



Integration Guide

LogicNow MAXfocus

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.

LOGICnow MAXfocus Integration Overview

MAXfocus, formerly known as GFI MAX, is an RMM (Remote Monitoring and Management) tool from LogicNow that is commonly used by Managed Service Providers (MSPs). An MSP typically installs RMM agents on customer endpoints to discover IT assets so that the MSP can remotely monitor and manage them. This document describes how to use MAXfocus to remotely monitor a WatchGuard Firebox.

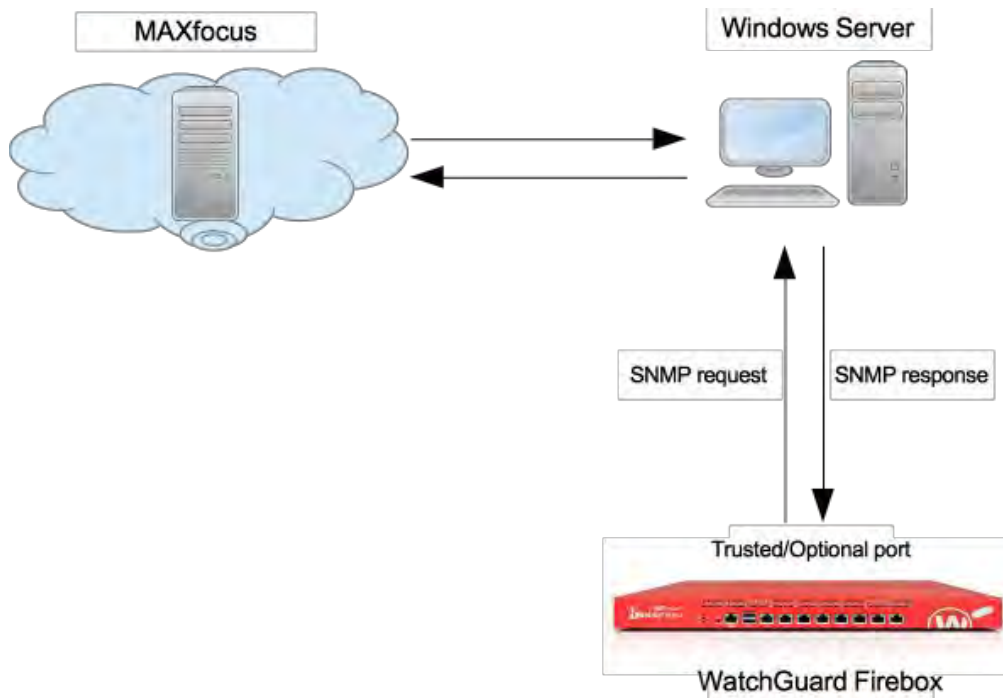
Platform and Software

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.
- MAXfocus v6.15.
- Windows Agent v10.0.1 on a Windows Server 2012 R2.

MAXfocus is a cloud-based solution. It is not available as an on-premises product.

The diagram below shows the MAXfocus solution integration. The Windows Server sends SNMP probes to the Firebox.



Firebox Configuration

You must use Fireware Web UI to configure the SNMP settings on the WatchGuard Firebox before you use MAXfocus to discover it. The URL to connect to the Web UI in your browser is:

`https://<Firebox-IP-address>:8080`

Enable SNMP

You must configure the Firebox to accept SNMP polls from an SNMP server. The IP address of the SNMP server is the IP address of the Windows server that will send SNMP probes to the Firebox and report information to the SNMP server.

1. Select **SYSTEM > SNMP**.

The SNMP Settings page appears.

SNMP Settings

Version: v1/v2c

Community String: public

User Name:

Authentication Protocol: MD5

Password:

Confirm:

Privacy Protocol: DES

Password:

Confirm:

SNMP TRAPS

Version: Disabled

SNMP Management Stations

✓	IP ADDRESS

ADD REMOVE

Use NAT for connections through the SNMP application layer gateway

2. From the **Version** drop-down list, select **v1/v2c**.
MAXfocus supports only v1 and v2c.
3. In the **Community String** text box, type the Community String on the SNMP server. Usually, **public** is used.

The Community String is used as a user ID or password that allows access to the statistics of a device.

