IBM Resilient

Security Orchestration, Automation and Response Platform

SYMANTEC ENDPOINT PROTECTION INTEGRATION GUIDE v1.0.1

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2020. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Resilient Security Orchestration, Automation and Response Platform
Symantec Endpoint Protection Integration Guide

Version	Publication	Notes
1.0.1	November 2020	App Host support added.
1.0.0	August 2019	Initial publication.

Table of Contents

1. Overview ... 5
1.1. Use cases ... 6
2. Installation ... 7
2.1. Useful links ... 8
3. Package contents ... 9
4. Custom layout ... 12
5. Function descriptions ... 14
5.1. SEP - Scan Endpoints ... 14
5.2. SEP - Upload File to SEPM ... 18
5.3. SEP - Get File Content as Base64 ... 20
5.4. SEP - Get Computers ... 21
5.5. SEP - Move Endpoint ... 25
5.6. SEP - Quarantine Endpoints ... 27
5.7. SEP - Get Fingerprint List ... 29
5.8. SEP - Add Fingerprint List ... 31
5.9. SEP - Update Fingerprint List ... 32
5.10. SEP - Get Groups ... 32
5.11. SEP - Assign Fingerprint List to Group ... 34
5.12. SEP - Delete Fingerprint List ... 35
5.13. SEP - Get Command Status ... 36
5.14. SEP - Get Domains ... 41
6. Script description ... 42
7. Notifications description ... 43
7.1. Configuration ... 43
7.2. Generic email script ... 45
7.3. Script – scr_sep_parse_email_notification ... 46
8. Configuring Symantec Endpoint Protection ... 47

1. Overview

Symantec Endpoint Protection (SEP) is a client-server solution that protects laptops, desktops, and servers in a network against malware, risks, and vulnerabilities. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure client computers against known and unknown threats, such as viruses, worms, Trojan horses, and adware.

The SEP integration with the Resilient platform allows for querying and updating of a SEP deployment.

The following type of queries can be executed:

- Execute an Evidence of Compromise (EOC) scan for artifacts of type file (name or path) and hash (MD5, SHA1 or SHA256).
- Get endpoint details or status.
- Get groups.
- Get fingerprint lists.

The integration can also be used to make the following changes to a SEP environment:

- Remediate (quarantine) files (by hash match) discovered in an EOC scan.
- Upload a file from an endpoint to the Symantec Endpoint Protect Manager (SEPM).
- Download a file from the SEPM as base64.
- Add an MD5 hash value or delete an MD5 has vale from a fingerprint list, which can be used to blacklist files.
- Assign a fingerprint list to a group for system lockdown.
- Delete a fingerprint list.
- Move an endpoint to a new group.
- Quarantine an endpoint.

The integration can also be used to automatically parse email notifications of critical events from the SEPM and create associated incidents.

The integration also has two user defined settings:

- Results limit

  The EOC scan query can return a total number of results which can overwhelm the Resilient platform's ability to process them. The integration configuration parameter, `sep_result_limit`, can limit the amount of results sent back to the Resilient platform. If the results returned is over the limit, the results sent to the Resilient platform are truncated to the results limit and the total results are added as an attachment to the originating Resilient incident.

- Results timeout

  The EOC scan command can take a long time for all endpoints to complete the command and return a result; such as when an endpoint is offline. The integration has a user defined parameter `sep_scan_timeout`, which can be used by the get scan results workflow, "Example: SEP - Get Scan results," to indicate that the command has timed-out. The get scan results workflow for the timed-out query is subsequently disabled.

1.1. Use cases

You can perform the following use cases with the SEP integration.

- A suspicious file or hash value is added as an artifact value to a Resilient incident.
  1. Initiate an EOC scan for the artifact in the SEP environment using rule/workflow “Example: SEP - Initiate EOC Scan for Artifact”.

     If a match is discovered, a row is added to data table “Symantec SEP - EOC scan results”. This enables SEP integration rules to be available from this row’s Action menu.
  2. If the file is an executable file type, upload the file to the SEPM server by selecting “Example: SEP - Upload file to SEPM server” from the row’s Actions menu.
  3. To quarantine the file on matching endpoint or all matching endpoints, select “Example: SEP - Remediate Artifact on Endpoint” from the row’s Actions menu.
  4. Use “Example: SEP - Get File Content as Base64 string” from the row’s Actions menu in conjunction with other utilities to add the suspicious file as an attachment to the Resilient incident.
- A suspicious endpoint name is added as an artifact value to a Resilient incident.
  1. Get information on an endpoint using one of the following methods:
     a. Use rule/workflow “Example: SEP - Get Endpoint Details for artifact”.
     b. From a match in the data table “Symantec SEP - EOC scan results” select “Example: SEP - Get Endpoint Details” from the row’s Action menu.

     When a matching endpoint name is discovered, a row is added to data table “Symantec SEP - Endpoint details”. This enables SEP integration rules to be available from this row’s Action menu.
  2. Move the endpoint to a quarantine group by selecting “Example: SEP - Move Endpoint” from the row’s Actions menu.
  3. Add the endpoint to network quarantine by selecting “Example: SEP - Quarantine Endpoint” from the row’s Actions menu.
- An MD5 hash value of a suspicious file is added as an artifact value to a Resilient incident.
  4. See if the hash exists in a blacklist in a target SEP domain using rule/workflow “Blacklist Example: SEP - Get Blacklist information”.

     A row is added to data table “Symantec SEP - Fingerprint lists” if the blacklist is found. This enables SEP integration rules to be available from this row’s Action menu.
  5. If the hash is not present in the blacklist, add the suspicious MD5 hash to the blacklist using rule/workflow “Example: SEP - Add Hash to Blacklist”.
  6. Get a list of SEP group information for the SEP domain by selecting “Example: SEP - Get Groups information” from the row’s Actions menu.

     Information on each SEP group is added as a row to data table “Example: SEP - Get Groups information”.
  7. Assign the blacklist to a group for system lockdown by selecting “Example: SEP - Assign Blacklist to lockdown group” from the row’s Actions menu.
  8. If the MD5 hash is no longer considered suspicious, delete the hash from the blacklist using workflow “Example: SEP - Delete Blacklist”.
  9. Delete the blacklist by selecting “Example: SEP - Delete Blacklist” from the row’s Actions menu.

2. Installation

2.1. Requirements

The functions included this package have the following requirements, which are above and beyond those listed in the *Resilient Integration Server Guide*.

- Resilient platform is version 32 or later.
- Symantec Endpoint Protection 14.2 or later.
- Resilient Generic Email Parsing Script 1.0.1 or later.

2.2. Installation on App Host

When installing the McAfee ESM integration onto the Resilient platform with App Host, be sure to use the package in .zip format. The .zip packaging contains critical data for the integration to successfully install via App Host.

For a complete guide on how to install and configure App Host for Resilient and install apps, please reference the App Host Deployment Guide Knowledge Center.

2.3. Installation on an Integration Server

When installing the McAfee ESM integration onto the Resilient platform with an integration server, be sure to use the package provided in .tar.gz format.

For a complete guide on how to install and configure on an Integration Server for Resilient and install integrations, please reference the Integration Server Guide Knowledge Center.

2.4. Configuration

After installing the package, a new section, *fn_sep*, is created in the app.config file. You need to edit the following settings in that section. If using App Host, see the Resilient System Administrator Guide. If using the integration server, see the Integration Server Guide.

```
[fn_sep]
sep_base_path=/sepm/api/v1
sep_auth_path=/sepm/api/v1/identity/authenticate
sep_host=<SEPM server dns name or ip address>
sep_port=8446
sep_username=<username>
sep_password=<password>
sep_domain=<SEP domain name>
# Settings for access to SEPM via a proxy.
#http_proxy=http':'http://proxy:80
#https_proxy=https':'http://proxy:80
# Limit result sent to Resilient, add full result as an attachment.
sep_results_limit=200
# Period of time (seconds) to wait for all endpoints to return a scan result.
sep_scan_timeout=1800
```

For the Generic Email Parsing Script setup instructions refer to Generic Email Parsing Script setup (PDF).

You need to configure the SEPM to send email notifications to the email address watched by the parsing script.

To avoid duplicate or false artifacts from being created, it is recommended to add custom Whitelists to the “Generic Email Parsing Script”.

```
# Customer-specific IP address whitelists
# Whitelist SEPM server ip addresses
customIPv4WhiteList = [CIDR("192.168.194.93")]
customIPv6WhiteList = [CIDR("2002:835:c36d::946:c25d")]
# Customer-specific domain whitelist
# Whitelist SEPM domain and/or hostname
customDomainWhiteList=[Domain("*.sepmdomain.com"), Domain("SEPM-SERVER")]
```

It will be necessary to either disable the rule “Process email message” from the “Generic Email Parsing Script” package or else alter the rule conditions to prevent interference with the example email processing rule supplied with the SEP integration.

2.5. Useful links

More information is available at: Symantec Endpoint Protection 14 documentation

And more specifically for the API: Symantec Endpoint Protection REST API documentation

Setting up SEPM quarantine policy: Creating a Quarantine policy for a failed Host Integrity check

Setting up SEPM for system lockdown: Running system lockdown in blacklist mode

Setting up SEPM for email notifications: How to Configure Symantec Endpoint Protection Manager to Send Email Alerts

3. Package contents

The following table lists the functions and scripts included in the package, along with associated workflows and rules.

Scan related functions

Function	Workflow	Rule	Support notes
SEP - Scan Endpoints	Example: SEP - Initiate EOC Scan for Artifact	Example: SEP - Initiate EOC Scan for Artifact	• MS Windows endpoints only.
	Example: SEP - Remediate Artifact on Endpoint	Example: SEP - Remediate Artifact on Endpoint	• MS Windows endpoints only. • Remediation (quarantine) artifact by hash value. • All instances of artifact (file) (by hash value) quarantined on targeted endpoints.
SEP - Upload File to SEPM	Example: SEP - Upload file to SEPM server	Example: SEP - Upload file to SEPM server	• MS Windows endpoints only. • Only executable file types such as binary executable (.exe), batch (.bat), Windows installer package (.msi) etc are supported.
SEP - Get File Content as Base64	Example: SEP - Get File Content as Base64 string	Example: SEP - Get File Content as Base64 string	• MS Windows endpoints only.

Endpoint related functions

Function	Workflow	Rule	Support notes
SEP - Get Computers	Example: SEP - Get Endpoint Details	Example: SEP - Get Endpoint Details	• MS Windows, MacOS and Linux endpoints. • Quarantine endpoint action on data table supported for MS Windows only.
	Example: SEP - Get Endpoint Details for artifact	Example: SEP - Get Endpoint Details for artifact	• MS Windows, MacOS and Linux endpoints. • Quarantine endpoint action on data table supported for MS Windows only.
	Example: SEP - Get Endpoints status summary	Example: SEP - Get Endpoints status summary	• MS Windows, MacOS and Linux endpoints. • Not all status information (e.g., Host integrity status) available for MacOS and Linux.
	Example: SEP - Get Endpoints status summary (refresh)	Example: SEP - Get Endpoints status summary (refresh)	• MS Windows, MacOS and Linux endpoints. • Not all status information (e.g. Host integrity status) available for MacOS and Linux.
	Example: SEP - Get Non-Compliant Endpoints status details	Example: SEP - Get Non-Compliant Endpoints status details	• MS Windows, MacOS and Linux endpoints. • Not all status information (e.g., Host integrity status) available for MacOS and Linux.
SEP - Move endpoint	Example: SEP - Move Endpoint	Example: SEP - Move Endpoint	• MS Windows, MacOS and Linux endpoints. • Endpoints cannot be moved between different SEP domains.
SEP - Quarantine Endpoints	Example: SEP - Quarantine Endpoint	Example: SEP - Quarantine Endpoint	• MS Windows endpoints only.

Fingerprint list related functions

Function	Workflow	Rule	Support notes
SEP - Get Fingerprint List	Example: SEP - Get Blacklist information	Example: SEP - Get Blacklist information	
SEP - Add Fingerprint List	Example: SEP - Add Hash to Blacklist	Example: SEP - Add Hash to Blacklist	MD5 hash only supported.
SEP - Update Fingerprint List	Example: SEP - Add Hash to Blacklist	Example: SEP - Add Hash to Blacklist	MD5 hash only supported.
	Example: SEP - Delete Hash from Blacklist	Example: SEP - Delete Hash from Blacklist	Fingerprint list (blacklist) is deleted if the target hash is the only remaining hash in the list.
SEP - Get Groups	Example: SEP - Get Groups information	Example: SEP - Get Groups information	
SEP - Assign Fingerprint List to Group	Example: SEP - Assign Blacklist to lockdown group	Example: SEP - Assign Blacklist to lockdown group	Target group must have “policy inheritance” is disabled.
SEP - Delete Fingerprint List	Example: SEP - Delete Blacklist	Example: SEP - Delete Blacklist	

Support functions

Function	Workflow	Rule	Support notes
SEP - Get Command Status	Example: SEP - Get Scan results	Example: SEP - Get Scan results	MS Windows endpoints only.
	Example: SEP - Get Remediation status	Example: SEP - Get Remediation status	MS Windows endpoints only.
	Example: SEP - Get Upload status	Example: SEP - Get Upload status	MS Windows endpoints only.
	Example: SEP - Get Quarantine status	Example: SEP - Get Quarantine status	MS Windows endpoints only.
SEP - Get Domains	Various as support function	Various as support function	

Notification related content

Script	Workflow	Rule
scr_sep_parse_email_notification	N/A	Example: SEP - Parse notification

Scripts

Script	Workflow	Rule
scr_sep_add_artifact_from_scan_results	N/A	Example: SEP - Add Artifact from Scan Result
scr_sep_parse_email_notification	N/A	Example: SEP - Parse notification

