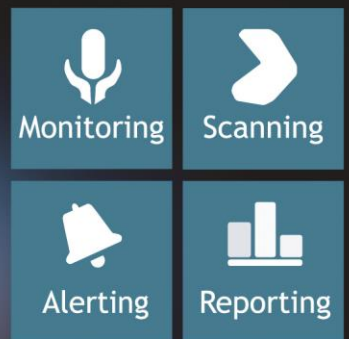




## GSX Monitor & Analyzer

Streamline your business-critical  
messaging & collaboration environments



GSX  
SOLUTIONS

# SCOM 2012 MANAGEMENT PACK

## INSTALLATION & CONFIGURATION GUIDE

## CONTENTS

INTRODUCTION .....	3
REQUIREMENTS .....	4
Installing the SNMP Service on GSX Monitor and SCOM Stations .....	4
Configuring GSX Monitor to Send SNMP Traps.....	7
INSTALLING THE SCOM 2012 MANAGEMENT PACK.....	8
CONFIGURING SCOM TO RECEIVE GSX MONITOR ALERTS .....	9
Adding GSX Monitor as a Network Device in SCOM.....	9
Alerts Severity.....	15

## INTRODUCTION

Providing extensive capabilities to anticipate problem before they impact users, GSX Monitor and Analyzer works with SCOM to build a complete solution that monitor and report on the High Availability of your key components in your collaborative and messaging environment.

Totally agentless, GSX Monitor and Analyzer allow you leveraging your SCOM investment. With a single instance of GSX Monitor and Analyzer, without installing anything on any of your server, you can measure, collect, alert and send reports on the key critical points of your Microsoft Exchange, SharePoint, BlackBerry and IBM environments.

GSX Monitor and Analyzer is the expert that administrators need to simply and efficiently get the most of SCOM, enabling proactivity, real high-availability and automatic reporting on their entire collaborative and messaging environment.

## REQUIREMENTS

The **SNMP** module must be enabled in your GSX Monitor license.

The **SNMP** option must have been enabled during the GSX Monitor installation.

The **SNMP** service must be started (page 4) on the station where GSX Monitor resides.

The alert profile must be **configured to send SNMP traps** (on page 7) in GSX Monitor.

## INSTALLING THE SNMP SERVICE ON GSX MONITOR AND SCOM STATIONS

The **SNMP** module must be enabled in your GSX Monitor license.

The **SNMP** option must have been enabled during the GSX Monitor installation.

### Checking if the SNMP Service is already installed and running

1. Right-click on *My Computer* and select *Manage > Services and Application > Services* (the location of the Services menu may vary depending on the operating system).
2. In the list of Services, search for **SNMP Service**:

Smart Card	Manages access to smar...		Manual	Local Service
Smart Card Removal Policy	Allows the system to be ...		Manual	Local System
SNMP Service	Enables Simple Network ...	Started	Automatic	Local System
SNMP Trap	Receives trap messages...	Started	Automatic	Local Service
Software Protection	Enables the download, i...	Started	Automatic (D...	Network S...

---

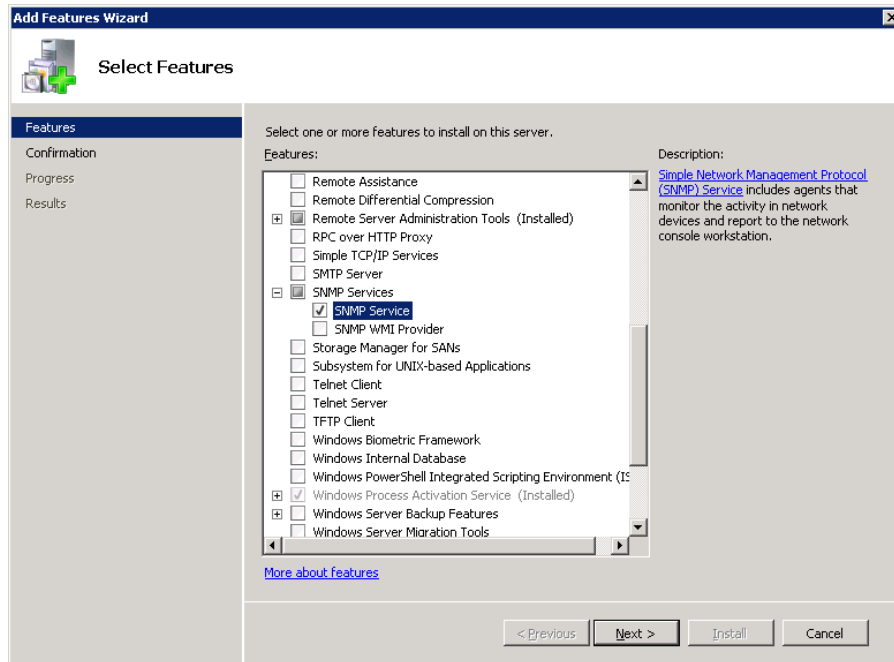
The **SNMP Trap Service** is not required by GSX Monitor and can be disabled if not used by another application.