Add an SNMP Policy

To enable the Firebox to receive SNMP polls from the Windows server, you must add an SNMP packet filter policy.

1. Select **Firewall > Firewall Policies**.
2. Click **Add Policy**.

Firewall Policies / Add Firewall Policy

Policy Name

Select a policy type

Packet Filter

Proxies

Custom

ADD EDIT REMOVE

PORT	PROTOCOL
161	UDP

Simple Network Management Protocol (SNMP) is used to collect information about and configure remote computers. This can be dangerous. Many Internet attacks use SNMP.

ADD POLICY CANCEL

3. From the **Packet Filter** drop-down list, select **SNMP**.
4. In the **Policy Name** text box, type a meaningful name.
5. Click **Add Policy**.

Now you can edit the policy.

Firewall Policies / Add

Name Enable

Settings Application Control Traffic Management Scheduling Advanced

Connections are

Policy Type

PORT	PROTOCOL
161	UDP

FROM

TO

ADD REMOVE ADD REMOVE

- In the **From** section, select **Any-Trusted** and click **Remove**.
- Click **Add**.

Add Member

Member type: Host IPv4

10.0.1.2

OK CANCEL

- From the **Member type** drop-down list, select **Host IPv4**.
- Type the IP address of the SNMP server. Click **OK**.
- In the **To** section, select **Any-External** and click **Remove**.
- Click **Add**.
- Select the alias **Firebox**. Click **OK**.

Firewall Policies / Add

Name: SNMP Enable

Settings Application Control Traffic Management Scheduling Advanced

Connections are: Allowed

Policy Type: SNMP

PORT	PROTOCOL
161	UDP

FROM: 10.0.1.2

TO: Firebox

ADD REMOVE ADD REMOVE

- Click **Save**.

MAXfocus Configuration

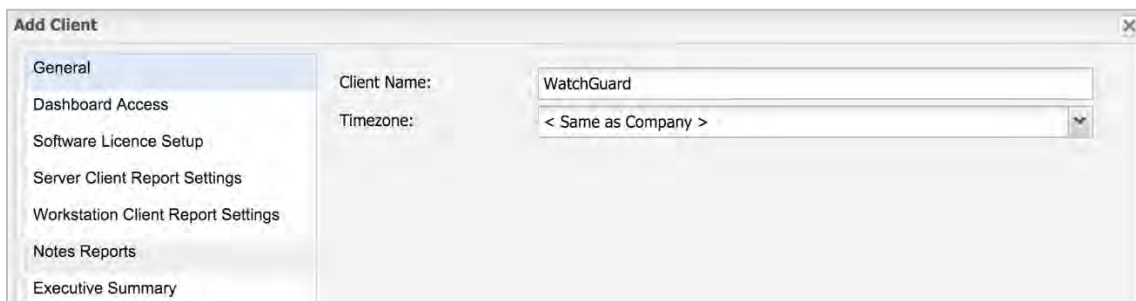
Log in to the MAXfocus Web UI with the account credentials provided by LOGICnow.

MAXfocus cannot monitor a Firebox directly as a single device. It must be monitored through an SNMP check sent by a Windows or Linux device that has an RMM agent installed.

Add a Client/Website

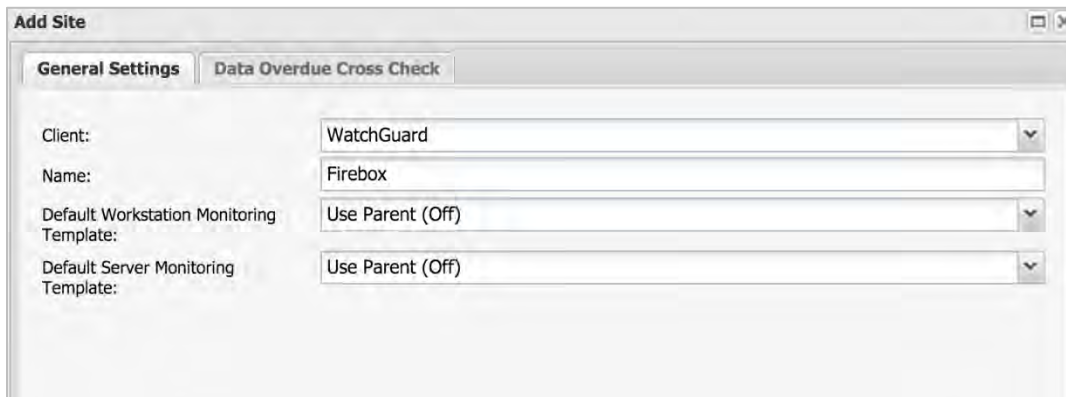
In MAXfocus you can add several Clients. For each Client you can add Sites to help you classify your devices easily.

