

IBM ECM System Monitor Field Guides

Integration with Message Channels

August 29th, 2023 CENIT AG Michael Wohland

Content

Introduction	3
Overview	3
Disclaimer	3
Purpose of this guide	4
Requirements	4
Step by Step setup	5
1. Prepare the message channel to accept webhooks	5
2. Preparing the JSON for forwarding the ESM information1	1
3. Setting up the Task13	3
Contact Information	0

Introduction

Overview

This guide describes in detail, how IBM ECM System Monitor (ESM) can be integrated with Message Channels to forward ESM incidents.

Disclaimer

The content of this document is based on ESM Version 5.5.9.1-000. The descriptions and guidelines in this document are for informational purposes only. Up-to-dateness, content completeness, appropriateness and validity for all possible scenarios cannot be guaranteed. All information is provided on an as-is basis. The author is not liable for any errors or omissions in this document or any losses, injuries and damages arising from its use.

If you are planning to setup or configure ESM or to adjust an existing installation, it is absolutely necessary to take into account current security whitepapers, release notes and announcements from the official IBM ECM System Monitor product documentation website.

Purpose of this guide

Message Channels are more and more used to interact as a team. These channels can be filled with incident information that is collected by ESM. Every member of the team is informed and the team can react and decide what to do with this information.

Requirements

- ESM Version 5.5.9.1-000 (already installed) any ESM Version that has the Webhook
- Task integrated should work
- Availability of a message channel (e.g. MS Teams or Slack)

Step by Step setup

1. Prepare the message channel to accept webhooks

Example for MS Teams:

For MS Teams there is a webpage available that describes how an incoming webhook connector can be set up for channels. The page URL is:

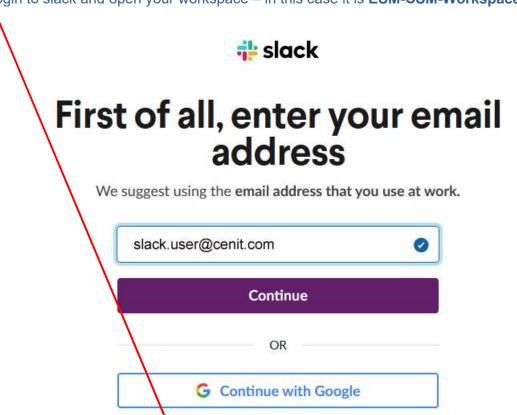
https://learn.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/howto/add-incoming-webhook?tabs=dotnet

At some point of the setup you will receive a webhook URL, which you need for the integration with ESM. Note it or copy it to a document. The URL looks like this:

https://cenitgroupglobal.webhook.office.com/webhookb2/baa589c7-5f5b-4a9d-89d3-7a4cbab7b71b@ce368477-a736-4353-b4ef-741ef2740d36/IncomingWebhook/343157e99ad946e5a166dd1d8ab5c8e7/a6858fdd-a65f-4093-867b-45a5958a51f1 Example for Slack:

For creating a workspace in slack there is a "how to" available.

The page URL is: <u>https://slack.com/help/articles/206845317-Create-a-Slack-workspace</u> Login to slack and open your workspace – in this case it is **ESM-CSM-Workspace**.



Continue with Apple

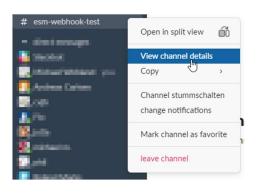
Already using Slack? Sign in to an existing workspace Once you have signed in, you can create a new channel or use an already existing one. For a new one, select the drop down at Channels and specify Create -> Create Channel:

Þ	Channels ~	0.	second of sind one ary produity by
#	Create	× b	Create channel
-	Administer	>	Create a sidebar folder PAID 🖉

