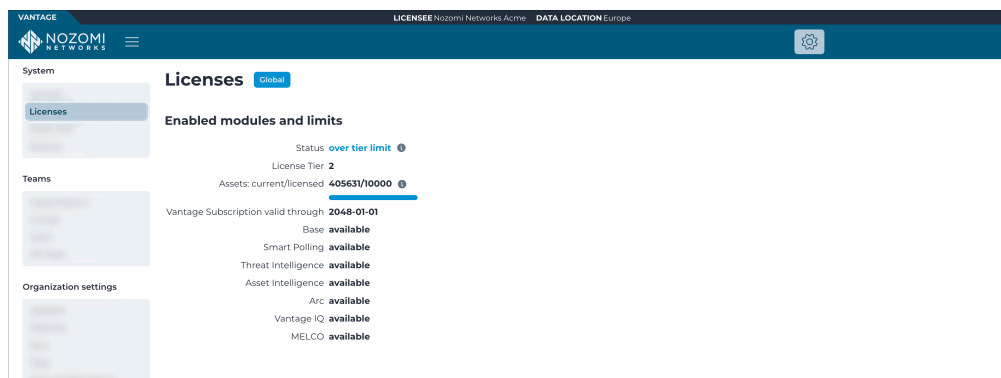


Figure 5. Licenses page

Enabled modules and limits

This section shows information for:

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

SAML Single Sign On

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

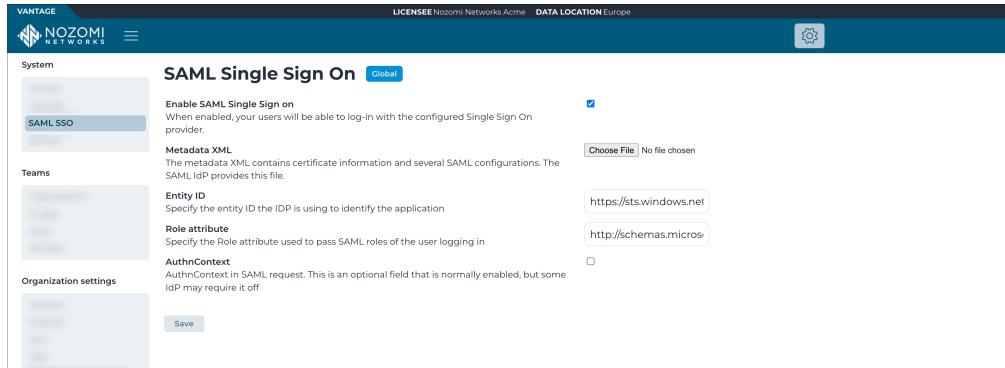


Figure 6. SAML SSO page

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.

Related information

- SAML integration configuration (on page 99)
- IdP configuration for SAML integration (on page 100)
- Troubleshooting SAML integration (on page 104)
- Configure your IdP for SAML integration (on page 101)
- Configure Vantage for SSO (on page 102)
- Configure a Google Workspace SAML application (on page 105)

Backup

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

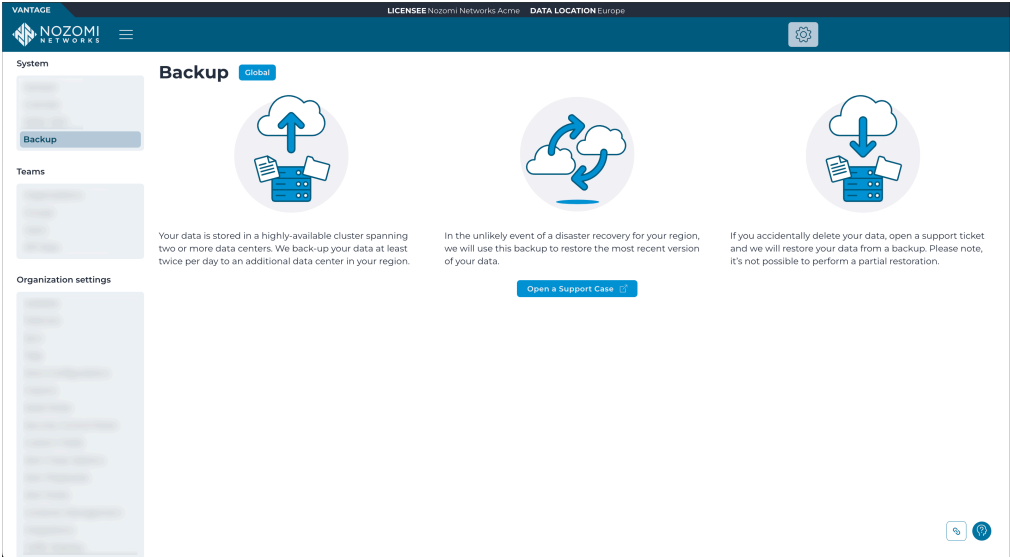


Figure 7. Backup page

Teams

Organizations

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

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

Figure 8. 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.

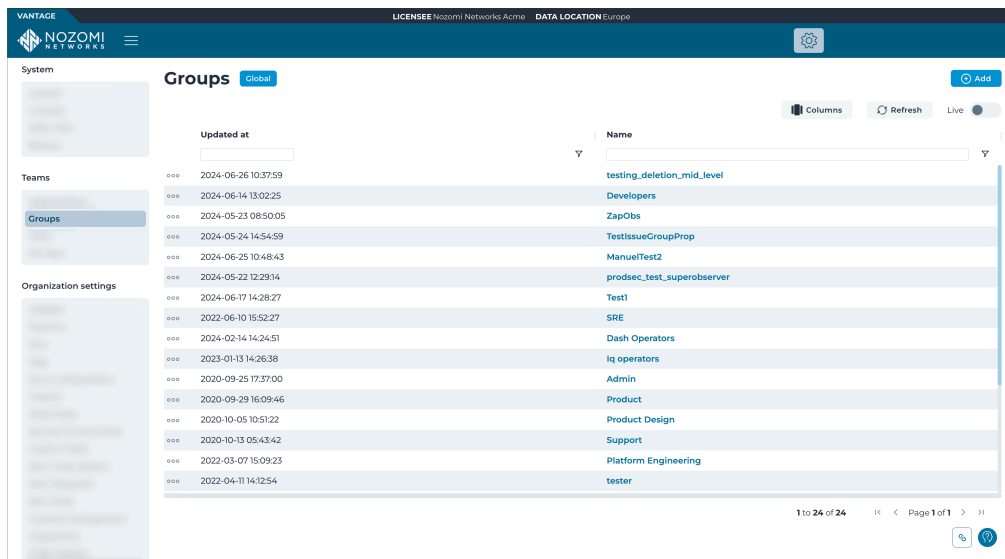


Figure 9. Groups page

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 \(on page 25\)](#).

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 \(on page 28\)](#).


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 **Role assignments**.
Result: Data entry fields show.
6. Select the **Roles** dropdown and select the role that you want to assign to the group.
Result: A matrix shows.
7. **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.
8. **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
 9. Select **Create**.
 10. **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.

Users

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

The screenshot shows the Vantage Users page. The header includes the Vantage logo, license information (Nozomi Networks Active), and data location (Europe). The page title is 'Users' with a 'Global' filter. There are navigation options for 'Columns', 'Refresh', and 'Live'. The main content is a table of users with the following columns: 'Created at', 'Display name', 'Email', and 'Groups'. The table contains 25 rows of user data. The 'Groups' column lists various roles such as Support, Test1, Developers, SRE, and SecurityResearch. At the bottom, there is a pagination indicator showing '1 to 25 of more' and 'Page 1 of more'.

Figure 10. Users page

General

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

- [SAML users \(on page 30\)](#)
- [Local users \(on page 31\)](#)



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 \(on page 24\)](#)
- [SAML integration configuration \(on page 99\)](#)

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 \(on page 39\)](#).

Invite

This button lets you [Invite a user \(on page 32\)](#) 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 the following fields and a button:

- Name and surname**: A text input field.
- Email address**: A text input field.
- Initial Group**: A dropdown menu.
- Invite**: A blue button.

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:

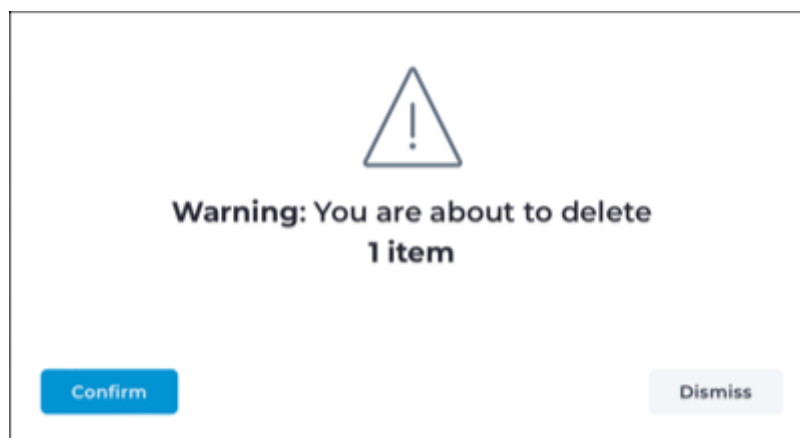
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **☰** icon

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.

