

# Nozomi plugin for Vista Manager EX

## User Guide

## Introduction

---

Vista Manager EX™ is a graphical network monitoring and management tool for Allied Telesis Autonomous Management Framework™ (AMF) networks. Vista Manager EX automatically creates a complete topology map from an AMF network of switches, firewalls and wireless access points (APs). Vista Manager EX facilitates simple management of many, or all, network devices from a dashboard that gives you a central overview of your network. From the dashboard you can monitor up-to-date network status, and take action to resolve any network problems.

The Nozomi plugin lets you discover and classify devices on your network. If you run an AMF network with AMF Device Discovery enabled, you can use Nozomi to add more information about devices into Vista Manager.

After you register the plugin, Vista Manager will poll for devices and discover them using the plugin. The devices will then be displayed on the Network Map and Asset Management pages, and you can change any desired custom details. When you remove or unregister the Nozomi plugin, the devices discovered by Nozomi will be removed from the map.

### Related documents

For more information, see:

- The [Vista Manager](#) web page.
- The [Vista Manager Network Appliance \(VST-APL\) Technical Documents](#)—for information about how to install and use the VST-APL and the applications supported on it.

- [Vista Manager Virtual \(VST-VRT\) Technical Documents](#)—for information about how to deploy and use the VST-APL and the applications supported on it.
- The [Vista Manager EX Technical Documents](#)—for information about how to install Vista Manager EX as Windows software on Windows Server 2012 R2 Hyper-V or VMware vSphere Hypervisor (ESXi) 6.0, 6.5, 6.7, 7.0, and 8.0. This page also shows how to use Vista Manager EX and its optional features.

The following documents give more information about AMF and AMF Plus:

- [AMF Plus and AMF Feature Overview and Configuration Guide](#)
- [AMF Feature Overview and Configuration Guide](#) (for earlier software versions)
- [AMF Introduction and videos](#)

These documents are available from the links above or on our website at [alliedtelesis.com](http://alliedtelesis.com)

# Contents

---

- Introduction ..... 1**
  - Related documents ..... 1
  
- Contents ..... 3**
  
- Installing and configuring the Nozomi plugin for Vista Manager ..... 4**
  - Install Nozomi Guardian ..... 4
  - Generate Nozomi Guardian key and token ..... 4
  - Register the Nozomi plugin with Vista Manager ..... 5
  - Nozomi Guardian traffic monitoring and smart polling ..... 6
  
- Using the Nozomi plugin ..... 10**
  - Vista Manager Network Map ..... 10
  - Vista Manager Asset Management ..... 11
  - Vista Manager Health Monitoring ..... 13
  - Nozomi alerts and device blocking ..... 14
  - Removing the Nozomi plugin ..... 18

# Installing and configuring the Nozomi plugin for Vista Manager

---

To add the Nozomi plugin to Vista Manager requires the following steps:

- "Install Nozomi Guardian" on page 4
- "Generate Nozomi Guardian key and token" on page 4
- "Register the Nozomi plugin with Vista Manager" on page 5

Additionally, you can configure smart polling to gather additional information. See the following sections for configuration examples:

- "Configure the SSH smart polling plan" on page 6
- "Configure the WinRM smart polling plan" on page 8

## Install Nozomi Guardian

A virtual version of the Nozomi Guardian sensor is required to collect information for Vista Manager. This sensor is installed on a virtual device in your network, and then configured to communicate with the Nozomi plugin in Vista Manager.

For more details on how to install and configure Nozomi Guardian, refer to the **Installing on a Virtual Machine (VM)** section of the Nozomi Guardian user manual on the [Nozomi Customer Support Portal](#).

## Generate Nozomi Guardian key and token

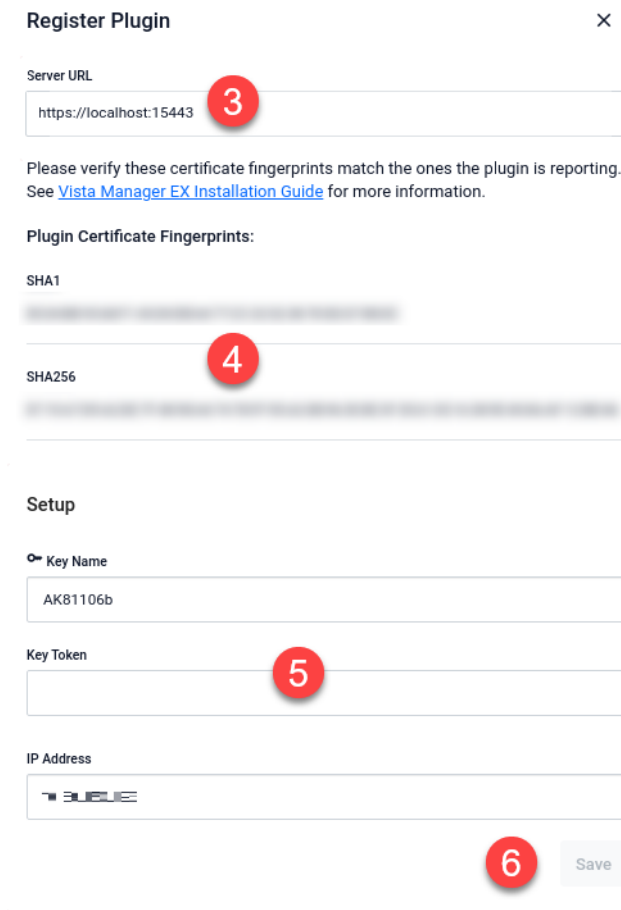
Nozomi Guardian uses OpenAPI keys to authenticate users. Using your OpenAPI key, you can generate a key token. This key token is used to create a secure connection between the Vista Manager and the Nozomi Guardian sensor. This key token is used in the ["Register the Nozomi plugin with Vista Manager"](#) section.