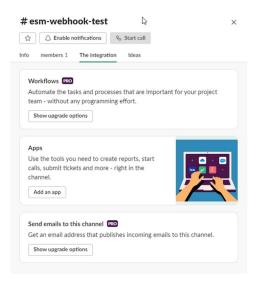
Specify a name and create:

create channel	s	×
Channels are used by your to be topic-related - #marketing	eam to communicate. Ideally, ng, for example.	, they should
🐣 Discourrissionaly 1990	unipriite a deared, and a	1997
Name	\square	
# esm-webhook-test	d	64
Description (optional)		
What is this channel about?		
Set to "Closed". When a channel is converte channel, viewing and joining		
		Create

Right click on the channel and specify "View channel details":



In the next window that opens, select the integration tab and click on "Add an app":



In the next window that opens, select "Opinion" next to Incoming Webhook:

# e	os too esm-webhook-test l to	View App Directory
Q S	earch by name or category (e.g. Productivity, Sales)	
n your wo	rkspace (12)	
	Jenkins Custom Slack Bot Jenkins Custom Slack Bot	Add to
	Giphy An online library of animated GIFs	Opinion
	Pulled off GitHub's scriptable chat bot.	Add to
	CENIT Webhook Easy way to send messages to different channels	Opinion
	sm	Add to
	Watson Watson Assistant Claims Accident Insurance (TEST)	Add to
	Jenkins Cl An open source continuous integration server.	Opinion
	Incoming WebHooks Send data into Slack in real-time.	Opinion

Then select configuration:

Incoming webhooks

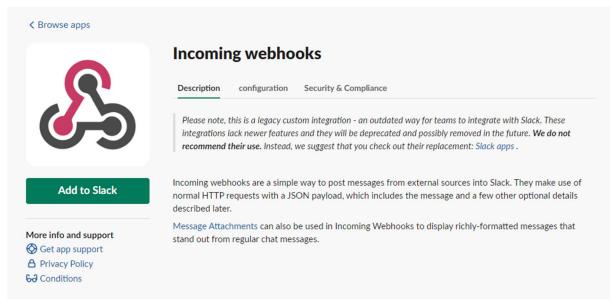


Incoming webhooks
Please note, this is a legacy custom integration - an outdated way for teams to integrate with Slack. These integrations lack newer features and they will be deprecated and possibly removed in the future. We do not
recommend their use. Instead, we suggest that you check out their replacement: Slack apps.

Incoming Webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details described later.

Message Attachments can also be used in Incoming Webhooks to display richly-formatted messages that stand out from regular chat messages.

Add to slack:



Select the channel that was just created or that you want to use for forwarding the info:



Incoming webhooks

Send data into Slack in real time.

Please note, this is a legacy custom integration - an outdated way for teams to integrate with Slack. These integrations lack newer features and they will be deprecated and possibly removed in the future. **We do not recommend their use.** Instead, we suggest that you check out their replacement: Slack apps.

Incoming webbooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details described later.

Message Attachments can also be used in Incoming Webhooks to display richly-formatted messages that stand out from regular chat messages.

∧ New to Slack integrations?

Check out our getting started guide to familiarize yourself with the most common integrations. You will also get a lot of tips that you should keep in mind when developing. You can also register as a developer to let us know what you're working on and to receive future updates on our APIs.

Start by choosing a channel for your	Wähle einen Channel		~
incoming webhook to post messages to.	Choose a channel		
	o Michael Wohland Michael Wohland		
	# generally		-
	• Andreas Carlsen Andreas Carlsen		
	• cvjb Christian Brussow		
	# esm webhook test	J.	
	• Flo Flo		
	# Freudenberg		

Click on "Add inbound webhooks integration":

Post to channel Start by choosing a channel for your	# esm webhook test ~
ncoming webhook to post messages	
0.	orcreate new channel
\searrow	
	Add inbound webhooks integration
	When you create an incoming webhook, you agree to the Slack API Terms of

The final page shows the Webhook URL along with other useful information such as possible message designs – Note the Webhook URL down:

Your workspace has reach	hed the maximum number of integrations. Upgrade your plan to get unlimited integration	ons.
Added by Michael Wohl		tivate • Removed
	om integration - an outdated way for teams to integrate with Slack. These integrations lack no emoved in the future. We do not recommend their use. Instead, we suggest that you check o	
	way to post messages from external sources into Slack. They make use of normal HTTP e message and a few other optional details described later.	requests with a
lessage Attachments can also be nessages.	e used in Incoming Webhooks to display richly-formatted messages that stand out from	regular chat
A New to Slack integrations	5?	
	rted guide to familiarize yourself with the most common integrations. You will also get a n developing. You can also register as a developer to let us know what you're working or ls.	
should keep in mind when future updates on our API Setup Guide	n developing. You can also register as a developer to let us know what you're working or	and to receive
should keep in mind when future updates on our API Setup Guide We'll walk you through all the	n developing. You can also register as a developer to let us know what you're working or Is.	and to receive

2. Preparing the JSON for forwarding the ESM information

Example for MS Teams:

For MS Teams it is possible to define a variety of JSON strings with different designs for the information that is forwarded. In this example here I am using the so called "Message Card" format. Again you can find more information for the creation of such cards in this URL from Microsoft:

https://learn.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/connectors-using?tabs=cURL

Message Card example for MS Teams:

```
"@type": "MessageCard",
 "@context": "http://schema.org/extensions",
 "title": "ESM - Incident created",
"themeColor": "0076D7",
 "summary": "ESM Webhook Test",
 "sections": [{
     "title": "$Situation.name - $Severity",
     "facts": [{
         "name": "Timestamp",
         "value": "$Sample.Timestamp"
     }, {
    "name": "Message",
    "^Message"
         "value": "$Message"
    "value": "$Error"
     }, {
    "name": "Value:",
    "^value"
         "value": "$Value"
     }],
     "startGroup": true,
     "markdown": true
}1,
"potentialAction": [{
   "@type": "OpenUri",
"name": "Connect to ESM Server",
    "targets": [{
            "os": "default",
             "uri": "https://myESMServer:9443/"
        }]
}]
```

As you can see in the facts section, there are name/value pairs. The name will be shown as identifier and the value is the related information from ESM. The \$Something is replaced with the actual information from the incident. This section can be enhanced as you need it.

Create a single line out of the above for later usage:

{ "@type": "MessageCard", "@context": "http://schema.org/extensions", "title": "ESM - Incident created", "themeColor": "0076D7", "summary": "ESM Webhook Test", "sections": [{ "title": "\$Situation.name - \$Severity", "facts": [{ "name": "Timestamp", "value": "\$Sample.Timestamp" }, { "name": "Message", "value": "\$Message" }, { "name": "Error:", "value": "\$Error" }, { "name": "Value:", "value": "\$Value" }], "startGroup": true, "markdown": true }], "potentialAction": [{ "@type": "OpenUri", "name": "Connect to ESM Server", "targets": [{ "os": "default", "uri": "https://myESMServer:9443/" }] }]

Example for Slack:

Single line example based on the message design from the final page when creating the Webhook URL above:

```
{ "text": "myservername | $Sample.Timestamp| $Severity| $Value| $Message| $Error| Classification"}
```

3. Setting up the Task

Example for MS Teams:

Open the ESM Console and switch to the configuration part. Select task in the left bar and click on the + next to WebHookExportIncident to create a new task:

	sm × +				~	- 0	×
← -	→ C A Nicht sicher https://smccos8esm552.de.	enit-group.com/#/config	juration/tasks		■ @ ☆	* 🗆 😩	
CEI	ENIT AG 🚺 10.10.0.1 🦲 CPRE 🍿 FLUGHAFENTRANS	Nutzerkonto Bund	🕙 FileNet P8 Fix Pack 📒	Verein 📝 Mein Flightright Fl 🙇 WEB.D	E fairplay 📙 Winner 📒 AND-E		>
	1 ESM 9.1-000	Monitoring Cor	figuration Administratio	n Help	277	adn	mii
Con	nfiguration 🕽 🏟 Tasks						
«							<
2		W .					
	• Example	Œ					
th.	FileExportIncident	Œ					
T	MailExportIncident						
-	MonitoringConfigTemplate	E					
S.	OnDemandStartLibraryServer	Œ					
¢°	Task Configuration ObjectServer						
	OnDemandStopLibraryServer	Œ					
E	OnDemandStopObjectServer	Œ					
~	ProcessExecution	Œ					
	SnmpExportIncident	Œ					
	StatusMail	Œ					
	WebHookExportIncident	Elun -					