API keys

API keys in Vantage

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

General

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

Third-party applications

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

1. Generate the [API](#) key and token in Vantage
2. Use your third-party application to call Vantage and pass the key and token for authentication

Nozomi Networks recommends that you:

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

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

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

For more information on choosing the right approach for your implementation, see [Considerations when you connect multiple applications to Vantage \(on page 38\)](#).

Application IP address ranges

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

Users

For [API](#) keys and users:

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



Note:

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

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

- Scope
- Permissions
- Allowed [IP](#) address ranges

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

- [Application IP address ranges \(on page 35\)](#)
- [User scope and permissions \(on page 36\)](#)

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 \(on page 38\)](#).

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.

The screenshot shows the Vantage API Keys page. The page title is "API Keys" with a "Global" filter. The table below lists various API keys with their details.

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.
	AK03dcbe	test1	n.a.	n.a.	12.3.4/24	n.a.
	AK6e7522	test	n.a.	n.a.	n.a.	n.a.
	AK44f199e	n.a.	n.a.	n.a.	n.a.	n.a.
	AK99e07f1	xxx	n.a.	n.a.	12.3.4/24	n.a.
	AK70e90f1	ssdsdsd	n.a.	n.a.	12.3.4/24	n.a.
	AK6e7522	qwewqe	n.a.	n.a.	12.3.4/24	n.a.
	AK5bd70ec	Swagger	n.a.	n.a.	0.0.0/32	n.a.
	AKe1f5d5	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.

At the bottom of the table, it indicates "1 to 25 of more" and "Page 1 of more".

Figure 11. API Keys page


Columns

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

Refresh

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

Live

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

Generate an API key

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

Before you begin


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

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

About this task

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

Procedure

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

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

4. In the **Description** field, enter a description for the [API](#) key.

Generate new API key

Give a human-friendly description to the API key.

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.

Organization
Acme

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.



Note:

Nozomi Networks recommends that the description includes the name of the application that will connect with the [API](#) key.

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

**Note:**

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

6. 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.

7. Select **Generate**.

Result: Vantage generates a key and displays its:

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

8. **!** **Important:**

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




Record these details:

- Key name
- Key token
- Allowed ips

Revoke an API key

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

Procedure

1. Log into Vantage as an administrator.
2. In the top navigation bar, select .
Result: The administration page opens.
3. In the **Teams** section, select **API Keys**.
Result: The **API Keys** page opens.
4. In the **Key name** column, hover your mouse over the **API** key that you want to revoke.
Result: The  icon shows.
5. Select the  icon.
Result: The **API** key has been revoked.

Organization Settings

Update Policy

The **Update Policy** 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.

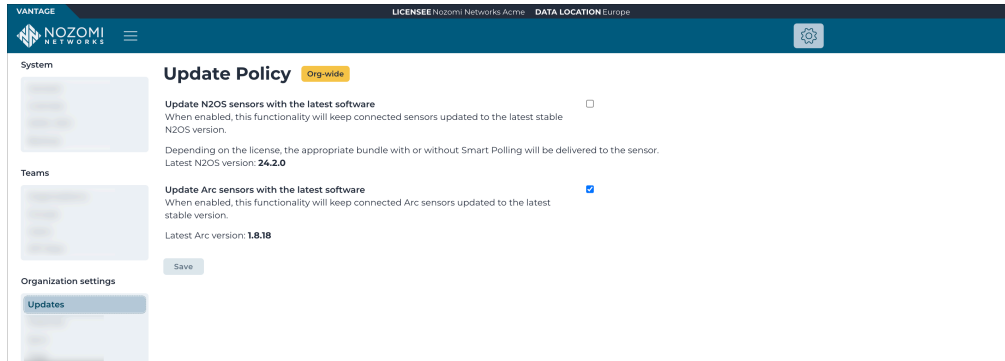


Figure 12. Update Policy page

Features

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

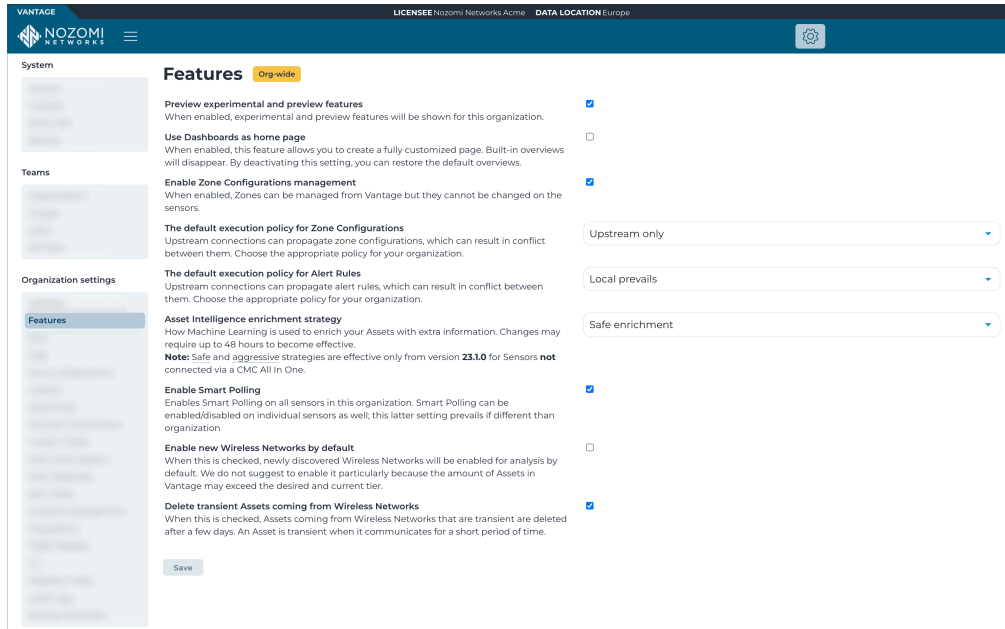


Figure 13. Features page

Sensors Synchronization Settings

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

The screenshot displays the 'Sensors Synchronization Settings' page in the Vantage interface. The page is titled 'Sensors Synchronization Settings' and is marked as 'Org-wide'. It features a sidebar with navigation options: System, Teams, and Organization settings (with 'Sync' selected). The main content area includes a 'Data Synchronization Interval' section with a timeline visualization, a 'Discard out of retention data' checkbox (checked), and a 'Use Vantage only for license provisioning' checkbox (unchecked). Below these are several organization settings, each with a description and a checkbox (all checked): Alerts, Assets, Audit Items, Health Logs, Nodes, Links, Variables, Subnets, Sessions, Backup schedules, Zones, Captured URLs, Smart Polling plans, Node points, Asset CPEs, and Reports. A 'Save' button is located at the bottom left, and a help icon is at the bottom right.

Figure 14. Sync page

Use Vantage only for license provisioning

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

Tags

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

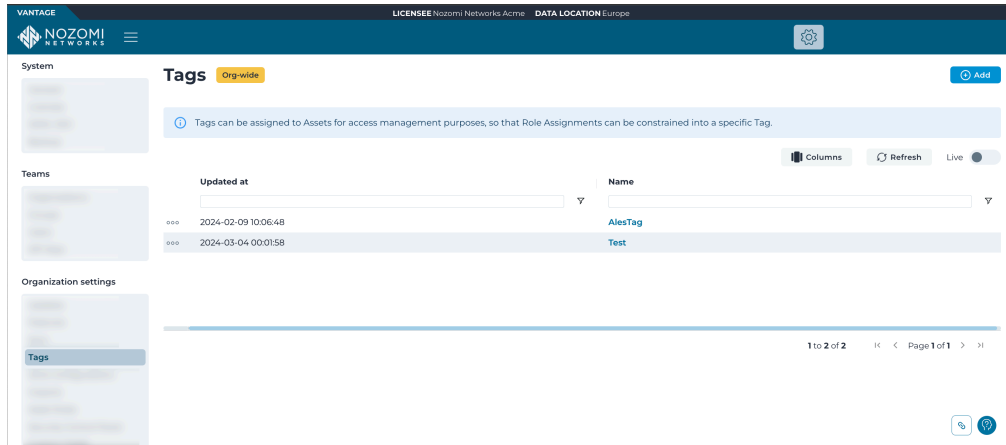


Figure 15. Tags page

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

Zone configurations in Vantage

An explanation of security zones and zone configurations.

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.

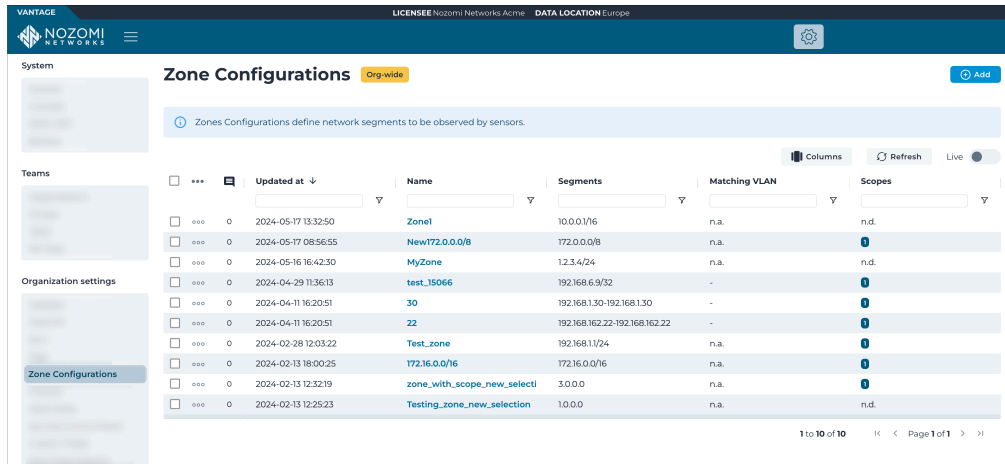
In Vantage, a zone configuration includes criteria that identify the assets that should belong to the zone. The configuration also specifies how Vantage handles these assets.

