Integration Guide

Kaseya

Revised: 15 April 2016

About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration.

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Kaseya Integration Overview

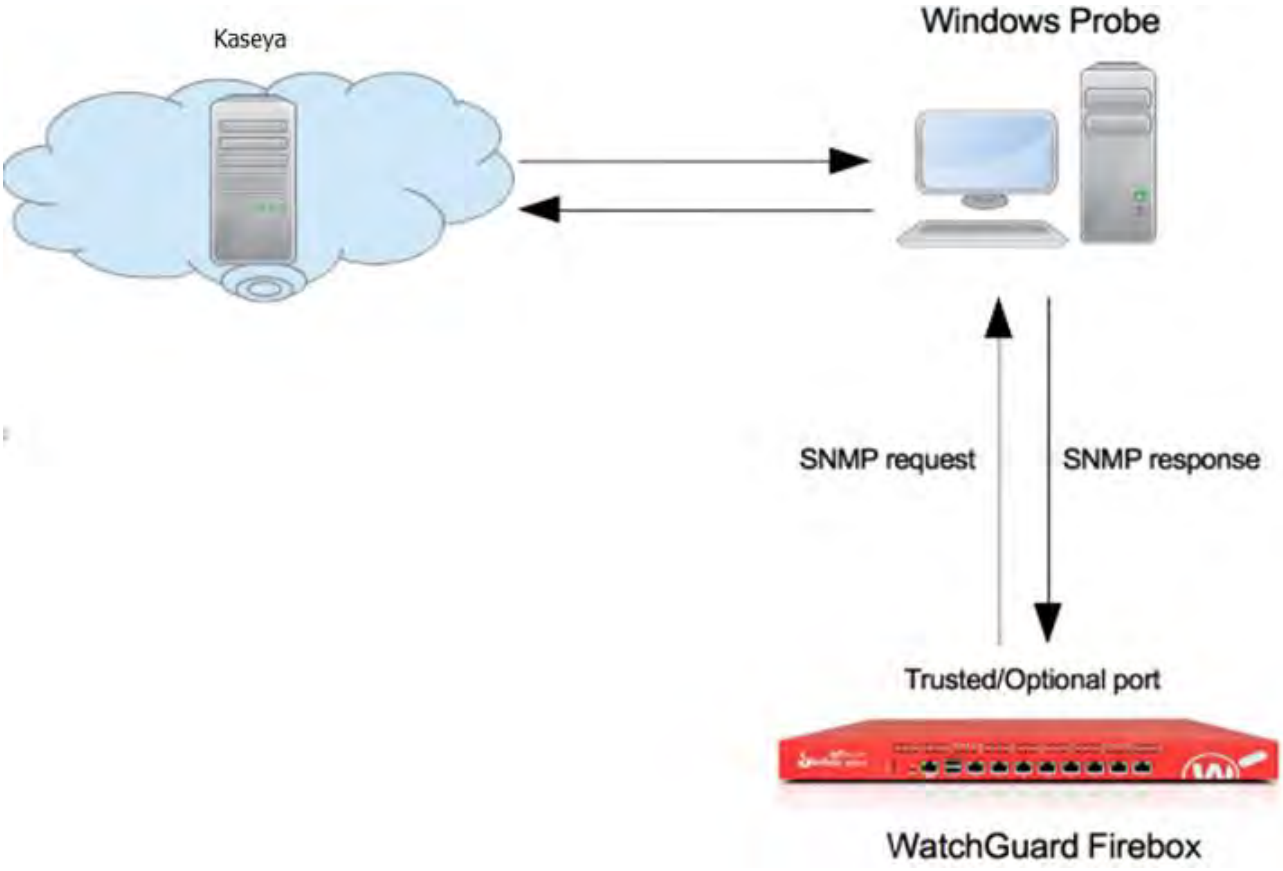
Kaseya is an RMM (Remote Monitoring and Management) tool used commonly among MSPs (Management Service Providers). RMM agents are installed on MSP customer endpoints to discover IT assets and remotely monitor/manage them. This document describes how to use Kaseya to discover and monitor a WatchGuard Firebox.

Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.x, with Interface 1 enabled as a trusted interface with the IP address 10.138.111.83. (You could also use an optional interface.)
- Kaseya version VSA R9.2 (web login).
- Probe IP address 10.138.111.2 installed in Windows Server 2012 Standard Edition.

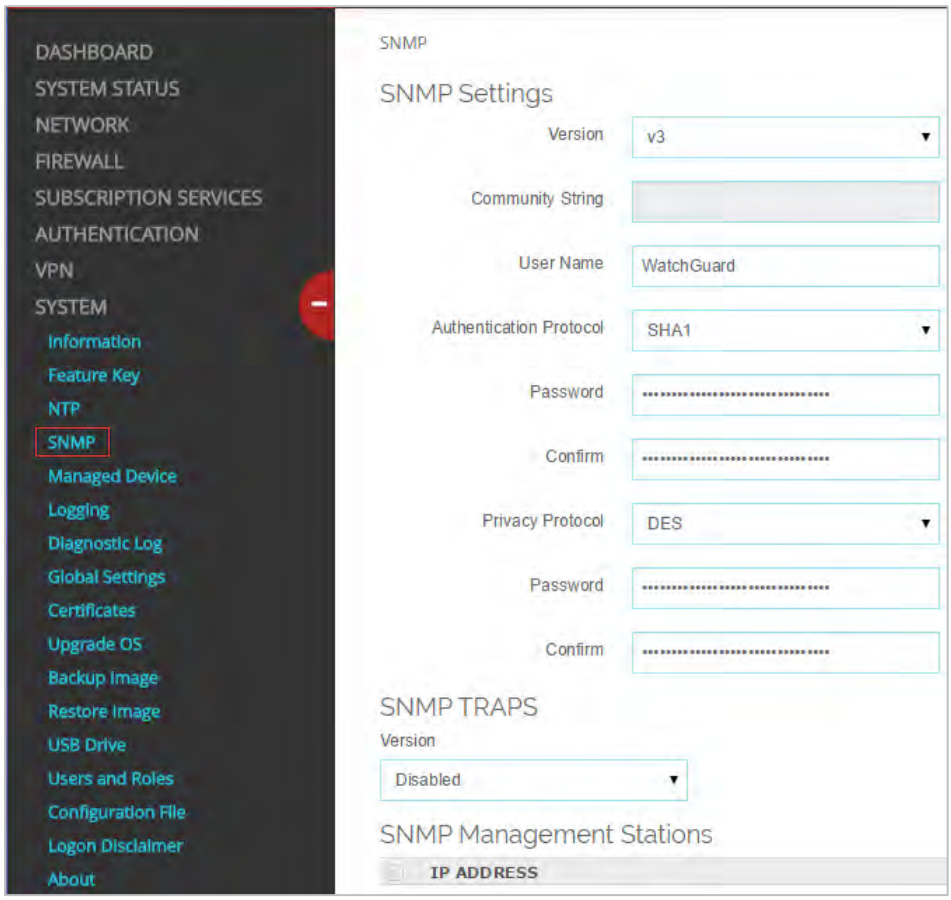
This diagram outlines the topology used in this integration:



Set Up the Firebox

You must configure the SNMP settings on the WatchGuard Firebox before you use Kaseya to discover it.

1. Use Fireware Web UI to connect to your Firebox.
2. Select **SYSTEM > SNMP**.

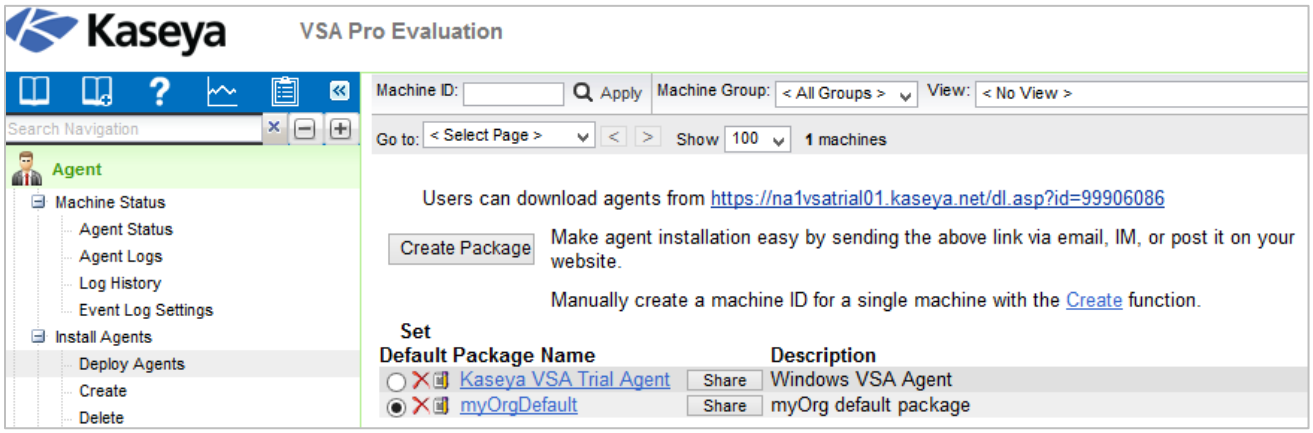


3. From the **Version** drop-down list, select **v3**.
4. From the **Authentication Protocol** drop-down list, select **SHA1**.
   In the adjacent **Password** and **Confirm** text boxes, type the authentication password.
5. From the **Privacy Protocol** drop-down list, select **DES**.
   In the adjacent **Password** and **Confirm** text boxes, type the encryption password.
6. In the **User Name** text box, type **WatchGuard**.
7. Click **Save**.
8. Select **FIREWALL > Firewall Policies**.
9. Add an SNMP packet filter policy for traffic from **Any-Trusted** to **Firebox**.
   If you connect to an optional interface, specify Any-Optional instead of Any-Trusted.

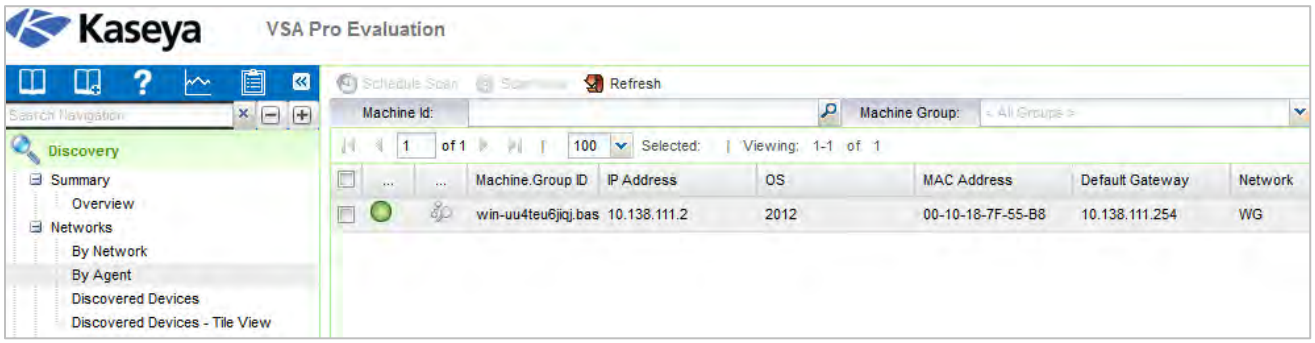
ORDER	ACTION	POLICY NAME	TYPE	FROM	TO	PORT
2	✓	SNMP	SNMP	Any-Trusted	Firebox	udp:161

