Technical Guide

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:

- AMF Feature Overview and Configuration Guide
- AMF Introduction and videos

These documents are available from the links above or on our website at alliedtelesis.com

Contents

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

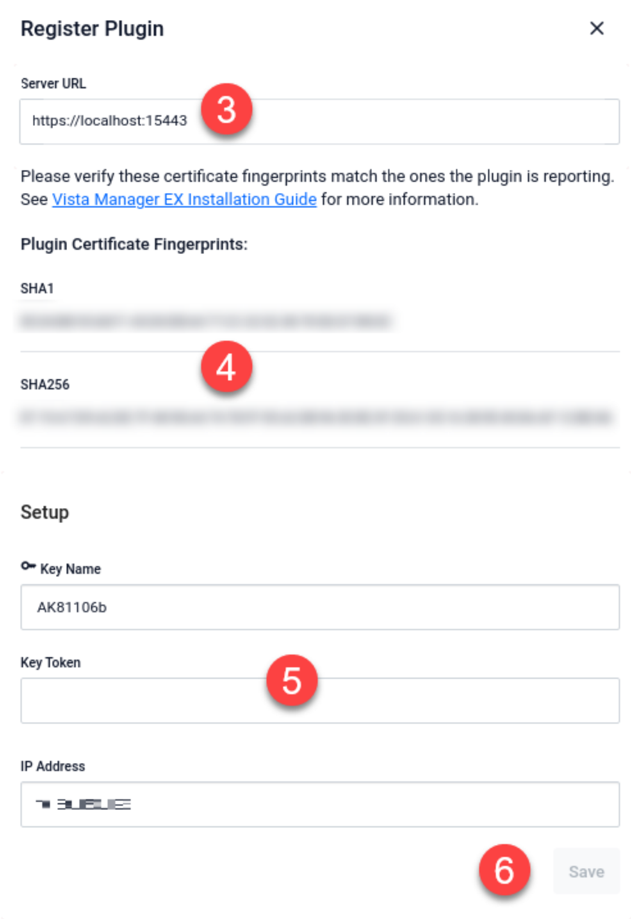
Nozomi Guardian uses OpenAPI keys to authenticate users. Using your OpenAPI key, you can generate a key token. This key token is used to create a secure connection between the Vista Manager and the Nozomi Guardian sensor. This key token is used in the “Register the Nozomi plugin with Vista Manager” section.

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 ×

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

SHA256

Setup

Key Name

AK81106b

Key Token

IP Address

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.

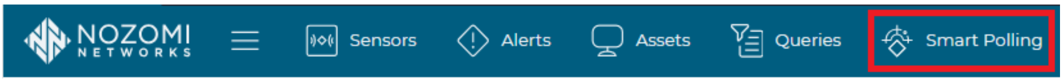
Nozomi Guardian offers a number of different smart polling methods. Below are examples of how to configure two of them for your network.

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.