The default task setup looks like this. The given parameters must be overwritten:

	1 5 1
×<><⊙	
📽 Task Configuration	
Select the type of the task and enter	er its configuration data.
*Name	1
active	
Task:	WebHookExportIncident ~
Template:	{"text" : "\$Timestamp: \$Severity: \$Value \$Message \$Error "}
Webhook URL:	https://hooks.slack.com/services/ <t>//<x></x></t>
Authorization Header:	apiToken
& Agent Select the location where the Task	should run.
[Run on Server]	v
🛗 Schedule	
If active when and how often shoul	Id the Task be executed?
If active when and how often shoul	Id the Task be executed?
Interval O Cron Start:	v
Interval Cron Start: End:	

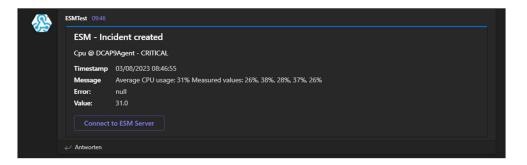
First specify a name and then overwrite the template with "single line" message card JSON we created in Part 2. Also overwrite the Webhook URL with the URL you have created in Part 1. Make sure you don't have any space in front or at the end of the entries. Do not make the task active, just save it with the button from above.

× < > <mark><</mark> 0			
Configuration			
Select the type of the task and ent	er its configuration data.		
*Name MyWebhookTest			
active			
Task:	WebHookExportIncid	ent	•
Template:	{ "@type": "MessageCare	I", "@context": "http://schen	na.org/extensions", "title":
Webhook URL:	https://cenitgroupglobal.v	vebhook.office.com/webhoo	kb2/baa589c7-5f5b-4a9d
Authorization Header:	apiToken		
& Agent Select the location where the Task	should run.		
[Run on Server]			-
Schedule	id the Task he succeded		
If active when and how often shou	id the task be executed?		
Interval O Cron			
Start: End:	•	*	
	Minute(s)	· ·	

You can now setup this task as automated task in any situation you like.

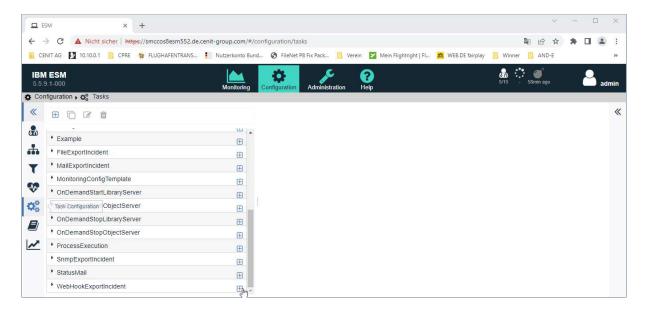
$x \leftrightarrow y$		00	
✿ Automation			
Trigger tasks automatically by occurrence of certain incidents.			
+			
Condition	Mode	Tasks	
All of: Severity >= Critical Situation == Cpu @ DCAP9Agent	First	 MyWebhookTest 	6

The output in MS Teams looks like this:



Example for Slack:

Open the ESM Console and switch to the configuration part. Select task in the left bar and click on the + next to WebHookExportIncident to create a new task:



The default task setup looks like this. The given parameters must be overwritten:

\times \langle \rangle \checkmark \odot	
📽 Task Configuration	
*	
Select the type of the task and enter its configuration data.	
*Name	
active	
Task: WebHookExportIncident	
Template: {"text" : "\$Timestamp: \$Severity: \$Value \$Message \$Error "}	
Webhook URL: https://hooks.slack.com/services/ <t>//<x></x></t>	
Authorization Header: apiToken	
& Agent	
Select the location where the Task should run.	
[Run on Server]	-
🛗 Schedule	
If active when and how often should the Task be executed?	
n active when and now often should the rask be executed?	
Interval O Cron	
Start:	
End:	
Interval: 10 🔶 Minute(s)	

First specify a name and then overwrite the template with "single line" JSON we created in Part 2. Also overwrite the Webhook URL with the URL you have created in Part 1. Make sure you don't have any space in front or at the end of the entries. Do not make the task active, just save it with the button from above. The "Authorization Header" might not be needed and can be removed.

x < > 🗸 O



*

Configuration

Select the type of the task and enter its configuration data.