---

- ▶ If the service is installed and running on both stations, refer to [Configuring the SNMP Agent](#).
- ▶ If the SNMP service is not installed on a server, follow the procedure below.

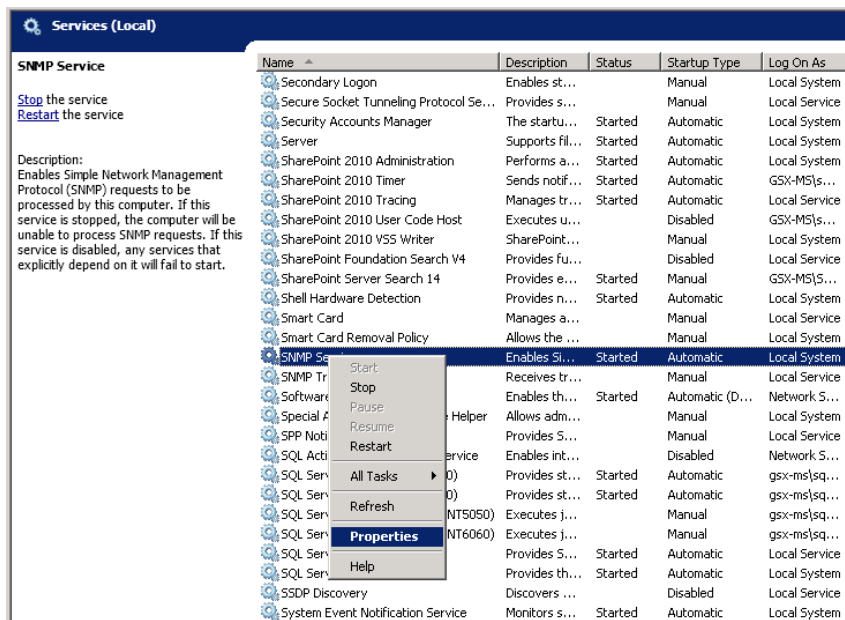
## Installing and configuring the SNMP Service

1. Go in *Control Panel > Programs > Turn Windows Features On or Off* and select the Simple Network Management Protocol feature (the location of the Features menu may vary depending on the operating system).

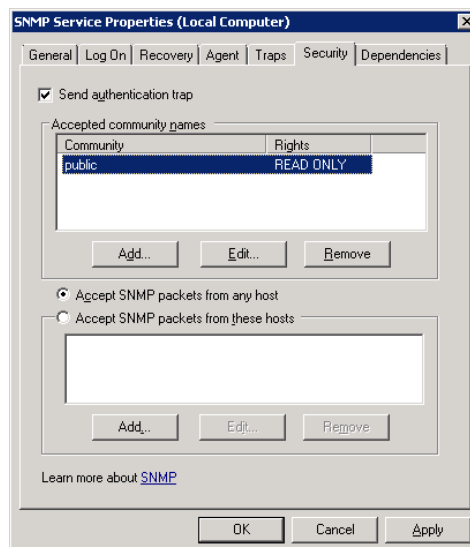


2. Wait during the SNMP feature installation and exit the installation program when done.
3. Go in the Windows Services: right-click on *My Computer* and select *Manage > Services and Application > Services* (the location of the Services menu may vary depending on the operating system).