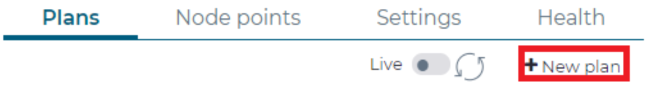
Configure the SSH smart polling plan

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

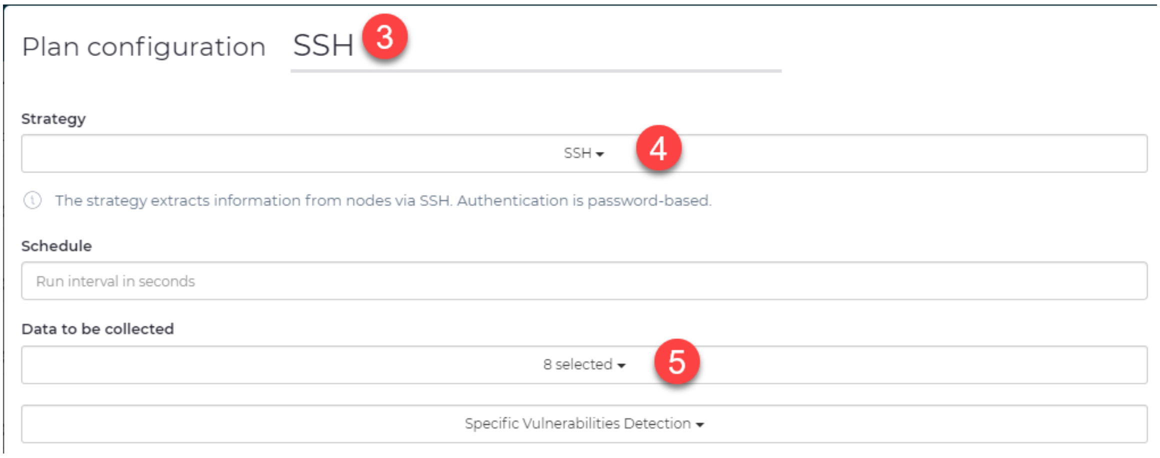
1. On the Nozomi Guardian main page, click on the **Smart Polling** tab.



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**.



Plan configuration SSH 3

Strategy

SSH ▾ 4

ⓘ The strategy extracts information from nodes via SSH. Authentication is password-based.

Schedule

Run interval in seconds

Data to be collected

8 selected ▾ 5

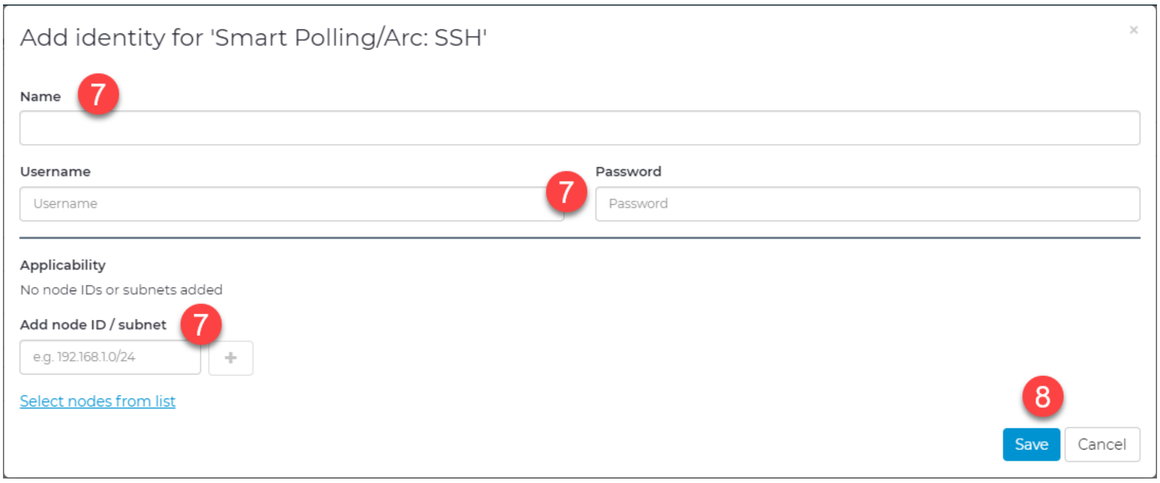
Specific Vulnerabilities Detection ▾

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.


Add identity for 'Smart Polling/Arc: SSH'

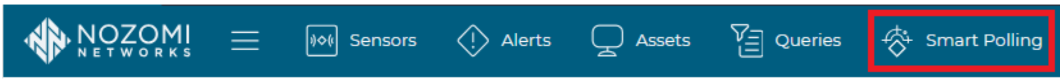
No node IDs or subnets added

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

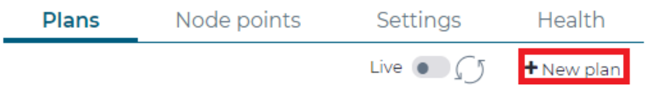
Configure the WinRM smart polling plan

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.