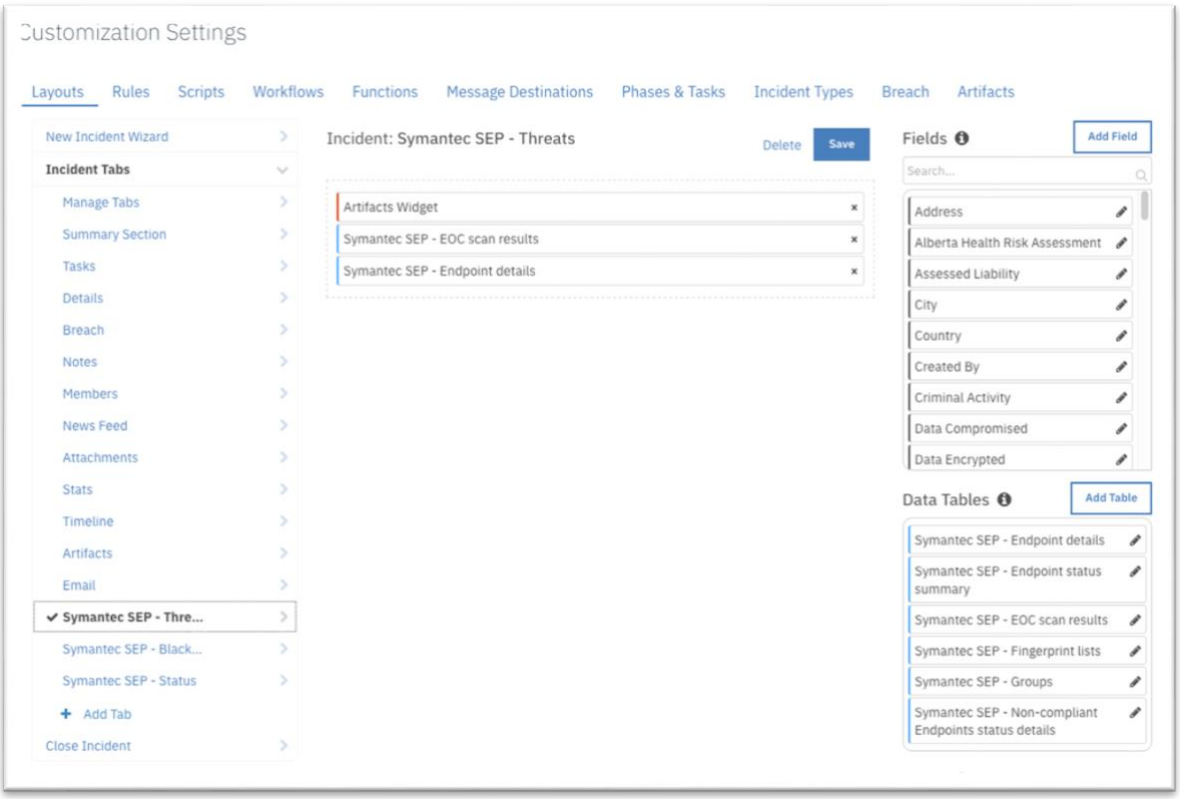
NOTE: The fnctions, SEP - Get Domains, SEP - Get Groups and SEP - Get Fingerprint List, are used in multiple workflows as support functions.

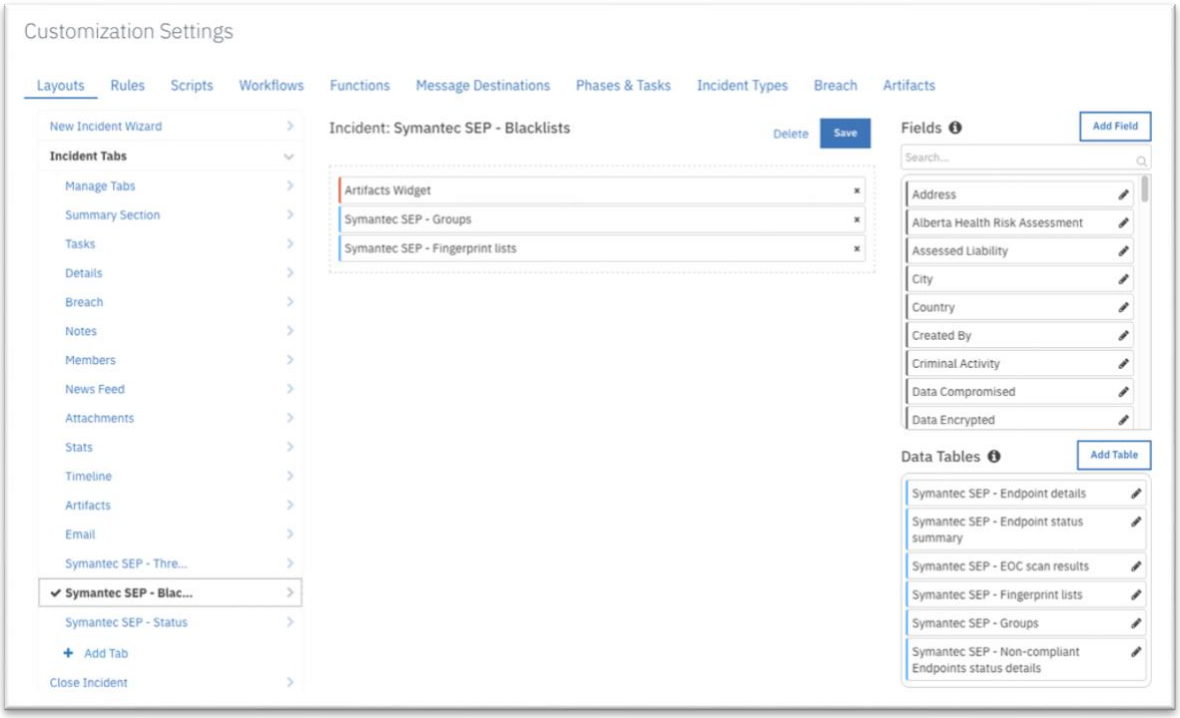
The package also includes the following data tables:

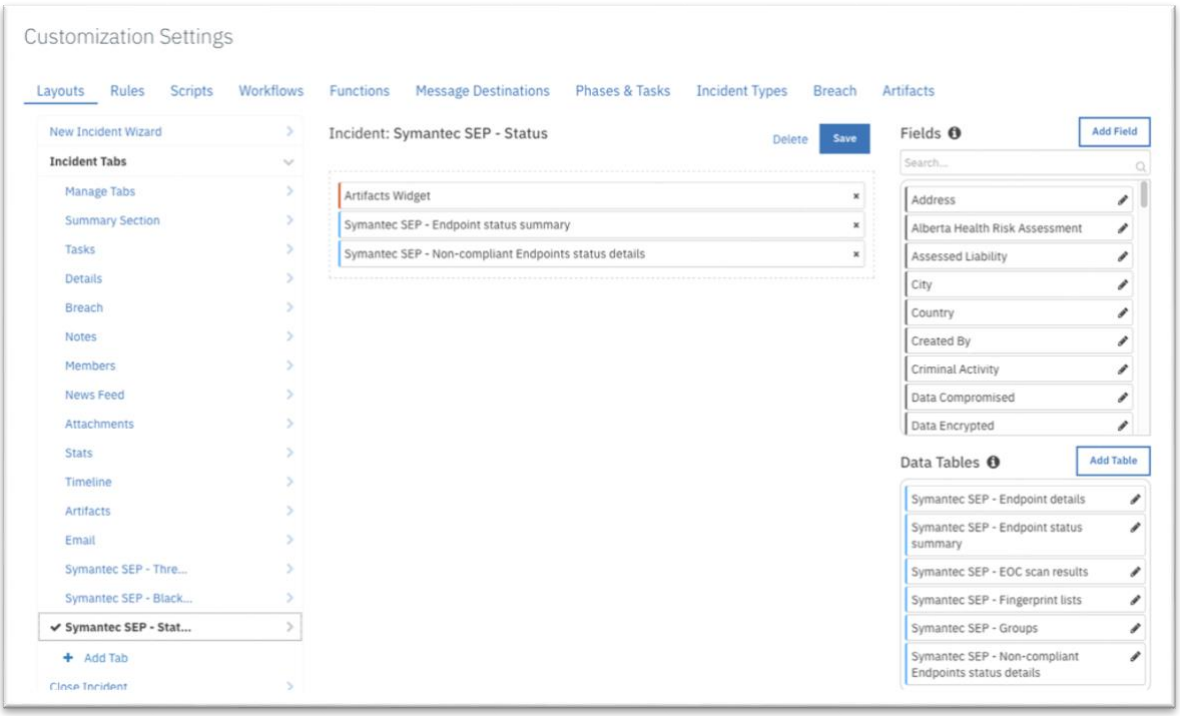
- Symantec SEP - EOC scan results
- Symantec SEP - Endpoint details
- Symantec SEP - Endpoint status summary
- Symantec SEP - Non-compliant Endpoints status details
- Symantec SEP – Groups
- Symantec SEP - Fingerprint lists

4. Custom layout

To use the functions, the Resilient playbook designer needs to create new Incident tabs containing the data tables. The examples in this guide assume that the incident tabs are named Symantec SEP - Threats, Symantec SEP - Blacklists and Symantec SEP - Status. For example:




Customization Settings
Layouts
Rules
Scripts
Workflows
Functions
Message Destinations
Phases & Tasks
Incident Types
Breach
Artifacts
New Incident Wizard
Incident Tabs
Manage Tabs
Summary Section
Tasks
Details
Breach
Notes
Members
News Feed
Attachments
Stats
Timeline
Artifacts
Email
Symantec SEP - Thre...
Symantec SEP - Blac...
Symantec SEP - Status
Add Tab
Close Incident
Incident: Symantec SEP - Blacklists
Delete
Save
Artifacts Widget
Symantec SEP - Groups
Symantec SEP - Fingerprint lists
Fields
Add Field
Search...
Address
Alberta Health Risk Assessment
Assessed Liability
City
Country
Created By
Criminal Activity
Data Compromised
Data Encrypted
Data Tables
Add Table
Symantec SEP - Endpoint details
Symantec SEP - Endpoint status summary
Symantec SEP - EOC scan results
Symantec SEP - Fingerprint lists
Symantec SEP - Groups
Symantec SEP - Non-compliant Endpoints status details


Customization Settings
Layouts
Rules
Scripts
Workflows
Functions
Message Destinations
Phases & Tasks
Incident Types
Breach
Artifacts
New Incident Wizard
Incident Tabs
Manage Tabs
Summary Section
Tasks
Details
Breach
Notes
Members
News Feed
Attachments
Stats
Timeline
Artifacts
Email
Symantec SEP - Thre...
Symantec SEP - Black...
Symantec SEP - Stat...
Add Tab
Close Incident
Incident: Symantec SEP - Status
Delete
Save
Artifacts Widget
Symantec SEP - Endpoint status summary
Symantec SEP - Non-compliant Endpoints status details
Fields
Add Field
Search...
Address
Alberta Health Risk Assessment
Assessed Liability
City
Country
Created By
Criminal Activity
Data Compromised
Data Encrypted
Data Tables
Add Table
Symantec SEP - Endpoint details
Symantec SEP - Endpoint status summary
Symantec SEP - EOC scan results
Symantec SEP - Fingerprint lists
Symantec SEP - Groups
Symantec SEP - Non-compliant Endpoints status details

5. Function descriptions

5.1. SEP - Scan Endpoints

Use the function to initiate an Evidence of Compromise (EOC) scan of an artifact value against a list of endpoints or groups. The function can also be used to complete a remediation (quarantine) scan action for hash value (MD5, SHA1 or SHA256). It uses the following input parameters:

Name	Type	Required	Tooltip
sep_computer_ids	text	No	List of computer IDs on which to run the SEP command.
sep_group_ids	text	No	List of groups on which to run the SEP command.
sep_scan_type	select	Yes	SEP EOC scan type. Possible values are: FULL_SCAN and QUICK_SCAN.
sep_file_path	text	No	File path of the suspect file.
sep_sha256	text	No	SHA256 hash value of the suspicious file.
sep_sha1	text	No	SHA1 hash value of the suspicious file.
sep_md5	text	No	MD5 hash value of the suspicious file.
sep_description	text	No	Scan description.
sep_scan_action	select	No	Action to be performed during a scan.

The input is populated by the workflows, “Example: SEP - Initiate EOC Scan for Artifact” and “Example: SEP - Remediate Artifact on Endpoint”.

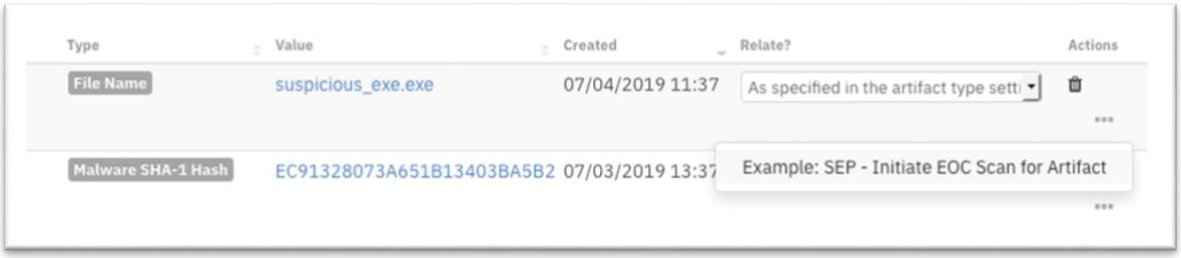
The workflow, “Example: SEP - Initiate EOC Scan for Artifact”, sets the function’s input fields:

- sep_file_path is mapped to a “File path” or “File name” artifact value.
- sep_md5 is mapped to an MD5 artifact value.
- sep_sha1 is mapped to a SHA1 artifact value.
- sep_sha256 is mapped to a SHA256 artifact value.
- sep_computer_ids is mapped to target endpoint IDs.
- sep_scan_type is mapped to “QUICK_SCAN” or “FULL_SCAN”.
- sep_description is derived for the artifact description.
- sep_scan_action is not set.

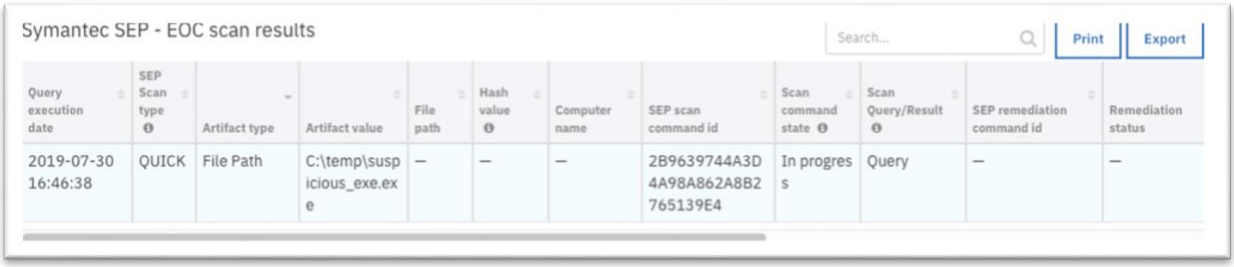
NOTE: Only one of sep_file_path, sep_md5, sep_sha1 or sep_sha256 is mapped to an artifact value for each execution.

