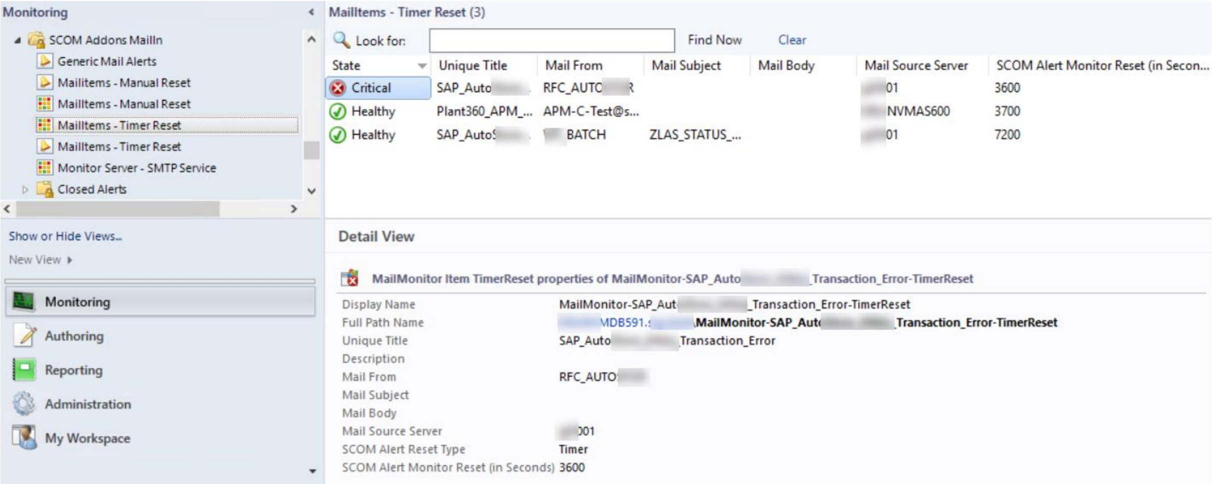
Monitor any workload that send E-Mails with SCOM

This Management Pack enriches SCOM with an E-Mail interface. Alerts can be created either by a generic rule or via a monitor that reacts on your custom filter pattern.



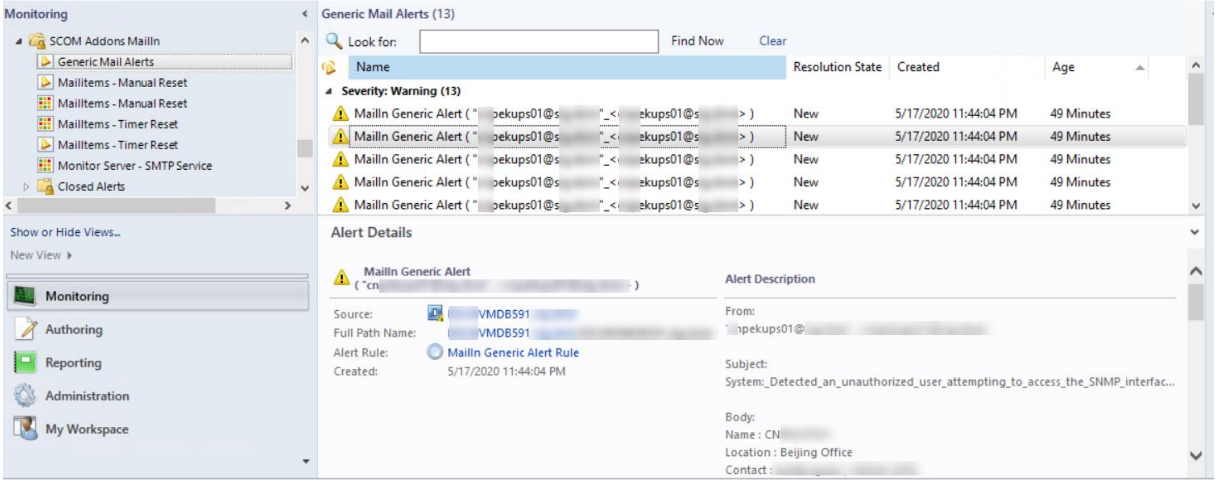
MailItems - Timer Reset (3)

State	Unique Title	Mail From	Mail Subject	Mail Body	Mail Source Server	SCOM Alert Monitor Reset (in Secon...
Critical	SAP_Auto[redacted]	RFC_AUTO[redacted]R			[redacted]01	3600
Healthy	Plant360_APM_...	APM-C-Test@s...			[redacted]NVMAS600	3700
Healthy	SAP_Auto[redacted]	[redacted] BATCH	ZLAS_STATUS_...		[redacted]01	7200

Detail View

MailMonitor Item TimerReset properties of MailMonitor-SAP_Auto[redacted]_Transaction_Error-TimerReset

Display Name	MailMonitor-SAP_Aut[redacted]_Transaction_Error-TimerReset
Full Path Name	[redacted]MDB591.[redacted]\MailMonitor-SAP_Aut[redacted]_Transaction_Error-TimerReset
Unique Title	SAP_Auto[redacted]_Transaction_Error
Description	
Mail From	RFC_AUTO[redacted]
Mail Subject	
Mail Body	
Mail Source Server	[redacted]001
SCOM Alert Reset Type	Timer
SCOM Alert Monitor Reset (in Seconds)	3600



Generic Mail Alerts (13)

Name	Resolution State	Created	Age
Severity: Warning (13)			
MailIn Generic Alert ("[redacted]ekups01@s[redacted]"_<[redacted]ekups01@s[redacted]>)	New	5/17/2020 11:44:04 PM	49 Minutes
MailIn Generic Alert ("[redacted]ekups01@s[redacted]"_<[redacted]ekups01@s[redacted]>)	New	5/17/2020 11:44:04 PM	49 Minutes
MailIn Generic Alert ("[redacted]ekups01@s[redacted]"_<[redacted]ekups01@s[redacted]>)	New	5/17/2020 11:44:04 PM	49 Minutes
MailIn Generic Alert ("[redacted]ekups01@s[redacted]"_<[redacted]ekups01@s[redacted]>)	New	5/17/2020 11:44:04 PM	49 Minutes
MailIn Generic Alert ("[redacted]ekups01@s[redacted]"_<[redacted]ekups01@s[redacted]>)	New	5/17/2020 11:44:04 PM	49 Minutes

Alert Details

MailIn Generic Alert
("cn[redacted])

Source: [redacted]VMDB591[redacted]
Full Path Name: [redacted]VMDB591[redacted]
Alert Rule: MailIn Generic Alert Rule
Created: 5/17/2020 11:44:04 PM

Alert Description

From:
[redacted]pekups01@[redacted]

Subject:
System:_Detected_an_unauthorized_user_attempting_to_access_the_SNMP_interfac...