## 4. Open the SNMP Service Properties:




## 5. Check the Community name. This name must have at least Read rights and configured in GSX Monitor:

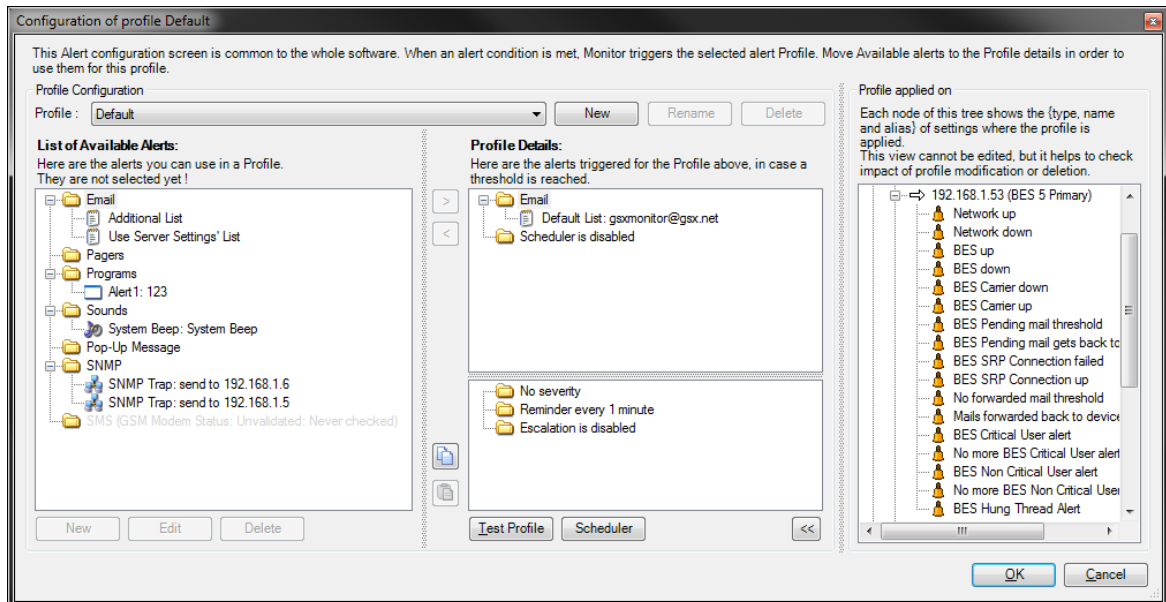


- Ensure the Accept SNMP packets from any host option is selected, or enter the IP address (or host name) of the SCOM station if you are on the GSX Monitor station, and vice-versa, in the list of authorized hosts.
- Click OK and restart the SNMP service if modifications have been made.

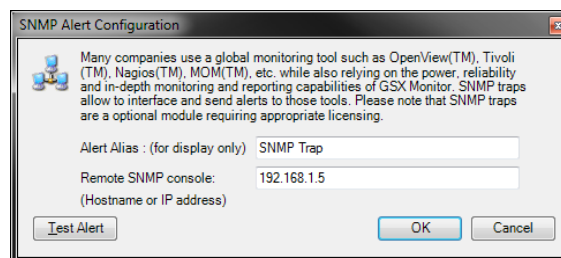
## CONFIGURING GSX MONITOR TO SEND SNMP TRAPS

*SNMP traps sending is an optional module that needs to be enabled in your GSX Monitor License.*

1. Open the alert profiles configuration windows by clicking the  button next to any alert in a server configuration wizard.



2. In the List of Available Alerts area, click on the SNMP node.
3. Click New. The SNMP Alert Configuration window is displayed:



4. Enter the configuration alias (used for display only).
5. Enter the IP address or hostname of the station where the traps will be sent.
6. Click OK to validate the SNMP alert configuration.

## INSTALLING THE SCOM 2012 MANAGEMENT PACK

*Make sure all the prerequisites listed in the [Requirements](#) (on page 4) chapter are fulfilled.*