1. Select **File > Add Client**.



The screenshot shows the 'Add Client' dialog box. On the left, there is a sidebar with the following options: General (selected), Dashboard Access, Software Licence Setup, Server Client Report Settings, Workstation Client Report Settings, Notes Reports, and Executive Summary. The main area contains two fields: 'Client Name' with the text 'WatchGuard' and 'Timezone' with a dropdown menu showing '< Same as Company >'.

2. In the **Client Name** text box, type a meaningful name to identify the client.
3. Select **File > Add Site**.



The screenshot shows the 'Add Site' dialog box. At the top, there are two tabs: 'General Settings' (selected) and 'Data Overdue Cross Check'. Below the tabs, there are four fields: 'Client' (dropdown menu with 'WatchGuard' selected), 'Name' (text box with 'Firebox'), 'Default Workstation Monitoring Template' (dropdown menu with 'Use Parent (Off)' selected), and 'Default Server Monitoring Template' (dropdown menu with 'Use Parent (Off)' selected).

4. From the **Client** drop-down list, select the **Client Name** you added earlier.
5. In the **Name** text box, type a meaningful name for this site.

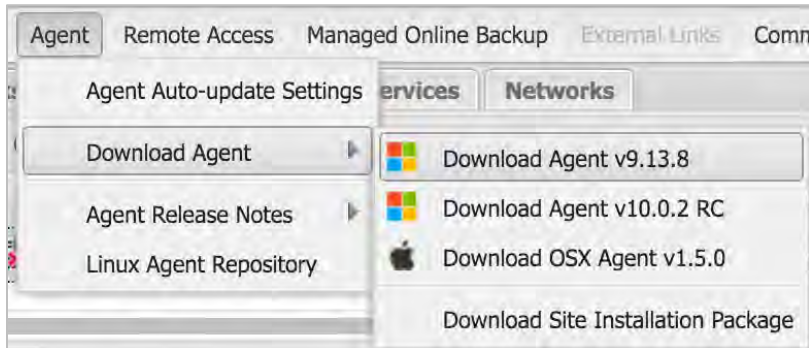
The site appears under the client.



Install Agent

You must install an agent on the device to be managed.

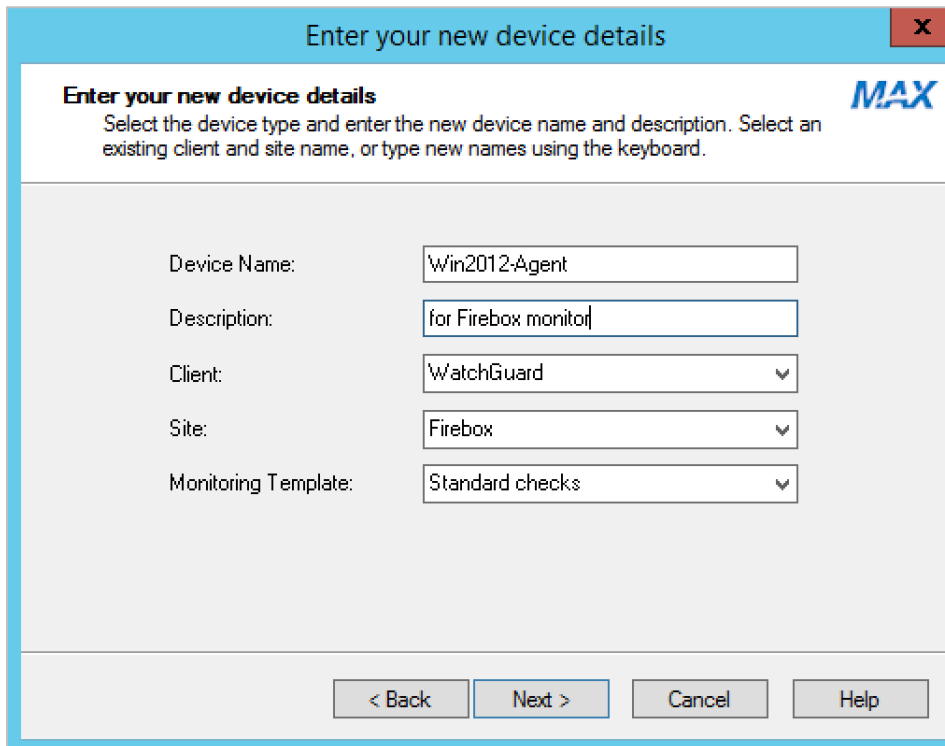
1. Select **Agent > Download Agent**.