The workflow can be initiated by the rule, “Example: SEP - Initiate EOC Scan for Artifact”.

1. Open an incident and select the “SEP – Threats" tab.
2. For the target artifact, click **Action-> Example: SEP - Initiate EOC Scan for Artifact** and select **QUICK_SCAN**.



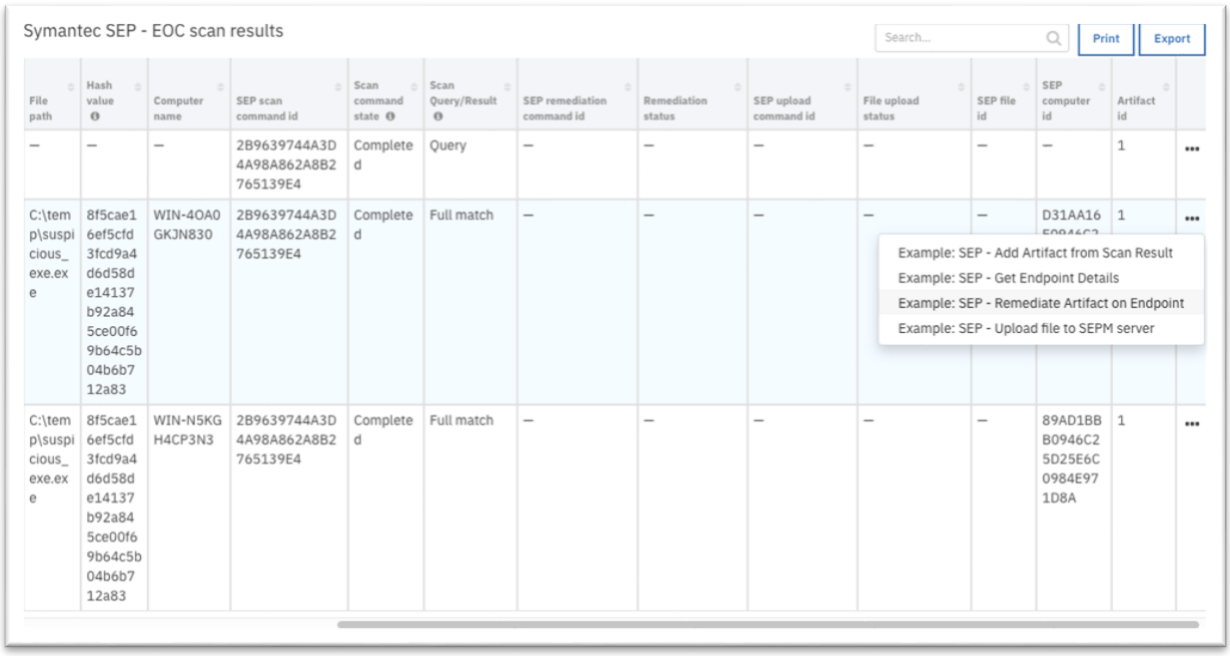
This invokes the “Example: SEP - Initiate EOC Scan for Artifact” workflow, which calls the “SEP - Scan Endpoints” function. The workflow initiates an EOC quick scan of the SEP environment and retrieves the initial status of the associated scan command ID. A row is added to data table “Symantec SEP - EOC scan result” with the initial command status details including “SEP scan command id”. The “Scan command state” is set to “In progress”.



The scan may take some time to complete. Interim status and results can be retrieved using the action “Example: SEP - Get Scan results”, which should be enabled for this data table query row.

See [SEP - Get Command Status]() for more information on rule/workflow “Example: SEP - Get Scan results”.

Once a match has been found, four actions are enabled for each matching row including "Example: SEP - Remediate Artifact on Endpoint":



File path	Hash value	Computer name	SEP scan command id	Scan command state	Scan Query/Result	SEP remediation command id	Remediation status	SEP upload command id	File upload status	SEP file id	SEP computer id	Artifact id
–	–	–	2B9639744A3D4A98A862A8B2765139E4	Completed	Query	–	–	–	–	–	–	1
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-4OA0GKJN830	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	–	–	–	D31AA16	1
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-N5KGH4CP3N3	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	–	–	–	89AD1BBB0946C25D25E6C0984E971D8A	1

For information on the other actions, see the section under the relevant function or script.

If the number of matches is greater than configuration parameter `sep_result_limit`, a row is added for each match up to the limit and the full result added as a csv attachment to the incident.

In the following example, `sep_result_limit` is set to 1.

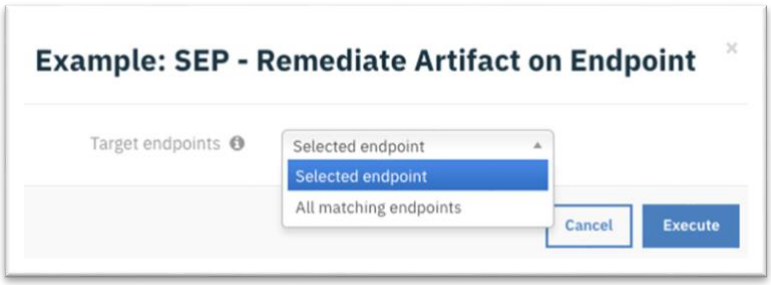
File path	Hash value	Computer name	SEP scan command id	Scan command state	Scan Query/Result	SEP remediation command id	Remediation status	SEP upload command id	File upload status	SEP file id	SEP computer id	Artifact id
–	–	–	2B9639744A3D4A98A862A8B2765139E4	Completed	Query: Matches over results limit see note/attachment.	–	–	–	–	–	–	1
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-4OA0GKJN830	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	–	–	–	D31AA16	1

The workflow, “Example: SEP - Remediate Artifact on Endpoint”, sets the function’s input fields:

- sep_file_path is mapped to a “File path” or “File name” artifact value.
- sep_md5 is mapped to an MD5 artifact value.
- sep_sha1 is mapped to a SHA1 artifact value.
- sep_sha256 is mapped to a SHA256 artifact value.
- sep_computer_ids is mapped to target endpoint IDs.
- sep_scan_type is mapped to value from selected data table row.
- sep_scan_action is set to "remediate".
- sep_description is derived for the file path.

The workflow is initiated by the rule, “Example: SEP - Remediate Artifact on Endpoint”.

To remediate (quarantine) the suspicious artifact on target endpoints, click **Action-> Example: SEP - Remediate Artifact on Endpoint.** The user is presented with a drop-down list with a choice of remediating the artifact on the “Selected endpoint” or “All matching endpoints”. Select “Selected endpoint”.



This invokes the “Example: SEP - Remediate Artifact on Endpoint” workflow, which calls the “SEP - Scan Endpoints” function. This workflow initiates a remediation or quarantine action for the selected artifact on the selected endpoints in the SEP environment. The selected row in the “Symantec SEP - EOC scan result” data table is updated with the “SEP remediation command id” and the “Remediation status”.

The remediation scan may take some time to complete. Interim status and results can be retrieved using action “Example: SEP - Get Remediation status”, which should be enabled for this data table query row. See SEP - Get Command Status for more information on rule/workflow “Example: SEP - Get Remediation status”.

NOTE: When a remediation action is successful on an endpoint, it quarantines the target file by hash value and not by file path. Any files with the matching hash found by the scan on the endpoint is quarantined on the endpoint.

5.2. SEP - Upload File to SEPM

Use the function to upload a file from an endpoint to the SEPM server. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_computer_ids	text	No	List of computer IDs on which to run the SEP command.
sep_group_ids	text	No	List of groups on which to run the SEP command.
sep_file_path	text	No	File path of the suspect file.
sep_sha256	text	No	SHA256 hash value of the suspicious file.
sep_sha1	text	No	SHA1 hash value of the suspicious file.
sep_md5	text	No	MD5 hash value of the suspicious file.
sep_source	text	No	File source to search for suspicious file. Possible values are: FILESYSTEM (default), QUARANTINE, or BOTH. 12.1.x clients use FILESYSTEM only.

The input is populated by the workflow, “Example: SEP - Upload file to SEPM server”.

The workflow, “Example: SEP - Upload file to SEPM server” sets the function’s input fields:

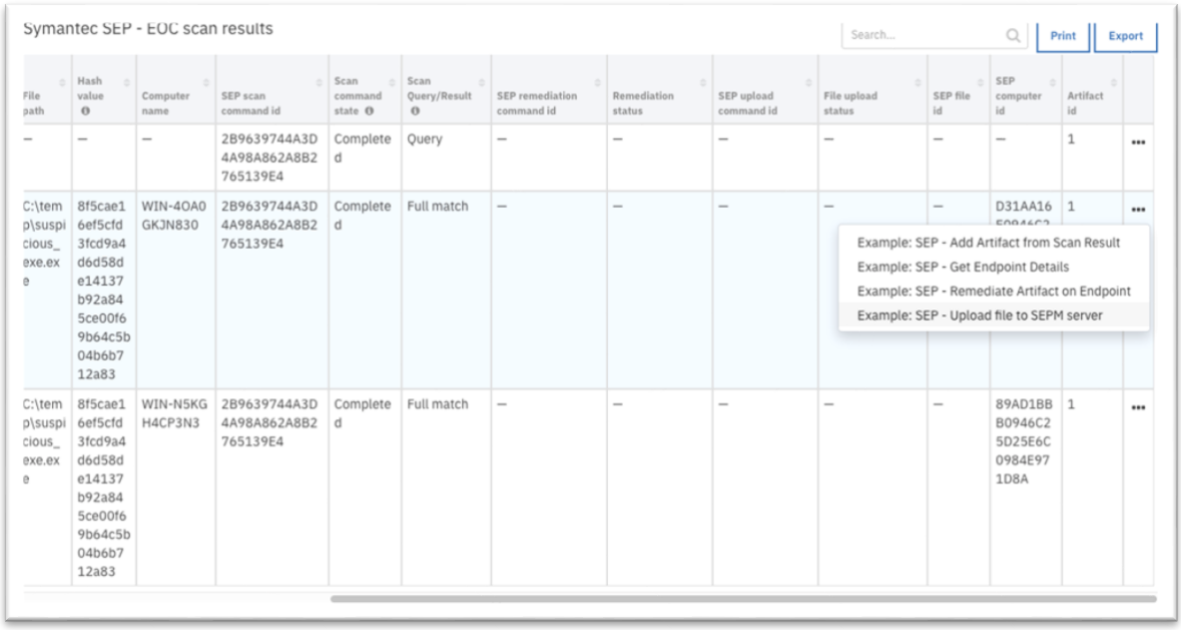
- sep_computer_ids parameter is mapped to the value from the selected data table row.
- sep_file_path is mapped to the value from the selected data table row.
- sep_sha256 is mapped to the value from the selected data table row.
- sep_sha1 is mapped to the value from the selected data table row.
- sep_md5 is mapped to the value from the selected data table row.
- sep_source is selected from the value in an activity field drop-down list.

NOTE 1: Only one of MD5, SHA1 or SHA256 is mapped to an artifact value for each execution.

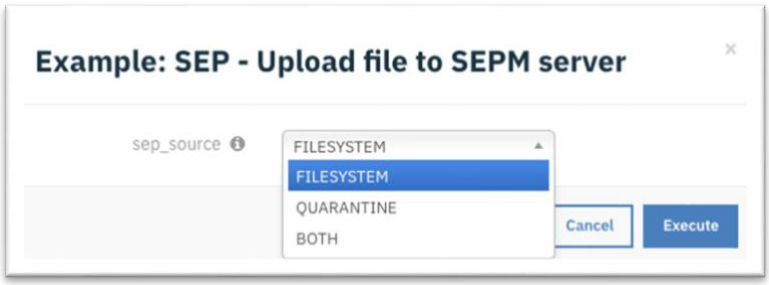
NOTE 2: Upload only supports executable file types such as (.exe), batch (.bat), and Windows installer package (.msi).

The workflow is initiated by the rule, “Example: SEP - Upload file to SEPM server”.

To upload a matched artifact on the target endpoint, Click **Action-> Example: SEP - Upload file to SEPM server.**



The user is presented with a drop-down list with options to remediate the artifact from “FILESYSTEM”, “QUARANTINED” or “BOTH”. Select “FILESYSTEM”.



This invokes the workflow “Example: SEP - Upload file to SEPM server”, which calls the “SEP - Upload File to SEPM” function. This workflow initiates an upload of the selected artifact in the SEP environment to the SEPM server. The data table “Symantec SEP - EOC scan result” is updated with the “SEP upload command id”, and the “File upload status” is set to “In progress”.

The remediation scan may take some time to complete, interim status and results can be retrieved using action “Example: SEP - Get Upload status”, which should be enabled for this data table query row. See SEP - Get Command Status for more information on rule/workflow “Example: SEP - Get Upload status”.

5.3. SEP - Get File Content as Base64

Use the function to get contents of a file uploaded to a SEPM server as a Base64 string. It uses the following input parameter:

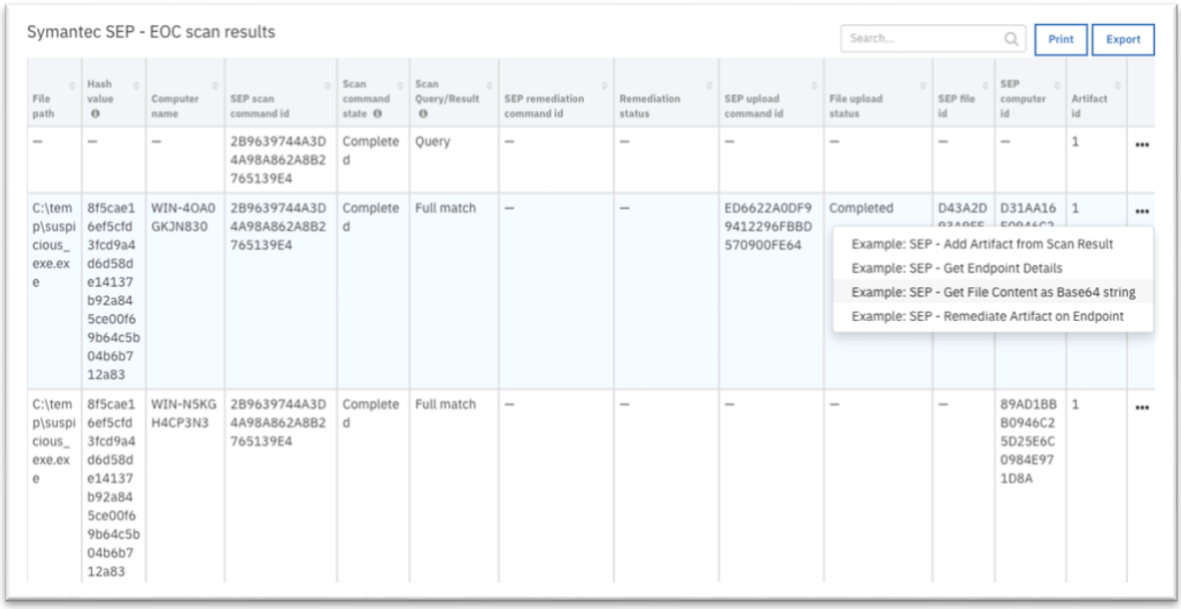
Name	Type	Required	Tooltip
sep_file_id	text	No	File ID from which to get detailed information.