*The Management pack must be installed on the Management Server.*

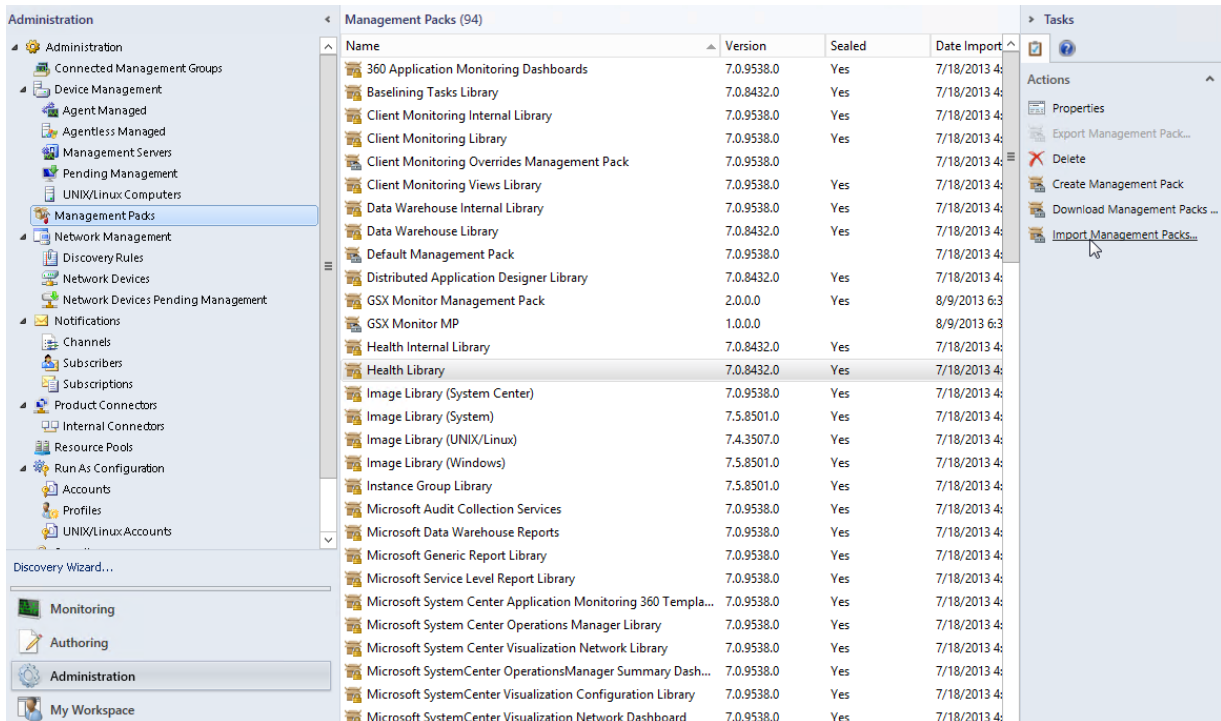
1. Download the SCOM 2012 Management Pack on [GSX Support web page](http://support.gsx.com/index.php) (<http://support.gsx.com/index.php>).
2. Place it anywhere on the SCOM Management server. It will be used during the [Import](#) (page 9) procedure.