2. Select the agent required for the OS of the device. In this example we want to install the agent on a Windows Server 2012 device, so we choose the latest released version of the agent for Windows, v9.13.8.

We recommend that you do not install RC (release candidate) versions. For example, some problems related to SNMP checks may exist in v10.0.2 RC.

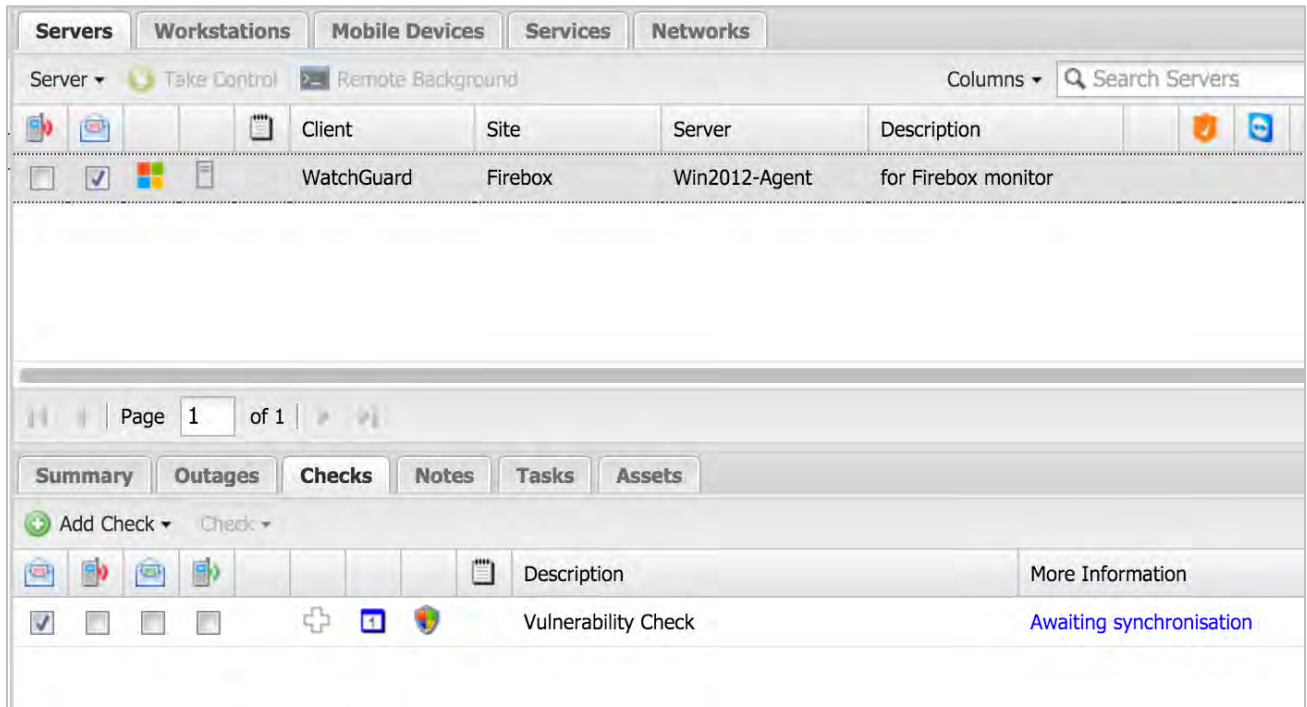
3. Install the downloaded agent on the Windows server.
4. Log in to the agent with the same credentials you used to log in to the MAXfocus Web UI.