Set Up Kaseya

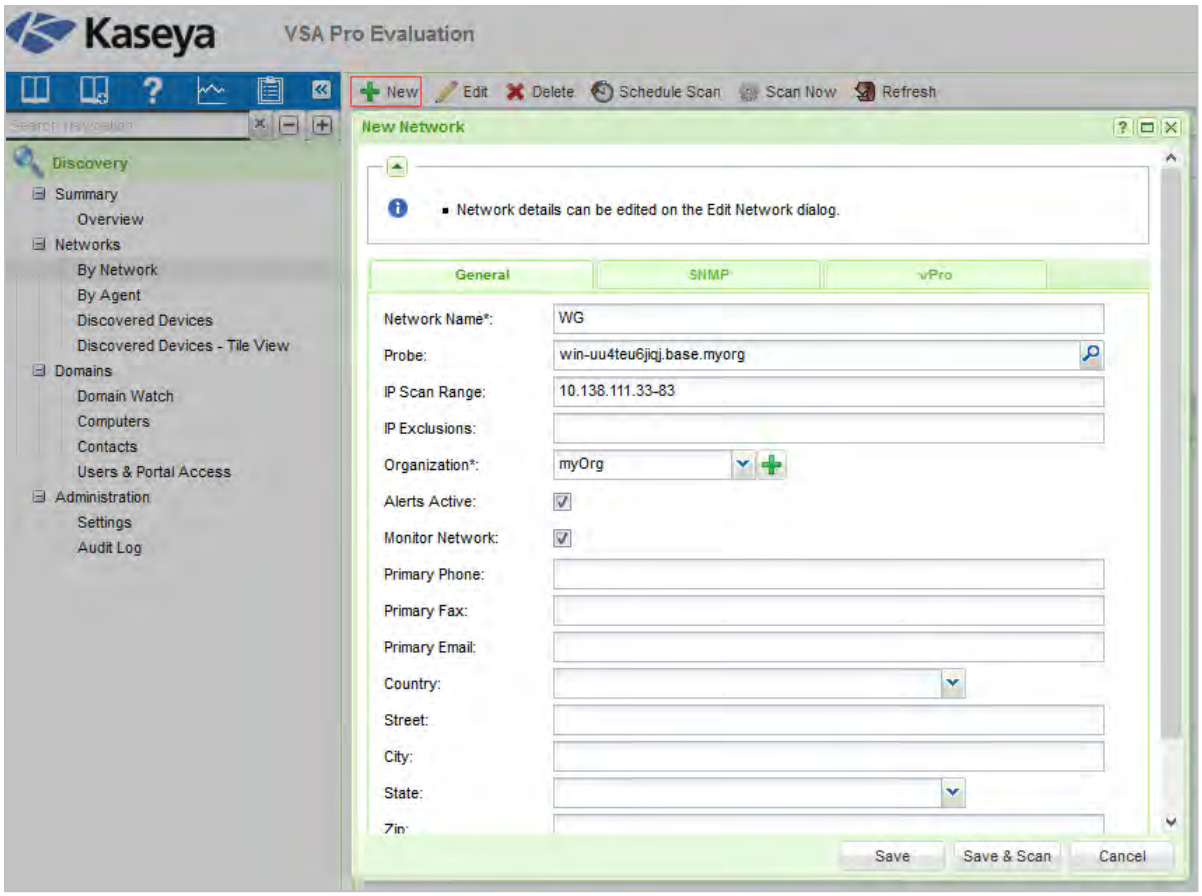
1. Log in to the Kaseya web page.
2. Download and install the Kaseya Agent on a probe computer. This computer must be in a LAN that connects to the WatchGuard Firebox.



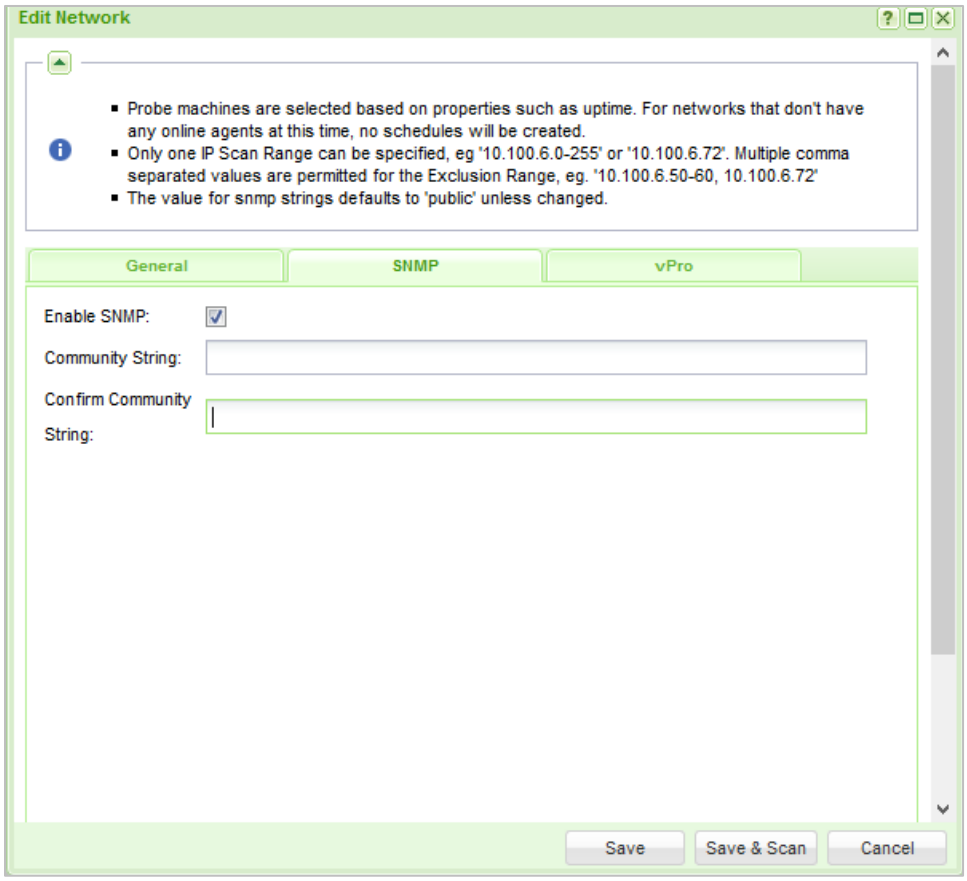
3. Go to the **Discovery** page. Probe the computer shown in **Networks > By Agent**.