For more details on how to generate your key and token, refer to the **OpenAPI keys** section of the Nozomi Guardian user manual on the [Nozomi Customer Support Portal](#).

## Register the Nozomi plugin with Vista Manager

Once the Nozomi Guardian configuration is complete, you need to register the Nozomi plugin in Vista Manager. This will allow Vista Manager and the Nozomi Guardian sensor to communicate.

1. In Vista Manager, navigate to **System Management > Plugins**.
2. Click on the **+Add Plugin** button.



**Register Plugin** X

Server URL  
https://localhost:15443

Please verify these certificate fingerprints match the ones the plugin is reporting. See [Vista Manager EX Installation Guide](#) for more information.

Plugin Certificate Fingerprints:

SHA1  
[blurred]

SHA256  
[blurred]

Setup

Key Name  
AKB1106b

Key Token  
[empty]

IP Address  
192.168.1.100

Save

3. In the **Server URL** field, enter “https://localhost:15443”.
4. When the Plugin Certificate Fingerprints are shown, verify that they are correct. Once you have verified them, click on the **Confirm Fingerprints** button.
5. On the **Setup** form, enter the following information:
  - **Key Name:** The name of the Nozomi OpenAPI key you have generated.
  - **Key Token:** The token of the Nozomi OpenAPI key.
  - **IP Address:** The IP address of your Nozomi Guardian installation.
6. Click on the **Save** button.

## Nozomi Guardian traffic monitoring and smart polling

The Nozomi Guardian sensor is able to discover nodes by monitoring network traffic. Once running, it passively observes local network traffic to provide details about network devices.

In addition, you can configure **smart polling** for active asset discovery. This can provide additional information about connected devices, including operating system, firmware, and patch status.

Nozomi Guardian offers a number of different smart polling methods. Below are examples of how to configure two of them for your network.

For more details on other smart polling methods and configuration, refer to the **Smart Polling** section of the Nozomi Guardian user manual on the [Nozomi Customer Support Portal](#).

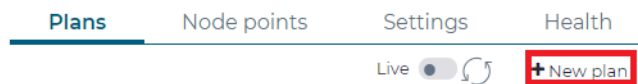
### Configure the SSH smart polling plan

The SSH polling plan extracts information using the SSH service. This lets you gather additional information about Linux devices.

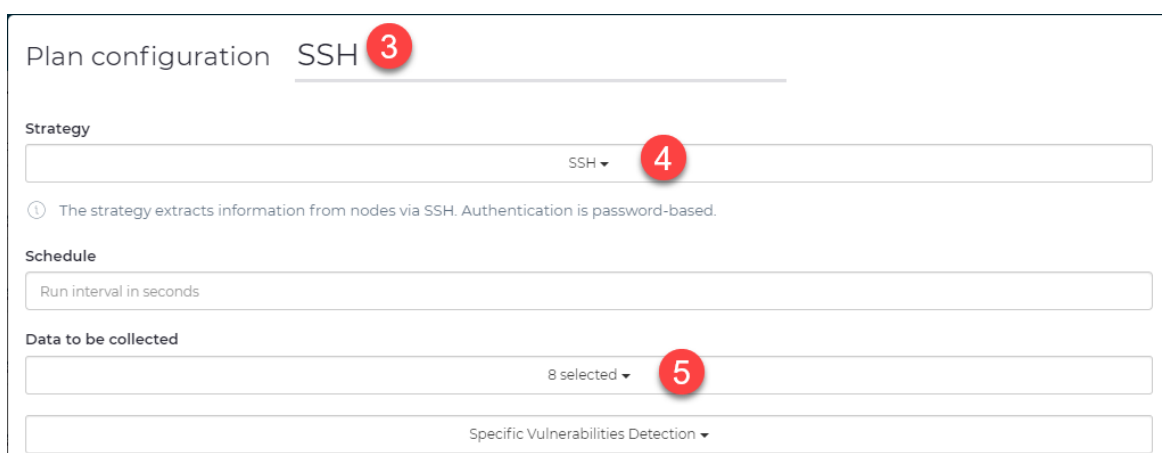
1. On the Nozomi Guardian main page, click on the **Smart Polling** tab.



2. On the **Smart Polling** page, click on **+New plan**.



3. On the **Plan configuration** page, enter a name for the new plan (SSH is a good identifier).
4. From the **Strategy** dropdown, select **SSH**.
5. From the **Data to be collected** dropdown, select **All**.

The image shows the 'Plan configuration' page for an SSH plan. The title is 'Plan configuration SSH' with a red circle '3' next to 'SSH'. Below the title, there are three main sections: 'Strategy', 'Schedule', and 'Data to be collected'. The 'Strategy' dropdown is set to 'SSH' with a red circle '4' next to it. Below the dropdown is a note: 'The strategy extracts information from nodes via SSH. Authentication is password-based.' The 'Data to be collected' dropdown is set to '8 selected' with a red circle '5' next to it. Below this dropdown is another dropdown menu set to 'Specific Vulnerabilities Detection'.

6. Click on the **Create identity** button.



7. In the **Add identity** dialog, enter the following information:

- **Name:** A name for the identity you are creating.
- **Username and Password:** The credentials used for the SSH connection.
- **Add node ID / subnet:** A list of the devices and subnets that Nozomi Guardian will attempt to create an SSH connection to.

8. Click on the **Save** button to save the new identity.

A screenshot of a dialog box titled "Add identity for 'Smart Polling/Arc: SSH'". The dialog contains several input fields: a "Name" field with a red circle containing the number 7; "Username" and "Password" fields with a red circle containing the number 7; and an "Add node ID / subnet" field with a red circle containing the number 7. Below the "Add node ID / subnet" field is a link that says "Select nodes from list". At the bottom right of the dialog are "Save" and "Cancel" buttons, with a red circle containing the number 8 over the "Save" button.