*Name MyWebhookTest					
active					
	WebHookExportIncident	-			
Template:	{ "text": "myservername \$Sample.Timestamp \$Severity \$Value \$Message \$Error Classification"}				
Webhook URL:	https://hooks.slack.com/services/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				
Authorization Header:					

& Agent

Select the location where the Task should run.

[Run on Server]

🛗 Schedule

If active when and how often should the Task be executed?

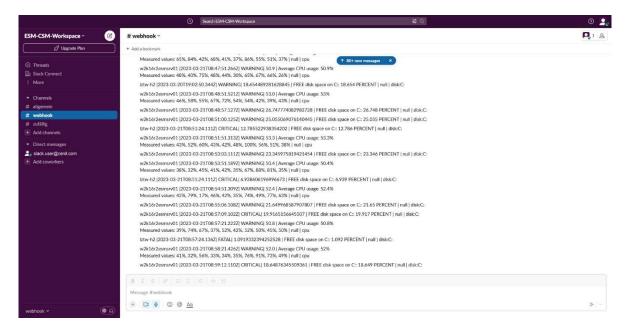
Interval O Cron

Start:		-		
End:		*		
Interval:	10 🌲	Minute(s)	-	

You can now setup this task as automated task in any situation you like.

IBM 5.5.9	ESM 9-000		Monitoring Configuration	n Hebo		🝰 🗰	💣 🔒	admin
Confi	uration 😻 Situations 🖿 All Situations							
«	8 C C C C Q V I	x < > ~	0	0 •		Cpu @ w2k1	S-cm36-agent	>>
	All Situations	os Automation				Probe		
		We Materiation				Name	Cpu @ w2k16-om86	
	😍 Cpu @ w2k16-cm86-agent	Trigger tasks automatically by occurrence of certain incidents.				Active Mode	METRIC	
T	👽 DatabaseConnectionStatus @ ICMNLSDB					Request Count	5	
-	👽 DatabaseConnectionStatus @ RMDB86	•				Callback	false	
	Diskspace_C_Drive @ w2k16-cm86-agent	Condition	Mode	Taska		Agent		
100	Diskspace_D_Drive @ w2k16-cm86-agent	All of: Severity >= Warning Situation == Cpu @ w2k16-cm86-agent	Always	WebHook	0 0	w2k16-cm86-egent		
	Diskspace_E_Drive @ w2k16-cm86-agent					Schedules Interval: 33 Second	dia)	
	-					Tags		
	Memory @ w2k16-cm86-agent					Agent: w2k16-om8i Subsystem: w2k16-	S-agent cm86-acent	
	😻 MemoryUsagePerProcess @ w2k16-cm86-agent					Probe: Cpu @ w2k	10-om80-agent	
	NumberOfFiles @ w2k16-cm86-agent					Casks CSNMPforward		
	👽 PingPeriod @ w2k16-cm86-agent					OCWebHook		
	👽 Process @ w2k16-cm86-agent							
	🐶 ProcessCount @ w2k16-cm86-agent							
	😯 ResourceManagerServices @ RM86							
	😵 ResourceManagerVolumeSpace @ RM86							
	👽 Swapspace @ w2k16-cm86-agent							
	👽 WmiQuery @ PoolPageBufferRequest							

Example of ESM-CSM-Workspace (configured and working)



Contact Information

If you have any questions, please contact us at ECM.SystemMonitor@cenit.com.

CENIT AG Phone: +49 711 7825 30 Email: <u>ECM.SystemMonitor@cenit.com</u>