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.

Zone Configurations

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



Updated at	Name	Segments	Matching VLAN	Scopes
2024-05-17 13:32:50	Zone1	10.0.0/16	n.a.	n.d.
2024-05-17 08:56:55	New172.0.0.0/8	172.0.0.0/8	n.a.	0
2024-05-16 16:42:30	MyZone	1.2.3.4/24	n.a.	n.d.
2024-04-29 11:36:13	test_15066	192.168.6.9/32	-	0
2024-04-11 16:20:51	30	192.168.1.30-192.168.1.30	-	0
2024-04-11 16:20:51	22	192.168.162.22-192.168.162.22	-	0
2024-02-28 12:03:22	Test_zone	192.168.1/24	n.a.	0
2024-02-13 18:00:25	172.16.0.0/16	172.16.0.0/16	n.a.	0
2024-02-13 12:32:19	zone_with_scope_new_selecti	3.0.0.0	n.a.	0
2024-02-13 12:25:23	Testing_zone_new_selection	1.0.0.0	n.a.	n.d.

Figure 16. Zone Configurations page

Add

This button lets you add a new zone configuration.


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 new**.

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

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



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 [Central Management Console \(CMC\)](#)s and Guardians, that aggregate and send data to Vantage

Result: A dialog opens.

17. Select the  icon. Select an option to filter for the item you want to select.

18. Select **Confirm**.

19. **Optional:** To add another item to define the scope, do steps [17 \(on page 52\)](#) and [18 \(on page 52\)](#) again as necessary.

20. Select **Create**.

Results

The zone configuration has been created.

Imports

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

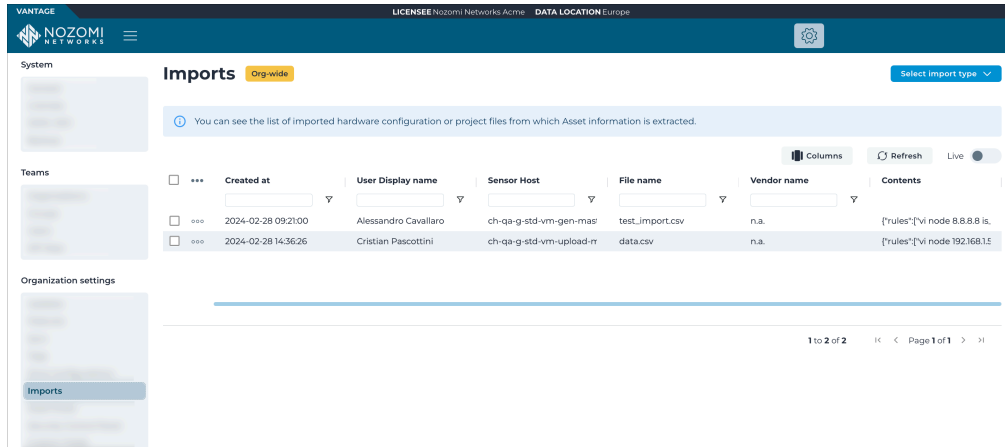


Figure 17. Imports page

Select import type

This button lets you select an type to import.


Columns

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

Refresh

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

Live

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

Asset Rules

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

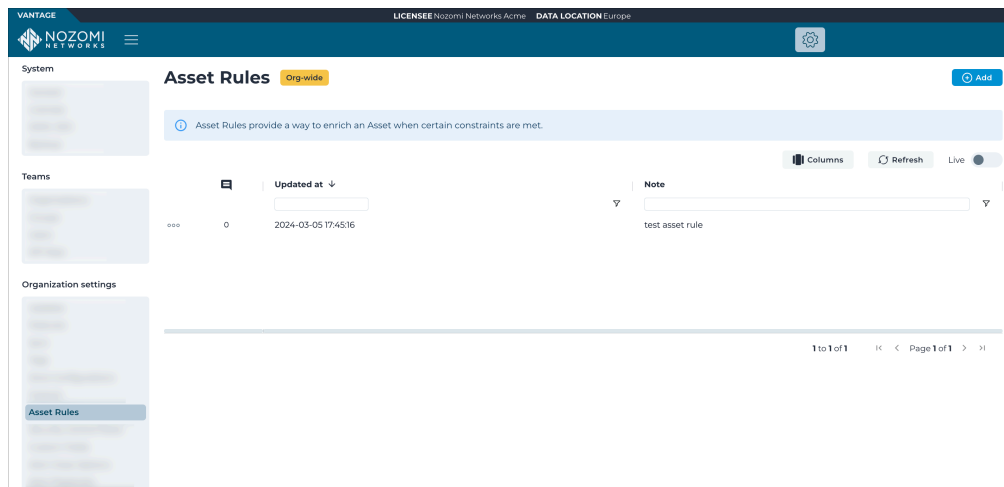


Figure 18. Asset Rules page

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:

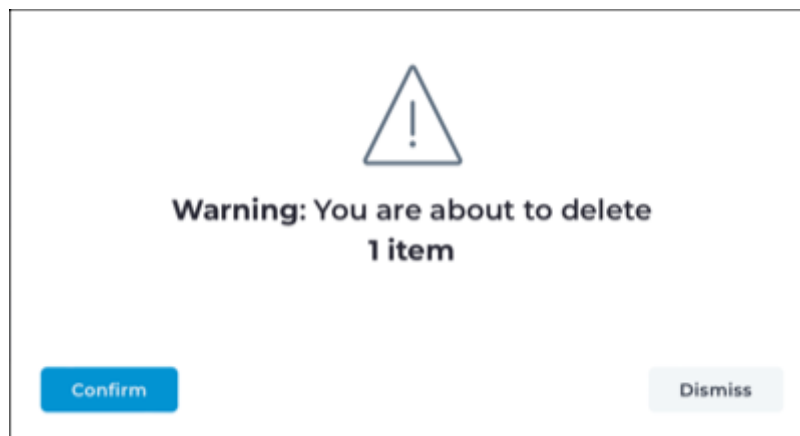
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **☰** icon

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.

Alert Close Options

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

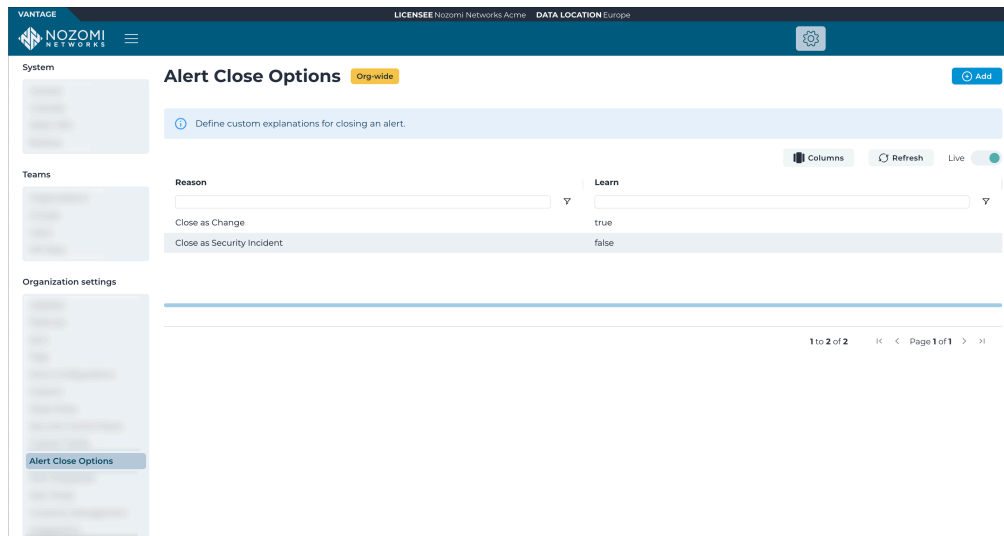


Figure 19. Alert Close Options page

Add

This button lets you add a new alert closing option.


Columns

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

Refresh

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


Live

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

Add an alert closing option

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

Procedure

1. In the top navigation bar, select .
Result: The administration page opens.
2. In the **Organization settings** section, select **Alert Close Options**.
Result: The **Alert Close Options** page opens.
3. Select **Add new**.
Result: The **Create Alert Option** page shows.
4. In the **Reason for closing** field, enter a reason.
5. Choose an option:
Choose from:
 - Treat as incident
 - Learn
6. Select **Create**.

Results

The alert closing option has been created.