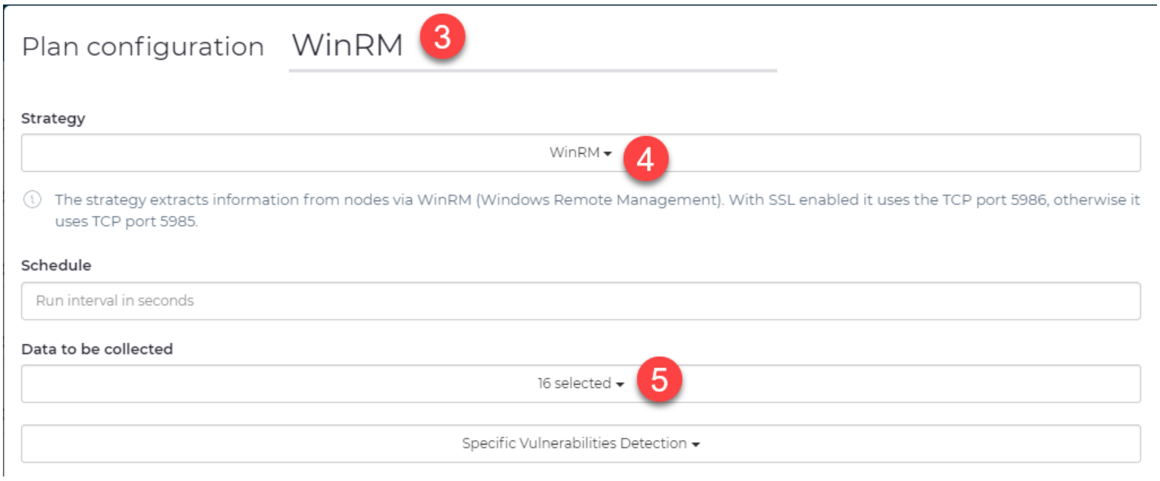
1. On the Nozomi Guardian main page, click on the **Smart Polling** tab.



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**.