4. Select **Discovery > Networks > By Networks**.
5. Click **New** to add a new network.



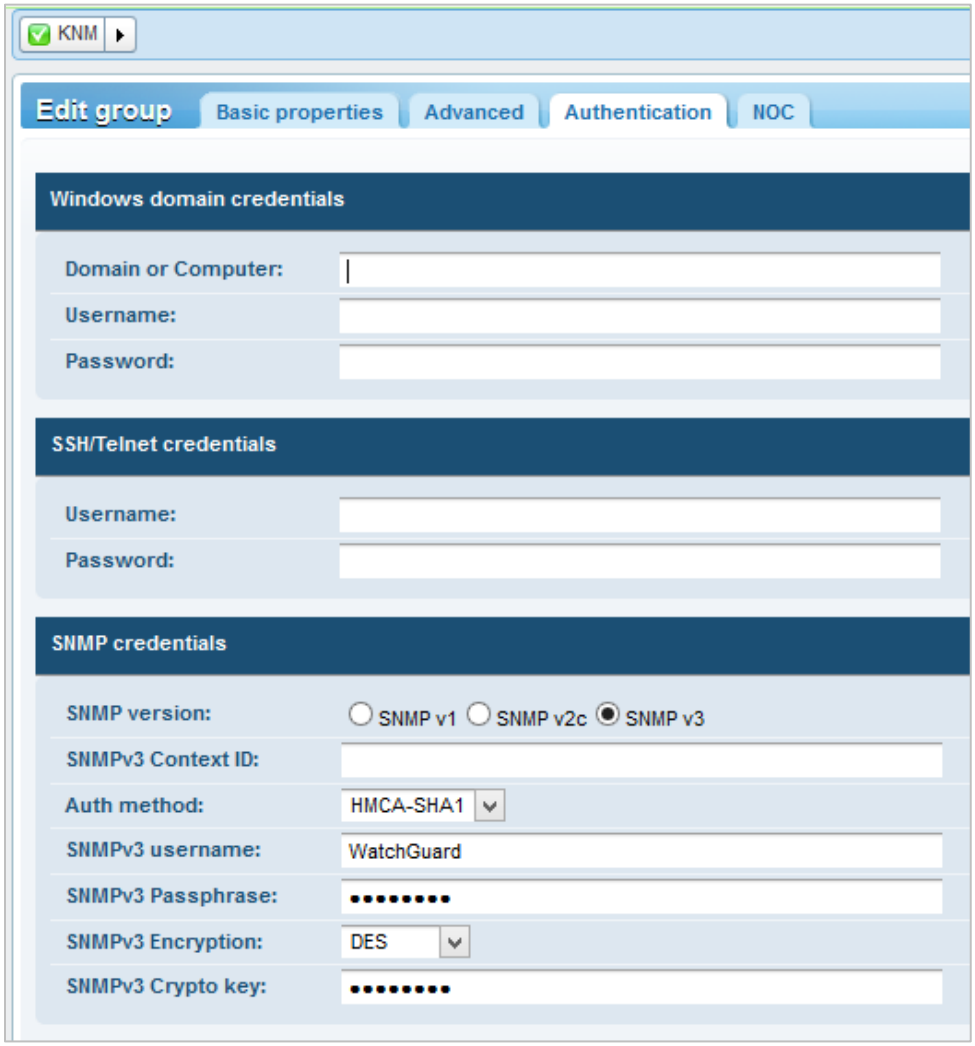
6. Select the **SNMP** tab.



7. Select the **Enable SNMP** check box.
8. Leave the **Community String** blank.
9. Click **Save**.
10. Type the gateway name in the popup window.
11. Select **Network Monitor > Monitoring > View > group (KNM) > Edit.**

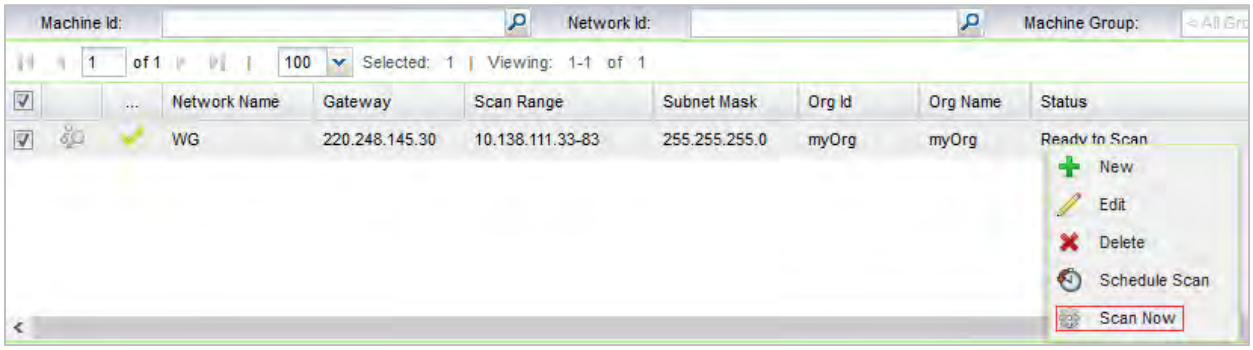
12. Select the **Authentication** tab.

13. Set the **SNMP version** to **SNMP v3**. Configure the same SNMP authentication method, encryption method, and credentials as you configured on the Firebox.