Body:
Name : CN[redacted]
Location : Beijing Office
Contact : [redacted]

Change History

Date	Build No.	Changes
2020-05-13	1.0.0.140	Initial Upload to GitHub
2020-05-18	1.0.0.190	Changed host from RMS to any Server

Contents

Initial setup

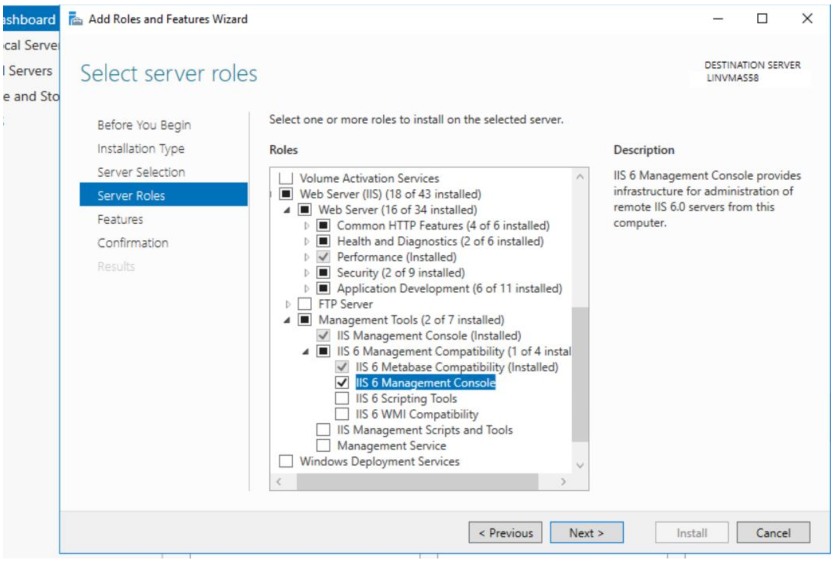
The following steps on any with SCOM agent monitored **Windows Server 2012 or higher** are required.:

- Install and configure SMTP service
- Set registry keys
- Import the Management Pack
- Create an override Management Pack
- Optional:
  - Add mail-match-pattern in XML configuration file for monitors
  - Configure mail routing to receive alert E-Mails via e-mail address

Install and configure SMTP service

To receive e-Mails the SMTP service needs to be installed and configured.

Open the **Server Manager**, choose … and adding IIS and IIS6 Management Tools



Select server roles

DESTINATION SERVER
LINVMAS58

Select one or more roles to install on the selected server.

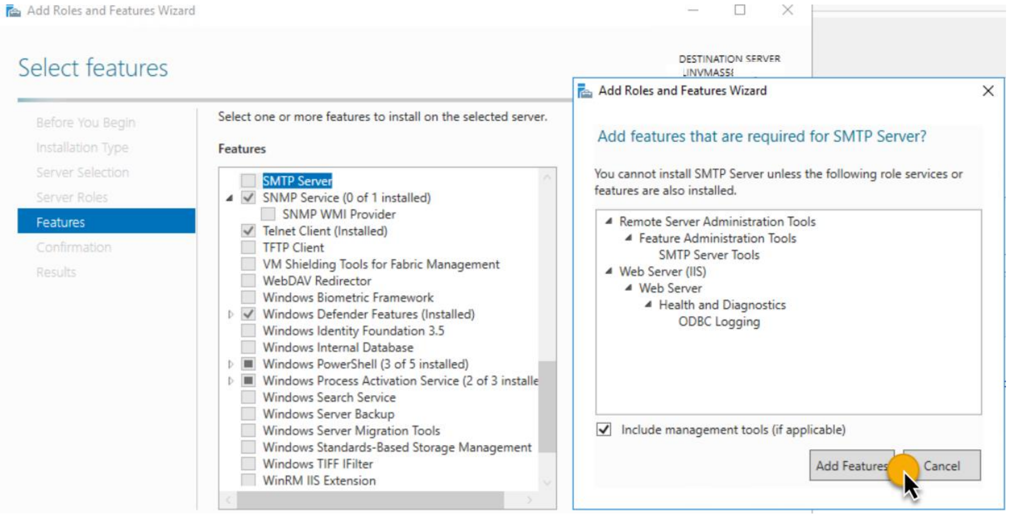
Roles

- ☐ Volume Activation Services
- ■ Web Server (IIS) (18 of 43 installed)
  - ■ Web Server (16 of 34 installed)
    - ■ Common HTTP Features (4 of 6 installed)
    - ■ Health and Diagnostics (2 of 6 installed)
    - ☑ Performance (Installed)
    - ■ Security (2 of 9 installed)
    - ■ Application Development (6 of 11 installed)
  - ☐ FTP Server
  - ■ Management Tools (2 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - ■ IIS 6 Management Compatibility (1 of 4 instal
      - ☑ IIS 6 Metabase Compatibility (Installed)
      - ☑ IIS 6 Management Console
      - ☐ IIS 6 Scripting Tools
      - ☐ IIS 6 WMI Compatibility
    - ☐ IIS Management Scripts and Tools
    - ☐ Management Service
- ☐ Windows Deployment Services

Description

IIS 6 Management Console provides infrastructure for administration of remote IIS 6.0 servers from this computer.

Next, adding **SMTP Server** and IIS ODBC Logging features



Select features

DESTINATION SERVER
LINVMAS5

Select one or more features to install on the selected server.

Features

- ☐ SMTP Server
- ☑ SNMP Service (0 of 1 installed)
  - ☐ SNMP WMI Provider
- ☑ Telnet Client (Installed)
- ☐ TFTP Client
- ☐ VM Shielding Tools for Fabric Management
- ☐ WebDAV Redirector
- ☐ Windows Biometric Framework
- ☑ Windows Defender Features (Installed)
- ☐ Windows Identity Foundation 3.5
- ☐ Windows Internal Database
- ■ Windows PowerShell (3 of 5 installed)
- ■ Windows Process Activation Service (2 of 3 installe
- ☐ Windows Search Service
- ☐ Windows Server Backup
- ☐ Windows Server Migration Tools
- ☐ Windows Standards-Based Storage Management
- ☐ Windows TIFF IFilter
- ☐ WinRM IIS Extension

Add features that are required for SMTP Server?