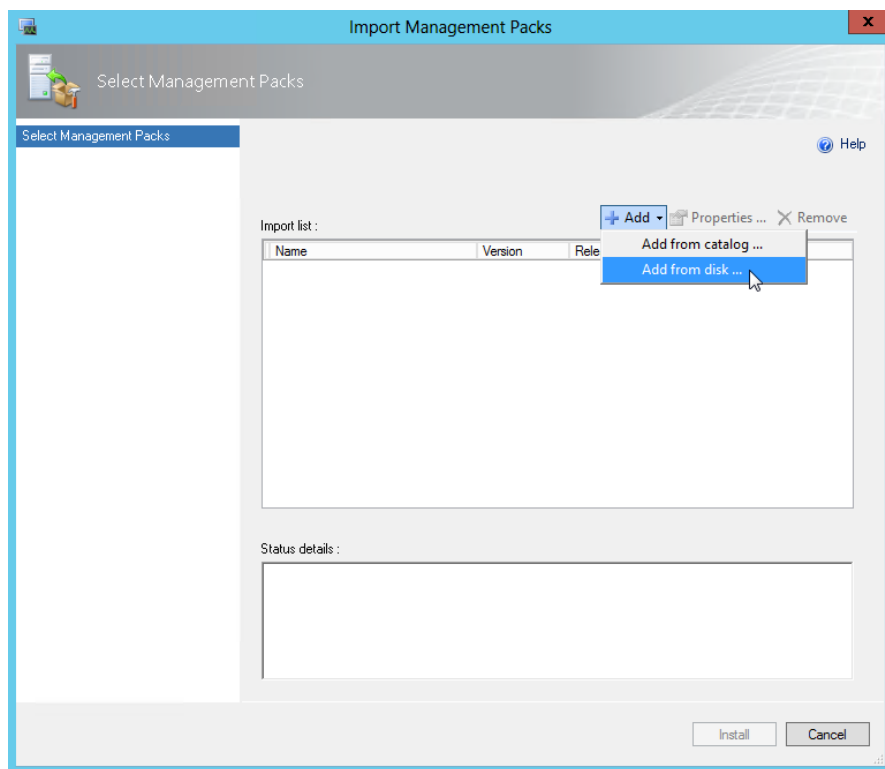
## CONFIGURING SCOM TO RECEIVE GSX MONITOR ALERTS

### ADDING GSX MONITOR AS A NETWORK DEVICE IN SCOM

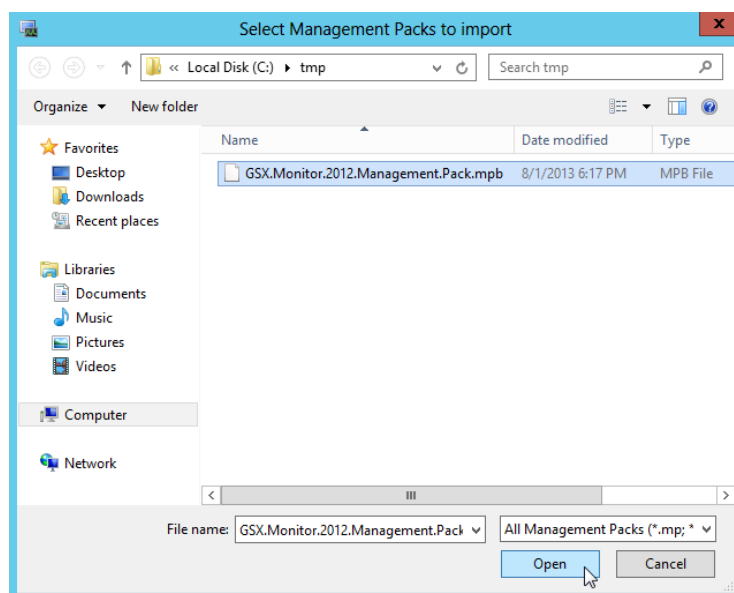
1. Open the Operation Console of SCOM.
2. From the left pane, click on the Administration tab.
3. Click Import Management Packs from the Tasks Panel:



- Click Add and select Add from disk:

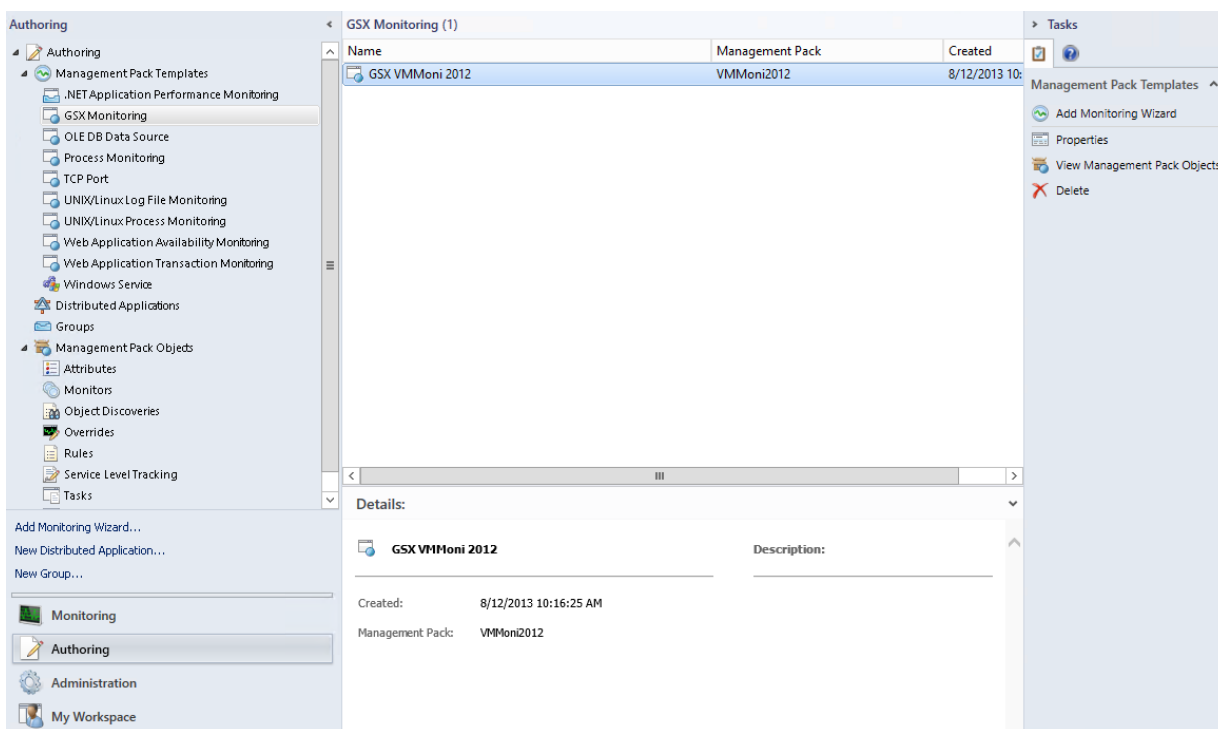


- Browse for the folder where you have downloaded the *GSX.Monitor.2012.Management.Pack.mpb* file and click Open:

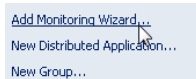


- Click Install. This makes take a few minutes.

