

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.

The screenshot shows the SCOM Monitoring console with the 'Generic Mail Alerts (120)' view selected. The left pane shows the 'Monitoring' tree with 'SCOM Addons Mailin' expanded. The main pane displays a table of alerts with columns: Name, Resolution State, Created, and Age. Four alerts are listed, all with a 'Warning' severity and a resolution state of 'New'. The alert details pane shows the 'Mailin Generic Alert' details, including the source, full path name, alert rule, and alert description.

Name	Resolution State	Created	Age
Mailin Generic Alert (" pekups01@ lom" <c @ lom>)	New	5/12/2020 10:56:49 PM	7 Minutes
Mailin Generic Alert (" pekups01@ lom" <c @ lom>)	New	5/12/2020 10:56:49 PM	7 Minutes
Mailin Generic Alert (" pekups01@ lom" <c @ lom>)	New	5/12/2020 10:56:49 PM	7 Minutes
Mailin Generic Alert (" pekups01@ lom" <c @ lom>)	New	5/12/2020 10:56:49 PM	7 Minutes

Alert Details

Mailin Generic Alert
(" lom" <cn lom>)

Source: [redacted]
Full Path Name: [redacted]
Alert Rule: Mailin Generic Alert Rule
Created: 5/12/2020 10:56:49 PM

Alert Description

From: [redacted]
Subject: System_Detected_an_unauthorized_user_attempting_to_access_the_SNMP_interfac...
Body: Name : [redacted]PEKUPS01
Location : Beijing Office
Contact : bot [redacted]

The screenshot shows the SCOM Monitoring console with the 'MailItems - Manual Reset (1)' view selected. The left pane shows the 'Monitoring' tree with 'SCOM Addons Mailin' expanded. The main pane displays a table of alerts with columns: Name, Resolution State, Created, and Age. One alert is listed with a 'Critical' severity and a resolution state of 'New'. The alert details pane shows the 'MailItem - ManualReset - Plant360_APM_PROD_Issue' details, including the source, full path name, alert monitor, and alert description.

Name	Resolution State	Created	Age
MailItem - ManualReset - Plant360_APM_PROD_Issue	New	5/9/2020 11:42:14 PM	2 Days, 23 Hour...

Alert Details

MailItem - ManualReset - Plant360_APM_PROD_Issue

Source: MailMonitor-Plant360_APM_PROD_Issue-ManualReset
Full Path Name: MailMonitor-Plant360_APM_PROD_Issue-ManualReset
Alert Monitor: MailItem Monitor - Manual Reset (SCOM Addons Mailin)
Created: 5/9/2020 11:42:14 PM

Alert Description

MailItem - ManualReset - Issues
UniqueTitle: Plant360_APM_PROD_Issue
MailSubject: Task_Extraction_Wrapper_failed.
MailFrom: "APM-C-PROD@ [redacted]" <APM-C-PROD@ [redacted]>
MailBody: The task "Extraction_Wrapper" has failed. Project: UNIFIED_PLATFORM_GIT Job name: Extraction_Wrapper Job version: 0.1 Context: Default Execution server: localhost

Change History

Date	Build No.	Changes
2020-05-13	1.0.0.140	Initial Upload to GitHub

Contents

Change History.....	1
Initial setup.....	2
Install and configure SMTP service	3
Set registry keys	5
Import the Management Pack.....	6
Create an override Management Pack.....	7
Configure mail-match-patterns in XML file for explicit monitors	8
Mail routing to receive alert E-Mails via e-mail address	10
Management Pack Components	11
Discoveries	11
Monitors	12
Rules.....	13
Views.....	15
License Terms	16