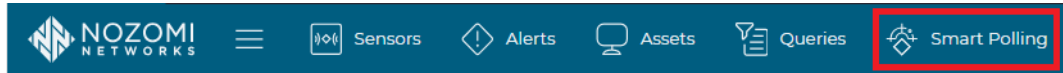
9. Click on the **New plan** button to save the new plan.



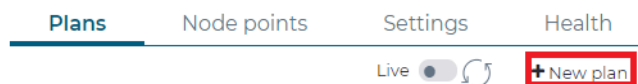
## Configure the WinRM smart polling plan

The WinRM smart polling plan extracts information using the WinRM service. This lets you gather information from devices running Windows Server 2016 and later, or Windows 10 and later, where WinRM has been enabled.

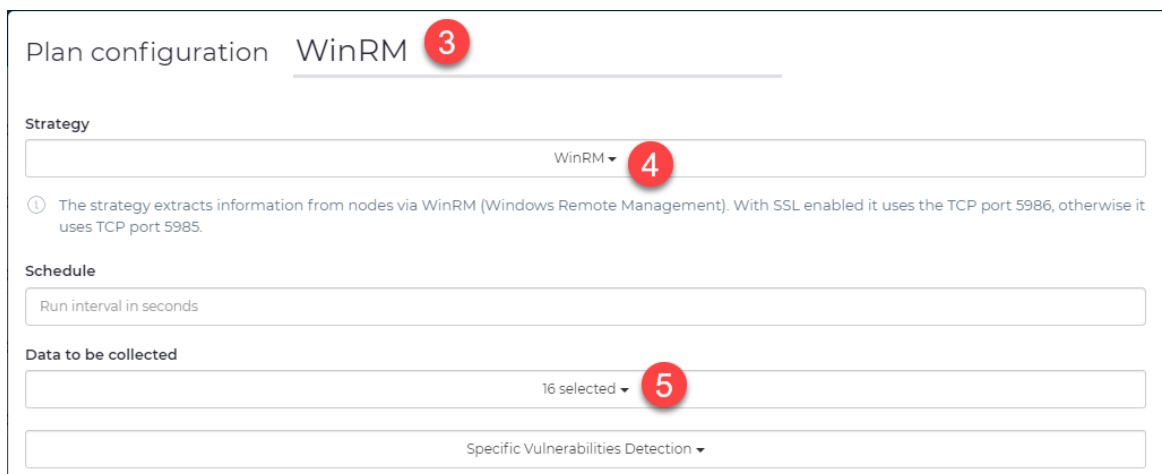
1. On the Nozomi Guardian main page, click on the **Smart Polling** tab.



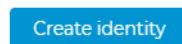
2. On the **Smart Polling** page, click on **+New plan**.



3. On the **Plan configuration** page, enter a name for the new plan (WinRM is a good identifier).
4. From the **Strategy** dropdown, select **WinRM**.
5. From the **Data to be collected** dropdown, select **All**.

A screenshot of the 'Plan configuration' page for a 'WinRM' plan. The page has a title 'Plan configuration WinRM' with a red circle containing the number '3' next to 'WinRM'. Below the title are several sections: 'Strategy' with a dropdown menu set to 'WinRM' (marked with a red circle '4'); a note below the dropdown stating 'The strategy extracts information from nodes via WinRM (Windows Remote Management). With SSL enabled it uses the TCP port 5986, otherwise it uses TCP port 5985.'; 'Schedule' with a text input field for 'Run interval in seconds'; 'Data to be collected' with a dropdown menu set to '16 selected' (marked with a red circle '5'); and a final dropdown menu set to 'Specific Vulnerabilities Detection'.

6. Click on the **Create identity** button.



7. In the **Add identity** dialog, enter the following information:
  - **Name:** A name for the identity you are creating.
  - **Username** and **Password:** The credentials used for the WinRM connection.
  - **Add node ID / subnet:** A list of the devices and subnets that Nozomi Guardian will attempt to create an WinRM connection to.
8. Click on the **Save** button to save the new identity.

Add identity for 'Smart Polling/Arc: WinRM'

**Name** 7  
WinRM

**Username** 7      **Password**  
Username      Password

**Applicability**  
No node IDs or subnets added

**Add node ID / subnet** 7  
e.g. 192.168.1.0/24 +

[Select nodes from list](#)

8  
Save      Cancel

9. Click on the **New plan** button to save the new plan.

New plan      Cancel

# Using the Nozomi plugin

Once you have installed and configured the Nozomi Guardian sensor, it will begin polling your network for information. It may take up to ten minutes for polling to begin.

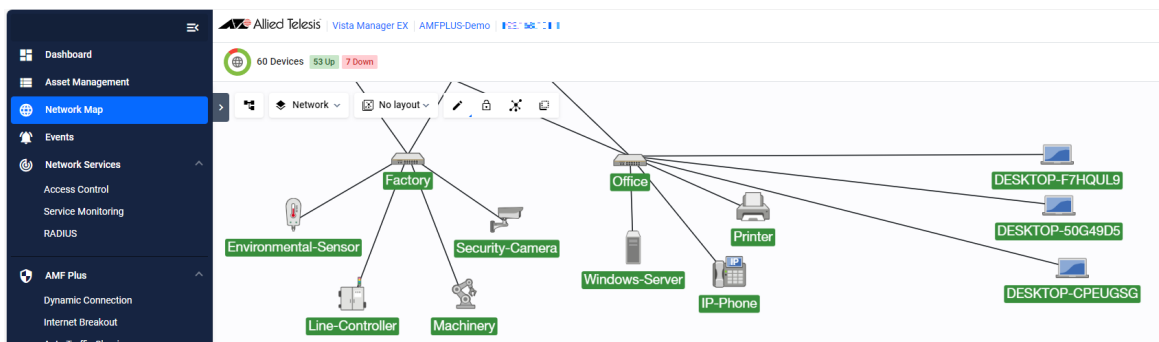
Once you have registered the Nozomi plugin in Vista Manager, Vista Manager begins polling the Nozomi Guardian sensor. Polling information in Vista Manager is refreshed every five minutes.