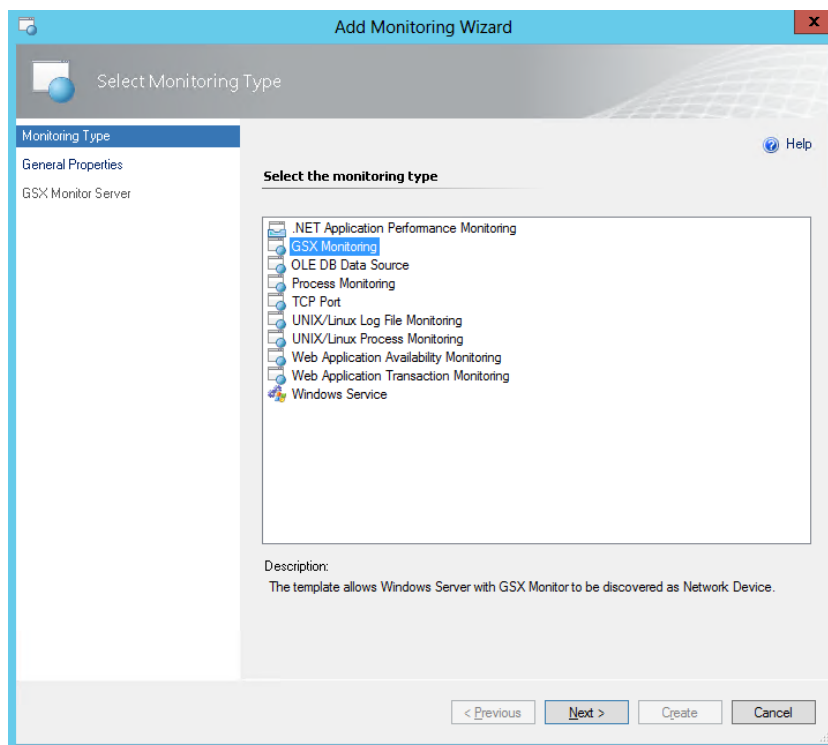
From the Authoring tab, a new Template is created:



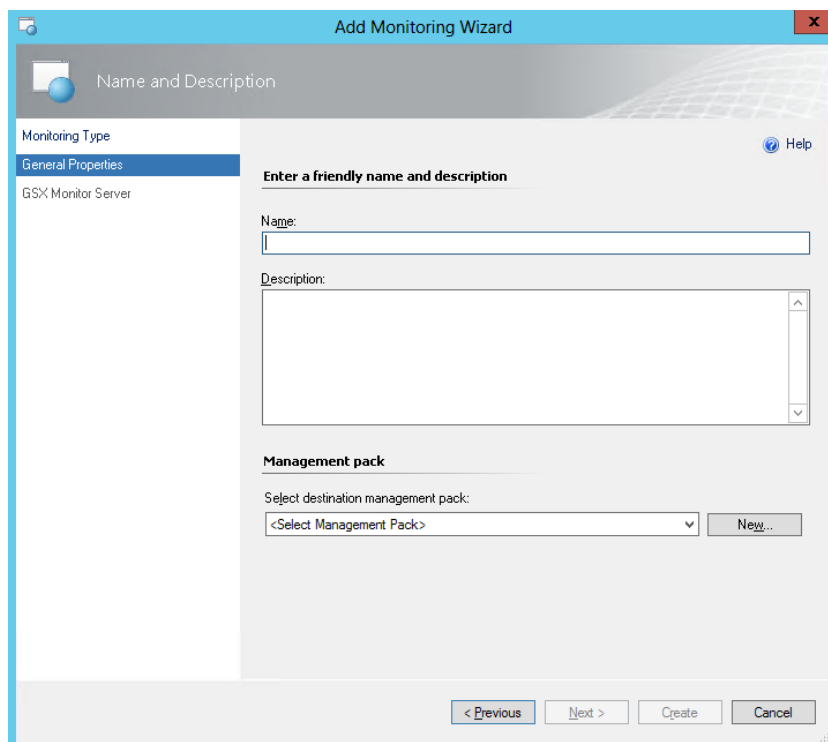
7. Click **Add Monitoring Wizard** to configure your GSX Monitor server(s) and start receiving alerts:



- From the **Monitoring Type** tab, select the **GSX Monitoring** item and click **Next**:



- Give the configuration a name, select the Management Pack and click **Next**:



10. Enter the GSX Monitor server IP address and its FQDN:

The screenshot shows the 'Add Monitoring Wizard' dialog box with the 'GSX Monitor Server Configuration' step selected. The 'Monitoring Type' is set to 'GSX Monitor Server'. The 'GSX Monitor Server' section contains fields for 'IP Address' and 'Fully Qualified Domain Name'. The 'Community String Run As Account' section has a dropdown menu and a 'New' button. The 'Create' button is highlighted.