Plan configuration WinRM

Strategy

WinRM

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

Run interval in seconds

Data to be collected

16 selected

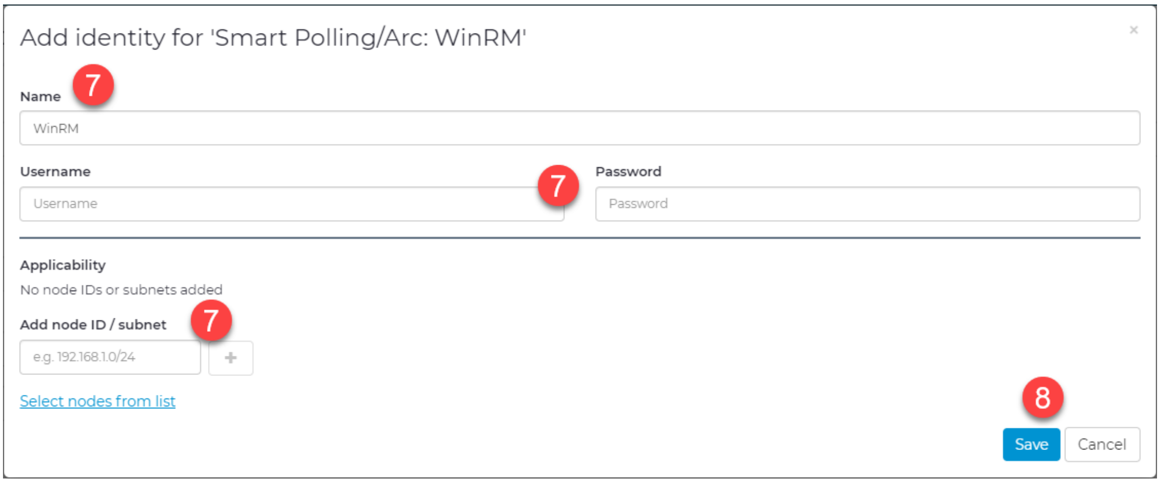
Specific Vulnerabilities Detection

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: WinRM

Username: Username

Password: Password

Applicability

No node IDs or subnets added

Add node ID / subnet: e.g. 192.168.1.0/24

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

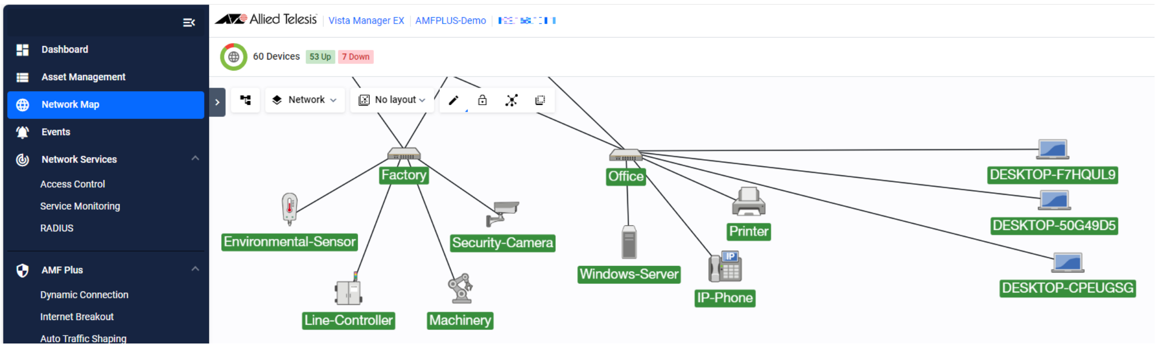
Using the Nozomi plugin

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.

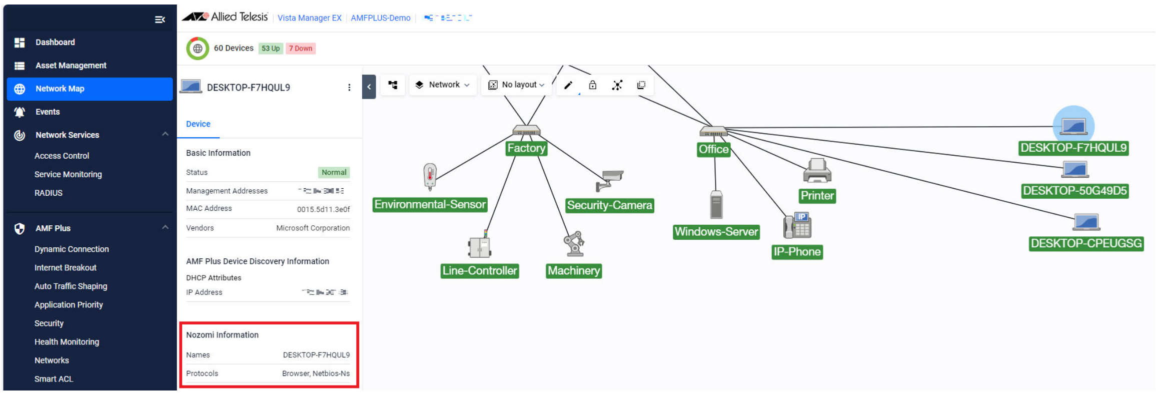
Once you have registered the Nozomi plugin in Vista Manager, Vista Manager begins polling the Nozomi Guardian sensor. Polling information in Vista Manager is refreshed every five minutes.

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.



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



DESKTOP-F7HQUL9

Device

Basic Information

Status: Normal

Management Addresses: [redacted]

MAC Address: 0015.5d11.3e0f

Vendors: Microsoft Corporation

AMF Plus Device Discovery Information

DHCP Attributes

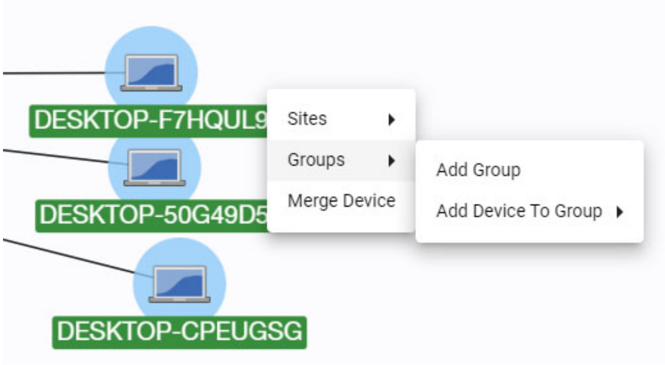
IP Address: [redacted]