Initial setup

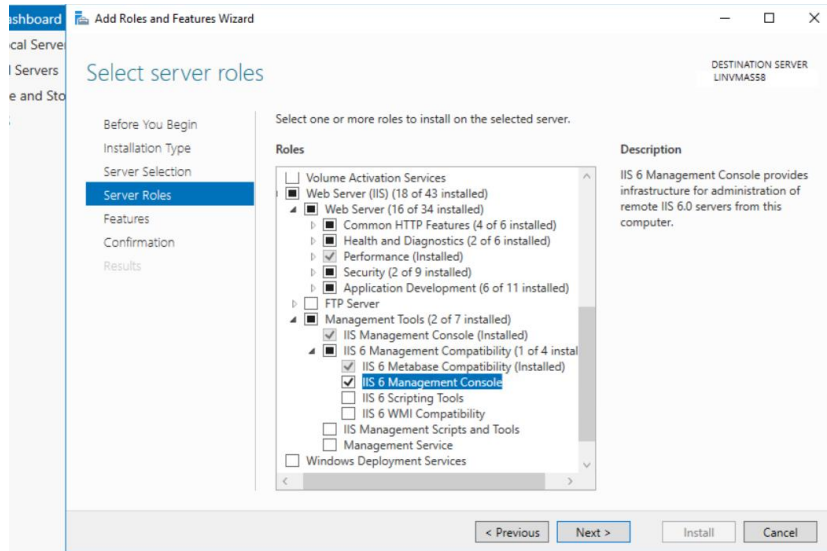
The following steps on the **SCOM Root Management Server** are required.:

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

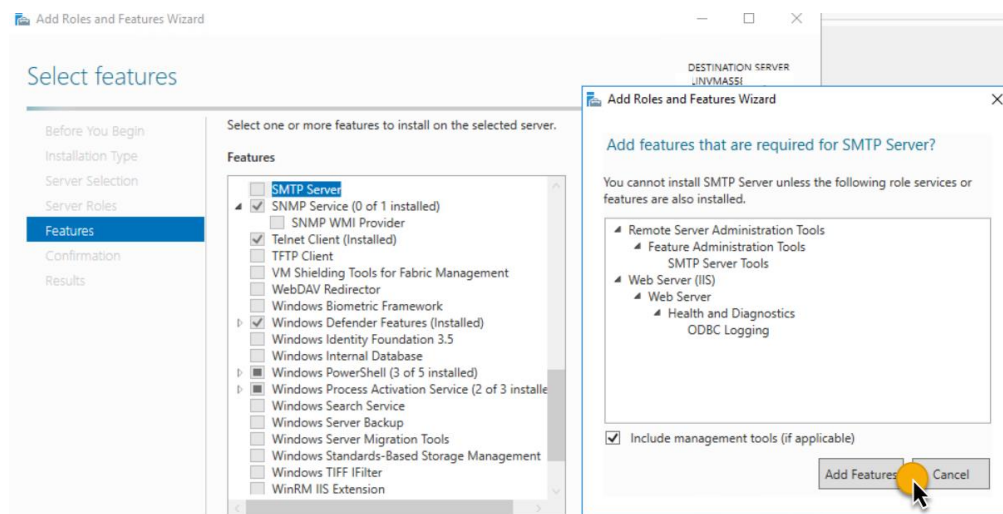
Install and configure SMTP service

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

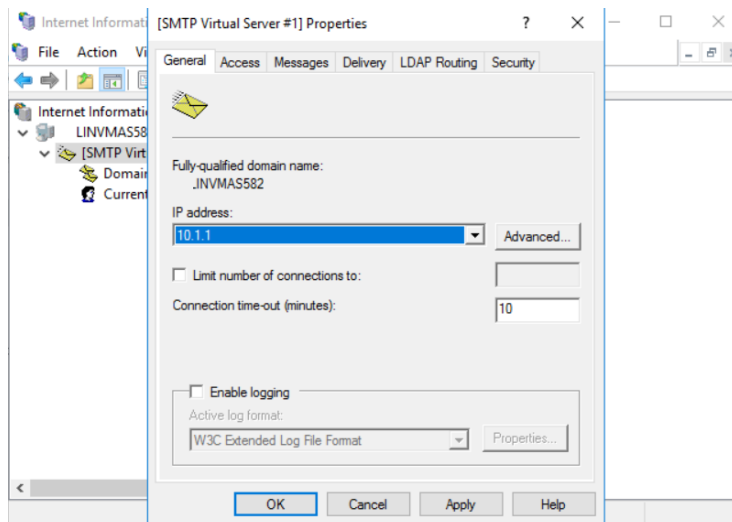


Next, adding **SMTP Server** and IIS ODBC Logging features

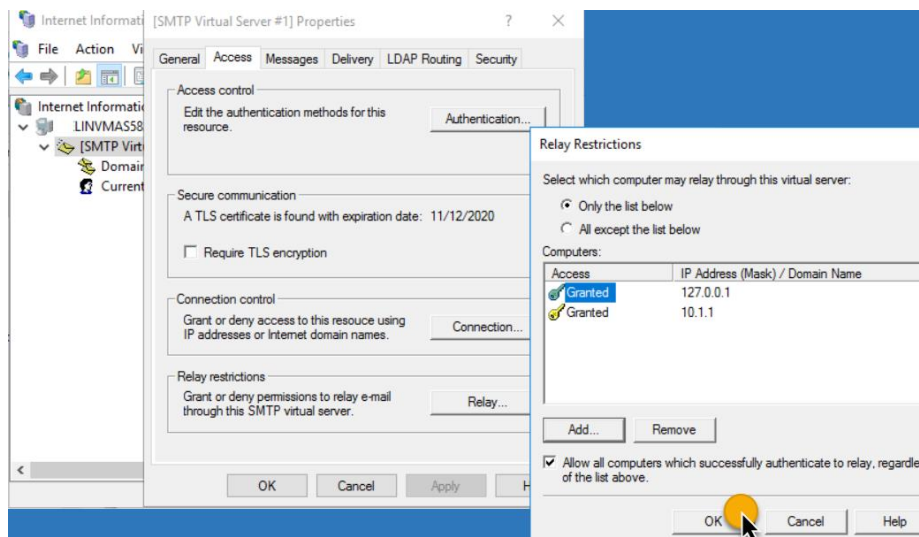


After installation, a restart may be required.

Next, open the IIS 6 MMC and specify the SMTP Virtual Servers' listing IP address.



Finish the SMTP service config by **restricting SMTP service relay** to own IP addresses



Set registry keys

Registry keys store basic information about the SMTP service. For convenience, paste the text in the yellow box into notepad and save 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 in the yellow box is the default location.

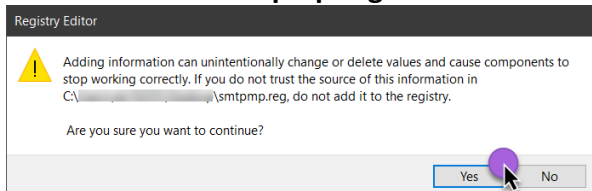
EmlArchive:

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

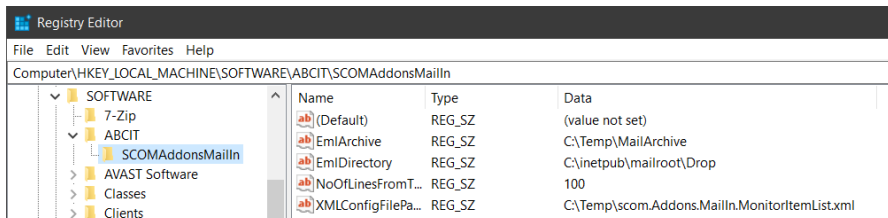
NoOfLinesFromTop:

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:

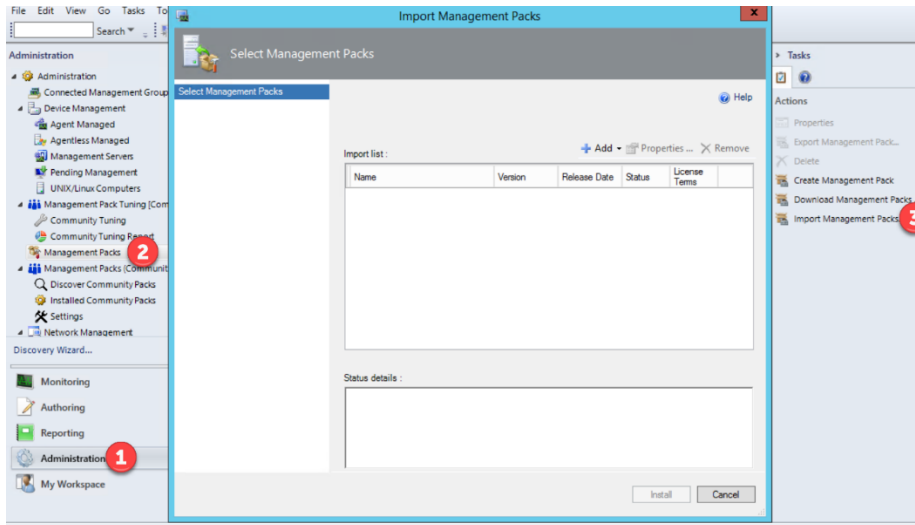


After importing the settings in the registry will look as follows:

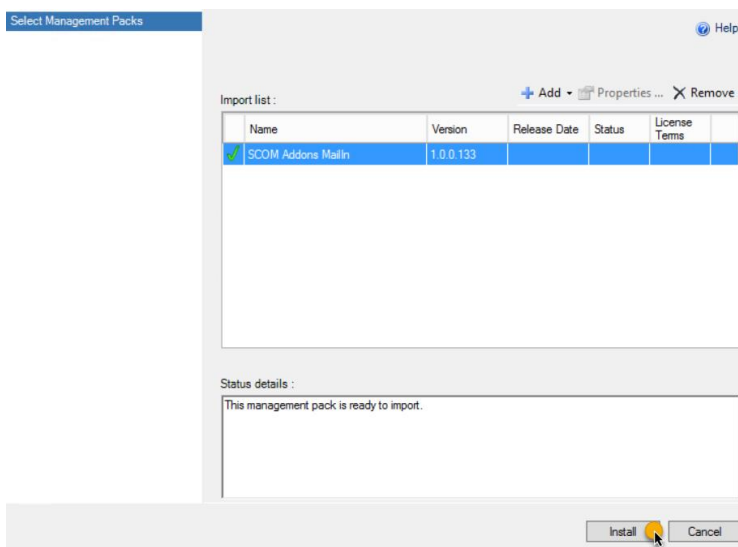


Import the Management Pack

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



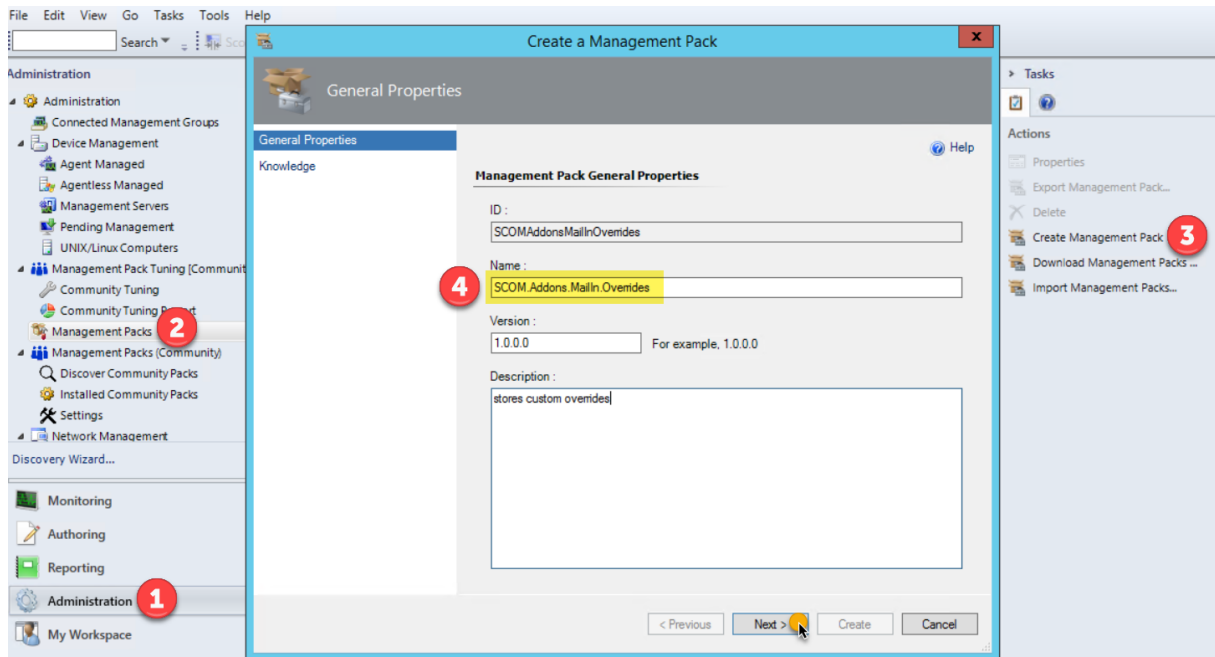
Add the SCOM.Addons.MailIn.mpb file from your downloads folder and import it.



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.