11. Select the SNMP community previously defined or create a new one. Refer to [SNMP Service Installation](#) (page 4) for more information.
12. Click **Create** and wait until the Network Device is created.

The screenshot shows the 'Add Monitoring Wizard' dialog box with the 'GSX Monitor Server Configuration' step selected. The 'IP Address' field is filled with '192.168.1.1' and the 'Fully Qualified Domain Name' field is filled with 'gsx-monitor-server.domain.local'. The 'Community String Run As Account' dropdown menu is set to 'Public Community String'. The 'Create' button is highlighted and a mouse cursor is clicking it.

If the discovery fails, check that no firewall prevents the traps to be sent.

GSX Monitor is now configured as a Network Device:

The screenshot displays the GSX Monitor web interface. On the left, the 'Monitoring' sidebar shows a tree view with 'Network Devices' selected. The main panel shows a table of 'Network Devices (2)'. The first device, 'VMMoni2012.ent.gsx.com', is in a 'Healthy' state. The second device, 'gsx-monitor-se...', is 'Not monitored'. Below the table, the 'Detail View' for 'VMMoni2012.ent.gsx.com' is shown, listing properties such as Display Name, Full Path Name, Access Mode, Certification, Description, Device Key, Location, Model, Port Number, and Primary Owner Contact. On the right, a 'Tasks' panel offers actions like 'Start Maintenance Mode...', 'Edit Maintenance Mode Set...', 'Stop Maintenance Mode...', and 'Personalize view...'. Below this, a 'Navigation' panel lists views like 'Alert View', 'Diagram View', 'Event View', 'Performance View', 'State View', 'Network Node Dashboard', and 'Network Vicinity Dashboard'. At the bottom right, a 'Node Tasks' panel includes 'Ping', 'SNMP GET', 'SNMP Walk', 'Telnet Console', and 'Traceroute'.

State	Maint...	Name	Location	Model	SNMP Agent Ac
Healthy		VMMoni2012.e...			192.168.1.168
Not monitored		gsx-monitor-se...			192.168.1.1

**Node properties of VMMoni2012.ent.gsx.com**

Display Name	VMMoni2012.ent.gsx.com
Full Path Name	VMMoni2012.ent.gsx.com
Access Mode	ICMPSNMP
Certification	
Description	
Device Key	192.168.1.168
Location	
Model	
Port Number	161
Primary Owner Contact	

GSX Monitor alerts are now collected and sorted depending on their criticality. Refer to Alerts Severity for more information.

The screenshot shows the 'Critical Alerts (9)' section of the GSX Monitor interface. The left sidebar has 'Critical Alerts' selected under 'GSX Monitor Alerts'. The main panel displays a table of critical alerts. The first alert is expanded, showing its source as 'VMMoni2012.ent.gsx.com (9)'. The table lists alerts with columns for Description, Resolution..., Created, and Custom Field.

Description	Resolution...	Created	Custom Field
<b>Source: VMMoni2012.ent.gsx.com (9)</b>			
10/14/2013 11:48:48 AM - Exchange Spot Check Report: LABMBX2.G...	New	10/14/2013 ...	635173481280
10/13/2013 11:48:51 AM - Exchange Spot Check Report: LABMBX2.G...	New	10/13/2013 ...	635172617310
10/12/2013 11:48:45 AM - Exchange Spot Check Report: LABMBX2.G...	New	10/12/2013 ...	635171753250
10/11/2013 6:04:36 PM - Mails forwarded back to devices: gsxbesex...	New	10/11/2013 ...	635171114760
10/11/2013 6:04:15 PM - Mails forwarded back to devices: GSXBES00...	New	10/11/2013 ...	635171114550
10/11/2013 11:48:47 AM - Exchange Spot Check Report: LABMBX2.G...	New	10/11/2013 ...	635170889270
10/10/2013 6:01:54 PM - Mails forwarded back to devices: gsxbesex...	New	10/10/2013 ...	635170249140
10/10/2013 6:01:23 PM - Mails forwarded back to devices: GSXBES00...	New	10/10/2013 ...	635170248830
10/10/2013 1:38:21 PM - Domino down: azer (azer) Down since 10/1...	New	10/10/2013 ...	635170091010