## Vista Manager Network Map

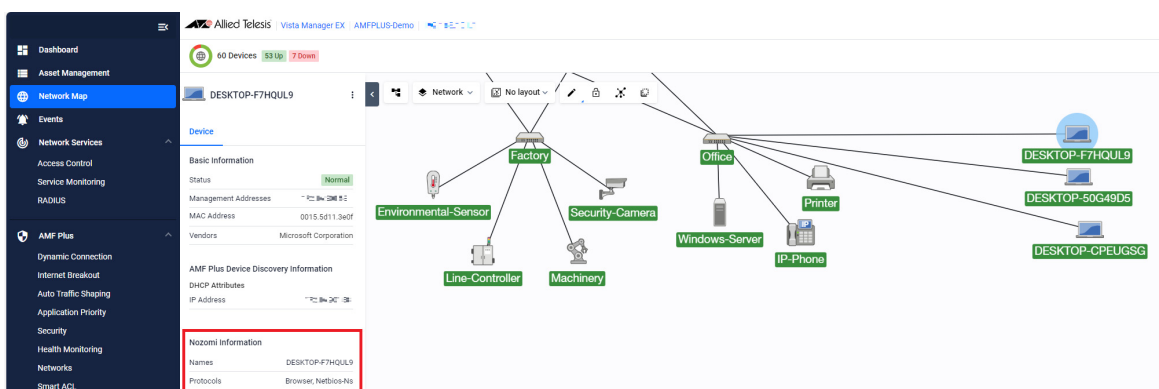
You can view detected devices on the **Network Map** screen. Nozomi will discover and classify these devices, and assign them an appropriate icon.

**Note:** Once a device has been discovered by Nozomi, it will remain on the network map until manually removed. While they are shown on the network map, they will be shown with a green status, regardless of the actual current state.

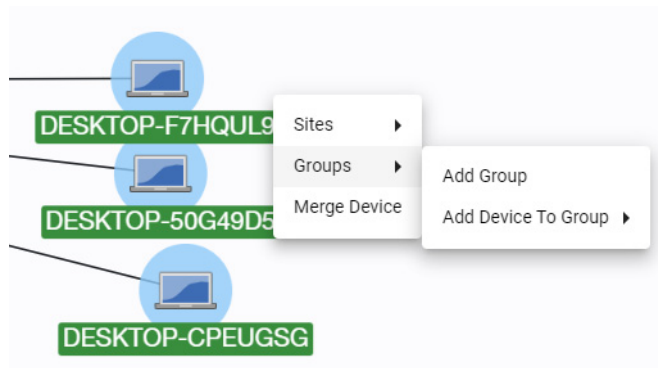
If the device is no longer present, you can remove it from the node details side panel or the Asset Management screen.



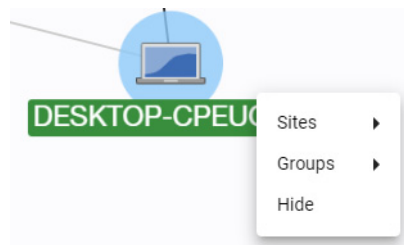
If you click on a device, you can see the information gathered by Nozomi in the side panel.



You can select multiple devices and create a group for them. Select the devices, right click, and select **Groups > Add Group**.



You can also hide discovered devices from the map. From the **Select Map Layer** drop-down, select **Edit**. Right click on the device you want to hide, and select **Hide**.



## Vista Manager Asset Management

You can manage discovered devices from the **Asset Management** screen. In the **Devices** tab, you can see devices discovered by Nozomi.

### Asset Management

Devices (175) Groups (4) Provision (0) Endpoints Firmware Report

All Groups Search by keyword

Discovery Source: Nozomi

Device Name	IP Addresses	Status	Device Type	MAC Addresses	Licens...	Discovery Source
ws-c3750x-24		Normal	-			Nozomi
WINSERVERDC	10.39.150.1	Normal	-	000C:29:8E:8E:8E:8E		Nozomi
WIN10PC01	10.39.150.2	Normal	-	000C:29:8E:8E:8E:8E		Nozomi
WIN-NJ9K01Q3I8G	10.39.150.3	Normal	-	000C:29:8E:8E:8E:8E		Nozomi

You can also create groups for the discovered devices. Click on the **Groups** tab, and then click **+Add Group**. You can then add devices to the group, as well as specify a group name. If you want to change the icons for the devices in the group, you can select a custom icon for them. When you have finished, click the **Save** button to create the group.

**Add Group**

Name  
Desktops

IP Range Start:  
E.g. '192.168.1.1'

IP Range End:  
E.g. '192.168.1.1'