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:

```
<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;
 - o **Timer** : Monitor will be forced to reset after threshold (SCOMAlertResetTimeInSeconds) reached. -> Object is healthy again
 - o **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.

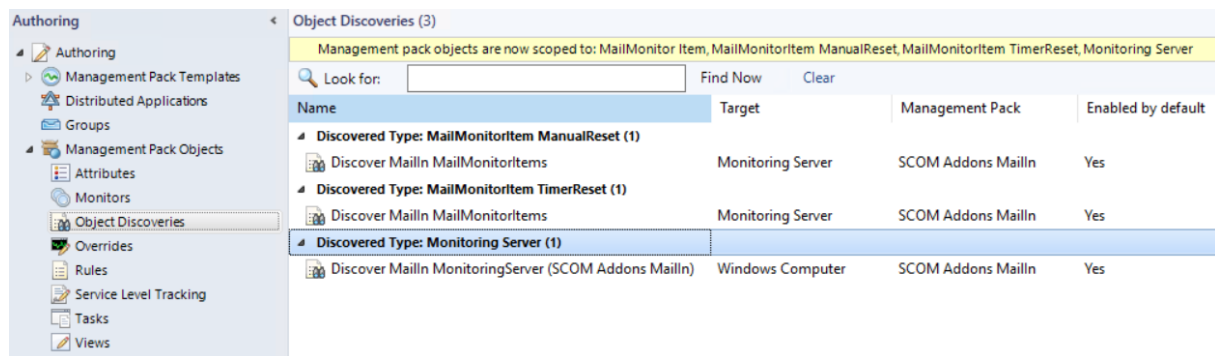
Example:

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. 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.



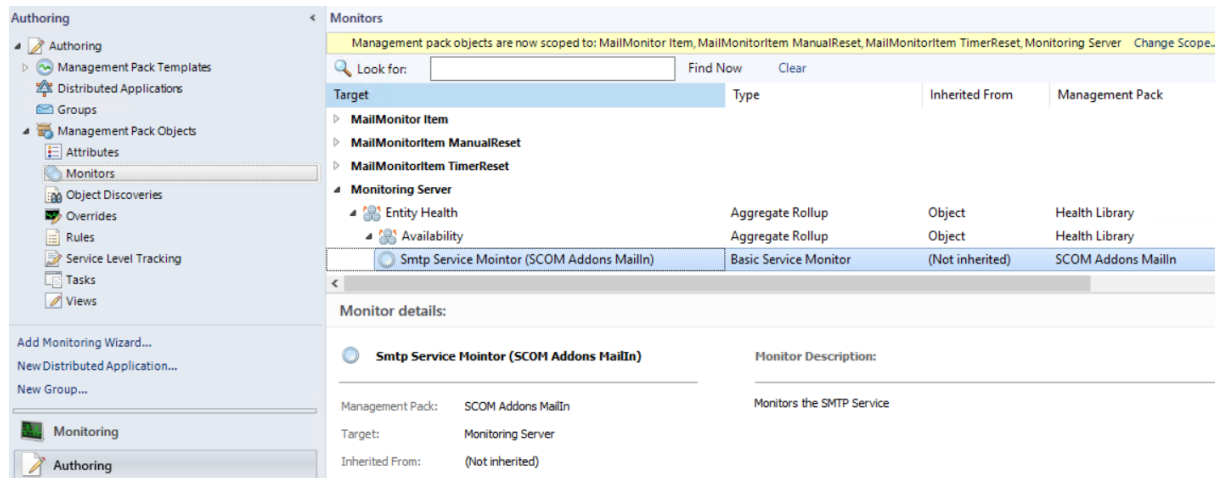
The screenshot shows the 'Authoring' console in SCOM. The left pane shows the 'Object Discoveries' node selected under 'Management Pack Objects'. The right pane displays a table of discovered objects. A yellow banner at the top states: 'Management pack objects are now scoped to: MailMonitorItem, MailMonitorItem ManualReset, MailMonitorItem TimerReset, Monitoring Server'. Below this is a search bar with 'Find Now' and 'Clear' buttons. The table has four columns: Name, Target, Management Pack, and Enabled by default. It lists three discovered types: MailMonitorItem ManualReset (1), MailMonitorItem TimerReset (1), and Monitoring Server (1). Each type has one associated discovery task.

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).



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.

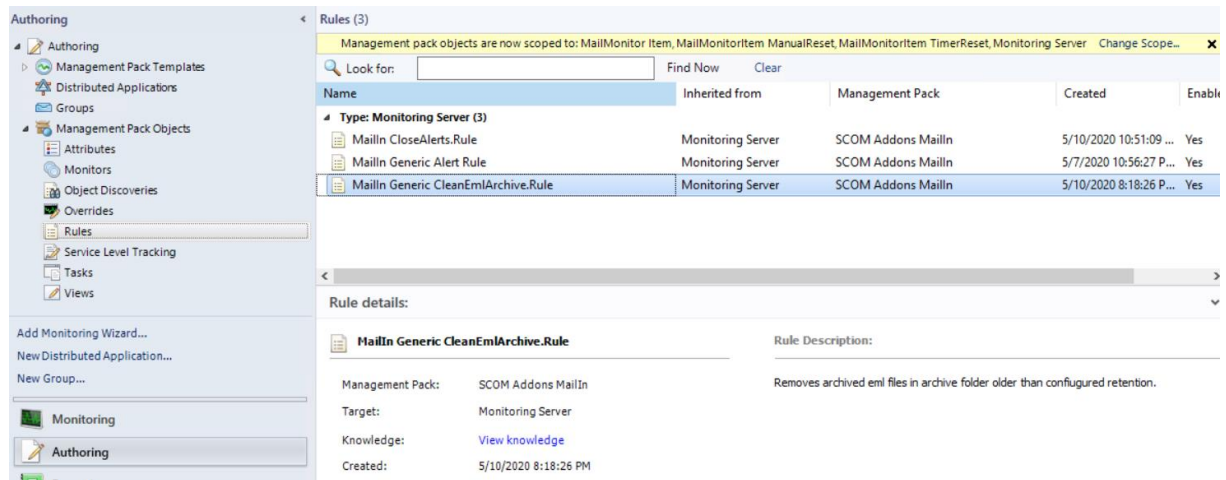
Monitoring Server

- Monitors the Windows SMTP Service

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

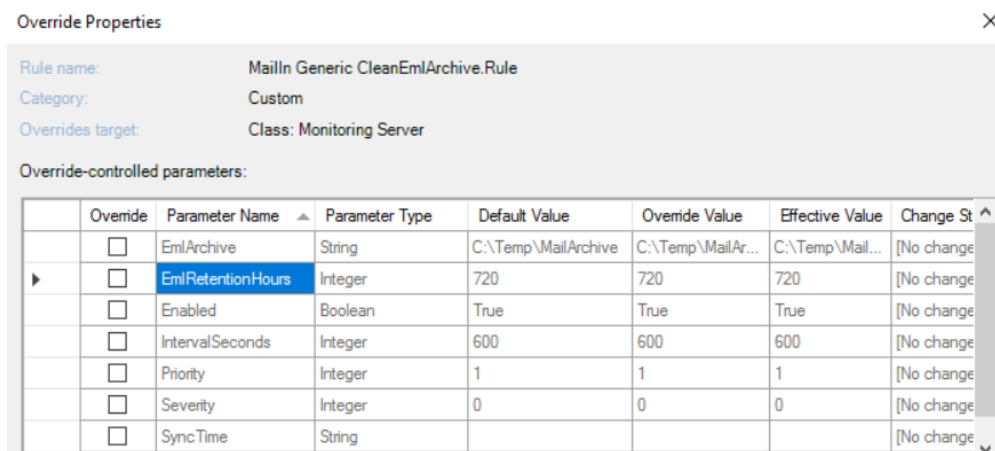
Rules

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



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.



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	