Nozomi Information

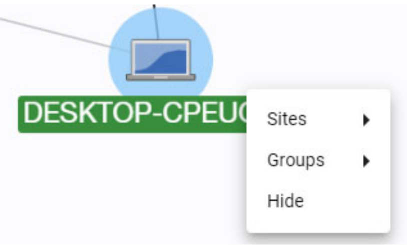
Names: DESKTOP-F7HQUL9

Protocols: Browser, Netbios-Ns

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

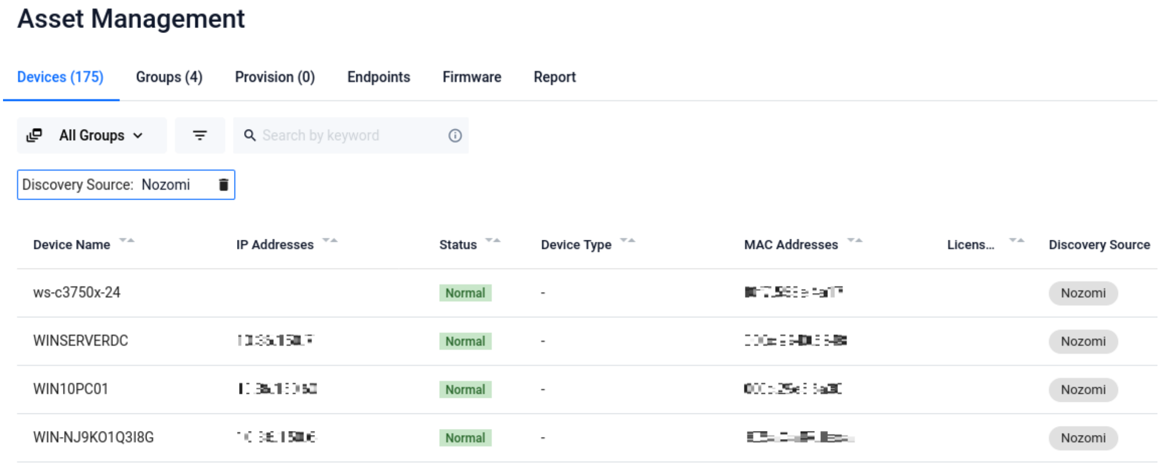


You can also hide discovered devices from the map. From the **Select Map Layer** drop-down, select **Edit**. Right click on the device you want to hide, and select **Hide**.



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

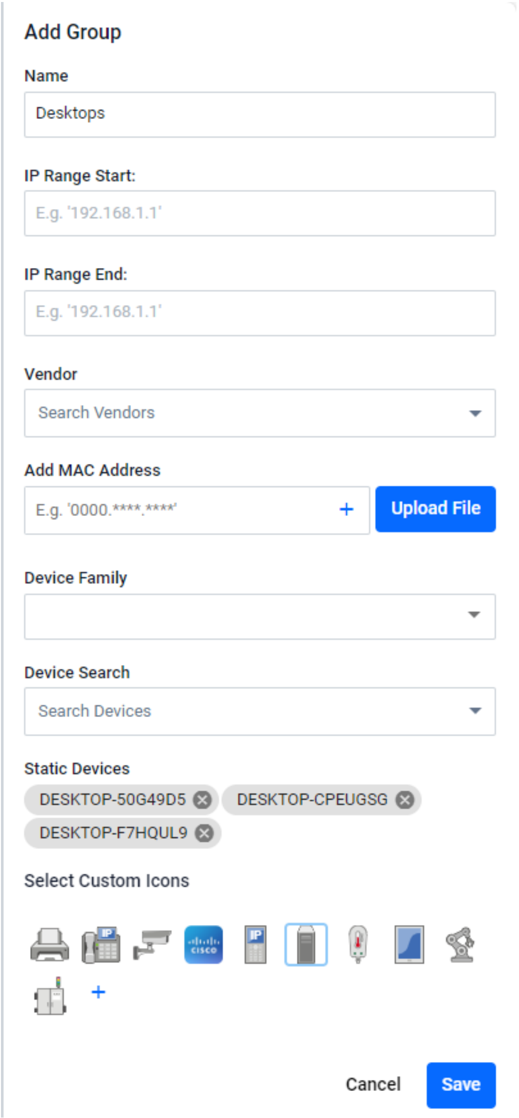
Devices (175) | Groups (4) | Provision (0) | Endpoints | Firmware | Report