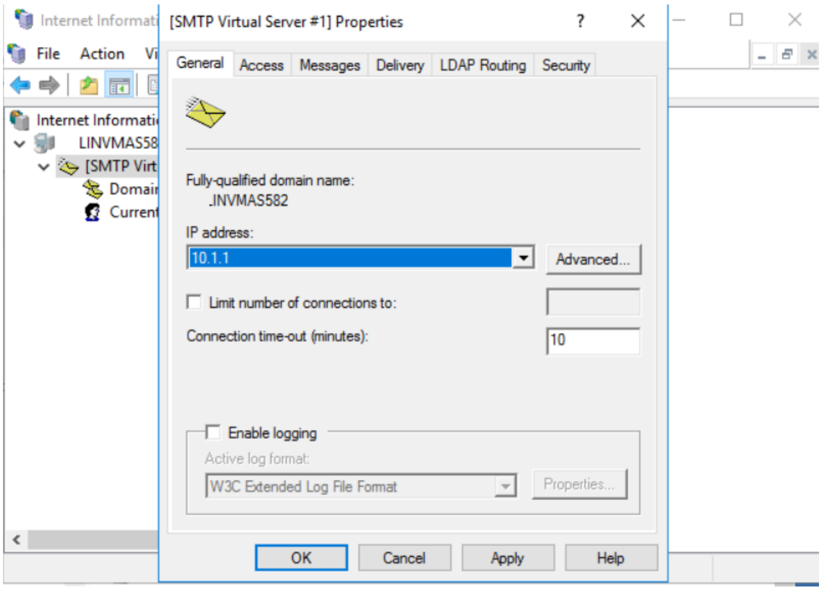
You cannot install SMTP Server unless the following role services or features are also installed.

- Remote Server Administration Tools
  - Feature Administration Tools
    - SMTP Server Tools
- Web Server (IIS)
  - Web Server
    - Health and Diagnostics
      - ODBC Logging

☑ Include management tools (if applicable)

After installation, a restart may be required.

After installing, the SMTP service the listing IP address and the relay restrictions to the own IP addresses, localhost and your internal mail-servers (e.g. Exchange hub transport).



[SMTP Virtual Server #1] Properties

Fully-qualified domain name: .INVMAS582

IP address: 10.1.1

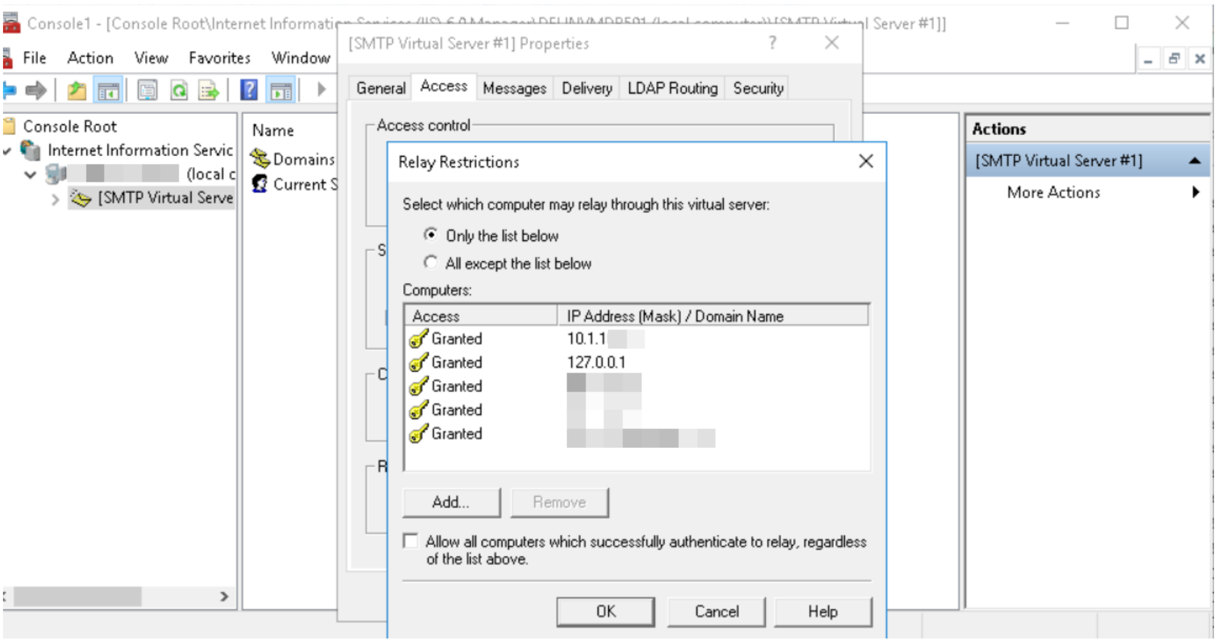
□ Limit number of connections to:

Connection time-out (minutes): 10

□ Enable logging

Active log format: W3C Extended Log File Format

Specify listing IP address in IIS6 MMC



Console1 - [Console Root\Internet Information Services (IIS) 6.0 Manager\ [SMTP Virtual Server #1]]
File Action View Favorites Window
Console Root
Internet Information Servic
(local c
[SMTP Virtual Serve
Name
Domains
Current S
General Access Messages Delivery LDAP Routing Security
Access control
Actions
[SMTP Virtual Server #1]
More Actions
Add... Remove
OK Cancel Help

[SMTP Virtual Server #1] Properties

Relay Restrictions

Select which computer may relay through this virtual server:

● Only the list below

○ All except the list below

Computers:

Access	IP Address (Mask) / Domain Name
Granted	10.1.1[redacted]
Granted	127.0.0.1
Granted	[redacted]
Granted	[redacted]
Granted	[redacted]

□ Allow all computers which successfully authenticate to relay, regardless of the list above.