Alert Playbooks

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

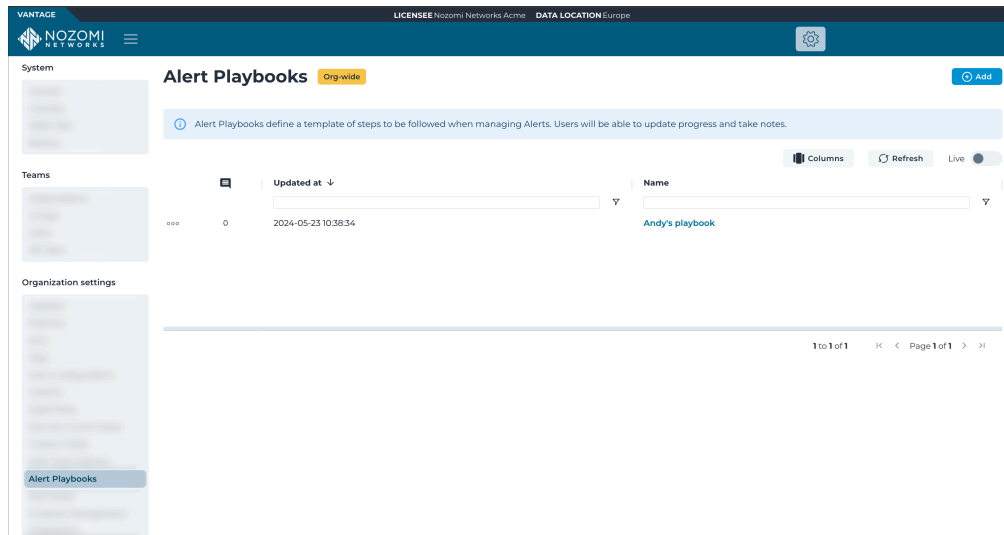


Figure 20. Alert Playbooks page

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:

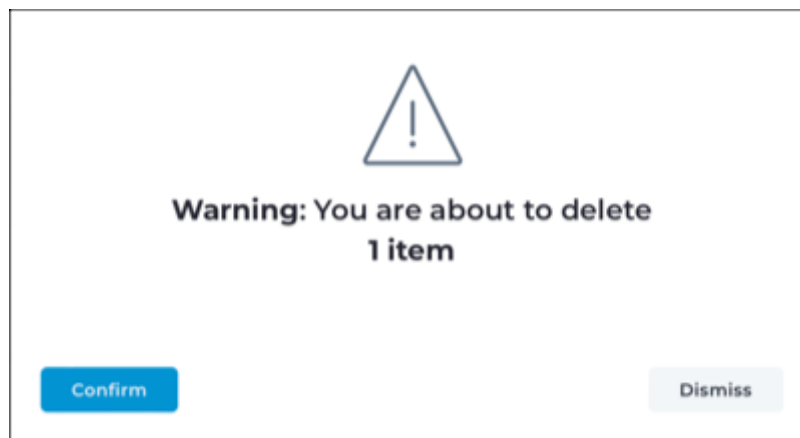
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **☰** icon

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.

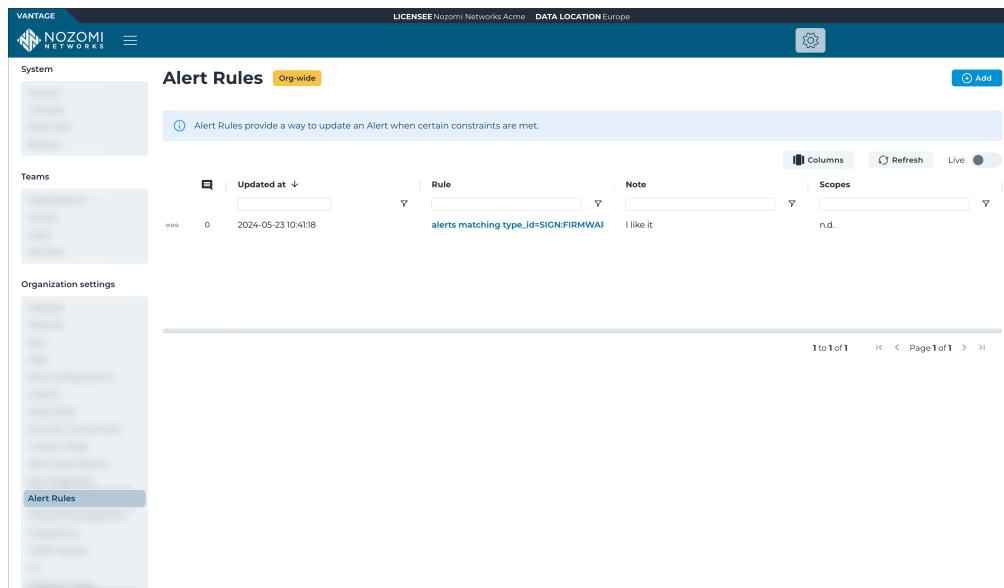


Figure 21. Alert Rules page

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:

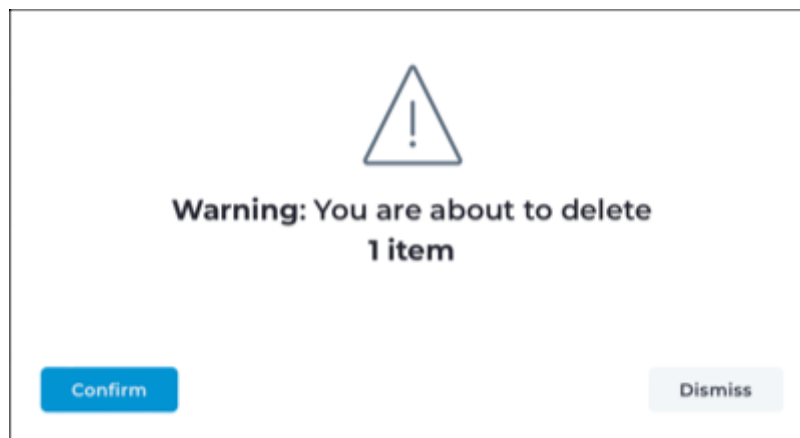
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **☰** icon

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.

Integrations

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

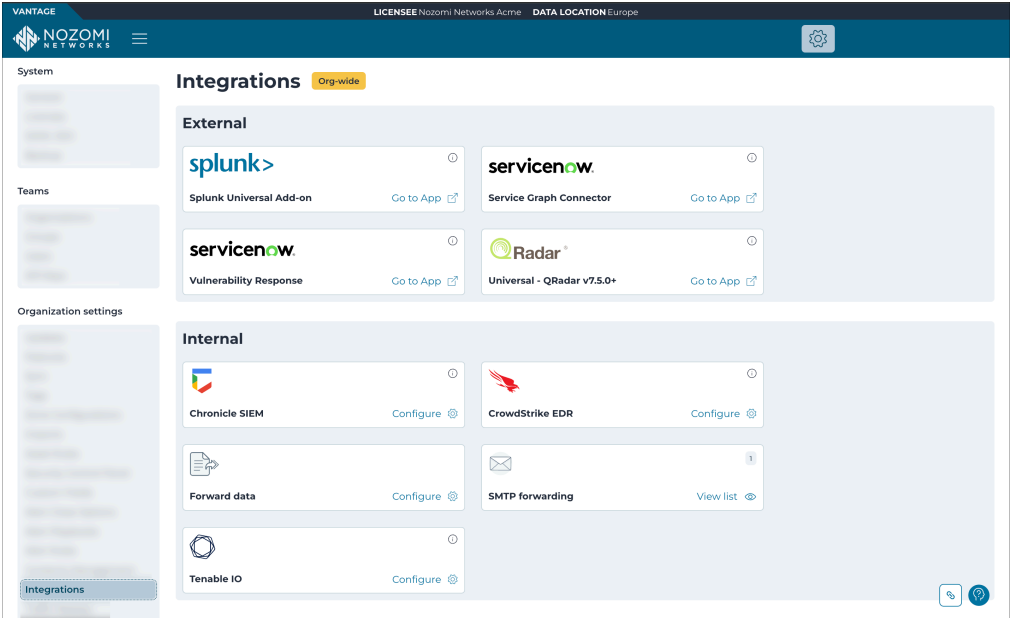


Figure 22. Integrations page

CrowdStrike

Overview

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

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

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

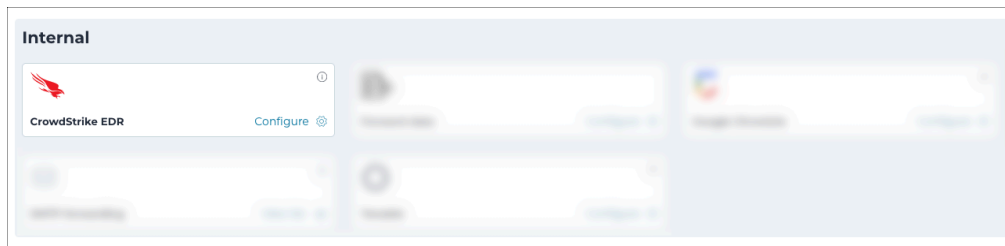


Figure 23. Internal integrations

Requirements

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

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

- Endpoint
- Client ID
- Client secret


Configure the CrowdStrike EDR integration

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

Before you begin

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

Procedure

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

Result: The **CrowdStrike EDR** integration settings page opens.