The input is populated by the workflow, “Example: SEP - Get File Content as Base64 string”.

The workflow, “Example: SEP - Get File Content as Base64 string”, sets the function’s input field, sep_file_id, which is mapped to the value from the selected data table row.

The workflow is initiated by the rule, “Example: SEP - Get File Content as Base64 string”.

To get file contents as base64 of a matched and uploaded artifact, click **Action-> Example: SEP - Get File Content as Base64 string.**



5.4. SEP - Get Computers

Use the function to get information about the computers in a specified domain. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_computername	text	No	Host name of computer. Wild card is supported as '*'.
sep_status	boolean	No	Get overall status for endpoints.
sep_status_details	boolean	No	Get endpoints status details.
sep_domain	text	No	SEPM domain.
sep_lastupdate	text	No	Indicates when a computer last updated its status. Default value of 0 gets all the results.
sep_order	text	No	Specifies the results order ASC or DESC.
sep_os	text	No	List of OS to filter by.
sep_pageindex	number	No	Index page that is used for the returned results. Default page index is 1.
sep_pagesize	number	No	Number of results to include on each page. Default is 20.
sep_sort	text	No	Column by which the results are sorted.
sep_matching_endpoint_ids	boolean	No	Get list of matching endpoints.

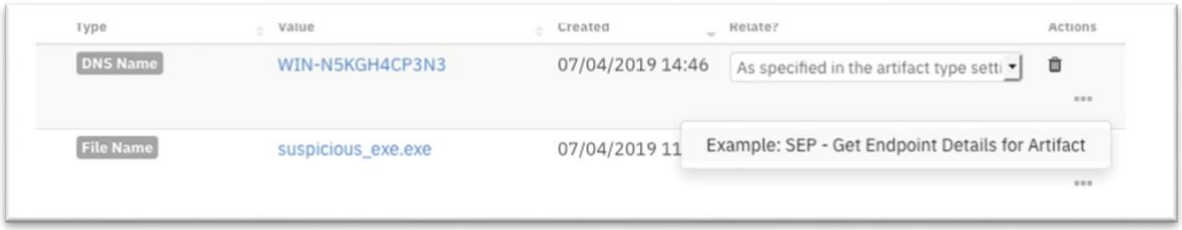
The input is populated by the workflows, "Example: SEP - Get Endpoint Details", "Example: SEP - Get Endpoint Details for artifact", "Example: SEP - Get Endpoints status", "Example: SEP - Get Endpoints status (refresh)", and "Example: SEP - Get Non-Compliant Endpoints status details".

The workflow, "Example: SEP - Get Endpoint Details for Artifact" sets the function's input fields:

- sep_computername is mapped to a "DNS Name" or "System Name" artifact value.
- None of the other fields are set.

The workflow is initiated by the rule, "Example: SEP - Get Endpoint Details for Artifact".

1. Open an incident and select the "SEP – Threats" tab.
2. For the target artifact, click **Action-> Example: SEP - Get Endpoint Details for Artifact**.



This invokes the "Example: SEP - Get Endpoint Details for Artifact" workflow, which calls the "SEP - Get Computers" function. The workflow retrieves the properties of the target endpoint. A row is added to data table "Symantec SEP - Endpoint details" with the endpoint properties.

The workflow, "Example: SEP - Get Endpoint Details" sets the function's input fields:

- sep_computername is mapped to the Computer name field in a selected row of data table "Symantec SEP - EOC scan results".
- None of the other fields are set.

The workflow is initiated by the rule, "Example: SEP - Get Endpoint Details".

1. Open an incident and select a row with a matching artifact in data table “Symantec SEP - EOC scan results”.
2. From the selected row Click **Action-> Example: SEP - Get Endpoint Details**

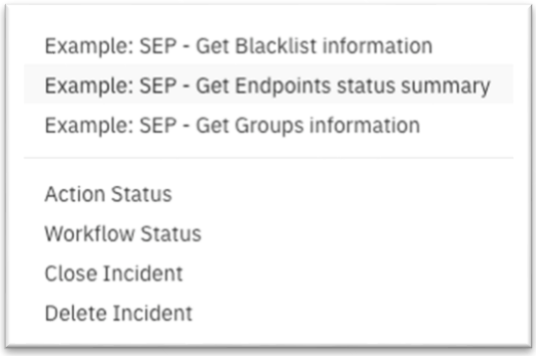
This invokes the “Example: SEP - Get Endpoint Details” workflow, which calls the “SEP - Get Computers” function. The workflow retrieves the properties of the target endpoint. A row is added to data table “Symantec SEP - Endpoint details” with the endpoint properties.

The workflow, “Example: SEP - Get Endpoints status” sets the function’s input fields:

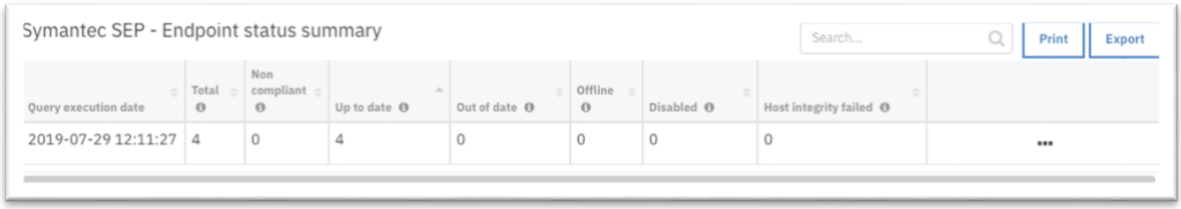
- sep_status is set to True.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Endpoints status summary”.

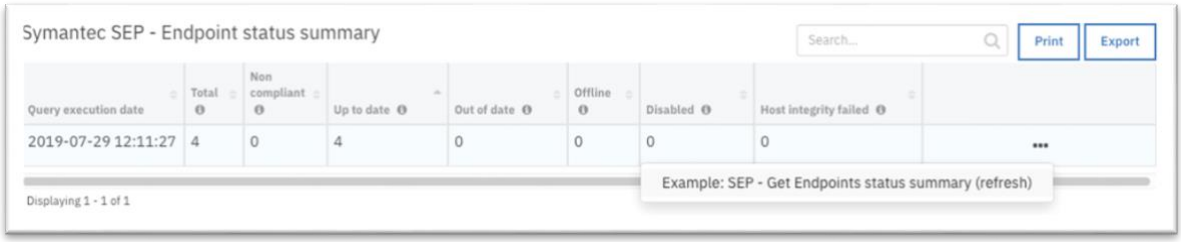
1. Open an incident and select the “SEP – Status” tab.
2. Click **Actions-> Example: SEP - Get Endpoints status summary**.



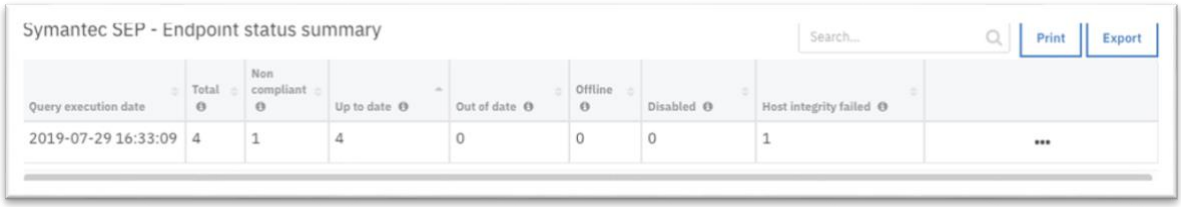
This invokes the “Example: SEP - Get Endpoints status summary” workflow, which calls the “SEP - Get Computers” function. The workflow retrieves the overall status for all endpoints. A row is added to data table “Symantec SEP - Endpoint status summary” with the overall endpoint status.



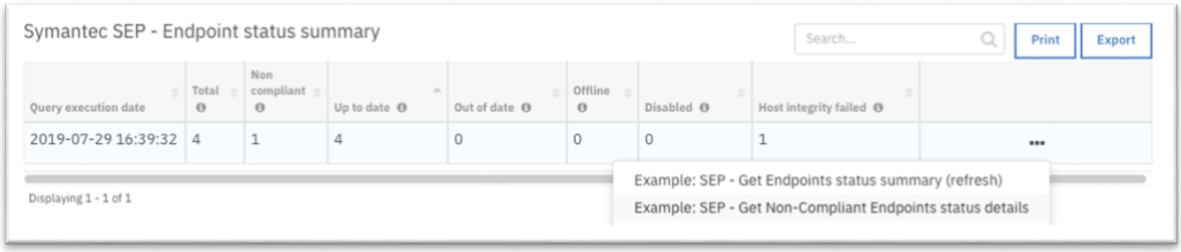
If all computers have good status (they are all compliant) an action “Example: SEP - Get Endpoints status summary (refresh)” is enabled for the matching data table row.



The data table row property “Non compliant” is incremented for each endpoint which has a bad status (is non-compliant). This column displays the total count of non-compliant endpoints in the SEP environment.



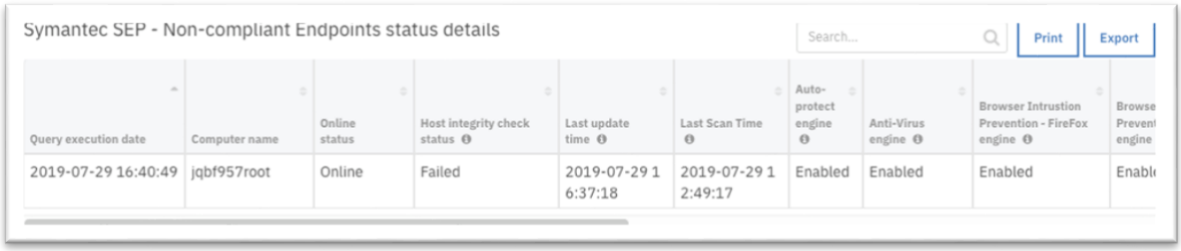
Action “Example: SEP - Get Non-Compliant Endpoints status details” is enabled for the data table row”.



The workflow, “Example: SEP - Get Non-Compliant Endpoints status details” sets the function’s input fields:

- sep_status_details parameter is set to True.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Non-Compliant Endpoints status details”.



This workflow returns more detailed status information for non-compliant endpoints.

5.5. SEP - Move Endpoint

Use the function to check for and move an endpoint to a different group. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_groupid	text	Yes	Group ID on which to run the SEP command.
sep_hardwarekey	text	Yes	Hardware key of SEP computer.

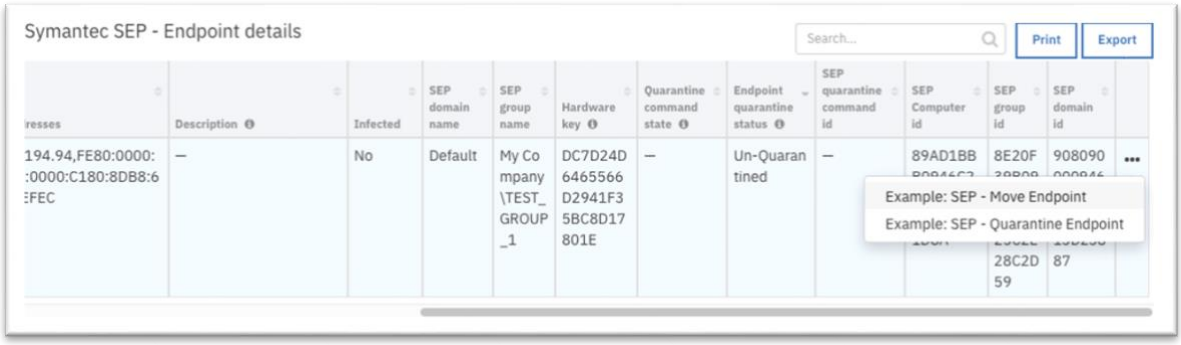
The input is populated by the workflow, “Example: SEP - Move Endpoint”.

The workflow, “Example: SEP - Move Endpoint”, sets the function’s input fields:

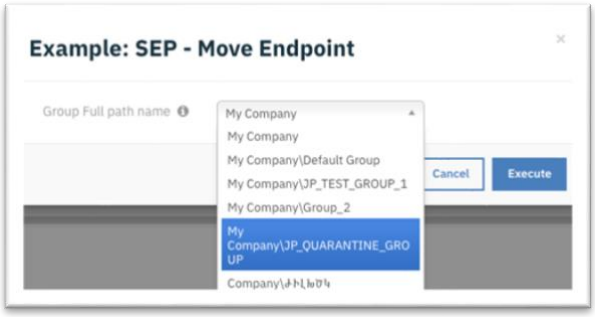
- sep_groupid is mapped to the value from the selected data table row.
- sep_hardwarekey is mapped to the value from the selected data table row.

The workflow is initiated by the rule, “Example: SEP - Move Endpoint”.

1. Open an incident and select a target row in data table “Symantec SEP - Endpoint details”.
2. From the selected row, click **Action-> Example: SEP - Move Endpoint**.



The user is presented with a drop-down list of user defined group path names. Select group “My Company\QUARANTINE_GROUP”.