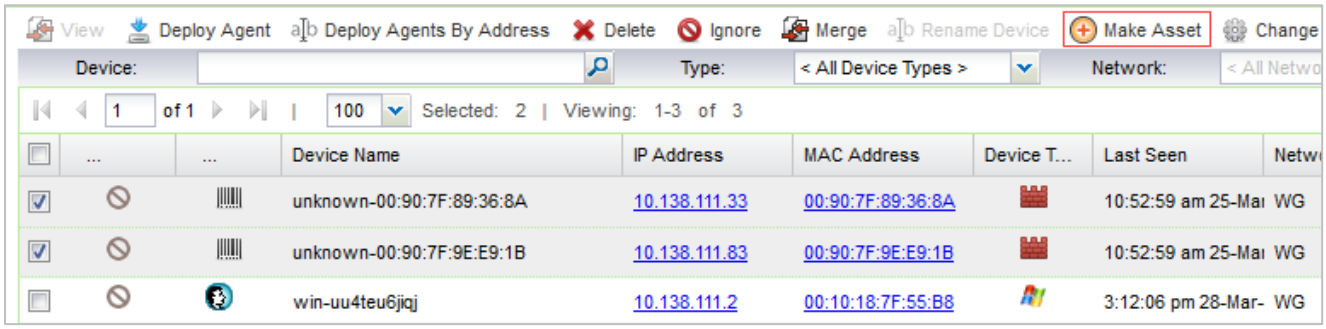


14. To trigger the scan, select **Discovery > Networks > By Networks > Scan Now**.

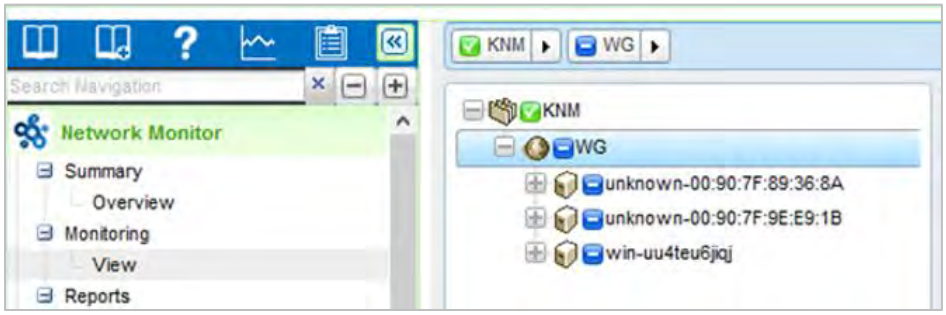
    While the network scan is in progress, click  to check process.



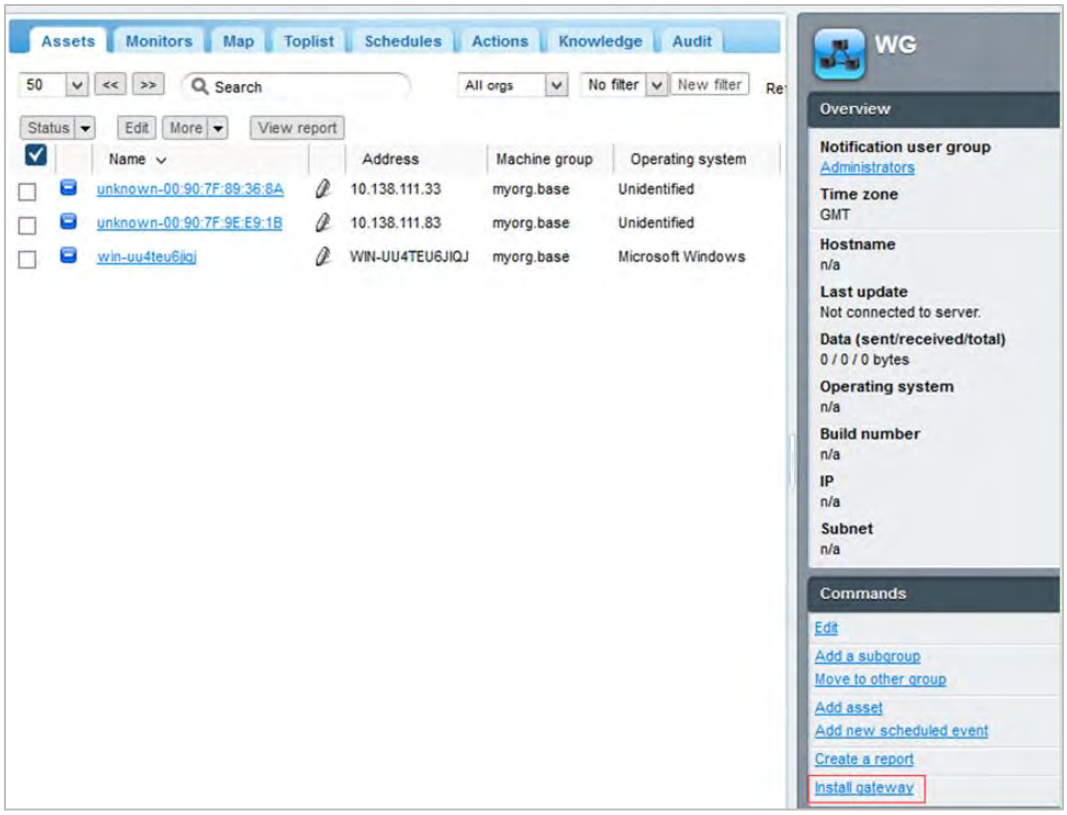
15. To see discovered devices, select **Discovery > Networks > Discovered Devices.** Make the target Firebox an Asset. In this example, two Fireboxes were discovered because two Fireboxes on this LAN were configured with SNMP enabled.



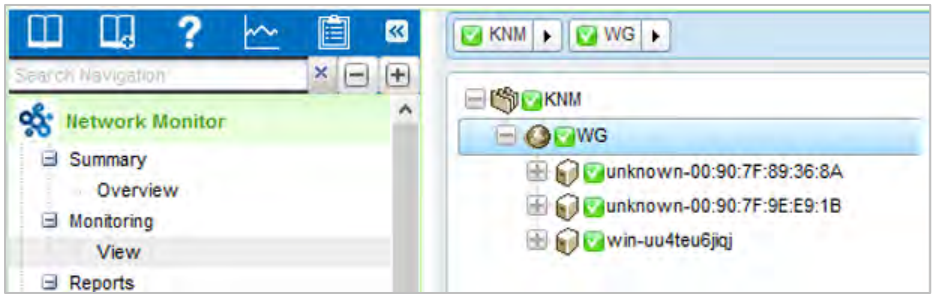
16. Select **Network Monitor > Monitoring > View > Gateway (WG)**.