3. In the **Description** field, enter details that will help you to easily identify it in the future.

The screenshot shows the 'Integrations' page with the following fields and options:

- Integrations** > CrowdStrike EDR > New integration
- How this integration works**: Vantage receives assets information from CrowdStrike. [Read more](#)
- Description***: Text input field with placeholder text: "Use a descriptive name, it will be used for listing all integrations, so you can easily find this one". Below the field is the label "Required".
- Endpoint***: Dropdown menu with the text "Select one endpoint". Below the field is the label "Required".
- Client ID***: Text input field. Below the field is the label "Required".
- Client secret***: Text input field. Below the field is the label "Required".
- Radio buttons for **Only enrich** (selected) and **Create and enrich**.
- Vantage Asset query filter**: Text input field with placeholder text: "filter the assets you want to enrich e.g. 'where os include? Window'".
- Buttons: **Add**, **Check**, and **Cancel**.

4. From the **Endpoint** dropdown, select the appropriate CrowdStrike endpoint.
5. In the **Client ID** field, enter the CrowdStrike client ID.
6. In the **Client secret** field, enter the CrowdStrike client secret.
7. Choose an option:
 - Choose from:**
 - **Only enrich**
 - **Create and enrich**
8. If you chose **Create and enrich**, enter details in the **CrowdStrike query filter**.

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

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

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



Note:

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

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

Tenable

Tenable data integration

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

Assets

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

**Note:**

Only assets that have a confirmed `MAC` address are taken into consideration.

The asset information that follows is sent to TenableIO:

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

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

Vulnerabilities

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

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

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

The vulnerabilities information that follows is sent to TenableIO:

- `cve`
- `time`

The output value of the TenableIO Plugin is set to `Imported from`, concatenated with the source value, and the accuracy value - as defined in the [Vulnerabilities \(on page 73\)](#) section above.

Edit configuration

It is possible to edit an existing integration configuration.

You can edit these fields:

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

Integrations
Integrations > Tenable > New integration

How this integration works
Vantage can send assets and vulnerabilities to TenableIO. [Read more](#)

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

Access Key*

Secret Key*

Enable sending Asset Vulnerabilities
Tenable Scan name
The name of the Tenable's Scan that the vulnerabilities will be associated with

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

Figure 24. Edit configuration fields

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

Integrations
Integrations > Tenable > New integration

How this integration works
Vantage can send assets and vulnerabilities to TenableIO. [Read more](#)

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

Access Key*

Secret Key*

Enable sending Asset Vulnerabilities
Tenable Scan name
The name of the Tenable's Scan that the vulnerabilities will be associated with

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

Figure 25. Update integrations

Requirements

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

The Tenable integration requires:

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

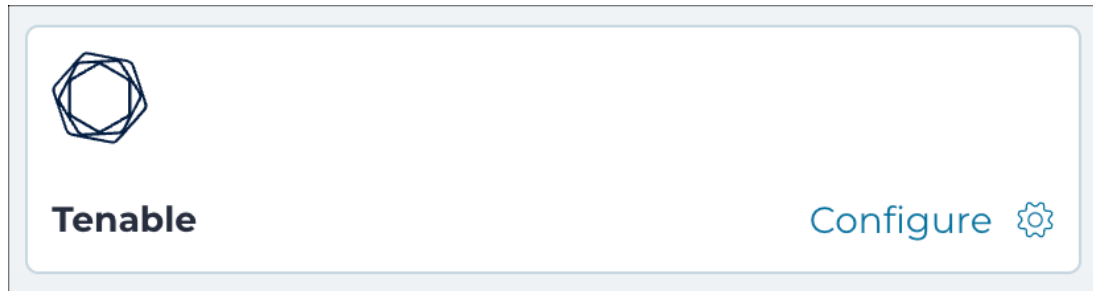
If the integration is configured to also send asset vulnerabilities, then you need to set user permissions to `ADMINISTRATOR [64]`.

Configure the Tenable integration

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

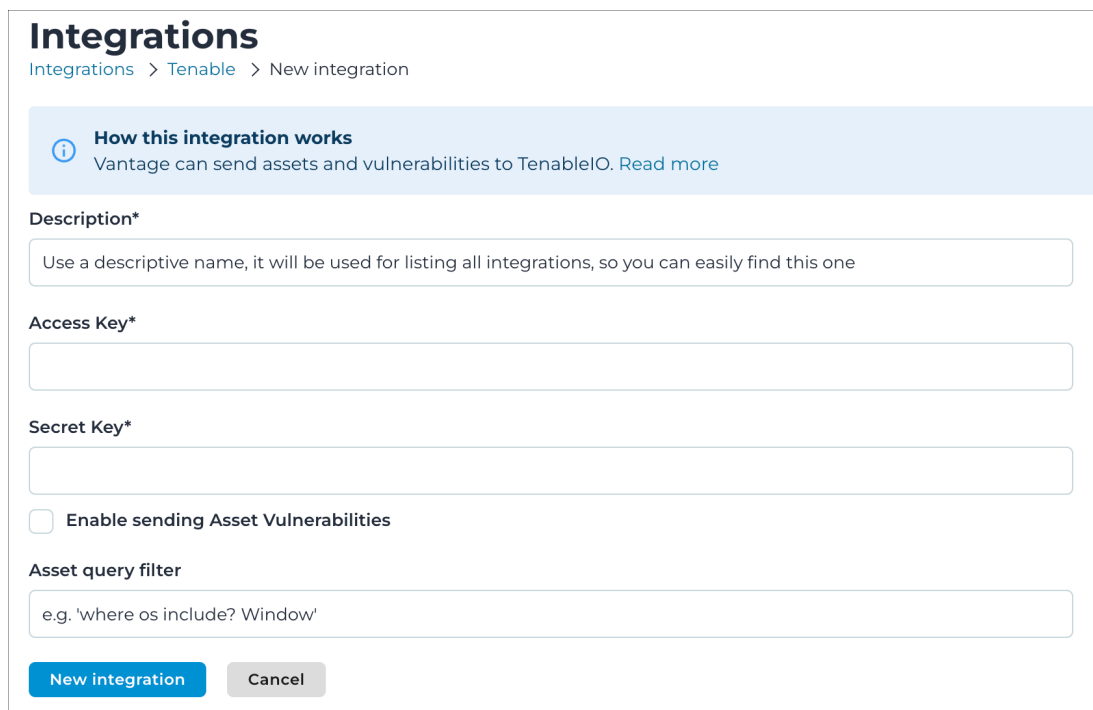
Procedure

1. Select **Administration**.

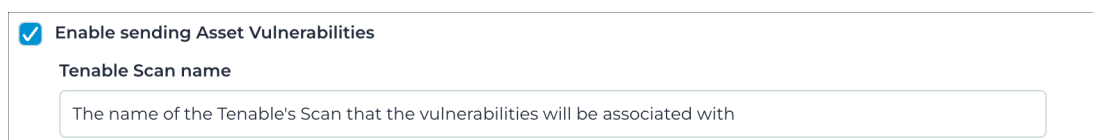


Result: Integrations and Tenable integration will show inside the **Internal integration** group.

2. Select **Configure**.



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



4. Optional:

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

Features

Org-wide
Preview experimental and preview features
When enabled, experimental and preview features will be shown for this organization.

5. Enter the information in the applicable fields, as necessary.

6. Select **New integration**.

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.