This invokes the workflow “Example: SEP - Move Endpoint”, which calls the “SEP - Move endpoint” function. This workflow executes a move of the endpoint to the target SEP group. If the workflow is successful, the field “SEP group name” on the target row of data table “Symantec SEP - Endpoint details” is updated with the new group name, in this case “My Company\QUARANTINE_GROUP” group.

Symantec SEP - Endpoint details

Search... Print Export

resses	Description	Infected	SEP domain name	SEP group name	Hardware key	Quarantine command state	Endpoint quarantine status	SEP quarantine command id	SEP Computer id	SEP group id	SEP domain id	
194.94,FE80:0000::0000:C180:8DB8:6:FEC	—	No	Default	My Company\QUARANTINE_GROUP	DC7D24D6465566D2941F35BC8D17801E	—	Un-Quarantined	—	89AD1BBB0946C25D25E6C0984E971D8A	7E4BB119A9FE9DC526EDABFB1EE261B8	908090000946C25D330E91913D23887	•••

The user can also determine if the command is successful by checking the Workflow status.

5.6. SEP - Quarantine Endpoints

Use the function to quarantine or un-quarantine SEP endpoints. The function adds or removes endpoints to or from network quarantine. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_computer_ids	text	No	List of computer IDs on which to run the SEP command.
sep_group_ids	text	No	List of groups on which to run the SEP command.
sep_undo	boolean	No	Boolean value, if set to true, undoes operation.

The input is populated by the workflow, “Example: SEP - Quarantine Endpoint”.

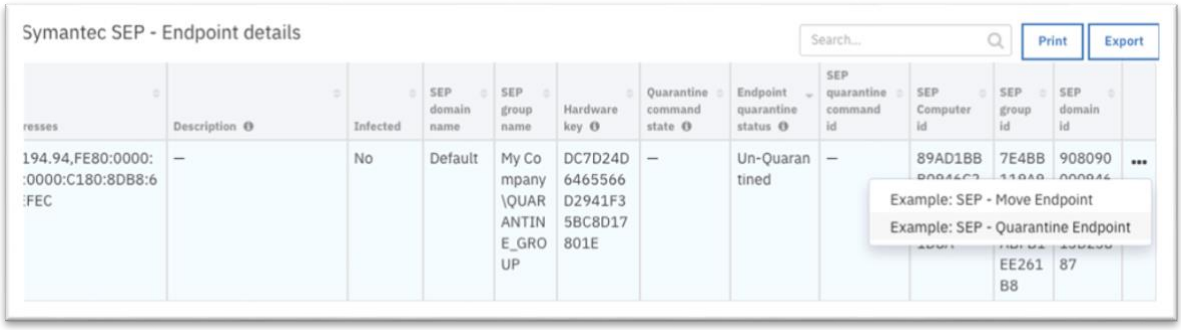
The workflow, “Example: SEP - Quarantine Endpoint”, sets the function’s input fields:

- sep_computer_ids are mapped to the value from the selected data table row.
- sep_undo is calculated based on the data table column with a value of “Endpoint status” from the selected row. If this input is set to True, an un-quarantine command is initiated.
- sep_groups_ids parameter is not set.

The workflow is initiated by the rule, “Example: SEP - Quarantine Endpoint”.

1. Open an incident and select the “SEP – Threats" tab.
2. Select a target row in data table, “Symantec SEP - Endpoint details”.
3. From the selected row, click **Action-> Example: SEP - Quarantine Endpoint**.

NOTE: Rule “Example: SEP - Quarantine Endpoint” is enabled if data table field “Endpoint quarantine status” is set to “Un-Quarantined”.



This invokes the “Example: SEP - Quarantine Endpoint” workflow, which calls the “SEP - Quarantine Endpoints” function. This workflow initiates a network quarantine of selected endpoints in the SEP environment. The selected row in data table “Symantec SEP - EOC scan result” is updated with the “SEP quarantine command id”, and the “Quarantine command state” is set to “In progress”.

The quarantine command may take some time to complete, interim status and results can be retrieved using action “Example: SEP - Get Quarantine status”, which should be enabled for this data table row. See SEP - Get Command Status for more information on rule/workflow “Example: SEP - Get Quarantine status”.

When the quarantine command has successfully completed, the data table field “Quarantine command state” is updated to state ”Completed”, and field “Endpoint quarantine status” is transitioned to “Quarantined”.

dresses	Description	Infected	SEP domain name	SEP group name	Hardware key	Quarantine command state	Endpoint quarantine status	SEP quarantine command id	SEP Computer id	SEP group id	SEP domain id
.194.94,FE80:0000:0:0000:C180:8DB8:6EFEC	–	No	Default	My Company\QUARANTINE_GROUP	DC7D24D6465566D2941F35BC8D17801E	Completed	Quarantined	398A628B20A74FECB7869E9A17CAA4B9	89AD1BBB0946C25D25E6C0984E971D8A	7E4BB119A9FE9DC526EDABFB1EE261B8	908090000946C25D330E919313D23887

To un-quarantine an endpoint, the workflow is initiated by the rule, “Example: SEP - Un-Quarantine Endpoint”.

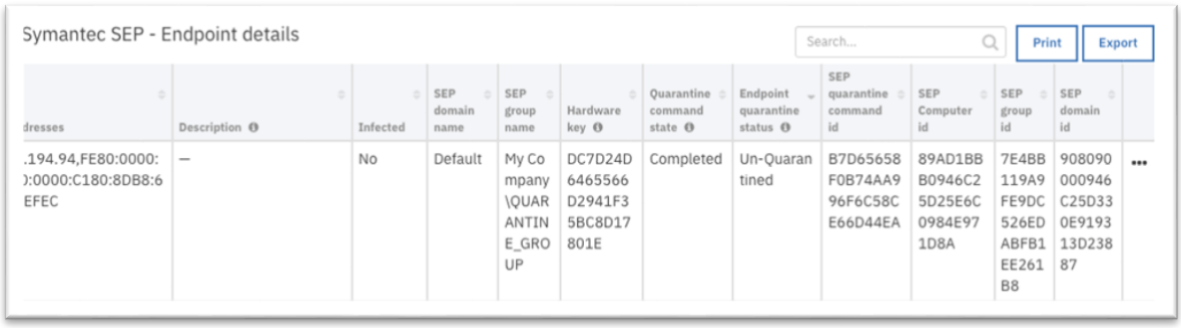
1. Open an incident and select the “SEP – Threats" tab.
2. Select a target row in data table “Symantec SEP - Endpoint details”.
3. From the selected row, click **Action-> Example: SEP – Un-Quarantine Endpoint**.

NOTE: Rule “Example: SEP - Un-Quarantine Endpoint” is enabled if data table field “Endpoint quarantine status” is set to “Quarantined”.

This invokes the “Example: SEP - Quarantine Endpoint” workflow, which calls the “SEP - Quarantine Endpoints” function. This workflow initiates a network remove from network quarantine of the selected endpoint in the SEP environment. The selected row in data table “Symantec SEP - Endpoint details” is updated with the “SEP quarantine command id”, and the “Quarantine command state” is set to “In progress”.

The un-quarantine command may take some time to complete. Interim status and results can be retrieved using action “Example: SEP - Get Quarantine status”, which should be enabled for this data table row. See SEP - Get Command Status for more information on rule/workflow “Example: SEP - Get Quarantine status”.

When the un-quarantine command has successfully completed, the data table field “Quarantine command state” is updated to the “Completed”, and field “Endpoint status status” is transitioned to “Un-Quarantined”.



5.7. SEP - Get Fingerprint List

Use the function to get the fingerprint list information for a specified name or ID. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_domainid	text	Yes	SEPM domain ID.
sep_fingerprintlist_id	text	No	ID of SEP fingerprint list.
sep_fingerprintlist_name	text	No	Name of a SEP fingerprint list.

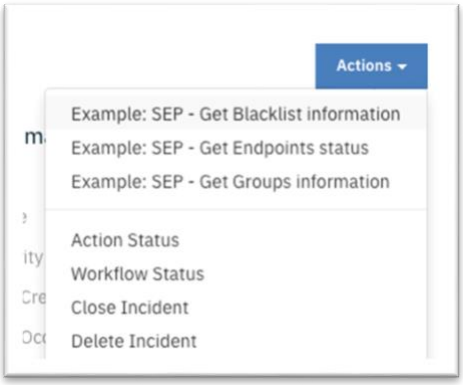
The input is populated by the workflows, “Example: SEP - Get Blacklist information”.

The workflow, “Example: SEP - Get Blacklist information”, sets the function’s input fields:

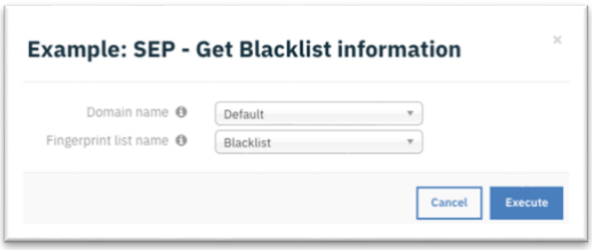
- sep_domainid is mapped to the ID of the domain name selected from the activity field drop-down.
- sep_fingerprintlist_id is mapped to the ID of the fingerprintlist name selected from the activity field drop-down.
- sep_fingerprintlist_name is mapped to the value selected from the activity field drop-down.

The workflow is initiated by the rule, “Example: SEP - Get Blacklist information”.

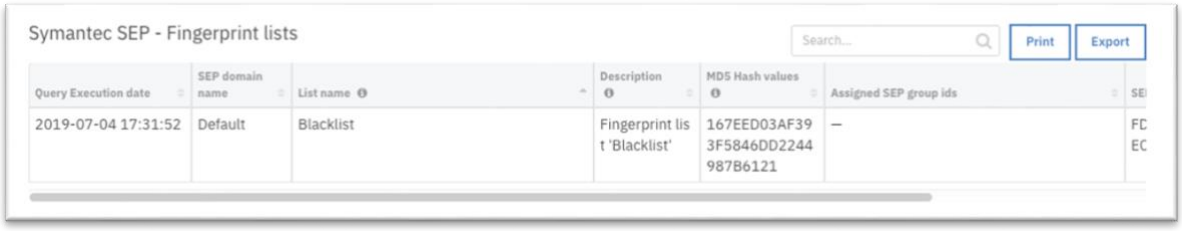
1. Open an incident and select the “SEP – Blacklists” tab.
2. Click **Actions-> Example: SEP - Get Blacklist information**.



The user is presented with a drop-down list of user defined domain name and fingerprint list names. In the example, domain name “Default” and fingerprint list name “Blacklist” is selected.



This invokes the “Example: SEP - Get Blacklist information” workflow, which calls the “SEP - Get Fingerprint List” function. The workflow retrieves the properties of the selected fingerprint list name for the selected domain name. A row is added to data table “Symantec SEP - Fingerprint lists” with the fingerprint list properties.



5.8. SEP - Add Fingerprint List

Use the function to add a hash to a new fingerprint list. Currently only supports MD5 hash type. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_fingerprintlist_name	text	No	Name of a SEP fingerprint list.
sep_description	text	No	SEP object description.
sep_domainid	text	No	SEPM domain ID.
sep_hash_value	text	No	Hash value. Can be MD5 or SHA256.

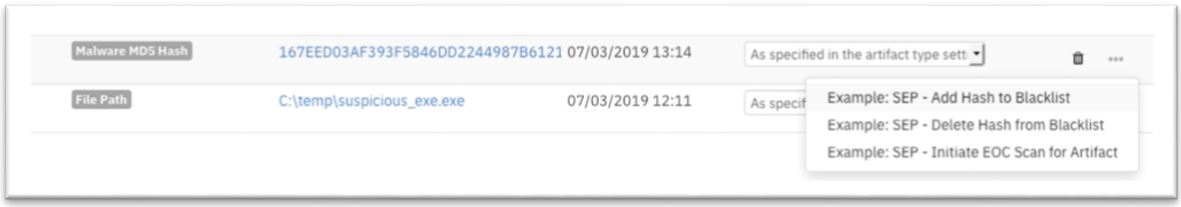
The input is populated by the workflows, “Example: SEP - Add Hash to Blacklist”.

The workflow, “Example: SEP - Add Hash to Blacklist”, sets the function’s input fields:

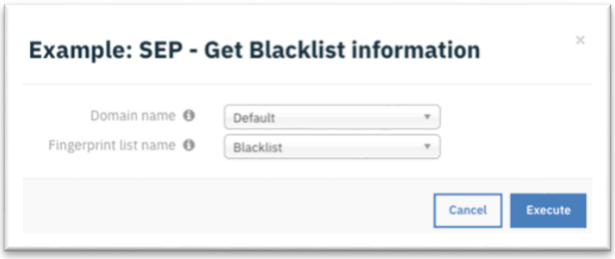
- sep_domainid is mapped to the ID of the domain name selected from the activity field drop-down.
- sep_fingerprintlist_name is mapped to the value selected from the activity field drop-down.
- sep_hash_value is mapped to an MD5 Resilient incident artifact value.
- sep_description is defined in the workflow.

The workflow is initiated by the rule, “Example: SEP - Add Hash to Blacklist”.

1. Open an incident and select the “Symantec SEP – Blacklists” tab.
2. For the target MD5 hash artifact, click **Action-> Example: SEP - Add Hash to Blacklist**.



The user is presented with a drop-down list of user defined domain names and fingerprint list names. In the example, domain name “Default” and fingerprint list name “Blacklist” is selected.



This invokes the “Example: SEP - Add Hash to Blacklist” workflow, which calls either the “SEP - Add Fingerprint List” or “SEP - Update Fingerprint List” function depending on whether the fingerprint list already exists. The workflow adds the selected hash to the selected fingerprint list if it exists; otherwise, a new fingerprint list is created. The user can determine if the command is successful by checking the Workflow status.

5.9. SEP - Update Fingerprint List

Use the function to update an existing fingerprint list with a set of hash values. Supports MD5 hash type only. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_fingerprintlist_name	text	No	Name of a SEP fingerprint list.
sep_fingerprintlist_id	text	No	ID of SEP fingerprint list.
sep_description	text	No	SEP object description.
sep_domainid	text	No	SEPM domain ID.
sep_hash_value	text	No	Hash value. Can be MD5 or SHA256.

The input is populated by the workflows, “Example: SEP - Add Hash to Blacklist” and “Example: SEP - Delete Hash from Blacklist”.