All Groups | Search by keyword

Discovery Source: Nozomi

Device Name	IP Addresses	Status	Device Type	MAC Addresses	Licens...	Discovery Source
ws-c3750x-24		Normal	-	[redacted]		Nozomi
WINSERVERDC	[redacted]	Normal	-	[redacted]		Nozomi
WIN10PC01	[redacted]	Normal	-	[redacted]		Nozomi
WIN-NJ9KO1Q3I8G	[redacted]	Normal	-	[redacted]		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.****.****'

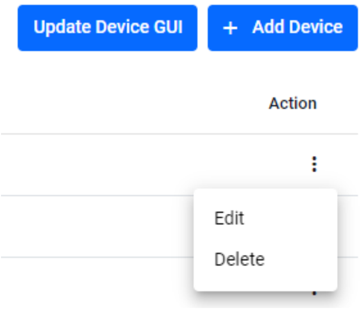
Device Family:

Device Search: Search Devices

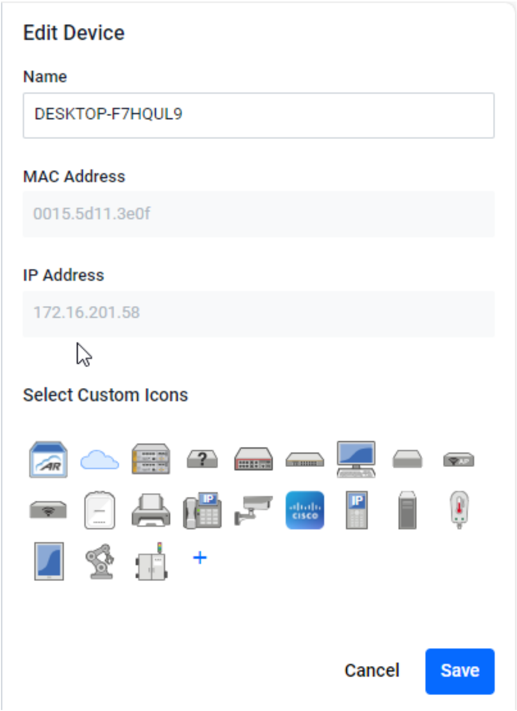
Static Devices: DESKTOP-50G49D5, DESKTOP-CPEUGSG, DESKTOP-F7HQUL9

Select Custom Icons

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.