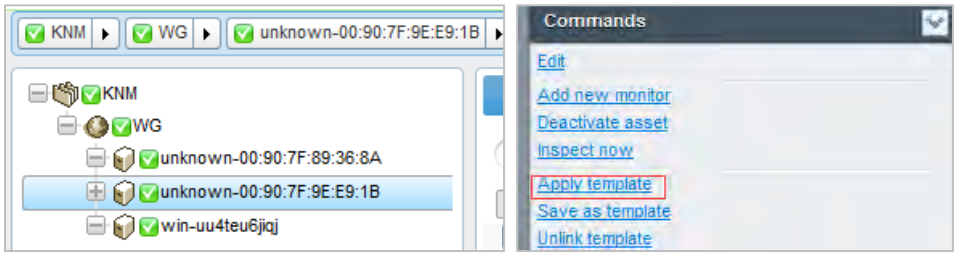
17. Select **Install gateway**.



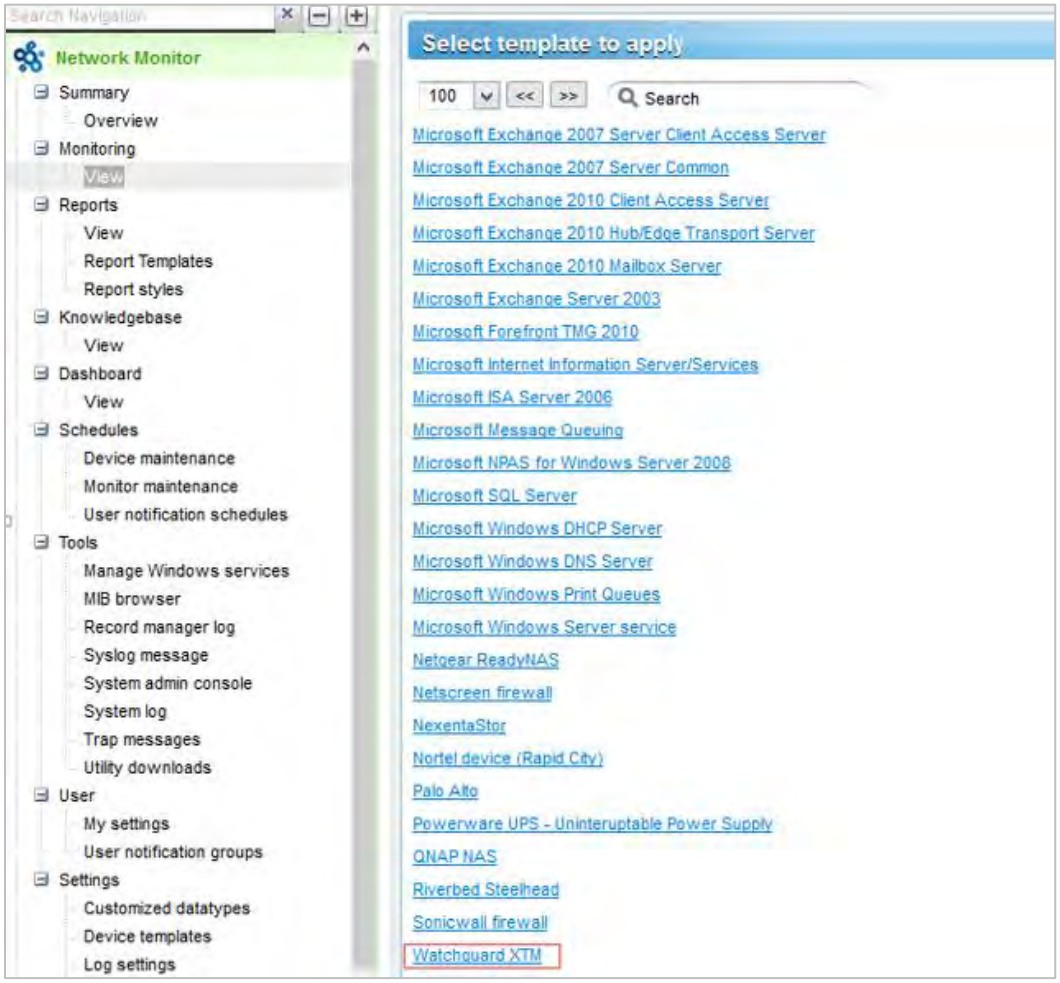
When the gateway installation is done, the page looks like this:



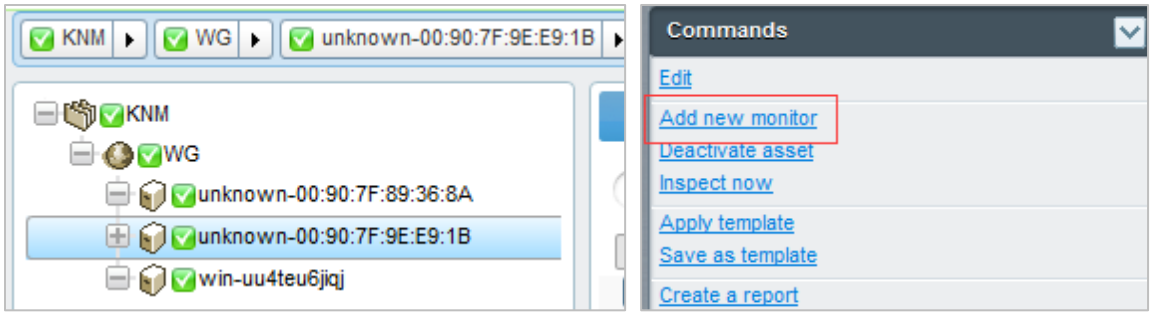
18. Select the target Firebox. Select **Apply template**.