The workflow, “Example: SEP - Add Hash to Blacklist” sets the function’s input fields:

- sep_domainid is mapped to the ID of the domain name selected from the activity field drop-down.
- sep_fingerprintlist_name is mapped to the value selected from the activity field drop-down.
- sep_fingerprintlist_id is mapped to the ID of the fingerprintlist name selected from the activity field drop-down.
- sep_hash_value is mapped to an MD5 Resilient incident artifact value.
- sep_description is defined in the workflow.

The workflow is initiated by the rule, “Example: SEP - Add Hash to Blacklist”.

See the function description in SEP – Add Fingerprint List for details.

5.10. SEP - Get Groups

Use the function to get the properties of all groups in a domain. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_domain	text	No	SEPM domain.
sep_fullpathname	text	No	Full path name of the group.
sep_mode	text	No	Presentation mode for the results, as a list (default) or as a tree.
sep_pageindex	number	No	Index page that is used for the returned results. Default page index is 1.
sep_pagesize	number	No	Number of results to include on each page. Default is 20.
sep_order	text	No	Specifies the results order ASC or DESC.
sep_sort	text	No	Column by which the results are sorted.

The input is populated by the workflow, “Example: SEP - Get Groups information”.

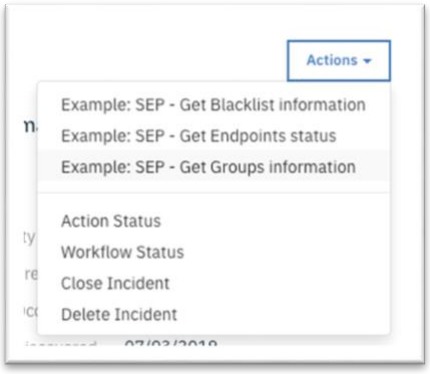
NOTE: This function is also used as a helper function in several other workflows.

The workflow, “Example: SEP - Get Groups information”, sets the function’s input fields:

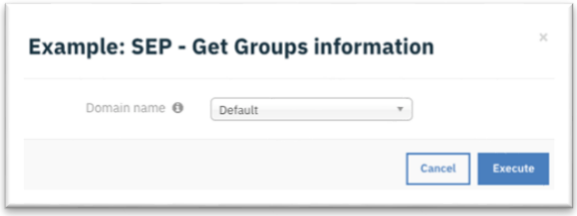
- sep_domain is mapped to the ID of the domain name selected from the activity field drop-down.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Groups information”.

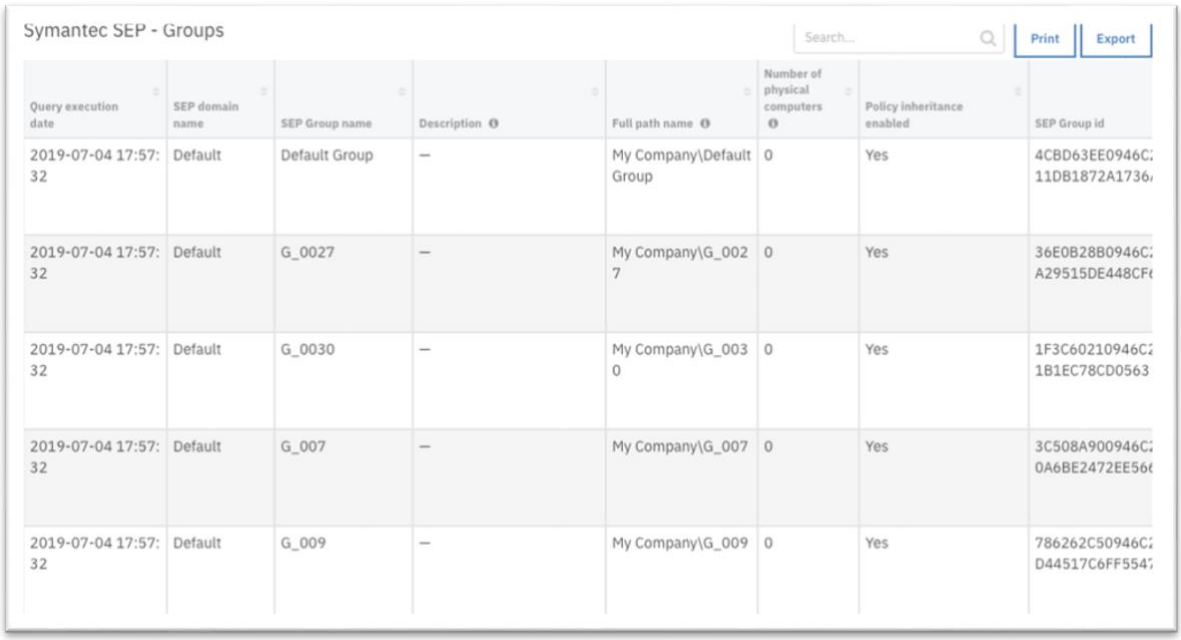
1. Open an incident and select the “SEP – Blacklists” tab.
2. Click **Actions-> Example: SEP - Get Groups information**.



The user is presented with a drop-down list of user defined domain names. In the example, domain name “Default” is selected.



This invokes the “Example: SEP - Get Groups information” workflow, which calls the “SEP - Get Groups” function. The workflow retrieves the properties of groups for the selected domain name. A row for each group in the selected domain is added to data table “Symantec SEP - Groups” with the group properties.



Query execution date	SEP domain name	SEP Group name	Description	Full path name	Number of physical computers	Policy inheritance enabled	SEP Group id
2019-07-04 17:57:32	Default	Default Group	–	My Company\Default Group	0	Yes	4CBD63EE0946C 11DB1872A1736
2019-07-04 17:57:32	Default	G_0027	–	My Company\G_0027	0	Yes	36E0B28B0946C A29515DE448CF
2019-07-04 17:57:32	Default	G_0030	–	My Company\G_0030	0	Yes	1F3C60210946C 1B1EC78CD0563
2019-07-04 17:57:32	Default	G_007	–	My Company\G_007	0	Yes	3C508A900946C 0A6BE2472EE56
2019-07-04 17:57:32	Default	G_009	–	My Company\G_009	0	Yes	786262C50946C D44517C6FF554

5.11. SEP - Assign Fingerprint List to Group

Use the function to assign a fingerprint list to a group for lock-down. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_groupid	text	Yes	Group ID on which to run the SEP command.
sep_fingerprintlist_id	text	Yes	ID of SEP fingerprint list.

The input is populated by the workflow, “Example: SEP - Assign Blacklist to lockdown group”.

The workflow, “Example: SEP - Assign Blacklist to lockdown group”, sets the function’s input fields:

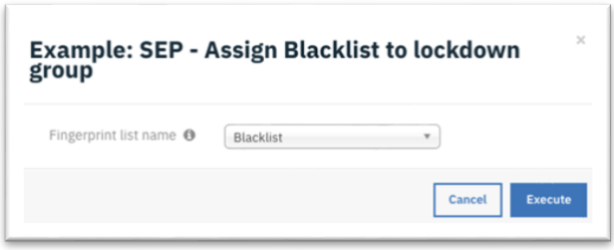
- sep_groupid is mapped to the value from the selected data table row.
- sep_fingerprintlist_id is mapped to the ID of fingerprintlist name selected from the activity field drop-down.

The workflow is initiated by the rule, “Example: SEP - Assign Blacklist to lockdown group”.

1. Open an incident and select the “SEP – Blacklists" tab.
2. Select a target row in data table “Symantec SEP - Groups”.
3. From the selected row, click **Action-> Example: SEP - Assign Blacklist to lockdown group**.

NOTE: The action is enabled only for groups for which “policy inheritance” is disabled.

The user is presented with a drop-down list of user defined fingerprint list names. The fingerprint list and group are expected to be in the same SEP domain. In the example, fingerprint list name “Blacklist” is selected.



This invokes the “Example: SEP - Assign Blacklist to lockdown group” workflow, which calls the “SEP - Assign Fingerprint List to Group” function depending on whether the fingerprint list exists. The workflow assigns the fingerprint list name to the selected group. The user can determine if the command is successful by checking the Workflow status.

5.12. SEP - Delete Fingerprint List

Use the function to delete a fingerprint list. It uses the following input parameter:

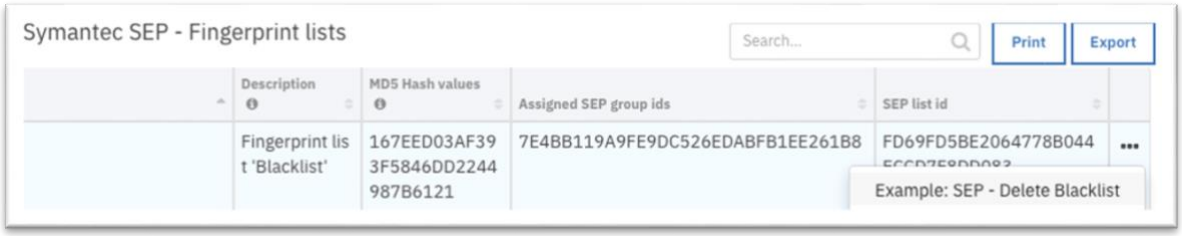
Name	Type	Required	Tooltip
sep_fingerprintlist_id	text	Yes	ID of SEP fingerprint list.

The input is populated by the workflows, “Example: SEP - Delete Blacklist”.

The workflow, “Example: SEP - Delete Blacklist”, sets the function’s input field, sep_fingerprintlist_id, which is mapped to the value from the selected data table row.

The workflow is initiated by the rule, “Example: SEP - Delete Blacklist”.

1. Open an incident and select the “SEP – Blacklists" tab.
2. Select a target row in data table “Symantec SEP - Fingerprint lists”.
3. From the selected row, click **Action-> Example: SEP - Delete Blacklist**.



This invokes the “Example: SEP - Delete Blacklist” workflow, which calls the “SEP - Delete Fingerprint List” function. The workflow deletes the selected fingerprint list. The user can determine if the command is successful by checking the Workflow status.

5.13. SEP - Get Command Status

Use the function to get the details of a command status from a command ID. It uses the following input parameters:

Name	Type	Required	Tooltip
sep_incident_id	number	Yes	Resilient incident ID.
sep_commandid	text	Yes	Command ID of SEP job.
sep_status_type	Text	Yes	Type of command status requested.
sep_matching_endpoint_ids	boolean	No	Get list of matching endpoints.
sep_order	text	No	Specifies whether the results are in ascending order (ASC) or descending order (DESC).
sep_pageindex	number	No	Index page that is used for the returned results. Default page index is 1.
sep_pagesize	number	No	Number of results to include on each page. Default is 20.
sep_sort	text	No	Column by which the results are sorted.

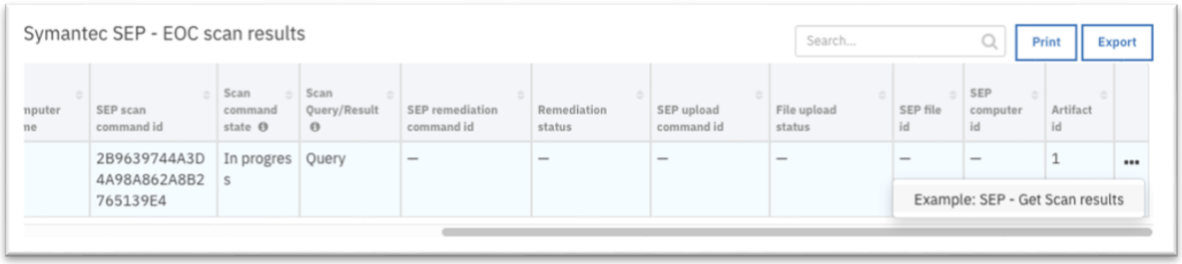
The input can be populated by the workflows, “Example: SEP - Get Scan results”, “Example: SEP - Get Remediation status”, “Example: SEP - Get Upload status”, and “Example: SEP - Get Quarantine status”.

The workflow, “Example: SEP - Get Scan results”, sets the function’s input fields:

- sep_scan_date is mapped to the scan date value from the selected data table row.
- sep_incident_id is mapped to the Resilient incident ID.
- sep_commandid is mapped to a command ID value from the selected data table row.
- sep_status_type is set to “scan”.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Scan results”.

1. Open an incident and select the “SEP – Threats" tab.
2. Select a target query row in data table “Symantec SEP - EOC scan result”.
3. From the selected row, click **Action-> Example: SEP - Get Scan results**.



If any matches have been discovered, new match rows are added to the data table.

Symantec SEP - EOC scan results

Search... Print Export

File path	Hash value	Computer name	SEP scan command id	Scan command state	Scan Query/Result	SEP remediation command id	Remediation status	SEP upload command id	File upload status	SEP file id	SEP computer id	Artifact id	
–	–	–	2B9639744A3D4A98A862A8B2765139E4	Completed	Query	–	–	–	–	–	–	1	•••
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-4OA0GKJN830	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	–	–	–	D31AA16E0946C25D40C83823C500518B	1	•••
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-N5KGH4CP3N3	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	–	–	–	89AD1BBB0946C25D25E6C0984E971D8A	1	•••

The new row(s) include the scan type, file path, hash value and Computer name of the matching endpoint.

The action can be re-run multiple times until the command either completes or times out waiting for all endpoints.

2019-07-04 13:06:51	QUICK	File Name	suspicious_exe.exe	–	–	–	32665A85C2DB4BCBBE927E761BBC9C4F	Timeout	Query	–

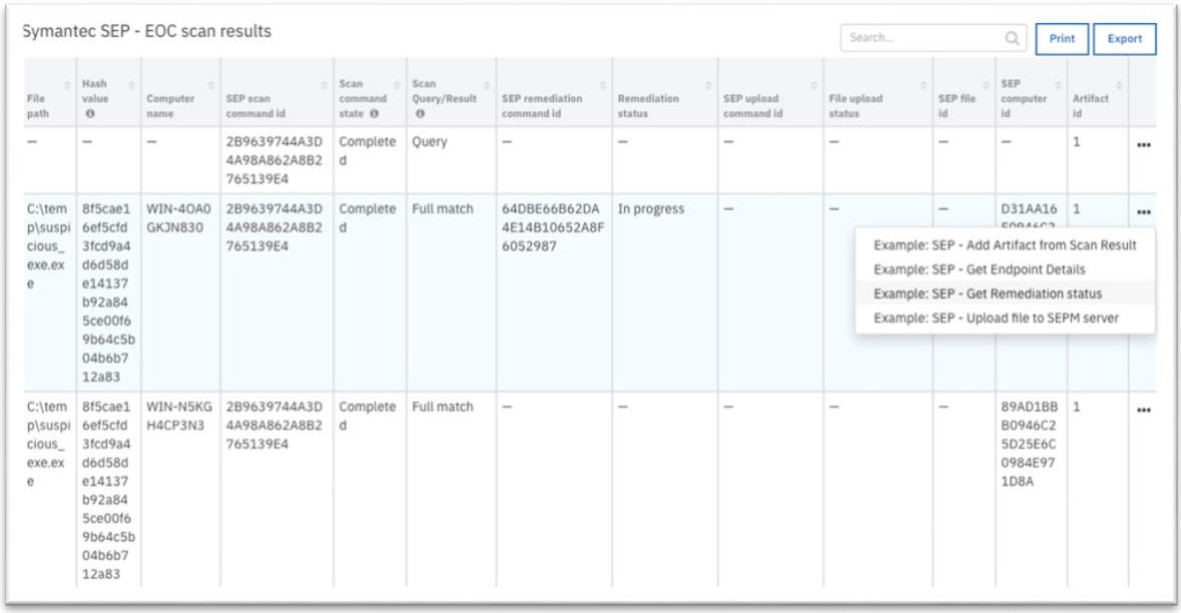
NOTE: If the action is re-run multiple times, the result may get added multiple times to the data table.