Vendor  
Search Vendors

Add MAC Address  
E.g. '0000.\*\*\*\*.\*\*\*\*' + Upload File

Device Family

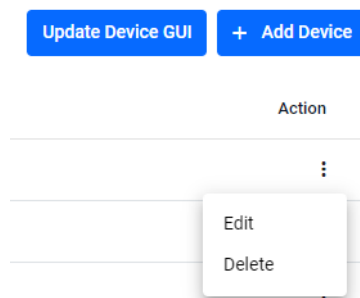
Device Search  
Search Devices

Static Devices  
DESKTOP-50G49D5 × DESKTOP-CPEUGSG ×  
DESKTOP-F7HQUL9 ×

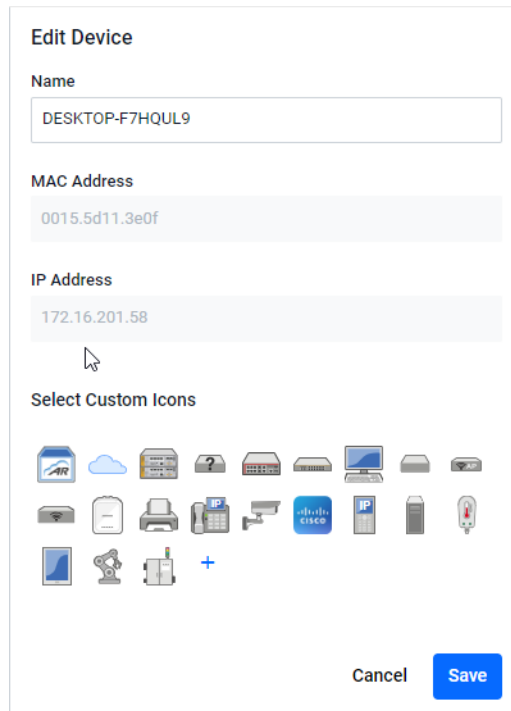
Select Custom Icons  
Printer, Fax, Scanner, Cisco, IP, Mobile Phone, Lightbulb, Tablet, Microscope, Server, +

Cancel Save

You can also change the icons for the discovered devices. From the **Devices** tab, click on the ellipsis for the device, and select **Edit**.



You can then change the custom icon for the device.

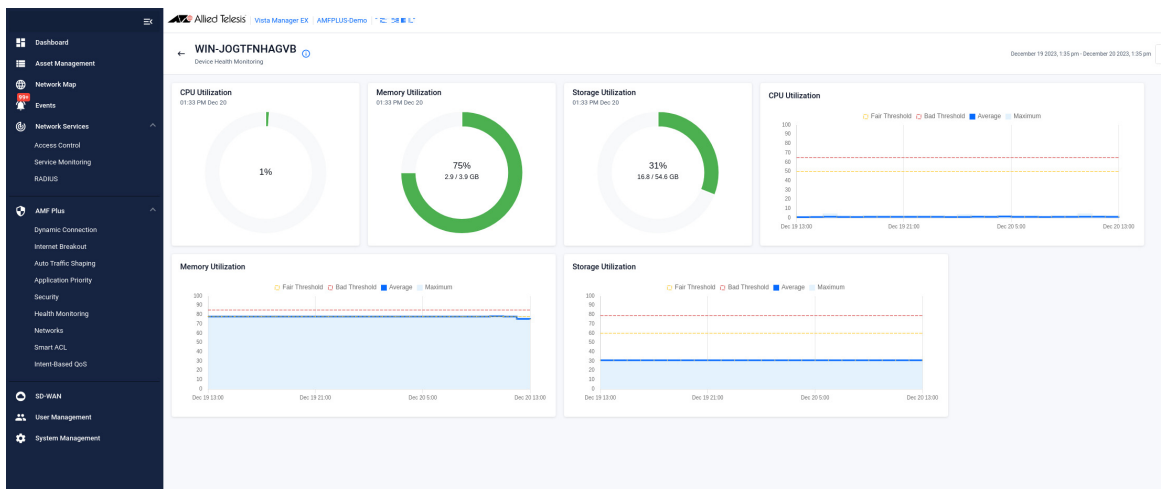


You can also change all the icons for a group in the same way. From the **Groups** tab, click on the ellipsis for the group, and select **Edit**. You can then change the custom icons for the devices in the group.

## Vista Manager Health Monitoring

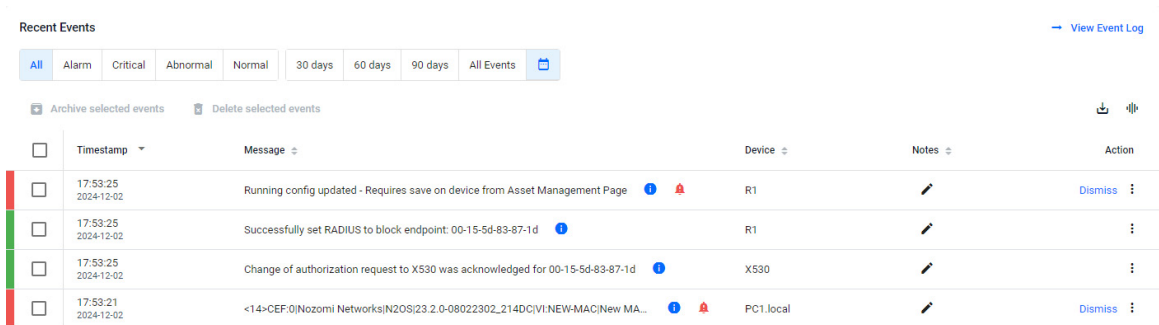
Nozomi can also provide health monitoring information. This information is gathered from these devices by Nozomi smart polling.

In Vista Manager, select **Health Monitoring**. When you click on a device discovered by Nozomi, you will be able to view information including CPU usage, memory usage, and disk usage.



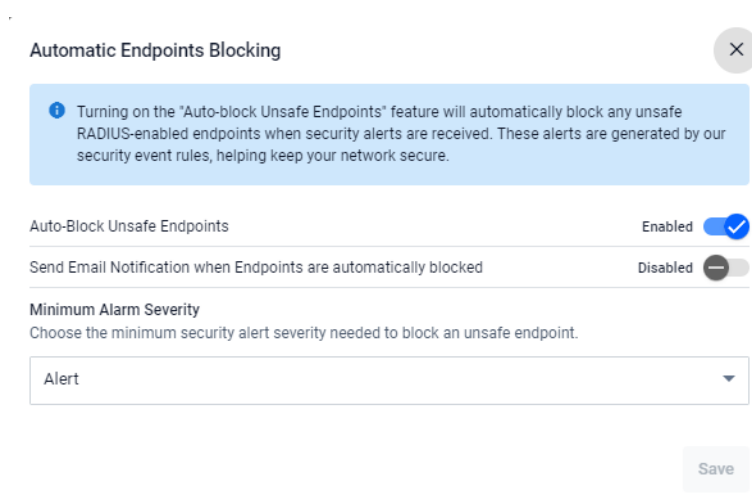
## Nozomi alerts and device blocking

From Vista Manager 3.13.1, you can view Nozomi alerts in the Vista Manager event logs.