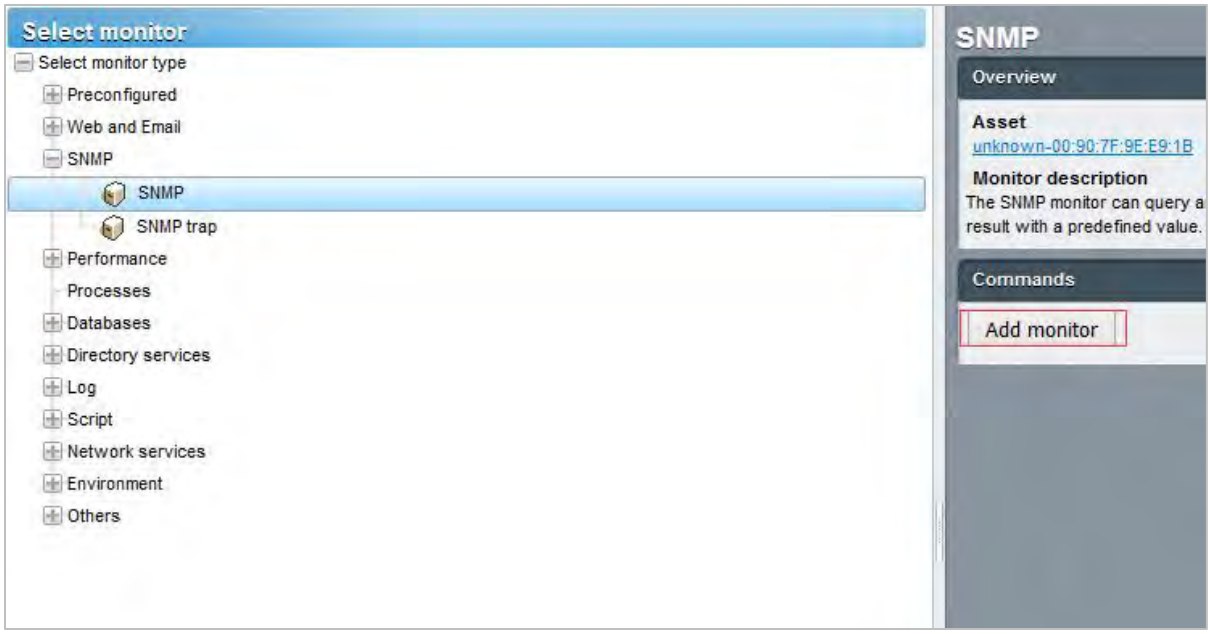
19. Select the **WatchGuard XTM** template.



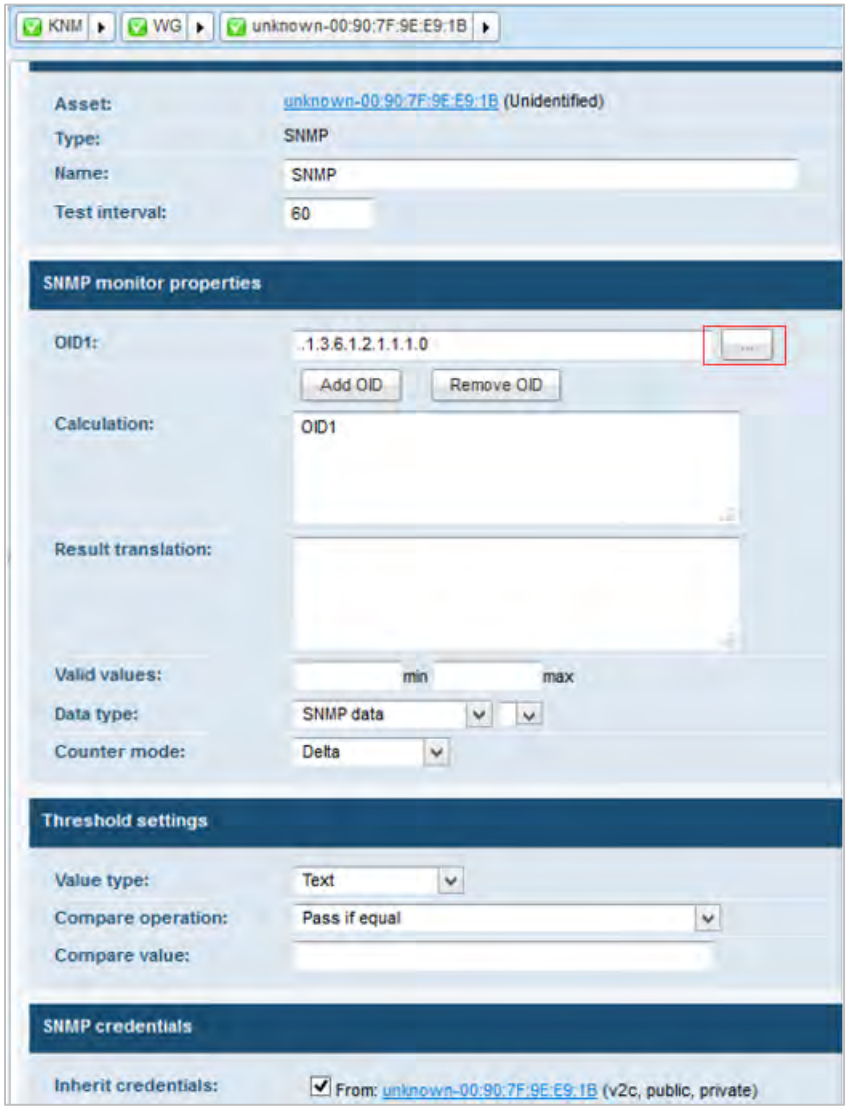
20. Select the target Firebox. Select **Add new monitor**.