▶	<input type="checkbox"/>	AlertRetentionHours	Integer	24	24	24	[No change]	
	<input type="checkbox"/>	Enabled	Boolean	True	True	True	[No change]	
	<input type="checkbox"/>	IntervalSeconds	Integer	7200	7200	7200	[No change]	
	<input type="checkbox"/>	Priority	Integer	1	1	1	[No change]	
	<input type="checkbox"/>	Severity	Integer	0	0	0	[No change]	
	<input type="checkbox"/>	SyncTime	String				[No change]	
	<input type="checkbox"/>	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.

The screenshot shows the 'Monitoring' console with the 'Closed Alerts' subfolder selected. The main pane displays a list of alerts under the heading 'MailItems - Timer Reset (32)'. The list has columns for Name, Resolution State, Created, and Age. The alerts are all marked as 'Closed' and have a 'Severity: Critical'.

Name	Resolution State	Created	Age
Severity: Critical (32)			
MailItem - TimerReset - SAP_Aut...)_Transaction_Error	Closed	5/12/2020 6:57:14 PM	5 Hours, 9 Minutes
MailItem - TimerReset - SAP_Aut...)_Job_Error	Closed	5/12/2020 5:47:14 PM	6 Hours, 19 Minutes
MailItem - TimerReset - SAP_Aut...)_Job_Error	Closed	5/12/2020 10:47:14 AM	13 Hours, 18 Minutes
MailItem - TimerReset - SAP_Aut...)_Transaction_Error	Closed	5/12/2020 10:17:14 AM	13 Hours, 48 Minutes
MailItem - TimerReset - Plant360_APM_Test_Issue	Closed	5/12/2020 5:12:14 AM	18 Hours, 53 Minutes
MailItem - TimerReset - Plant360 APM_Test_Issue	Closed	5/11/2020 2:27:14 PM	1 Day, 9 Hours, 38 Min...

Alert Details

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

License Terms

SCOM Addons MailIn Copyright (C) 2020 Ruben Zimmermann (Juanito99)

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.