A screenshot of a dialog box titled 'Enter your new device details'. The dialog box contains the following fields and options:

- Device Name: Win2012-Agent
- Description: for Firebox monitor
- Client: WatchGuard (dropdown menu)
- Site: Firebox (dropdown menu)
- Monitoring Template: Standard checks (dropdown menu)

At the bottom of the dialog box, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The MAX logo is visible in the top right corner of the dialog box.

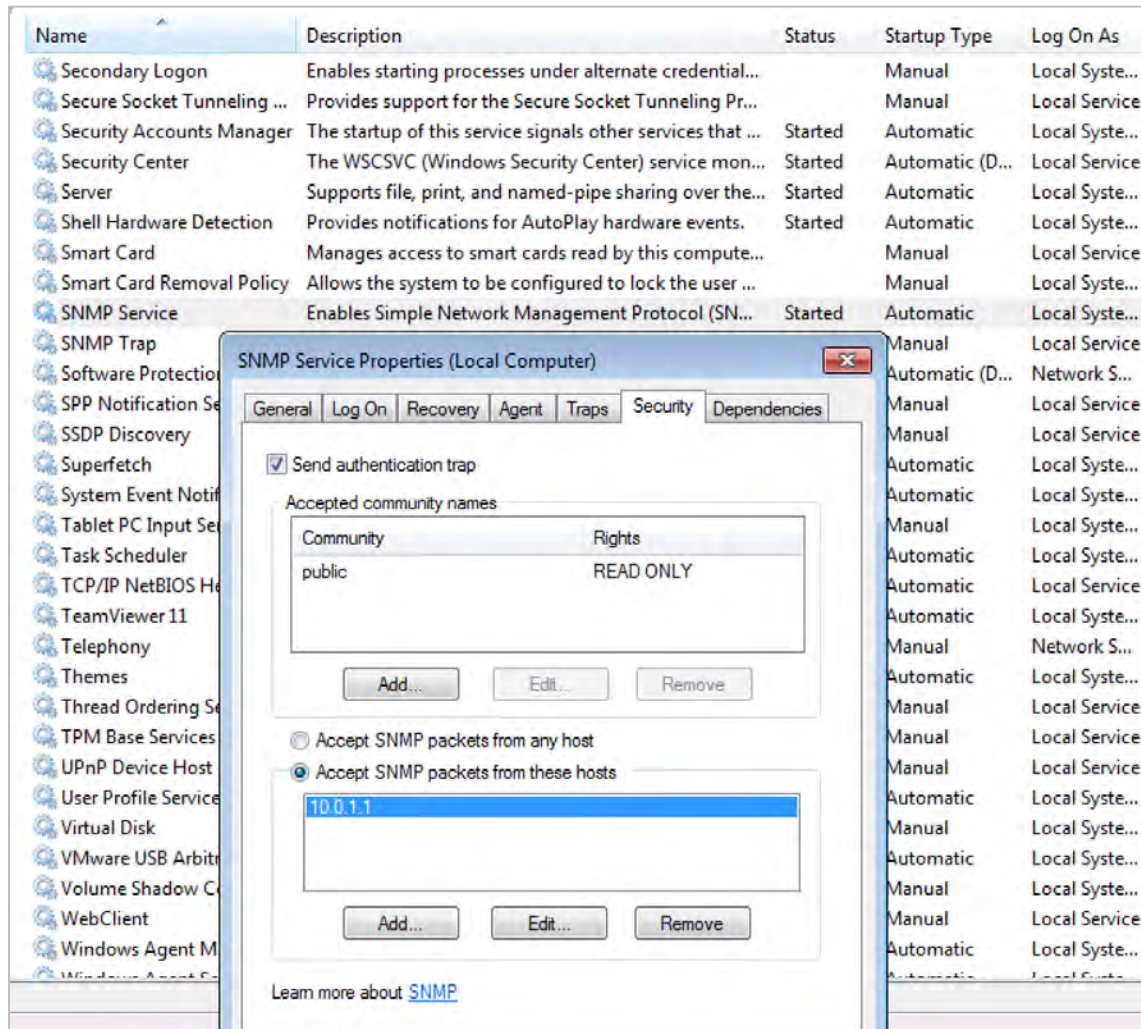
The agent automatically synchronizes information to the MAXfocus server. Information about the Firebox will appear in the **Checks** tab at the bottom of the MAXfocus server dashboard page after everything is configured.