	Timestamp	Message	Device	Notes	Action
<input type="checkbox"/>	17:53:25 2024-12-02	Running config updated - Requires save on device from Asset Management Page	R1		Dismiss
<input type="checkbox"/>	17:53:25 2024-12-02	Successfully set RADIUS to block endpoint: 00-15-5d-83-87-1d	R1		
<input type="checkbox"/>	17:53:25 2024-12-02	Change of authorization request to X530 was acknowledged for 00-15-5d-83-87-1d	X530		
<input type="checkbox"/>	17:53:21 2024-12-02	<14>CEF:0 Nozomi Networks N2OS 23.2.0-08022302_214DC VI:NEW-MAC New MA...	PC1.local		Dismiss

In addition, you can configure Vista Manager to automatically block devices discovered by Nozomi based on security severity levels. Once automatic blocking is enabled, you can choose the severity level that triggers the automatic blocking. You can also configure an email notification when an endpoint has been blocked.



**Automatic Endpoints Blocking**

Turning on the "Auto-block Unsafe Endpoints" feature will automatically block any unsafe RADIUS-enabled endpoints when security alerts are received. These alerts are generated by our security event rules, helping keep your network secure.

Auto-Block Unsafe Endpoints **Enabled**

Send Email Notification when Endpoints are automatically blocked **Disabled**

**Minimum Alarm Severity**  
Choose the minimum security alert severity needed to block an unsafe endpoint.

Alert

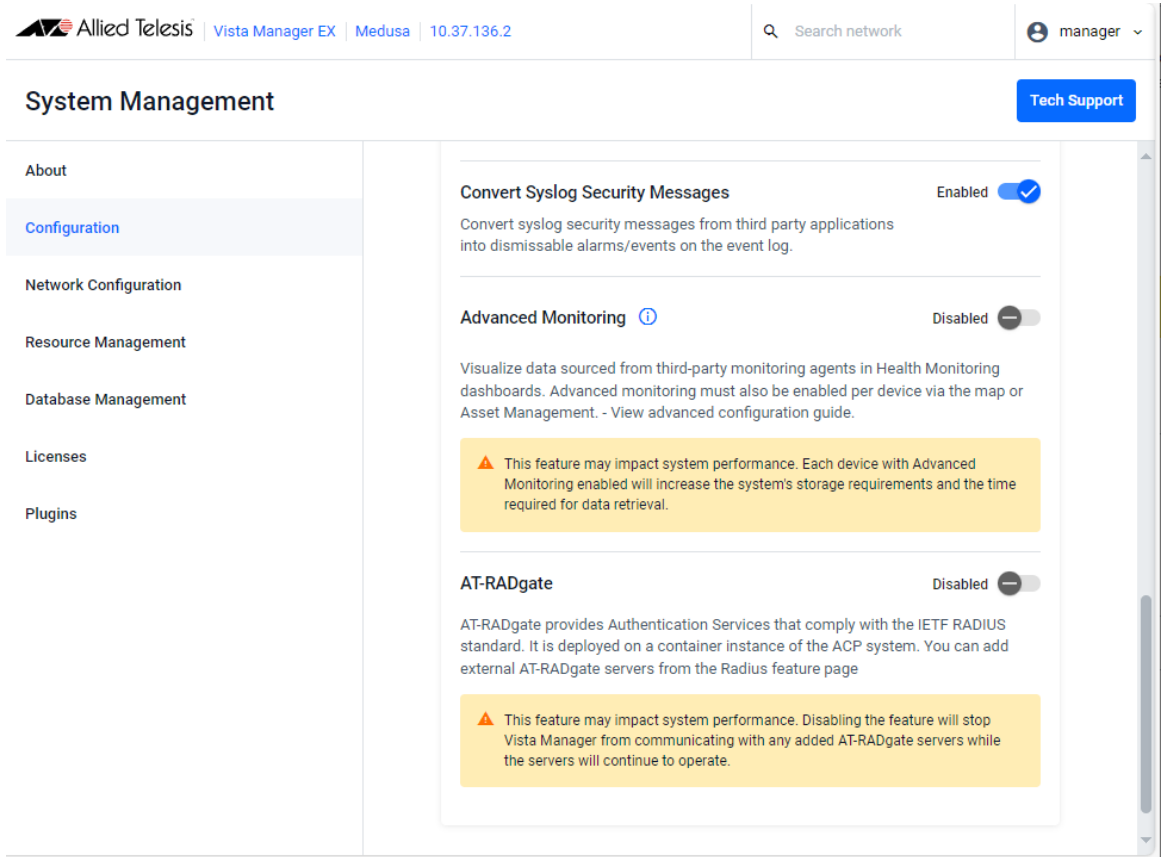
Save

There are four types of Nozomi alerts:

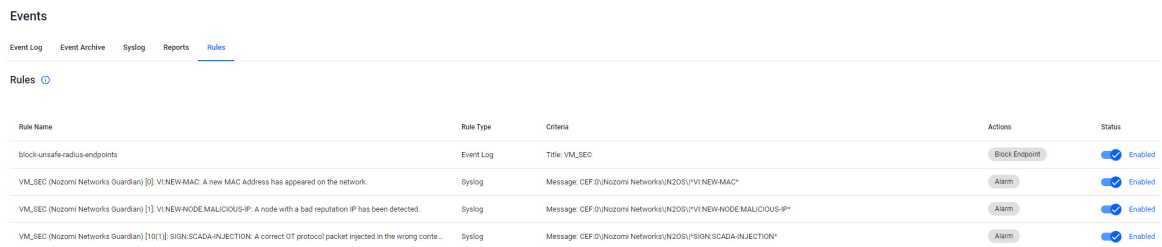
- **Protocol validations** - This alert detects undesired protocol behaviour. For example, process time issue and DHCP operation.
- **Virtual image** - This alert detects deviations from expected network behaviours. For example, variable flow anomaly and new ARP.
- **Built-in checks** - This alert detects specific signatures known to ICS threats provided by Threat Intelligence.
- **Custom checks** - This alert detects check set in place by the user. For example, not allowed variable quality and critical state on.