The workflow, “Example: SEP - Get Remediation status”, sets the function’s input fields:

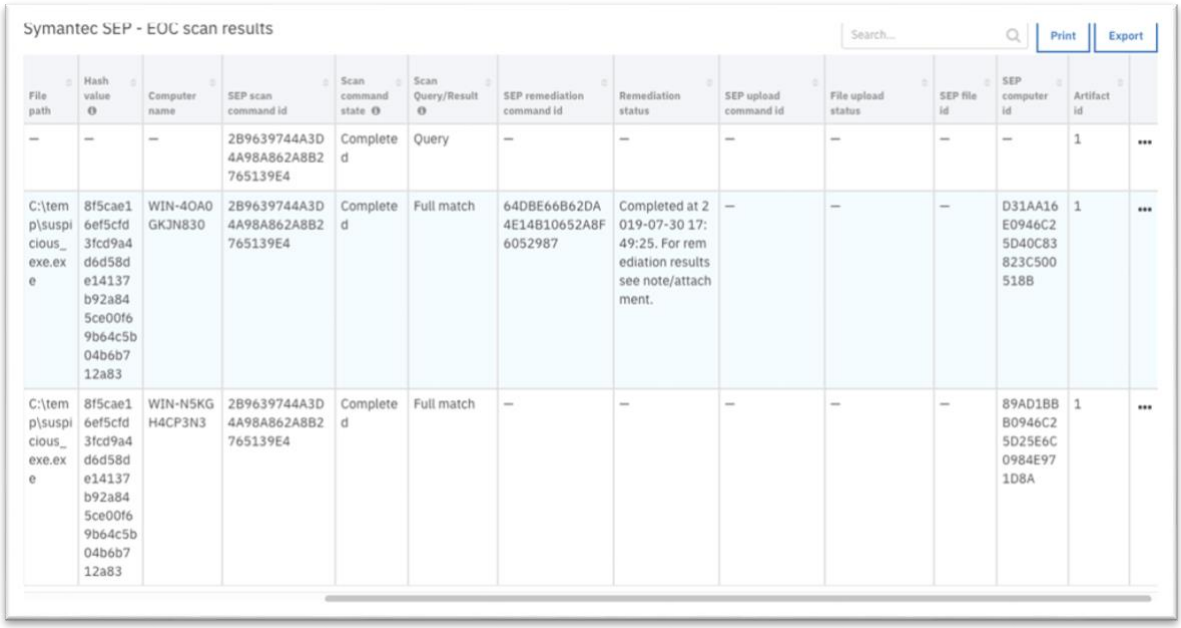
- sep_incident_id is mapped to the Resilient incident ID.
- sep_commandid is mapped to a command ID value from the selected data table row.
- sep_status_type is set to “remediation”.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Remediation status”.

1. Open an incident and select the “SEP – Threats" tab.
2. Select a target match row in data table “Symantec SEP - EOC scan result”.
3. From the selected row, click **Action-> Example: SEP - Get Remediation status**.



The “Remediation status” field is updated with the current action status.



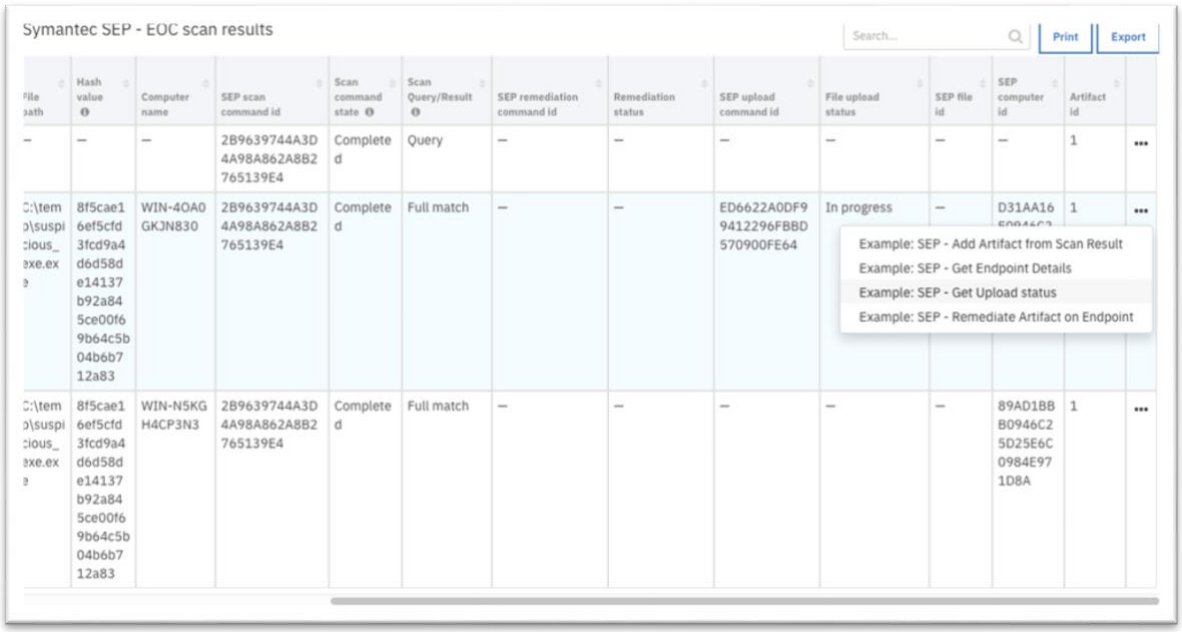
A CSV file attachment is added to the incident with details of all copies of the file matching the selected hash value which have been remediated/quarantined on the target endpoints.

The workflow, “Example: SEP - Get Upload status”, sets the function’s input fields:

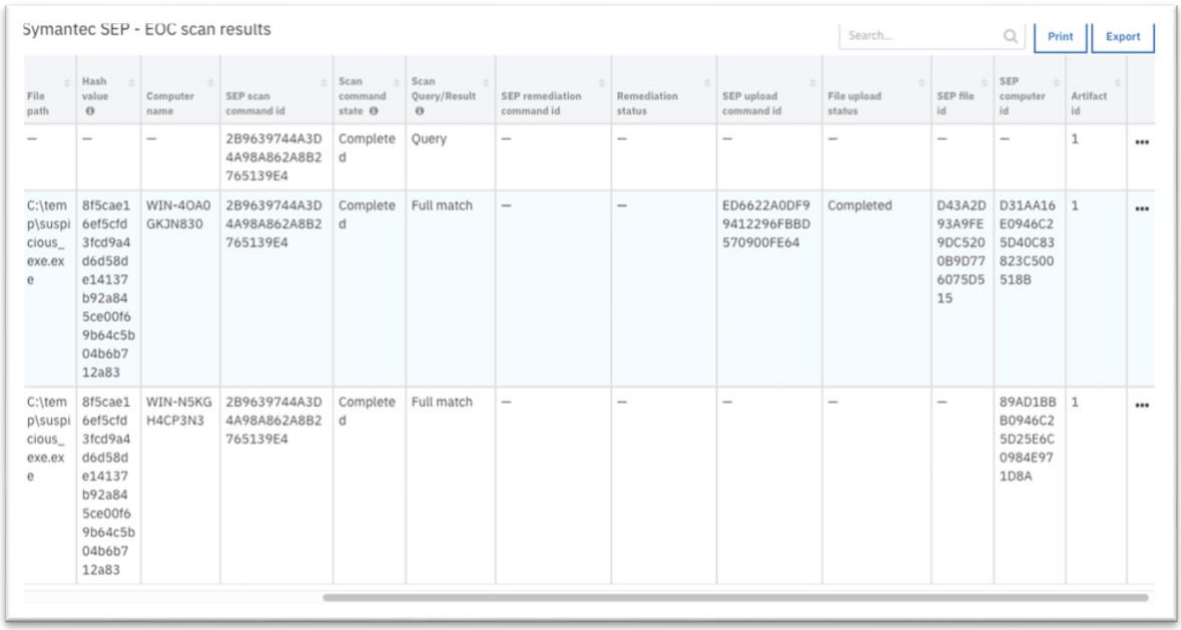
- sep_commandid is mapped to the command ID value from the selected data table row.
- sep_status_type is set to “upload”.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Upload status”.

1. Open an incident and select the “SEP – Threats" tab.
2. Select a target match row in data table “Symantec SEP - EOC scan result”.
3. From the selected row, click **Action-> Example: SEP - Get Upload status**.



If the upload is successful, the “File upload status” field is set to “Completed” and the “SEP file id” field is set to the uploaded file ID.



Symantec SEP - EOC scan results

File path	Hash value	Computer name	SEP scan command id	Scan command state	Scan Query/Result	SEP remediation command id	Remediation status	SEP upload command id	File upload status	SEP file id	SEP computer id	Artifact id
–	–	–	2B9639744A3D4A98A862A8B2765139E4	Completed	Query	–	–	–	–	–	–	1
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-4OA0GKJN830	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	ED6622A0DF9 9412296FBBD 570900FE64	Completed	D43A2D93A9FE9DC5200B9D776075D515	D31AA16E0946C25D40C83823C500518B	1
C:\temp\suspicious_exe.exe	8f5cae16ef5cfd3fcd9a4d6d58de14137b92a845ce00f69b64c5b04b6b712a83	WIN-N5KGH4CP3N3	2B9639744A3D4A98A862A8B2765139E4	Completed	Full match	–	–	–	–	–	89AD1BBB0946C25D25E6C0984E971D8A	1

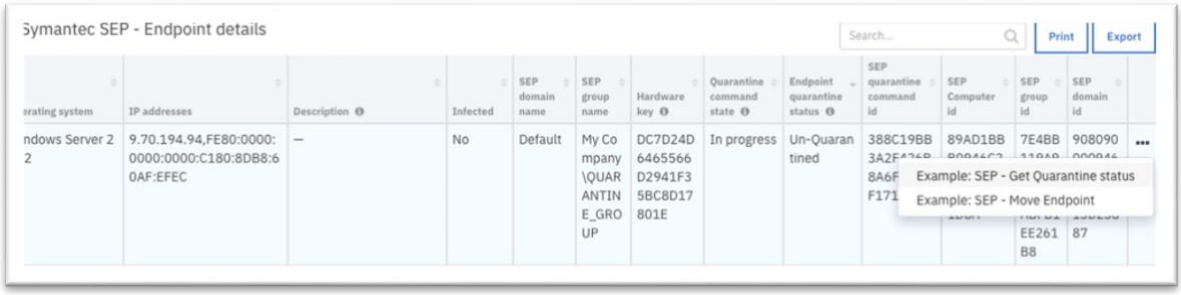
The workflow, “Example: SEP - Get Quarantine status”, sets the function’s input fields:

- sep_commandid is mapped to the command ID value from the selected data table row.
- sep_status_type is set to “quarantine”.
- None of the other fields are set.

The workflow is initiated by the rule, “Example: SEP - Get Quarantine status”.

The user is presented with a drop-down list of user defined fingerprint list names. The fingerprint list and group are expected to be in the same SEP domain. In the example, fingerprint list name “Blacklist” is selected.

1. Open an incident and select the “SEP – Threats" tab.
2. Select a target row in data table “Symantec SEP - Endpoint details”.
3. From the selected row, click **Action-> Example: SEP - Get Quarantine status**.



Symantec SEP - Endpoint details

erating system	IP addresses	Description	Infected	SEP domain name	SEP group name	Hardware key	Quarantine command state	Endpoint quarantine status	SEP quarantine command id	SEP Computer id	SEP group id	SEP domain id
ndows Server 2 2	9.70.194.94,FE80:0000:0000:0000:C180:8DB8:60AF:EFEC	–	No	Default	My Company \QUARANTINE_GROUP	DC7D24D6465566D2941F35BC8D17801E	In progress	Un-Quarantined	388C19BB3A2F 8A6F F171	89AD1BB	7E4BB EE261B8	908090 87

Example: SEP - Get Quarantine status
Example: SEP - Move Endpoint

The action can be re-run while the field “Quarantine command state” is in the “In progress” state.

5.14. SEP - Get Domains

Use the function to get a list of all accessible domains. It uses no input parameters.

This function is not the main function for any of the workflows, but it is used in a support role in a number of different workflows to get a domain ID from a domain name. Workflows that utilize this function include, “Example: SEP - Add Hash to Blacklist”, “Example: SEP - Delete Hash from Blacklist”, “Example: SEP - Get Blacklist information” and “Example: SEP - Get Groups information”.