Restricting SMTP Service Relay restrictions to all which need to connect via SMTP

Set registry keys

Registry keys store basic information about the SMTP service. For convenience, paste the text in the yellow box into notepad and safe it as **smtpmp.reg**.:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\ABCIT\SCOMAddonsMailIn]
"XMLConfigFilePath"="C:\\Temp\\scom.Addons.MailIn.MonitorItemList.xml"
"EmlDirectory"="C:\\inetpub\\mailroot\\Drop"
"EmlArchive"="C:\\Temp\\MailArchive"
"NoOfLinesFromTop"="100"
```

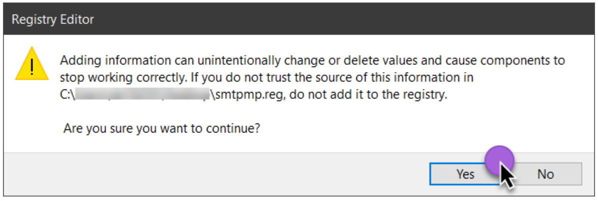
XMLConfigFilePath:
Location of the XML file which holds information about the custom-mailmonitor-patterns.

EmlDirectory:
Path in which the SMTP service stores the emails. The value is the yellow box is the default location.

EmlArchive:
Storage folder for emails that have been already process by SCOM. – A rule will take care for automatic deletion of old files.

NoOfLinesFromTop:
Specifies how many lines of the email body are read by SCOM.

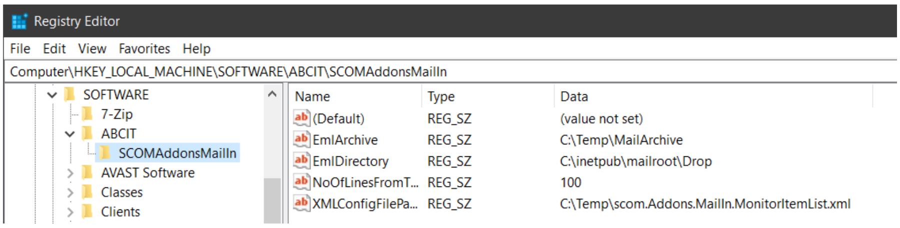
Double click the **smtpmp.reg** file and confirm the import of the settings:



Adding information can unintentionally change or delete values and cause components to stop working correctly. If you do not trust the source of this information in C:\[redacted]\smtpmp.reg, do not add it to the registry.

Are you sure you want to continue?

After importing the settings in the registry will look as follows:

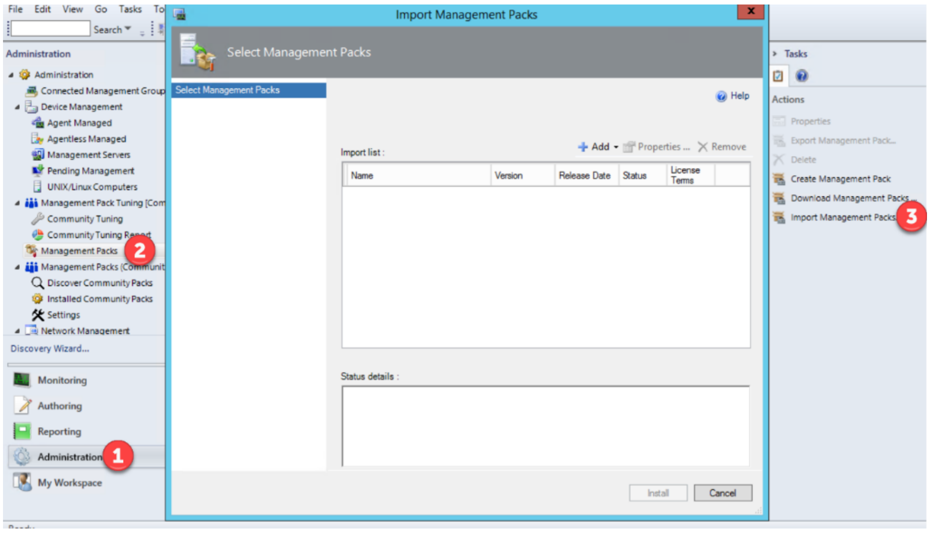


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\ABCIT\SCOMAddonsMailIn

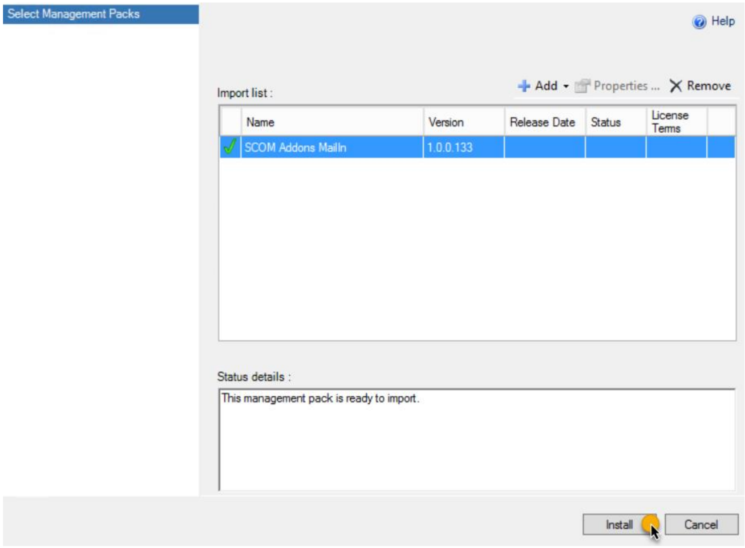
Name	Type	Data
(Default)	REG_SZ	(value not set)
EmlArchive	REG_SZ	C:\Temp\MailArchive
EmlDirectory	REG_SZ	C:\inetpub\mailroot\Drop
NoOfLinesFromT...	REG_SZ	100
XMLConfigFilePa...	REG_SZ	C:\Temp\scom.Addons.MailIn.MonitorItemList.xml

Import the Management Pack

In the SCOM Console, choose the Administration section, choose Management Packs and click on Import Management Packs.



Add the SCOM.Addons.MailIn.mpb file from your downloads folder and import it.



Name	Version	Release Date	Status	License Terms
✓ SCOM Addons MailIn	1.0.0.133			

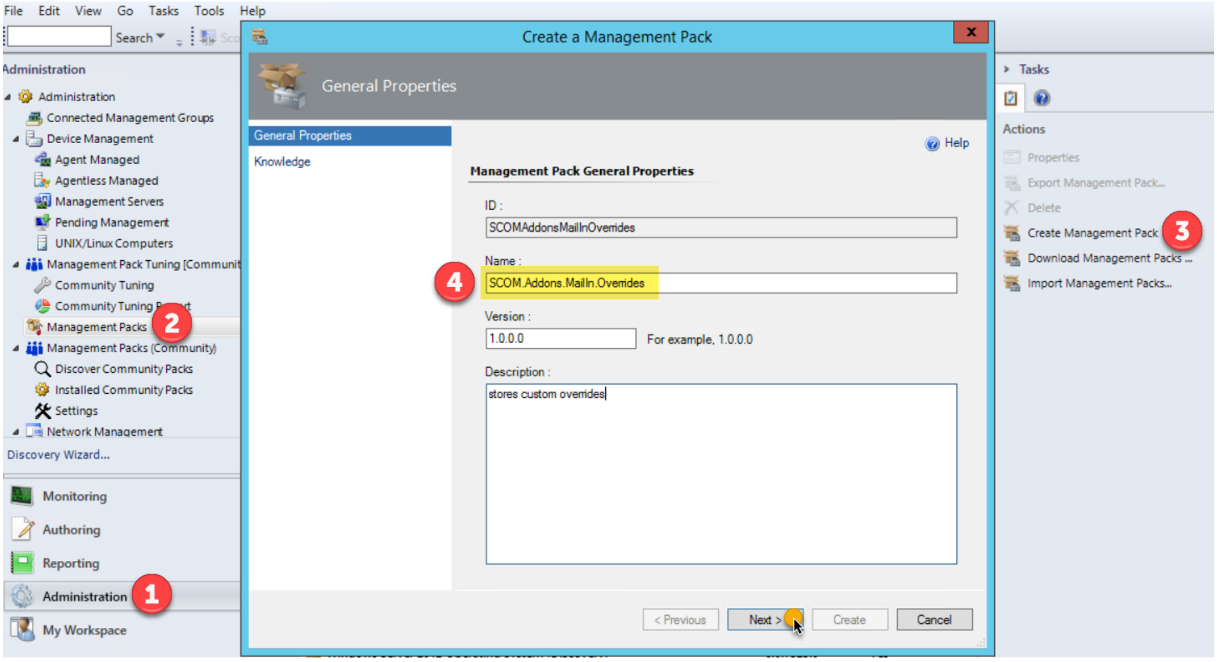
Status details :

This management pack is ready to import.

Proceed the wizard by confirming defaults.

Create an override Management Pack

Still in Administration, Management Packs, click on Create and name it SCOM.Addons.MailIn.Overrides to store customizations.



ID : SCOMAddonsMailInOverrides

Name : SCOM.Addons.MailIn.Overrides

Version : 1.0.0.0 For example, 1.0.0.0

Description : stores custom overrides

Follow the wizard by confirming defaults.

Configure mail-match-patterns in XML file for explicit monitors

Create a file named **SCOM.Addons.MailIn.MonitorItemList.xml** and store in C:\Temp for example and configure desired mail matching patterns.

A part of the text is enough for the match pattern. – E.g.:

```
Original subject: NYHKFW01
_IP:_10.25.10.21_changed_state_to_Down_on_Saturday,_May_9,_2020
Match pattern in XML: changed_state_to_Down

Original MailFrom: "APM-C-Test@abc.de"_<APM-C-Test@abc.de>
Match pattern in XML: APM-C-Test@abc.de
```

The patterns are used to created objects and monitors will then be triggered if an email, that matches the description arrives.

At least 2 items must match to let SCOM create the object (MailMonitor Item).
The logic will try to match any specified information.
More values are specified in the XML will reflect in more concrete objects and matching
Less values will make the matching not so accurate so to react more flexible on alerts, e.g. need to have for any message that was send by the air-condition system.

In regards of the minimum of 2 items match that means for example:

- Mail-From & Mail-Subject matches
- Mail-SourceServer & Mail-Subject matches
- Mail-From & Mail-Subject & Mail-SourceServer matches

The XML file could look like this:

```xml
<MailInMonitorList>
        <MailMonitorItem>
                <UniqueTitle>P360 APM Issue</UniqueTitle>
                <Description>Application errors in TEST system</Description>
                <MailFrom>APM-C@yourcompany.abc</MailFrom>
                <MailSubject></MailSubject>
                <MailBody></MailBody>
                <MailSourceServer>Linux05</MailSourceServer>
                <SCOMAlertResetType>Manual</SCOMAlertResetType>
                <SCOMAlertResetTimeInSeconds></SCOMAlertResetTimeInSeconds>
        </MailMonitorItem>
        <MailMonitorItem>
                <UniqueTitle>SAP Auto Job Error</UniqueTitle>
                <Description>Auto booking table issue</Description>
                <MailFrom>NightJobber</MailFrom>
                <MailSubject>ZLAS_STATUS</MailSubject>
                <MailBody></MailBody>
                <MailSourceServer>SAPAppSrv05</MailSourceServer>
                <SCOMAlertResetType>Timer</SCOMAlertResetType>
                <SCOMAlertResetTimeInSeconds>7200</SCOMAlertResetTimeInSeconds>
        </MailMonitorItem>
</MailInMonitorList>
```

The first line and last line are needed to indicate start and end of the object list.

- **UniqueTitle*** is the key property and must be unique. It should be short and descriptive.
- **Description** is only for usability to store information for those who check in SCOM
- **MailFrom*** either text of From field text or the sender email address
- **MailSubject*** text that is found in the mail subject
- **MailBody** text that may be found in the body
- **MailSourceServer** server or device that sends the email to SCOM
- **SCOMAlertResetType** set it to Timer or Manual to influence how this object should be monitored;