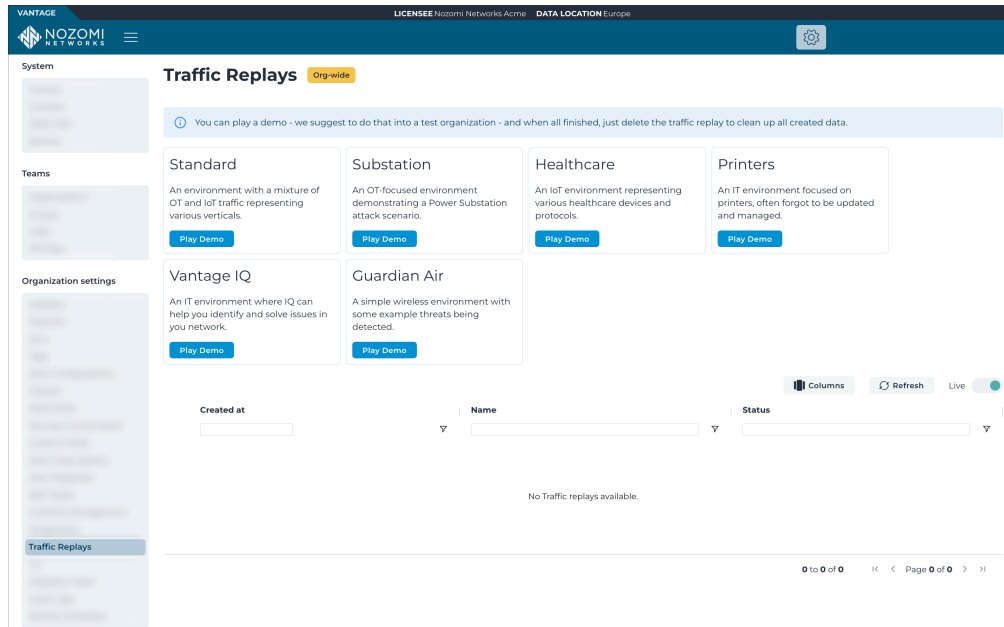


Figure 26. Traffic Replays page


Columns

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

Refresh

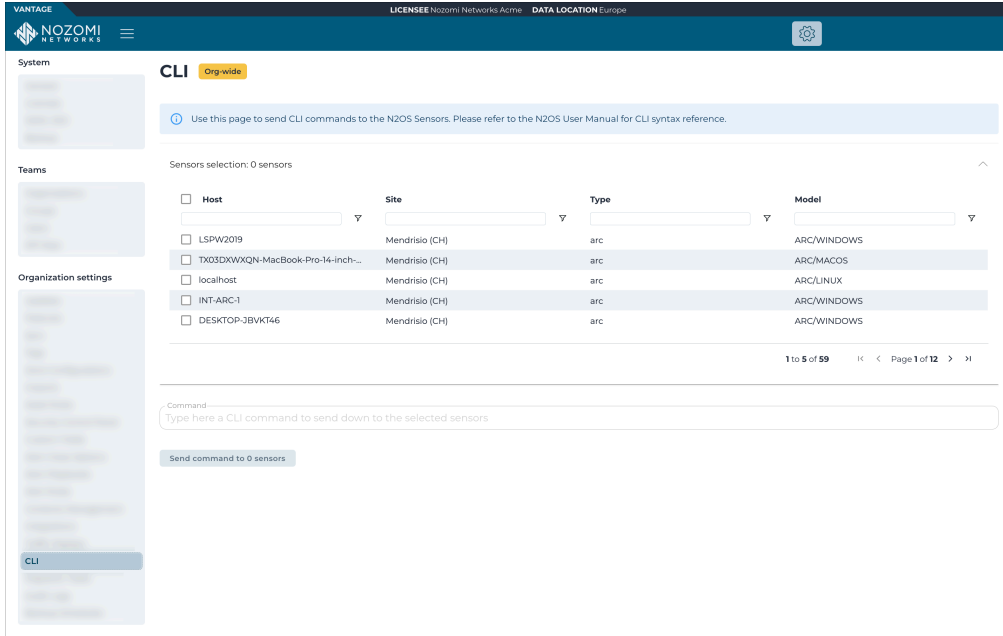
The **Refresh**  icon lets you immediately refresh the current view.

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.



The screenshot displays the Vantage CLI interface. At the top, the header includes the Vantage logo, the Nozomi Networks logo, and navigation links for 'LICENSE: Nozomi Networks Acme' and 'DATA LOCATION: Europe'. The main content area is titled 'CLI' and includes a sub-header 'Org-wide'. A blue banner provides instructions: 'Use this page to send CLI commands to the N2OS Sensors. Please refer to the N2OS User Manual for CLI syntax reference.' Below this, a section for 'Sensors selection: 0 sensors' features a table with columns for Host, Site, Type, and Model. The table lists five sensors, each with a checkbox in the Host column. A 'Command' text field is located below the table, with a 'Send command to 0 sensors' button underneath. The interface also shows a sidebar with 'System', 'Teams', and 'Organization settings' sections, and a pagination indicator at the bottom right of the table area.

Host	Site	Type	Model
<input type="checkbox"/> LSPW2019	Mendrisio (CH)	arc	ARC/WINDOWS
<input type="checkbox"/> TX03DXWXQN-MacBook-Pro-14-inch...	Mendrisio (CH)	arc	ARC/MACOS
<input type="checkbox"/> localhost	Mendrisio (CH)	arc	ARC/LINUX
<input type="checkbox"/> INT-ARC-1	Mendrisio (CH)	arc	ARC/WINDOWS
<input type="checkbox"/> DESKTOP-JBVKT46	Mendrisio (CH)	arc	ARC/WINDOWS

Figure 27. 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.

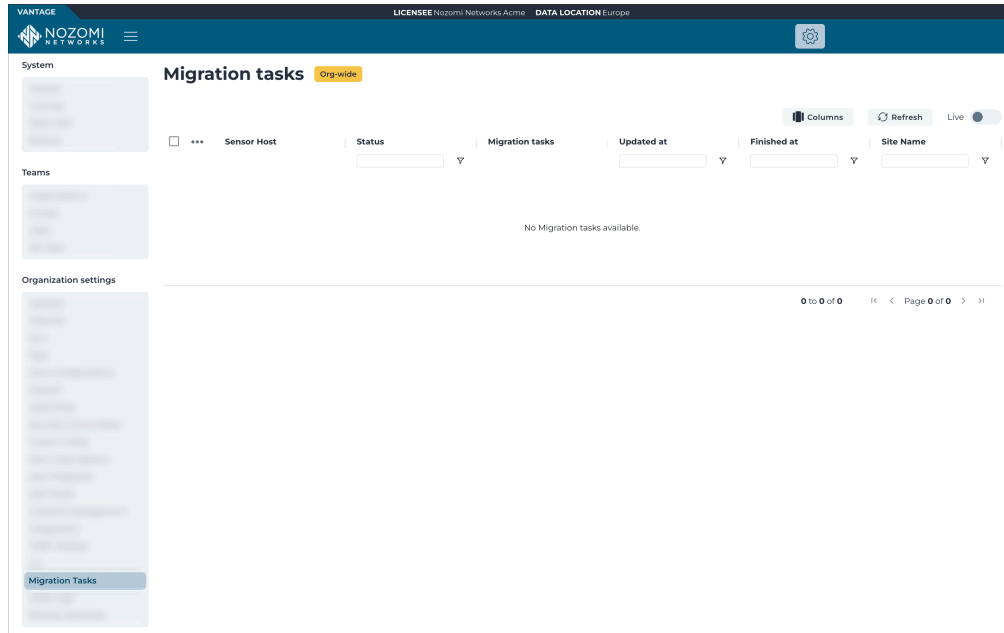


Figure 28. Migration tasks page


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.

The screenshot displays the Vantage Audit Logs interface. At the top, there's a header with 'VANTAGE NOZOMI NETWORKS' and 'LICENSEE Nozomi Networks Acme DATA LOCATION Europe'. Below the header, there's a navigation menu on the left with 'System', 'Teams', 'Groups', and 'Organization settings'. The main content area is titled 'Audit Logs' and includes a search bar for 'Site (1)' and 'Name (25)'. Below the search bar, there's a table of audit logs with the following columns: Time, Sensor Host, Name, Event, Username, and Site Name. The logs are sorted by time, showing various events such as 'User root logged in via ssh', 'Remove label for interface', 'Set up new label for interface', 'User signed in', 'Login via SAML', 'Deleted report file from list', 'Scheduled backup file created', and 'Ingested pcap'. The 'Live' toggle is currently turned on.

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

Figure 29. 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.

The screenshot shows the 'Backup Schedules' page in the Vantage Admin interface. The page title is 'Backup Schedules' with a sub-label 'Org-wide'. There is an 'Add' button in the top right corner. Below the title, there are two informational messages: 'Define backup archive generation schedules on sensors' and 'This feature requires NZOS 24.2 or greater.' Below these messages, there is a table of backup schedules. The table has columns for 'Name', 'Frequency', 'Strategy', 'Include traces', 'Max backups number', and 'Enc'. The table lists three schedules: 'GenMasterBackup_edit', 'HourlyBackup', and 'BackupCmcLabMaster'. The 'HourlyBackup' schedule is highlighted. At the bottom of the table, there is a pagination control showing '1 to 3 of 3' and 'Page 1 of 1'. There are also 'Columns', 'Refresh', and 'Live' controls above the table.

	Name	Frequency	Strategy	Include traces	Max backups number	Enc
<input type="checkbox"/>	GenMasterBackup_edit	daily at 13:00	local	false	1	true
<input type="checkbox"/>	HourlyBackup	hourly at minute 30	local	false	3	false
<input type="checkbox"/>	BackupCmcLabMaster	daily at 13:10	local	false	4	false

Figure 30. Backup Schedules page

Add

This button lets you [Add a backup schedule \(on page 84\)](#).


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:

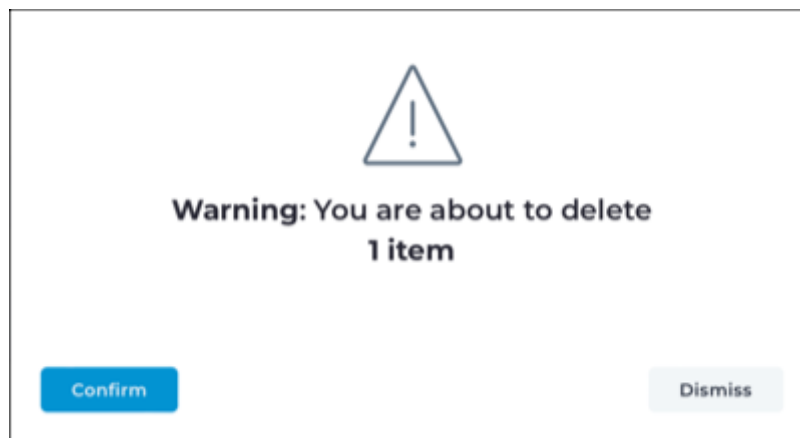
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **☰** icon

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.