**Note:** This functionality requires that both the Nozomi plug-in and RADIUS are configured and running.

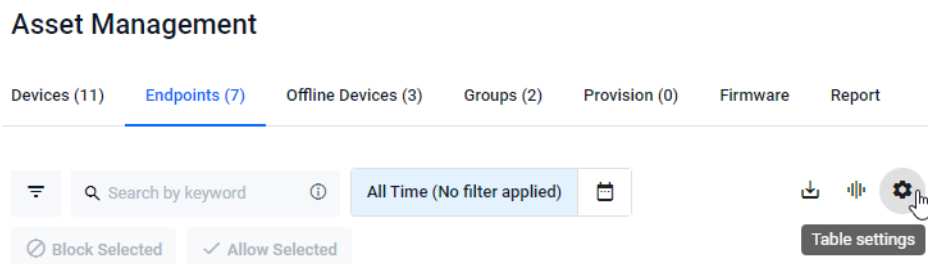
To enable this feature, in the **System Management > Configuration** screen, set the **Convert Syslog Security Messages** tick button to **Enabled**.



Once you have enabled this feature, a number of rules will be added on the **Events > Rules** screen. You can enable or disable individual rules on this screen. By default, they are all **Enabled**.



Once enabled, you can configure automatic blocking by going to the **Asset Management > Endpoints** screen and clicking on the **Table settings** button.



From this window, you can turn automatic blocking on or off, as well as the minimum severity level to trigger blocking. You can also configure whether to send an email when an endpoint has been blocked.

**Automatic Endpoints Blocking** ✕

**?** Turning on the "Auto-block Unsafe Endpoints" feature will automatically block any unsafe RADIUS-enabled endpoints when security alerts are received. These alerts are generated by our security event rules, helping keep your network secure.

Auto-Block Unsafe Endpoints Enabled

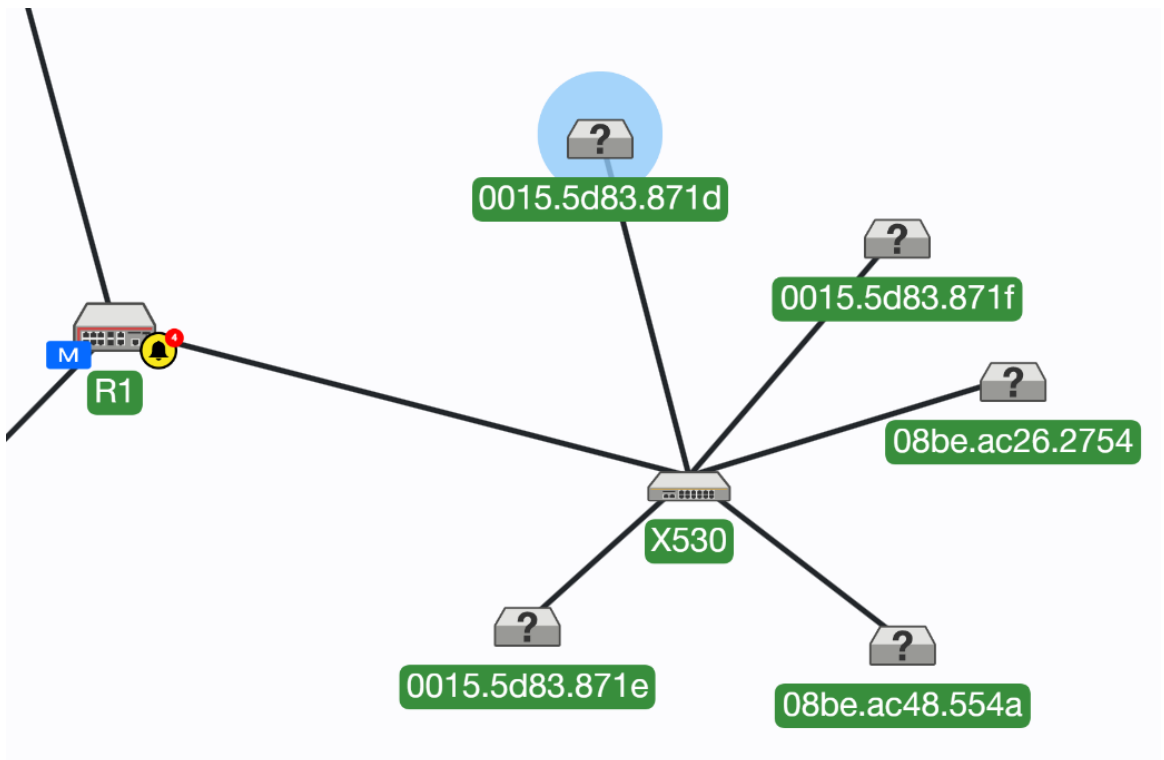
Send Email Notification when Endpoints are automatically blocked Disabled