6. Script description

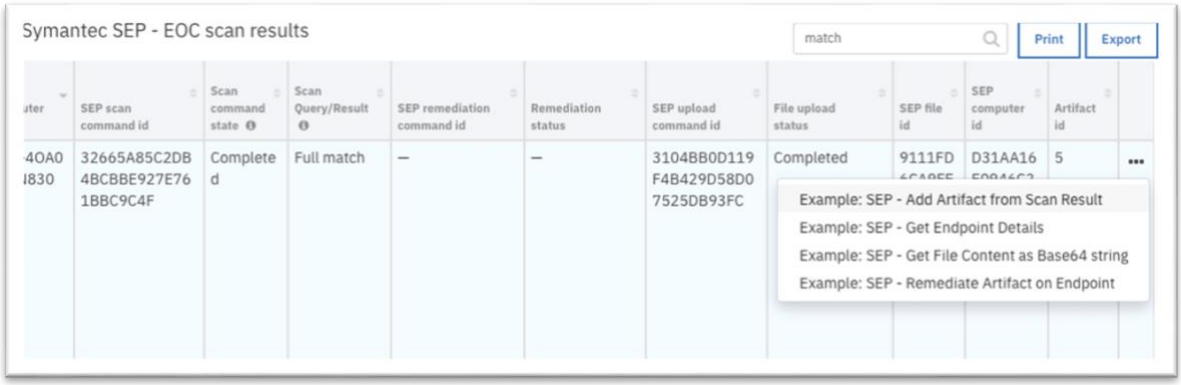
There is one script, scr_sep_add_artifact_from_scan_results.

The script adds a Resilient artifact from a property of a match in the 'Symantec SEP - EOC scan results' data-table.

Name	Type	Required	Tooltip
hash_value	text	Yes	Hash value of a matching artifact, typically SHA256.
computer_name	text	Yes	Computer name of a matching artifact.
file_path	Text	Yes	File path of a matching artifact.

The script is initiated by the rule, “Example: SEP - Add Artifact from Scan Result”.

1. Open an incident and select the “SEP – Threats" tab.
2. Select a target match row in data table “Symantec SEP - Endpoint details”.
3. From the selected row, click **Action-> Example: SEP - Add Artifact from Scan Result**.



The user is presented with a drop-down list of Resilient artifact types to add from the scan match. Select “Malware SHA-256 Hash”.

A new Resilient artifact is created in the target incident based on the matching row value.

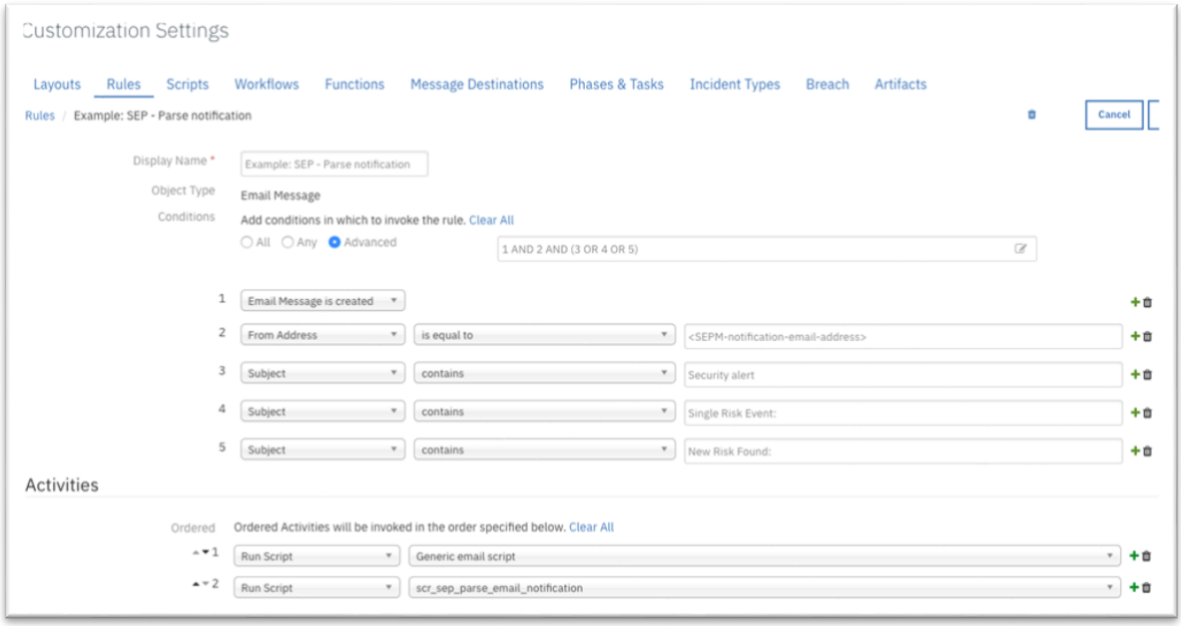
7. Notifications description

The package includes a rule and a script which can be used in conjunction with the “Generic Email Parsing Script” package to automatically parse email notifications of critical events from the SEPM. An incident is generated from the notification event which includes artifacts for suspect files and endpoint names.

7.1. Configuration

Out of the box, the rule is configured to parse emails with “Security alert”, “Single Risk Event:” and “New Risk Found:” in the subject.

NOTE: The user or administrator needs to configure the “From address” to point to the actual SEPM username that sends the notifications.



The SEPM user or administrator can add additional event types and update the example SEP parsing script if required. The following is an example of a generated email notification.

```
Subject: Single Risk Event: machine TEST-ENDPOINT infected with Trojan.Gen.NPE,
action Cleaned by deletion

At least one security risk found:

Risk name: Trojan.Gen.NPE
File path: C:\suspicious_exe.exe
Event time: Feb 28, 2019 3:40:12 AM
Database insert time: Feb 28, 2019 3:45:30 AM
Source: Real Time Scan
Description:
User: Administrator
Computer: TEST-ENDPOINT
IP Address: 192.168.194.94
Domain: Default
Server: SEPM-SERVER
Client Group: My Company\TEST_GROUP_1
Action taken on risk: Cleaned by deletion
```

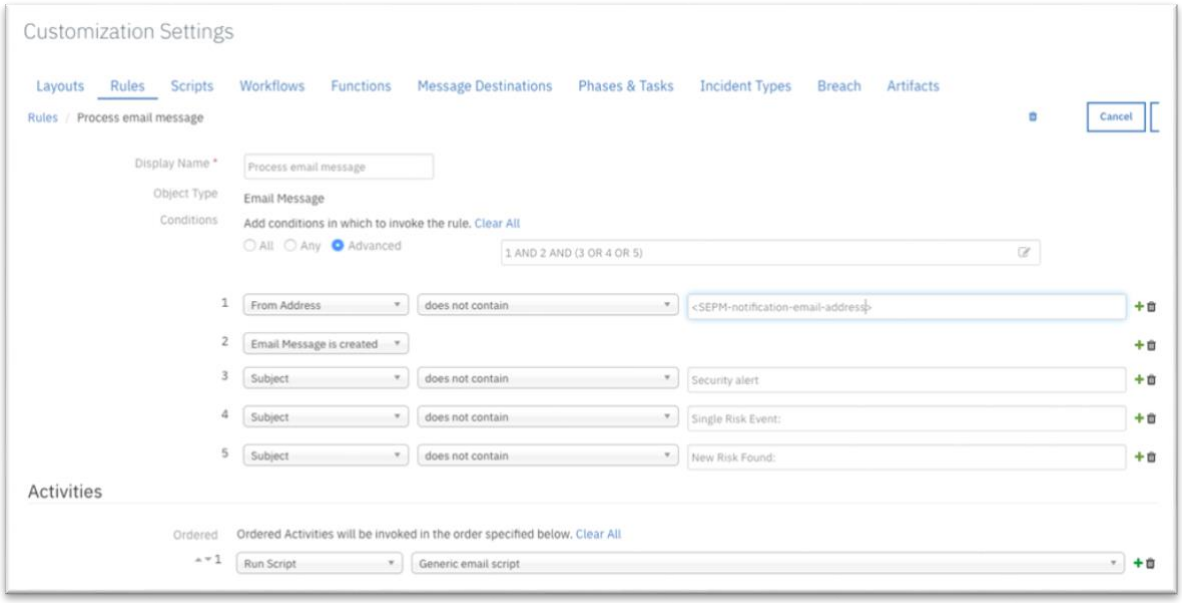
```
This alarm was generated at Feb 28, 2019 3:50:21 AM (Reporter host Time).
This alarm was generated by admin, with the following filters:
Domain: *
Group: *
Server: *
Computer: *
Risk name: *


Symantec Endpoint Protection detected a new risk on client computers. For
more information, see the Reports page, Quick Reports tab. Select the Risk
report type and run the "New Risks Detected in the Network" report.
```

The rule “Process email message” from the “Generic Email Parsing Script” package either needs to be deleted/disabled or else the rule conditions need to be altered to prevent interference with the example email processing rule supplied with the SEP integration.

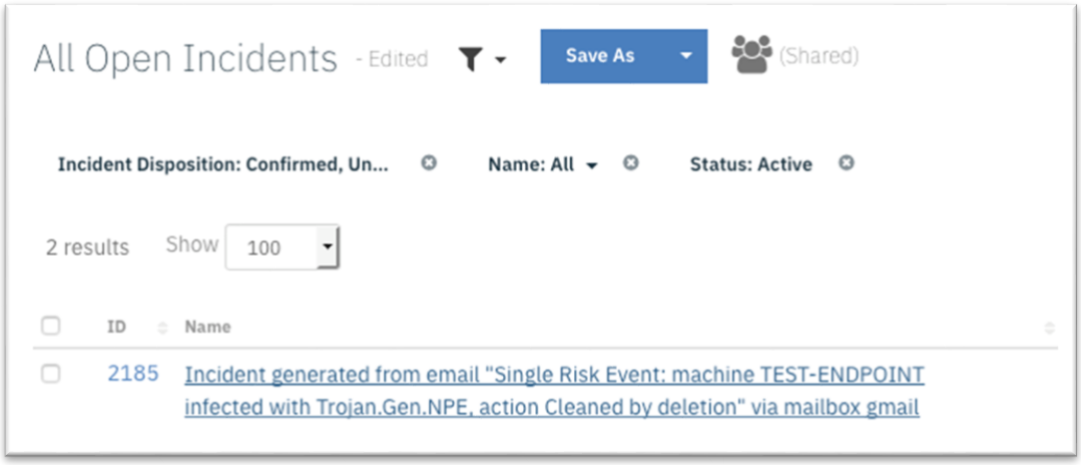
The following is an example where “Process email message” rule has had conditions added to prevent interference with example rule.

NOTE: The user or administrator needs to configure the “From address” to point to the actual SEPM username that sends the notifications.



7.2. Generic email script

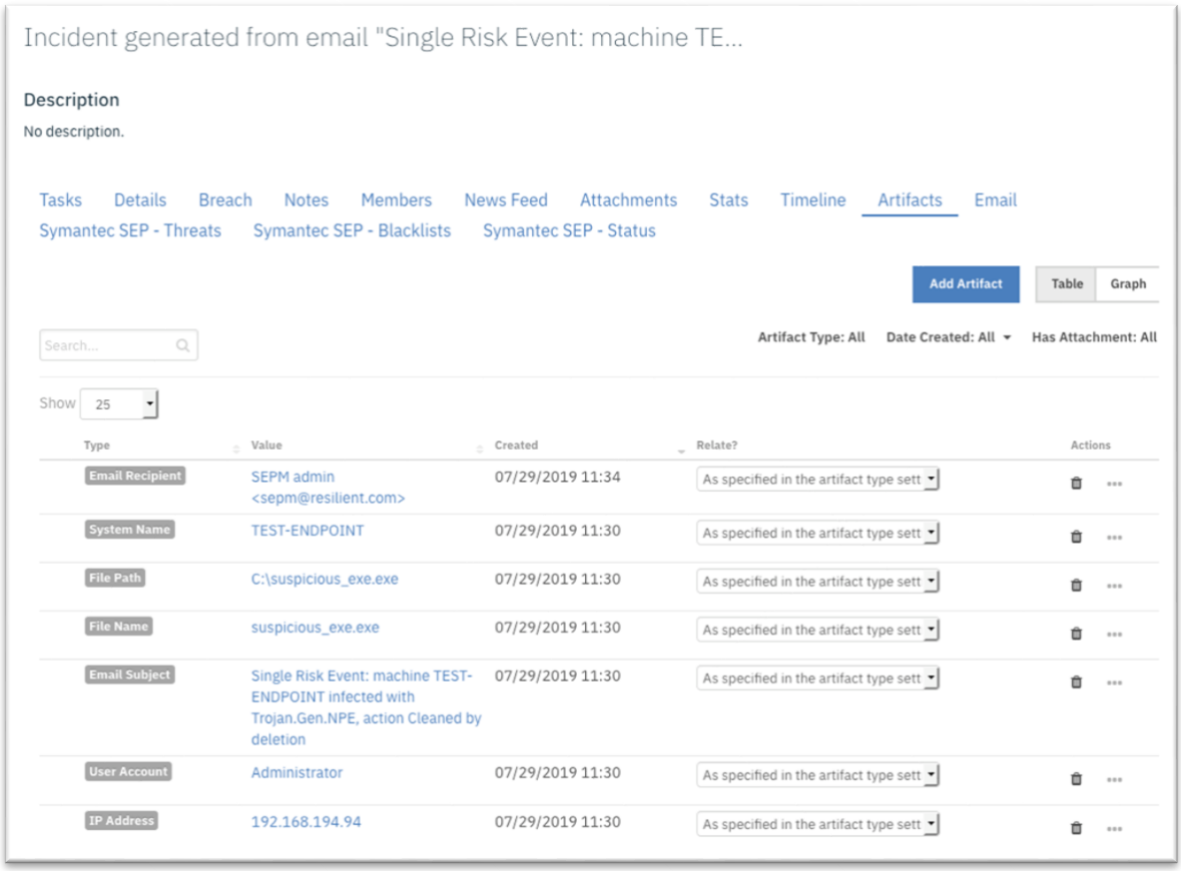
This script from the “Generic Email Parsing Script” package parses the notification email, generates a new incident for the notification details and adds basic artifacts.



A new incident is generated for the notification event.

7.3. Script – scr_sep_parse_email_notification

This script further parses the notification email for specific artifacts, such as a “File Path” or “File Name”, for the file that triggered the event, and a “System Name” artifact for the hostname where the event was raised. It adds the artifacts to the Resilient incident generated by the generic script.



These artifacts can be used to initiate lookups, scans, and remedial actions with Symantec Endpoint Protection or another 3rd party tool.

8. Configuring Symantec Endpoint Protection

Access to the Symantec Endpoint Protection Manager REST API is allowed by providing a username and password in the request.

Much of the integration functionality requires that the credentials map to a system administrator account on the SEPM.

A number of the functions, including “SEP - Quarantine Endpoints” and “SEP - Assign Fingerprint List to Group,” require that the administrator sets the appropriate policies on the SEPM to achieve an optimum outcome from the integration.