Chapter 3. Migration



Migration to N2OS 22.6.0

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


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

Credentials Manager

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

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

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

 Action required: **Legacy credentials**

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

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

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

Data Model Manager

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

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

When you upgrade to [N2OS](#) version 22.6.0, you can manage this migration from Vantage.

**Note:**

In some cases, other systems integrated with [N2OS](#) through the [API](#) are also impacted.

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

If you need to delay these changes, you should disable automatic software updates for your downstream installation.

Complete strings and substrings

The migration might affect these two types of strings:

- Complete strings: Complete strings are those where the items to be changed appear as a whole
- Substrings: Substrings are those that do not show the full name

Where a complete string is used to reference the table field, or value, Vantage can automatically migrate your sensors to use the new data model. Where a substring is used to refer to a table field or value that has changed, you must take additional steps outside of the [Migration tasks \(on page 81\)](#) page.

Examples of complete strings:

- `query: alerts | where type_id == SIGN:TCP-MALFORMED`
- `alert rule having in scope type_id: SIGN:TCP-MALFORMED`

Examples of substrings:

- `query: alerts | where type_id include? SIGN:TCP`
- `query: alerts | where type_id include? SIGN:`
- `query: alerts | where type_id include? LINK`

Migrate to the N2OS 22.6.0 data model

This procedure gives you all the steps that you might need to do to migrate to the N2OS 22.6.0 data model.

Procedure

1. Upgrade to N2OS 22.6.0 to get the health logs to help migration to the new data model.

2. In the top navigation bar, select 

Result: The administration page opens.

3. In the **Organization settings** section, select **Migration Tasks**.


Result: The **Migration Tasks** page opens.

4. In the **Description** field, enter the string `Recommended` changes of the table to search for instances of the old names.

Result: Vantage returns the complete strings that need to be updated. By default, the health logs where this data is collected are synchronized to Vantage, so you see an overview of all such logs throughout your entire installation.



5. Before you do the next steps, review the results to understand these changes.

Migration tasks



 Action required: **Breaking changes**

The names and values of some table fields have changed in N2OS version **22.6.0**. You should ensure that existing items will continue to function after upgrading. Any saved queries, assertions, alert rules, or data integration scopes referencing the affected tables are updated by selecting the Execute button.

Note: that it can only identify full string references to these table field names and values.

Choose columns:  Refresh  Live

<input type="checkbox"/>	***	Sensor Host	Status	Migration tasks	Updated at	Finished at
<input type="checkbox"/>	...	n.a.	pending		2022-11-17 02:10:22	n.a.
<input type="checkbox"/>	...	Guardian-CustomNef	pending		2022-11-17 06:28:12	n.a.

1 to 2 of 2  Page 1 of 1 



Note:

The changes are applied to the complete downstream installation. This means that when you execute the changes in Vantage, the changes will be applied to all CMCs and Guardians that are connected downstream.

6. Choose the method that you want to use.

Choose from:

- If you want to execute or ignore the changes individually, do steps [7 \(on page 92\)](#) and [8 \(on page 92\)](#).
- If you want to execute all the changes together, go to step [9 \(on page 92\)](#)



Note:

Nozomi Networks recommends that you execute all the changes together.

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

Choose from:

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

8. Select **Execute** or **Ignore** as applicable.

9. Select **Execute all**.

10. To verify that the changes have been successfully applied in your [N2OS](#) environment, run the shell command: `n2os-recommended-changes`

Result: If the changes were made successfully, the list will be empty.

11. **Optional:** If necessary, update substrings that have changed.



Note:

Because Vantage can only manage migration for complete strings, you might need to take additional steps to address substrings that are used for:

- Saved queries
- Assertions
- Custom reports
- Alert rules
- Other items within the scope of integration

- a. Review the table and field names that have changed in [N2OS 22.6.0 Data Model Changes \(on page 94\)](#) and make a note of those that might impact your installation.
- b. Review your sensors' contents to identify all the references that still need to be updated.
- c. To replace the old names with the new names, manually edit the applicable substrings.

N2OS 22.6.0 Data Model Changes

A list of the changes to the table fields and values in N2OS version 22.6.0.

Field in scope	Current	New	Description/Rationale
alerts: type_id	SIGN:TCP- MALFORMED	SIGN:NET- MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE- CHANGE	SIGN:FIRMWARE- TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM- DOWNLOAD	SIGN:PROGRAM- TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM- UPLOAD	SIGN:PROGRAM- TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA- NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA- MALFORMED	SIGN:MALFORMED- TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK- MALFORMED	SIGN:MALFORMED- TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA- INJECTION	SIGN:PROTOCOL- INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN- FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization

Field in scope	Current	New	Description/Rationale
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL- APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL- CONFIRMED	VI:NEW-LINK- CONFIRMED	Name harmonization



Chapter 4. SAML integration



SAML integration configuration

It is important to understand how Vantage uses security assertion markup language (SAML) single sign-on (SSO) for authentication.

General

Vantage supports [SAML SSO](#) authentication. Our integration requires your [IdP](#) to be compatible with [SAML 2.0](#). To authenticate, Vantage requires the user's:

- Email address
- Entity ID attributes

The [SAML](#) configuration process is often error prone. This section assumes that you're familiar with:

- The [SAML](#) protocol
- Your [IdP](#) software
- The exact details of your specific [IdP](#) implementation

You will need to configure:

- [Configure your IdP for SAML integration \(on page 101\)](#)
- [Configure Vantage for SSO \(on page 102\)](#)

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 \(on page 24\)](#).

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.

This means that the complete [URL](#) you need to define in your [IdP](#) might be:

- ACS:
`https://customer1.customers.us1.vantage.nozominetworks.io/api/v1/saml/auth`
- Entity ID: `https://my.idp.net/0000-0000-0000-000-0000000000001/`

Vantage can integrate with many [IdP](#). For more details about specific [IdP](#), see:

- [Configure an Azure Active Directory enterprise application \(on page 109\)](#)
- [Configure an Okta enterprise application \(on page 107\)](#)
- [Configure a Google Workspace SAML application \(on page 105\)](#)

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 \(on page 100\)](#).

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 \(on page 101\)](#) 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 `da10ff75-d045-4a5a-8747-6d2a2ee47cdd`, the [IdP](#) looks for the `da10ff75-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 **SAML 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.

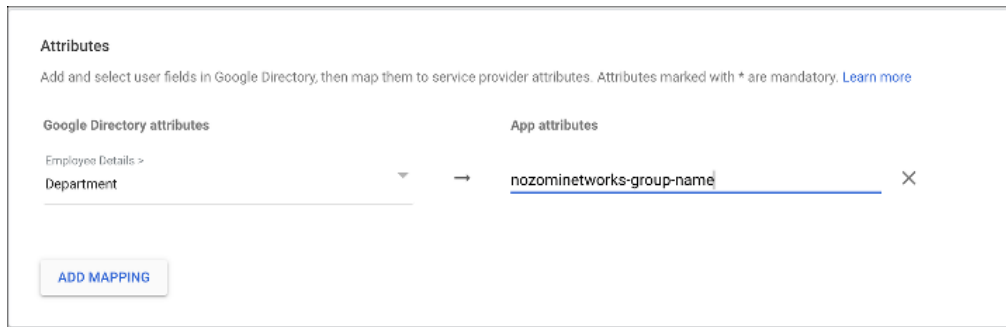
Procedure

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 columns: "Google Directory attributes" and "App attributes".

In the "Google Directory attributes" column, there is a dropdown menu with "Employee Details >" above it. The selected item is "Department".

An arrow points from the "Department" dropdown to the "App attributes" column.

In the "App attributes" column, there is a text input field containing the value "nozominetworks-group-name". To the right of the input field is a close button (X).

At the bottom left of the configuration area 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 \(on page 102\)](#).

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 \(on page 99\)](#).

Procedure

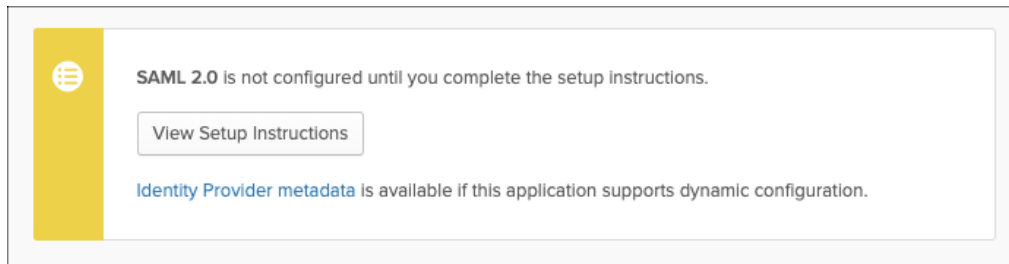
1. In the Okta Admin console, select **Applications > > Create App Integration**.
2. Select **SAML 2.0**.
3. Enter a name such as **Vantage**.
4. Select **Next**.
5. Enter the **Single sign on URL** that corresponds to the [ACS URL](#) for Vantage. For example: `https://YOUR_VANTAGE_URL/api/v1/saml/auth`
6. Enter the **Audience URI**. For example:
`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 \(on page 102\)](#).