**Minimum Alarm Severity**  
Choose the minimum security alert severity needed to block an unsafe endpoint.

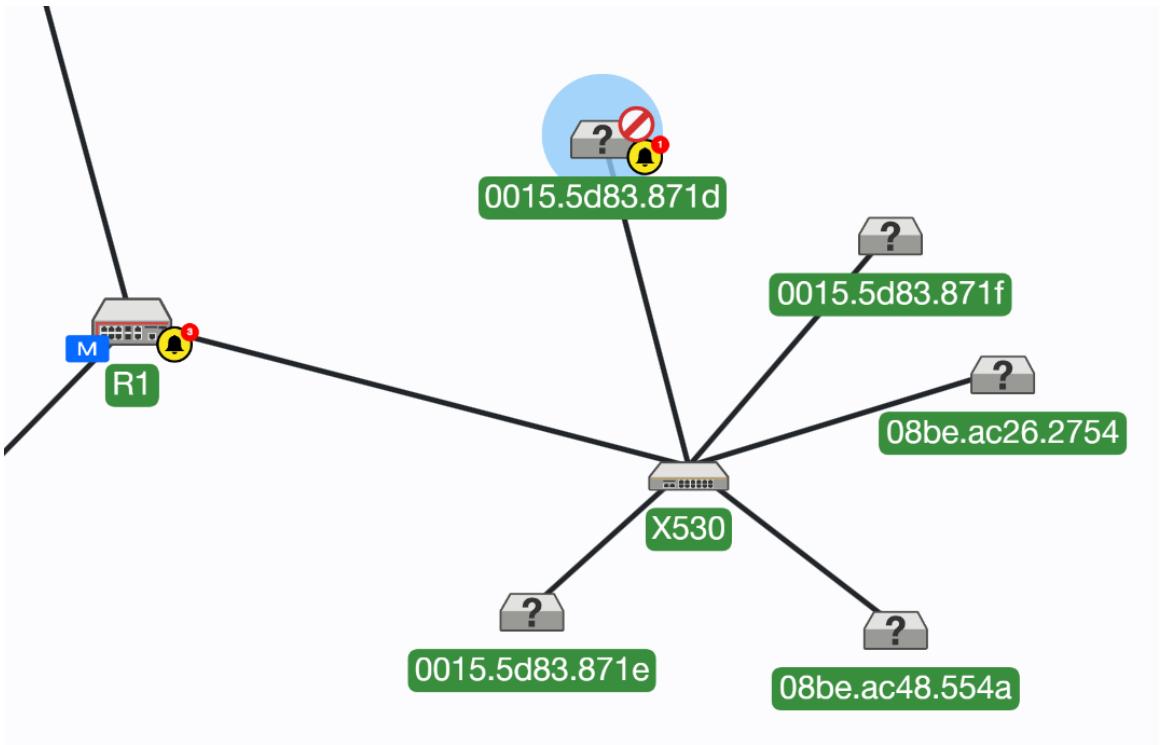
Alert ▾

Save

In the image below, we can see a number of endpoints connected to a device in the Network Map.



When an event is detected by Nozomi, following the configured rules, it automatically blocks the device and generates an alert.



You can also see that the device has been blocked in the Asset Management screen.

<input type="checkbox"/>	MAC Address	Hostname	Status	Authentication	Last Interaction Time	RADIUS Username	NAS Hostname	NAS Interface	Alarms
<input type="checkbox"/>	08be.ac48.554a	08be.ac48.554a	Allowed	Authenticated		08-be-ac-48-55-4a	X530	port1.0.16	0
<input type="checkbox"/>	08be.ac26.2754	08be.ac26.2754	Allowed	Authenticated		08-be-ac-26-27-54	X530	port1.0.2	0
<input type="checkbox"/>	0015.5d83.871f	0015.5d83.871f	Allowed	Authenticated		00-15-5d-83-87-1f	X530	port1.0.16	0
<input type="checkbox"/>	0015.5d83.871e	0015.5d83.871e	Allowed	Authenticated		00-15-5d-83-87-1e	X530	port1.0.16	0
<input type="checkbox"/>	0015.5d83.871d	0015.5d83.871d	Blocked			00-15-5d-83-87-1d	X530	port1.0.16	1

You can choose to allow a device to rejoin the network from the Asset Management screen by selecting **Allow device**.

The screenshot shows a table with columns for MAC Address, Hostname, Status, Last Interaction Time, RADIUS Username, NAS Hostname, NAS Interface, and Alarms. The device with MAC address 0015.5d... is shown with a 'Blocked' status. A dropdown menu is open over the device, showing options 'Block device' and 'Allow device'. The 'Allow device' option is highlighted by the mouse cursor.

## Removing the Nozomi plugin

If you want to remove all the devices and information discovered by Nozomi, you can unregister the plugin. Go to the **System Management** screen, and click on the **Plugins** tab. Select **Nozomi** and click on **Delete Plug-in** to unregister it.

The screenshot shows the 'System Management' interface with a sidebar menu on the left containing: About, Configuration, Network Configuration, Resource Management, Database Management, Licenses, and Plugins (highlighted). The main content area is titled 'Plugins' and contains two sections. The first section, 'Vista Manager's Certificate Fingerprints', lists SHA1 and SHA256 hashes. The second section, 'Plugins', is a table with the following data:

Plugin Name	Actions	SHA1	SHA256
Nozomi	<a href="#">Delete Plug-in</a> <a href="#">Edit</a>		
Forescout Plugin		E5705E 848004 C840A9E017 7E64 9A0B1E3DE7C AF 5F	4E916C 0B00 87A81F45 06 8A2811A 000 007F0F704F5E0E8 1E0 03==7A5770C43E

C613-04165-00 REV D



NETWORK SMARTER

**North America Headquarters** | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895

**Asia-Pacific Headquarters** | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

**EMEA & CSA Operations** | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

[alliedtelesis.com](http://alliedtelesis.com)

© 2025 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.