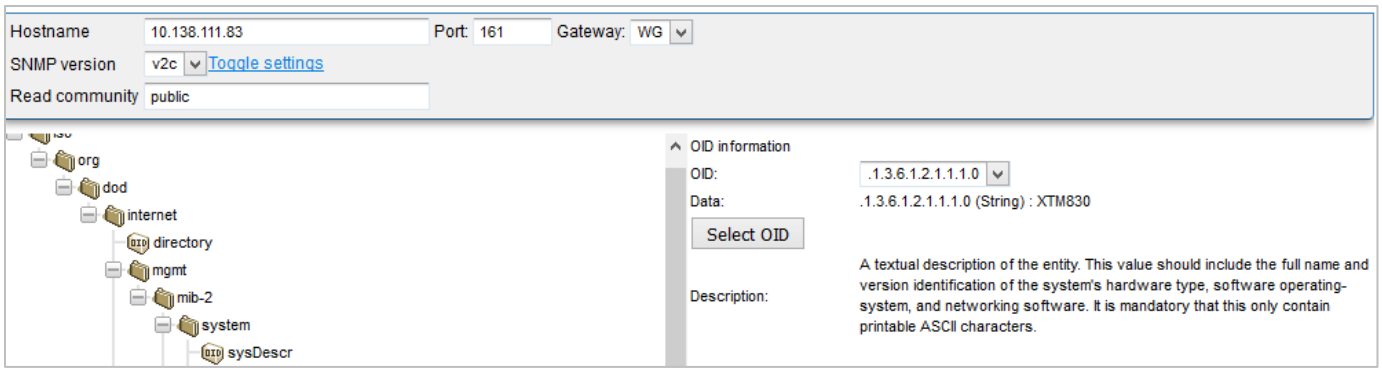


21. Select **SNMP > SNMP**.
22. Select **Add monitor**.



23. Configure the Object Identifier (**OID**). You can type the OID or select it from the MIB tree. If the OID value is a string, set the **Value type** to **Text**.





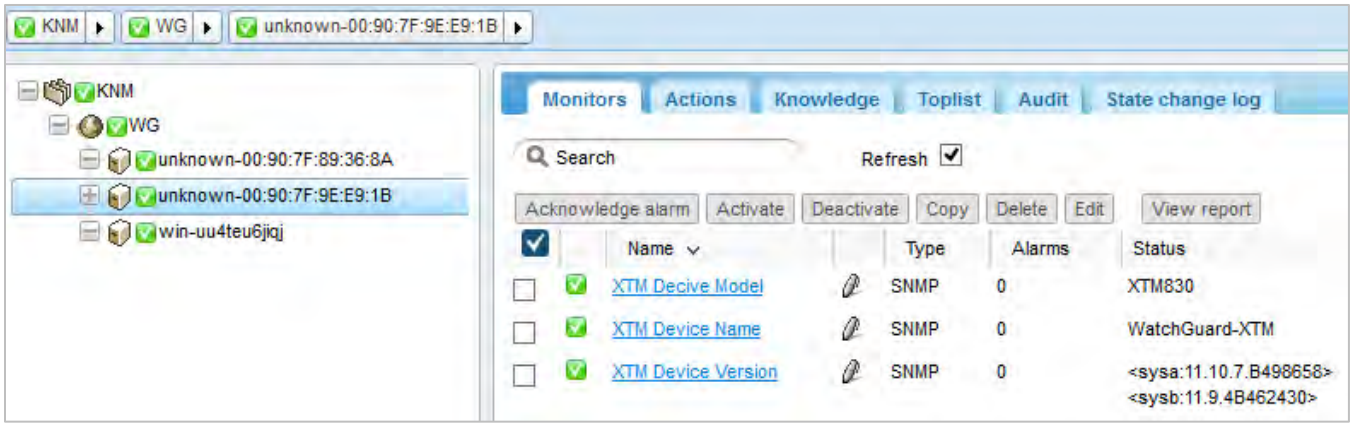
24. Add three SNMP monitors:

- XTM Device Model: OID .1.3.6.1.2.1.1.1.0
- XTM Device Name: OID .1.3.6.1.2.1.1.5.0
- XTM Device Version: OID .1.3.6.1.4.1.3097.6.3.1.0

For details about Firebox MIB objects, see:

http://www.watchguard.com/help/docs/fireware/11/en-US/index.html#en-US/basicadmin/snmp_mibs_details_c.html

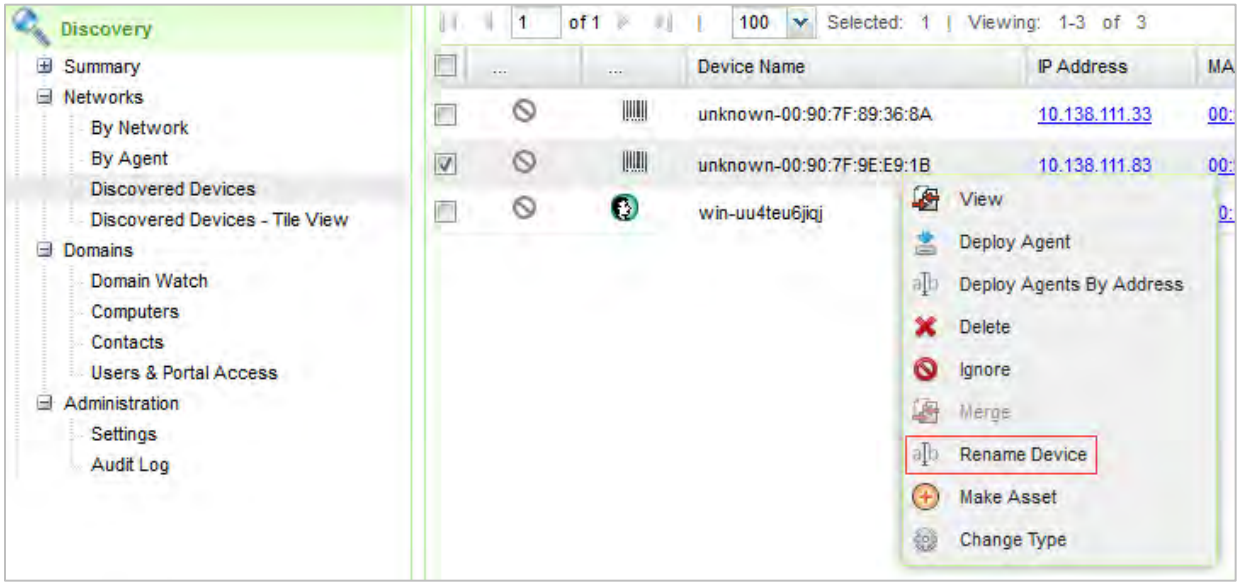
SNMP monitors information appears on the **Monitors** tab for the monitored device.



Note: Because of security programs or the firewall configuration, Kaseya may set the name of the discovered device to **unknown-MAC address**.

To rename a device:

1. Select **Discovery > Networks > Discovered Devices**.
2. Select the device and then select **Rename Device**.



The new device name appears in Network Monitor.