Edit Device

Name: DESKTOP-F7HQUL9

MAC Address: 0015.5d11.3e0f

IP Address: 172.16.201.58

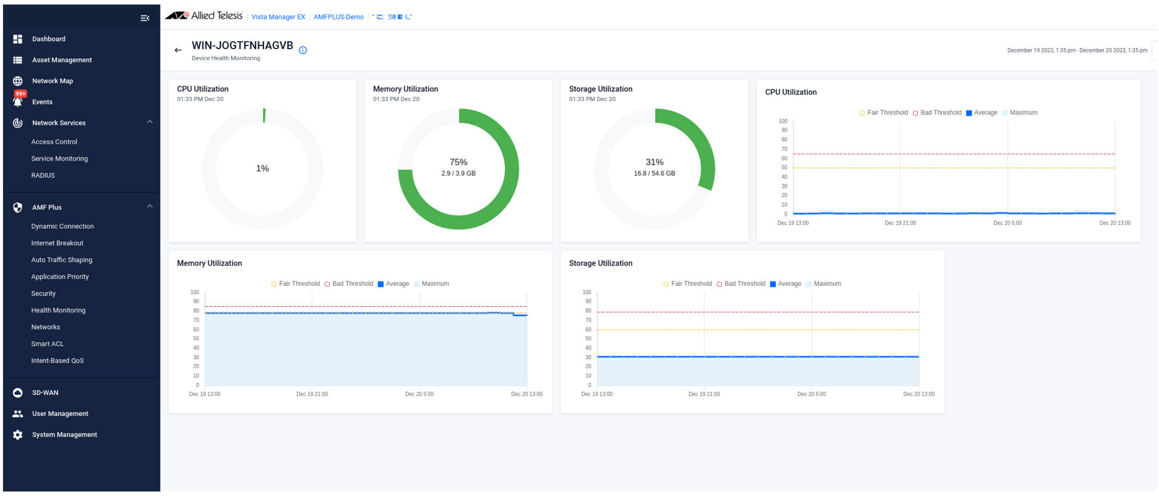
Select Custom Icons

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.



WIN-JOGTFNHAGVB
Device Health Monitoring

December 19 2023, 1:35 pm - December 20 2023, 1:35 pm

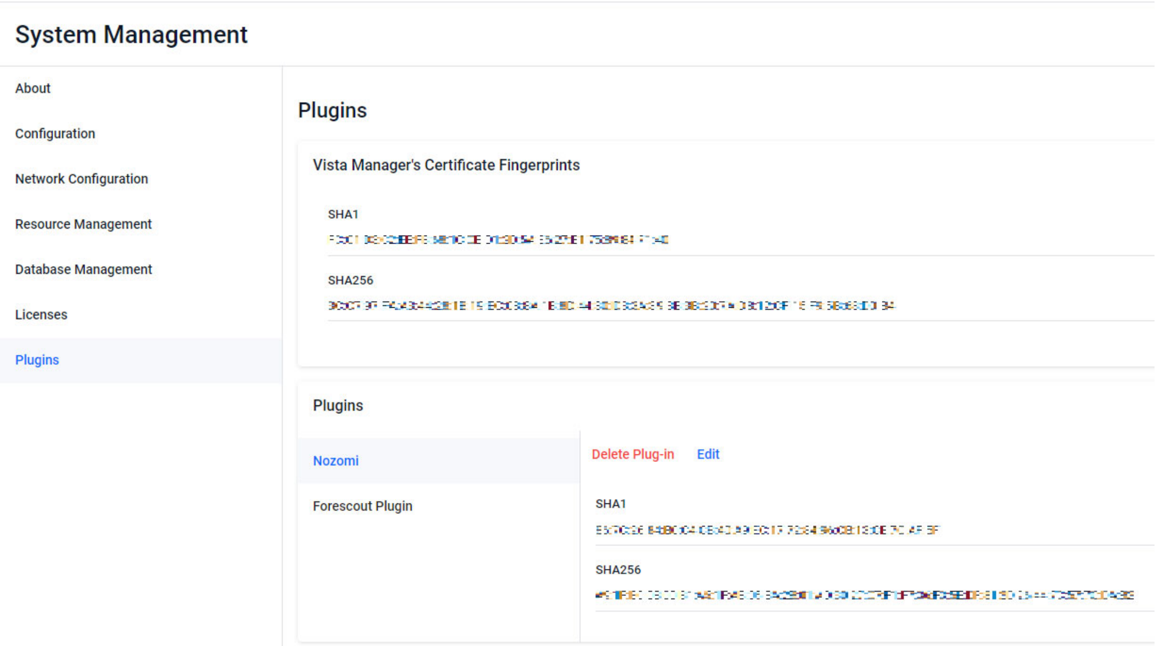
CPU Utilization
01:33 PM Dec 20
1%

Memory Utilization
01:33 PM Dec 20
75%
2.9 / 3.9 GB

Storage Utilization
01:33 PM Dec 20
31%
16.8 / 54.6 GB

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.



System Management

Plugins

Vista Manager's Certificate Fingerprints

SHA1
[illegible]

SHA256
[illegible]

Plugins

SHA1
[illegible]

SHA256
[illegible]