    - Timer : Monitor will be forced to reset after threshold (SCOMAlertResetTimeInSeconds) reached. -> Object is healthy again
    - Manual: Monitor keeps in Error / Warning state until a SCOM Admin does the reset
- **SCOMAlertResetTimeInSeconds** applies when Timer is specified as SCOMAlertResetType – value must be bigger than 900 (15 minutes) to avoid resource exhaust in SCOM.

(*) – must contain values, of not item will be ignored

Mail routing to receive alert E-Mails via e-mail address

After completing the steps above, SCOM can receive mails and creates alerts only if the SCOM server is specified as SMTP server for the sending device (server, application, etc.).

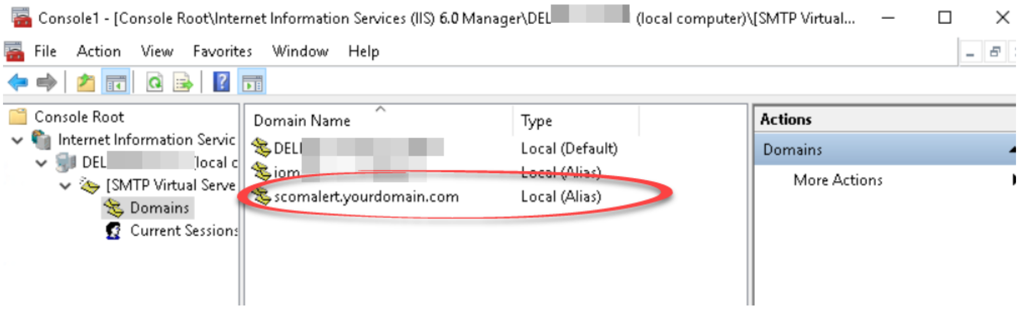
To be more flexible, mail routing can be customized so that only an email address for the SCOM servers is required.

Example:

1. **Create a DNS Alias (CName):** scomalert.yourdomain.com which points to scomserver.yourdomain.com

2. **In Exchange, use SendConnector:** to specify that scomalert.yourdomain.com will be send to the **SmartHost** scomserver.yourdomain.com

3. **In the SMTP Service**: add additional alias domains to receive e-mails for scomalert.yourdomain.com



Console1 - [Console Root\Internet Information Services (IIS) 6.0 Manager\DEL[redacted] (local computer)\[SMTP Virtual...

Domain Name	Type
DEL[redacted]	Local (Default)
iom[redacted]	Local (Alias)
scomalert.yourdomain.com	Local (Alias)

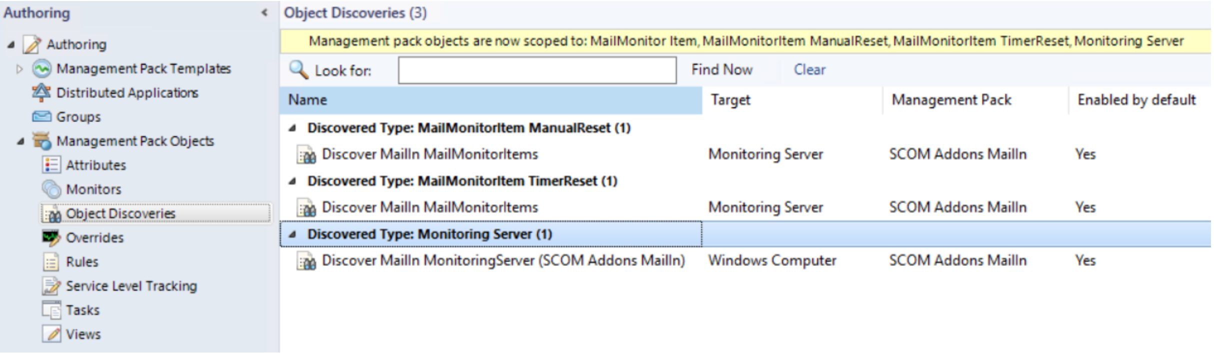
Adding Alias Domains in SMTP Server configuration

Now you can use anyText@scomalert.yourdomain.com on your sender and the mail routing will take care that the messages are delivered to SCOM.

Management Pack Components

Discoveries

Everything in SCOM that has a health state is an object. Instead of checking all Windows computers whether those files exist, we define a dedicated computer class.



Management pack objects are now scoped to: MailMonitor Item, MailMonitorItem ManualReset, MailMonitorItem TimerReset, Monitoring Server

Name	Target	Management Pack	Enabled by default
Discovered Type: MailMonitorItem ManualReset (1)			
Discover MailIn MailMonitorItems	Monitoring Server	SCOM Addons MailIn	Yes
Discovered Type: MailMonitorItem TimerReset (1)			
Discover MailIn MailMonitorItems	Monitoring Server	SCOM Addons MailIn	Yes
Discovered Type: Monitoring Server (1)			
Discover MailIn MonitoringServer (SCOM Addons MailIn)	Windows Computer	SCOM Addons MailIn	Yes

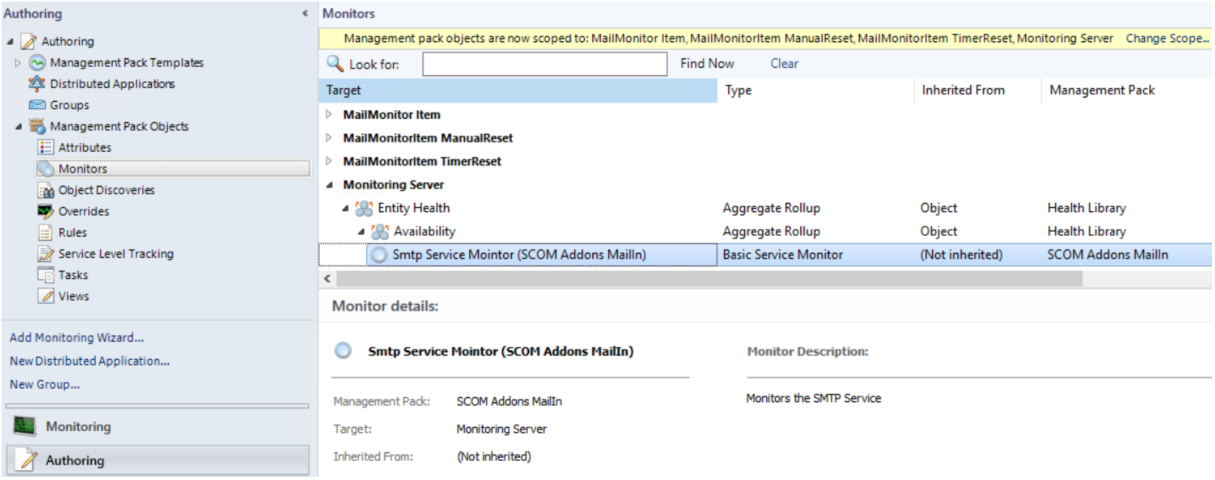
- **MailMonitorItem ManualReset:**
  - Items specified in SCOM.Addons.MailIn.MonitorItemList.xml which have set the SCOMAlertResetType as Manual.

- **MailMonitorItem TimerReset:**
  - Items specified in SCOM.Addons.MailIn.MonitorItemList.xml which have set the SCOMAlertResetType as Timer.

- **Monitoring Server:**