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:

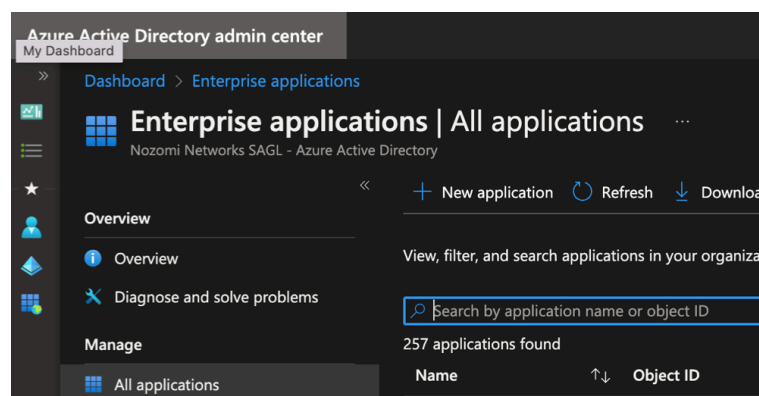
Users, guests, and applications contained directly in this group are granted access to Vantage. Azure denies access to users contained in the group's subgroups.

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 \(on page 99\)](#).

Procedure

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



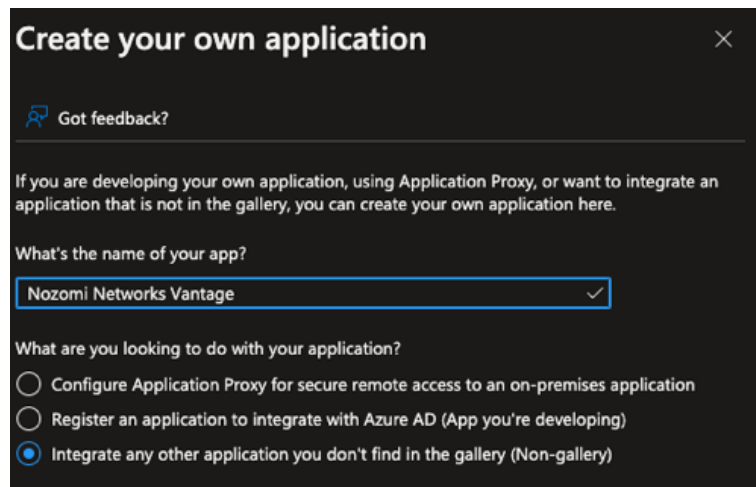
2. Select **+ New application**.

Result: A dialog shows.

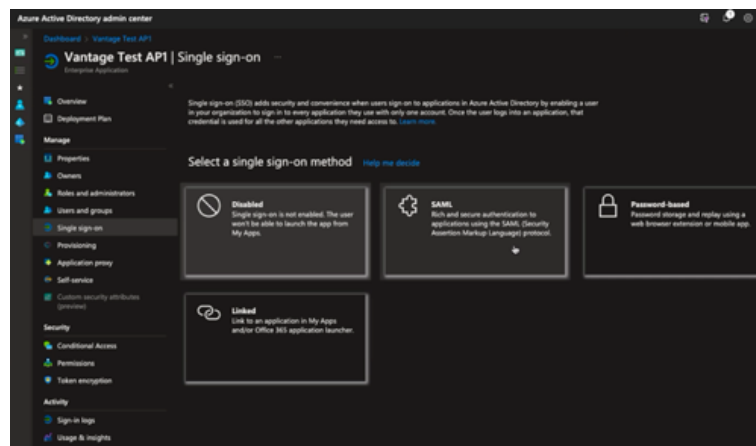
3. Select **Create your own application**.

Result: A dialog shows.

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



5. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.
6. Enter any other Azure Active Directory details that are needed to complete the configuration of the new application. Select **Create**.
- Result:** The application has been created.
7. Open the application.
8. Select **Single sign-on > SAML**.



9. Specify the **Reply URL** which corresponds to the **ACS URL** for Vantage. For example: `https://YOUR_VANTAGE_URL/api/v1/saml/auth`
10. Define the **Entity ID**. For example:
`https://sts.windows.net/6a8e8a37-ca05-4453-a502-cb8649b44db1/`

11. Define attributes and claims.

**Note:**

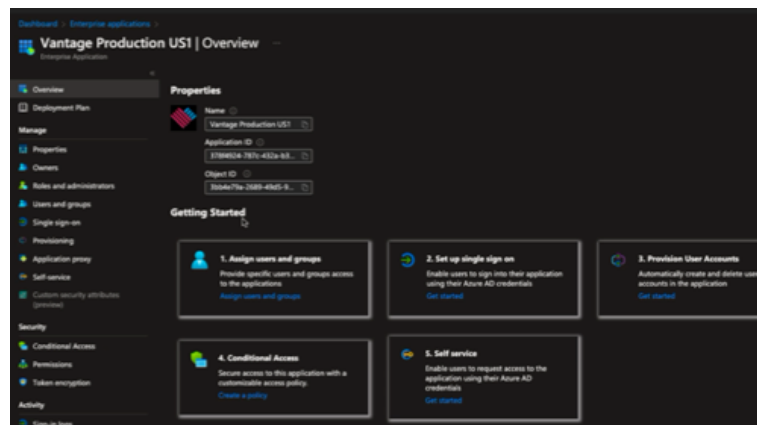
Vantage authentication relies on user group claims. You must create such claims for any group used for authentication. Users that belong to the group pass the claim that you define. *XREF*

12. **Optional:**

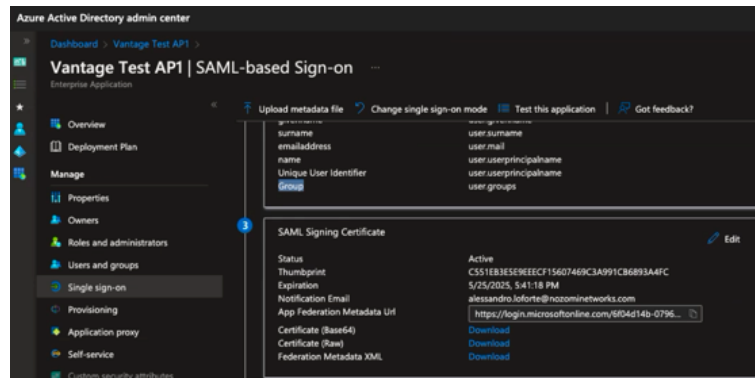
Upload an image to use as an icon in the [SAML](#) app.



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 \(on page 102\)](#).

Results

The application has been configured.

Glossary



Adaptive Learning

Adaptive Learning is when deviations are evaluated at a global level, rather than at the level of a single node. For example, using adaptive learning approach, the sensor doesn't raise an alert when it detects a device similar to those already installed in the network. This also applies for newly-detected communications that are similar to those previously detected. Adaptive learning is especially powerful and offers its best effect when combined with Asset Intelligence.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Artificial Intelligence

AI is computer intelligence, as opposed to human or animal intelligence. It is *artificial* because it is a digital computer that can perform tasks that are commonly associated with intelligent beings. *Intelligence* is the ability to learn and to reason.

Assertion Consumer Service

An ACS is a version of the SAML standard that is used to exchange authentication and authorization identities between security domains.

Asset Intelligence™

Asset Intelligence is a continuously expanding database of modeling asset behavior used by N2OS to enrich asset information, and improve overall visibility, asset management, and security, independent of monitored network data.

Central Management Console

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

Classless Inter-Domain Routing

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

Command-line interface

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

Comma-separated Value

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

Common Vulnerabilities and Exposures

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

Extensible Markup Language

XML is a markup language and file format for the storage and transmission of data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Identifier

A label that identifies the related item.

Identity Provider

An IdP is a system entity that creates, maintains, and manages identity information. It also provides authentication services to applications within a federation, or a distributed network.

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.

Media Access Control

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

National Institute of Standards and Technology

NIST is an agency of the United States Department of Commerce. NIST's mission is to promote American innovation and industrial competitiveness.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

Remote Terminal Unit

An RTU is a microprocessor-controlled electronic device that acts as an interface between a SCADA (supervisory control and data acquisition) system, or distributed control system, to a physical object. It transmits telemetry data to a master system, and uses messages from the master supervisory system to control connected objects.

Security Assertion Markup Language

SAML is an open standard, XML-based markup language for security assertions. It allows for the exchange of authentication and authorization data different parties such as a service provider and an identity provider.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Single Sign-on

SSO is an authentication method that lets users log in to one or more related, but independent, software systems.

Software as a Service

SaaS is a software licensing and delivery model. This type of software is hosted centrally and licensed on a subscription basis.

Strict (Learning)

Strict (Learning) is a mode which relies on a detailed anomaly-based approach. Each node is evaluated at the node level; when deviations from the baseline are detected, the sensor raises alerts. This approach is called strict because once a system is learned, it is expected to always behave as it did during the learning phase; maintaining systems with the Strict approach requires detailed knowledge of your system.

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 Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

User Interface

An interface that lets humans interact with machines.

Virtual Local Area Network

A VLAN is a broadcast domain that is isolated and partitioned in a computer network at the data link layer (OSI layer 2).