Enable the SNMP Service

For the Windows server to monitor the Firebox, you must enable the SNMP service.

1. On the Windows server, select **Start > Run**.
2. Type **services.msc**, and start the SNMP service.
3. Right-click the SNMP service and select **Properties**.
4. Select the **Security** tab.
5. In the **Accepted community names** list add **public**.
6. In the **Accept SNMP packets from these hosts** list, add the IP address of the Firebox.



Now the agent can use the Windows probe server to detect and monitor devices in the same network.

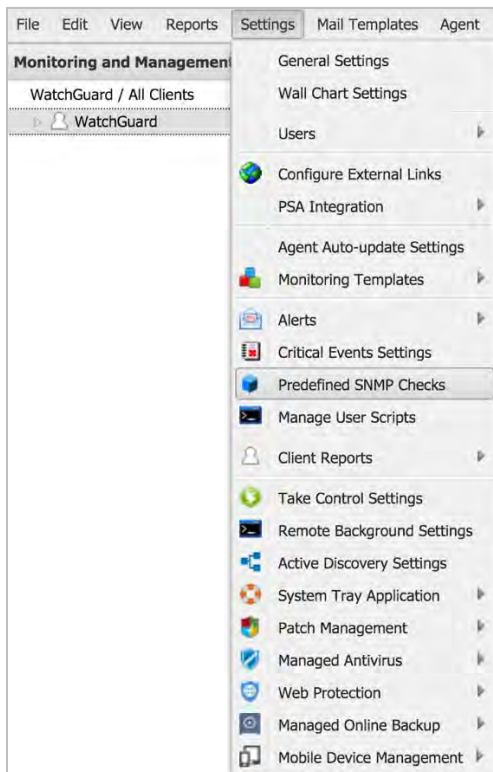
Add SNMP Checks

In MAXfocus, the information to be monitored on the Firebox is defined by SNMP checks that go through a Windows or Linux server. There are several ways to add checks:

- Predefined SNMP Checks
- Checks for a specified server
- Global predefined Monitoring Templates including checks
- Dedicated Monitoring Templates for a server.

This document describes how to add Predefined SNMP Checks.

1. In the MAXfocus Web UI, select **Settings > Predefined SNMP Checks**.



2. Click **New** at the bottom of the dialog box.
The Predefined SNMP Check dialog box appears.

Use this dialog to view, add, edit and delete Predefined SNMP checks. Enter the product name, a description of the variable being monitored, an optional reference to an online MIB document and the object identifier (OID). A "*" denotes required fields.

Predefined Check

Vendor:

Check:

Predefined Check Settings

Vendor*:

Monitored Product*:

OID description*:

MIB reference:

OID*:

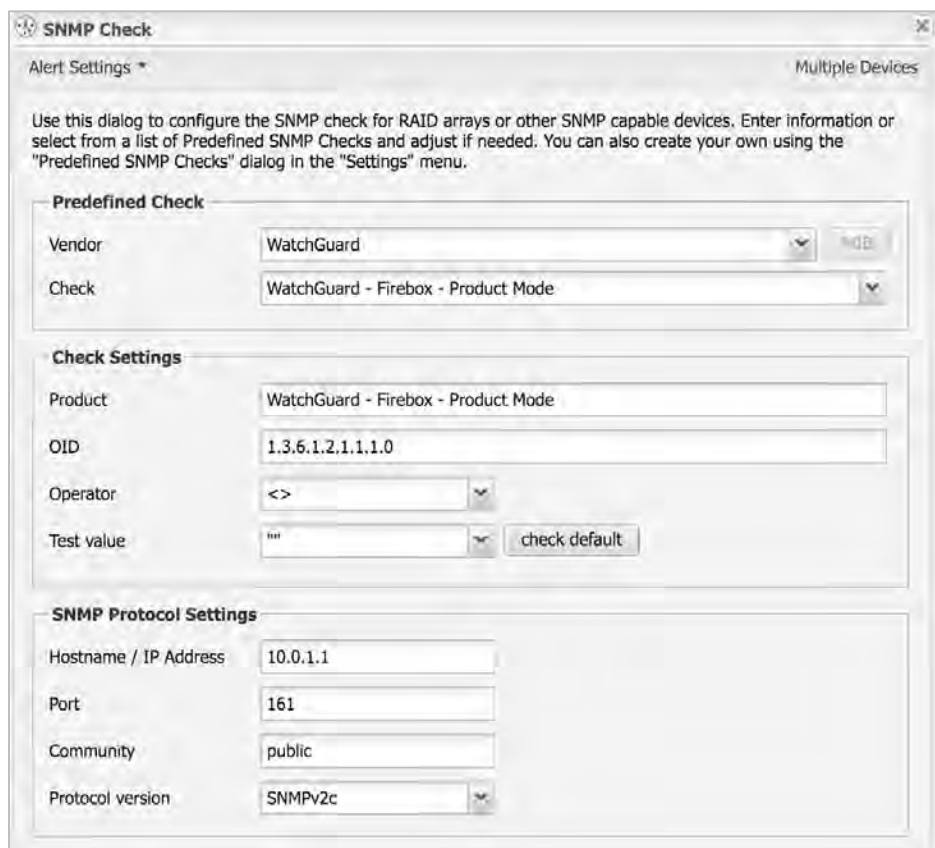
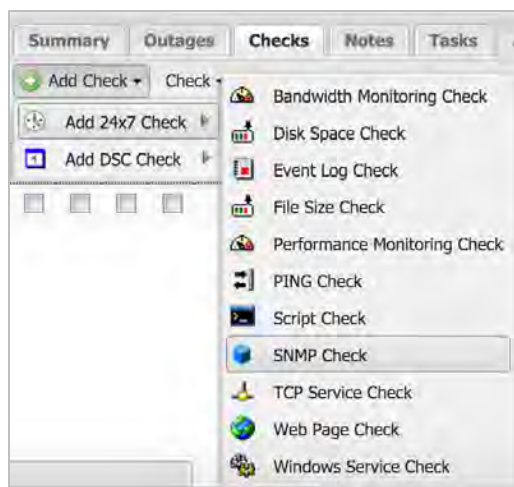
Default operator*:

Default test value*:

Return Values

Number	String	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>

3. In the **Vendor** text box, type the vendor name.
4. In the **Monitored Product** text box, type the product name.
5. In the **OID description** text box, type a meaningful description of this SNMP check.
6. In the **OID** text box, type the accurate OID for this check. You must exclude the leading period when you type the OID. For example, type **1.3.6.1.2.1.1.1.0** rather than **.1.3.6.1.2.1.1.1.0**.
For more information about Firebox OIDs see: http://www.watchguard.com/help/docs/fireware/11/en-US/index.html#en-US/basicadmin/snmp_mibs_details_c.html.
7. Configure the **Default operator** and **Default test** values to define the pass condition for this SNMP check.
8. Click **Save** to save this check.
9. To add another check, click **New** and repeat the steps above.
10. In the **Checks** tab at the bottom of server list page, select **Add Check > Add 24x7 Check > SNMP Check**.



11. In the **Predefined Check** section, select the **Vendor** and **Check** in the predefined SNMP check defined earlier.

The corresponding settings automatically appear in the Check Settings section.

12. In the **Hostname / IP Address** text box, type the IP address of the Firebox.

13. In the **Port** text box, type the port used for SNMP on the Firebox. Usually this is the default port, 161.

14. In the **Community** text box, type 'public'. This must match the **Community String** configured on the Firebox.

Test the Integration

After you add the SNMP checks to the server, the checks are shown in the **Checks** tab at the bottom of the MAXfocus dashboard. After an SNMP check is executed, information about that check appears in the **More Information** column.



The screenshot shows the 'Checks' tab in the MAXfocus dashboard. At the top, there are navigation tabs: Summary, Outages, Checks (selected), Notes, Tasks, Assets, and Patches. Below the tabs, there is a toolbar with 'Add Check' and 'Check' buttons. The main area displays a table of checks with columns for 'Description' and 'More Information'.

				Description	More Information
				SNMP Check - WatchGuard - Firebox - Product Mode	XTM330
				SNMP Check - WatchGuard - Firebox - System Name	WatchGuard-XTM