  - The registry keys mentioned in (Initial setup / Set registry keys) are used to set the SCOM Root Management Server as e-Mail server and target for discoveries, rules and monitors.

Monitors

Monitors are for finding out which Health State an object has. – An object can be either Healthy (green), in Warning (yellow) or Critical (red).



Management pack objects are now scoped to: MailMonitor Item, MailMonitorItem ManualReset, MailMonitorItem TimerReset, Monitoring Server   Change Scope...

Target	Type	Inherited From	Management Pack
MailMonitor Item			
MailMonitorItem ManualReset			
MailMonitorItem TimerReset			
Monitoring Server			
Entity Health	Aggregate Rollup	Object	Health Library
Availability	Aggregate Rollup	Object	Health Library
Smtp Service Mointor (SCOM Addons MailIn)	Basic Service Monitor	(Not inherited)	SCOM Addons MailIn

Monitor details:

Smtp Service Mointor (SCOM Addons MailIn)

Management Pack: SCOM Addons MailIn

Target: Monitoring Server

Inherited From: (Not inherited)

Monitor Description:

Monitors the SMTP Service

MailMonitor Item

- No direct monitor. Appears here because it is the base class of Manual- and TimerReset MailMonitor Items.

MailMonitorItem Manual Reset

- Reacts if an incoming email matches the configured pattern in the XML file.
- The SCOM administrator needs to reset this monitor manually.
- By default, this monitor runs every 5 minutes

MailMonitoritem Timer Reset

- Raises if an incoming email matches the configured pattern in the XML file.
- After the specified threshold in the XML file reaches, the monitor is reset when it’s checked the next time. In other words; the threshold is only checked when the monitor runs which is by default every 5 minutes.

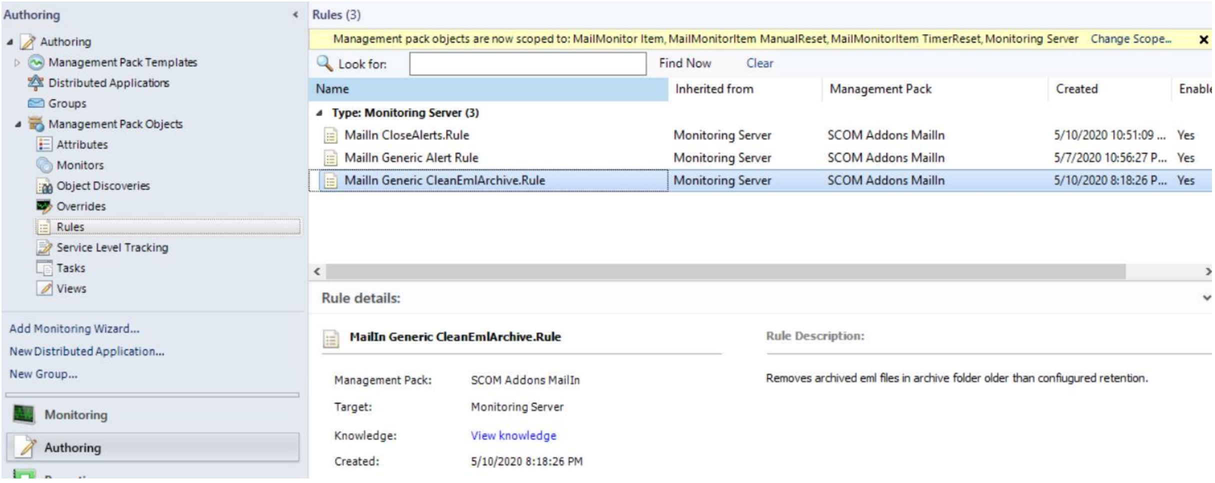
Monitoring Server

- Monitors the Windows SMTP Service

Note: XML file = **SCOM.Addons.MailIn.MonitorItemList.xml**

Rules

In this Management Packs rules perform alerting and cleanup jobs to avoid manual maintenance. Main parameters of the rules can be changed via override.



Management pack objects are now scoped to: MailMonitor Item, MailMonitorItem ManualReset, MailMonitorItem TimerReset, Monitoring Server

Name	Inherited from	Management Pack	Created	Enabl
Type: Monitoring Server (3)				
MailIn CloseAlerts.Rule	Monitoring Server	SCOM Addons MailIn	5/10/2020 10:51:09 ...	Yes
MailIn Generic Alert Rule	Monitoring Server	SCOM Addons MailIn	5/7/2020 10:56:27 P...	Yes
MailIn Generic CleanEmlArchive.Rule	Monitoring Server	SCOM Addons MailIn	5/10/2020 8:18:26 P...	Yes

MailIn Generic CleanEmlArchive.Rule

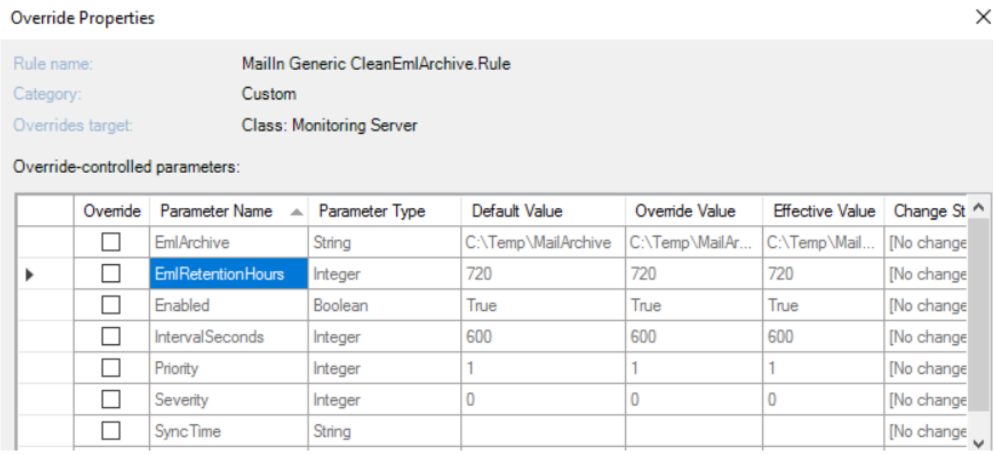
Management Pack: SCOM Addons MailIn
Target: Monitoring Server
Knowledge: View knowledge
Created: 5/10/2020 8:18:26 PM

Rule Description:

Removes archived eml files in archive folder older than confiugured retention.

MainIn Generic CleanEmlArchive Rule

- After an email was processed the EML message will be moved to an archive folder which by default is C:\Temp\EmlArchive.
- All EML files older than 720 hours (30 days) will be deleted.



Rule name: MailIn Generic CleanEmlArchive.Rule
Category: Custom
Overrides target: Class: Monitoring Server

Override-controlled parameters:

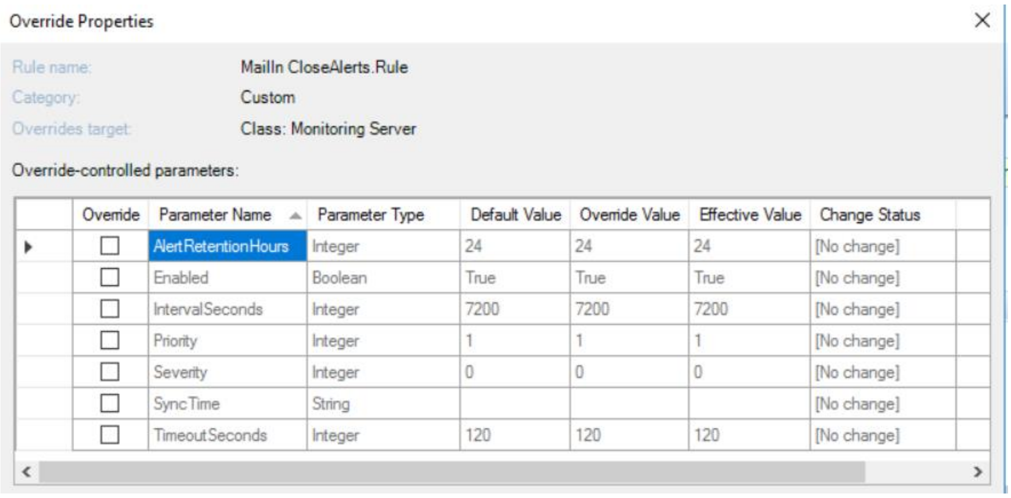
	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change St
	☐	EmlArchive	String	C:\Temp\MailArchive	C:\Temp\MailAr...	C:\Temp\Mail...	[No change
▶	☐	EmlRetentionHours	Integer	720	720	720	[No change
	☐	Enabled	Boolean	True	True	True	[No change
	☐	IntervalSeconds	Integer	600	600	600	[No change
	☐	Priority	Integer	1	1	1	[No change
	☐	Severity	Integer	0	0	0	[No change
	☐	SyncTime	String				[No change

MailIn Generic Alert Rule

- If an incoming email does not match the pattern configured in the XML file a warning alert will be created
- If preferred warning can be changed to critical and the check interval can be checked as well.

MailIn Close Alerts Rule

- To reduce the manual effort of closing alerts of the rule above, this rule will perform closure after a customizable value



Override Properties

Rule name: MailIn.CloseAlerts.Rule

Category: Custom

Overrides target: Class: Monitoring Server

Override-controlled parameters:

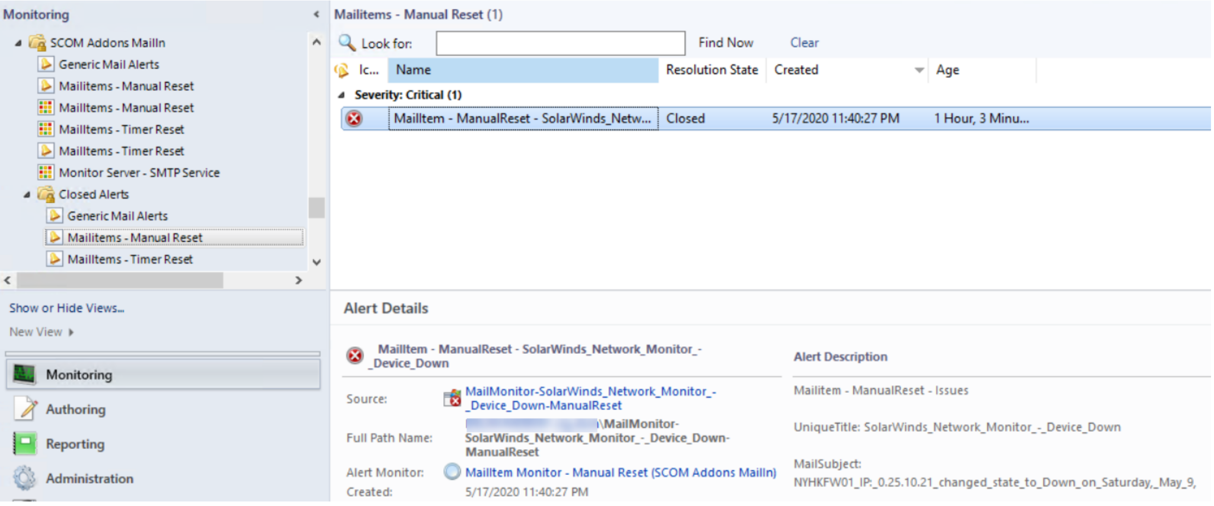
	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
▸	□	AlertRetentionHours	Integer	24	24	24	[No change]
	□	Enabled	Boolean	True	True	True	[No change]
	□	IntervalSeconds	Integer	7200	7200	7200	[No change]
	□	Priority	Integer	1	1	1	[No change]
	□	Severity	Integer	0	0	0	[No change]
	□	SyncTime	String				[No change]
	□	TimeoutSeconds	Integer	120	120	120	[No change]

Note: XML file = **SCOM.Addons.MailIn.MonitorItemList.xml**

Views

To make all discovered objects and their health state visible a state views are used.

The Closed Alerts subfolder helps to check information about last closures.



Ic...	Name	Resolution State	Created	Age
Severity: Critical (1)				
	MailItem - ManualReset - SolarWinds_Netw...	Closed	5/17/2020 11:40:27 PM	1 Hour, 3 Minu...

Alert Details

MailItem - ManualReset - SolarWinds_Network_Monitor_-_Device_Down

Source: MailMonitor-SolarWinds_Network_Monitor_-_Device_Down-ManualReset

Full Path Name: [redacted]\MailMonitor-SolarWinds_Network_Monitor_-_Device_Down-ManualReset

Alert Monitor: MailItem Monitor - Manual Reset (SCOM Addons MailIn)

Created: 5/17/2020 11:40:27 PM

Alert Description

MailItem - ManualReset - Issues

UniqueTitle: SolarWinds_Network_Monitor_-_Device_Down

MailSubject: NYHKFW01_IP:_0.25.10.21_changed_state_to_Down_on_Saturday,_May_9,

License Terms