## ALERTS SEVERITY

GSX Monitor alerts are all gathered in the GSX Monitor Dashboard of the Monitoring tab and sorted in three categories depending on their severity:

**Monitoring**

- Distributed Applications
- Task Status
- UNIX/Linux Computers
- Windows Computers
- Agentless Exception Monitoring
- Application Monitoring
- Data Warehouse
- GSX Monitor Management Pack
  - GSX Monitor Dashboard
  - GSX Monitor Alerts
    - Critical Alerts
    - Information Alerts
    - Warning Alerts
  - GSX Monitor MP
- Microsoft Audit Collection Services
- Microsoft Windows Client
- Microsoft Windows Server
- Network Monitoring
  - Active Alerts
  - Hosts
  - HSRP Groups
  - Legacy Network Devices
  - Network Devices
  - Network Summary Dashboard
  - Routers
  - Switches
  - VLANs

**GSX Monitor Dashboard**

**Critical Alerts (11)**

Description	Resolution ...	Created	Custom Field 8
Source: VMMoni2012.ent.gsx.com (11)			
10/14/2013 6:02:39 PM - Mails forwarded back to devices: gsxbesexc1 (gsxbesexc1)	New	10/14/2013 ...	6351737055900...
10/14/2013 6:01:51 PM - Mails forwarded back to devices: GSXBES002 (GSXBES002)	New	10/14/2013 ...	6351737051100...

**Warning Alerts (0)**

Description	Resolution State	Created	Custom Field 8
-------------	------------------	---------	----------------

**Information Alerts (12)**

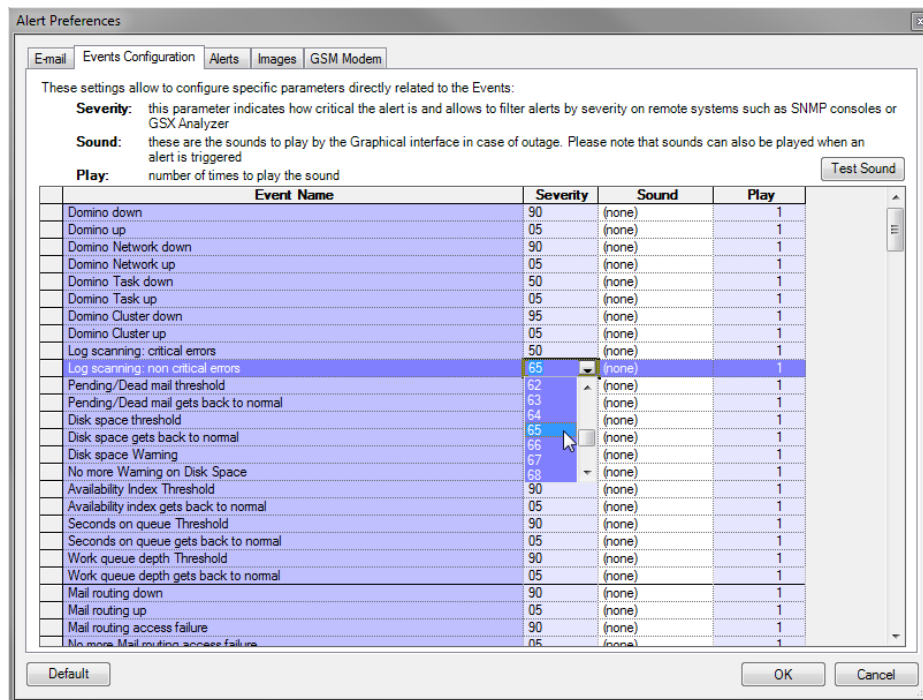
Description	Resolution State	Created
Source: VMMoni2012.ent.gsx.com (12)		
10/14/2013 5:05:12 PM - Traveler Devices Synchronisation Date: GSX Pool (GSX Pool)	New	10/14/2013 5:05:13 PM
10/14/2013 4:06:38 PM - No forwarded mail threshold: GSXBES002 (GSXBES002) No m...	New	10/14/2013 4:06:39 PM
10/14/2013 4:03:35 PM - No forwarded mail threshold: gsxbesexc1 (gsxbesexc1) No m...	New	10/14/2013 4:03:35 PM

**Alert Details**

Select an item in the view above to display its details.

- ▶ Critical alerts (severity 80 to 99)
- ▶ Warning alerts (severity 60 to 79)
- ▶ Information alerts (severity 1 to 59)

The severity can be set for each Event in the *Preferences > Alerts > Events Configuration* window of GSX Monitor.



If a severity value is set on an alert profile, it overrides the default value of the event. All alerts related to that profile will then have the same severity.

